

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В.ЛОМОНОСОВА
ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ

На правах рукописи

Федотов Никита Егорович

**Применение информационных технологий в здравоохранении:
конституционно-правовые аспекты**

Специальность 5.1.2. Публично-правовые (государственно-правовые) науки

ДИССЕРТАЦИЯ

на соискание ученой степени
кандидата юридических наук

Научный руководитель:
доктор юридических наук,
доцент Шевердяев
Станислав Николаевич

Москва - 2026

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ	4
ГЛАВА 1. ФОРМИРОВАНИЕ СОВРЕМЕННОЙ МОДЕЛИ ПРАВОВОГО РЕГУЛИРОВАНИЯ ПРИМЕНЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ЗДРАВООХРАНЕНИИ	19
§ 1. Информационные технологии в сфере здравоохранения: правовая терминология, классификация и эволюция	19
§ 2. Международно-правовые стандарты защиты прав человека в области цифрового здравоохранения	34
§ 3. Основные зарубежные модели правового регулирования применения информационных технологий в здравоохранении	47
3.1. Рамочное правовое регулирование применения информационных технологий в сфере здравоохранения.....	54
3.2. Фрагментированное правовое регулирование вопросов здравоохранения в части применения информационных технологий.....	68
3.3. Специализированное правовое регулирование применения информационных технологий в сфере здравоохранения	84
ГЛАВА 2. КОНСТИТУЦИОННО-ПРАВОВЫЕ ОСНОВЫ ПРИМЕНЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ЗДРАВООХРАНЕНИИ НА СОВРЕМЕННОМ ЭТАПЕ В РОССИИ	97
§ 1. Конституционализация применения информационных технологий в сфере здравоохранения в Российской Федерации	97
§ 2. Особенности становления системных правовых основ применения информационных технологий в российском здравоохранении	111
2.1. Технологии обработки первичных данных	125
2.2. Технологии анализа больших данных	132
2.3. Технологии Интернета вещей.....	145
2.4. Технологии искусственного интеллекта	158
2.5. Телемедицинские технологии.....	176

§ 3. Проблемы реализации отдельных конституционных прав человека в России в условиях применения информационных технологий в здравоохранении	185
3.1. Конституционное право на охрану здоровья и медицинскую помощь	189
3.2. Конституционное право на доступ к информации.....	213
3.3. Конституционное право на неприкосновенность частной жизни.....	226
ЗАКЛЮЧЕНИЕ	245
СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ	251

ВВЕДЕНИЕ

Актуальность темы исследования.

В настоящее время в России проводится политика цифровизации, которая играет важную роль в совершенствовании деятельности в сфере здравоохранения. При наличии соответствующих условий она обеспечивает более высокое качество профилактики, диагностики, лечения и поддержки здоровья граждан. Пандемия COVID-19, развитие информационных технологий, широкое распространение практики сбора информации о здоровье граждан определили существующие ограничения и пробелы в обеспечении соблюдения конституционных прав в области здравоохранения. Даже хорошо развитые системы здравоохранения в передовых зарубежных государствах сталкиваются с беспрецедентными проблемами, вызванными демографическими, эпидемиологическими и медицинскими изменениями. Здравоохранение должно воспользоваться преимуществами новых информационных технологий, способных повысить возможности профилактики, диагностики и лечения заболеваний.

Бурное развитие информационных технологий непосредственно затрагивает конституционные права и свободы человека, а также публичные интересы, что отражается в законодательстве. Российская правовая дискуссия относительно конституционализации применения информационных технологий в сфере здравоохранения в настоящее время актуализируется еще больше в силу того, что в результате конституционной реформы 2020 года в тексте Конституции Российской Федерации был закреплен термин «информационные технологии» (пункт «и» статьи 71 Конституции Российской Федерации). Кроме того, признано, что в исключительном ведении Российской Федерации находится обеспечение безопасности личности, общества и государства при применении информационных технологий и обороте цифровых данных (пункт «м» статьи 71 Конституции Российской Федерации). Данное обстоятельство придает более очевидную конституционно-правовую значимость проблемам, возникающим при применении

информационных технологий в здравоохранении, среди которых выделяют вопросы защиты и соблюдения права на охрану здоровья и медицинскую помощь, права на доступ к информации, права на неприкосновенность частной жизни и надлежащей их реализации в условиях цифровизации здравоохранения.

В связи с этим обеспечение надлежащего осуществления конституционных прав граждан может быть определено как основное соображение для внедрения информационных технологий в сферу здравоохранения. Решение указанных проблем становится приоритетным стратегическим направлением конституционно-правового регулирования применения информационных технологий в здравоохранении, поскольку нормативно-правовая база в России отстает от развития информационных технологий. Отсутствие в законодательстве России в сфере здравоохранения четких и последовательных концептуальных подходов к регулированию применения информационных технологий препятствует эффективному разрешению возникающих в практике проблем, что повышает значимость обращения к передовому зарубежному опыту и подготовки соответствующих изменений в отечественное законодательство.

Степень научной разработанности темы исследования.

Выбранная тема исследования относится в современной юридической науке к числу наиболее актуальных направлений. Проблемам защиты прав человека и обеспечения их соблюдения в условиях применения информационных технологий в здравоохранении в развитых странах уделяется значительное внимание в научной доктрине, в законодательстве, а также в судебной практике. Исследуемая тема носит межотраслевой характер и является не разработанной в России в достаточной степени.

Среди отечественных ученых, которые исследовали разновидности информационных технологий и разрабатывали проблему их классификации, следует выделить А.А. Амадаева, И.Л. Бачило, А.Б. Венгерова, В.Н. Волкову, Н.Н. Ковалеву, Г.М. Киселева, К.К. Костоломову, В.Н. Лопатина, И.И. Начхоева, И.О. Несмиянову, Т.А. Николенко, А.Г. Пронкину, И.В. Свищеву, М.А. Федотова и др.

Зарубежный опыт правового регулирования информационных технологий в здравоохранении анализировался с привлечением работ иностранных ученых: П. Аннамараджу, Ж. Вэя, М. Зохара, Ф.В. Ли, А. Мантелеро, М.М. Мелло, К. Сингхала, Х. Цай, Х.В. Чунга, Х. Ши, П.Ф. Эдемеконга и др.

В исследовании проблем реализации права на неприкосновенность частной жизни в условиях применения информационных технологий диссертантом были использованы работы С.Н. Алямкина, П.П. Баранова, А.Р. Белова, Л.А. Бердегуловой, Г. Е. Волковой, А.А. Карцхия, А.В. Пресняковой, А.А. Троицкой, А.С. Федосина и др. При изучении проблем реализации права на охрану здоровья и медицинскую помощь автор опирался на работы С.С. Алексеевой, И. Р. Бегишева, Т.В. Заметиной, Т.А. Ковелиной, В.М. Марухно, Е.С. Лисицыной, М. А. Липчанской, В.В. Пучковой, М.Э. Стародубцева, Е.В. Юдина. В части исследования проблем реализации права на доступ к информации – И.М. Акулина, Г.Г. Камаловой, С.Ю. Лапина, Р.А. Осипова, Т.А. Поляковой, Р.А. Преснякова, О.В. Романовской, Г.Б. Романовского, Е.А. Чесноковой, С.Н. Шевердяева.

В работах таких авторов, как С.А. Авакьян, Т.Ю. Архирейская, Н.С. Бондарь, И.В. Гончаров, А.Г. Дейнеко, И.А. Кравец, Е.В. Киричек, М.А. Липчанская, А.С. Лолаева, В.В. Петроченков, И.А. Умнова-Конюхова, Я.К. Чепенко, Ю.А. Чернышева, Д.И. Шокина отражен характер цифровизации и ее влияние на конституционное право, а также на права и свободы граждан.

Научной базой для диссертации явились также труды таких исследователей, изучавших различные аспекты конституционно-правового регулирования информационных технологий в здравоохранении, как Е.И. Аксенова, И.В. Балтутите, В.С. Буланова, С.Ю. Горбатов, А.О. Иншакова, А.Ю. Киселева, М.А. Коваленко, А.С. Купцова, М.А. Лапина, И.С. Сушильников, И.А. Филипова, А.А. Шутова и др.

В рамках публично-правовой научной специальности, в том числе конституционно-правовой, близкие вопросы в последние годы изучались в работах Я.В. Акимцевой через призму биомедицинских исследований на человеке; А.А.

Громова разрабатывала вопросы реализации конституционного права на охрану здоровья и медицинскую помощь в условиях применения биомедицинских технологий в Российской Федерации.

Вместе с тем стоит отметить, что системные научные исследования, посвященные собственно конституционно-правовому регулированию применения информационных технологий в здравоохранении, отсутствуют.

Объектом диссертационного исследования являются конституционно-правовые отношения и нормы, складывающиеся в сфере здравоохранения и связанные с применением информационных технологий, а также отечественная и зарубежная научная доктрина в этой области.

Предметом диссертационного исследования являются современные модели и методы конституционно-правового регулирования применения информационных технологий в здравоохранении, а также механизмы их воздействия на систему управления здравоохранением и на реализацию конституционных прав в условиях цифровизации.

Цель диссертационного исследования заключается в установлении наиболее актуальных конституционно-правовых аспектов применения информационных технологий в сфере здравоохранения для выработки научного обоснования эффективных правовых гарантий конституционных прав человека в данной области и совершенствования концепции развития соответствующего отечественного законодательства.

Задачи диссертационного исследования для достижения указанной цели:

- определить виды информационных технологий, используемых в здравоохранении;
- установить конституционно-правовые аспекты применения информационных технологий в сфере здравоохранения в России;
- выявить преимущества и недостатки правового регулирования применения информационных технологий в сфере здравоохранения в законодательстве передовых зарубежных стран (США, ЕС, КНР);

- определить текущие проблемы реализации конституционного права на неприкосновенность частной жизни, на охрану здоровья и медицинскую помощь, на доступ к информации в условиях применения информационных технологий в здравоохранении и оценить риски их нарушения;

- разработать предложения по решению выявленных проблем реализации вышеуказанных прав граждан в условиях применения информационных технологий в здравоохранении;

- определить наиболее перспективные для России направления совершенствования правового регулирования применения искусственного интеллекта, технологий Интернета вещей в здравоохранении на основе зарубежного опыта.

Теоретическую основу исследования составили труды отечественных и зарубежных исследователей в области конституционного, информационного и медицинского, административного права: диссертационные исследования, авторефераты, монографии, научные статьи, учебная и учебно-методическая литература и др.

Методологическая основа диссертационного исследования состоит из комплекса методов научного познания: общенаучных, а также частно-научных методов, включая сравнительно-правовой метод, формально-юридический метод.

Метод анализа использован при рассмотрении существующих определений основных понятий исследования, в частности, «информационные технологии», «конституционализация», «технологии Интернета вещей» и др., а также теоретических и практических подходов в вопросе о влиянии информационных технологий на реализацию конституционных прав человека.

Синтез применен для формирования целостной картины конституционно-правового регулирования применения информационных технологий в здравоохранении, обобщения выводов по отдельным проблемам нарушения конституционных прав человека при применении информационных технологий и разработки комплексных предложений по их разрешению.

Большое значение в рамках исследования имеет метод классификации, позволивший обобщить доктринальные источники о разновидностях информационных технологий.

Метод правового моделирования применяется для разработки подхода к регулированию применения искусственного интеллекта и конкретных предложений по совершенствованию законодательства в области применения информационных технологий в здравоохранении и механизмов защиты прав в условиях цифровизации здравоохранения.

Благодаря системному методу показана взаимосвязь лежащих в основе отношений в области применения информационных технологий в здравоохранении конституционных принципов. Системный метод позволил рассмотреть конституционно-правовое регулирование применения информационных технологий в здравоохранении как целостную, динамическую систему, элементы которой (нормы, правоотношения, правовые институты) находятся во взаимодействии с внешней средой (технологическим прогрессом, социальными вызовами, зарубежным опытом). В рамках данного подхода особое значение придается выявлению системных противоречий и пробелов в регулировании.

Метод индукции позволил сделать ряд обобщающих выводов в отношении исследуемых конституционно-правовых отношений в сфере правового регулирования информационных технологий в здравоохранении.

С помощью сравнительно-правового метода выявлены преимущества и недостатки правового регулирования применения информационных технологий в здравоохранении в зарубежных странах. Его использование также позволяет установить какие из норм, уже разработанных в зарубежном законодательстве, могут быть использованы в исследовании, ориентированном на отечественную правовую действительность.

Формально-юридический метод позволил выявить противоречия и пробелы в правовом регулировании применения информационных технологий в

здравоохранении и правоприменительной практике, выявить взаимосвязь между моделями государств, регулирующими применение информационных технологий в здравоохранении, содержание исследуемых отечественных и зарубежных нормативных правовых актов в указанной области. Также он применяется для анализа конституционных основ применения информационных технологий в здравоохранении в России и для изучения связанных с ним конституционных принципов – равноправия, защиты достоинства личности и прав человека и гражданина, свободы экономической деятельности и автономии личности.

Нормативной основой диссертационного исследования являются Конституция Российской Федерации, международные акты, федеральные законы, подзаконные акты Российской Федерации, конституционные акты зарубежных стран, законы, подзаконные акты и иные нормативные правовые акты зарубежных стран.

Эмпирическую основу диссертационного исследования составили решения Конституционного Суда Российской Федерации, Европейского суда по правам человека и судебных органов зарубежных стран, статистические доклады о состоянии информационных технологий в Российской Федерации и в мире, данные из доступных в сети Интернет докладов и иных источников о фактах общественной жизни относительно последствий влияния информационных технологий в здравоохранении, а также сведения о результатах регулирования применения отдельных видов информационных технологий в России.

Научная новизна диссертационного исследования определяется тематикой научного исследования, его предметом и кругом анализируемых проблем, связанных с применением информационных технологий в здравоохранении, недостаточной разработанностью отдельных научных направлений в области применения информационных технологий в здравоохранении.

Автором исследуются конституционно-правовые аспекты применения информационных технологий в сфере здравоохранения и их влияние на

реализацию основных конституционных прав человека.

Значимость исследования заключается в том, что в нем выявляется характер конституционализации применения информационных технологий в здравоохранении, а также формируется системное представление о том, как цифровизация влияет в настоящее время на общественные отношения в области здравоохранения. Многие имеющиеся научные исследования в основном сосредоточены на правовых последствиях применения телемедицинских технологий и искусственного интеллекта либо вообще не рассматривают современные виды информационных технологий в здравоохранении, поэтому целесообразным представляется использовать междисциплинарный подход к изучению применения информационных технологий в здравоохранении.

На основе анализа теоретических и практических проблем в части нарушения отдельных конституционных прав человека в условиях цифровизации здравоохранения и конституционно-правового регулирования применения информационных технологий сформулированы актуальные и научно обоснованные предложения по их разрешению с учетом опыта зарубежных стран, которые позволят усовершенствовать отечественное законодательство.

Наиболее существенные результаты, отражающие научную новизну диссертационного исследования, содержатся в следующих **положениях, выносимых на защиту:**

1. Существующие в российской научной юридической литературе классификации информационных технологий не основываются на критериях, которые позволяли бы дифференцировать информационные технологии по степени их воздействия на конституционные права человека и публично-правовые механизмы управления здравоохранением. Восполнение указанного пробела осуществлено в работе за счет установления соответствующих видов информационных технологий, выделенных на базе критерия их функциональной направленности на управление медицинской информацией и взаимодействие с пациентами.

2. Конституционные поправки 2020 года (пункты «и» и «м» статьи 71 Конституции Российской Федерации) привели к формальной конституционализации применения информационных технологий в здравоохранении, которая требует трансформации механизмов реализации целого ряда конституционных прав и свобод. Закрепление информационных технологий в исключительном ведении Российской Федерации явилось необходимостью, вызванной существовавшей в субъектах Российской Федерации противоречивой и непоследовательной практикой регулирования применения информационных технологий в здравоохранении. Поэтому новая редакция пункта «м» статьи 71 Конституции Российской Федерации накладывает на федеральные органы власти соответствующие обязательства по развитию текущего законодательства в этой области.

Однако это привело к противоречию, связанному с сохраняющимся отставанием российского законодательства от технологических реалий. Данное противоречие выражается в отсутствии единых концептуальных подходов, что порождает правовые пробелы, коллизии в регулировании применения актуальных информационных технологий и неадекватные механизмы защиты конституционных прав граждан в условиях цифровизации здравоохранения. Для преодоления этого противоречия требуется не просто точечное совершенствование норм, а разработка концепции, которая, основываясь на конституционных принципах, установит четкие правовые основы, гарантии и баланс публичных и частных интересов при применении информационных технологий в сфере здравоохранения.

3. Концепция развития законодательства о применении информационных технологий в здравоохранении должна предусматривать специальные правовые гарантии об информированном добровольном согласии на применение искусственного интеллекта в здравоохранении. Исходя из принципа автономии пациента, любой медицинский работник, желающий применять искусственный интеллект для оказания услуг в области медицинской помощи, должен сообщать

своим пациентам о таком намерении и предоставлять им возможность выразить согласие или отказ на применение искусственного интеллекта.

4. Предложенная концепция совершенствования российского законодательства в сфере применения технологий Интернета вещей (Internet of Things, IoT) в здравоохранении, направленная на комплексное снижение рисков нарушения прав пациентов, включает в себя:

1) создание системы правовых гарантий, касающихся сбора личной информации, который должен быть ограничен минимальным объемом для целей обработки при недопущении чрезмерного сбора личной информации с последующей разработкой специального нормативного руководства, чтобы определить, какие типы данных считаются необходимыми для медицинских приложений, в результате чего любые попытки сбора личной информации за пределами установленного объема могут быть признаны незаконными;

2) закрепление за субъектом персональных данных права выразить предварительное и явное согласие или отказ на любую коммерческую передачу третьим лицам его медицинских данных, собранных с использованием технологии Интернета вещей, что обеспечит необходимый уровень прозрачности и контроля со стороны пациента за дальнейшим использованием своей информации и исключит практику ее несанкционированной монетизации;

3) установление в отношении производителей устройств на базе технологий Интернета вещей для минимизации технических рисков при использовании данных технологий в медицинских целях обязательных требований по внедрению встроенных средств информационной защиты, проведению аудита информационной безопасности и информированию потребителей о функциональных возможностях и уязвимостях устройств через систему стандартизированной маркировки.

5. Действующее правовое регулирование в части применения телемедицинских технологий в Российской Федерации содержит критический пробел, выражающийся в отсутствии адекватных механизмов защиты врачебной

тайны, что приводит к системной уязвимости конфиденциальных сведений о пациентах и требует незамедлительного решения путем разработки в отечественном законодательстве комплексных организационно-правовых стандартов информационной безопасности, основанных на принципе доверительного характера взаимодействия пациента и врача при применении телемедицинских технологий, включая установление обязанности поставщиков телемедицинских услуг по уведомлению пациентов об условиях обработки их персональных данных.

6. Для гарантирования конституционного права на неприкосновенность частной жизни при применении информационных технологий в здравоохранении требуется создание организационно-правовой и программной среды, которая обеспечивает возможность пациентов эффективно контролировать и ограничивать доступ третьих лиц к разделам своей электронной медицинской карты (ЭМК) для различных категорий пользователей (медицинских работников, административных сотрудников, иных третьих лиц), исходя из принципа законного интереса.

Кроме того, во избежание дискриминации граждан по месту их жительства (ч. 2 ст. 19 Конституции РФ) и для гарантирования конституционного права на доступ к информации, а также принципа равенства требуется обеспечить единые федеральные стандарты персонализированной модели ЭМК в рамках обеспечения для всех граждан права на добровольное самостоятельное внесение данных о показателях здоровья в ЭМК.

7. Внедрение в России Единой государственной информационной системы здравоохранения (ЕГИСЗ) привело к повышению риска несанкционированного распространения информации ограниченного доступа при обмене медицинскими данными пациентов между операторами различных информационных систем. Во избежание ущемления конституционного права на неприкосновенность частной жизни требуется предусмотреть обязанность операторов соответствующих информационных систем запрашивать согласие или отказ граждан на передачу чувствительной для них медицинской информации.

8. В России действует процедура государственной регистрации медицинских изделий, однако не выработаны критерии, которые позволят отличить такие устройства, как фитнес-браслеты, смарт-часы, портативные приборы и иные носимые устройства фиксации данных о состоянии здоровья от прочих медицинских изделий в случае, если они имеют медицинскую основу и могут использоваться для принятия клинических решений. Правовое отграничение подобных устройств на базе технологий Интернета вещей от прочих медицинских изделий должно основываться на функциональном критерии – способности устройства содержать медицинский контент и быть направленным на оказание медицинской помощи и принятия клинических решений, независимо от его потребительского формата. Это влечет необходимость разработки специальной правовой процедуры, позволяющей дифференцировать медицинские функции устройств и все иные их функции в условиях конвергенции технических возможностей таких устройств, включая следующие стадии: 1) анализ заявленного производителем медицинского назначения устройства; 2) оценка фактической способности диагностировать, мониторить, лечить заболевания или модифицировать физиологические функции человека; 3) проверка нацеленности устройства на оказание медицинской помощи.

9. В основе правового регулирования искусственного интеллекта (ИИ) в здравоохранении должна лежать регулятивная модель, интегрирующая, с одной стороны, риск-ориентированный подход, предусматривающий классификацию систем ИИ по уровням потенциального вреда — от неприемлемого до минимального риска — с установлением дифференцированных требований к каждому классу, а с другой стороны, принцип прозрачности алгоритмов. Данная модель обеспечивает системное единство частных и публичных интересов, поскольку предусматривает не только отсутствие избыточных требований для низкорисковых устройств, но и установление жестких требований к тем устройствам, от которых зависит жизнь и здоровье пациента, а также гарантирует реализацию права пациента на содержательное разъяснение автоматизированных

решений.

Теоретическая значимость диссертационного исследования выражается в научной проработке основных проблем, касающихся применения информационных технологий в здравоохранения и их влияния на реализацию гражданами конституционных прав. Диссертант вносит вклад в изучение конституционализации применения информационных технологий в сфере здравоохранения, а также в развитие научных представлений о совершенствовании концепции дальнейшего развития действующей нормативной правовой базы России в этой области.

Выводы и предложения диссертанта могут быть использованы в дальнейших научных исследованиях вопросов, связанных с применением информационных технологий в здравоохранении.

Практическая значимость диссертационного исследования заключается в выявлении и обобщении наиболее актуальных проблем, связанных с правовым регулированием применения информационных технологий, а также с соблюдением отдельных прав граждан Российской Федерации в текущих условиях цифровизации здравоохранения. С практической точки зрения изложенные в диссертации предложения имеют значение для совершенствования отечественного законодательства, закрепляющего гарантии права граждан на неприкосновенность частной жизни, права на охрану здоровья и медицинскую помощь, права на доступ к информации, а также могут быть учтены российскими органами власти при выработке как системных, так и прикладных правотворческих решений, направленных на регулирование применения информационных технологий в сфере здравоохранения.

Основные положения диссертационного исследования также могут быть использованы при подготовке учебных изданий по конституционному, административному, информационному и медицинскому праву. Результаты исследования представляются значимыми для включения в учебные курсы и использования в разработке методических пособий для обучающихся по

юридическим специальностям.

Личный вклад автора заключается в самостоятельном выполнении диссертационного исследования и выработке выносимых на защиту положений.

Достоверность результатов исследования обеспечивается совокупностью примененных методов исследования, которые позволили рассмотреть конституционно-правовые аспекты применения информационных технологий в здравоохранении, выявить системные связи и закономерности их развития. Также достоверность определяется всесторонним изучением доктринальных источников, судебной практики и нормативных правовых актов России и ведущих зарубежных стран в части регулирования применения информационных технологий в здравоохранении. Кроме того, достоверность результатов подтверждается их апробацией.

Апробация результатов диссертационного исследования.

Диссертация подготовлена на кафедре конституционного и муниципального права юридического факультета Московского государственного университета имени М.В. Ломоносова.

Основные выводы и положения исследования отражены в четырех научных статьях, опубликованных в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности и отрасли наук.

Кроме того, основные положения диссертационного исследования были представлены на следующих научных конференциях:

1) в декабре 2022 г. - на Международной научно-практической аспирантской конференции памяти В.Ф. Яковлева "Межотраслевой подход в юридической науке: Экономика. Право. Суд", РАНХИГС (доклад на тему «Текущее состояние правового регулирования экспериментальной телемедицины в РФ и зарубежных странах»);

2) в октябре 2022 г. - на Всероссийской научно-практической конференции «Становление и развитие института Уполномоченного по правам человека в Республике Саха (Якутия)», СВФУ им. М.К. Аммосова (доклад на тему «Правовой

анализ современного законодательства РФ в области защиты права на охрану здоровья и медицинскую помощь»);

3) в сентябре 2023 г. - на Всероссийской научно-практической конференции «Конституционные основы отраслевого нормотворчества: проблемы теории и практики», посвященная 30-летию Конституции Российской Федерации, СВФУ им. М.К. Аммосова (доклад на тему «Роль конституционного права в правовом регулировании информационных технологий в здравоохранении»);

4) в апреле 2023 г. - на Международной научной конференции студентов, аспирантов и молодых учёных «Ломоносов-2023», МГУ имени М.В. Ломоносова (доклад на тему «Опыт правового регулирования телемедицинских технологий в России, Франции и США»).

Структура диссертационного исследования включает в себя введение, две главы, шесть параграфов, заключение, список использованной литературы.

ГЛАВА 1. ФОРМИРОВАНИЕ СОВРЕМЕННОЙ МОДЕЛИ ПРАВОВОГО РЕГУЛИРОВАНИЯ ПРИМЕНЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ЗДРАВООХРАНЕНИИ

§ 1. Информационные технологии в сфере здравоохранения: правовая терминология, классификация и эволюция

В настоящее время процесс цифровизации приобрел глобальный масштаб, а информационные технологии активно внедряются в различные сферы общественных отношений. Поскольку информационные технологии тесно связаны с реализацией прав человека и непосредственно влияют на общественные отношения, возникающие в связи с их применением правовые системы разных стран оказались перед необходимостью регулирования принципиально новых общественных отношений, порожденных цифровой эпохой, поэтому обоснованным представляется стремление законодательных органов нормативно определить понятие информационных технологий и регламентировать процедуру применения информационных технологий в контексте прав человека.

На данный момент в России осуществляется трансформация права в связи с цифровизацией и развитием информационных технологий. Актуальным становится вопрос конкретизации новых терминов и понятий, охватывающих новые технологические процедуры и имеющих правовое значение, который поднимал еще А.Б. Венгеров. Упорядочение дефиниций в законодательстве государства в связи с внедрением информационных технологий в разные сферы жизнедеятельности является продиктованной цифровизацией необходимостью. Как отмечал вышеуказанный ученый, это позволит усовершенствовать правоприменительную деятельность во избежание разногласий относительно того или иного понимания новой терминологии и неоправданного расширительного (либо ограничительного) толкования технических понятий, имеющих правовое

значение¹. В дополнение к указанному мнению И.Л. Бачило подчеркнула следующее: «Широкое использование новых технологий позволяет сделать выводы о работе с понятийным аппаратом, а анализ законодательства, базирующийся на институциональном подходе, — уточнить предметные области информационной сферы, установить назначение правовых институтов»².

Сфера здравоохранения является одной из главных социальных сфер, поскольку благодаря ей создаются условия для повышения доступности и качества медицинской помощи, в результате чего реализуется право граждан на охрану здоровья и медицинскую помощь. В целях развития здравоохранения осуществляется разработка и внедрение информационных технологий. Совершенствование технологий закономерно ведет к росту затрат на здравоохранение – «становится ясно, что есть медицинские технологии, которые все более предсказуемо обеспечивают ожидаемый эффект»³. Действительно, как отмечается Минздравом России, в 2023 году в 85 субъектах Российской Федерации было внедрено 106 медицинских изделий с искусственным интеллектом. Общий объем расходов бюджетных средств на развитие искусственного интеллекта в здравоохранении увеличится «с 4,9 млрд долларов от 2020 года до 45,2 млрд долларов к 2026 году»⁴.

Перспективы развития здравоохранения связаны с масштабированием и внедрением новых видов информационных технологий, таких как технологии анализа больших данных, технологии Интернета вещей и других. Данный тезис

¹ Венгеров А. Б. Научно-технический прогресс и применение права // Правоведение : научный журнал. 1983. № 3. С. 21—28.

² Бачило И. Л. Понятийный аппарат информационного права и система обеспечения информационной безопасности // Труды Института государства и права Российской академии наук. 2016. № 3 (55). С. 5-16.

³ Разговор с экспертом: «Здравоохранение – самая ресурсоемкая отрасль из всех отраслей социальной сферы». URL: <https://mednet.ru/novosti/razgovor-s-ekspertom-zdravooxranenie-%E2%80%93-samaya-resursoemkaya-otrasl-iz-vsex-otraslej-soczialnoj-sferyi> (дата обращения: 15.08.2024)

⁴ Цифровизацию и технологии искусственного интеллекта обсудят на Форуме будущих технологий. URL: <https://minzdrav.gov.ru/news/2024/02/10/20871-tsifrovizatsiyu-i-tehnologii-iskusstvennogo-intellekta-obsudyat-na-forume-buduschih-tehnologiy-2024> (дата обращения: 15.08.2024)

находит подтверждение в Стратегии развития здравоохранения в Российской Федерации на период до 2030 года, утвержденной Указом Президента Российской Федерации от 8 декабря 2025 г. № 896, в которой установлено, что основной задачей развития здравоохранения в Российской Федерации является создание условий для повышения качества и безопасности медицинской помощи, увеличения ее доступности по приоритетному направлению разработки и внедрения в систему здравоохранения наиболее актуальных и востребованных новых персонализированных, биотехнологических, высокотехнологичных и радиофармацевтических, медицинских изделий, а также методов оказания медицинской помощи и медицинских технологий⁵.

Важно подчеркнуть, что понятия «медицина» и «здравоохранение» не являются синонимами. Под медициной в широком толковании понимается область деятельности, направленная на сохранение индивидуального здоровья человека, а здравоохранение - область деятельности, направленная на сохранение здоровья общества с использованием медицинских знаний⁶. При этом, как отмечает, И.А. Умнова-Конюхова, здоровье конкретного человека, здоровье социальных общностей и групп, а также человеческой популяции в целом регулируется в правовом контексте⁷. Поэтому в исследовании слова «информационные технологии» используются в сочетании со здравоохранением, поскольку оно как сфера деятельности распространяется на все общество, а не на конкретного человека.

Согласимся с мнением, высказанным в научной доктрине, о том, что термины «информационные технологии» и «цифровые технологии» используются как «взаимозаменяемые понятия, характеризующие технологии так называемой

⁵ Указ Президента Российской Федерации от 8 декабря 2025 г. № 896 «О Стратегии развития здравоохранения в Российской Федерации на период до 2030 года». URL: <http://publication.pravo.gov.ru/document/0001202512090003> (дата обращения: 12.12.2025).

⁶ Хай Г.А. Информатика для медиков: учебное пособие. СПб.: СпецЛит, 2009. 223 с.

⁷ Умнова-Конюхова И. А. Экология человека, биоправо и право биобезопасности: межотраслевые и междисциплинарные взаимосвязи // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4, Государство и право. 2024. №. 2. С. 7-25.

«четвертой промышленной революции»⁸. По сути, информационные технологии, как и цифровые технологии и информационные и цифровые системы (компьютеры, сети, программное обеспечение), применяются для сбора, хранения, управления и передачи данных в целях поддержки деятельности организаций. Однако в целях единообразия и системности мы будем в тексте исследования использовать термин «информационные технологии», при этом данный термин по сравнению со вторым появился намного раньше и более распространен в российской научной доктрине и в отечественном законодательстве.

Целесообразно также выявить подходящее для дальнейшего исследования определение понятия «информационные технологии» именно в сфере здравоохранения и выявить основные их виды, используемые в здравоохранении.

Согласно пункту 2 ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», под информационными технологиями понимаются «процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов»⁹.

Авторская позиция по вопросу определения информационных технологий в сфере здравоохранения может быть представлена следующим образом. Ключевой характеристикой информационной технологии является автоматизированная обработка данных (в отличие от ручной обработки). Ярким примером служит применение телемедицинских технологий, целью которых является обеспечение равноправного доступа к медицинской помощи в требуемом объеме и в актуальные сроки, независимо от местонахождения пациента и медицинских работников¹⁰ или

⁸ *Хомяков Э.Г.* Современные информационные и цифровые технологии и отдельные направления их использования в правоохранительной деятельности // Вестник Удмуртского университета. Серия «Экономика и право». 2024. Т. 34. № 5. С. 950-957.

⁹ Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // «Собрание законодательства РФ», 31.07.2006, № 31 (1 ч.), ст. 3448

¹⁰ *Владимирский А. В., Морозов С. П., Урванцева И. А., Коваленко Л. В., Воробьев А. С.* Применение телемедицинских технологий в кардиологии : учеб. пособие; Сургут. гос. ун-т. Сургут : Изд-во СурГУ, 2019. 115 с.

применение медицинской информационной системы в организациях здравоохранения, которая применяется в целях хранения и обработки данных (в первую очередь, диагностических), автоматизации и минимизации ошибок в составлении документации, что уменьшает время принятия решений и работы персонала, способствует своевременному оказанию услуг¹¹.

В настоящее время многие медицинские организации совместно используют технологии обработки первичных данных через медицинские информационные системы и телемедицинские технологии, к примеру, через медицинскую информационную систему происходит запись к врачу для получения телемедицинской консультации.

Постоянный технологический прогресс в сфере здравоохранения создает предпосылки для совершенствования решений существующих проблем в данной сфере, а также находит новые способы решения проблем, которые ранее даже не ставились. Информационные технологии рассматриваются как потенциально эффективный инструмент для организации здравоохранения, позволяющий справиться с необходимостью повышения качества услуг в условиях растущего спроса. Основной целью применения информационных технологий в здравоохранении является автоматизация и облегчение задач, которые раньше выполнялись вручную, в том числе оцифровка медицинских карт, клинических карт и бумажных запросов на проведение клинических анализов¹². Помимо этого, информационные технологии направлены на обеспечение более качественного ухода за пациентами и повышение эффективности медицинского обслуживания, повышение эффективности оказания медицинской помощи пациентам, повышение безопасности пациентов, снижение количества врачебных ошибок¹³.

¹¹ Гуськов Д.Д., Абугалиева Ж. М. Перспективы развития медицинских информационных систем в России // Научный аспект. 2023. Т. 29. № 12. С. 3581-3588.

¹² *Pendyala VS, Figueira S. (2017). Automated medical diagnosis from clinical data. Proceedings of 2017 IEEE 3rd International Conference on Big Data Computing Service and Applications (BigDataService); Apr 6–9; Redwood City, CA. p. 185-90.*

¹³ *Popescu, C., El-Chaarani, H., El-Abiad, Z., & Gigauri, I. (2022). Implementation of health information systems to improve patient identification. International Journal of Environmental Research and Public Health, 19(22), P.15236.*

В 2005 году Всемирная организация здравоохранения (ВОЗ) определила электронное здравоохранение, раскрыв ее как «безопасное и экономически эффективное использование информационных и коммуникационных технологий для поддержки здравоохранения и связанных со здоровьем областей, включая медицинские услуги, наблюдение за здоровьем, медицинскую литературу и образование, медицинские знания и исследования»¹⁴. Помимо термина «электронное здравоохранение» ВОЗ применяет термин «цифровое здравоохранение», концепция которого уходит корнями в электронное здравоохранение, но выходит далеко за его рамки. Цифровое здравоохранение включает использование новых информационных технологий, таких как искусственный интеллект, технологии Интернета вещей. Исходя из этого, ВОЗ определяет цифровое здравоохранение как «всеобъемлющий термин, включающий в себя электронное здравоохранение и новые области, такие как использование вычислительных наук в области искусственного интеллекта, больших данных и геномики»¹⁵. Согласно данному определению, основное отличие цифрового здравоохранения от других терминов заключается в том, что цифровое здравоохранение имеет более широкий охват.

Упоминание в определении понятия информационных технологий в здравоохранении слов «компьютерное оборудование», «аппаратное оборудование» не совсем уместно в условиях постоянно развивающейся инфраструктуры информационных технологий, поскольку она включает в себя широкий спектр устройств (например, носимые устройства, медицинские импланты, «умные» диагностические приборы, относящиеся к технологиям Интернета вещей), функционал которых выходит за рамки классического понимания компьютерного оборудования, ориентированного в первую очередь на универсальные вычислительные задачи.

¹⁴ Global diffusion of eHealth: Making universal health coverage achievable. URL: <https://www.statista.com/topics/2409/digital-health/#topicOverview> (дата обращения: 15.09.2024)

¹⁵ Там же.

Поэтому под информационными технологиями в сфере здравоохранения можно понимать методы и способы, направленные на сбор, обработку, хранение, предоставление, использование и распространение медицинской информации.

В отношении видов информационных технологий, в том числе и в здравоохранении, имеется множество мнений ученых.

В классификации информационных технологий И.Л. Бачило, В.Н. Лопатин, М.А. Федотов (коллектив авторов учебника по информационному праву) отдают предпочтение высоким интеллектуальным информационным технологиям: к ним относятся такие, на основе которых осуществляется генерация технических решений; реализуются текстологические системы (поиск, реферат, анализ содержания); осуществляется ситуационное моделирование, позволяющее выявить связь элементов, их динамику, обозначить объективные закономерности среды, выделенной в ситуационный анализ¹⁶.

В.Н. Волкова с соавторами выделяет 15 видов информационных технологий¹⁷. Также исследователи классифицируют информационные технологии по видам обрабатываемой информации и по типу пользовательского интерфейса¹⁸, по степени типизации операций и по типу информации¹⁹, а также по способу построения компьютерной сети, по виду обработки технологии информации, по области управления социально-экономическим процессом²⁰. Может образоваться

¹⁶ Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право: учебник / Под ред. Топорнина Б.Н. – СПб.: Юрид. центр Пресс, 2001. 789 с.

¹⁷ Волкова В. Н. и др. Классификация информационных технологий // Прикладная информатика. 2015. №. 5 (59). С. 124-141.

¹⁸ Киселев Г. М. К вопросу о понятии «информационные технологии // Научный поиск. 2013. № 4.1. С. 33-34.

¹⁹ Костоломова К.К., Николенко Т.А. К вопросу классификации информационных технологий // Математические методы и модели в управлении, экономике и социологии : Сборник научных трудов. Том Выпуск 7. – Тюмень : Тюменский государственный нефтегазовый университет. 2013. С. 167-170.

²⁰ Титоренко Г. А. Информационные системы в экономике: учебник для студентов вузов, обучающихся по специальностям «Финансы и кредит», «Бухгалтерский учет, анализ и аудит» и специальностям экономики и управления / Под ред. Г. А. Титоренко. – 2-е изд., перераб. и доп. – М.: ЮНИТИ-ДАНА. 2008. 463 с.

деление на первичные и вторичные²¹, «новые» и «старые» информационные технологии²². С.А. Дятлов выделяет 6 типов информационных технологий, исходя из эволюционно-информационных стадий развития человеческой цивилизации²³.

Ряд других авторов предлагают приближенные к современности следующие виды информационных технологий: информационные технологии обработки данных; информационные технологии управления; информационные технологии поддержки принятия решений; информационные технологии экспертных систем²⁴.

По мнению И.В. Свищевой и А.Г. Пронкиной классификация информационных технологий в здравоохранении выглядит следующим образом:

1. Информационные технологии как инструмент лечения и реабилитации пациентов (VR-технологии в реабилитации, ИИ в диагностике заболеваний, аппаратные средства лечения – приборы МРТ, УЗИ).

2. Информационные технологии как инструмент организационной деятельности (CRM-системы для клиник, единые государственные системы - ЕМИАС, ЕГИСЗ).

3. Информационные технологии как инструмент анализа данных регионального и федерального уровня (BI-системы аналитики – QlikView, Tableau, Prognost Platform, IBM Cognos).

4. Информационные технологии как способ коммуникации и обучения медицинского персонала (Портал Минздрава, онлайн-сервис «Мое здоровье», дистанционные курсы учебных центров, коммуникационные платформы – Skype, Zoom)²⁵.

²¹ Авдулов А.Н., Кулькин А.М. Классификация информационных технологий // Вестник Российского фонда фундаментальных исследований. 2004. № 1(35). С. 36-45.

²² Амадаев А.А., Начхоев И.И. Понятие и классификация информационных технологий // Вопросы устойчивого развития общества. 2021. № 12. С. 869-873.

²³ Дятлов С.А. Принципы информационного общества // Информационное общество. 2000. Т. 2. С. 77-85.

²⁴ Володченко В.С., Ланцова Д.С., Миронова Т.А. Понятие и классификация информационных технологий // Достижения науки и образования. 2020. №. 12 (66). С. 41-43.

²⁵ Свищева И.В., Пронкина А.Г. Исследование и анализ процессов внедрения информационных технологий в сферу здравоохранения РФ: актуальность и дальнейшие пути развития // Международный журнал гуманитарных и естественных наук. 2022. № 11-2(74). С. 146-152.

По нашему мнению, данная классификация представляет научный интерес, однако она не обладает достаточной степенью дифференциации видов информационных технологий, поскольку указанные в 1 группе виды технологий можно отнести и к другим группам, например, VR-технологии применяются при обучении будущего медицинского персонала в образовательных учреждениях. При этом среди информационных технологий в 1 группе не указаны иные виды, например, телемедицинские технологии или мобильные устройства и приложения (технологии Интернета вещей), которые предназначены и для лечения, и для реабилитации пациентов.

Р.В. Амелин, Л.В. Бессонов выделяют следующую классификацию медицинских информационных технологий в здравоохранении:

1. Технологии управления в сфере медицины (включая планирование, учет, контроль, оказание государственных и муниципальных услуг в сфере здравоохранения);

2. Технологии электронного документооборота;

3. Телемедицинские технологии;

4. Технологии анализа медицинских данных и принятия медицинских решений (включая технологии «больших данных» и искусственного интеллекта, которые могут быть выделены и в отдельные подгруппы)²⁶.

Предложенная классификация обладает ограниченной полнотой, поскольку в ней не нашли отражения такие активно применяющиеся технологии, как технологии Интернета вещей или технологии виртуальной и дополненной реальности. Также следует разделить технологии анализа больших данных и искусственного интеллекта: нецелесообразно объединять искусственный интеллект с технологиями анализа больших данных, так как технологии искусственного интеллекта разделяются на несколько видов, которые могут как генерировать собственные суждения, так и применяться в рамках заданного

²⁶ Амелин Р. В., Бессонов Л. В. О некоторых вопросах правового регулирования телемедицинских технологий // Информационное право. 2019. № 2. С. 21-25.

алгоритма. В свою очередь, технологии анализа больших данных направлены на поддержку принятия решений в больницах, то есть для решения административных и финансовых задач.

В качестве дальнейшего исследования логичным представляется выявить следующие виды информационных технологий. При этом стоит подчеркнуть, что цель выделения информационных технологий заключается не в том, чтобы охватить все информационные технологии, используемые или предлагаемые в здравоохранении. Скорее, цель состоит в том, чтобы определить конституционно-правовые аспекты применения информационных технологий в здравоохранении.

Нижеуказанные разновидности выделены с точки зрения необходимости правового регулирования и связаны со здравоохранением, в частности порядком оказания медицинской помощи пациентам. Они непосредственно влияют на конституционные права человека в сфере здравоохранения, а также на систему государственного управления в данной области. Такие виды технологий можно отнести к категории управления медицинской информацией и взаимодействия с пациентами.

1. *Технологии обработки первичных данных.* Технологии информационных систем позволяют обрабатывать большие объемы информации, необходимой для поддержки исследований в области здравоохранения, например, чтобы обеспечить целостность клинических испытаний. Как в любой информационной системе, к ним относится сбор информации, которому предшествует получение первичных данных о пациенте в результате его осмотра или автоматически с помощью специального оборудования для регистрации состояния больного и с помощью других специализированных медицинских информационных систем²⁷.

2. *Технологии анализа больших данных (Big Data)*²⁸. Электронные медицинские карты, относящиеся к технологиям анализа больших данных,

²⁷ Информационные технологии в сфере здравоохранения. URL: <https://mirror-info.ucoz.com/medicine/InfoTecMed.pdf> (дата обращения: 15.08.2024)

²⁸ «Технологии анализа больших данных» - устоявшийся термин (Big Data), под которым понимается совокупность методов, инструментов и процессов для извлечения ценной

предоставляют централизованные данные о пациентах и улучшают управление информацией. Электронные медицинские карты – наиболее распространенный тип применения больших данных в сфере здравоохранения²⁹. Помимо них также к технологиям анализа больших данных можно отнести хранилища и облачные платформы. Например, Data Warehouse — единое корпоративное хранилище с обработанной и структурированной информацией. Хранилище упрощает анализ полученных данных, но требует структурированности³⁰.

3. *Технологии Интернета вещей*³¹. Сегодня технологии Интернета вещей отслеживают все показатели здоровья пациента - от частоты сердечных сокращений до режима сна, играя важнейшую роль в профилактическом здравоохранении.

4. *Технологии искусственного интеллекта*. Потенциал искусственного интеллекта огромен: от алгоритмов, способных выявлять заболевания по снимкам, до систем искусственного интеллекта, которые могут прогнозировать риски пациентов.

5. *Телемедицинские технологии*. Данные технологии получили широкое распространение, позволив пациентам в отдаленных районах консультироваться со специалистами, находящимися за много километров от них.

После того, как в исследовании установлено определение содержания понятия «информационные технологии» в здравоохранении и их основные виды, необходимые для исследования, следует рассмотреть этапы внедрения информационных технологий в сферу здравоохранения. Это необходимо для более

информации из очень больших, сложных и быстро меняющихся наборов данных, которые невозможно обработать традиционными способами.

²⁹ Кисель А. А., Нестеренков С. Н. Электронные медицинские карты как представитель big data в медицине // Редакционная коллегия. 2022. С. 378.

³⁰ Big Data. URL: <https://yandex.cloud/ru/docs/glossary/bigdata> (дата обращения: 15.10.2025)

³¹ «Технологии Интернета вещей» – устоявшийся термин (IoT, Internet of Things). Под технологиями Интернета вещей понимается обширный комплекс аппаратного и программного обеспечения, стандартов и протоколов, которые позволяют физическим объектам («вещам») собирать данные, обмениваться ими через интернет и взаимодействовать друг с другом без участия человека. В российском законодательстве термин содержится в Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы, утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203.

глубокого понимания эволюции правового регулирования применения информационных технологий.

Многие авторы выделяют пять этапов развития информационных технологий с точки зрения видов технического инструментария, начиная со второй половины XX века и по настоящее время³². Эволюция информационных технологий в здравоохранении имеет похожую периодизацию.

Первый этап. В сфере здравоохранения первые наработки применения информационных технологий начинают появляться в 50-е годы XX века, когда они использовались больницами для управления финансовыми ресурсами, например, проект «MEDINET» от General Electric.

Второй этап. Позднее, в 60-х годах XX века, начали появляться информационные медицинские системы, направленные на улучшение доступа населения к медицинскому обслуживанию. Наиболее известные в это время были информационные системы, разработанные под государственные программы здравоохранения оказания медицинской помощи Medicare и Medicaid в США.

Третий этап. В 70-е годы XX века начали применять технологии, направленные на поддержку принятия решений в больницах. Впервые информационные технологии в здравоохранении возникли для поддержки административных и финансовых отделов больниц путем автоматизации конкретных задач, таких как платежи и получение доходов. Например, проект Technicon от TDS в США.

Четвертый этап. В 80-е годы XX века начали развиваться технологии обработки данных, которые собирали информацию о пациентах и создавали базы данных, где хранилась персональная медицинская информация пациентов. Медицинские информационные системы продвинулись до установления и

³² Несмиянова И. О. Информационные технологии: этапы развития, понятие и классификация // Известия Тульского государственного университета. Экономические и юридические науки. 2020. № 1. С. 149-155; Магрицкая А. В. Информационные технологии в управлении предприятием: эволюция развития и классификация // Огарёв-Online. 2023. №. 10 (195). С. 8; Троянская М. А., Еременков А. А. Информационные технологии в государственном управлении: понятие, виды, задачи и направления регулирования // Вестник Академии знаний. 2022. № 50(3). С. 331-337.

хранения электронной истории болезни пациента: проект Composite Health Care System в США. Однако в связи с отсутствием правового регулирования информационных технологий в сфере здравоохранения и финансирования проект не получил должной реализации³³.

Пятый этап. С начала XXI века и по настоящее время сфера здравоохранения получила новый виток развития информационных технологий: было внедрено несколько технологий, которые применяются на практике в целях улучшения оказания медицинской помощи пациентам.

Ранние разработки информационных технологий для здравоохранения начались с усовершенствования средств и инструментов, используемых в сфере здравоохранения. В этом контексте, к примеру, профессор Питер Л. Райхерц объяснял технологические разработки в больницах, подчеркнув социальную сторону технологии³⁴.

С каждым годом повышается интерес к информационным технологиям в здравоохранении, поскольку они могут обеспечить необходимое улучшение сферы здравоохранения и улучшить меры по оказанию медицинской помощи пациентам. Так что можно сказать, что развитие информационных технологий привело к значительным изменениям в сфере здравоохранения. Относительно недавно, если рассматривать с точки зрения эволюции, появились такие понятия, как «большие данные», «Интернет вещей», а сегодня они уже стали частью повседневной жизни в здравоохранении. Внедрение таких технологий, как отмечают многие исследователи, сделали медицинские услуги доступными³⁵, недорогими³⁶,

³³ Гурyleва М. Э. История развития медицинских информационных систем // Российская академия медицинских наук. Бюллетень Национального научно-исследовательского института общественного здоровья. 2013. № S1. С. 54-56.

³⁴ Reichertz, P. L. (2006). Hospital information systems—Past, present, future. *International journal of medical informatics*, 75(3-4), pp. 282-299.

³⁵ Nichani A. V., Pistolwala S. T., Deshmukh A. A., Godse M. J. Telemedicine: making health care accessible. In: Vasudevan H., Deshmukh A., Ray K., editors. *Proceedings of International Conference on Wireless Communication*. Vol. 19. Singapore: Springer; 2018. pp. 255–263.

³⁶ Talwar, Y. K., Karthikeyan, S., Bindra, N., & Medhi, B. (2016). Smartphone-a user-friendly device to deliver affordable healthcare—a practical paradigm. *J Health Med Informat*, 7(7), P. 3.

ориентированными на пациента³⁷, менее подверженными ошибкам³⁸ и интерактивными³⁹.

В результате увеличиваются затраты и инвестиции на внедрение все большего количества информационных технологий в сферу здравоохранения. На момент 2022 года глобальное финансирование цифрового здравоохранения составило 330 миллиардов долларов, а к 2025 году, по прогнозам, планируется, что объем рынка цифрового здравоохранения превысит 650 миллиардов долларов в мире, это свидетельствует о нарастающем стремлении внедрять информационные технологии в сферу здравоохранения⁴⁰.

Из вышеуказанной эволюции развития информационных технологий можно прийти к выводу, что информационные технологии изначально были направлены на решение административных задач и в результате привели к комплексной трансформации сферы здравоохранения, что и породило современные правовые вызовы.

Ускорение внедрения информационных технологий в здравоохранение сделало проблемы защиты прав пациентов на частную жизнь, конфиденциальности и безопасности данных еще более актуальными. Стоит согласиться с мнением И.Ф. Колонтаевской, что одной из главных правовых проблем, связанных с применением информационных технологий в сфере здравоохранения, является отставание в их правовом регулировании и отсутствие соответствующей

³⁷ Baysari, M. T., & Westbrook, J. I. (2015). Mobile applications for patient-centered care coordination: a review of human factors methods applied to their design, development, and evaluation. *Yearbook of medical informatics*, 24(01), pp. 47-54.

³⁸ Sakushima, K., Umeki, R., Endoh, A., Ito, Y. M., & Nasuhara, Y. (2015). Time trend of injection drug errors before and after implementation of bar-code verification system. *Technology and health care*, 23(3), pp. 267-274.

³⁹ Rachas, A., Farmer, A. J., Inzitari, M., & Shepperd, S. (2015). Interactive telemedicine: effects on professional practice and health care outcomes. *Cochrane Database of Systematic Reviews*, (9), pp. 1-512.

⁴⁰ Digital health - Statistics & Facts. URL: <https://www.statista.com/topics/2409/digital-health/#topicOverview> (дата обращения: 15.09.2024)

нормативной правовой базы в данной сфере⁴¹. По большей части это относится и к законодательству России.

В.Н. Лопатин справедливо указал, что широкое распространение информационных технологий способствует появлению новых угроз конституционным правам и свободам граждан, безопасности Российского государства в целом⁴².

Но прежде чем переходить к проблемам в сфере реализации прав граждан при использовании информационных технологий, следует для начала определить, каким образом на международном уровне, в зарубежных странах и в России регулируется применение информационных технологий в здравоохранении, а также каким образом в России конституционализируется применение информационных технологий в здравоохранении. Последний аспект будет раскрыт в следующей главе.

Подводя итог, можно подчеркнуть следующее.

1. Выработанное определение понятия «информационные технологии» в сфере здравоохранения позволяет точнее очертить предмет исследования, в то время как термины «компьютерное оборудование», «аппаратное оборудование» не совсем уместно рассматривать в условиях постоянно развивающейся инфраструктуры информационных технологий.

2. Выделенные разновидности информационных технологий позволят установить уровень правового регулирования их применения в отечественном законодательстве и то, какие проблемы возникают в связи с их влиянием на конституционные права граждан и систему управления здравоохранением.

⁴¹ Колонтаевская, И. Ф. Правовое регулирование цифровой медицины в Российской Федерации // Новое в науке и образовании : Материалы Международной ежегодной научно-практической конференции, Москва, 04 апреля 2023 года / Отв. редактор Е.В. Дмитриев, сост. Э.Н. Замега. – Ростов-на-Дону: Общество с ограниченной ответственностью «Манускрипт», 2023. С. 177-181.

⁴² Лопатин В. Н. Информационная безопасность России : специальность 12.00.01 "Теория и история права и государства; история учений о праве и государстве" : диссертация на соискание ученой степени доктора юридических наук 12.00.01/ Лопатин Владимир Николаевич. - Санкт-Петербург, 2000. 433 с.

§ 2. Международно-правовые стандарты защиты прав человека в области цифрового здравоохранения

В качестве основы для развития национального законодательства о здравоохранении могут выступать международные нормы, закрепляющие такие права человека, как право на неприкосновенность частной жизни, право на доступ к медицинским технологиям и право на наивысший достижимый уровень здоровья. При этом важно, что на международном уровне также приняты специализированные акты в сфере здравоохранения в части регулирования применения информационных технологий, по большей части носящие рекомендательный характер.

Основным специализированным международным документом, который нам интересен в контексте разрабатываемой проблематики и в котором установлены правовые модели разрешения вопросов применения информационных технологий в здравоохранении, можно признать принятую Всемирной организацией здравоохранения (далее - ВОЗ) Глобальную стратегию по развитию цифрового здравоохранения на 2020–2025 годы. В указанной стратегии отмечается, что информационно-технологическая инфраструктура здравоохранения будет основана на общепринятых сценариях ее использования в сфере здравоохранения; ее функциональные требования и набор функциональных и технических спецификаций, стандартов и профилей, разработанных на их основе, должны быть созданы на прочной нормативно-правовой базе, гарантирующей защиту данных, конфиденциальность и целостность. Также она предоставляет рекомендации по внедрению информационных технологий, включая технологии Интернета вещей, телемедицинские технологии и искусственный интеллект с акцентом на обеспечение справедливого доступа и качества услуг⁴³.

⁴³ Global strategy on digital health 2020-2025. URL: <https://www.who.int/docs/default-source/documents/g4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf> (дата обращения: 15.09.2024)

Прочная нормативно-правовая база послужит основой и для защиты медицинских данных, поскольку они являются конфиденциальными персональными данными, требующими высоких стандартов безопасности.

Иначе говоря, Глобальная стратегия ВОЗ по развитию цифрового здравоохранения на 2020–2025 годы формирует концептуальные основы для развития законодательства в этой области.

ВОЗ играет ведущую роль в формировании общемировых стандартов цифрового здравоохранения. Среди ее ключевых документов можно выделить также «Классификацию цифровых вмешательств, услуг и приложений в здравоохранении», которая предлагает общую терминологию и рамки для категоризации информационных технологий, что способствует их стандартизации и внедрению⁴⁴. Указанные и прочие документы ВОЗ подчеркивают, что использование информационных технологий затрагивает интересы всего международного сообщества.

Другими важными международными документами в области применения информационных технологий в здравоохранении являются следующие.

Конвенция о защите прав и достоинства человека в связи с применением достижений биологии и медицины 1997 года формирует правовую основу для дальнейших дискуссий, формулируя основополагающие стандарты в отношении решений, находящихся в процессе развития биомедицинских и биотехнологических наук.

Статья 10 Конвенции прямо гарантирует право на уважение частной жизни в отношении сведений о здоровье. В цифровую эпоху это трансформируется в конституционную гарантию защиты персональных медицинских данных, хранящихся в информационных системах (электронные истории болезни, базы

⁴⁴ Классификация цифровых действий, услуг и приложений в здравоохранении: общий язык для описания использования цифровых технологий в интересах здравоохранения. URL: <https://whodc.mednet.ru/ru/osnovnye-publikaczii/informaczionnye-texnologii-v-zdravooxranenii/4147.html> (дата обращения: 15.09.2024)

данных медицинских учреждений, приложения для здоровья)⁴⁵. Также это создает обязательства для государства развивать инфраструктуру (например, личные кабинеты пациента), обеспечивающую гражданам легкий доступ к их медицинским записям и результатам анализов.

Тем не менее Конвенция сталкивается с вызовами, которые не были очевидны в 1997 году, например, положения об информированном согласии в ст. 5 не предусматривают осознанное согласие на использование искусственного интеллекта в лечении, при этом применение телемедицинских технологий очевидно требует адаптации стандартов информированного согласия с учетом современных реалий цифровизации.

Всеобщая декларация о биоэтике и правах человека 2005 года затрагивает этические вопросы, касающиеся медицины, наук о жизни и связанных с ними технологий применительно к человеку, с учетом их социальных, правовых и экологических аспектов (часть 1 ст. 1)⁴⁶.

Хотя Декларация была разработана в ответ на вызовы в области биомедицины, ее принципы обладают значительным потенциалом для применения в цифровой сфере.

Принцип неприкосновенности частной жизни и конфиденциальности (ст. 9) напрямую соотносится с правом на неприкосновенность частной жизни. В эпоху информационных технологий он приобретает новое звучание, требуя надежной защиты персональных медицинских данных от несанкционированного доступа, использования или раскрытия. Принцип информированного согласия (ст. 6), фундаментальный для здравоохранения, предполагает, что пациенты должны давать явное, осознанное и добровольное согласие на использование своих данных, в том числе в исследовательских целях. Принцип социальной ответственности и

⁴⁵ Конвенция о защите прав и достоинства человека в связи с применением достижений биологии и медицины: Конвенция о правах человека и биомедицине. URL: <http://hrlibrary.umn.edu/russian/euro/Rz37.html> (дата обращения: 28.03.2025)

⁴⁶ Всеобщая декларация о биоэтике и правах человека. URL: https://www.un.org/ru/documents/decl_conv/declarations/bioethics_and_hr.shtml (дата обращения: 28.03.2025)

здоровья (ст. 13) предполагает, что обладание наивысшим достижимым уровнем здоровья является одним из основных прав всякого человека. Декларация подчеркивает, что развитие науки и технологий должно служить благу общества. Применительно к информационным технологиям это означает, что преимущества от их использования должны способствовать улучшению системы здравоохранения и расширению доступа к качественным медицинским услугам.

Данный документ является частью так называемых инструментов мягкого права, то есть международных документов, которые «слабее» конвенций, и не являются обязательными для исполнения, они предлагают государствам следовать положениям соответствующих правил и соблюдать их. Эта процедура позволяет государствам разделить с другими странами обязательства, которые они в противном случае не взяли бы на себя. Рекомендательный формат вышеуказанной декларации позволяет обеспечить консенсус стран-участниц в отношении отдельных положений документа, оказывающих влияние на вопросы биоэтики, в контексте современного стремительного технологического развития.

Принципиальное значение имеет Конвенция о защите физических лиц при автоматизированной обработке персональных данных 1981 года. Данная Конвенция является международным договором и юридически обязывающим документом для государств-членов Совета Европы, призванным защищать право на неприкосновенность частной жизни отдельных лиц. Статья 6 Конвенции устанавливает повышенный уровень защиты для специальных категорий данных, включая информацию о здоровье⁴⁷. Такие данные не могут обрабатываться автоматически, если национальное законодательство не предусматривает для этого адекватных гарантий, что имеет ключевое значение для развития информационных технологий.

Анализ данной Конвенции позволяет констатировать, что уже на заре цифровой эры законодатель осознавал: автоматизированная обработка данных

⁴⁷ Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Заключена в г. Страсбурге 28.01.1981) // "Собрание законодательства РФ", 03.02.2014, № 5, ст. 419.

одновременно и повышает эффективность, и создает системные риски для конфиденциальности. Данная проблема до сих пор является центральным противоречием, которое пытаются разрешить современные государства. При этом определение «автоматизированной обработки» в ст. 2 сформулировано специально широко, чтобы оно охватывало не только существовавшие на момент подписания информационные технологии, но и будущие, включая технологии Интернета вещей, технологии анализа больших данных и технологии искусственного интеллекта.

Ключевое значение в международных актах придается праву на доступ к медицинским технологиям и праву на наивысший достижимый уровень здоровья, а также праву на неприкосновенность частной жизни. Отметим, что последнее также закреплено в таких фундаментальных актах о правах человека, как Международный пакт о гражданских и политических правах (ст. 17) и Всеобщая декларация прав человека (ст. 12).

Мы придерживаемся позиции ряда ученых, заключающейся в том, что право на наивысший достижимый уровень здоровья, в том числе право на охрану здоровья и медицинскую помощь, является элементом права на здоровье, поскольку «право на здоровье является более общей, родовой категорией, и его конкретизация позволяет выделить различные аспекты содержания данного права»⁴⁸, при этом право на охрану здоровья и медицинскую помощь закрепляется в национальном законодательстве, акцентируя внимание на необходимости предоставления позитивных услуг от государства⁴⁹. Кроме того, производными от права на здоровье является право на доступность и качество медицинских услуг или на качественное медицинское обслуживание, право на доступ к медицинским технологиям⁵⁰.

⁴⁸ Умнова-Конюхова И. А. Право на здоровье: актуальные аспекты природы, содержания и регулирования в международном и национальном праве // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4, Государство и право. 2025. № 2. С. 7-25.

⁴⁹ Романовский Г. Б. Право на здоровье и право на охрану здоровья в международном и национальном праве // Гражданин и право. 2021. № 5. С. 3-14.

⁵⁰ Там же, С. 13.

Право на доступ к медицинским технологиям, в свою очередь, неразрывно связано с правом на доступ к достижениям научного прогресса, а также с правом на участие в научном прогрессе и пользования его благами, сформулированными в ряде международных актов (в ст. 27 Всеобщей декларации прав человека⁵¹; в пункте «б» части 1 ст. 15 Международного пакта об экономических, социальных и культурных правах⁵², а также в региональных договорах, в частности в: части 2 ст. 13 Американской декларации прав и обязанностей человека 1948 г.⁵³; в пункте «с» части 1 ст. 14 Дополнительного протокола к Американской конвенции о правах человека в области экономических, социальных и культурных прав 1988 года («Сан-Сальвадорский протокол»)⁵⁴; в ст. 1 Протокола № 1 к Конвенции о защите прав человека и основных свобод 1952 года)⁵⁵ и является, по справедливому замечанию В.С. Маличенко, «одним из важнейших компонентов реализации права на наивысший достижимый уровень здоровья. Право на доступ к медицинским технологиям закреплено во всех универсальных и региональных документах по правам человека»⁵⁶.

Данное право было включено в Декларацию о праве на развитие, принятую Генеральной Ассамблеей ООН в 1986 году, в которой сформулировано, что государства должны принимать все необходимые меры для осуществления права

⁵¹ Там же.

⁵² Международный пакт об экономических, социальных и культурных правах. URL: https://www.un.org/ru/documents/decl_conv/conventions/pactecon.shtml (дата обращения: 28.03.2025)

⁵³ Американская декларация прав и обязанностей человека (обзор). URL: <https://hrlib.kz/document/199513> (дата обращения: 28.03.2025)

⁵⁴ Additional protocol to the American convention on human rights in the area of economic, social and cultural rights "Protocol of San Salvador". URL: <https://www.oas.org/juridico/english/treaties/a-52.html> (дата обращения: 28.03.2025)

⁵⁵ Протокол к Конвенции о защите прав человека и основных свобод. URL: <http://hrlibrary.umn.edu/russian/euro/Rz20prot1.html> (дата обращения: 28.03.2025)

⁵⁶ Маличенко В. С. Международно-правовые механизмы регулирования доступа к технологиям здравоохранения // Право. Журнал Высшей школы экономики. 2021. №. 5. С. 256-285.

на развитие и обеспечить, в частности, равенство возможностей для всех в том, что касается доступа к основным ресурсам и здравоохранению⁵⁷.

Право на наивысший достижимый уровень здоровья признано на международном уровне в качестве одного из прав человека и закреплено в различных документах, включая Международный пакт об экономических, социальных и культурных правах и Всеобщую декларацию прав человека. Оно подразумевает, что каждый человек имеет право на медицинскую помощь, которая должна быть в наличии, доступна, приемлема и качественна, т.е. право на такой уровень физического и психического здоровья человека, который позволяет ему вести достойную жизнь⁵⁸.

Данная система параметров часто используется для описания предоставления медицинских услуг.

Так, «наличие» предполагает, что медицинская помощь должна предоставляться в достаточном объеме.

«Доступность»: предоставление медицинских услуг должно быть физически доступным и недорогим. Они также должны быть недискриминационными. Информация об услугах также должна быть доступной, без ущерба для защиты данных.

«Приемлемость»: при оказании медицинской помощи необходимо соблюдать медицинскую этику, конфиденциальность и учитывать культурные особенности.

«Качество»: предоставление медицинской помощи должно быть научно обоснованным. Оно должно быть безопасным, эффективным, ориентированным на человека, своевременным, справедливым, комплексным и действенным.

⁵⁷ Хабриев Р. У., Абашидзе А. Х., Маличенко В. С. Роль развития системы регулирования обращения лекарственных средств в реализации права человека на наивысший достижимый уровень здоровья // Журнал зарубежного законодательства и сравнительного правоведения. 2016. №. 2 (57). С. 16-22.

⁵⁸ Availability, Accessibility, Acceptability and Quality framework. URL: <https://gbvguidelines.org/wp/wp-content/uploads/2019/11/AAAQ-framework-Nov-2019-WEB.pdf> (дата обращения: 29.02.2025).

Использование информационных технологий в здравоохранении должно, как минимум, соответствовать указанным четырем ключевым параметрам. Эти требования означают, что государства должны обеспечить наличие и доступность цифровой инфраструктуры по всей стране как с точки зрения технических средств, так и с точки зрения программного обеспечения.

Приемлемость, качество, доступность формируют важные взаимосвязи с другими правами человека: доступ к качественной медицинской помощи, доступ к информации о здоровье. По этому поводу О.А. Авдеева отметила: «Право человека на доступ к медицинскому обслуживанию предполагает доступ к необходимым средствам и услугам для диагностики, лечения и профилактики заболеваний на протяжении всей его жизни»⁵⁹.

Таким образом, право на наивысший достижимый уровень здоровья включает в себя право на доступ к различным объектам, товарам, услугам и условиям, которые являются необходимыми для достижения наивысшего уровня здоровья.

Поскольку информационные технологии задействованы в медицинских организациях в отношении пациентов, то непосредственно влияют на реализацию права на доступ к качественной медицинской помощи и на доступ к информации о здоровье. Отсюда следует, что их применение влияет и на право на наивысший достижимый уровень здоровья, повышая его значимость в современном мире. Право обязывает государства обеспечивать доступ к качественной медицинской помощи, включая современные цифровые услуги, такие как телемедицина и диагностика с использованием искусственного интеллекта. В результате мы можем говорить о достижении такого уровня физического и психического здоровья, который позволяет вести достойную жизнь пациенту, когда применяются информационные технологии.

⁵⁹ Авдеева О. А. Право на здоровье в международном праве: от аморфного архетипа к синтетической концепции // Российское право: образование, практика, наука. 2023. №. 4. С. 45-52.

Использование информационных технологий, в частности телемедицины, выступает одним из инструментов обеспечения этого уровня, особенно в условиях ограниченного доступа к очным консультациям. Примером влияния информационных технологий на указанное право служит положение ст. 7 Конвенции Международной организации труда № 164 «О здравоохранении и медицинском обслуживании моряков», в которой говорится, что компетентный орган власти обеспечивает с помощью заранее созданной системы, чтобы суда в море получали медицинскую консультацию по радио или по спутниковой связи, включая консультацию специалиста, в любой час дня или ночи⁶⁰. Данная норма предполагает использование телемедицинских технологий, чтобы обеспечить моряков такой медицинской помощью, которая должна быть приемлема и качественна в условиях ее дистанционного оказания, что позволяет оперативно получать специализированную помощь и тем самым повышать качество медицинского обслуживания в экстремальных условиях. Следовательно, телемедицинские технологии обеспечивают доступность квалифицированной медицинской помощи в удаленных условиях морского плавания, что является практической реализацией обязательств государства по созданию предусмотренной Конвенцией медицинском обслуживании моряков.

Другой пример использования телемедицинских технологий в целях реализации права на наивысший достижимый уровень здоровья заключается в следующем.

Помимо глобальных инициатив, тенденция к правовому закреплению телемедицинских технологий отчетливо прослеживается и на международном региональном уровне. Ярким примером служит Соглашение о сотрудничестве государств – участников СНГ в создании совместимых национальных телемедицинских систем и дальнейшем их развитии, и использовании от 19 ноября 2010 года.

⁶⁰ Конвенция о здравоохранении и медицинском обслуживании моряков. URL: https://www.ilo.org/sites/default/files/wcmsp5/groups/public/@ed_norm/@normes/documents/normativeinstrument/wcms_c164_ru.htm (дата обращения: 28.03.2025)

Положения Соглашения определяют механизмы имплементации актуальных технологических и управленческих новаций в сфере охраны здоровья. Документ также устанавливает унифицированные регуляторные подходы на пространстве договаривающихся государств к формированию совместимых национальных телемедицинских систем и фиксирует основные принципы и основополагающие начала сотрудничества в области оказания медпомощи с применением дистанционных технологий.

Как отметил И.В. Григорьев, указанным Соглашением закрепляется «необходимость создания Сторонами совместных национальных телемедицинских систем или обеспечения совместимости существующих национальных телемедицинских систем в целях обеспечения в государствах - участниках Соглашения условий для оказания квалифицированных телемедицинских услуг при гарантированной государствами защищенности прав и законных интересов физических и юридических лиц в процессе получения и предоставления медицинской помощи»⁶¹.

24 мая 2024 года были одобрены изменения в указанном Соглашении, обусловленные развитием информационных технологий в здравоохранении. Изменения направлены на уточнение и расширение взаимодействия стран – участников СНГ в создании единого информационного медицинского пространства, основанного на интеграции региональных и национальных телемедицинских консультационно-диагностических систем. Это учитывает новые возможности для предоставления телемедицинских услуг гражданам этих стран, включая высокотехнологичную и профессиональную медицинскую помощь с использованием современных инфокоммуникационных технологий⁶².

⁶¹ Григорьев И. В. Международно-правовая регламентация медицинской помощи с применением телемедицинских технологий // Право и политика. 2024. №. 12. С. 132-142.

⁶² На заседании Совета глав правительств СНГ утверждены изменения в Соглашение о сотрудничестве в создании совместимых национальных телемедицинских систем. URL: <https://e-cis.info/news/564/118441/> (дата обращения: 28.03.2025); Протокол о внесении изменений в Соглашение о сотрудничестве государств - участников СНГ в создании совместимых национальных телемедицинских систем и дальнейшем их развитии и использовании от 19 ноября 2010 года. URL:

Так, в ст. 2 Соглашения заменен термин «телемедицина» на «телемедицинские технологии», которые определены как «информационные технологии, обеспечивающие дистанционное взаимодействие медицинских работников между собой, с пациентами и (или) их законными представителями, идентификацию и аутентификацию указанных лиц, документирование совершаемых ими действий при проведении консилиумов, консультаций, дистанционного медицинского наблюдения за состоянием здоровья пациента»⁶³.

Кроме того, на международном уровне приняты акты, направленные на решение этических вопросов, возникающих в результате применения информационных технологий, а также акты, содержащие нормы относительно соблюдения и защиты прав человека в результате применения данных технологий.

Так, в 2021 году ЮНЕСКО опубликовала Рекомендацию по этике искусственного интеллекта, которая устанавливает глобальные этические стандарты для искусственного интеллекта⁶⁴, направленные на реализацию основных ценностей и принципов в целях защиты прав человека, обеспечения равноправия и справедливости и развития сферы здравоохранения⁶⁵, а в 2024 году Совет Европы принял первый международный договор, касающийся искусственного интеллекта, – Рамочную Конвенцию об искусственном интеллекте, правах человека, демократии и верховенстве права. Эта Конвенция направлена на то, чтобы проектирование, разработка и применение систем искусственного интеллекта полностью соответствовали требованию уважения прав человека, к тому же она имеет потенциал стать первым юридически обязательным

https://www.mid.ru/ru/foreign_policy/international_contracts/international_contracts/multilateral_contract/62714/ (дата обращения: 28.03.2025)

⁶³ Протокол о внесении изменений в Соглашение о сотрудничестве государств - участников СНГ в создании совместимых национальных телемедицинских систем и дальнейшем их развитии и использовании от 19 ноября 2010 года. URL: https://www.mid.ru/ru/foreign_policy/international_contracts/international_contracts/multilateral_contract/62714/ (дата обращения: 28.03.2025)

⁶⁴ Рекомендация об этических аспектах искусственного интеллекта. URL: https://unesdoc.unesco.org/ark:/48223/pf0000380455_rus (дата обращения: 28.03.2025)

⁶⁵ Умнова-Конюхова И. А. Искусственный интеллект и международное право: настоящее и будущее // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4, Государство и право. 2025. №. 3. С. 63-75.

международным договором (для всех подписавших ее сторон), специально ориентированным на искусственный интеллект⁶⁶.

Однако несмотря на формально свой «юридически обязательный» статус Конвенции, в ней отсутствуют «сильные» механизмы правоприменения. Кроме того, широкие, основанные на принципах положения Конвенции могут привести к расхождениям в толковании и применении между участниками, что потенциально может подрвать согласованные международные стандарты.

Конвенция применяется к государственным органам или негосударственным организациям, действующим от их имени путем делегирования полномочий, но по умолчанию не распространяется на деятельность негосударственных организаций. Государства-участники обладают большой гибкостью - они могут решить, как устранять риски, возникающие в течение жизненного цикла систем искусственного интеллекта. В частности, они могут выбрать применение правил и принципов, изложенных в Конвенции, или принять другие соответствующие меры для устранения рисков и воздействия, возникающих в результате деятельности искусственного интеллекта. Однако в тексте Конвенции не разъясняется, какими могут быть эти «другие надлежащие меры» и в чем конкретно заключается это обязательство.

Отсутствие ясности может негативно сказаться на определенности и предсказуемости национального закона, поставив под угрозу общую цель Конвенции, которая заключается в обеспечении соответствия всех видов деятельности в рамках жизненного цикла системы искусственного интеллекта правам человека, демократии и верховенству закона⁶⁷. Риск представляется еще более серьезным, учитывая ту важную роль, которую играет частный сектор в разработке и внедрении систем искусственного интеллекта.

⁶⁶ Committee on Artificial Intelligence (CAI) - Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. URL: [https://search.coe.int/cm#{%22CoEIdentifier%22:\[%220900001680afb11f%22\],%22sort%22:\[%22CoEValidationDate%20Descending%22\]}](https://search.coe.int/cm#{%22CoEIdentifier%22:[%220900001680afb11f%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}) (дата обращения: 28.03.2025)

⁶⁷ Karolína Babická, Cristina Giacomini. Understanding the Scope of the Council of Europe Framework Convention on AI. URL: <https://opiniojuris.org/2024/11/05/understanding-the-scope-of-the-council-of-europe-framework-convention-on-ai/> (дата обращения: 28.03.2025)

Тем не менее, стоит подчеркнуть, что Рамочная Конвенция об искусственном интеллекте, правах человека, демократии и верховенстве права предлагает ценную правовую основу для глобального управления искусственным интеллектом. Ее успех в конечном итоге будет зависеть от широкой ратификации, качественной реализации и устранения существующих ограничений. По мере развития технологий искусственного интеллекта устойчивая приверженность государств идеям Конвенции, постоянное участие многих заинтересованных сторон и готовность к адаптации будут иметь решающее значение для реализации потенциала Конвенции в качестве международного руководства по ответственному развитию искусственного интеллекта в глобальном масштабе.

Таким образом, по итогам рассмотрения материала данного параграфа можно выделить следующие наблюдения.

1. При изучении правового регулирования применения информационных технологий в здравоохранении на международном уровне установлено, что права человека, закрепленные в международных правовых актах, влияют на развитие, внедрение и использование информационных технологий в здравоохранении.

2. Рассмотренные международные документы подчеркивают важность уважения прав человека, защиты частной жизни и обеспечения доступа к новым технологиям, что является ключевым для адаптации права к технологической трансформации здравоохранения.

Имеющиеся среди них акты «мягкого права» (например, Всеобщая декларация о биоэтике и правах человека) задают необязательные к исполнению, но важные концептуальные и этические ориентиры. Применительно к России, их значение заключается в формировании «дорожной карты» для национального законодателя, позволяя избежать концептуальных ошибок и заранее выявить системные риски, такие как цифровое неравенство или несовместимость стандартов данных.

В недавних международных инициативах, таких как Рамочная Конвенция об искусственном интеллекте 2024 года, наблюдается стремление к более системному

регулированию новых технологий. Этот документ акцентирует внимание на необходимости участия всех заинтересованных сторон в процессе разработки и применения искусственного интеллекта, что может способствовать более эффективной защите прав человека и демократических ценностей. Однако, несмотря на ее значимость, существует ряд проблем, включая отсутствие четких механизмов правоприменения, а также присутствие широко сформулированных положений, которые могут привести к расхождениям в толковании и применении между участниками.

3. Право на наивысший достижимый уровень здоровья предполагает возможность доступа к различным объектам, товарам, услугам и условиям, которые являются необходимыми для достижения наивысшего уровня здоровья, а также учитывает право на доступ к медицинским технологиям.

В связи с тем, что многие государства являются странами-участниками международных конвенций и договоров, в которых закрепляется право на наивысший достижимый уровень здоровья, право на доступ к медицинским технологиям, право на неприкосновенность частной жизни, страны обязаны на национальном уровне обеспечить защиту указанных прав человека. В этой связи в следующем параграфе настоящего исследования будет рассмотрено законодательство зарубежных стран, которые устанавливают правовое регулирование применения информационных технологий в здравоохранении в целях реализации и соблюдения прав человека в условиях цифровизации.

§ 3. Основные зарубежные модели правового регулирования применения информационных технологий в здравоохранении

Как было установлено ранее в настоящем исследовании, на международном уровне сформирована авторитетная правовая основа для реализации права на неприкосновенность частной жизни, права на доступ к медицинским технологиям и права на наивысший достижимый уровень здоровья. Теперь следует обратиться

к опыту тех зарубежных стран, которые обеспечили во внутреннем законодательстве надежные гарантии защиты и соблюдения данных прав, а также выработали правовые механизмы решения проблем, связанных с применением информационных технологий, посредством совершенствования национального законодательства.

В различных национальных юрисдикциях используются разные подходы к правовому регулированию применения информационных технологий в сфере здравоохранения. Сравнительный анализ может дать ценную информацию о передовой практике и потенциальных проблемах, способствуя определению правовых доктрин, эффективно решающих проблемы, связанные с технологическим прогрессом.

В связи с этим, целесообразно обратиться к национальному законодательству стран, которые признаются передовыми в части внедрения информационных технологий и правового урегулирования их использования в сфере здравоохранения. Это позволит провести более детальный сравнительно-правовой анализ и сделать выводы о возможности учета зарубежного опыта при совершенствовании правового регулирования применения информационных технологий в здравоохранении в рамках отечественного законодательства.

Выбор для дальнейшего изучения таких стран, как США, Швейцария, Германия, Австрия, Франция, Великобритания, Финляндия, КНР обусловлен их передовым опытом в области регулирования применения информационных технологий в здравоохранении и схожестью технологических вызовов, стоящих перед Российской Федерацией, а также общей проблематикой, связанной с влиянием информационных технологий на конституционные права граждан, в частности, с развитием:

- электронных медицинских карт (EHR/EMR);
- медицинских информационных систем;
- телемедицинских технологий;
- искусственного интеллекта и машинного обучения в здравоохранении;

- технологии Интернета вещей в здравоохранении;
- средств обеспечения кибербезопасности и защиты от утечек медицинских данных.

Это общее проблемное поле делает сравнение осмысленным, показывая, что государства ищут правовые ответы на одни и те же вызовы.

Для американского подхода, основанного на принципах рыночной экономики, стимулирования инноваций и минимизации прямого государственного вмешательства, характерна фрагментированная регулятивная система, то есть разделенная на два территориальных уровня публичной власти федеративного государства (федеральный уровень и уровень штатов). Также здесь упор делается на стимулирование инноваций через Управление по санитарному надзору за качеством пищевых продуктов и медикаментов (FDA) (одобрение технологий Интернета вещей как медицинских устройств - Software as a Medical Device, SaMD). Акцент на концепции SaMD является не столько правовым, сколько экономико-стратегическим решением, направленным на сохранение глобального лидерства США в сфере информационных технологий в здравоохранении. Лоббирование отраслевых ассоциаций привело к созданию «предсказуемых путей» одобрения различных информационных технологий, что снижает барьеры для выхода на рынок венчурного капитала. Таким образом, право в США служит прямым инструментом поддержки национального технологического бизнеса.

В отличие от конституций многих других стран, Конституция США не гарантирует прямо право на медицинскую помощь или охрану здоровья. Это фундаментальным образом влияет на всю систему здравоохранения, включая информационные технологии. Регулирование носит рамочный характер и имеет своей основной целью развитие инноваций, а не обеспечение универсального доступа к информационным медицинским услугам как блага.

Поправка IV к Конституции США (неприкосновенность личности и имущества) является основой для защиты медицинских данных от необоснованного вмешательства со стороны государства. Данная поправка стала

конституционной основой для судебных решений, ограничивающих доступ государственных органов к персональным данным, включая медицинские, без надлежащего судебного разрешения⁶⁸.

Поправка XIV (раздел 1) запрещает ограничение со стороны штатов привилегий и льгот граждан и устанавливает обязанность штатов обеспечивать равную защиту на основе законов. Это оказывает опосредованное влияние на правовое регулирование использования алгоритмов искусственного интеллекта, которые должны быть свободны от предвзятости, чтобы не дискриминировать пациентов по расовому, гендерному или иному признаку⁶⁹.

Таким образом, регулирование применения информационных технологий в здравоохранении в США является предметом совместного ведения федерального центра и штатов. Это приводит к созданию сложной, многоуровневой правовой системы.

Подход европейского законодательства основан на конституционных правах человека, особенно на праве на неприкосновенность частной жизни и защиту персональных данных. Регулятивная система гармонизирована и централизована (регламенты прямого действия). Общий регламент ЕС о защите данных (GDPR) и Регламенты о медицинских изделиях (MDR/IVDR) создают очень строгие, но предсказуемые «рамочные» условия для всех участников рынка. Правоприменение – жесткое со значительными штрафами от надзорных органов.

Национальное законодательство стран ЕС в области регулирования информационных технологий базируется на Хартии основных прав Европейского Союза, закрепившей конституционные права.

Ее ст. 3 гарантирует уважение физической и психической целостности человека, что непосредственно относится к медицинским вмешательствам, включая использование в этом процессе информационных технологий⁷⁰.

⁶⁸ Конституция Соединенных Штатов Америки. URL: <https://www.wipo.int/wipolex/ru/legislation/details/21129> (дата обращения: 15.09.2024)

⁶⁹ Там же.

⁷⁰ Хартия Европейского союза об Основных правах. URL: <https://eulaw.ru/treaties/charter/> (дата обращения: 15.09.2024)

Статья 7 о праве на уважение частной и семейной жизни, а также ст. 8 о защите персональных данных формируют основу для регулирования обработки медицинских данных, которые относятся к особо защищаемым категориям персональных данных⁷¹.

Статья 35 о праве на охрану здоровья гарантирует высокий уровень охраны здоровья человека при определении и осуществлении политики и деятельности ЕС⁷².

Регулирование применения информационных технологий в здравоохранении должно соответствовать принципам пропорциональности и субсидиарности. Согласно этим принципам, действия ЕС должны быть соразмерны поставленным целям и предприниматься на уровне, максимально близком к гражданину.

В отличие от европейской модели подход Китая к регулированию информационных технологий в здравоохранении имеет иную природу и выступает, прежде всего, инструментом государственного управления и социального контроля. Он сочетает жесткое централизованное регулирование с активным поощрением национальных компаний. Многие Законы КНР дают государству широкий доступ к данным о гражданах в интересах «национальной безопасности» и «общественного благосостояния».

Конституция КНР устанавливает верховенство государства в регулировании ключевых отраслей, включая здравоохранение. Это обеспечивает централизованный контроль над внедрением информационных технологий в этой области⁷³.

Статья 21 Конституции КНР гарантирует право на охрану здоровья народа, развивает медико-санитарное дело, современную и традиционную отечественную медицину. В цифровую эпоху это интерпретируется как обеспечение доступа к телемедицине и электронным медицинским услугам⁷⁴.

⁷¹ Там же.

⁷² Там же.

⁷³ Конституция КНР 1982 г. (с изм. 1988, 1993, 1999, 2004 гг.). URL: https://chinalawinfo.ru/constitutional_law/constitution (дата обращения: 15.09.2024)

⁷⁴ Там же.

Если в сравнении с указанными зарубежными моделями предварительно охарактеризовать российский подход, то можно сказать, что пока он находится в стадии формирования и представляет собой гибридную модель с сильным влиянием европейских норм (в части защиты данных) и сильным влиянием логики государственного суверенитета.

К примеру, в России принят аналог Общего регламента ЕС о защите данных (Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»), есть нормы о телемедицинских технологиях, электронных медицинских картах. Ключевая особенность – требование к локализации данных и глубокой интеграции информационно-технологических систем с государственными информационными системами (пример – Единая государственная информационная система в области здравоохранения).

Статья 41 Конституции Российской Федерации гарантирует каждому право на охрану здоровья и медицинскую помощь⁷⁵; ст. 23 обеспечивает право на неприкосновенность частной жизни, личную и семейную тайну, что напрямую относится к защите медицинских данных⁷⁶; часть 1 ст. 24 запрещает сбор, хранение и распространение информации о частной жизни без согласия лица⁷⁷; часть 2 ст. 24 гарантирует право каждого на ознакомление с документами и материалами, непосредственно затрагивающими его права и свободы⁷⁸; ст. 29 гарантирует свободу информации⁷⁹. Эти конституционные нормы формируют основу для регулирования применения информационных технологий в здравоохранении, обеспечивая баланс между инновациями и защитой прав граждан в России.

Более подробный анализ российского подхода и проблемы, которые возникают в связи применением информационных технологий и касаются

⁷⁵ Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // «Российская газета», № 237 (853).

⁷⁶ Там же.

⁷⁷ Там же.

⁷⁸ Там же.

⁷⁹ Там же.

обеспечения и защиты соответствующих конституционных прав, будут представлены во второй главе диссертации.

У каждой национальной модели правового регулирования есть свои сильные и слабые стороны, сложно выделить лучшую из них: американская гибкость стимулирует инновации, но может страдать от фрагментированности; европейская защита прав высока, но порождает высокие издержки. КНР преследует цели усиленного государственного контроля.

Поэтому сравнение регулятивных подходов США, ЕС, КНР и России в области информационных технологий в здравоохранении уместно и ценно, особенно учитывая, что Германия и Франция входят в ту же правовую семью, что и Россия. Законодательство США интересно России в том плане, что оно гибкое и предполагает развитие инноваций. К тому же отдельные нормативные правовые акты штатов позволяют решить многие проблемы, связанные с применением информационных технологий в сфере здравоохранения, которые имеются в России. Иначе говоря, сравнительный анализ проводится с учетом того, что правовые решения анализируются не в вакууме, а в конкретных социально-правовых условиях, важно осознавать невозможность прямого копирования правовых институтов без учета национального правового, социального и культурного контекста.

Анализ зарубежных концепций регулирования применения информационных технологий в здравоохранении основывается на выделении трех правовых моделей.

Первую группу составят акты, содержащие общие нормы, которые касаются информационных технологий в здравоохранении.

Во второй группе находятся те акты, в которых дано фрагментированное (двухуровневое) регулирование применения информационных технологий в сфере здравоохранения.

И третья группа включает в себя специализированные акты, направленные строго на регулирование применения информационных технологий в здравоохранении.

3.1. Рамочное правовое регулирование применения информационных технологий в сфере здравоохранения

Базовые нормы, направленные на регулирование применения информационных технологий в сфере здравоохранения, содержатся в федеральных законах, которые обеспечивают защиту прав граждан в условиях цифровизации общества.

Наглядным примером рамочного регулирования применения информационных технологий в сфере здравоохранения является Закон о переносимости и подотчетности медицинского страхования США от 21 августа 1996 г. (Health Insurance Portability and Accountability Act) – основной нормативный акт в сфере безопасности и конфиденциальности медицинских данных, обеспечения безопасности охраняемой информации о состоянии здоровья человека, регулирующий использование и раскрытие защищенной медицинской информации на любом носителе, а также сбор, использование, хранение или передачу электронной информации⁸⁰.

Когда медицинская информация хранится в определенных типах организаций здравоохранения, таких как больницы, она называется защищенной медицинской информацией. Защищенной называется любая медицинская информация с идентификатором, который связывает конкретного пациента с медицинской информацией (имя, номер социального страхования, номер телефона, адрес электронной почты, почтовый адрес и т. д.)⁸¹.

⁸⁰ Health Insurance Portability and Accountability Act of 1996. URL: <https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996> (дата обращения: 15.09.2024)

⁸¹ Edemekong PF, Annamaraju P, Haydel MJ. Health Insurance Portability and Accountability Act. [Updated 2024 Feb 12]. In: StatPearls [Internet]. Treasure Island (FL): StatPearls Publishing; 2024 Jan-. Available from: <https://www.ncbi.nlm.nih.gov/books/NBK500019/>.

Закон о переносимости и подотчетности медицинского страхования требует от поставщиков медицинских услуг и организаций защищать конфиденциальную информацию о пациентах независимо от того, осуществляется ли лечение традиционными методами или с использованием современных технологий, таких как телемедицинские технологии. Закон обязывает предоставлять пациентам полный доступ к своей защищенной медицинской информации, ограничивая доступ к ней других лиц. Медицинское учреждение, в котором произошла утечка подобной информации, может быть оштрафовано. Следовательно, поставщики медицинских услуг должны принимать необходимые меры для защиты электронных передач от несанкционированного просмотра.

Аналогичным образом Правила конфиденциальности Закона о переносимости и подотчетности медицинского страхования, изданные Министерством здравоохранения и социальных служб США для реализации Закона о переносимости и подотчетности медицинского страхования, одинаковы по отношению к сбору, хранению, доступу и раскрытию защищенной медицинской информации, независимо от того, находится ли информация в бумажной или электронной форме. Таким образом, Закон о переносимости и подотчетности медицинского страхования содержит положения, которые оказались адаптивными к развитию электронного обмена информацией, создав тем самым эффективную правовую основу для передачи медицинской информации. Помимо указанного эти правила устанавливают стандарт для деидентификации⁸² защищенной медицинской информации⁸³.

⁸² Деидентификация или анонимизация данных защищенной медицинской информации — это процесс шифрования любой информации в медицинской документации, которая может быть использована для идентификации человека; которая была создана, использована или раскрыта в ходе предоставления медицинской услуги, такой как диагностика или лечение. Деидентификация обеспечивается с помощью функции «человек в цикле» для большей точности анонимизации конфиденциальных данных в текстовом контенте. Этот подход использует методы деидентификации Закона о переносимости и подотчетности медицинского страхования, включая экспертное определение и «безопасную гавань», для преобразования, маскировки, удаления или иного сокрытия конфиденциальной информации.

⁸³ Office for Civil Rights (OCR), 2002. Standards for privacy of individually identifiable health information. Final rule. Federal Register, 67(157), p.53181, §164.514 (a).

Если сравнивать законодательство других стран в области общего правового регулирования, то примечательным является европейское правовое пространство. Общеввропейское законодательство включает помимо законодательства ЕС законодательство стран-участниц ЕС, а также некоторых отдельных европейских государств, не входящих в состав союза. В результате чего возник более разносторонний подход, охватывающий все государства-члены, установивший жесткие требования и наложивший большую ответственность в отношении производителя медицинских устройств в целях защиты прав пациентов. Одним из важных актов в ЕС как наглядный пример общего регулирования является Общий регламент о защите данных от 27 апреля 2016 года г. (General Data Protection Regulation - 2016/679), который направлен на обеспечение конфиденциальности, целостности и доступности любой передаваемой информации⁸⁴. Он применяется с 25 мая 2018 года (ст. 99) во всех государствах-членах ЕС и открывает новую эру в развитии законодательства о защите данных в ЕС.

В контексте организации системы здравоохранения особенно актуально определение «данных, касающихся здоровья» в соответствии с пунктом 15 ст. 4 Общего регламента ЕС о защите данных: «персональные данные, относящиеся к физическому или психическому здоровью физического лица, включая предоставление медицинских услуг, которые раскрывают информацию о состоянии его здоровья»⁸⁵.

Таким образом, по сравнению с Законом о переносимости и подотчетности медицинского страхования США Общий регламент ЕС о защите данных гораздо шире по своей сфере действия, так как американский Закон охватывает только конкретную медицинскую информацию, относящуюся к подпадающим под Закон организациям или их «деловым партнерам». При этом согласно пункту 1 ст. 3 Общего регламента ЕС о защите данных акт применяется к обработке персональных данных в контексте деятельности образованного в ЕС контролера

⁸⁴ General Data Protection Regulation. URL: <https://gdpr-info.eu/> (дата обращения: 28.11.2024)

⁸⁵ Там же.

или обработчика, независимо от того, происходит ли обработка в ЕС или за его пределами (понятия «контролер» и «обработчик» раскрываются в ст. 4). Разница между контролером и обработчиком данных заключается в том, что первый устанавливает цели обработки данных, которые должны определять порядок обращения с персональными данными и которые могут быть полностью раскрыты субъекту данных. Вторым обычно является доверенное лицо контролера данных, внутреннее или внешнее по отношению к его организации, которое «обрабатывает персональные данные в соответствии с целями, установленными контролером данных»⁸⁶. Дополнительно стоит отметить, что Общий регламент ЕС о защите данных в отношении контролера или обработчика, не созданного в ЕС, будет применяться только в том случае, если их деятельность будет направлена на пациентов в ЕС.

Общий регламент ЕС о защите данных закрепляет ряд важных гарантий для субъектов данных в связи с использованием систем искусственного интеллекта. В частности, согласно ст. 13, 14 Общего регламента ЕС о защите данных при сборе персональных данных контролеры данных, как правило, должны предоставлять субъектам данных информацию о «существовании автоматизированного принятия решений, включая профилирование, упомянутое в пунктах 1 и 4 ст. 22, и, по крайней мере, в этих случаях, предоставлять содержательную информацию о задействованной логике, а также о значении и предполагаемых последствиях такой обработки для субъекта данных»⁸⁷ (понятие «профилирование» раскрывается в ст. 4).

Термин «автоматизированное принятие решений» означает решение, которое принимается без участия человека исключительно с помощью

⁸⁶ *Carmi, L., Zohar, M., & Riva, G. M. (2023). The European General Data Protection Regulation (GDPR) in mHealth: Theoretical and practical aspects for practitioners' use. Medicine, Science and the Law, 63(1), 61-68.*

⁸⁷ General Data Protection Regulation. URL: <https://gdpr-info.eu/> (дата обращения: 28.11.2024)

автоматизированных средств⁸⁸. Вышеуказанная информация включает в себя автоматизированную систему принятия решений, принцип работы этой системы в целом, прогнозируемые последствия, а также другие функциональные возможности данной системы, такие как «ветви» решений и классификационные структуры⁸⁹.

Также в целях реализации европейской стратегии в области персональных данных были разработаны предложения для Регламента ЕС по использованию и обмену электронными данными о здоровье от 11 февраля 2025 г. (European Health Data Space and amending Directive), который является первым документом об общем пространстве персональных данных в здравоохранении⁹⁰. Основным элементом предложений для Регламента ЕС по использованию и обмену электронными данными о здоровье является разграничение между первичным использованием и вторичным использованием⁹¹. То есть указанные предложения предоставляют людям возможность контролировать свои медицинские данные и облегчить обмен данными для оказания медицинской помощи на территории ЕС (первичное использование данных) и способствует созданию подлинного единого рынка электронных медицинских карт, а также обеспечивает последовательную систему повторного использования медицинских данных для исследований, инноваций, разработки политики и нормативной деятельности (вторичное использование данных)⁹².

⁸⁸ Working Party on the Protection of Individuals with Regard to the Processing of Personal Data. Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679. WP251rev.01; 2018.

⁸⁹ Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the general data protection regulation. *International data privacy law*, 7(2), pp. 76-99.

⁹⁰ Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847. URL: <https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng> (дата обращения: 28.11.2024)

⁹¹ Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space COM/2022/197 final. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0197> (дата обращения: 28.11.2024)

⁹² Там же.

Еще одним ключевым элементом предложений для Регламента ЕС по использованию и обмену электронными данными о здоровье является механизм использования данных «по желанию/отказу» в соответствии с Общим регламентом ЕС о защите данных. В этой системе для первичного использования требуется подход «opt-in»: пациент может контролировать и, следовательно, явно выражать согласие/несогласие на использование своих данных. Для вторичного использования данных предпочтителен подход «opt-out», при котором человек может отозвать свое согласие, не ограничиваясь основной целью оказания медицинской помощи, например, в исследовательских целях.

Законодательство Китая также предусматривает систему общего регулирования вопросов применения информационных технологий в здравоохранении.

Ярким примером такого регулирования выступает принятый 20 августа 2021 г. Закон КНР о защите персональной информации (Personal Information Protection Law), обеспечивающий последовательную правовую базу для защиты персональной информации, включая медицинские данные. С 2016 года представительные органы и соответствующие учреждения Китая выпускают программные документы по снижению рисков конфиденциальности персональных данных в здравоохранении, что, по мнению исследователя Синьюань Ши, позволило усовершенствовать потенциал Китая в области защиты конфиденциальности больших данных в здравоохранении (Руководящие мнения по продвижению и стандартизации развития приложений больших данных в здравоохранении, Руководящие принципы технической проверки мобильных медицинских устройств, Национальные стандарты больших данных в здравоохранении, безопасность и управление услугами и др.)⁹³. Правительство Китая также запретило незаконную обработку, торговлю или раскрытие личной медицинской информации в ст. 92 Закона КНР о базовом медицинском

⁹³ Shi, X. (2024). Reducing privacy risks of China's healthcare big data through the policy framework. *Frontiers in Public Health*, 12, pp 1-9.

обслуживании и укреплении здоровья от 28 декабря 2019 г. (Law of the People's Republic of China on Basic Medical and Health Care and Promotion of Health)⁹⁴.

В Законе КНР о защите персональной информации такая информация определяется в ст. 73 как «различная информация, относящаяся к идентифицированным или идентифицируемым физическим лицам, записанную в электронном виде или с помощью других средств»⁹⁵. В нем проводится различие между персональной информацией и «чувствительной» персональной информацией, а для определения «чувствительной» персональной информации применяется система критериев, предполагающая два уровня дифференциации, при этом он не запрещает обработку «чувствительных» персональных данных; вместо этого он предусматривает более строгие обязанности для обработчиков персональных данных.

В соответствии со ст. 6 Закона о защите персональной информации КНР при обработке личной информации должен соблюдаться принцип ограничения целей. Это означает, что сбор личной информации должен быть минимальным и не должен быть чрезмерным по отношению к цели обработки. В целях ограничения получения избыточного количества информации, получаемой с мобильных медицинских приложений, было выпущено Положение об объеме необходимой личной информации для общих типов мобильных приложений от 12 марта 2021 г. (Provisions on the Scope of Necessary Personal Information for Common Types of Mobile Internet Applications). В этом Положении перечислены 39 различных категорий мобильных приложений и указаны типы личной информации, которые считаются необходимыми для поддержания основных функций и услуг этих приложений⁹⁶. Следовательно, любой сбор личной информации за пределами

⁹⁴ Law of the People's Republic of China on Basic Medical and Health Care and Promotion of Health. URL: http://en.moj.gov.cn/2021-06/26/c_636455.htm (дата обращения: 28.11.2024)

⁹⁵ Personal Information Protection Law of the People's Republic of China. URL: <https://personalinformationprotectionlaw.com/PIPL/category/general-provisions/definitions/> (дата обращения: 28.11.2024)

⁹⁶ Provisions on the Scope of Necessary Personal Information for Common Types of Mobile Internet Applications. URL: <https://www.chinalawtranslate.com/en/necessary-app-info/> (дата обращения: 28.11.2024)

установленного объема может считаться незаконным. Например, в ст. 5 данного Положения для телемедицинских приложений, предназначенных для онлайн-консультаций и записи на прием, необходимая персональная информация включает номер мобильного телефона зарегистрированного пользователя; имя пациента, его идентификационный номер, информацию о больнице и отделении, необходимую для записи на прием; описание заболеваний, которые являются предметом консультаций⁹⁷. Эти правила дополняют принцип ограничения целей, предусмотренный Законом о защите персональной информации КНР при обработке личной информации, предоставляя конкретизированные и детализированные указания для операторов мобильных приложений.

Для законной обработки медицинских данных требуется одно или несколько правовых оснований, указанных в ст. 13 Закона КНР о защите персональной информации, например, согласие или реагирование на чрезвычайные ситуации в области здравоохранения⁹⁸. Важно отметить, что, когда в качестве правового основания для обработки медицинских данных используется согласие, необходимо получить «отдельное согласие» от отдельных лиц (ст. 29), тогда как для обработки личной информации, которая не является конфиденциальной, требуется только согласие. Если другие законы или нормативные акты разрешают обработку медицинских данных, это также может быть использовано в качестве законного основания.

Отдельное согласие является уникальным для Закона КНР о защите персональной информации. Это защитная мера, которая в ст. 29 устанавливает, что обработчик личной информации не должен получать согласие физического лица в целом, смешивая различное содержание, цели обработки и виды деятельности по обработке личной информации, требующие согласия. Вместо этого должно быть отдельное согласие между различными действиями по сбору личной информации.

⁹⁷ Там же.

⁹⁸ Там же.

Данное положение устанавливает более строгие требования к обработке конфиденциальной личной информации.

Если Закон КНР о защите персональной информации выделяет шесть исключений из информированного согласия, то в §164.502(a) Закона о переносимости и подотчетности медицинского страхования США предусмотрены исключения для получения согласия, в том числе, когда информация используется «в медицинских исследованиях и для других видов деятельности в области общественного здравоохранения»⁹⁹. А ст. 9 Общего регламента ЕС о защите данных, напротив, устанавливает «исключения для обработки специальных категорий персональных данных»¹⁰⁰. В отношении данных о здоровье обработка персональных данных запрещена, если не соблюдены определенные условия. В отличие от этого, исключения из Закона КНР о защите персональной информации для здравоохранения сформулированы как необходимые для реагирования на внезапные инциденты в области общественного здравоохранения или защиты жизни, здоровья и безопасности имущества физических лиц в чрезвычайных условиях¹⁰¹.

С точки зрения баланса интересов, китайская модель демонстрирует явный перекос в сторону государственного контроля и национальной безопасности в ущерб индивидуальной автономии и приватности, что проявляется в широких исключениях из требования согласия.

В отличие от Закона КНР о защите персональной информации, Общий регламент ЕС о защите данных имеет более широкую сферу применения: когда контролеры данных делают персональные данные общедоступными, они обязаны

⁹⁹ Health Insurance Portability and Accountability Act of 1996. URL: <https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996> (дата обращения: 15.09.2024)

¹⁰⁰ General Data Protection Regulation. URL: <https://gdpr-info.eu/> (дата обращения: 28.11.2024)

¹⁰¹ Personal Information Protection Law of the People's Republic of China. URL: <https://personalinformationprotectionlaw.com/PIPL/category/general-provisions/definitions/> (дата обращения: 28.11.2024)

по требованию субъекта стереть его персональные данные¹⁰². Контролеры данных не просто удаляют данные, находящиеся под их контролем, но и обязаны уведомить другие третьи стороны о необходимости прекратить использование и удалить данные, которые они публично распространили. Аналогичное положение отсутствует в Правиле конфиденциальности Закона о переносимости и подотчетности медицинского страхования США. Это правило не требует изменения данных для медицинских карт или других записей.

Иным заметным примером рамочного регулирования является принятый в 2024 году Европейским парламентом Закон об искусственном интеллекте от 13 июня 2024 г. (Регламент (ЕС) 2024/1689), установивший гармонизированные правила в области искусственного интеллекта, в том числе четкие требования и обязательства в отношении конкретных видов использования искусственного интеллекта.

Так, согласно ст. 6 Закона об искусственном интеллекте ЕС системам искусственного интеллекта присваивается высокий риск, если они негативно влияют на безопасность выпускаемого продукта (или иным образом подпадают под действие законодательства ЕС о гармонизации здравоохранения и безопасности) или нарушают основные права человека¹⁰³. К ним относятся в том числе медицинские устройства. Поэтому в сфере здравоохранения эти требования в первую очередь распространяются на медицинские устройства с искусственным интеллектом, которые должны пройти оценку соответствия третьей стороной в соответствии с Положением ЕС о медицинских устройствах, как следует из подпункта «б» пункта 1 ст. 6 Закона об искусственном интеллекте. Это означает, что к системам искусственного интеллекта высокого риска относятся медицинские изделия класса риска IIa и выше, используемые в медицинских целях для

¹⁰² General Data Protection Regulation. URL: <https://gdpr-info.eu/> (дата обращения: 28.11.2024)

¹⁰³ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng> (дата обращения: 28.11.2024)

диагностики, профилактики, мониторинга, прогнозирования, лечения или облегчения состояния при заболеваниях, травмах или инвалидности и использующие искусственный интеллект¹⁰⁴.

Большинство других видов искусственного интеллекта, связанных со здоровьем, которые не направлены только на медицинские цели, считаются искусственным интеллектом с низким уровнем риска (класс I). Сюда входят такие системы искусственного интеллекта, которые используются для улучшения самочувствия, укрепления здоровья или мониторинга активности. Например, искусственный интеллект, отслеживающий настроение и самочувствие или предлагающий персональные рекомендации по питанию на основе данных пациента, а также датчики на базе искусственного интеллекта, используемые для оказания помощи пожилым людям.

Важно отметить, что некоторые разделы Закона об искусственном интеллекте ЕС касаются непосредственно здравоохранения. В частности, в Приложении III Закона об искусственном интеллекте ЕС указывается, что к системам искусственного интеллекта высокого риска, к которым предъявляются самые строгие нормативные требования, относятся системы искусственного интеллекта, «предназначенные для использования государственными органами или от имени государственных органов для оценки права физических лиц на получение основных государственных пособий и услуг, включая услуги здравоохранения, а также для предоставления, сокращения, отмены или истребования таких пособий и услуг»¹⁰⁵. В группу повышенного риска также входят системы искусственного интеллекта, «предназначенные для оценки и классификации вызовов экстренных служб физическими лицами или

¹⁰⁴ Singhal K., Azizi S., Tu T., Mahdavi S. S., Wei J., Chung H. W., Natarajan V. (2023). Large language models encode clinical knowledge. *Nature*, 620(7972), pp. 172-180.

¹⁰⁵ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng> (дата обращения: 28.11.2024)

используемые для отправки или установления приоритета при отправке экстренных служб первого реагирования, включая медицинскую помощь»¹⁰⁶.

Закон об искусственном интеллекте ЕС вводит такие положения, как раскрытие контента, сгенерированного искусственным интеллектом, и особые требования для систем с высоким уровнем риска. Статья 13 Закона определяет требования прозрачности для поставщиков систем искусственного интеллекта, обязывая их предоставлять достаточную информацию для руководства по использованию системы и интерпретации ее результатов¹⁰⁷. Закон об искусственном интеллекте ЕС фокусируется на минимизации, а не на полном устранении рисков, связанных с решениями с использованием искусственного интеллекта, посредством предварительных требований и оценок соответствия. Эти требования в основном применяются к разработчикам на этапах проектирования и разработки.

По сравнению с Европейским пространством данных в здравоохранении и Общим регламентом ЕС о защите данных Закон об искусственном интеллекте не предоставляет правовых оснований для первичного или вторичного использования персональных данных, особенно относящихся к специальным категориям, таким как данные о здоровье.

Важно отметить, что рассматриваемый Закон об искусственном интеллекте ЕС не посвящен индивидуальным правам лиц, пострадавших от его применения. Например, в Закон не включено право пациентов давать согласие на использование или отказ от использования медицинским работником системы искусственного интеллекта для постановки диагноза. Вместо этого он устанавливает требования к поставщикам и разработчикам. Ряд ученых утверждают, что Закон требует перечисления потенциальных воздействий на права и не содержит четкого

¹⁰⁶ Там же.

¹⁰⁷ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng> (дата обращения: 28.11.2024)

обязательства по оценке их приемлемости или возможности предотвращения¹⁰⁸. Кроме того, как утверждает Алессандро Мантелеро, отсутствие четкой обязательной оценки основных прав для частных поставщиков медицинских услуг может привести к неравенству в защите прав пациентов между поставщиками, а также между государствами-членами¹⁰⁹.

Тем не менее стоит подчеркнуть, что Закон об искусственном интеллекте ЕС все же содержит некоторые правомочия, направленные на защиту граждан. Так, в ст. 85 данного Закона предусмотрено у любого физического или юридического лица «право на подачу жалобы в соответствующий надзорный орган, имеющее основания считать, что имело место нарушение положений данного Закона»¹¹⁰.

Также ст. 86 вводит право на разъяснение индивидуального принятия решений со стороны должностного лица. В принципе, это право распространяется на отношения между медицинским работником и пациентом. Однако эта норма распространяется только на системы искусственного интеллекта с высоким уровнем риска и действует только в том случае, если решение оказывает существенное негативное влияние на здоровье, безопасность или основные права пользователя. На практике это означает, что в контексте здравоохранения данное право существует только в отношении решений искусственного интеллекта, касающихся страхования жизни и здоровья, вызова скорой помощи или направления служб экстренного реагирования, а также сортировки неотложной медицинской помощи.

¹⁰⁸ Day, J., Iwańska, K., Simon, E., & Willamo, K. (2024). Packed with loopholes: Why the AI Act fails to protect civic space and the rule of law. URL: https://dq4n3btxmr8c9.cloudfront.net/files/hj0z6a/AI_Act_RoL_Analysis.pdf (дата обращения: 28.11.2024)

¹⁰⁹ Mantelero, A. (2024). The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template. *Computer Law & Security Review*, 54, pp. 1-18.

¹¹⁰ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng> (дата обращения: 28.11.2024)

Следовательно, Закон об искусственном интеллекте ЕС в силу широкой направленности содержит только положения о требованиях к системам искусственного интеллекта различного риска, используемого в здравоохранении.

Таким образом, на основе проведенного в этой части параграфа анализа рамочного правового регулирования применения информационных технологий в сфере здравоохранения можно сделать следующие выводы.

1. Закон о переносимости и подотчетности медицинского страхования США устанавливает отраслевой подход к регулированию, ориентированный на конкретные организации здравоохранения и их деловых партнеров.

Общий регламент ЕС о защите данных представляет собой всеобъемлющий межотраслевой подход, устанавливающий высокие стандарты защиты персональных данных.

Закон КНР о защите персональной информации сочетает элементы как отраслевого, так и межотраслевого регулирования с акцентом на государственный контроль.

Наиболее комплексную защиту прав граждан обеспечивает Общий регламент ЕС о защите данных, который устанавливает широкий спектр прав субъектов данных, вводит специальные правила для автоматизированного принятия решений, предусматривает максимальные штрафные санкции за нарушения. Европейская модель, обеспечивая наиболее комплексную защиту прав, демонстрирует высокие барьеры для входа на рынок и сложность для малого инновационного бизнеса.

В этой связи потребность учета зарубежных вариантов рамочного подхода к регулированию ставит перед Россией дилемму: воспроизвести европейский уровень гарантий, рискуя замедлить технологическое развитие, или взять модель, подобную американской, дав свободу рыночному и экономическому развитию, или же использовать китайскую модель, основанную на централизованном государственном контроле с многими ограничениями, или же найти некую

гибридную, компромиссную модель с усилением конкретных прав пациентов в условиях применения информационных технологий в здравоохранении.

2. Интересным представляются положения Закона об искусственном интеллекте ЕС, законодательно закрепившие риск-ориентированный подход в отношении изделий с искусственным интеллектом в зависимости от их области и характера применения. Что примечательно: Закон об искусственном интеллекте ЕС классифицирует медицинские устройства с искусственным интеллектом на различные классы и уровни риска. Также следует учесть тот факт, что данный Закон не содержит формулировки, связанные с потенциальным воздействием искусственного интеллекта на права человека, не включает обязательств по оценке их приемлемости или возможности предотвращения воздействия. Однако в поддержку данного акта стоит сказать, что Общий регламент ЕС о защите данных в большей степени направлен на соблюдение и защиту прав человека в условиях цифровизации, чем Закон об искусственном интеллекте. Как показывает опыт ЕС, такой подход не блокирует внедрение искусственного интеллекта, создавая для бизнеса и врачей предсказуемое поведение и формируя основания для доверия со стороны пациентов. Таким образом, предлагаемые меры направлены на создание устойчивых правовых рамок для развития искусственного интеллекта. Более подробно данный вопрос будет изложен во второй главе.

3.2. Фрагментированное правовое регулирование вопросов здравоохранения в части применения информационных технологий

Фрагментированное правовое регулирование характеризуется множеством нормативных правовых актов на региональном и федеральном уровнях, которые часто сильно отличаются друг от друга и содержат разные требования в отношении применения различных видов информационных технологий в здравоохранении.

Типичными примерами фрагментированных актов являются законы штатов США, регулирующие телемедицинские технологии и обеспечивающие защиту прав как поставщиков телемедицинских услуг, так и пациентов. Эти правила

варьируются в зависимости от штата, хотя некоторые общие принципы применяются во всех юрисдикциях. Например, все штаты требуют от врачей соблюдения установленных профессиональных стандартов оказания медицинской помощи при взаимодействии с пациентом посредством телемедицинских технологий, таких как получение информированного согласия от пациента перед оказанием медицинской помощи. Кроме того, при оказании медицинской помощи в виртуальном режиме врачи должны соблюдать все применимые требования штата по лицензированию, например, получить действующую лицензию от соответствующего подразделения штата по оказанию медицинской помощи через телемедицинские технологии. При этом в нормативных правовых актах используется термин «телемедицина», а не «телемедицинские технологии», как в законодательстве России. Определение вышеуказанного термина имеет как сходства, так и отличия в зависимости от законодательства штата, что отмечается и в доктрине. Так, М.Д. Прилуков справедливо указывает, что «юридическое содержание телемедицины позволяет более четко определить объем данного понятия, разграничить со смежными отношениями, определить круг субъектов, их права и обязанности»¹¹¹. В качестве примера можно привести Поправку к Закону 2018 года о расширении программы Medicaid в области телемедицины округа Колумбия, которая в определении понятия «телемедицина» уточняет, какие электронные способы взаимодействия не могут использоваться в телемедицине. Термин не включает услуги, предоставляемые с помощью только аудиотелефонов, электронных почтовых сообщений или факсимильных передач¹¹².

Помимо регионального регулирования есть федеральные законы, обеспечивающие общие единые стандарты оказания телемедицинских технологий в стране. Например, Закон о расширении телементального здравоохранения США (Telemental Health Expansion Act) от 24 декабря 2020 г. отменяет географические

¹¹¹ Прилуков М. Д. Проблемы правового регулирования телемедицины. Российский и международный опыт // Вестник Нижегородского университета им. Н.И. Лобачевского. 2018. № 6. С. 136-141.

¹¹² D.C. Law 22-126. Telehealth Medicaid Expansion Amendment Act of 2018. URL: <https://code.dccouncil.gov/us/dc/council/laws/22-126> (дата обращения: 28.11.2024)

ограничения в правилах возмещения расходов программы Medicare на услуги по охране психического здоровья, предоставляемые посредством телемедицинских технологий, а также признает дом пациента допустимым местом оказания телемедицинских услуг, что дает право на их получение в данном месте¹¹³.

Множественность нормативных актов на уровне штатов и федерации порождает правовую неопределенность, что затрудняет их восприятие и применение, поскольку у каждого штата могут быть свои требования. В результате, как отмечают исследователи, в сфере телемедицины наиболее ярко проявляется конфликт, связанный с ограничением медицинской деятельности юрисдикциями штатов¹¹⁴. Правовая неопределенность также создает затруднения в правоприменительной практике и выступает сдерживающим фактором для обмена медицинской информацией как внутри штата, так и между штатами, а в исследовании, проведенном Национальной ассоциацией губернаторов в 2016 году, зафиксирована нерешенность данной проблемы, так как не было достигнуто достаточного прогресса для создания общего понимания или единых законов¹¹⁵.

Фрагментированность правового поля проявляется в области сбора медицинских данных с использованием технологий Интернета вещей. В частности, остро стоит проблема доступа пациентов к данным, собираемым мобильными приложениями: пациенты не могут напрямую получить доступ к медицинским данным через любые существующие мобильные приложения для смартфонов или иных мобильных переносимых устройств, собирающих медицинские данные с целью проведения дистанционного мониторинга здоровья пациента¹¹⁶. Многие

¹¹³ Telemental Health Expansion Act of 2020, H.R.5201, 116th Cong. (2020). URL: <https://www.congress.gov/bill/116th-congress/house-bill/5201/text> (дата обращения: 28.11.2024)

¹¹⁴ Богдановская И.Ю. Правовое регулирование телемедицины: опыт США // Материалы конференции «Информатизация здравоохранения и социальной сферы в регионах России: проблемы координации и информационного обмена». М., 2007. № 3. С. 64–68.

¹¹⁵ Mello, M. M., ADLER-MILSTEIN, J. U. L. I. A., Ding, K. L., & Savage, L. (2018). Legal barriers to the growth of health information exchange—boulders or pebbles? *The Milbank Quarterly*, 96(1), pp. 110-143.

¹¹⁶ Rosenbaum, S., & Goldstein, M. M. (2015). Regulation of information technology in behavioral health. *Public Health Reports*, pp.130(4).

приложения, устройства позволяют передавать данные врачам с подтверждением статуса передачи, но фактически данные не доступны для просмотра пациентам.

Данная проблема обусловлена ограничительной трактовкой Закона о переносимости и подотчетности медицинского страхования, который распространяется на подпадающих под действие закона организаций, таких как компании медицинского страхования по программам Medicare, Medicaid; медицинские клиринговые центры (общественные информационные системы здравоохранения) и поставщики медицинских услуг (врачи, клиники, больницы), которые считаются традиционными сборщиками медицинских данных. Однако в силу развития технологий Интернета вещей возник правовой пробел в отношении технологических компаний (например, Amazon, Apple, Facebook, Google и т. д.), выпускающих на рынок мобильные приложения и мобильные переносимые устройства, способные проводить удаленный мониторинг здоровья пациента и собирать медицинские данные¹¹⁷.

В то же время на федеральном уровне был принят Закон о лечении в XXI веке (21st Century Cures Act) от 13 декабря 2016 года, который направлен на получение доступа пациентов к своей электронной медицинской информации, чтобы принимать обоснованные решения о своем лечении. Закон обязывает медицинские организации предоставлять пациентам электронную медицинскую информацию, такую как история болезни и результаты медицинских анализов, сразу же после того, как информация будет окончательно обработана¹¹⁸. Получение доступа пациентами к своей электронной медицинской информации осуществляется только в рамках тех организаций, на которых распространяются требования Закона о переносимости и подотчетности медицинского страхования.

Потребность пациентов в доступе к собственным данным связана со стремлением к активному участию в управлении своим здоровьем, в некоторых

¹¹⁷ Roger Kuan, David Wallace. Digital Health Laws and Regulations Introduction 2024. URL: <https://iclg.com/practice-areas/digital-health-laws-and-regulations/01-introduction> (дата обращения: 15.09.2024)

¹¹⁸ 21st Century Cures Act. URL: <https://www.congress.gov/bill/114th-congress/house-bill/34> (дата обращения: 28.11.2024)

случаях с такой степенью срочности или внимания, которая в противном случае была бы нецелесообразной. Следовательно, учитывая автономию личности пациента, следует предоставить пациентам более широкий доступ к данным их устройств, в которых содержатся медицинские данные. Право пациента на активное участие в процессе поддержания здоровья, направленное на его охрану и получение качественной медицинской помощи является достаточным основанием для предоставления такого доступа.

Однако можно предположить с противоположной точки зрения, что производители, утверждая о сложности данных, намеренно ограничивают доступ, поскольку пациенты не имеют необходимой подготовки для правильной интерпретации медицинских данных, полученных с помощью переносимого медицинского устройства. Производители полагают, что данные, получаемые с помощью таких устройств, объемны, часто носят технический характер и имеют нюансы, превосходящие другие формы медицинских данных, например, труднопонимаемые лабораторные анализы. Поэтому ограничение доступа пациентов может рассматриваться через призму патерналистского подхода в отношении пациента, в рамках которого происходит ограждение пациентов от ненужного беспокойства, тревоги или замешательства от полученной информации о своем здоровье.

По нашему мнению, ограничивая прямой доступ, компании снимают с себя обязательства по разъяснению данных и потенциальные претензии, связанные с их самостоятельной интерпретацией пациентами. Несмотря на то, что такие данные могут быть действительно сложными для понимания или требовать соответствующих медицинских знаний для интерпретации, одним из преимуществ просмотра пациентами собственных лабораторных данных и получения доступа к ним является то, что это обеспечивает еще один уровень гарантии права пациента на охрану здоровья. Также при наличии постоянного доступа к данным пациента не будут пропущены важные результаты, связанные с его здоровьем в результате контроля со стороны пациента.

Аналогичная проблема присутствует в законодательстве Российской Федерации, о чем подробно будет рассказано во второй главе настоящего исследования.

Проблема на уровне США решается положениями принятого в 2018 году Закона Калифорнии о защите персональных данных потребителей (California Consumer Privacy Act), который предоставляет жителям Калифорнии несколько прав в отношении частной жизни, поскольку положения данного Закона не распространяются на Закон о переносимости и подотчетности медицинского страхования, а он, в свою очередь, не применяется в части получения доступа к медицинским данным, собираемым именно через мобильные приложения для смартфонов или иные мобильные переносимые устройства. Иные федеральные законы США в указанной части о конфиденциальности данных, которые бы распространялись на все виды медицинской информации, отсутствуют.

Так, согласно пункту 1 ст. 1798.100 Закона Калифорнии о защите персональных данных потребителей потребитель имеет право потребовать, чтобы организация, собирающая личную информацию потребителя, раскрыла потребителю категории и конкретные части личной информации, которую она собрала¹¹⁹.

Слово «собирает» в соответствии с пунктом 5 ст. 1798.140 указанного Закона Калифорнии означает покупку, аренду, сбор, приобретение, получение или доступ к любой личной информации, относящейся к потребителю, любым способом. Это включает в себя получение информации от потребителя: активным или пассивным способом, или наблюдение за его поведением¹²⁰. Таким образом, действие Закона Калифорнии распространяется и на необработанные медицинские данные, собранные мобильными приложениями для смартфонов или иных мобильных переносимых устройств, поскольку производители получают информацию от

119

ССРА

Text.

URL:

https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 (дата обращения: 15.09.2024)

¹²⁰ Там же.

потребителя пассивно через устройство. Более того, необработанные данные также считаются личной информацией согласно Закону Калифорнии о защите персональных данных потребителей, если необработанные данные, например, объединены с идентификаторами, такими как имя пациента (п. 15 ст. 1798.140 Закона Калифорнии о защите персональных данных потребителей).

Закон Калифорнии о защите персональных данных потребителей гласит в пункте 4 ст. 1798.100, что организация, получившая от потребителя поддающийся проверке запрос на доступ к личной информации, должна незамедлительно принять меры для раскрытия и бесплатной доставки потребителю личной информации, требуемой в соответствии с настоящим разделом. Информация может быть доставлена по почте или в электронном виде, и, если информация предоставляется в электронном виде, она должна быть в портативном и, насколько это технически возможно, легко используемом формате, позволяющем потребителю беспрепятственно передать эту информацию другому субъекту¹²¹. Соответственно, пациенты могут получить доступ к своей собираемой мобильными приложениями для смартфонов или иными мобильными переносимыми устройствами медицинской информации на основе вышеуказанных положений Закона Калифорнии о защите персональных данных потребителей, что является важным шагом в реализации права на тайну частной жизни и охрану здоровья пациента.

Похожие законы были приняты и в других штатах. Например, в штате Вашингтон был в 2023 г. принят Закон «Мое здоровье - мои данные» (Washington my health my data Act), имеющий широкую сферу действия и применения и направленный на защиту медицинских данных потребителей, выходящую за рамки федерального Закона о переносимости и подотчетности медицинского страхования. Закон регулирует сбор, обмен и продажу медицинских данных

¹²¹ Там же.

потребителей любой организацией, которая ведет бизнес, контролирует или обрабатывает медицинские данные потребителей в Вашингтоне¹²².

Также в штате Нью-Йорк Закон о конфиденциальности медицинской информации от 08 января 2025 г. (New York Health Information Privacy Act) направлен на более строгое регулирование данных о здоровье потребителей с учетом растущей монетизации потребительских данных, распространенности технологий онлайн-слежения и опасений, возникших в связи с решением по делу «Доббс против Джексонской организации по охране здоровья женщин» (*Dobbs v. Jackson Women's Health Organization*), которое показало, что информация, хранящаяся или полученная в цифровом виде, может быть использована для преследования лиц, желающих сделать аборт¹²³. В частности, широкое применение Закона Нью-Йорка о конфиденциальности медицинской информации к различным организациям и огромным объемам данных, а также его ограничения на сбор, использование, раскрытие и продажу данных о здоровье потребителей направлены на устранение и смягчение этих опасений¹²⁴. Кроме того, как и в других законах штатов о конфиденциальности данных о здоровье потребителей, обоснование для принятия Закона Нью-Йорка о конфиденциальности медицинской информации заключается в ужесточении требований в отношении организаций, которые собирают данные о здоровье потребителей через технологии Интернета вещей и которые не регулируются Законом о переносимости и подотчетности медицинского страхования США.

Калифорнийская и Вашингтонская модели регулирования носят универсальный характер и предоставляют доступ к персональным данным широкого спектра, что потенциально затрагивает и медицинские данные с технологиями Интернета вещей. Нью-Йоркская модель специально нацелена на

¹²² Washington my health my data Act. URL: <https://app.leg.wa.gov/RCW/default.aspx?cite=19.373&full=true> (дата обращения: 28.11.2024)

¹²³ Dobbs v. Jackson Women's Health Organization. URL: <https://www.oyez.org/cases/2021/19-1392> (дата обращения: 02.05.2025)

¹²⁴ Senate Bill S929. New York Health Information Privacy Act. URL: <https://www.nysenate.gov/legislation/bills/2025/S929> (дата обращения: 02.05.2025)

медицинскую информацию, вводя более строгие запреты на ее монетизацию. Это создает новый вызов для компаний, работающих в нескольких штатах, вынуждая их соблюдать различные регуляторные стандарты, что является прямым следствием фрагментированности.

В связи с вышеуказанным можно подчеркнуть, что нечеткие правила дают компаниям больше полномочий для сбора и передачи (продажи) частных данных пользователей без контроля.

В продолжение темы мобильных приложений для смартфонов или иных мобильных переносимых устройств, которые относятся к технологиям Интернета вещей, следует упомянуть Закон США об улучшении кибербезопасности технологий Интернета вещей от 12 апреля 2020 года (IoT Cybersecurity Improvement Act of 2020). Этот Закон требует от Национального института стандартов и технологий и Управления по управлению и бюджету США предпринять определенные шаги для повышения кибербезопасности устройств из числа технологий Интернета вещей. В частности, Закон требует разработать и опубликовать стандарты и рекомендации для федерального правительства по надлежащему использованию и управлению федеральными агентствами устройствами из числа технологий Интернета вещей, принадлежащими агентствам и подключенными к информационным системам, включая минимальные требования к информационной безопасности для управления рисками кибербезопасности, связанными с такими устройствами¹²⁵. Анализ позволяет утверждать, что этот Закон, хотя и касается в основном государственных закупок устройств из числа технологий Интернета вещей и не содержит порядок обеспечения защиты конфиденциальных данных при применении таких устройств, создает предпосылки для содействия широкой безопасности технологий Интернета вещей.

¹²⁵ IoT Cybersecurity Improvement Act of 2020. URL: <https://www.congress.gov/bill/116th-congress/house-bill/1668> (дата обращения: 28.11.2024)

Во исполнение упомянутого Закона США был принят исполнительный Указ о повышении уровня кибербезопасности страны в 2021 г. Указ предписывает установить минимальные стандарты безопасности для устройств из числа технологий Интернета вещей, эксплуатируемых федеральным правительством, обеспечивая защиту этих устройств от киберугроз. Часть приказа включает разработку программы маркировки устройств из числа технологий Интернета вещей, чтобы информировать потребителей о функциях безопасности этих продуктов, подобно маркировке энергоэффективности на бытовых приборах. Приказ также требует от агентств повысить уровень кибербезопасности, включая безопасность устройств из числа технологий Интернета вещей в цепочках поставок программного обеспечения, сделав ее приоритетной для федеральных закупок и операций. В целом этот Указ представляет собой согласованные усилия по защите инфраструктуры технологий Интернета вещей в рамках более широкой инициативы по повышению уровня кибербезопасности страны¹²⁶.

До принятия федерального закона ранее на уровне штата Калифорния в сентябре 2018 года был принят Закон о безопасности подключенных устройств (SB-327 The Security of Connected Devices). Закон направлен на обеспечение пользователям устройств из числа технологий Интернета вещей более надежной защиты, он требует от производителей прилагать усилия для активного продвижения безопасности в этих устройствах: производители должны обеспечить «разумные меры кибербезопасности», соответствующие характеру устройства и собираемой им информации. Они также должны быть способны защитить устройство от любых несанкционированных попыток получить доступ или изменить информацию, содержащуюся в устройстве¹²⁷.

¹²⁶ Executive Order on Improving the Nation's Cybersecurity. URL: <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/> (дата обращения: 28.11.2024)

¹²⁷ Senate Bill No. 327. The Security of Connected Devices URL: https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327 (дата обращения: 28.11.2024)

В Российской Федерации отсутствует законодательство в сфере кибербезопасности технологий Интернета вещей, поэтому целесообразно будет обратиться к данному опыту и определить меры кибербезопасности, в том числе и процедуру наложения санкций в отношении производителей, которые выпустили технологии Интернета вещей, признанные не соответствующими мерам кибербезопасности, о чем подробно будет рассказано во второй главе настоящего исследования.

В части регулирования применения искусственного интеллекта в сфере здравоохранения на федеральном уровне Конгрессом США было принято не так много нормативных правовых актов.

Значимым для сферы здравоохранения является Правило Федеральной торговой комиссии об уведомлении о нарушениях в сфере здравоохранения (FTC's Health Breach Notification Rule), возлагающее на ряд компаний обязанность предоставлять потребителям уведомления об использовании искусственного интеллекта в сфере здравоохранения после утечки информации о личных медицинских данных. Обязанность включает также предоставлять уведомление о данных, используемых для обучения, верификации и эксплуатации соответствующих систем (часть 318 Раздела 16 Свода федеральных нормативных актов США (Code of Federal Regulations)).

По состоянию на 2026 год на федеральном уровне в США в разработке все ещё находятся два законопроекта, направленные на внедрение искусственного интеллекта в сферу здравоохранения.

Так, законопроект о технологиях здравоохранения 2025 года (Healthy Technology Act of 2025) был представлен 7 января 2025 года, чтобы установить, что технологии искусственного интеллекта могут иметь возможность выписывать лекарства. Согласно этому закону, технологии искусственного интеллекта допускаются к назначению лекарств, если искусственный интеллект одобрен, разрешен или авторизован Управлением по санитарному надзору за качеством пищевых продуктов и медикаментов (FDA) и, если штат, в котором применяется

искусственный интеллект, разрешает его использование для назначения лекарств¹²⁸.

Законопроект о готовности к пандемиям и другим опасностям и реагировании на них (Pandemic and All-Hazards Preparedness and Response Act) был представлен в июле 2023 года. В соответствии с законопроектом в течение 45 дней после принятия закона министр здравоохранения и социальных служб должен провести исследование совместно с Национальной академией наук, инженерии и медицины, чтобы оценить потенциальные риски для здравоохранения, связанные с использованием или неправильным использованием искусственного интеллекта, включая большие языковые модели. Такие риски включают химические, биологические, радиологические или ядерные угрозы. В течение двух лет после проведения исследования Национальные академии должны представить Комитету по здравоохранению, образованию, труду и пенсиям Сената и Комитету по энергетике и торговле Палаты представителей отчет о мерах, принятых для смягчения и мониторинга рисков для безопасности здоровья в результате неправильного использования искусственного интеллекта¹²⁹.

Кроме того, Управление по санитарному надзору за качеством пищевых продуктов и медикаментов опубликовало проект руководства по медицинским устройствам, работающим на основе искусственного интеллекта, который устанавливает стандарты и требования в отношении искусственного интеллекта в здравоохранении в целях управления рисками, мониторинга прозрачности и производительности, а также обеспечения безопасности при его использовании¹³⁰.

Параллельно с федеральными инициативами, активная нормотворческая деятельность ведется в отдельных штатах США. Так, на уровне штатов, по данным

¹²⁸ Healthy Technology Act of 2025. URL: <https://www.congress.gov/bill/119th-congress/house-bill/238> (дата обращения: 28.01.2026)

¹²⁹ S.2333 - Pandemic and All-Hazards Preparedness and Response Act. URL: <https://www.congress.gov/bill/118th-congress/senate-bill/2333/text> (дата обращения: 28.01.2026)

¹³⁰ Considerations for the Use of Artificial Intelligence To Support Regulatory Decision-Making for Drug and Biological Products. URL: <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/considerations-use-artificial-intelligence-support-regulatory-decision-making-drug-and-biological> (дата обращения: 28.01.2025)

Стэнфордского университета, в период с 2016 по 2022 год соответствующие законы приняли 14 штатов, лидером среди которых является Мэриленд с семью законами, касающимися искусственного интеллекта, за ним следует Калифорния с шестью, а также Массачусетс и Вашингтон с пятью¹³¹. Наиболее релевантными для настоящего исследования представляются закон штата Колорадо, а также два закона штата Калифорния и законопроект, внесенный на рассмотрение в 2024 году в штате Массачусетс, которые закрепляют применение искусственного интеллекта именно в сфере здравоохранения.

Закон штата Колорадо о защите прав потребителей при взаимодействии с системами искусственного интеллекта (Concerning consumer protections in interactions with artificial intelligence systems), принятый 17 мая 2024 г., устанавливает требования к поставщику медицинских услуг, который должен применять разумные меры предосторожности для защиты потребителей от любых известных или разумно предвидимых рисков алгоритмической дискриминации при использовании искусственного интеллекта¹³².

Закон штата Калифорния № 1120 «Медицинское страхование: обзор использования» (Senate Bill No. 1120 «Health care coverage: utilization review»), принятый в 2024 г., требует, чтобы специализированный медицинский страховщик, который использует искусственный интеллект, алгоритм или другое программное обеспечение в целях использования в своей деятельности или функций по их управлению, либо который заключает договор или иным образом работает через организацию, использующую эти инструменты, обеспечивал соблюдение определенных требований, включая то, чтобы искусственный интеллект, алгоритм

¹³¹ Artificial Intelligence Index Report 2023. CHAPTER 6: Policy and Governance. – 2023.
URL: https://aiindex.stanford.edu/wp-content/uploads/2023/04/HAI_AI-Index-Report-2023_CHAPTER_6-1.pdf (дата обращения: 28.11.2024)

¹³² Concerning consumer protections in interactions with artificial intelligence systems. – 2024.
URL: https://leg.colorado.gov/sites/default/files/2024a_205_signed.pdf (дата обращения: 28.11.2024)

или другое программное обеспечение применялись на основе определенной информации, а также справедливо и беспристрастно¹³³.

Требования к использованию генеративного искусственного интеллекта устанавливаются Законом штата Калифорния № 3030 «Медицинские услуги: искусственный интеллект» (Senate Bill No. 3030 «Health care services: artificial intelligence»), принятый в 2024 г. Согласно ему, медицинское учреждение, клиника, частный врач, использующие генеративный искусственный интеллект для создания письменных или устных сообщений для пациентов, относящихся к их клинической информации, обеспечивали следующие требования:

(1) заявление, указывающее пациенту, что сообщение было сгенерировано с помощью генеративного искусственного интеллекта;

(2) должны присутствовать четкие инструкции, описывающие, как пациент может связаться с медицинским работником, сотрудником или другим соответствующим лицом. Закон освобождает от этого требования сообщение, прочитанное и рассмотренное лицензированным или сертифицированным медицинским работником. Согласно Закону, нарушение этих положений врачом будет подпадать под юрисдикцию Медицинского совета Калифорнии или Остеопатического медицинского совета Калифорнии, в зависимости от ситуации¹³⁴.

Законопроект штата Массачусетс о регулировании использования искусственного интеллекта при оказании услуг в области психического здоровья человека (An Act regulating the use of artificial intelligence (AI) in providing mental health services) от 2024 г. направлен на обеспечение безопасности и благополучия людей, обращающихся за психиатрической помощью, а также на ответственное использование искусственного интеллекта. Законопроект требует, чтобы любой лицензированный специалист в области психического здоровья, желающий

¹³³ Senate Bill No. 1120 «Health care coverage: utilization review». URL: <https://legiscan.com/CA/text/SB1120/id/3023335> (дата обращения: 28.10.2025)

¹³⁴ AB-3030 Health care services: artificial intelligence. URL: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB3030 (дата обращения: 28.11.2025)

использовать искусственный интеллект для оказания услуг в данной области, должен получить разрешение от соответствующего лицензионного совета. Лица, получившие такую лицензию, должны сообщать своим пациентам об использовании искусственного интеллекта и предоставлять им информированное согласие, а также предоставлять им выбор получать лечение от человека, а не искусственного интеллекта. Кроме того, системы искусственного интеллекта, используемые при оказании психиатрических услуг, должны быть разработаны таким образом, чтобы обеспечить безопасность и благополучие пациента¹³⁵.

Таким образом, на основе анализа модели фрагментированного правового регулирования вопросов здравоохранения в части применения информационных технологий можно сделать следующие выводы.

1. Фрагментированное правовое регулирование вопросов здравоохранения, характерное в нашей классификации правовых моделей для федеративных государств, целесообразно исследовать на примере законодательства США. В части применения информационных технологий оно насчитывает множество нормативных правовых актов. Так, на федеральном уровне в США наблюдается активное принятие законов, направленных на защиту прав пациентов и улучшение доступа к медицинской информации, что свидетельствует о высоком уровне законодательной активности и адаптации к новым технологиям. Основная проблема, обнаруженная в результате анализа законодательства США, связана с тем, что мобильные приложения и устройства для мониторинга здоровья не подпадают под действие существующих федеральных законов, таких как Закон о переносимости и подотчетности медицинского страхования США. Поэтому невозможно получать доступ к своей собираемой мобильными приложениями для смартфонов или иными мобильными переносимыми устройствами медицинской информации.

¹³⁵ An Act regulating the use of artificial intelligence (AI) in providing mental health services. URL: <https://malegislature.gov/Bills/193/H1974> (дата обращения: 28.11.2024)

Эта проблема, которая актуальна и для России, относительно успешно решается на уровне законодательства штатов Калифорния и Нью-Йорк. Поэтому Закон Калифорнии о защите персональных данных потребителей и Закон Нью-Йорка о конфиденциальности медицинской информации представляются эффективными в плане развития правового регулирования применения информационных технологий в России, так что целесообразным представляется обратиться к опыту США в указанном направлении, в особенности в той части, где закреплена возможность для пациентов получать доступ к своей собираемой мобильными приложениями для смартфонов или иными мобильными переносимыми устройствами медицинской информации и защищать права пациентов путем установления ограничения на сбор, использование, раскрытие и продажу данных о здоровье потребителей различными организациями.

Несмотря на кажущийся законодательный хаос, в регулировании применения информационных технологий в здравоохранении США формируется новая, децентрализованная парадигма, где «фрагментированность» является не патологией, а адаптивным механизмом. Роль федерального центра смещается от унификации к созданию «рамочных» стандартов (кибербезопасность), в то время как штаты становятся «инновационными полигонами» по защите прав пациентов в условиях применения различных информационных технологий. С точки зрения концепции пациентоориентированности, в соответствии с которой эффективность регулирования оценивается по тому, насколько оно расширяет возможности и права пациента, Закон Калифорнии о защите персональных данных потребителей и Закон Нью-Йорка о конфиденциальности медицинской информации усиливают автономию пациента.

2. Проблема отсутствия гарантий полной кибербезопасности в случае применения технологий Интернета вещей также актуальна для отечественного законодательства. Закон США об улучшении кибербезопасности технологий Интернета вещей от 2020 года представляет научный и практический интерес как первая попытка системного федерального регулирования в данной области,

который направлен на разработку стандартов и рекомендаций по надлежащему использованию и управлению устройствами, относящимися к данной технологий.

3. Представляется не вполне целесообразным использовать модель фрагментированного регулирования в отношении применения телемедицинских технологий для совершенствования отечественного законодательства в указанной области, поскольку большое количество нормативных правовых актов на уровне штатов и федерации США вызывает неопределенность в понимании того, как лучше всего урегулирован механизм применения телемедицинских технологий, поскольку у разных штатов США свои требования к оказанию телемедицинских услуг и применению данных технологий для оказания медицинской помощи пациентам. При этом оно приводит к созданию барьеров для доступа пациента к услугам, так как врач должен иметь действующую лицензию на медицинскую деятельность в случае использования телемедицинских технологий, а в США эта лицензия привязана к конкретному штату. Таким образом, опыт США в сфере телемедицины обладает ограниченной применимостью для прямого заимствования в российскую правовую систему в силу фундаментальных различий в структуре законодательства и вытекающей из этого сложности и противоречивости регулирования на уровне штатов.

4. Если ставить задачу точно урегулировать применение искусственного интеллекта в сфере здравоохранения России, то следует рассмотреть возможность заимствования законопроектного опыта ряда штатов США, которые предусматривают раскрытие информации об использовании искусственного интеллекта, обязанность информировать пациентов о том, как используется искусственный интеллект, получение разрешения на использование искусственного интеллекта медицинскими специалистами.

3.3. Специализированное правовое регулирование применения информационных технологий в сфере здравоохранения

Специализированное правовое регулирование характеризуется наличием отдельных нормативных актов, ориентированных непосредственно на внедрение информационных технологий в сферу здравоохранения и установление порядка их применения.

В то время как в США регулирование телемедицины во многом складывается из правоприменительной практики и актов штатов, в европейских странах вопросы, касающиеся телемедицины, регулируются отдельными нормативными правовыми актами национального права. Так, во Франции согласно ст. L6316-1 Кодекса общественного здравоохранения Франции, «телемедицина» определяется как «форма удаленной медицинской практики с использованием информационных и коммуникационных технологий», которая «приводит медицинского работника в контакт с одним или несколькими медицинскими работниками, между собой или с пациентом и, при необходимости, с другими специалистами, оказывающими помощь пациенту»¹³⁶.

В Германии в 1997 г. была утверждена концепция развития национальной телемедицинской сети и был принят Профессиональный кодекс для врачей, практикующих в Германии, что, в свою очередь, привело к значительному росту количества видеоконсультаций, онлайн-рецептов и других видов дистанционного лечения пациентов¹³⁷.

Профессиональный кодекс для врачей, практикующих в Германии, определяет требования к телемедицинскому лечению и разрешает телемедицинские услуги в целом как вспомогательное лечение, при условии, что лечение пациента в основном происходит при личном контакте¹³⁸. Врачам также разрешено выдавать справку о болезни во время видеоконсультации.

¹³⁶ Code de la santé publique. URL: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006072665/LEGISCTA000038841870/#LEGISCTA000038841870 (дата обращения: 28.11.2024)

¹³⁷ *Владимирский А.В.* Телемедицина: Curatio Sine Temporaet Distantia. М.: Aegitas, 2016, С. 662.

¹³⁸ Образец профессионального кодекса для врачей, работающих в Германии – (МВО-Ä 1997)-, сформулированный на основании решения 114-го съезда врачей в г. Киль 2011. URL: <https://nacmedpalata.ru/?action=show&id=8962> (дата обращения: 28.11.2024)

Одновременно с этим в определенной степени были сняты ограничения на рекламу телемедицины, что, по всей видимости, было направлено на стимулирование рыночной конкуренции и повышение информированности пациентов о новых возможностях получения медицинской помощи. Несмотря на это телемедицина по-прежнему подвержена многочисленным нормативным ограничениям.

Консультация или лечение исключительно средствами телемедицины (без личного контакта) допустимы при соблюдении следующих условий:

(i) эксклюзивное телемедицинское лечение оправдано с медицинской точки зрения, т. е. для получения прямой и полной картины состояния пациента и его заболевания не требуется дополнительных медицинских обследований¹³⁹;

(ii) соблюдается необходимая врачебная обязанность проявлять заботу (*ärztliche Sorgfaltspflicht*)¹⁴⁰, в частности, при проведении диагностики, консультации, лечения и документирования;

(iii) пациент четко информирован о специфике и ограничениях лечения исключительно через средства связи¹⁴¹.

Приведенные условия существенно сужают сферу применения исключительно телемедицинского обслуживания, что подтверждает тезис о его строгом регламентировании в Германии. Несмотря на детальную регламентацию, германская модель оставляет значительное пространство для усмотрения врача, что, с одной стороны, гибко, а с другой — может приводить к правовой неопределенности и различиям в практике между федеральными землями.

В КНР с 2018 года органы государственной власти реализуют целенаправленную политику, направленную на регулирование развития

¹³⁹ *Jana Grieb, Dr. Deniz Tschammler, Dr. Claus Färber, Steffen Woitz. Digital Health Laws and Regulations Germany 2024. URL: <https://iclg.com/practice-areas/digital-health-laws-and-regulations/germany> (дата обращения: 28.11.2024)*

¹⁴⁰ Под обязанностью проявлять заботу понимается обязанность врача осуществлять медицинское лечение своих пациентов с целью достижения успешного излечения на основе новейших медицинских научных знаний и сопутствующего необходимого ухода.

¹⁴¹ TELEMEDICINE: A GLOBAL APPROACH TO TRENDS AND PRACTICES. URL: <https://www.ibanet.org/document?id=Healthcare-Telemedicine-Survey-Germany> (дата обращения: 28.11.2024)

телемедицинских технологий. Так, Управление киберпространства КНР, Министерство промышленности и информационных технологий КНР и другие ведомства обязаны издавать руководящие документы о мерах управления для регулирования интернет-диагностики пациентов и их лечения, уточнять стандарты надзора, обеспечивать качество и безопасность медицинских и оздоровительных услуг¹⁴².

Также применение искусственного интеллекта в здравоохранении является важным стратегическим направлением для китайского правительства. Например, в планах «Здоровый Китай 2030» говорится, что Китай будет осуществлять поддержку исследований и разработок искусственного интеллекта в области здравоохранения, медицинских роботов, крупного медицинского оборудования, вспомогательных устройств для здоровья и реабилитации, умных носимых устройств и соответствующих микросенсорных устройств¹⁴³.

Учитывая опыт ЕС, в 2023 г. китайская компартия решила разработать «Модельный закон об искусственном интеллекте, версия 1.0 (проект экспертного предложения)», а в 2024 г. - «Модельный закон об искусственном интеллекте, версия 2.0», которые «содержат элементы риск-ориентированного подхода, предполагающего дифференциацию регулирования в зависимости от уровня рисков, т.е. они устанавливают более строгий надзор за «базовыми моделями» искусственного интеллекта, обученными на больших объемах данных и используемыми в различных продуктах на основе искусственного интеллекта»¹⁴⁴. Как и в европейском законе, китайские проекты Закона об искусственном интеллекте будут использовать риск-ориентированный подход в отношении изделий с искусственным интеллектом в зависимости от их области и характера применения. При этом, как отмечает А.Г. Шейкин, «проектируемые нормы

¹⁴² Мнения о содействии развитию «Интернет + медицина-здоровье». URL: https://www.gov.cn/zhengce/content/2018-04/28/content_5286645.htm (дата обращения: 28.11.2024)

¹⁴³ Центральный комитет Коммунистической партии Китая и Госсовет опубликовали План планирования «Здоровый Китай 2030». URL: https://www.gov.cn/zhengce/2016-10/25/content_5124174.htm (дата обращения: 28.11.2024)

¹⁴⁴ Филипова И. А. Правовое регулирование искусственного интеллекта: опыт Китая //Journal of Digital Technologies and Law. 2024. Т. 2. №. 1. С. 46-73.

относительно того, какие органы власти будут выпускать эти списки либо сформулированы неопределенно (Проект-2023), либо передают эту функцию отраслевым департаментам соответствующих ведомств (Проект-2024)»¹⁴⁵.

В части правового регулирования регистрации технологий Интернета вещей в здравоохранении стоит упомянуть, что в США единственные правила по регистрации устройств из числа технологий Интернета вещей выпускает Управление по санитарному надзору за качеством пищевых продуктов и медикаментов США (FDA), которое разработало план программы предварительной сертификации программного обеспечения для цифрового здравоохранения, учитывающая уникальные и быстро меняющиеся аспекты приложений mHealth и направленная на оптимизацию нормативного надзора за программными медицинскими устройствами¹⁴⁶. Вместо регулирования и оценки устройств эта пилотная программа будет рассматривать историю производителя устройства по производству безопасных, эффективных устройств и его предыдущие обязательства по оценке и мониторингу производительности устройства после того, как оно попадет к потребителю. Для получения сертификата необходимо соблюсти пять принципов: безопасность пациентов, качество продукции, клиническая ответственность, ответственность за кибербезопасность и проактивная культура. После сертификации компания может производить новые «предварительно сертифицированные» технологии Интернета вещей без необходимости проходить весь процесс сертификации снова. Она может пройти «упрощенные проверки» или, в некоторых случаях, быть освобождена от всего процесса проверки, если продукт имеет низкий уровень риска. «Упрощенная проверка» будет впоследствии зависеть от ряда факторов, выходящих за рамки

¹⁴⁵ Шейкин А. Г. Правовое регулирование искусственного интеллекта в Китайской Народной Республике: состояние, перспективы, сравнительный анализ законопроектных предложений (часть 1) // Пролог: журнал о праве. 2025. №. 1 (45). С. 38-54.

¹⁴⁶ Food and Drug Administration (FDA). “Developing Software Precertification Program: A Working Model.” U.S. Food & Drug Administration. Retrieved. URL: <https://www.fda.gov/media/113802/download> (дата обращения: 28.02.2025)

статуса и уровня предварительной сертификации организации, одним из которых является стратификация рисков программного обеспечения.

FDA ранее разъясняло, что, когда программное приложение используется для анализа данных в медицинских целях, оно традиционно регулируется как принадлежность медицинского устройства или как программное обеспечение медицинского устройства. В 2014 году Международный форум регуляторов медицинских изделий создал глобально согласованную терминологию для таких программных приложений и определил термин «Программное обеспечение как медицинское изделие (SaMD)»¹⁴⁷. Как и в случае с традиционными медицинскими изделиями, некоторые функции программного обеспечения, являющиеся функциями устройства, могут представлять потенциальный риск для здоровья населения. Более того, некоторые функции программного обеспечения устройств могут представлять риски, зависящие от характеристик платформы, на которой выполняется функция программного обеспечения.

В 2022 году FDA выпустило официальное руководство, устанавливающее регуляторный подход к «мобильным медицинским приложениям»¹⁴⁸. В них приоритет отдается мониторингу и процессу утверждения мобильных приложений, которые напрямую управляют медицинскими устройствами или сами по себе функционируют как такие устройства. Мобильные приложения, которые носят образовательный характер или способствуют «здоровому образу жизни», считаются менее опасными. Они представляют меньший риск для безопасности и здоровья населения и поэтому требуют меньшего надзора или не требуют его вовсе. В руководстве описано, что устройства на базе технологий Интернета вещей подлежат регистрации и будут тщательно регулироваться, если они функционируют как медицинские устройства, т. е. соответствуют определению

¹⁴⁷ The International Medical Device Regulators Forum final document, “Software as a Medical Device (SaMD): Key Definitions. URL: <http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-131209-samd-key-definitions-140901.pdf> (дата обращения: 28.02.2025)

¹⁴⁸ Policy for Device Software Functions and Mobile Medical Applications Guidance for Industry and Food and Drug Administration Staff. URL: <https://www.fda.gov/media/80958/download> (дата обращения: 28.02.2025)

устройства и либо используются в качестве аксессуара к регулируемому медицинскому устройству, либо превращают мобильную платформу в регулируемое медицинское устройство, и могут представлять риск для безопасности пациента, если они не функционируют так, как задумано¹⁴⁹.

В европейском законодательстве в указанной области имеются два новых регламента ЕС, которые 25 мая 2017 года вступили в силу: Регламент о медицинских изделиях (2017/745-MDR) и Регламент о медицинских изделиях для диагностики *in vitro* (2017/746-IVDR).

В соответствии с пунктами 1 и 2 ст. 2 Регламента о медицинских изделиях технологии Интернета вещей (мобильные переносимые устройства, «умные» медицинские устройства, мобильные приложения и др.) подпадают под действие данного регламента, если они имеют целевое медицинское назначение или являются принадлежностью к медицинскому изделию. Новый Регламент о медицинских изделиях внес некоторые изменения в процесс классификации медицинских изделий. В частности, медицинским изделием, согласно пункту 1 ст. 2 Регламента о медицинских изделиях, является программное обеспечение, которое используется для людей с медицинской целью предсказания или прогноза заболевания. При этом в ст. 19 Регламента о медицинских изделиях также четко разъясняется, что программное обеспечение само по себе, если оно специально предназначено производителем для использования в одной или нескольких медицинских целях, указанных в определении медицинского изделия, квалифицируется как медицинское изделие, в то время как программное обеспечение общего назначения, даже если оно используется в медицинских учреждениях, или программное обеспечение, предназначенное для целей поддержания здорового образа жизни и благополучия, не является медицинским изделием. Квалификация программного обеспечения как устройства или

¹⁴⁹ FDASIA Health IT Report. Proposed Strategy and Recommendations for a Risk-Based Framework. URL: https://www.healthit.gov/sites/default/files/fdasia_healthitreport_final.pdf (дата обращения: 28.11.2024)

аксессуару не зависит от места расположения программного обеспечения или типа связи между программным обеспечением и устройством¹⁵⁰.

Медицинские изделия в соответствии с пунктом 1 ст. 51 Регламента о медицинских изделиях будут подразделяться на четыре категории, а именно классы I, IIa, IIb и III, в зависимости от предназначения медицинских изделий и присущих им рисков. Регламент о медицинских изделиях также вводит новые правила внедрения и классификации программного обеспечения в главах II и III Приложения VIII.

Среди европейских стран отдельно в 2020 г. Германия приняла Постановление по применению цифровых технологий в здравоохранении (Digitale-Gesundheitsanwendungen-Verordnung, DiGAV). Концепция данного Постановления распространяется на мобильные приложения, которые являются медицинскими устройствами, сертифицированными по стандарту CE в соответствии с Постановлением (ЕС) 2017/745 о медицинских устройствах («MDR»), класс риска I или IIa. Чтобы получить разрешение на возмещение расходов, производитель должен доказать, что медицинское приложение отвечает требованиям безопасности, функциональности и качества, а также соблюдает требования по защите данных. Кроме того, производитель должен доказать, что приложение оказывает положительное влияние на лечение пациентов¹⁵¹.

Во Франции выпустили «Руководство по надлежащей практике в отношении приложений для здравоохранения и интеллектуальных устройств (мобильное здравоохранение или mHealth)» для производителей, а также список надлежащей

¹⁵⁰ Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0745> (дата обращения: 28.11.2024)

¹⁵¹ Verordnung über das Verfahren und die Anforderungen zur Prüfung der Erstattungsfähigkeit digitaler Gesundheitsanwendungen in der gesetzlichen Krankenversicherung (Digitale Gesundheitsanwendungen-Verordnung - DiGAV). URL: <https://www.gesetze-im-internet.de/digav/BJNR076800020.html> (дата обращения: 28.11.2024)

практики для субъектов здравоохранения¹⁵². Эти рекомендации распространяются на медицинские приложения и смарт-устройства, которые не имеют заявленного медицинского назначения.

Великобритания разработала руководящий документ, позволяющий производителям приложений определять, подлежат ли их приложения регулированию как медицинские устройства, тем самым предоставляя производителям большую ясность в назначении своих устройств¹⁵³.

Регулирование медицинских изделий в Китае выросло из принципов и механизмов регулирования, применяемых к фармацевтической продукции с 1949 года. В соответствии с Положением о надзоре и управлении медицинскими изделиями (приказ № 739) и Правилами классификации медицинских изделий, некоторые носимые изделия считаются медицинскими изделиями, и на них распространяются соответствующие нормативные требования к медицинским изделиям¹⁵⁴.

Имеет смысл упомянуть, что в отечественном законодательстве на данный момент отсутствуют нормы о регистрации устройств на базе технологий Интернета вещей и критериях их разграничения от иных медицинских устройств. Более детально данный вопрос будет рассмотрен во второй главе настоящего исследования.

В части регулирования применения технологий анализа больших данных в здравоохранении, к которым относятся электронные медицинские карты, стоит выделить несколько специализированных актов, принятых за рубежом.

Несмотря на то, что в США имеются нормативные правовые акты фрагментированного уровня, на территории страны действует принятый в 2009 году как часть Закона о восстановлении и реинвестировании американской

¹⁵² Good practice guidelines on health apps and smart devices (mobile health or mhealth). URL: https://www.has-sante.fr/jcms/c_2681915/en/good-practice-guidelines-on-health-apps-and-smart-devices-mobile-health-or-mhealth (дата обращения: 28.02.2025)

¹⁵³ Guidance: Medical device stand-alone software including apps. URL: <https://www.fda.gov/media/113802/download> (дата обращения: 28.02.2025)

¹⁵⁴ Положение о надзоре и управлении медицинскими изделиями. URL: <https://www.nmpa.gov.cn/xxgk/fgwj/flxzhfg/20210319202057136.html> (дата обращения: 28.11.2024)

экономики от 2009 года (American Recovery and Reinvestment Act) Закон об информационных технологиях в здравоохранении для экономического и клинического здоровья (Health Information Technology for Economic and Clinical Health Act), предусматривавший внедрение электронных медицинских карт к 2014 году и устанавливавший несколько этапов внедрения таких карт. Принятие данного Закона было продиктовано не только задачами цифровизации здравоохранения, но и необходимостью стимулирования экономики в период рецессии, что объясняет масштаб финансовых вложений в виде поощрительных выплат для врачей и госпиталей. Поскольку этот Закон предполагает масштабное расширение обмена электронной защищенной медицинской информацией, он также расширяет сферу защиты конфиденциальности и безопасности, предусмотренную Законом США о переносимости и подотчетности медицинского страхования. Данный Закон повышает потенциальную юридическую ответственность за несоблюдение требований и предусматривает более жесткое правоприменение¹⁵⁵.

В Австрии систематическая реализация политики электронного здравоохранения была инициирована в 2012 г., когда был принят Закон об электронной медицинской карте (ELGA-Gesetz), в результате налажена работа австрийской национальной системы электронных медицинских карт (Elektronische Gesundheitsakte, ELGA), которая объединяет все медицинские учреждения: больницы, частные медицинские клиники, дома-интернаты для престарелых и инвалидов, аптеки¹⁵⁶. Особенностью данной системы является право пациента распоряжаться доступом к своим данным. Пациенты имеют возможность отслеживать, кто знакомился с информацией, содержащейся в их электронной медицинской карте, и решить вопрос о расширении или сокращении доступа, либо даже запретить доступ к определенной информации. Также платформа предусматривает создание медицинских документов в единообразной форме, что

¹⁵⁵ HITECH Act Summary. URL: <https://www.hipaasurvivalguide.com/hitech-act-summary.php> (дата обращения: 15.09.2024)

¹⁵⁶ Демкина А. Е. Эволюция цифровой медицины. Мировой и отечественный опыт // Вестник Московского университета. Серия 21. Управление (государство и общество). 2023. № 2. С. 3-26.

обеспечивает возможность обмена между разными учреждениями¹⁵⁷. В Австрии активное вовлечение пациентов, доказательство и подтверждение клинического результата, не уступающего обычному лечению, считаются решающими критериями для внедрения электронных медицинских карт.

В Швейцарии был принят первый Федеральный закон об электронной карте пациента от 19 июня 2015 г. (Gesetz über das elektronische Patientendossier), который направлен на регулирование правовых, организационных и технических условий для подключения первичных систем к электронному досье пациента. Аналогично, как и в Австрии, данный Закон регулирует право каждого пациента решать, кто может получить доступ к электронной карте, какие задачи стоят перед поставщиками медицинских услуг, и обеспечивает высочайший уровень безопасности¹⁵⁸. Как результат, были внедрены соответствующие платформы, где размещаются электронные карты пациентов, к которым они могут подключаться, а медицинские специалисты - получать доступ к карте, если пациенты разрешат им это.

В Германии был принят Закон о цифровых технологиях 25 марта 2024 г. (Digitalgesetz, DigiG). На основании данного Закона с 15 января 2025 года фонды обязаны предоставлять каждому застрахованному лицу электронную карту пациента, если после предварительного уведомления это застрахованное лицо в течение шести недель не заявит о своем несогласии с созданием такой карты¹⁵⁹.

В Финляндии в 2023 г. принят Закон об обработке данных клиентов в здравоохранении и социальном обеспечении (Act on the Electronic Processing of Client Data in Healthcare and Social Welfare, 703/2023), регулирующий использование единой платформы электронного здравоохранения Kanta.

¹⁵⁷ Коданева С.И. Цифровые технологии в здравоохранении: зарубежный опыт // Россия: тенденции и перспективы развития. 2020. № 15–1. С. 617–620.

¹⁵⁸ Gesetzgebung Elektronisches Patientendossier (EPDG). URL: <https://www.bag.admin.ch/bag/de/home/gesetze-und-bewilligungen/gesetzgebung/gesetzgebung-mensch-gesundheit/gesetzgebung-elektronisches-patientendossier.html> (дата обращения: 28.11.2024)

¹⁵⁹ Digital-Gesetz (DigiG). URL: <https://www.bundesgesundheitsministerium.de/service/gesetze-und-verordnungen/detail/digital-gesetz.html> (дата обращения: 28.11.2024)

Отличительной особенностью финской модели цифрового здравоохранения является возможность добровольного внесения данных самими гражданами. При этом у пациента есть возможность управлять своей информацией о здоровье, предоставлять ее поставщикам медицинских услуг, как в Германии и в Австрии¹⁶⁰.

В Китае системы управления электронными медицинскими картами должны соответствовать положениям Административного регламента по применению электронных медицинских карт, Положения об управлении медицинскими картами в медицинских учреждениях, Уведомления Национальной комиссии по здравоохранению о дальнейшем содействии информатизации медицинских учреждений с использованием электронных медицинских карт в качестве основы и других соответствующих нормативных правовых актов¹⁶¹.

Важно отметить, что в России по сравнению с вышеуказанными странами, нет законодательного регулирования вопроса права пациента широко распоряжаться доступом к своей электронной медицинской карте, в том числе ограничивать его. Более детально данный вопрос будет рассмотрен во второй главе настоящего исследования.

Таким образом, на основе анализа модели специализированного правового регулирования применения информационных технологий в сфере здравоохранения можно сделать следующие выводы.

1. Для совершенствования регулирования регистрации технологий Интернета вещей в России может быть целесообразно обратиться к правовой модели, предложенной во Франции и Великобритании, поскольку в этих странах установлены требования в отношении разграничения изделий на базе технологий Интернета вещей широкого доступа от тех же изделий, но уже относящихся к медицинским изделиям. Более подробно об этом будет сказано в следующей главе применительно к российской проблематике.

¹⁶⁰ Act on the Electronic Processing of Client Data in Healthcare and Social Welfare. URL: <https://www.kanta.fi/en/legislation> (дата обращения: 28.11.2024)

¹⁶¹ Cindy Hu, Jason Gong, Jiaxin Yang. Digital Health Laws and Regulations China 2024. URL: <https://iclg.com/practice-areas/digital-health-laws-and-regulations/china> (дата обращения: 28.11.2024)

2. Не представляется целесообразным использовать опыт США в части регулирования применения электронных медицинских карт. Стимулирование внедрения ЭМК в США было тесно связано с частной страховой моделью здравоохранения и реализовывалось через систему поощрительных выплат частным медицинским провайдерам, что существенно отличает его от модели с доминирующим государственным финансированием, как в России. При этом положения Закона США об информационных технологиях в здравоохранении для экономического и клинического здоровья действуют в связке с другими давно существующими нормативными актами, в первую очередь с Законом о восстановлении и реинвестировании американской экономики и Законом о переносимости и подотчетности медицинского страхования.

Интересным для российской правовой системы представляется соответствующее законодательство Австрии и Швейцарии, которое наделяет пациента правом распоряжаться доступом к своим данным и позволяют решить вопрос о расширении или сокращении доступа, либо даже запретить доступ к определенной информации, а также положения Закона Финляндии об обработке данных клиентов в здравоохранении и социальном обеспечении, регулирующий использование единой платформы электронного здравоохранения Kanta, где пациенты на добровольной основе могут вносить данные в свои электронные медицинские карты.

ГЛАВА 2. КОНСТИТУЦИОННО-ПРАВОВЫЕ ОСНОВЫ ПРИМЕНЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ЗДРАВООХРАНЕНИИ НА СОВРЕМЕННОМ ЭТАПЕ В РОССИИ

§ 1. Конституционализация применения информационных технологий в сфере здравоохранения в Российской Федерации

В настоящее время в нашей стране усиливается нормотворческая деятельность, направленная на решение конституционных проблем, связанных с цифровизацией общественных отношений. Существующие конституционные нормы изменяются или модернизируются таким образом, чтобы лучше соответствовать преобразованиям цифровой эпохи. Как отмечает И.А. Кравец, «конституционализируется цифровое и информационное пространство, на которое распространяются некоторые конституционные принципы и конституционные права; происходит цифровизация конституционных прав и свобод, их техническое оснащение посредством цифровых технологий»¹⁶².

Под конституционализацией мы понимаем процесс возведения общественных отношений в различных сферах на высший, конституционный уровень путем создания основополагающей нормы, защищенной конституцией.

Процесс конституционализации включает в себя не только появление новых норм, но и адаптацию существующих правовых механизмов к вызовам, связанным с развитием информационных технологий. Согласимся с позицией М. Лохлина в переводе И.А. Умновой, подразумевавшего под конституционализацией «подчинение деятельности органов публичной власти структурам, процессам, принципам и ценностям конституции»¹⁶³. Поэтому конституционализация применения информационных технологий выражается в конституционно-

¹⁶² Кравец И.А. Цифровой конституционализм: методологические и правовые аспекты // Государство и право. 2022. № 1. С. 19-33.

¹⁶³ Умнова И.А. «Лохлин М. Что означает конституционализация? Реф. статьи: Loughlin M. What is constitutionalisation?» // Современный конституционализм: Теория, доктрина и практика. 2013. С. 155-159.

правовом регулировании, в первую очередь принципами и нормами Конституции Российской Федерации, которые позволяют решать проблемы, связанные с реализацией конституционных прав, посредством правотворческой деятельности.

Российская конституционная реформа 2020 г. напрямую коснулась темы настоящего исследования. Если до конституционных поправок 2020 года пункт «м» ст. 71 Конституции Российской Федерации был изложен в следующей редакции: «В ведении Российской Федерации находятся: оборона и безопасность; оборонное производство; определение порядка продажи и покупки оружия, боеприпасов, военной техники и другого военного имущества; производство ядовитых веществ, наркотических средств и порядок их использования»¹⁶⁴, то в новой редакции он был дополнен словами «обеспечение безопасности личности, общества и государства при применении информационных технологий, обороте цифровых данных»¹⁶⁵.

Соответственно после внесения изменений 2020 года в Конституцию России пункт «м» ст. 71 предусматривает, что государство теперь обязано обеспечить безопасность личности, общества и государства при применении информационных технологий, обороте цифровых данных. Это подразумевает, что в случае применения информационных технологий государство берет на себя обязанность обеспечить гарантии реализации прав граждан, так как «информатизация несет угрозу личной и государственной безопасности, связанную с возможностью несанкционированного вторжения в сферы частной жизни и контроля за ней»¹⁶⁶. При этом в соответствии с пунктом «и» ст. 71 Конституции Российской Федерации информационные технологии относятся к ведению Российской Федерации, как и установление единых правовых основ системы здравоохранения согласно пункту

¹⁶⁴ Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // «Российская газета», № 237 (853).

¹⁶⁵ Там же.

¹⁶⁶ Лолаева А.С. Электронная демократия в России: юридическая форма и доктринальная интерпретация // Журнал российского права. 2023. № 4. С. 37-48

«е» ст. 71 Конституции Российской Федерации¹⁶⁷. Ранее в старой редакции вышеуказанные положения отсутствовали в пункте «е» ст. 71 и в пункте «и» ст. 71 Конституции Российской Федерации.

Важно отметить, что в совместном ведении Российской Федерации и субъектов Российской Федерации в соответствии с пунктом «ж» части 1 ст. 72 Конституции Российской Федерации находится только «координация вопросов здравоохранения, в том числе обеспечение оказания доступной и качественной медицинской помощи, сохранение и укрепление общественного здоровья, создание условий для ведения здорового образа жизни, формирования культуры ответственного отношения граждан к своему здоровью; социальная защита, включая социальное обеспечение»¹⁶⁸.

Также нельзя не упомянуть, что поправками 2020 года внесены касающиеся нашего вопроса изменения в главу о местном самоуправлении: теперь в соответствии с частью 1 ст. 132 Конституции Российской Федерации органы местного самоуправления в соответствии с федеральным законом обеспечивают в пределах своей компетенции доступность медицинской помощи¹⁶⁹. Этот факт может свидетельствовать об укреплении роли органов муниципальной власти в сфере здравоохранения, поскольку они принимают на себя обязанность по организации предоставления доступности медицинской помощи гражданам. Тем самым согласимся с позицией В.П. Григонис, Н.Ю. Немовой, Е.Ю. Одиноковой, отметивших, что «сотрудничество органов государственной власти и местного самоуправления в сфере здравоохранения позволит государству обеспечить медицинскую помощь обществу на более достойном уровне»¹⁷⁰.

¹⁶⁷ Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // «Российская газета», № 237 (853).

¹⁶⁸ Там же.

¹⁶⁹ Там же.

¹⁷⁰ *Григонис В.П., Немова Н.Ю., Одинокова Е.Ю.* Местное самоуправление в России: развитие законодательства и вопросы соотношения полномочий с государственными органами публичной власти // Государственная власть и местное самоуправление. 2024. № 1. С. 27 - 31.

С другой стороны, существует иная точка зрения, согласно которой положения Федерального закона от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» закрепляют исключительные полномочия органов местного самоуправления по созданию условий для оказания медицинской помощи населению по объему правомочий существенно уже, чем предусмотрено в Конституции Российской Федерации, поэтому новые конституционные положения не коррелируются с действующим федеральным законодательством¹⁷¹. Отметим, что пункт 6 части 1 ст. 32 нового Федерального закона от 20 марта 2025 г. № 33-ФЗ «Об общих принципах организации местного самоуправления в единой системе публичной власти» в части участия органов местного самоуправления в осуществлении охраны здоровья граждан на территории муниципального образования, включая обеспечение доступности медицинской помощи, отсылает на положения Федерального закона от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», что не позволяет подробно конкретизировать полномочия органов местного самоуправления по созданию условий для оказания медицинской помощи населению¹⁷².

Тем не менее вышеуказанные поправки в Конституцию России явились отправной точкой в совершенствовании российского законодательства с дальнейшей целью закрепления в нормативных правовых актах вопросов применения информационных технологий¹⁷³. С.А. Авакьян в своей статье отмечал

¹⁷¹ Вичева А. А. Обеспечение доступности медицинской помощи как новый уровень конституционных полномочий органов местного самоуправления в России // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2022. Т. 8. № 1. С. 54-61.

¹⁷² Федеральный закон от 20 марта 2025 г. № 33-ФЗ «Об общих принципах организации местного самоуправления в единой системе публичной власти» // "Собрание законодательства РФ", 28.11.2011, № 48, ст. 6724.

¹⁷³ Аналогичные процессы конституционализации применения информационных технологий имеются и в ряде зарубежных стран.

Почти так же, как и в Конституции России, упоминаются информационные технологии в Конституции Германии, однако имеется существенное отличие, которое заключается в том, что данные технологии закрепляют механизм взаимодействия органов государственной власти на федеральном и региональном уровнях, что подразумевает совместное ведение полномочий в данной области.

в части поправок: «был развит, пополнен ряд положений всех глав, кроме гл. 1, 2, 9, что сделало Конституцию более соответствующей современным реалиям»¹⁷⁴. Конституция Российской Федерации служит фундаментом информатизации общества, поэтому можно ожидать, что на основе новых положений ст. 71 Конституции будет формироваться вся необходимая нормативно-правовая база в указанной сфере.

Однако не все авторы согласны с содержанием новых формулировок и предлагают свои варианты. Например, Т.В. Заметина, Е.В. Комбарова считают, что подход, при котором устанавливается приоритет Российской Федерации, ограничивает возможность использования именно искусственного интеллекта в ущерб защищаемым Конституцией РФ ценностям, основам конституционного строя страны¹⁷⁵. Исходя из данного мнения, из-за закрепления в Конституции Российской Федерации информационных технологий в ведении Российской Федерации, к которым относится в том числе искусственный интеллект, возможность их использования оказывается ограниченной. А.С. Лолаева отмечает, что нужно было информационные технологии закрепить в ст. 72 Конституции и вопросы информации и информационных технологий должны относиться к совместному ведению Российской Федерации и субъектов Российской Федерации, поскольку субъекты Федерации вполне «самостоятельно решают многочисленные и многообразные вопросы, связанные с созданием и поддержкой информационных региональных систем, а также доступа к региональным информационным

Примечательно, что Конституция Мексики наделяет исключительным полномочием федеральную власть Мексики в лице Конгресса Союза по регулированию информационных и коммуникационных технологий (ст. XVII Конституции Мексики), и точно так же, как Конституция России, закрепляет за государством исключительное ведение области информационных технологий и связи.

¹⁷⁴ *Авакьян С.А.* Конституционная реформа 2020 и российский парламентаризм: реальность, решения, ожидания // Вестник Моск. гос. обл. университета. Сер. Юриспруденция. 2020. № 3. С. 8

¹⁷⁵ *Заметина Т. В., Комбарова Е. В.* Искусственный интеллект и конституционные вопросы его внедрения в современной России // Правовая политика и правовая жизнь. 2021. № 1. С. 180-189.

ресурсам, регулируемые законодательством субъектов Федерации, насчитывающим сотни нормативных актов»¹⁷⁶.

С данным мнением нельзя согласиться, так как огромное количество нормативных актов, издаваемых на уровне субъектов Российской Федерации, содержали разные противоречивые положения, направленные на регулирование применения информационных технологий в здравоохранении, что создавало правовые коллизии, затрудняло оказание медицинской помощи и нарушало принцип единства правового пространства. Например, до конституционных поправок в ранее принятых субъектами Российской Федерации актах в части применения телемедицинских технологий отсутствовало единообразие и последовательность, только в некоторых из них присутствовали нормы об информационной безопасности в связи с использованием телемедицинских технологий. Многие нормативные правовые акты субъектов РФ содержали определение понятия «телемедицина», при этом устанавливалось, что в задачи телемедицины включаются не только проведение телеконсультаций, но и организация обучения, проведение научных мероприятий, решение управленческих задач¹⁷⁷, что не соответствует смыслу телемедицинских технологий, закрепленных в Федеральном законе от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации». В этой связи закрепление информационных технологий и обеспечение безопасности личности, общества при применении информационных технологий в исключительном ведении Российской Федерации является необходимым условием для создания единого правового пространства. Данный шаг направлен на унификацию правового регулирования применения информационных технологий и обеспечение единообразия правоприменительной практики на всей территории России. Его

¹⁷⁶ Лолаева А. С. Вопросы цифровизации в новой редакции Конституции Российской Федерации // Международный журнал конституционного и государственного права. 2021. № 1. С. 110-113

¹⁷⁷ Акулин И. М., Чеснокова Е.А., Пресняков Р.А., Прядко А.Е. Телемедицина: правовой опыт регулирования субъектов Российской Федерации, перспективы развития // Проблемы стандартизации в здравоохранении. 2020. №. 5-6. С. 15-22.

реализация позволила привести региональное законодательство в области применения информационных технологий в строгое соответствие с федеральными нормативными правовыми актами, устранив тем самым правовые коллизии и формируя целостное правовое поле.

И.М. Акулин с соавторами на этот счет справедливо подчеркивает, что существующие на момент 2020 года «отличия в правовых актах субъектов Российской Федерации, регламентирующих порядок проведения телемедицинских консультаций, будут создавать в дальнейшем препятствия для оказания оперативной помощи с помощью телемедицинских технологий»¹⁷⁸.

Тем не менее, по данному вопросу имеется конструктивное замечание А.Г. Дейнеко, который верно подметил: «с учетом того, что Конституция России относит информационные технологии к исключительным полномочиям Российской Федерации, в Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» нет разъяснений по поводу того, как отличить их от иных видов информационных технологий, а часть 2 ст. 12 этого Закона указывает на полномочия государственных органов и органов местного самоуправления в сфере применения информационных технологий»¹⁷⁹, что свидетельствует о делегировании соответствующих полномочий на другие территориальные уровни власти. В этой связи полагаем, что было бы целесообразно внести изменения в указанный Федеральный закон и уточнить часть 2 ст. 12, определив виды информационных технологий. Такая практика имеется на уровне подзаконных актов федеральных ведомств. Например, в приказе Минкомсвязи России от 23 апреля 2020 г. № 195 «Об утверждении методик расчета показателей федерального проекта «Цифровые технологии» и постановлении Правительства Российской Федерации от 15 декабря

¹⁷⁸ Там же, С. 20.

¹⁷⁹ Дейнеко А.Г. Информационно-правовой комментарий к поправкам в Конституцию Российской Федерации // Труды по интелл. собственности. 2021. Т. 37, № 1/2. С. 9–10.

2020 г. № 2110¹⁸⁰ указаны некоторые технологии, относящиеся к «сквозным» цифровым технологиям.

О.Ю. Архирейская выделила очень важное замечание: «Применение информационных технологий не должно создавать угрозу пренебрежения конституционными правами и свободами человека и гражданина, снижения уровня жизни и социально-экономического развития, суверенитету государства»¹⁸¹.

Соглашаясь с указанным мнением, считаем, что законодатель верно определил информационные технологии в тексте Конституции Российской Федерации именно в статье об исключительном ведении Российской Федерации. Упоминание информационных технологий в пункте «и» ст. 71 Конституции Российской Федерации в исключительном ведении явилось необходимостью со стороны государства, ведь еще в 2017 году Конституционный Суд Российской Федерации в своем постановлении от 26 октября 2017 г. № 25-П указывал по поводу информации, что «обязанность обеспечить баланс прав и законных интересов в связи с современными условиями развития информации, а также определенность правового положения участников правоотношений, объектом которых она выступает, и правоотношений, связанных с ее поиском, получением, передачей, производством и распространением лежит на федеральном законодателе»¹⁸².

¹⁸⁰ Приказ Минкомсвязи России от 23 апреля 2020 г. № 195 «Об утверждении методик расчета показателей федерального проекта "Цифровые технологии" национальной программы "Цифровая экономика Российской Федерации». URL: <https://base.garant.ru/74858195/> (дата обращения: 28.11.2024); Постановление Правительства Российской Федерации от 15 декабря 2020 г. № 2110 «Об утверждении Правил предоставления из федерального бюджета субсидии на проведение повышения квалификации преподавателей высшего и среднего профессионального образования по новым программам для ИТ-специальностей и различных предметных отраслей и обеспечение достижения отдельных результатов федерального проекта «Кадры для цифровой экономики» на базе автономной некоммерческой организации высшего образования «Университет Иннополис» // «Собрание законодательства РФ», 28.12.2020, № 52 (Часть I), ст. 8808

¹⁸¹ Архирейская Т.Ю. Поправка-2020: обеспечение безопасности личности, общества и государства при применении информационных технологий, обороте цифровых данных // Труды Оренбургского института (филиала) Московской государственной юридической академии. 2021. № 1(47). С. 6.

¹⁸² Постановление Конституционного Суда Российской Федерации от 26 октября 2017 г. № 25-П «По делу о проверке конституционности пункта 5 статьи 2 Федерального закона «Об

Следовательно, федеральный уровень правового регулирования должен включать основополагающие принципы оказания медицинской помощи, определяющие систему здравоохранения в целом, обеспечивающую равные условия и объем получения медицинской помощи российскими гражданами, в том числе с использованием информационных технологий. В обеспечении же ее доступности и качества участвуют субъекты Российской Федерации, поскольку данный процесс зависит от географических, национальных, экологических и других особенностей субъекта РФ. В любом случае информационные технологии впервые были включены в текст Конституции Российской Федерации, что говорит о восполнении недостающих элементов в положениях Конституции Российской Федерации, регулирующих круг правоотношений в сфере цифровизации.

Российская Федерация также регулирует те отношения, которые возникают при защите прав субъектов отношений, участвующих в информационных процессах и цифровизации. Конституционно-правовое воздействие на политику цифровизации было отмечено Н.С. Бондарем: конституционное право способно оказывать нормативно-ориентирующее воздействие на новое, активно формирующееся информационно-цифровое пространство¹⁸³. Рассмотрение сферы информационного пространства с точки зрения конституционного права предполагает ее конституционализацию¹⁸⁴, при этом дополнительно происходит цифровизация конституционных прав и свобод посредством применения информационных технологий¹⁸⁵.

Таким образом, формирование конституционно-правового регулирования применения информационных технологий в сфере здравоохранения с

информации, информационных технологиях и о защите информации» в связи с жалобой гражданина А.И. Сушкова» // «Собрание законодательства РФ», 06.11.2017, № 45, ст. 6735

¹⁸³ *Бондарь Н.С.* Информационно-цифровое пространство в конституционном измерении: из практики конституционного Суда Российской Федерации // Журнал российского права. 2019. № 11. С. 25-42.

¹⁸⁴ *Киричек Е.В.* Цифровизация в конституционно-правовом измерении // Вестник Восточно-Сибирского института МВД России. 2020. № 4(95). С. 29-40.

¹⁸⁵ *Кравец И.А.* Цифровизация, право и конституция // Право цифровой среды: Монография / Под редакцией Т.П. Подшивалова, Е.В. Титовой, Е.А. Громовой. Москва, 2022. С. 185-200.

одновременной реализацией действующих конституционных принципов в целях соблюдения и защиты конституционных прав человека представляется первостепенной задачей государства.

Согласимся с мнением Д.И. Шокиной, что в Конституции Российской Федерации в результате изменений задается направление дальнейшего развития законодательного регулирования отношений в области информационных технологий, закрепляется сама необходимость регулирования и определяется субъект, в чьем ведении это регулирование должно находиться¹⁸⁶. Такие изменения могут затронуть различные общественные отношения во всех сферах жизнедеятельности человека, поднимая тем самым вопрос о более эффективном и совершенном правовом регулировании. Наиболее убедительный пример такого внедрения новых информационных технологий в конституционно-правовую жизнь содержится в сфере здравоохранения.

Принципы, содержащиеся в Конституции Российской Федерации, определяют основные направления развития государственной политики в области цифровизации здравоохранения. Фундаментальная трансформация правоотношений, связанных с применением информационных технологий, предполагает модернизацию конституционно-правового регулирования в сфере здравоохранения.

В Российской Федерации в соответствии с пунктом 2 ст. 19 Конституции Российской Федерации государство гарантирует равенство прав и свобод человека и гражданина независимо от пола, расы, национальности, языка, происхождения, имущественного и должностного положения, места жительства, отношения к религии, убеждений, принадлежности к общественным объединениям, а также

¹⁸⁶ Шокина Д. И. Влияние поправок к конституции 2020 на повышение роли информационных технологий в избирательном процессе // Стабильность и динамизм Российской Конституции : Материалы XII Международного Конституционного Форума, посвященного 15-летию возрождения юридического факультета СГУ имени Н.Г.: сборник научных статей, Саратов, 16–18 декабря 2020 года. Том Часть 1. – Саратов: Издательство "Саратовский источник", 2021. С. 243-248.

других обстоятельств¹⁸⁷. Что касается обеспечения фактического равенства, то в соответствии с частью 2 ст. 7 Конституцией Российской Федерации фактическое правовое равенство реализуется в Российской Федерации на уровне минимальных государственных социальных стандартов: оказания медицинской помощи в государственных и муниципальных учреждениях здравоохранения, охраны здоровья людей и др.

Принцип равноправия часто оказывается под угрозой из-за особенностей цифровизации общественных отношений. Вмешательство в личную жизнь граждан, связанное с использованием информационных технологий, вызывает тревогу у людей, создает напряженность между обществом и государством, дестабилизирует общественные отношения и затрудняет защиту прав человека, что в свою очередь может привести к различным нарушениям конституционных прав и свобод.

Принцип защиты достоинства личности и прав человека и гражданина играет ключевую роль в сфере здравоохранения в организации и предоставлении медицинской помощи, признавая приоритет интересов пациента и его личности. При оказании медицинской помощи необходимо учитывать не только медицинские показания, но и личные предпочтения и потребности пациента, что подчеркивает индивидуальный подход к каждому человеку.

В литературе признается, что в настоящее время соблюдение прав человека в области здравоохранения остается важным вопросом, который пока не нашел должного правового регулирования в новых реалиях. С учетом текущей ситуации в правовом поле и распространением политики цифровизации в части общественных отношений, связанных с применением информационных технологий, поднимается проблема защиты прав человека при их использовании. В такой ситуации возникают принципиально новые отношения, в связи с чем, соответственно, повышаются риски нарушения реализации прав граждан. Так,

¹⁸⁷ Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // «Российская газета», № 237 (853).

Бондарь Н.С., например, по этому поводу отмечал, что возникают проблемы, связанные с реализацией цифровых прав, пределами вмешательства в частную жизнь¹⁸⁸.

А.Я. Неверов справедливо поднимает вопрос: «обеспечивают ли конституционные нормы и созданные на базе Конституции нормативные акты, безопасное развитие общественных отношений в условиях развития информационных технологий?»¹⁸⁹. В результате он приходит к выводу, что конституционное регулирование применения информационных технологий осуществляется неэффективно, оно «не в полной мере справляется с возложенной на него функцией по обеспечению и защите прав и свобод человека»¹⁹⁰.

С данной позицией согласны и другие авторы, например, по мнению И.А. Петроченкова, актуальным цифровым разработкам и технологиям не хватает комплексного нормативного правового сопровождения при их развитии и внедрении. Указанные процессы сопровождаются принятием актов, которые носят в большей степени технический или утилитарный нежели конституционно-правовой характер¹⁹¹. Поэтому в дальнейшем законодательство России неизбежно придет к правовому регулированию таких направлений медицинской деятельности, как «интернет медицинских вещей», анализ больших медицинских данных, применение искусственного интеллекта и других¹⁹².

Мы солидарны с позициями вышеуказанных исследователей, тем не менее следует все же отметить, что активная работа по урегулированию применения

¹⁸⁸ Бондарь Н.С. Информационно-цифровое пространство в конституционном измерении: из практики Конституционного суда Российской Федерации // Журнал российского права. 2019. № 11. С. 25—42.

¹⁸⁹ Неверов А.Я. О месте и роли конституционно-правового регулирования общественных отношений в условиях развития информационных технологий // Вестник Московского университета МВД России. 2021. № 6. С. 207-214.

¹⁹⁰ Там же. С. 211.

¹⁹¹ Петроченков И. А. К вопросу о практике реализации конституционных новелл в сфере информационных технологий // Право и государство: теория и практика. 2023. № 6(222). С. 427-432.

¹⁹² Ковалева Н. Н., Новикова Е. А. Особенности правового регулирования телемедицинских технологий в условиях цифровизации // Право и государство: теория и практика. 2021. № 7 (199). С. 150–152.

некоторых информационных технологий в здравоохранении началась в России с конца 2010-х и продолжается в настоящее время.

Федеральный закон от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» с 2017 года содержит термин «телемедицинские технологии», а также определяет особенности медицинской помощи, оказываемой с их применением, а также специфику медицинской деятельности с соблюдением требований, установленных законодательством в области персональных данных¹⁹³.

Нормативным основанием для принятия подзаконных актов в части медицинской информационной системы и обработки персональных данных пациентов стала ст. 91 Федерального закона от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»¹⁹⁴. В 2021 г. вступил в силу приказ Минздрава России от 7 сентября 2020 г. № 947н «Об утверждении Порядка организации системы документооборота в сфере охраны здоровья в части ведения медицинской документации в форме электронных документов», который создает правовые основания для перехода от бумажной на электронную медицинскую карту и регламентирует правила медицинского электронного документооборота, устанавливая требования к формированию, подписанию и хранению электронных медицинских документов, включая обмен ими и передачу в Единую государственную информационную систему здравоохранения¹⁹⁵.

После конституционных поправок 2020 года внедрение информационных технологий в здравоохранение было обусловлено реализацией изменений в ст. 71 Конституции Российской Федерации об информационных технологиях, что выразилось в разработке новых нормативных правовых актов. Принятие поправок

¹⁹³ Федеральный закон от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» // «Собрание законодательства РФ», 28.11.2011, № 48, ст. 6724.

¹⁹⁴ Там же.

¹⁹⁵ Приказ Минздрава России от 7 сентября 2020 г. № 947н «Об утверждении Порядка организации системы документооборота в сфере охраны здоровья в части ведения медицинской документации в форме электронных документов». URL: <http://publication.pravo.gov.ru/Document/View/0001202101120007> (дата обращения: 28.11.2024).

послужило импульсом для более активного внедрения экспериментальных правовых режимов в сфере здравоохранения. Среди них выделяются экспериментальные правовые режимы по искусственному интеллекту (2020 г.), и телемедицинским технологиям (2022-2023 гг.), которые мы затронем в следующем параграфе.

Таким образом, можно сделать следующие выводы по данному параграфу.

Конституционные поправки 2020 года, закрепившие отнесение информационных технологий к исключительному ведению Российской Федерации, создали фундаментальную правовую основу для цифровой трансформации ключевых сфер общественной жизни, в том числе здравоохранения. Это решение законодателя является логичным и обоснованным ответом на вызовы цифровой эпохи, поскольку оно направлено на обеспечение единообразия правового регулирования, национальной безопасности и защиты прав граждан от потенциальных угроз, связанных с несанкционированным использованием данных.

Однако конституционное закрепление предметов ведения и полномочий является лишь отправной точкой. Актуальной проблемой остается системное отставание текущего законодательства от динамично развивающихся технологических реалий.

Иными словами, использование новых технологий в условиях новой информационной реальности не всегда позитивно, и значимость реализации принципов конституционного права при активном использовании современных цифровых технологий возрастает¹⁹⁶. Поэтому требуется разработка и принятие комплексных нормативных актов, которые, опираясь на конституционные принципы, установят требования для применения информационных технологий в здравоохранении. Это обеспечит не только требуемый технологический прогресс,

¹⁹⁶ Государство и право в новой цифровой реальности : монография / под общ. ред. д-ра юрид. наук, проф. И.А. Умновой-Конюховой и д-ра техн. наук, проф. Д.А. Ловцова. – М.: РАН. ИНИОН, 2020. 259 с.

но и надежные гарантии соблюдения конституционных прав и свобод человека и гражданина в условиях цифровизации.

Следовательно, необходим детальный анализ тех разновидностей информационных технологий, которые выделены в первом параграфе первой главы настоящего исследования, в целях выявления проблем в правовом регулировании, рисков и определения путей совершенствования законодательства. Такой подход позволяет не только диагностировать существующие проблемы в правовом поле, но и сформулировать научно обоснованные предложения по его оптимизации с учетом баланса публичных и частных интересов в условиях цифровизации.

§ 2. Особенности становления системных правовых основ применения информационных технологий в российском здравоохранении

Активная цифровая трансформация сферы здравоохранения, инициированная на государственном уровне, обусловила необходимость поиска гибких правовых механизмов, позволяющих синхронизировать динамичное развитие технологий и традиционную систему правового регулирования. Одним из таких инструментов, призванных сократить отставание законодательства от технологических реалий, стал экспериментальный правовой режим, получивший второе название «регуляторная песочница», одна из основных целей которой, как отмечает И.А. Умнова-Конюхова, заключается в том, чтобы сделать правовое регулирование более гибким¹⁹⁷.

В 2020 году был принят Федеральный закон от 31 июля 2020 № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых и технологических инноваций в Российской Федерации», который «представляет собой специальное регулирование, направленное на сотрудничество органов публичной власти с

¹⁹⁷ Умнова-Конюхова И.А. Трансформация современного права под влиянием научно-технологического развития: общие тенденции и опыт России // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4, Государство и право. 2024. №. 4. С. 9-25.

широким кругом предпринимателей, улучшение экономического состояния государства, удовлетворение общественных нужд и поиск компромисса при принятии общественно значимых решений»¹⁹⁸.

Согласно ст. 4 данного Федерального закона основным принципом экспериментального правового режима является «недопустимость ограничения конституционных прав и свобод граждан, нарушения единства экономического пространства на территории Российской Федерации или иного умаления гарантий защиты прав граждан и юридических лиц, предусмотренных Конституцией Российской Федерации»¹⁹⁹. В соответствии с принципом верховенства Конституции Российской Федерации экспериментальный правовой режим должен соответствовать положениям Конституции Российской Федерации. Исключение из данного правила привело бы к возникновению разного рода экспериментальных правовых режимов, которые произвольно устанавливали бы требования к различным информационным технологиям, противоречащим конституционным основам и установленным законным ценностям. В этом контексте также важен конституционный принцип равенства. Он не будет нарушен, если экспериментальный характер правового режима будет определен прозрачно, останется публичным, условия будут точно регламентированы, а с учетом ожидаемых эффектов риски будут соразмерны ожидаемым выгодам.

На его основе к концу 2024 года запущено 16 экспериментальных правовых режимов по различным информационным технологиям. Такие режимы возникли с целью выявления эффективности информационных технологий и их внедрения в сферы общественной жизни на временной основе в определенных субъектах РФ с последующим их полноценным регулированием, это позволяет сократить отставание законодательства от развития новейших информационных технологий.

¹⁹⁸ Сушильников И.С. Конституционно-правовые основы экспериментальных правовых режимов // Теоретическая и прикладная юриспруденция. 2023. № 1(15). С. 109-121.

¹⁹⁹ Федеральный закон от 31 июля 2020 г. № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых и технологических инноваций в Российской Федерации // «Собрание законодательства РФ», 03.08.2020, № 31 (часть I), ст. 5017.

По мнению И.С. Сушильникова, экспериментальные правовые режимы «затрагивают конституционные принципы единого экономического пространства в тесной взаимосвязи с принципом свободного использования своих способностей и имущества для предпринимательской и иной не запрещенной законом экономической деятельности»²⁰⁰. Отсюда следует, что экспериментальные правовые режимы направлены на стимулирование использования информационных технологий в условиях гармоничного экономического пространства, где субъекты имеют равные и прозрачные правовые условия, что позволит решить экономические и социальные проблемы, а также распространить в будущем практику на всю территорию России. Следовательно, экспериментальные правовые режимы обеспечивают определённую степень контроля, помогая законодателю лучше внедрять информационные технологии, прежде чем принимать решение о необходимости и порядке их полноценного регулирования.

Кроме того, экспериментальный правовой режим позволяет соблюсти права и законные интересы граждан в рассматриваемой предметной сфере, поскольку регулирование особенностей оказания телемедицинских услуг, дистанционного наблюдения за состоянием здоровья через информационную систему позволяет перевести возникающие в этой связи общественные отношения в правовое русло. В противном случае отсутствие регулирования области применения информационных технологий в здравоохранении может привести к ущемлению прав и законных интересов граждан. Например, в части отсутствия регламентации особенностей обработки персональных данных, выдачи электронных рецептов, ответственности врача за коррекцию ранее назначенного лечения и т.п.²⁰¹.

Стоит отметить, что применение информационных технологий поднимает множество острых правовых проблем, связанных с ответственностью в сфере

²⁰⁰ Сушильников И. С. Конституционно-правовые основы экспериментальных правовых режимов // Теоретическая и прикладная юриспруденция. 2023. № 1(15). С. 109-121.

²⁰¹ Коваленко М. А. К вопросу о применении экспериментального правового режима в области телемедицины в России // Пролог: журнал о праве. 2024. №. 1 (41). С. 43-53.

здравоохранения. Например, в случае нанесения вреда при использовании искусственного интеллекта. Так, И.В. Понкин и А.И. Редькина поднимают проблему персонификации и квалификации ответственности за действия искусственного интеллекта в части возмещения ущерба²⁰². И.В. Балтутите, в свою очередь, рассматривает вопрос корректного определения юридической ответственности за вред здоровью пациента, наступивший в результате применения технологий искусственного интеллекта и робототехники в процессе оказания медицинской помощи²⁰³. При этом было установлено, что искусственный интеллект не может обладать правосубъектностью, а значит, его невозможно привлечь к ответственности²⁰⁴. Конкретно в сфере здравоохранения, как отмечает А.Ю. Киселева, круг и сфера ответственности лиц, несущих ответственность за некачественное оказание медицинской помощи однозначно не определены, когда применяется искусственный интеллект²⁰⁵.

Вышеуказанная проблема находится в стадии разрешения, о чем свидетельствуют недавние поправки в Федеральный закон от 31 июля 2020 № 258-ФЗ «Об экспериментальных правовых режимах», в результате которых в экспериментальных правовых режимах была введена процедура выявления ответственных за инциденты с решениями, принятыми искусственным интеллектom. Федеральным законом от 8 июля 2024 г. № 169-ФЗ «О внесении изменений в Федеральный закон «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» вводится новая ст. 18.1, которая закрепляет возможность создания отдельной комиссии после инцидента с

²⁰² Понкин И.В., Редькина А.И. Искусственный интеллект с точки зрения права // Вестник Российского университета дружбы народов. Серия: Юридические науки. 2018. Т. 22. №. 1. С. 91-109.

²⁰³ Балтутите И. В. Правовые проблемы использования искусственного интеллекта в сфере здравоохранения // Правовая парадигма. 2022. Т. 21, № 2. С. 140-148.

²⁰⁴ Федотов Н. Е. Искусственный интеллект и его правосубъектность: философско-правовая интерпретация // Традиции и новации в системе современного российского права : Материалы XX Международной конференции молодых ученых. В 3-х томах, Москва, 09–10 апреля 2021 года. Том 3. Москва: Московский государственный юридический университет имени О.Е. Кутафина (МГЮА), 2021. С. 399-401.

²⁰⁵ Киселева А. Ю. Применение искусственного интеллекта в здравоохранении: аспекты медицинского права // Медицинское право: теория и практика. 2020. Т. 6, № 2(12). С. 29-38.

причинением вреда технологическим решением с искусственным интеллектом²⁰⁶. Она исследует инцидент и выявляет, по какой причине тестируемое решение принесло вред. Данные изменения рассматриваются как первый шаг к установлению ответственности, связанной с вредом, причиненным искусственным интеллектом.

Таким образом, экспериментальный правовой режим направлен на стимулирование использования информационных технологий в условиях гармоничного экономического пространства и помогает законодателю понять, какой нужен наиболее эффективный способ реализации информационных технологий, прежде чем принимать решение о необходимости и порядке их полноценного регулирования, что исходит из конституционного принципа поддержки конкуренции. Поэтому экспериментальный правовой режим позволяет по истечении некоторого временного промежутка определить адекватный подход к правовому регулированию информационных технологий с учетом полученных результатов, а также соотношения баланса публичных и частных интересов и развития экономики в условиях цифровизации.

Законодатель попытался найти этот баланс в экспериментальных правовых режимах в области здравоохранения, установив их для телемедицинских технологий и искусственного интеллекта. Экспериментальные правовые режимы по телемедицинским технологиям на данный момент реализуются в некоторых субъектах РФ, особенности взаимодействия органов государственной власти и пациентов, связанные с применением информационных технологий, непосредственно устанавливаются в таких режимах.

В г. Москве вводился экспериментальный правовой режим по использованию искусственного интеллекта в области компьютерного зрения с обработкой обезличенных персональных данных в рамках Федерального закона от 24 апреля 2020 г. № 123-ФЗ «О проведении эксперимента по установлению

²⁰⁶ Федеральный закон от 8 июля 2024 г. № 169-ФЗ «О внесении изменений в Федеральный закон «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» // «Собрание законодательства РФ», 15.07.2024, № 29 (Часть II), ст. 4098

специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в ст. 6 и 10 Федерального закона «О персональных данных»²⁰⁷. Как отмечают исследователи, эксперимент удался: в 2023 г. в Москве по результатам эксперимента был введен специальный тариф в рамках ОМС на анализ результатов профилактических маммографических исследований с помощью систем искусственного интеллекта²⁰⁸.

В экспериментальном правовом режиме в сфере цифровых инноваций по направлению медицинской деятельности с применением технологий сбора и обработки сведений о состоянии здоровья и диагнозов граждан «Персональные медицинские помощники», утвержденном постановлением Правительства Российской Федерации от 9 декабря 2022 № 2276, основное положение касается мер, направленных на минимизацию рисков причинения вреда жизни, здоровью, имуществу человека.

Ключевым элементом экспериментального правового режима выступает информационная система «Персональные медицинские помощники», предназначенная для осуществления дистанционного наблюдения за состоянием здоровья пациентов. Она обеспечивает сбор и обработку сведений о состоянии здоровья и диагнозах граждан при осуществлении дистанционного наблюдения за состоянием здоровья пациентов²⁰⁹.

²⁰⁷ Федеральный закон от 24 апреля 2020 г. № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в ст. 6 и 10 Федерального закона «О персональных данных» // "Собрание законодательства РФ", 27.04.2020, № 17, ст. 2701.

²⁰⁸ Казакова В. А., Тюлякова С. А., Шивилов Е. В., Аничкина К. А., Мифтахова А. Л., Юрканова Д. Д. Правовые основы применения технологий искусственного интеллекта в лучевой диагностике // Радиология—практика. 2023. №. 2. С. 63-77.

²⁰⁹ Постановление Правительства Российской Федерации от 9 декабря 2022 г. № 2276 «Об установлении экспериментального правового режима в сфере цифровых инноваций и утверждении Программы экспериментального правового режима в сфере цифровых инноваций по направлению медицинской деятельности с применением технологий сбора и обработки сведений о состоянии здоровья и диагнозов граждан в отношении реализации инициативы

По результатам эксперимента в Новосибирской области установлено, что он оправдал себя и теперь следует распространить систему на уровень всей федерации, а не отдельных субъектов РФ²¹⁰. Однако перед этим необходимо доработать платформу, на которую направляются данные пациентов.

Указанная информационная система позволяет собирать и обрабатывать информацию пациентов о состоянии здоровья и диагнозах граждан, что необходимо при дистанционном наблюдении за состоянием здоровья пациентов. Но в то же время необходимы более строгие меры, направленные на защиту этой системы от незаконного раскрытия такой информации, чего нет в нормах постановления Правительства Российской Федерации от 9 декабря 2022 № 2276. Например, в данном постановлении, как отмечает В.Э. Мамедова, не содержится указания на метод обезличивания, который следует использовать медицинской организации. Не установлено, в чью компетенцию входит вопрос о выборе такого метода²¹¹.

В свою очередь, постановлением Правительства Российской Федерации от 18 июля 2023 г. № 1164 «Об установлении экспериментального правового режима в сфере цифровых инноваций и утверждении Программы экспериментального правового режима в сфере цифровых инноваций по направлению медицинской деятельности, в том числе с применением телемедицинских технологий и технологий сбора и обработки сведений о состоянии здоровья и диагнозах граждан» введён экспериментальный правовой режим, направленный на дерегулирование.

В частности, постановлением исключено действие норм различных нормативных правовых актов в области применения телемедицинских технологий.

социально-экономического развития Российской Федерации «Персональные медицинские помощники» // «Собрание законодательства РФ», 19.12.2022, № 51, ст. 9237.

²¹⁰ «Персональные медицинские помощники» помогли 2,5 тысячам новосибирцев. URL: <https://zdrav.nso.ru/news/9006> (дата обращения: 11.09.2025)

²¹¹ Мамедова В. Э. Экспериментальные правовые режимы в сфере медицинской деятельности и персонифицированная медицинская информация: снижение уровня защищенности или дополнительные гарантии? // Юридический вестник Самарского университета Juridical Journal of Samara University. 2024. Т. 10. №. 3. С. 17-25.

Например, пациент имеет право в рамках экспериментального правового режима в случае возможности оказания медицинской помощи с применением телемедицинских технологий заменить врача, который проводил очный осмотр, на другого врача с 7-летним стажем той же медицинской организации, где был проведен очный осмотр²¹². Как отмечает В. О. Макаров, «при обращении за телемедицинской консультацией пациент может быть первично осмотрен врачом, который находится на территории муниципального образования или субъекта федерации, в котором проживает пациент, а в дальнейшем уже целенаправленно наблюдаться у профильного специалиста, являющегося врачом той же медицинской организации»²¹³.

Также устранены положения о письменной форме договора на оказание услуг – появилась электронная форма, изъяты нормы о даче информированного добровольного согласия только с помощью Единой системы идентификации и аутентификации²¹⁴.

Дополнительно в экспериментальном правовом режиме установлено «назначение лабораторных, инструментальных и иных дополнительных исследований в рамках телемедицинских технологий; назначение и осуществление дистанционного наблюдения за состоянием здоровья пациента; назначение (коррекция) лечения при условии установления лечащим врачом диагноза и назначения лечения (при его наличии) по тому же заболеванию после первичного

²¹² Постановление Правительства Российской Федерации от 18 июля 2023 г. № 1164 «Об установлении экспериментального правового режима в сфере цифровых инноваций и утверждении Программы экспериментального правового режима в сфере цифровых инноваций по направлению медицинской деятельности, в том числе с применением телемедицинских технологий и технологий сбора и обработки сведений о состоянии здоровья и диагнозах граждан» // "Собрание законодательства РФ", 24.07.2023, № 30, ст. 5693.

²¹³ Макаров В. О. Этапы развития правового регулирования телемедицины в России // Медицинское право: новые правовые вызовы в работе медицинских организаций : Материалы IV Международного форума по медицинскому праву, Екатеринбург, 25–26 апреля 2024 года. – Екатеринбург: Уральский государственный юридический университет им. В.Ф. Яковлева, 2024. С. 79-85.

²¹⁴ Усенков И. А. Стабильность законодательства о телемедицине: актуальные проблемы // Право и современные государства. 2023. № 6. С. 36-40.

очного приема пациента, совершенного в течение 30 дней до телемедицинской консультации»²¹⁵.

Согласимся с мнением А.М. Хурматуллиной в том, что «ЭПР в сфере здравоохранения ориентирован на участников частноправовых отношений в рамках оказания медицинской помощи на возмездных началах, при этом полностью исключена сфера бесплатного оказания гражданам медицинской помощи в соответствии с программой государственных гарантий»²¹⁶. Действительно, имеется нарушение конституционного принципа равноправия, поскольку экспериментальные правовые режимы в сфере здравоохранения содержат регулирование применения телемедицинских технологий в рамках оказания медицинской помощи пациентам только на платной основе, бесплатное оказание гражданам медицинской помощи с использованием указанных технологий исключено, что свидетельствует о необходимости внесения изменений в законодательство, которые позволили бы это сделать.

Разделяя позицию Н.И. Платоновой, отметим, что при принятии экспериментальных правовых режимов в сфере здравоохранения должно обеспечиваться соблюдение прав пациента, подразумевающих получение качественной медицинской помощи, сохранение врачебной тайны, а также должны быть соблюдены принципы открытости, разумности, обоснованности и прозрачности указанного режима, предусматривающего опубликование результатов, в том числе промежуточных, эксперимента²¹⁷.

Государства имеют особые обязательства в области прав человека в этой сфере.

²¹⁵ Макаров В.О., Коваленко М.А. К вопросу об эффективности регулятивных ограничений при проведении телемедицинских консультаций // Право и политика. 2024. № 4. С. 24-35.

²¹⁶ Хурматуллина А.М. Конституционно-правовые основы экспериментальных правовых режимов в сфере здравоохранения // Lex russica. 2024. Т. 77. №. 8 (213). С. 65-74.

²¹⁷ Платонова Н.И. К вопросу об экспериментальном правовом режиме в сфере телемедицинских технологий // Журнал Белорусского государственного университета. Право. 2021. № 3. С. 32-37.

Во-первых, государства должны обеспечить гарантии соблюдения и защиты конституционных прав от их нарушений третьими сторонами, и это обязательство распространяется на субъектов экспериментального правового режима. Это включает в себя обеспечение доступа к правосудию в случае нарушений прав человека, связанных с бизнесом.

Во-вторых, государства должны установить требования к субъектам экспериментального правового режима в отношении соблюдения прав человека.

Субъекты экспериментального правового режима также несут обязательства, связанные с правами человека, включая, как минимум, обязанность соблюдать стандарты в области прав человека.

В постановлениях Правительства Российской Федерации от 9 декабря 2022 г. № 2276 и от 18 июля 2023 года № 1164 указаны меры, направленные на минимизацию рисков причинения вреда жизни, здоровью, имуществу человека и другим субъектам, установлены обязанности субъектов экспериментального правового режима²¹⁸. Такие обязанности распределены между медицинской организацией, оператором медицинской информационной системы, разработчиком такой системы в целях защиты персональных данных пациента. Например, как отмечает В.Э. Мамедова, «к обязанностям разработчика относится определение информации, подлежащей защите от неправомерного доступа, а в обязанности оператора медицинской информационной системы включается организация

²¹⁸ Постановление Правительства Российской Федерации от 9 декабря 2022 г. № 2276 «Об установлении экспериментального правового режима в сфере цифровых инноваций и утверждении Программы экспериментального правового режима в сфере цифровых инноваций по направлению медицинской деятельности с применением технологий сбора и обработки сведений о состоянии здоровья и диагнозов граждан в отношении реализации инициативы социально-экономического развития Российской Федерации «Персональные медицинские помощники» // «Собрание законодательства РФ», 19.12.2022, № 51, ст. 9237; Постановление Правительства Российской Федерации от 18 июля 2023 года № 1164 «Об установлении экспериментального правового режима в сфере цифровых инноваций и утверждении Программы экспериментального правового режима в сфере цифровых инноваций по направлению медицинской деятельности, в том числе с применением телемедицинских технологий и технологий сбора и обработки сведений о состоянии здоровья и диагнозах граждан» // «Собрание законодательства РФ», 24.07.2023, № 30, ст. 5693.

мероприятий по аттестации системы по требованиям защиты информации»²¹⁹. Однако в постановлениях не установлены меры ответственности и механизм восстановления нарушенных прав пациентов в случае, если при сбое информационной системы «Персональные медицинские помощники» или телемедицинской системы персональные данные пациентов будут раскрыты.

П.С. Сивоконева отмечает по этому поводу: «без определения порядка ликвидации и способов защиты прав пациента нормативный правовой акт не сможет обеспечить качественное оказание медицинской помощи с применением дистанционных устройств»²²⁰. Поэтому представляется необходимым в экспериментальных правовых режимах закрепить меры ответственности и механизм восстановления прав пациентов в случае сбоя государственной информационной системы, иначе это может снижать меры защиты персональных данных пациентов, которые гарантируются государством.

Следовательно, экспериментальный правовой режим в сфере здравоохранения представляет собой управленческий механизм, призванный сформировать условия для развития цифровых решений. Его задача — модернизировать систему управления здравоохранением с помощью новых информационных технологий. При этом экспериментальный характер правовых режимов, установленных постановлениями Правительства Российской Федерации от 9 декабря 2022 г. № 2276 и от 18 июля 2023 года № 1164, исходит из принципа конституционного равенства субъектов регулирования, поскольку только в случае прозрачного содержания, конкретности условий порядка применения информационной технологии, соразмерности рисков ожидаемым выгодам, будет соблюден баланс публичных и частных интересов и развития экономики в области цифровизации.

²¹⁹ Мамедова В.Э. Экспериментальные правовые режимы в сфере медицинской деятельности и персонифицированная медицинская информация: снижение уровня защищенности или дополнительные гарантии? // Юридический вестник Самарского университета. 2024. Т. 10, № 3. С. 17-25.

²²⁰ Сивоконева П.С. Защита прав пациентов при использовании персональных медицинских помощников в рамках экспериментального правового режима // Право и практика. 2024. № 4. С. 72-75.

Иначе говоря, координация и установление общих правил для подобных инновационных механизмов относятся к компетенции федеральной власти. Ключевая роль в этом процессе принадлежит Правительству Российской Федерации, поскольку оно в результате конституционных изменений 2020 года в соответствии с пунктами «в» и «в.1» части 1 ст. 114 Конституции Российской Федерации обеспечивает «проведение единой социально ориентированной государственной политики в области здравоохранения» и «обеспечивает государственную поддержку научно-технологического развития Российской Федерации, сохранение и развитие ее научного потенциала»²²¹. Правительство Российской Федерации обеспечивает создание научно-технологической среды, в которой приверженность развитию безопасных информационных технологий может сочетаться с технологическим прогрессом.

Правительство Российской Федерации ответственно за осуществление политики в области внедрения информационных технологий. Это и обуславливает тот факт, что правовая регламентация информационных технологий представлена законодательством федерального уровня, поскольку установлено исключительное ведение Российской Федерации в формировании правовых рамок внедрения данных технологий на территории всего российского государства.

Например, Правительством на данный момент осуществляется реализация стратегического направления цифровой трансформации в сфере госуправления до 2030 года, в рамках которого планируется сокращение сроков предоставления госуслуг в онлайн-формате, обеспечение дальнейшего перехода на электронный документооборот органов местного самоуправления, государственных и муниципальных учреждений, автоматизация и упрощение межведомственного взаимодействия. Утверждённое распоряжением Правительства Российской Федерации от 16 марта 2024 г. № 637-р стратегическое направление предполагает реализацию ряда масштабных проектов. Один из них - развитие государственной

²²¹ Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // «Российская газета», № 237 (853).

информационной системы «Типовое облачное решение системы электронного документооборота» даст возможность к 2030 году перевести все органы местного самоуправления, а также государственные и муниципальные учреждения на электронный документооборот и сделать их участниками единого информационного пространства взаимодействия²²².

Данный пример свидетельствует о постепенном развитии информационных технологий в государственном управлении, которое в итоге привело к формированию в России концепции «электронного правительства». Его внедрение направлено, в том числе на обеспечение равного и удобного доступа граждан к государственным услугам, что коррелирует с целями конституционного принципа равноправия. «Электронное правительство» подразумевает деятельность федеральных и региональных органов исполнительной власти Российской Федерации по дистанционному оказанию государственных услуг по широкому кругу вопросов. По мнению И.Н. Исакова, благодаря высоким технологиям расширяется действие принципа правового равенства, обеспечивается его органическая связанность с нравственными началами, присутствующими в нормах первичного регулирования. Электронное правительство Российской Федерации можно характеризовать как «новый и достаточно сложный компонент российской правовой системы, выполняющий социально значимые функции на всех уровнях правового регулирования»²²³.

Разумеется, одной из областей, требующих пристального внимания, является здравоохранение. Её развитие напрямую затрагивает интересы каждого гражданина и имеет приоритетное значение для национальной повестки. В настоящее время на всей территории Российской Федерации активно реализуются

²²² Распоряжение Правительства Российской Федерации от 16 марта 2024 г. № 637-р «Об утверждении стратегического направления в области цифровой трансформации государственного управления» // "Собрание законодательства РФ", 25.03.2024, № 13, ст. 1837

²²³ Исаков И. Н. Новые технологии в праве как высокоэффективное средство реализации конституционного принципа равенства в условиях разноуровневого правового регулирования // Вестник Российского университета дружбы народов. Серия: Юридические науки. 2023. Т. 27. № 4. С. 919-938.

проекты, направленные на создание и внедрение цифровых сервисов для получения медицинских услуг в электронном формате.

Этот процесс является частью проекта по построению электронного правительства, центральной задачей которого является перевод взаимодействия граждан с властью в онлайн-формат. Такое взаимодействие осуществляется преимущественно через специализированные порталы и официальные сайты государственных и муниципальных ведомств.

Таким образом, экспериментальные правовые режимы в области здравоохранения напрямую вытекают из тенденции ее цифровизации: динамичное развитие информационных технологий в здравоохранении непрерывно опережает возможности традиционной, более консервативной, системы правового регулирования.

Экспериментальные правовые режимы представляют собой стратегический и неизбежный ответ законодателя на этот вызов. Они выступают не просто как один из инструментов, а как основной «правовой полигон», который позволяет:

- обеспечивать гибкость в условиях изменчивой среды и управлять неопределенностью и рисками, так как экспериментальные правовые режимы направлены на тестирование разных моделей регулирования в контролируемых условиях, не ставя под угрозу всю систему здравоохранения;

- создавать доказательную базу для будущих законов. Результаты экспериментов предоставляют законодателю не теоретические предположения, а фактические данные о последствиях, экономической эффективности и общественной реакции.

Тем самым только после этого становится возможным переход к этапу устойчивого и безопасного регулирования конкретных технологий на уровне всей страны. Следовательно, акцент на рассмотрении особенностей экспериментальных правовых режимов в здравоохранении логически предваряет и обуславливает последующее обсуждение отдельных информационных технологий. Поэтому далее необходимо выявить текущее состояние правового регулирования

применения информационных технологий в российском здравоохранении, чтобы установить особенности ее совершенствования и трансформации в результате развития цифровизации.

2.1. Технологии обработки первичных данных

Важной особенностью электронного правительства как особого комплекса организационно-технических средств в различных сферах является взаимодействие государства с гражданами (система отношений G2C, Government-to-Citizen)²²⁴. Поэтому для оценки российского опыта целесообразно упомянуть электронную систему принятия решений в сфере здравоохранения и улучшения доступа пациентов к медицинскому обслуживанию с помощью информационных технологий обработки первичных данных. Особого внимания в этом контексте заслуживает Единая государственная информационная система здравоохранения (ЕГИСЗ). Отечественная сфера здравоохранения трансформируется в результате внедрения ЕГИСЗ, которая направлена на решение административных задач и функций в системе здравоохранения.

Правовой основой для формирования ЕГИСЗ выступил Федеральный закон от 29 июля 2017 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам применения информационных технологий в сфере охраны здоровья», который унифицировал правила использования информационных технологий в сфере охраны здоровья²²⁵.

Концепция ЕГИСЗ претерпела изменения: до принятия Федерального закона от 29 июля 2017 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам применения информационных

²²⁴ *Шевурдяев С. Н.* Правовое сопровождение развития "электронного правительства" в России: новые идеалы и старые проблемы // Государственная власть и местное самоуправление. 2008. № 11. С. 30-37.

²²⁵ Федеральный закон от 29 июля 2017 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам применения информационных технологий в сфере охраны здоровья» // «Собрание законодательства РФ», 31.07.2017, № 31 (Часть I), ст. 4791.

технологий в сфере охраны здоровья»²²⁶ существовал централизованный подход к сбору медицинской информации для анализа, обработки и использования. После внесения поправок появилось разделение, и теперь ЕГИСЗ является федеральной медицинской информационной системой, действующей обособленно от медицинских информационных систем субъектов РФ, а также медицинских организаций, которые теперь применяются в том числе для координации, сотрудничества и взаимодействия с подсистемами ЕГИСЗ.

Медицинская информационная система в широком смысле определяется как система, которая объединяет сбор, обработку, отчетность и использование информации, необходимой для повышения эффективности и результативности медицинских услуг посредством лучшего управления на всех уровнях оказания медицинских услуг²²⁷. Целью внедрения медицинской информационной системы является снижение трудоемкости процессов использования информационного ресурса и повышение их надежности и оперативности.

Медицинские информационные системы можно отнести к технологиям обработки первичных данных, поскольку, как отмечает ряд авторов, у данных систем имеются следующие функции:

1. «Сбор и обработка данных пациентов, среди которых персональные, медицинские, демографические и т.д.
2. Внедрение электронных медицинских карт для упрощения работы.
3. Синхронизация с государственными системами учета для регистрации и обновления данных.
4. Автоматический сбор статистических данных, позволяющий в дальнейшем оптимизировать работу медицинской организации.

²²⁶ Федеральный закон от 29 июля 2017 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам применения информационных технологий в сфере охраны здоровья» // «Собрание законодательства РФ», 31.07.2017, № 31 (Часть I), ст. 4791.

²²⁷ *Shrank, W. H., Rogstad, T. L., & Parekh, N. (2019). Waste in the US health care system: estimated costs and potential for savings. Jama, 322(15), pp. 1501-1509.*

5. Формирование в цифровом виде расписаний работы медицинского персонала.
6. Уменьшение трудозатрат врача за счет автоматизации использования форм и шаблонов»²²⁸.

Особенно важной среди перечисленных функций является функция по сбору и обработке информации, так как процессы сбора и обработки информации предполагают получение первичных данных о пациенте, которые уже впоследствии оцифровываются и сохраняются в базах данных. Особенностью медицинской информационной системы является переход от локальной работы с медицинской информацией к интегрированной системе, где все данные, проходящие через медицинскую организацию, доступны из единой информационной среды.

Кроме того, административная часть медицинской информационной системы отвечает за оказание поддержки руководству медицинской организации (например, управление человеческими ресурсами, управление государственными закупками, управление материалами и лекарствами, бухгалтерский учет, учет рабочего времени, выставление счетов за услуги, оказанные пациентам, и т. д.). С другой стороны, медицинская часть медицинской информационной системы обеспечивает поддержку при ведении учета лечения пациентов. Таким образом, использование современных медицинских информационных систем позволяет улучшить качество медицинских услуг, оптимизировать управление различными структурными медицинскими подразделениями и создать основу для достижения мирового уровня медицинского обслуживания. Медицинская информационная система воплощает сочетание программного и аппаратного обеспечения, баз данных и знаний, предназначенное для автоматизации различных процессов, происходящих в больницах и системе здравоохранения.

²²⁸ *Монаков Д. М., Алтунин Д. В.* Медицинские информационные системы: современные реалии и перспективы. Литературный обзор // Журнал телемедицины и электронного здравоохранения. 2022. Т. 8. №. 4. С. 46-53.

ЕГИСЗ представляет собой общегосударственную информационную платформу, разработанную для координации всех участников системы здравоохранения России: организаций, государственных органов и граждан. Её целью является обеспечение информационного взаимодействия в процессах оказания и получения медицинской помощи. ЕГИСЗ способствует оптимизации организационных процессов деятельности медицинских организаций.

В целом можно констатировать, что ЕГИСЗ соответствует положениям Глобальной стратегии по развитию цифрового здравоохранения на 2020–2025 годы, поскольку ЕГИСЗ предназначена для достижения следующих стратегических целей по укреплению управления электронным здравоохранением на национальном уровне:

- согласовать глобальные стандарты надлежащего использования данных о здоровье и сформулировать принципы справедливого обмена данными для целей исследований, анализа данных, первичного и вторичного использования данных;

- разработать руководство по новым областям, которые стали возможными благодаря информационным технологиям в здравоохранении, таким как электронные больницы, электронные терапевтические средства, персонализированная медицина²²⁹.

Функционирование ЕГИСЗ подразумевает информационное обеспечение государственного регулирования в сфере здравоохранения, в том числе эффективное взаимодействие медицинских организаций, а также информационную поддержку их деятельности, включая поддержку осуществления медицинской деятельности. С помощью ЕГИСЗ осуществляется развитие электронных медицинских карт, электронной регистратуры, электронных больничных и рецептов с федеральным порталом «Госуслуги», что обеспечивает реализацию права граждан на доступ к медицинским услугам в электронной форме. Между медицинскими организациями формируется система взаимодействия на

²²⁹ Global strategy on digital health 2020-2025. URL: <https://www.who.int/docs/default-source/documents/g4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf> (дата обращения: 28.01.2025)

основе электронного документооборота, которая позволяет обмениваться информацией без участия пациента.

Еще в 2014 году в одном исследовании важным достижением реализации ЕГИСЗ как приоритетного направления дальнейшей работы отметили именно электронную запись на прием к врачу, - и не только потому, что она облегчает получение услуг гражданам, но и потому, что она способствует оптимизации административных процессов в медицинских учреждениях²³⁰.

В 2024 году, как подчеркивают некоторые исследователи, в результате реализации ЕГИСЗ улучшилась система взаимодействия между медицинскими учреждениями, которые долгое время работали изолированно, развивается система телемедицинских консультаций²³¹. В настоящее время реализуется федеральный проект «Создание единого цифрового контура в здравоохранении на основе единой государственной информационной системы здравоохранения (ЕГИСЗ)» в рамках проекта «Здравоохранение», который определил основы электронного взаимодействия между медицинскими организациями, что является дальнейшим этапом для трансформации здравоохранения.

На основании полученных данных за 2022-2024 годы по использованию ЕГИСЗ можно отметить, что ЕГИСЗ обеспечивает повышение эффективности функционирования здравоохранения, трансформируя ее в условиях развития цифровизации на создание необходимых условий для широкого использования гражданами России электронных медицинских услуг и сервисов.

Так, в одном исследовании анализа результатов применения ЕГИСЗ отмечается, что в 2023 году по отношению к 2022 году количество лиц, воспользовавшихся медицинскими услугами на Госуслугах увеличилось на 33,3%,

²³⁰ Дьякова Е. Г. Переход к электронному правительству как процесс социальной адаптации технологии (на примере информатизации здравоохранения Свердловской области) // Антиномии. 2014. Т. 14. №. 4. С. 78-90.

²³¹ Вороньжева И. И., Федотова Г. В. Единый цифровой контур здравоохранения (ЕГИСЗ) // Актуальные тренды цифровой трансформации промышленных предприятий: сборник статей Всероссийской научно-практической конференции, Казань, 30–31 октября 2024 года. Курск: ЗАО «Университетская книга», 2024. С. 70-74.

а по отношению в 2024 году к 2023 году увеличилось на 18,75%²³². В 2023 году по отношению к 2022 году удельный вес ЕГИСЗ, гарантирующих доступность для граждан электронных медицинских документов в Личном кабинете пациента «Мое здоровье» на Госуслугах, возрос на 44,8%, по отношению в 2024 году к 2023 году увеличение составило 19,05%²³³.

На основании данных о росте числа пользователей электронных медицинских услуг можно сделать вывод о повышении доступности и востребованности сервисов ЕГИСЗ среди граждан, что является одним из индикаторов ее успешного внедрения в систему здравоохранения. Это означает, что граждане реализуют конституционные права на доступ к информации и на охрану здоровья и медицинскую помощь, что говорит о положительном воздействии ЕГИСЗ как информационной системы управления здравоохранением.

Тем не менее в использовании ЕГИСЗ существуют некоторые проблемы, которые рассматриваются в научной доктрине.

Считаем, что одной из актуальных проблем на данный момент является, проблема, поднимаемая В.В. Якуньковым: в случае, если медицинские данные пациента, содержащиеся в электронном документе в Федеральном реестре электронных медицинских документов, которая является одной из подсистем ЕГИСЗ, передаются в другие государственные информационные системы посредством взаимодействия, должен ли пациент – носитель персональных данных – давать свое согласие для передачи данной документации? Законодательством не предусмотрено получение такого согласия, так как в реальности сложно определить действительное согласие пациента передачу данных при обмене медицинской информации²³⁴.

²³² Коробкова О. К., Воронина Н. В. Промежуточные результаты Федерального проекта «Создание единого цифрового контура в здравоохранении на основе единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ)» // Международный научно-исследовательский журнал. 2024. №. 10 (148). С. 65.

²³³ Там же.

²³⁴ Якуньков В. В. Проблемы правового регулирования информационно-технологических систем в сфере охраны здоровья населения // Право и государство: теория и практика. 2024. №. 3 (231). С. 68-73.

Действительно, такая проблема в практике имеется, поскольку при обмене электронных данных пациента между информационными системами у пациента не запрашивается соответствующее разрешение. Чтобы решить данную проблему, можно обратиться за помощью к положениям Регламента ЕС по использованию и обмену электронными данными о здоровье, в котором заложен механизм использования данных «по желанию/отказу» в соответствии с Общим регламентом ЕС о защите данных. В этой системе, как мы ранее выяснили в разделе 3.1. параграфа 3 главы 1 исследования, для первичного использования данных используется подход «opt-in»: пациент может контролировать и, следовательно, явно выражать согласие/несогласие на использование своих данных²³⁵. Поэтому целесообразным представляется в отечественном законодательстве, а именно в главе VIII. «Порядок обмена информацией с использованием единой государственной информационной системе в сфере здравоохранения» постановления Правительства Российской Федерации от 9 февраля 2022 г. № 140 «О единой государственной информационной системе в сфере здравоохранения»²³⁶ отразить норму о выражении согласия/несогласия на использование своих данных при обмене между информационными системами.

Таким образом, на основе проведенного в этой части параграфа анализа отечественного правового регулирования применения технологий обработки первичных данных в сфере здравоохранения на примере ЕГИСЗ можно сделать следующий вывод.

ЕГИСЗ как информационная технология обработки первичных данных является медицинской информационной системой, которая непосредственно предназначена для управления сферой здравоохранения, в том числе принятия решений в ней и улучшения доступа пациентов к медицинскому обслуживанию.

²³⁵ Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space COM/2022/197 final. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0197> (дата обращения: 28.11.2024)

²³⁶ Постановление Правительства Российской Федерации от 9 февраля 2022 г. № 140 «О единой государственной информационной системе в сфере здравоохранения» // "Собрание законодательства РФ ", 21.02.2022, № 8, ст. 1152.

На основании полученных результатов по реализации ЕГИСЗ за время ее существования подтвердилось, что она обеспечивает повышение эффективности функционирования здравоохранения как информационной системы управления здравоохранением, трансформируя ее в условиях развития цифровизации на создание необходимых условий для широкого использования гражданами России электронных медицинских услуг и сервисов.

С одной стороны, система демонстрирует успех в повышении доступности и административной эффективности, о чем свидетельствует рост пользовательской активности. С другой стороны, она порождает новые вызовы в области защиты автономии пациента и его права на согласие при сквозном обмене данными, в целях разрешения которых предложено обратиться к опыту ЕС. Следовательно, дальнейшее развитие ЕГИСЗ требует не только технологического масштабирования, но и надлежащего правового регулирования, направленного на баланс между эффективностью управления и конституционными правами граждан.

2.2. Технологии анализа больших данных

В настоящее время в законодательстве Российской Федерации понятие «большие данные» (Big Data) содержится только в ГОСТ Р ИСО/МЭК 20546-2021 «Информационные технологии. Большие данные. Обзор и словарь», а также упоминается в Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы, утверждённой Указом Президента Российской Федерации от 9 мая 2017 г № 203, в пункте 15 которой утверждается, что в современном мире конкурентные преимущества будут иметь государства, экономика которых основана на технологиях анализа больших данных²³⁷.

При этом в научной доктрине отмечается, что проведенных исследований в данной области на сегодняшний момент недостаточно для формирования многостороннего подхода к урегулированию их правомерного использования в

²³⁷ Указ Президента Российской Федерации от 9 мая 2017 года № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» // «Собрание законодательства РФ», 15.05.2017, № 20, ст. 2901.

Российской Федерации²³⁸. Основное отличие технологий обработки первичных данных от анализа больших данных заключается в том, что в первом случае — это приведение необработанных данных в порядок, приведение к виду, пригодному для анализа. Анализ больших данных, в свою очередь, предполагает извлечение ценной информации из уже подготовленных данных с помощью сложных алгоритмов и мощных систем.

Большие данные в здравоохранении позволяют обрабатывать огромные массивы клинических, генетических и эпидемиологических данных для выявления факторов риска заболеваний, разработки индивидуальных схем лечения и профилактики, открытия новых биомаркеров и лекарств.

Электронные медицинские карты относятся к технологиям анализа больших данных²³⁹, которые относятся к информационным технологиям, что подтверждается научной доктриной²⁴⁰. Целесообразно рассмотреть из всех разновидностей технологий анализа больших данных именно электронные медицинские карты, поскольку они наиболее распространены и чаще применяются в сфере здравоохранения. К тому же в законодательстве России значительное внимание уделяется регулированию применения электронных медицинских карт.

Их активное внедрение в России находится в русле общемирового тренда цифровизации здравоохранения и подтверждается статистикой: если в 2019 году было зарегистрировано около 4 миллионов электронных медицинских документов, то к 2024 году этот показатель достиг 1,7 миллиарда²⁴¹. Подобный рост

²³⁸ Косоруков А.А., Кшеменецакая М.Н. Большие данные в практике управления современным государством // Тренды и управление. 2019. № 1. С. 90.

²³⁹ Ross, M. K., Wei, W., & Ohno-Machado, L. (2014). "Big data" and the electronic health record. *Yearbook of medical informatics*, 23(01), pp. 97-104; Умаров М. Ф., Мирзоджанова М. К. О возможности применения технологии больших данных в медицине и в системе здравоохранения // Информатизация и связь. 2025. № 1. С. 42-49; Кисель А. А., Нестеренков С. Н. Электронные медицинские карты как представитель big data в медицине // Редакционная коллегия. 2022. С. 378.

²⁴⁰ Лантев В. А. Искусственный интеллект в системе правовых инструментов стабилизации политических режимов мировых держав // Вестник Российского университета дружбы народов. Серия: Политология. 2023. Т. 25. №. 4. С. 831-847.

²⁴¹ В России фиксируют рекордный рост электронных медицинских документов. URL: <https://vmeste-rf.tv/news/v-rossii-fiksiryuyut-rekordnyy-rost-elektronnykh-meditsinskikh-dokumentov/> (дата обращения: 28.11.2024)

свидетельствует о том, что электронные медицинские карты становятся основным инструментом документооборота в отечественной системе здравоохранения. В настоящее время одной из актуальных задач развития здравоохранения в России является создание единого информационного пространства на основе разработки общей экосистемы электронного здравоохранения²⁴². Основным способом решения этой задачи является создание единой электронной медицинской карты для всех пациентов страны²⁴³. Как подчеркивает С.С. Собянин, электронные медицинские карты играют ключевую, системообразующую роль, аккумулируя весь массив данных о пациенте, и потом становятся доступным для врачей, которые оказывают медицинскую помощь конкретному человеку²⁴⁴.

В соответствии с приказом Минздрава России от 11 ноября 2013 года № 18-1/1010 «Основные разделы электронной медицинской карты» под электронной медицинской картой (ЭМК) понимается «совокупность электронных персональных медицинских записей, относящихся к одному пациенту, собираемых, хранящихся и используемых в рамках одной медицинской организации»²⁴⁵. «Электронная персональная медицинская запись (ЭПМЗ) - любая медицинская запись, сохраненная на электронном носителе (ГОСТ Р 52636-2006)»²⁴⁶.

По мнению ряда авторов, термин «ЭМК» «предполагает объединение всех ЭПМЗ о пациенте, имеющейся в медицинской организации, в электронную форму. При этом ЭПМЗ внутри ЭМК могут быть дополнительно объединены в группы, относящиеся, например, к конкретному законченному случаю заболевания (в

²⁴² *Лень Л.С., Никулина Т.Н.* Управление медицинским учреждением в современных условиях: проблемы и пути решения // Вестник АГТУ. Сер.: Экономика. 2016 г. № 2. С. 73-80.

²⁴³ *Оленева И.В.* Современное состояние проблемы внедрения электронных медицинских карт в единой государственной информационной системе // Медицинский алфавит. 2011 г. № 4 (20). С. 8-10.

²⁴⁴ *Собянин С. С., Ракова А.* Об электронной медицинской карте, о телемедицине, об искусственном интеллекте // Московская медицина. 2021. № 2(42). С. 26-29.

²⁴⁵ Приказ Минздрава России от 11 ноября 2013 года № 18-1/1010 «Основные разделы электронной медицинской карты». URL: <https://www.garant.ru/products/ipo/prime/doc/70425516/> (дата обращения: 28.11.2024)

²⁴⁶ Там же.

амбулаторной практике) или к конкретной госпитализации (при стационарном лечении)»²⁴⁷.

Определения федеральной интегрированной электронной медицинской карты (ИЭМК) не содержится в нормативных документах, поэтому приведем определение, данное группой ученых: ИЭМК - это «совокупность электронных персональных медицинских записей, относящихся к одному человеку, собираемых, передаваемых и используемых несколькими медицинскими организациями»²⁴⁸. В соответствии с пунктом 22 Приложения № 1 к Положению о единой государственной информационной системе в сфере здравоохранения, утвержденного постановлением Правительства Российской Федерации от 9 февраля 2022 года № 140 ИЭМК «собирает медицинскую документацию и (или) сведения о состоянии здоровья гражданина, предоставленные с согласия гражданина (его законного представителя) или размещенные гражданином (его законным представителем)»²⁴⁹.

Федеральная ИЭМК представляет собой «подсистему единой системы, предназначенную для сбора, систематизации и обработки структурированных обезличенных сведений о лицах, которым оказывается медицинская помощь, а также о лицах, в отношении которых проводятся медицинские экспертизы, медицинские осмотры и медицинские освидетельствования, посредством информационного обмена с государственными информационными системами в сфере здравоохранения»²⁵⁰. ИЭМК чаще всего используется для региональных

²⁴⁷ Гусев А. В., Зингерман Б. В., Тюфилин Д. С., Зинченко В. В. Электронные медицинские карты как источник данных реальной клинической практики // Реальная клиническая практика: данные и доказательства. 2022. Т. 2, № 2. С. 8-20.

²⁴⁸ Емелин И. В., Зингерман Б. В., Лебедев Г. С. Проблемы определения ключевых терминов медицинской информатики // Информационно-измерительные и управляющие системы. 2009. Т. 7. №. 12. С. 15-22.

²⁴⁹ Постановление Правительства Российской Федерации от 9 февраля 2022 года № 140 «О единой государственной информационной системе в сфере здравоохранения» // "Собрание законодательства РФ", 21.02.2022, № 8, ст. 1152.

²⁵⁰ Горovenko С. В., Бородин О. Л. Актуальные вопросы правового регулирования применения электронной медицинской карты пациента как элемента процедуры оказания телемедицинских услуг // Вестник Уральского финансово-юридического института. 2019. № 1(15). С. 14-16.

государственных информационных систем и федеральной информационной системы, она также может использоваться и для сетей клиник или ведомственных сетей, использующих различные медицинские информационные системы²⁵¹. Федеральная ИЭМК, в свою очередь, является государственным информационным ресурсом, что накладывает на оператора (государство) особые обязательства по обеспечению доступа, целостности и конфиденциальности данных.

Субъектом обязанности по предоставлению доступа к информации в рамках локальной ЭМК является медицинская организация, в которой эта карта ведется. За качество, полноту и своевременность внесения данных в нее несет ответственность главный врач. Субъектом обязанности по обеспечению доступа к данным в федеральной ИЭМК выступает оператор системы — Минздрав России, который должен гарантировать техническую доступность и бесперебойную работу портала «Госуслуги» и связанных с ним сервисов.

На ранних этапах цифровизации здравоохранения ЭМК не были так распространены. Создание коммерческого рынка медицинских информационных систем произошло в России на рубеже конца 1990-х — начала 2000-х гг., когда появлялись отдельные программы для диагностики и первые медицинские информационные системы, позволявшие вести некое подобие ЭМК²⁵². К середине 2000-х гг. в среде практического здравоохранения в целом сформировалось понимание, что информационные технологии действительно могут стать эффективным инструментом для развития медицины, но в то же время уровень их использования в медицинских организациях был невысок²⁵³. За несколько лет сфера здравоохранения сильно развилась, вслед за созданием проекта ЕГИСЗ в

²⁵¹ Зингерман, Б. В., Шкловский-Корди, Н. Е., Карп, В. П., Воробьев, А. И. Интегрированная электронная медицинская карта: задачи и проблемы // Врач и информационные технологии. 2015. №. 1. С. 24-34.

²⁵² Гусев А. В., Зингерман Б. В., Тюфилин Д. С., Зинченко В. В. Электронные медицинские карты как источник данных реальной клинической практики // Реальная клиническая практика: данные и доказательства. 2022. Т. 2, № 2. С. 8-20.

²⁵³ Фролов С. В. Маковеев С.Н., Семенова С.В., Фареев С.Г. Современные тенденции развития рынка медицинских информационных систем // Вестник Тамбовского государственного технического университета. 2010. Т. 16. №. 2. С. 266-272.

2011-2012 гг. логическим продолжением стал проект «Создание единого цифрового контура в сфере здравоохранения на основе Единой государственной информационной системы в сфере здравоохранения». Таким образом, внедрение и ведение ЭМК на практике невозможно без медицинских информационных систем, представляющих собой прикладное специализированное программное обеспечение, предназначенное для решения различных медицинских задач, в том числе и ведение ЭМК пациента.

Статистические данные фиксируют устойчивый рост числа медицинских организаций, внедривших медицинские информационные системы, в том числе и ведение ЭМК. В 2007 г. доля составляла 3,9 %, в 2009-м — 10,6 %, а в 2011 г. — 15 %²⁵⁴, то уже в 2012 г. она увеличилась до 36,4%, в 2021 г. составила 91 %²⁵⁵.

С 1 января 2024 г. произошел пересмотр законодательства в этой сфере. Основные предложения были нацелены на автоматическое создание ЭМК (бесплатно для всех граждан) при допустимости внесения отказа от нее. Активные действия пациента будут заключаться не в выражении согласия на создание, а в оформлении отказа от ЭМК²⁵⁶. Если человек захочет, чтобы медицинская организация продолжала вести бумажную карту, то понадобится написать соответствующее заявление²⁵⁷.

Электронные медицинские карты позволяют врачам быстро получать доступ к истории болезни пациента, результатам анализов и другой важной информации, что способствует более точной диагностике и назначению лечения. Граждане могут получать доступ к информации о лекарствах, медицинских учреждениях,

²⁵⁴ Гусев А. В. Медицинские информационные системы: состояние, уровень использования и тенденции // Врач и информационные технологии. 2011. № 3. С. 6-14.

²⁵⁵ Гусев А. В., Зингерман Б. В., Тюфиллин Д. С., Зинченко В. В. Электронные медицинские карты как источник данных реальной клинической практики // Реальная клиническая практика: данные и доказательства. 2022. Т. 2, № 2. С. 8-20.

²⁵⁶ Романовская О.В., Романовский Г.Б. Право и цифровизация современного здравоохранения // Вестник Российского университета дружбы народов. Серия: Юридические науки. 2024. Т. 28. №3. С. 565-583.

²⁵⁷ С 1 января 2024 года вступают в силу новые правила посещения поликлиник в РФ. URL: <https://ufafabry.ru/posts/s-1-ianvaria-2024-goda-vstupiat-v-silu-novye-pravila-poseshcheni> (дата обращения: 28.11.2024)

врачах, а также записываться на прием через Интернет, что упрощает процесс получения медицинской помощи. ЭМК предоставляет пациентам ряд преимуществ по сравнению с бумажными носителями, среди которых выделяются следующие:

1. Эффективность работы медицинского персонала (автоматизация процессов учета и отчетности упрощает работу административного персонала).

2. Улучшение качества медицинского обслуживания (сбор и анализ больших объемов данных из ЭМК для выявления трендов и улучшения общественного здоровья, и возможность создания индивидуальных планов лечения на основе анализа данных из ЭМК).

3. Упрощение администрирования (снижение бумажной работы и упрощение процессов администрирования в медицинских учреждениях. Использование ЭМК позволяет администрации распределять ресурсы и планировать нагрузку на медицинские учреждения).

4. Снижение затрат (переход на электронный формат позволяет сократить расходы на бумажные носители и физическое хранение документов).

Внедрение удаленного доступа к ЭМК обеспечивает более высокую оперативность и удобство доступа, который требует лишь наличия компьютера или иного устройства с доступом в Интернет, в том числе мобильного телефона, входа в систему и выбора интересующей информации. Данный механизм является важным инструментом реализации права на доступ к медицинской информации, которое является важной составляющей права на наивысший достижимый уровень здоровья.

Электронная медицинская документация каждый раз создается на основе данных, обрабатываемых в электронных базах данных, и служит инструментом, позволяющим пациенту осуществлять контроль за тем, какие данные и информация о нем хранятся, обрабатываются и становятся доступными. В результате пациент имеет право потребовать, чтобы данные о нем, полученные в процессе лечения, использовались только в том объеме, в котором он согласен с этим.

Некоторые авторы отмечают, что данные ЭМК представляют собой информацию о состоянии здоровья пациента, процессе его лечения и результатах лечения: демографических данных пациента, диагнозов, протоколов врачебных осмотров, лабораторных, инструментальных и патологоанатомических исследований, выполненных процедур и операций, записей о лекарственных назначениях и рекомендациях и т.д.²⁵⁸.

Перечисленные преимущества носят потенциальный характер и могут быть в полной мере реализованы лишь при условии создания правовой модели, гарантирующей не только технологическую возможность, но и полноценную реализацию прав пациента.

Считаем, что одной из актуальных проблем на данный момент в области правового регулирования применения ЭМК в российском законодательстве является проблема отсутствия у пациентов права ограничивать доступ к своей информации, хранящейся в ЭМК. Право пациента определять границы доступа к информации о своем здоровье в ЭМК дает ему возможность самостоятельно решать, хочет ли он, чтобы тот или иной медицинский работник мог видеть определенную информацию о нем. С одной стороны, человек сам имеет возможность контролировать доступ к своей ЭМК, то есть самостоятельно решает, разрешать ему знакомиться со своей историей болезни или нет. С другой стороны, пациент не всегда может понять, к какой информации необходимо получить доступ врачу, чтобы оказать квалифицированную помощь и поставить правильный диагноз, поскольку системы организма взаимосвязаны, полнота медицинской информации напрямую влияет на точность диагностики и эффективность лечения.

Указанная проблема отсутствия права пациента ограничивать доступ к своей информации рассматривалась в деле Европейского суда по правам человека «I против Финляндии» (I v. FINLAND) в 2008 году, которое касалось ВИЧ-инфицированной заявительницы. В этом деле заявительница жаловалась на то, что

²⁵⁸Кафтанов А. Н., Андрейченко А. Е., Гусев А. В. Обзор методических подходов к оценке качества ведения электронных медицинских карт // Врач и информационные технологии. 2024. № 3. С. 6-19.

региональные органы здравоохранения не обеспечили достаточной защиты для предотвращения несанкционированного доступа к медицинским данным.

Суд указал, что заявительница проиграла свой гражданский иск, поскольку не смогла доказать на деле причинно-следственную связь между недостатками в правилах безопасности доступа и распространением информации о состоянии ее здоровья. Однако возлагать такое бремя доказывания на заявительницу - значит упускать из виду очевидные недостатки в ведении документации в больнице на тот момент. Очевидно, что, если бы больница обеспечила больший контроль над доступом к медицинской документации, ограничив его медицинскими работниками, непосредственно участвующими в лечении заявителя, или ведя журнал учета всех лиц, имевших доступ к медицинской карте заявителя, заявительница оказалась бы в менее невыгодном положении в национальных судах. Для Суда решающим является тот факт, что существующая в больнице система учета явно не соответствовала правовым требованиям, содержащимся в национальном Законе о личных делах, и этот факт не был должным образом учтен национальными судами²⁵⁹. Иными словами, если бы заявительница могла ограничить доступ к своим данным о здоровье медицинских работников, то можно было бы избежать несанкционированного доступа к медицинским данным.

Как следствие проблемы возникает вопрос: каким образом можно ограничить доступ к ЭМК в одной организации, а предоставить доступ в другой, если у пациента заведена ЭМК в двух и более медицинских организациях? Также возникает вопрос синхронизации медицинских данных из разных медицинских учреждений.

На это в России направлена ИЭМК, поскольку она предполагает наличие интегрированного личного кабинета пациента, контролируемого им и предоставляющего ему открытый и полный доступ ко всему содержимому электронной медицинской карты в разных медицинских организациях. Согласимся

²⁵⁹ I v. FINLAND. URL: <https://hudoc.echr.coe.int/eng#%7B%22itemid%22%3A%5B%22001-87510%22%5D%7D> (дата обращения: 14.01.2025)

с мнением А. Е. Михеева, который подчеркнул следующее: «Пациенты должны быть заинтересованы не столько в наличии личного кабинета (а тем более, не столько в наличии нескольких личных кабинетов разных медицинских организаций), сколько в координации медицинской помощи, получаемой в разных местах, на это и направлена интегрированная электронная медицинская карта, которая объединяет все данные пациента из различных медицинских организаций»²⁶⁰.

Важно отметить, что ИЭМК недостаточно обширна, как этого хотелось бы. ИЭМК, действующая на базе Госуслуг в ЕГИСЗ, хотя и должна предоставлять полную медицинскую информацию пациентам и врачам, она является фактически расширением ЭМК, контролируемой не одним, а разными медицинскими организациями. Кроме того, попытки интеграции медицинских данных, предпринятые в рамках проектов ЕГИСЗ и ЕМИАС, недостаточно эффективны, а известная технология отправки документов в ЕГИСЗ далека от естественной²⁶¹.

Аналогичную проблему поднимают авторы и в отношении ИЭМК: «в отношении ИЭМК следует предусмотреть процедуру, позволяющую субъекту ограничить свой доступ к своей ИЭМК. В случае же, если пациент не воспользовался данной процедурой, то доступ к его ИЭМК не ограничивается для врачей в целях оказания этому пациенту медицинской помощи»²⁶². Права доступа к электронной медицинской карте должны быть четко регламентированы, чтобы обеспечить доступ и использование данных только уполномоченными лицами²⁶³.

Отсюда следует, что процедура ограничения доступа через ИЭМК медицинских данных одной медицинской организации и предоставление другой не

²⁶⁰ Михеев А. Е. Личный кабинет и расширение полномочий пациентов в цифровых экосистемах медицинской помощи // Менеджер здравоохранения. 2023. №. S1. С. 46-54.

²⁶¹ Михеев А. Е. Возможности, проблемы и перспективы информационных технологий в сфере клинической безопасности // Менеджер здравоохранения. 2023. №. S1. С. 5-20.

²⁶² Зингерман Б. В., Шкловский-Корди Н. Е., Карп В. П., Воробьев А. И. Интегрированная электронная медицинская карта: задачи и проблемы // Врач и информационные технологии. 2015. № 1. С. 24-34.

²⁶³ Mayer, A. H., C. A. da Costa, & R. D. R. Righi. (2020). Electronic Health Records in aBlockchain: A Systematic Review. Health Informatics Journal,26(2), pp. 1273-1288

представляется возможной на данный момент в силу отсутствия законодательного закрепления такой возможности.

Для решения этой проблемы целесообразно обратиться к законодательству зарубежных стран, которое было проанализировано в разделе 3.3. параграфа 3 главы 1 исследования.

Интересным в этой связи представляется законодательство Австрии по ЭМК (ELGA-Gesetz), которое позволяет пациентам видеть, кто ознакомился с информацией, содержащейся в их ЭМК, и решить вопрос о расширении или сокращении доступа, либо запретить доступ к определенной информации. Субъекты ЭМК (ELGA) могут предотвратить доступ конкретного медицинского учреждения к определенной части или всем своим данным своей ELGA. Так, согласно пункту 2 части 1 ст. 16 раздела 4 и части 3 ст. 21 раздела 4 Закона о телематике в здравоохранении 2012 года субъекты ELGA имеют право определять индивидуальные разрешения на доступ в соответствии с частью 3 ст. 21 путем:

а) показывания или сокрытия электронных ссылок и медицинских данных ELGA, включая данные о лекарствах, для поставщиков медицинских услуг ELGA и удалить их; если удаление исключено из-за обязательств по юридической документации или пункта 1 части 5 ст. 22, ссылки должны быть сделаны недоступными для ELGA, или

б) сокращения сроков действия существующих разрешений на доступ в соответствии с частью 6 ст. 18 или

с) назначения поставщика медицинских услуг ELGA, пользующегося особым доверием, в соответствии с частью 7 ст. 18. Поставщик медицинских услуг ELGA должен быть проинформирован об этом участником ELGA²⁶⁴.

Федеральный закон Швейцарии об электронной карте пациента (Gesetz über das elektronische Patientendossier) аналогично регулирует то, что каждый пациент

²⁶⁴ Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Gesundheitstelematikgesetz 2012. URL: <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20008120> (дата обращения: 28.11.2024)

может сам решать, кто может получить доступ к ЭМК. Данная норма закреплена в ст. 9 указанного Федерального закона Швейцарии:

1. Медицинские работники могут получать доступ к данным пациентов при условии, что пациенты предоставили им права доступа.

2. Федеральный совет определяет базовые настройки прав доступа и уровня конфиденциальности, применяемые после создания электронной карты пациента. Пациент может изменять эти настройки.

3. Пациент может назначить права доступа конкретным медицинским работникам или группам медицинских работников или вообще исключить отдельных медицинских работников из прав доступа.

4. Он может настроить уровни конфиденциальности отдельных данных.

5. В экстренных медицинских ситуациях медицинские работники также могут получить доступ к данным из электронной карты пациента без прав доступа, если пациент не исключил этого в рамках настройки основных параметров. Пациент должен быть проинформирован о таком доступе²⁶⁵.

Кроме того, часть 15 главы 4 Положения о порядке ведения медицинской документации в медицинских организациях КНР предусматривает ограничения права доступа к ЭМК в отношении третьих лиц, не относящихся к медицинскому персоналу. Ни одна организация или отдельное лицо не имеют права доступа к медицинской карте пациента, за исключением медицинского персонала, оказывающего медицинские услуги пациентам, органов здравоохранения и планирования семьи, органов традиционной китайской медицины или уполномоченных медицинских учреждений по управлению медицинской картой и персонала²⁶⁶.

²⁶⁵ Bundesgesetz über das elektronische Patientendossier. URL: <https://www.fedlex.admin.ch/eli/cc/2017/203/de> (дата обращения: 28.11.2024)

²⁶⁶ Regulation on medical records management in medical institutions. URL: https://english.www.gov.cn/policies/latest_releases/2014/08/23/content_281474983027052.htm (дата обращения: 28.11.2024)

Анализ законодательства стран СНГ показывает, что в некоторых из них уже урегулировано право пациента на ограничение доступа к данным ЭМК (Армения, Кыргызстан и Казахстан²⁶⁷).

Поэтому имеет смысл внести изменения и в законодательство России, предусмотрев норму, позволяющую пациенту ограничить доступ к своим медицинским данным в ЭМК определенному кругу лиц, в том числе и медицинским работникам на основании вышеуказанных положений ряда нормативных правовых актов зарубежных стран. Наиболее перспективными, на наш взгляд, являются подходы, обнаруженные в законах Австрии и Швейцарии, поскольку в них наиболее полно описан способ ограничения доступа к данным ЭМК пациента. Австрийская и швейцарские модели, в отличие от российской, предоставляют пациенту функцию управления доступом своей ЭМК, что соответствует принципу информационного самоопределения и снимает с законодателя необходимость детального описания всех возможных жизненных ситуаций. Это гибкое решение, которое может быть адаптировано для России в постановлении Правительства Российской Федерации от 9 февраля 2022 г. № 140 «О единой государственной информационной системе в сфере здравоохранения».

Таким образом, на основе проведенного в этой части параграфа исследования отечественного правового регулирования применения технологий анализа больших данных в сфере здравоохранения на примере ЭМК можно сделать следующий вывод.

Характерной чертой российского законодательства является отсутствие прямого закрепления права пациента на ограничение доступа к своей ЭМК.

В Австрии и Швейцарии пациенты имеют право контролировать, кто может получать доступ к их ЭМК. Это право включает возможность предоставлять доступ для конкретных медицинских работников и исключать его для других. Законодательство Китая предоставляет доступ к медицинским картам строго

²⁶⁷ Федотов Н.Е. Электронные медицинские карты и право на доступ к информации: зарубежный опыт и российские реалии // Юридический мир. 2025. №. 8 (343). С. 56-59.

только медицинским работникам и уполномоченным учреждениям, что подчеркивает важность конфиденциальности данных, исключая третьих лиц. В некоторых странах СНГ также предусмотрено на законодательном уровне право пациента на ограничение доступа к данным электронной медицинской карты.

В целях решения проблемы предлагается обратиться к зарубежному опыту и внести изменения в постановление Правительства Российской Федерации от 9 февраля 2022 г. № 140 «О единой государственной информационной системе в сфере здравоохранения», установив порядок права пациента на установление ограничения доступа к своей информации, содержащейся в ЭМК, в том числе ИЭМК третьих лиц, включая медицинских работников, подобно нормам, содержащимся в пункте 2 части 1 ст. 16 раздела 4 и части 3 ст. 21 раздела 4 Закона о телематике в здравоохранении 2012 года Австрии, а также в ст. 9 Федерального закона Швейцарии об электронной карте пациента.

2.3. Технологии Интернета вещей

Технологии Интернета вещей концептуально относятся в науке к числу информационных технологий²⁶⁸. В Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы, утвержденной Указом Президента РФ от 9 мая 2017 г. № 203, Интернет вещей также относится к основным направлениям развития российских информационных технологий (подпункт «е» пункта 36)²⁶⁹.

Особенностью технологий Интернета вещей является то, что к Интернету вещей возможно подключение всех информационных устройств с интеграцией в единую систему под общим высокоэффективным управлением. Благодаря этому возможности использования Интернета вещей в производстве и потреблении

²⁶⁸ *Popkova, E.G.* (2019). Ubiquitous Computing and the Internet of Things: Prerequisites for the Development of ICT (Vol. 826). Springer., P. 1235.

²⁶⁹ Указ Президента Российской Федерации от 9 мая 2017 г. № 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы" // «Собрание законодательства РФ», 15.05.2017, № 20, ст. 2901.

гораздо шире, чем у традиционного Интернета²⁷⁰. Поэтому в наименовании группы технологий присутствует слово «Интернет». В этой связи А. С. Купцова выделяет три основных критерия в отношении технологий Интернета вещей:

1) наличие большого количества устройств, подключённых к сети Интернет;

2) аккумулярование данных об окружающем пространстве (как персональных данных, так и иной информации) и обмен ими между соединёнными устройствами;

3) осуществление устройствами Интернета вещей функций автоматически (т.е. без участия человека), юридическое значение действий системы и способность иметь последствия для человека и общества в целом²⁷¹.

Для данной технологии характерны высокие темпы развития: по имеющимся прогнозам, глобальное количество подключенных к сети устройств достигнет 24 млрд единиц к 2030 году²⁷². При этом некоторые исследования, опубликованные в 2017 году, предполагали еще более стремительный рост — к 2025 г. количество устройств «Интернета вещей» составит около 75 млрд единиц²⁷³. Ожидается рост мирового рынка технологий Интернета вещей в здравоохранении «с 127,7 млрд долл. США в 2023 году до 289,2 млрд долл. США к 2028 году при среднегодовом темпе роста (CAGR) 17,8% в течение прогнозируемого периода»²⁷⁴. Причинами роста рынка данных технологий, среди прочего, как отметили Е. И. Аксенова и С. Ю. Горбатов, являются «развитие инфраструктуры здравоохранения, медицинских

²⁷⁰ *Иншакова А. О.* Право как основа инфраструктурного обеспечения цифровой экономики и технологии Интернета вещей // *Правовая парадигма.* 2019. Т. 18, № 3. С. 6-11.

²⁷¹ *Купцова А. С.* Правовое регулирование использования интернета вещей // *Образование и право.* 2021. №. 7. С. 225-230.

²⁷² *Global IoT Market Will Grow to 24.1 Billion Devices in 2030, Generating \$1.5 Trillion Annual Revenue* // PR Newswire. URL: <https://www.prnewswire.com/news-releases/global-iot-market-will-grow-to-24-1-billion-devicesin-2030--generating-1-5-trillion-annual-revenue-301061873.html> (дата обращения: 28.02.2025)

²⁷³ *Чайка В. К., Вустенко В. В., Морозова Н. А.* О рисках цифровизации здравоохранения // *Медико-социальные проблемы семьи.* 2022. Т. 27, № 4. С. 64-74.

²⁷⁴ *IoT in Healthcare Market by Component (Medical Device, Systems & Software, Services, and Connectivity Technology), Application (Telemedicine, Connected Imaging, and Inpatient Monitoring), End User and Region - Global Forecast to 2028.* URL: <https://www.marketsandmarkets.com/Market-Reports/iot-healthcare-market-160082804.html?gclid=CjwKCAjw> (дата обращения: 28.02.2025)

приборов и цифровая трансформация в сфере здравоохранения, а также необходимость контроля затрат в сфере здравоохранения, растущее внимание к уходу, ориентированному на пациента, развитие высокоскоростных сетевых коммуникационных технологий»²⁷⁵.

В России аналогично развиваются и внедряются в сферу здравоохранения различные устройства на базе технологий Интернета вещей.

По данным на 2024 год, объем российского рынка технологий Интернета вещей достиг 181 млрд. рублей. Согласно статистическим данным, в России к концу 2024-го насчитывается примерно 102,3 млн. всевозможных технологий Интернета вещей (по всем технологиям, но без учета носимых гаджетов вроде умных часов и фитнес-трекеров). Это на 19% больше по сравнению с предыдущим годом, когда показатель равнялся 85,8 млн. устройств²⁷⁶.

В 2020 году в Сколково в целях внедрения современных технологических решений для медицины начал работу «Центр инноваций и Интернета вещей в здравоохранении» по направлениям: хроническая сердечная недостаточность, онкогематология, рак молочной железы, рак яичников, рак предстательной железы. По результатам исследований в указанных направлениях выйдут на российский рынок здравоохранения различные информационные технологии²⁷⁷.

Согласно пункту 4 Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы, утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203, под Интернетом вещей понимается «концепция вычислительной сети, соединяющей вещи (физические предметы),

²⁷⁵ Аксенова Е. И., Горбатов С. Ю. Применение технологий Интернета вещей в здравоохранении // Здоровье мегаполиса. 2021. Т. 2, № 4. С. 101-113.

²⁷⁶ Интернет вещей, IoT, M2M рынок России. URL: [\(дата обращения: 29.02.2025\).](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9,_IoT_(%D1%80%D1%8B%D0%BD%D0%BE%D0%BA_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8))

²⁷⁷ В Центре инноваций и Интернета вещей в здравоохранении в «Сколково» открылись пять новых терапевтических зон. URL: <https://sk.ru/news/v-centre-innovaciy-i-interneta-veschey-v-zdravoohranenii-v-skolkovo-otkrylis-pyat-novyh-terapevticheskikh-zon/> (дата обращения: 28.02.2025)

оснащенные встроенными информационными технологиями для взаимодействия друг с другом или с внешней средой без участия человека»²⁷⁸.

На основании приведенного нормативного определения представляется возможным сформулировать авторское определение технологий Интернета вещей применительно к сфере здравоохранения на основе следующей информации.

Интеллектуальные и электронные медицинские устройства относятся к технологиям Интернета вещей в здравоохранении, с помощью которых возможно собирать данные, контролировать и улучшать состояние здоровья пациентов в режиме реального времени, обеспечивая при этом экономическую эффективность. В рамках технологий Интернета вещей в исследовании рассматриваются мобильные переносимые приборы, «умные» медицинские устройства и мобильные приложения, которые, в свою очередь, образуют понятие m-Health, подразумевающее под собой медицинское обслуживание с использованием мобильных устройств и беспроводных технологий передачи данных²⁷⁹. В научной литературе преобладает точка зрения, согласно которой мобильное здравоохранение (m-Health) является важной составляющей «интернета медицинских вещей»²⁸⁰.

Выделяют несколько видов технологий Интернета вещей в здравоохранении, например²⁸¹:

²⁷⁸ Указ Президента Российской Федерации от 9 мая 2017 г. № 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы" // «Собрание законодательства РФ», 15.05.2017, № 20, ст. 2901.

²⁷⁹ *Сорокин Д.А., Гречушкина Н.В.* Цифровые технологии в медицине // Актуальные проблемы физики и технологии в образовании, науке и производстве: материалы IV Всероссийской научно-практической конференции, посвященной 120-летию Александра Васильевича Пёрышкина. Рязань, 2022. С. 173-175; *Цветкова Л. А., Кузнецов П. П., Куракова Н. Г.* Оценка перспектив развития мобильной медицины-mHealth на основании данных наукометрического и патентного анализа // *Врач и информационные технологии.* 2014. №. 4. С. 66-77.

²⁸⁰ *Цветкова Л. А., Кузнецов П. П., Куракова Н. Г.* Оценка перспектив развития мобильной медицины-mHealth на основании данных наукометрического и патентного анализа // *Врач и информационные технологии.* 2014. №. 4. С. 66-77.

²⁸¹ *Лебедев, Г. С., Шадркин, И. А., Фомина, И. В., Лисненко, А. А., Рябков, И. В., Качковский, С. В., Мелаев, Д. В.* Интернет медицинских вещей: первые шаги по систематизации // *Журнал телемедицины и электронного здравоохранения.* 2017. №. 3 (5). С. 128-136.

1) Носимые устройства, которые предназначены для ношения на теле и включают в себя такие популярные технологии, как умные часы, фитнес-трекеры и умную одежду. Эти устройства способны отслеживать различные аспекты здоровья человека, такие как частота сердечных сокращений, артериальное давление, режим сна и физическая активность. Благодаря возможности связи с поставщиками медицинских услуг носимые устройства позволяют осуществлять мониторинг здоровья пациента в режиме реального времени.

2) Умные медицинские приборы (имплантируемые). Медицинские устройства на базе технологий Интернета вещей, известные как интеллектуальные медицинские устройства, созданы с определенной целью - для оказания медицинской поддержки. Они позволяют обеспечивать мониторинг здоровья пациентов в режиме реального времени. Медицинские устройства, оснащенные интеллектуальными технологиями, производят огромные объемы данных, которые могут улучшить лечение пациентов и продвинуть медицинские инновации. Использование этих интеллектуальных медицинских устройств может минимизировать расходы на здравоохранение за счет снижения частоты госпитализаций, поездок в отделение неотложной помощи и консультаций врачей. Многочисленные исследования, представленные в научной литературе, подтверждают эффективность носимых устройств для мониторинга состояния здоровья в реальном времени²⁸².

3) Приложения категории mHealth, доступные в Google Play или Apple app store, разнообразны и располагают широким функционалом²⁸³. Мобильные приложения отображают связь мобильных вычислений, датчиков,

²⁸² Kraft, D., Srinivasan, K., & Bieber, G. (2020). Deep learning based fall detection algorithms for embedded systems, smartwatches, and IoT devices using accelerometers. *Technologies*, 8(4), P. 72; Mendonça, M., Jerónimo, T., Julião, M., Santos, J., Pombo, N., & Silva, B. M. (2020). An IoT-based healthcare ecosystem for home intelligent assistant services in smart homes. In *IoT Technologies for HealthCare: 6th EAI International Conference, HealthyIoT, Braga, Portugal, Proceedings 6*. pp. 142-155.

²⁸³ Ozdalga, E., Ozdalga, A., & Ahuja, N. (2012). The smartphone in medicine: a review of current and potential use among physicians and students. *Journal of medical Internet research*, 14(5), P.1994.

коммуникационных технологий и облачных вычислений для отслеживания информации о состоянии здоровья пациента и других физиологических состояниях. К настоящему времени опубликовано несколько крупных исследований о применении мобильных вычислений в здравоохранении²⁸⁴.

Таким образом, под технологией Интернета вещей в здравоохранении мы понимаем концепцию вычислительной сети, объединяющую любое устройство, мобильное приложение, которое может собирать данные о состоянии здоровья людей и окружающей его среды.

Возможность подключения медицинских устройств и приложений к информационным системам здравоохранения посредством сетевых технологий создает условие для удаленного доступа пациентов к медицинским услугам. С развитием технологии Интернета вещей они стали более доступными и экономически эффективными, что привело к новой эре медицинских услуг.

Нельзя не отметить, что внедрение технологий Интернета вещей в повседневную жизнь приводит к возникновению различных правовых проблем. Так, А.А. Баранов отмечает, что технологии Интернета вещей потребуют проведения дополнительных широких правовых исследований общественных отношений, как минимум связанных с обеспечением приватности (защиты персональных данных), безопасности, в частности кибербезопасности, регулированием использования частотного спектра и предоставлением телекоммуникационных услуг, определением принципов стандартизации устройств, технологий и систем, защитой интеллектуальной собственности и авторского права, определением ответственности и тому подобных, уже известных направлений правового регулирования²⁸⁵. Другой исследователь Я. Браун

²⁸⁴ *Nazir, S., Ali, Y., Ullah, N., & García-Magariño, I. (2019). Internet of things for healthcare using effects of mobile computing: a systematic literature review. Wireless Communications and Mobile Computing, 2019(1), pp. 593-1315; Mora, H., Gil, D., Terol, R. M., Azorín, J., & Szymanski, J. (2017). An IoT-based computational framework for healthcare monitoring in mobile environments. Sensors, 17(10), P. 2302.*

²⁸⁵ *Баранов А. А. Интернет вещей: теоретико-методологические основы правового регулирования. Т.1: Сферы применения, риски и барьеры, проблемы правового регулирования:*

подчеркнул, что актуальными вопросами являются правовые последствия применения Интернета вещей для таких областей, как лицензирование, стандартизация, безопасность и конфиденциальность²⁸⁶.

В Российской Федерации ключевым правовым пробелом остается отсутствие комплексного механизма правового регулирования технологий Интернета вещей в здравоохранении.

Согласимся с позицией о том, что особое внимание должно быть уделено созданию отдельного классификатора (класса приборов) и требований к медицинской регистрации изделий, разработанных в рамках технологий Интернета вещей²⁸⁷. Аналогичного мнения придерживаются Ю.В. Забайкин и Д.А. Лунькин: «необходимо установить правила регистрации и лицензирования устройств технологий Интернета вещей, а также определить механизмы контроля и мониторинга их использования. Такие правила помогут обеспечить эффективную и безопасную эксплуатацию технологий Интернета вещей и защитить интересы пользователей и общества в целом»²⁸⁸.

Необходимо подчеркнуть, что обозначенная проблема сохраняет свою актуальность, поскольку исследователи подчеркивают, что такие устройства, как фитнес-браслеты, смарт-часы и иные носимые устройства фиксации данных о состоянии согласно классификации Росздравнадзора Российской Федерации, не являются медицинскими изделиями²⁸⁹. Стоит согласиться с мнением ряда авторов, что вышеуказанные фитнес-трекеры, смарт-часы, портативные приборы

монография / О.А. Баранов; НИИ ИП НАПрН Украины – К.: Издательский дом «АртЕк». 2018. 344 с.

²⁸⁶ *Brown I.* (2015). Regulation and the Internet of Things. GSR Discussion Paper, 15th Global Symposium for. Regulators. pp. 1-34.

²⁸⁷ *Лебедев Г. С., Шадркин И. А., Фомина И. В., Лисненко А. А., Рябков И. В., Качковский С. В., Мелаев Д. В.* Интернет медицинских вещей: первые шаги по систематизации // Журнал телемедицины и электронного здравоохранения. 2017. №. 3 (5). С. 128-136.

²⁸⁸ *Забайкин Ю. В., Лунькин Д. А.* Направления развития права в сфере Интернета вещей // Вопросы российского и международного права. 2023. Т. 13, № 1-2-1. С. 208-214.

²⁸⁹ *Ильяшенко О. Ю. Карантан, Д. Н., Лукьянченко Е. Л.* Архитектура платформенных решений медицинской организации на основе технологии "Интернет вещей": практики, проблемы, инструменты // Вестник Димитровградского инженерно-технологического института. 2021. № 3(25). С. 24-35.

потенциально могут использоваться для принятия клинических решений - постановки диагноза, назначения и изменения диагностических и лечебных процедур, в связи с этим должны иметь статус «медицинских изделий» и потому подлежать регистрации²⁹⁰. Регулирование данных технологий сопряжено с рядом трудностей, обусловленных неоднородностью технологий (например, перевязочные материалы, медицинские устройства визуализации, приложения mHealth), медицинскими целями (например, диагностика, уход, профилактика) и связанными с ними рисками (например, биосовместимость материалов, проблемы безопасности данных). Но тем не менее решить проблему все равно необходимо в целях соблюдения прав и интересов граждан-пользователей технологии Интернет вещей в здравоохранении.

Когда медицинские приложения и иные устройства на базе технологий Интернета вещей не регулируются, то отсутствует реальный надзор за их политикой конфиденциальности и имеется очень мало контроля над тем, как они используют собранные данные. Такая ситуация создает опасения по поводу безопасности пациентов и использования личной медицинской информации, поскольку многие из медицинских приложений на базе технологий Интернета вещей не являются медицинскими изделиями. В этой связи актуализируется необходимость появления в России более четкого правового регулирования применения указанных технологий.

Для решения вышеуказанной проблемы можно обратиться к практике регулирования регистрации технологий Интернета вещей в здравоохранении в странах ЕС и в США.

Управление по санитарному надзору за качеством пищевых продуктов и медикаментов США, как ранее мы выяснили в разделе 3.3. параграфа 3 главы 1 исследования, будет регулировать приложения только в том случае, если они функционируют как медицинские устройства (определены как «мобильные

²⁹⁰ Лебедев, Г. С., Шадеркин, И. А., Фомина, И. В., Лисненко, А. А., Рябков, И. В., Качковский, С. В., Мелаев, Д. В. Эволюция интернеттехнологий в системе здравоохранения //Журнал телемедицины и электронного здравоохранения. 2017. №. 2 (4). С. 63-78.

медицинские приложения»), т. е. соответствуют определению устройства и используются в качестве аксессуара к регулируемому медицинскому устройству, либо превращают мобильную платформу в регулируемое медицинское устройство и могут представлять риск для безопасности пациента, если они не функционируют так, как задумано²⁹¹.

Среди европейских стран выделяются Франция с «Руководством по надлежащей практике в отношении приложений для здравоохранения и интеллектуальных устройств (мобильное здравоохранение или mHealth)» для производителей, а также список надлежащей практики для субъектов здравоохранения²⁹² и Великобритания со своим руководящим документом, позволяющим производителям приложений определять, подлежат ли их приложения регулированию как медицинские устройства, что предоставляет производителям большую ясность в назначении своих устройств²⁹³.

Для разработки национальных руководящих принципов в области правового регулирования технологий Интернета вещей в здравоохранении в России необходимо обратить внимание на нормативные решения вышеуказанных европейских стран, так как подход Франции позволяет урегулировать те приложения и устройства, которые относятся к технологиям Интернета вещей, и никак не могут подпадать под медицинские изделия, что выглядит интересно.

Подход Великобритании позволил бы в России определить, подлежат ли российские медицинские приложения, регулированию как медицинские устройства в соответствии с постановлением Правительства Российской Федерации от 30 ноября 2024 г. № 1684 «Об утверждении Правил государственной регистрации медицинских изделий».

²⁹¹ FDASIA Health IT Report. Proposed Strategy and Recommendations for a Risk-Based Framework. URL: https://www.healthit.gov/sites/default/files/fdasia_healthitreport_final.pdf (дата обращения: 28.11.2024)

²⁹² Good practice guidelines on health apps and smart devices (mobile health or mhealth). URL: https://www.has-sante.fr/jcms/c_2681915/en/good-practice-guidelines-on-health-apps-and-smart-devices-mobile-health-or-mhealth (дата обращения: 28.02.2025)

²⁹³ Guidance: Medical device stand-alone software including apps. URL: <https://www.fda.gov/media/113802/download> (дата обращения: 28.02.2025)

В отличие от них подход США по разработке программы предварительной сертификации более рыночный, что отмечается в содержании Плана инноваций FDA в области цифрового здравоохранения для оптимизации предварительного одобрения рынка и разработки более интенсивного пострыночного надзора с целью разработки специального, всеобъемлющего подхода к регулированию mHealth. FDA по этому поводу заявило, что эта политика была разработана для того, чтобы позволить полезным технологиям с меньшим риском стать доступными для американцев, гарантируя при этом, что подключенные продукты будут оставаться высококачественными, безопасными и эффективными²⁹⁴.

Таким образом, в целях решения обозначенной проблемы предлагается разработать аналогичные рекомендации в России, которые бы могли установить критерии проверки устройств, медицинских приложений, разработанных на основе технологий Интернета вещей, на наличие медицинского контента и направленность на оказание медицинской помощи, в том числе и принятие клинических медицинских решений.

Внедрение данной системы критериев позволит создать прозрачный и предсказуемый правовой режим для разработчиков и производителей, обеспечит адекватный уровень контроля за оборотом устройств, используемых в медицинских целях, и защитит права пациентов за счет исключения из клинической практики непроверенных и потенциально опасных решений.

Критериями, например, будет определено, что в зависимости от предполагаемого назначения устройство может быть классифицировано как устройство медицинского назначения, если оно: предотвращает, диагностирует, контролирует, лечит или облегчает заболевание; исследует или изменяет физиологические процессы человека; контролирует зачатие и др.

Разработка подобных рекомендаций, безусловно, является первым необходимым шагом. Однако ее практическая реализация потребует решения ряда

²⁹⁴ Digital health innovation action plan. URL: <https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/UCM568735.pdf> (дата обращения: 28.02.2025)

сопутствующих задач, например, наделения конкретного органа власти полномочиями по надзору за соблюдением соответствия выпускаемых устройств критериям и выстраивания прозрачной процедуры для производителей, которая не станет избыточным административным барьером.

Также важным аспектом правового регулирования использования технологий Интернета вещей в России является вопрос их безопасности, защиты конфиденциальной информации и персональных данных, который не раз поднимался в научной доктрине.

Так, Ж. Ф. Мухитдинов отмечал, что атаки на технологии Интернета вещей могут иметь серьезные последствия, «от нарушения работы критической инфраструктуры до компрометации личных данных миллионов пользователей»²⁹⁵.

Согласимся с мнением А.А. Громовой, отметившей, что использование трекеров для здоровья потенциально может создать угрозу национальной безопасности страны и требует более детального регулирования, а также создания особых протоколов защиты таких данных²⁹⁶.

Решение этой проблемы и обеспечение безопасности в области технологий Интернета вещей должно быть основным приоритетом. Пользователи должны быть уверены в том, что устройства из числа технологий Интернета вещей и связанные с ними услуги в области данных не имеют уязвимых мест, особенно по мере распространения этой технологии и ее внедрения в повседневную жизнь. В случае если пользователь не будет обладать информацией о том, что устройства на основе технологий Интернета вещей были проверены и подтвердили свою безопасность, а также о том, как они работают и собирают данные, то, по мнению К. Роуз, С. Элдриджа и Л. Чапина, это создает «уязвимость в области безопасности, когда пользователь считает, что устройство выполняет определенные функции, в

²⁹⁵ Мухитдинов Ж. Ф. Правовое регулирование Интернет вещей // International Multidisciplinary Research in Academic Science (IMRAS). 2024. №. 7 (9). С. 1-10.

²⁹⁶ Громова А.А. Реализация конституционного права на охрану здоровья и медицинскую помощь в условиях применения биомедицинских технологий в Российской Федерации : Дис. ... канд. юрид. наук : 5.1.2/ Громова Арина Алексеевна - Москва, 2025, 233 с.

то время как на самом деле оно может выполнять нежелательные действия или собирать данные, которые пользователь не намерен предоставлять»²⁹⁷.

В России отсутствуют нормы в сфере информационной безопасности технологий Интернета вещей, поскольку положения Федерального закона 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», устанавливающего нормы о безопасности критической информационной структуры²⁹⁸, и Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», устанавливающего общие принципы информационной безопасности²⁹⁹, не распространяются на технологии Интернета вещей. К такому же выводу приходят разработчики отрывной концепции «Интернет-вещей: правовые аспекты (Российская Федерация)», установившие, что нормы российского законодательства в сфере информационной безопасности не в полной мере содержат системные решения, необходимые в условиях ожидаемого повсеместного распространения технологий Интернета вещей, и выражают сомнения в том, что российское законодательство может в полной мере отвечать особенностям и предназначению технологий Интернета вещей, а также учитывать специфику угроз информационной безопасности программного обеспечения технологий Интернета вещей³⁰⁰.

Поэтому для решения данной проблемы следует обратиться к законодательству США и с использованием ранее рассмотренных в разделе 3.2. параграфа 3 главы 1 исследования положений Закона США об улучшении кибербезопасности технологий Интернета вещей и исполнительного Указа о

²⁹⁷ Роуз К., Эдридж С., Чатин Л. Интернет вещей: краткий обзор // Вопросы и проблемы использования сети Интернет в более глобальном масштабе. ICOS. 2015. С. 1-75

²⁹⁸ Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // «Собрание законодательства РФ», 31.07.2006, № 31 (1 ч.), ст. 3448

²⁹⁹ Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // «Собрание законодательства РФ», 31.07.2017, № 31 (Часть I), ст. 4736.

³⁰⁰ Открытая концепция «Интернет-вещей: правовые аспекты (Российская Федерация)». URL: <https://www.ifar.ru/pr/2016/160712aa.pdf> (дата обращения: 28.10.2025)

повышении уровня кибербезопасности страны принять в России Руководство по информационной безопасности технологий Интернета вещей. В нем необходимо установить процедуру наложения санкций в отношении производителей, которые выпустили изделия, принадлежащие к технологиям Интернета вещей, признанные не соответствующими мерам информационной безопасности, а также требования к информационной безопасности, в рамках которых производители устройств из числа технологий Интернета вещей должны разрабатывать устройства на критериях информационной безопасности и уточнять, какую информацию оно собирает, а также предпринимать все усилия, чтобы защитить устройство от любых несанкционированных попыток получить доступ или изменить информацию, содержащуюся в нем. При этом стоит разработать и правила маркировки устройств из числа технологий Интернета вещей, чтобы информировать потребителей о функциях безопасности этих устройств.

Таким образом, на основе проведенного в этой части параграфа анализа отечественного правового регулирования применения технологий Интернета вещей в сфере здравоохранения можно сделать следующие выводы.

1. В настоящее время проблема отсутствия отдельного классификатора (класса приборов) и требований к медицинской регистрации изделий, разработанных в рамках технологий Интернета вещей, остается актуальной в России.

Проанализированный ранее зарубежный опыт позволяет систематизировать модели регулирования по ключевому критерию - соотношению предварительного и последующего контроля. На одном полюсе находится либеральная, риск-ориентированная модель США, делающая ставку на предварительную сертификацию добросовестного производителя и последующий пост-маркетинговый надзор. На другом - Великобритания и Франция, фокусирующиеся на создании гибких руководств, которые помогают самому производителю квалифицировать свой продукт и определить применимый регуляторный режим.

Предпочтительный выбор опыта Франции и Великобритании (несмотря на ее общее право) для решения проблемы обусловлен тем, что они по части регулирования применения технологий Интернета вещей делают упор на четкие, структурированные нормативные правовые акты, что близко российской правовой системе с ее акцентом на систематизированные нормативные правовые акты. Это соответствует задаче формирования предсказуемой правовой среды, декларируемой в качестве одной из целей современной правовой политики Российской Федерации.

2. В России актуальной также остается проблема безопасности, защиты конфиденциальной информации и персональных данных в отношении технологий Интернета вещей. Для ее решения предложено обратиться к Закону США об улучшении кибербезопасности технологий Интернета вещей от 2020 года и исполнительного Указа о повышении уровня кибербезопасности страны. Целесообразность использования указанных нормативных правовых актов состоит в том, что именно в них наиболее подробно описаны стандарты и рекомендации по надлежащему пользованию и управлению устройствами из числа технологий Интернета вещей, включая минимальные требования к информационной безопасности для управления рисками, связанными с такими устройствами, а также положения о программе маркировки устройств из числа технологий Интернета вещей в целях информирования потребителей о функциях безопасности устройств по сравнению с иными существующими в этой области документами.

2.4. Технологии искусственного интеллекта

Технологии искусственного интеллекта (ИИ) открывают большие перспективы в здравоохранении.

Согласно подпункту «а» пункта 5 Национальной стратегии развития искусственного интеллекта на период до 2030 года, утвержденной Указом Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» под ИИ понимается

«комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их»³⁰¹. Первым нормативным актом, давшим официальное определение ИИ, стала обозначенная выше Национальная стратегия развития искусственного интеллекта на период до 2030 года, а вторым - Федеральный закон от 24 апреля 2020 г. № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации - городе федерального значения Москве и внесении изменений в ст. 6 и 10 Федерального закона «О персональных данных» от 24.04.2020 № 123-ФЗ».

Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений. Под машинным обучением понимается процесс машинного анализа подготовленных статистических данных для поиска закономерностей и создания на их основе нужных алгоритмов (настройки параметров нейронной сети), которые затем будут использоваться для прогнозов³⁰². Машинное обучение использует данные и алгоритмы для имитации того, как учатся люди, постепенно повышая точность³⁰³.

Несмотря на нормативное закрепление, вышеуказанное определение ИИ, по мнению некоторых авторов, не является общепринятым. В.В. Архипов, А.В. Грачева, В.Б. Наумов, Т.А. Полякова и А.В. Минбалеев, критикуя подход

³⁰¹ Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» // "Собрание законодательства РФ", 14.10.2019, № 41, ст. 5700.

³⁰² Гусев А. В., Добридюк С. Л. Искусственный интеллект в медицине и здравоохранении // Информационное общество. 2017. № 4-5. С. 78-93.

³⁰³ Левченко О. Н. Системы искусственного интеллекта в здравоохранении: текущее состояние, проблемы и перспективы // ЭФО: Экономика. Финансы. Общество. 2023. № 4(8). С. 52-71.

законодателя к определению ИИ, предлагают раскрывать его как информационную систему, обеспечивающую функцию формирования алгоритмов решения задач, отличных от заложенных разработчиками системы, в том числе с помощью нейронной сети³⁰⁴.

И.Р. Бегишева и З.И. Хисамова, оценивая ситуацию с подходами к определению ИИ в 2020 году, отмечали, что на сегодняшний день нет единообразного толкования рассматриваемых дефиниций, притом что «вариантов определения данного понятия в науке более дюжины»³⁰⁵.

По мнению А.И. Медведева, понимание ИИ в юридической науке по-прежнему остается неоднородным, и в таких условиях словосочетание «искусственный интеллект» в настоящий момент предстает скорее как «зонтичный» термин, включающий в себя разные подходы к его пониманию (технология, информационная система и т.д.), нежели как категория, имеющая четкое и лаконичное определение, что никак не идет на пользу развитию единого законодательства о робототехнике и ИИ³⁰⁶.

Можно предположить, что трудность установления стандартного и общепринятого определения ИИ связана с его динамической природой. Подход к этой технологии постоянно развивается, как и различные условия, в которых она может применяться для создания ценности. В некоторой степени было бы нежелательно давать жесткое определение ИИ, поскольку эта неопределенность является одним из факторов, способствующих его росту и быстрому развитию. Поэтому мы будем исходить из определения, которое установил законодатель.

³⁰⁴ *Архипов В.В., Грачева А.В., Наумов В.Б., Полякова Т.А., Минбалеев А.В.* Определение искусственного интеллекта в контексте российской правовой системы: критический подход // Государство и право. 2022. № 1. С. 168–178.

³⁰⁵ *Бегишев И.Р., Хисамова З.И.* Искусственный интеллект и робототехника: теоретико-правовые проблемы разграничения понятийного аппарата // Вестник Удмуртского университета. Серия Экономика и право. 2020. Т. 30. № 5. С. 706–713.

³⁰⁶ *Медведев А.И.* Когда машинная логика неочевидна: проблема прозрачности искусственного интеллекта с точки зрения права // Информационное право. 2023. № 1(75). С. 9–13.

В сфере здравоохранения государственная политика в сфере внедрения и применения ИИ установлена в положениях Указа Президента Российской Федерации от 7 мая 2024 г. № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года», согласно которым к 2030 году предполагается достигнуть «цифровой зрелости» отрасли здравоохранения, предполагающей автоматизацию большей части транзакций в рамках единых отраслевых цифровых платформ и модели управления на основе данных с учетом ускоренного внедрения технологий обработки больших объемов данных, машинного обучения и искусственного интеллекта³⁰⁷.

В Стратегии развития здравоохранения в Российской Федерации на период до 2030 года, утвержденной Указом Президента Российской Федерации от 8 декабря 2025 г. № 896, подчеркивается, что основной задачей развития здравоохранения в Российской Федерации является разработка информационных систем в сфере здравоохранения с поддержкой принятия врачебных решений с использованием технологий искусственного интеллекта³⁰⁸. Применение ИИ в здравоохранении можно разделить на виртуальную и физическую ветви. К виртуальной части относятся поддержка принятия медицинских решений, рекомендации на основе работы нейронных сетей. Физическая часть включает в себя роботов, используемых в медицинских целях³⁰⁹.

Согласно прогнозам, мировой рынок ИИ в сфере здравоохранения вырастет с 20,9 млрд долл. в 2024 г. до 148,4 млрд долл. к 2029 г.; ожидается, что в 2024-2029 гг. рост составит в среднем на 48,1% в год³¹⁰.

³⁰⁷ Указ Президента Российской Федерации от 7 мая 2024 г. № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» // «Собрание законодательства РФ», 13.05.2024, № 20, ст. 2584.

³⁰⁸ Указ Президента Российской Федерации от 8 декабря 2025 г. № 896 «О Стратегии развития здравоохранения в Российской Федерации на период до 2030 года». URL: <http://publication.pravo.gov.ru/document/0001202512090003> (дата обращения: 12.12.2025).

³⁰⁹ Malik, P., Pathania, M., & Rathaur, V. K. (2019). Overview of artificial intelligence in medicine. *Journal of family medicine and primary care*, 8(7), pp. 2328-2331.

³¹⁰ Artificial Intelligence (AI) in Healthcare Market worth \$148.4 billion by 2029 - Exclusive Report by MarketsandMarkets. URL: <https://www.prnewswire.com/news-releases/artificial-intelligence-ai-in-healthcare-market-worth-148-4-billion-by-2029---exclusive-report-by-marketsandmarkets-302052956.html> (дата обращения: 28.02.2025)

Также быстро растет рынок ИИ в российском здравоохранении. По данным Национального центра развития искусственного интеллекта при Правительстве Российской Федерации, около 37% организаций в сфере здравоохранения внедряют решения с ИИ. Еще порядка 43% планируют это сделать в ближайшее время³¹¹. Министерство экономического развития утвердило дорожную карту развития ИИ на период до 2030 г³¹². Предусмотрено бюджетное финансирование в размере 24,1 млрд руб., а также 5,1 млрд руб. из внебюджетных источников³¹³.

Алгоритмы ИИ демонстрируют высокую эффективность в решении задач раннего обнаружения и диагностики заболеваний. Например, модели глубокого обучения ИИ (подмножество машинного обучения, в котором искусственные нейронные сети обучаются или изучаются на больших наборах данных) были обучены на больших наборах данных медицинских изображений для выявления закономерностей, указывающих на такие состояния, как рак и сердечно-сосудистые заболевания. Эти модели используются в лечении рака, например, для прогнозирования прогрессирования рака, рецидива и выживаемости. Они могут анализировать медицинские изображения с точностью, сопоставимой или даже превосходящей точность экспертов-людей.

Важным достижением применения ИИ в здравоохранении стала возможность разработки персонализированных планов лечения. Анализируя генетический состав, образ жизни и историю болезни человека, алгоритмы ИИ могут предсказать, как пациенты будут реагировать на конкретные виды лечения³¹⁴. Это позволяет настраивать терапию, что приводит к более эффективному и действенному здравоохранению.

³¹¹ Как искусственный интеллект помогает решить задачи здравоохранения. URL: <https://www.rbc.ru/society/11/10/2024/66f681ba9a79471b04d22aaa> (дата обращения: 29.02.2025).

³¹² Искусственный интеллект в российском здравоохранении: информация о последних тенденциях и влиянии на медицинскую практику. URL: <https://med.roche.ru/innovations/blog/ai-russia.html> (дата обращения: 29.02.2025).

³¹³ В России готовятся госстандарты для искусственного интеллекта. URL: https://www.cnews.ru/news/top/2023-03-01_v_rossii_gotovyat_standarty (дата обращения: 29.02.2025).

³¹⁴ *Topol, E.J.* (2019) High-Performance Medicine: The Convergence of Human and Artificial Intelligence. *Nature Medicine*, 25, pp. 44-56.

С помощью технологий ИИ точность, гибкость и контроль при проведении радиологических, патологических, эндоскопических, ультразвуковых и биохимических исследований, а также хирургических операций достигают уровня, превосходящего возможности человека, при этом нагрузка на врача уменьшается³¹⁵.

Следовательно, системы искусственного интеллекта улучшают оказание медицинской помощи пациентам за счет автоматизации административных задач, оптимизации распределения ресурсов и предоставления поддержки принятия решений в режиме реального времени.

Несмотря на преимущества ИИ, многие авторы обозначают различные проблемы, связанные с применением ИИ в здравоохранении.

Так, Н.С. Минько и М.П. Курилович выделяют проблемы сертификации и лицензирования ИИ, включая лицензирование медицинских систем искусственного интеллекта³¹⁶.

Однако на данный момент в России эта проблема решена. В случае если программное обеспечение, созданное на основе ИИ, предназначено производителем для лечебно-диагностических целей (при оказании медицинской помощи), оно относится к медицинским изделиям³¹⁷.

Постановление Правительства Российской Федерации от 30 ноября 2024 г. № 1684 «Об утверждении Правил государственной регистрации медицинских изделий» упрощает процедуру регистрации медицинских изделий на базе ИИ.

³¹⁵ Liu, P. R., Lu, L., Zhang, J. Y., Huo, T. T., Liu, S. X., & Ye, Z. W. (2021). Application of artificial intelligence in medicine: an overview. *Current Medical Science*, 41(6), pp. 1105-1115; Милкова Э. Г. Искусственный интеллект в здравоохранении: к чему приведет цифровизация? //Иновации и инвестиции. 2021. №. 4. С. 353-356.

³¹⁶ Минько Н.С., Курилович М. П Перспективы развития правовых отношений в области здравоохранения в условиях внедрения систем искусственного интеллекта // Правовое регулирование в сфере здравоохранения в условиях новых вызовов: вопросы теории и практики : Материалы Всероссийской научно-практической конференции с международным участием, Тамбов, 25–26 марта 2022 года / Отв. редактор Р.В. Зелепукин. Тамбов: Издательский дом "Державинский", 2022. С. 102-117.

³¹⁷ Гусев, А. В., Владимирский, А. В., Шарова, Д. Е., Арзамасов, К. М., Храмов, А. Е. Развитие исследований и разработок в сфере технологий искусственного интеллекта для здравоохранения в Российской Федерации: итоги 2021 года // Digital Diagnostics. 2022. Т. 3. – №. 3. С. 178-194

Например, пункт 24 Правил государственной регистрации медицинских изделий, утвержденных указанным постановлением, предусматривает, что государственная регистрация программного обеспечения с применением технологий искусственного интеллекта, предназначенного для обработки медицинских изображений, полученных при проведении рентгенологических исследований, включая компьютерную томографию, рентгенографию, флюорографию и маммографию, при условии проведения клинических испытаний в государственном бюджетном учреждении здравоохранения города Москвы «Научно-практический клинический центр диагностики и телемедицинских технологий Департамента здравоохранения города Москвы», предусмотрены пунктами 101 - 109 настоящих Правил³¹⁸.

Как результат по состоянию на 1 января 2025 г. Росздравнадзором было зарегистрировано всего 25 медицинских изделий на базе ИИ. Большинство из них (19 или 76%) являются отечественными. Из общего числа выданных регистрационных удостоверений 16 предназначены для анализа медицинских изображений³¹⁹. По итогам 2023 г. 84 (94 %) субъекта Российской Федерации выполнили минимально установленный показатель в части закупки медицинских изделий на базе ИИ³²⁰. Решения с использованием ИИ в медицине в настоящий момент внедряют 70 российских регионов, в основном это технологии, работающие с медицинскими изображениями: маммографией, компьютерной томографией органов грудной клетки и головного мозга, рентген-снимками органов грудной клетки³²¹.

³¹⁸ Постановление Правительства Российской Федерации от 30 ноября 2024 г. № 1684 «Об утверждении Правил государственной регистрации медицинских изделий» // "Собрание законодательства РФ", 09.12.2024, № 50, ст. 7744.

³¹⁹ Ванько В. В., Артемова О. Р., Карпов О. Э., Матвиенко А. В., Гусев А. В., Еникеев И. М., Костина Е. В. Итоги внедрения искусственного интеллекта в здравоохранении России // Врач и информационные технологии. 2024. № 3. С. 32-43.

³²⁰ Гусев А. В., Артемова О. Р., Васильев Ю. А., & Владимирский А. В. Внедрение медицинских изделий с технологиями искусственного интеллекта в здравоохранении России: итоги 2023 г // Национальное здравоохранение. 2024. Т. 5, № 2. С. 17-24.

³²¹ Для чего в российских регионах используют ИИ в медицине. URL: <https://rg.ru/2023/10/24/nejroseti-staviat->

Ряд авторов поднимает проблему отсутствия этических принципов и стандартов в области применения искусственного интеллекта³²².

Стоит отметить, что в настоящее время данная проблема уже не актуальна, поскольку в национальной стратегии развития искусственного интеллекта на период до 2030 года, утвержденной Указом Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» закреплены этические принципы развития и использования ИИ: защиты прав и свобод человека; безопасности; прозрачности; технологического суверенитета; целостности инновационного цикла; наиболее эффективного использования технологий искусственного интеллекта; поддержки конкуренции; открытости и доступности; преемственности; защищённости и достоверности исходных данных³²³.

В целях решения указанной проблемы в России был создан «Кодекс этики в сфере искусственного интеллекта», который определяет принципы этики и правила поведения ИИ. Данный Кодекс распространяется на отношения, связанные с этическими аспектами создания (проектирования, конструирования, пилотирования), внедрения и использования технологий искусственного интеллекта на всех этапах жизненного цикла, которые в настоящее время не урегулированы законодательством Российской Федерации и/или актами технического регулирования³²⁴.

Подчеркнем, что данный Кодекс следует дополнить некоторыми этическими требованиями к системам ИИ. В частности, для систем высокого риска следует закрепить:

diagnoz.html?ysclid=lt0d7znqod817828204&utm_referrer=https%3A%2F%2Fwww.elibrary.ru%2F (дата обращения: 28.02.2025)

³²² Гусев А. В. Шарова Д. Е. Этические проблемы развития технологий искусственного интеллекта в здравоохранении // Общественное здоровье. 2023. Т. 3, № 1. С. 42-50.

³²³ Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» // "Собрание законодательства РФ", 14.10.2019, № 41, ст. 5700.

³²⁴ Кодекс этики в сфере искусственного интеллекта. URL: https://ethics.a-ai.ru/assets/ethics_files/2023/05/12/%D0%9A%D0%BE%D0%B4%D0%B5%D0%BA%D1%81_%D1%8D%D1%82%D0%B8%D0%BA%D0%B8_20_10_1.pdf (дата обращения: 28.02.2025)

1. Обязательство по документированию используемых обучающих выборок для последующей проверки на предмет смещений, ведущих к дискриминационным результатам.

2. Требование к интерфейсу системы ИИ о том, что ее рекомендации носят вспомогательный, а не предписывающий характер для исключения рисков «слепого доверия» со стороны пользователя.

В России было принято несколько стандартов для ИИ в здравоохранении, которые направлены на регулирование методологической основы процесса клинических испытаний, порядок их проведения, показателей точности, аудита и контроля качества медицинских систем искусственного интеллекта, а также обучение систем искусственного интеллекта.

Созданы и приняты многие стандарты по ИИ в здравоохранении, например, ГОСТ Р 59921.0-2022 «Системы искусственного интеллекта. Системы искусственного интеллекта в клинической медицине. Основные положения», ГОСТ Р 59921.1-2022 «Системы искусственного интеллекта. Системы искусственного интеллекта в клинической медицине. Часть 1. Клинические испытания» и др.

Несмотря на наличие данных стандартов, которые носят в основном методический характер и не покрывают ключевые вопросы ответственности, прозрачности алгоритмов ИИ, согласимся с мнением Н.С. Морозовой, отметившей, что «существующая нормативно-правовая база использования ИИ в медицине крайне неполна, бессистемна и не позволяет обеспечить адекватное регулирование многих важных вопросов - таких как стандарты разработки и применения технологий ИИ в здравоохранении»³²⁵.

Таким образом, наличие стандартов не решает фундаментальной проблемы отсутствия единого правового режима для ИИ. В России необходимо четкое, эффективное правовое регулирование применения ИИ в здравоохранении.

³²⁵ Морозова Н. С. Задачи этико-правового обеспечения технологического развития системы здравоохранения //Lex Genetica. 2024. Т. 3. №. 1. С. 44-56.

Приходится констатировать, что в настоящее время в нашей стране отсутствует полноценный механизм правового регулирования ИИ в здравоохранении, который бы учитывал требования прозрачности к ИИ, риски, связанные с ИИ и влияющие на здоровье человека, вплоть до причинения физического вреда или смерти. Кроме того, набор критериев для оценки вероятности и серьезности потенциального ущерба со стороны ИИ, а также необходимые действия для его минимизации в законодательстве России не предусмотрены, также отсутствует возможность получать информацию о принципах работы системы ИИ, а также об используемых данных пользователя. Это является главной проблемой, которую предлагаем решить следующим образом.

Правовое регулирование отстает от темпов технологических изменений при применении ИИ в здравоохранении, а законодательство в этой области отстает от реальных потребностей. С целью избегания трудностей при внедрении ИИ в законодательство в науке ученые предлагают придерживаться двух основных подходов:

во-первых, учитывать, как положительные, так и отрицательные последствия для прав человека при использовании ИИ;

во-вторых, определить влияние и воздействие ИИ на изменение содержания прав человека и их реализацию в конкретной области внедрения технологии³²⁶. Если использование ИИ усиливает гарантии прав человека и способствует их реализации, то следует их развивать и применять. И наоборот, если происходит уменьшение гарантий прав человека и деформируется практика их реализации, очевидно, от этой технологии следует отказаться³²⁷.

³²⁶ *Филатова А. О.* К вопросу о выделении нового поколения прав человека: цифровые правомочия активного избирательные права // Вестник образовательного консорциума Среднерусский университет. Серия: Юриспруденция. 2021. № 18. С. 56-58.

³²⁷ *Алешикова И. А.* Искусственный интеллект и его взаимосвязь с правами человека // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4, Государство и право. 2021. №. 1. С. 70-78.

Разработка нормативных требований для применения технологий ИИ в здравоохранении — сложная задача.

С.А. Привалов указывает, что предусмотренные федеральные проекты в сфере здравоохранения страдают широтой и неконкретностью формулировок, это осложняет процесс развития технологий искусственного интеллекта в России, и предлагает принять узкий, специализированный нормативно-правовой акт, регулирующий развитие и применение технологий искусственного интеллекта в сфере здравоохранения³²⁸.

На наш взгляд, с данным мнением сложно согласиться в силу следующих причин.

Во-первых, общее регулирование более эффективное. Разрабатывая единый набор правил, который применяется ко всем системам ИИ, регулирующие органы могут избежать необходимости разрабатывать отдельные правила для каждой новой системы ИИ.

Во-вторых, общее регулирование более последовательное. Применяя одни и те же правила ко всем системам ИИ, регулирующие органы могут помочь обеспечить справедливое отношение к системам ИИ.

В-третьих, общее регулирование более гибкое. Общее регулирование может обеспечить основу для последующего точечного регулирования, которое может помочь устранить конкретные риски и способствовать инновациям. Допуская гибкость в применении правил, регулирующие органы могут адаптировать правила к меняющимся обстоятельствам.

В поддержку нашей позиции приведем мнения других авторов, например, Н.В. Аликперова справедливо пишет, что «единого закона об ИИ в нашей стране до сих пор не принято, а профильное законодательство в сфере охраны здоровья практически не содержит положений, касающихся особенностей использования

³²⁸ Привалов С. А. Технологии искусственного интеллекта в сфере обеспечения права на охрану здоровья, доступную и качественную медицинскую помощь: перспективы и проблемы регулирования // Вестник Саратовской государственной юридической академии. 2021. № 4(141). С. 34-43.

интеллектуальных систем в медицинской деятельности»³²⁹. Т.В. Воротилина аналогично предлагает разработать и принять единый нормативный правовой акт в области регулирования искусственного интеллекта³³⁰.

Важно, что общие правила по ИИ подчеркивают значимость подотчетности и прозрачности, которые также имеют решающее значение в сфере здравоохранения. Алгоритмы ИИ, используемые для диагностики или прогнозирования состояния здоровья, должны быть полностью объяснимыми, а их процессы принятия решений должны быть прозрачными для проверки и подотчетности.

Обеспечение подотчетности и прозрачности возможно лишь при использовании риск-ориентированного подхода, применяемого в ЕС. М.А. Лапина также подтверждает, что развитие правового регулирования ИИ в области здравоохранения следует вести в зависимости от рисков³³¹.

Согласимся с мнением Г.Г. Камаловой в том, что «правовое регулирование применения ИИ в сфере здравоохранения сегодня требует научного и практического осмысления в целях формирования общей теоретической концепции регулирования данной сферы, а также выработки практических предложений и рекомендаций»³³².

Считаем, что первым шагом на пути осмысления правового регулирования ИИ в России представляется формирование совокупности специальных

³²⁹ *Аликперова Н.В.* Искусственный интеллект в здравоохранении: риски и возможности // *Здоровье мегаполиса.* 2023. № 3. с. 41–49.

³³⁰ *Воротилина Т. В., Коротченко А. В.* Место искусственного интеллекта в правовой системе России // *Юридический вестник Дагестанского государственного университета.* – 2024. Т. 49. №. 1. С. 166-172.

³³¹ *Лапина М. А.* Организационно-правовые и финансовые аспекты цифровизации и внедрения технологий искусственного интеллекта в области здравоохранения // *Финансы: теория и практика.* 2022. Т. 26, № 3. С. 169-185.

³³² *Камалова Г. Г.* Перспективы правового регулирования применения искусственного интеллекта и робототехники в здравоохранении // *Исследование и практика в социально-экономической и гуманитарной сфере: сборник избранных статей Всероссийской (национальной) научно-практической конференции, Санкт-Петербург, 13 января 2022 года.* – Санкт-Петербург: ГНИИ «Нацразвитие», 2022. С. 55-58.

конституционно-правовых принципов, которые позволят определить основу для последующих разрабатываемых и принимаемых правил и норм.

В этой связи А.Н. Мещеряков подчеркнул, что присутствие ИИ во всех сферах общественных отношений естественным образом приводит к его конституционно-правовому регулированию, концептуальной основой которого может стать система принципов приоритета человека, его прав и свобод, невозможности причинения вреда человеку и человечеству, ограничения автономии искусственного интеллекта и его технологий³³³. К аналогичному выводу приходит И.А. Петроченков, выделивший принципы верховенства прав и свобод человека и гражданина, равенства перед законом, свободы слова и информации³³⁴. М.А. Липчанская, Е.А. Отставнова рассматривают применение ИИ как «средство реализации принципа социального государства, от которого зависит эффективность реализации гарантированных Конституцией Российской Федерации социальных прав и свобод человека»³³⁵.

С точки зрения здравоохранения важнейшее место занимают принцип гуманности, предполагающий приоритет охраны интересов человека в ходе оказания медицинской помощи, принцип доступности медицинской информации пациенту и принцип конфиденциальности медицинских данных. В.С. Буланова также упоминает принцип достоверности информации и отмечает, что

³³³ Мещеряков А. Н. Искусственный интеллект в предмете конституционного права // Право в эпоху искусственного интеллекта: перспективные вызовы и современные задачи : сборник научных статей по материалам Международного научно-практического форума «VI Сибирские правовые чтения», г. Тюмень, 17-19 октября 2024 г. / гл. ред. С. С. Зенин ; отв. ред. Л. В. Иванова ; Министерство науки и высшего образования Российской Федерации, Тюменский государственный университет, Институт государства и права. - Тюмень : ТюмГУ-Press, 2024. С. 36-40.

³³⁴ Петроченков И. А. Перспективы защиты прав человека в контексте принятия Евросоюзом регламента об искусственном интеллекте. Гражданин. Выборы // Власть. 2024. Т. 2. С. 104-115.

³³⁵ Липчанская М. А., Отставнова Е. А. Конституционно-правовые и нравственные основы использования искусственного интеллекта в реализации социальных прав и свобод человека // Вестник Саратовской государственной юридической академии. 2020. №. 3 (134). С. 69-78.

несоблюдение этого принципа в медицинской сфере может привести к причинению ущерба здоровью пациента и морального вреда³³⁶.

Стоит отметить, что в России Министерством инноваций и цифрового развития Российской Федерации уже разработана Концепция регулирования ИИ до 2030 г. В документе не указаны конкретные регуляторные правила и обязательные требования, а указаны только правовые принципы, на которых должно основываться будущее развитие ИИ.

В Концепции определяется как осуществляется процедура проверки технологий ИИ на безопасность, при этом указывается, что в основе будущего регулирования ИИ должен быть положен человекоориентированный подход на основе доверия к технологиям, принципа технологического суверенитета, уважения к автономии и свободе воли человека, запрета на причинение вреда человеку и недопущения антропоморфизации («очеловечения») технологий³³⁷.

Европейский подход характеризуется большим прагматизмом и, как заявляется в вышеуказанной концепции, включает принцип технологического суверенитета и является риск-ориентированным, а также антропоцентричным, что означает: человек и защита его прав и свобод всегда должны оставаться в центре всех политических и законодательных соображений³³⁸.

Ю.А. Климан справедливо отметил, что текущее состояние правового регулирования применения информационных технологий в сфере здравоохранения не регламентирует вопросы использования информационных технологий при оказании медицинской помощи как комплекса мероприятий, направленных на поддержание и (или) восстановление здоровья и включающих в себя

³³⁶ Буланова В.С. Информационно-правовое обеспечение оказания телемедицинских услуг в условиях цифровой трансформации: дис.... канд. юрид. наук. 12.00.13/ Буланова Валерия Сергеевна - М., 2021. 210 с.

³³⁷ Минцифры подготовило концепцию регулирования искусственного интеллекта. URL: <https://www.vedomosti.ru/economics/articles/2025/08/20/1132830-mintsifri-podgotovilo-kontseptsiyu-regulirovaniya-iskusstvennogo-intellekta> (дата обращения: 28.08.2025)

³³⁸ Филипова, И. А. Искусственный интеллект: европейский подход к регулированию // Журнал зарубежного законодательства и сравнительного правоведения. 2023. Т. 19, № 2. С. 54-65.

предоставление медицинских услуг пациенту³³⁹. Особенно это касается ИИ, поскольку в России до сих пор нет комплексного правового регулирования применения ИИ во всех сферах жизнедеятельности человека.

В результате целесообразно было бы предложить принять федеральный закон в целях развития правового регулирования ИИ, в котором можно было бы учесть положения Закона об искусственном интеллекте ЕС, построенного на риск-ориентированном подходе, направленном на минимизацию наиболее серьезных рисков. При этом такой федеральный закон, как представляется, должен включать следующие положения о рисках применяемого ИИ³⁴⁰:

1. Неприемлемый риск. Системы ИИ с неприемлемым риском рассматриваются как потенциальная угроза для людей и будут запрещены. К таким методам относятся: когнитивно-поведенческое манипулирование людьми или целевыми группами населения, технологии биометрической идентификации в реальном времени и на расстоянии, такие как распознавание лиц.

2. Высокий риск. Компании должны пройти предварительную «оценку соответствия» и выполнить полный набор критериев, гарантирующих безопасность системы.

3. Ограниченный риск. Системы ИИ должны придерживаться основных стандартов прозрачности, чтобы пользователи могли делать осознанный выбор. После взаимодействия с программами пользователь может выбрать, что ему предпочтительнее для дальнейшего использования. Это относится к системам ИИ, которые создают или изменяют визуальные, слуховые или аудиовизуальные материалы, например, дипфейки (deep fakes).

³³⁹ *Климан, Ю. А.* Правовые проблемы применения искусственного интеллекта в сфере здравоохранения // Теория и практика общественного развития. 2024. № 11(199). С. 237-243.

³⁴⁰ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng> (дата обращения: 28.11.2024)

4. Минимальный риск. Системы ИИ из данного ряда уже широко применяются во всех сферах и составляют большинство из всех используемых в настоящее время.

Классификация систем ИИ по различным категориям риска определяется рядом критериев, включая целевое назначение системы ИИ, исходя из уровня потенциального вреда, связанного с системой, ее технологических качеств и возможного влияния на здоровье, безопасность и основные права людей. Эти категории риска призваны определять уровень регулятивного контроля и надзора, применяемого к различным типам приложений ИИ, обеспечивать ответственную разработку и внедрение технологий ИИ, гарантировать безопасность и основные права, обеспечивать надлежащий регулятивный надзор, способствовать инновациям.

Реализация риск-ориентированной стратегии регулирования ИИ, всесторонне учитывающей риски и выгоды, предоставит частному сектору в России набор критериев для оценки вероятности и серьезности потенциального ущерба, а также необходимые действия для его минимизации.

На этом основании предлагаем принять общий федеральный закон об искусственном интеллекте, в котором также будут использованы помимо положений Закона об искусственном интеллекте ЕС практический опыт Казахстана, который разработал Закон РК «Об искусственном интеллекте» от 12 мая 2025 года № 6-18-12-119, основанный на подходе, реализованном в Закона об искусственном интеллекте ЕС.

ИИ в Казахстане будет классифицирован по уровням риска согласно ст. 18 законопроекта. В тексте документа определяется база и статус национальной платформы искусственного интеллекта. Согласно ст. 16 Закона пользователь обладает следующими правами:

«1) получать от собственника или владельца системы искусственного интеллекта разъяснения о результатах ее деятельности, затрагивающей его права,

свободы и законные интересы, в порядке, предусмотренном пользовательским соглашением и законодательством Республики Казахстан;

2) на защиту своих персональных данных и конфиденциальной информации, обрабатываемой системой искусственного интеллекта;

3) осуществлять меры по защите своих прав на объекты интеллектуальной собственности, созданные с использованием систем искусственного интеллекта»³⁴¹.

Отдельное внимание в Законе уделено усиленной защите персональных данных. В частности, вводятся строгие ограничения на использование искусственного интеллекта для оценки людей по социальным, биометрическим и поведенческим характеристикам, а также запрет на создание и использование ИИ, способного манипулировать поведением человека. Также в Законе закреплены принципы регулирования общественных отношений в сфере ИИ, которые должны обязательно соблюдаться при использовании ИИ.

Также можно отметить, что в отличие от опыта ЕС и Казахстана, основанного на рисках и санкциях, Южная Корея в декабре 2025 г. приняла Закон «О развитии ИИ и формировании доверительной основы», который одновременно с этим закрепляет обязанность государства поддерживать развитие отрасли. В Законе предусмотрены создание национального комитета по ИИ, разработка трехлетних базовых планов, меры по адаптации граждан к распространению технологий и формирование этических принципов их применения, а также норма о пересмотре законодательства каждые три года, что должно позволить оперативно подстраиваться под технологические и международные изменения³⁴².

Между тем, ясно, что перенос риск-ориентированной модели ЕС в российские правовые условия требует предварительного укрепления

³⁴¹ Досье на проект Закона Республики Казахстан «Об искусственном интеллекте» (январь 2025 года). URL: https://online.zakon.kz/Document/?doc_id=34868071&pos=133;-54#pos=133;-54 (дата обращения: 28.02.2025)

³⁴² Южная Корея станет первой страной в мире, где будет действовать закон об ИИ. URL: <https://rg.ru/2025/12/15/iuzhnaia-koreia-stanet-pervoj-stranoj-v-mire-gde-budet-dejstvovat-zakon-ob-ii.html> (дата обращения: 28.12.2025)

институционального потенциала отрасли. Ключевым вызовом является создание системы аккредитованных органов по оценке соответствия, способных проводить комплексную проверку алгоритмов ИИ. Без решения задач в данной области заимствование формальных правовых конструкций рискует остаться декларацией.

Государства должны обеспечить, чтобы те, кто может подвергнуться негативному воздействию систем искусственного интеллекта, имели эффективные и доступные средства правовой защиты против разработчиков или установщиков систем искусственного интеллекта, которые несут за это ответственность. Эффективные средства правовой защиты должны предусматривать возмещение любого причиненного вреда и могут включать меры в рамках гражданского, административного или, в соответствующих случаях, уголовного права.

На основании всего вышеизложенного, полагаем, что в России следует разработать федеральный закон об искусственном интеллекте, в нормах которого, в частности, должны содержаться критерии риска в отношении устройств с ИИ (1. Неприемлемый риск. 2. Высокий риск. 3. Ограниченный риск. 4. Минимальный риск) с учетом опыта ЕС, реализованного в Законе об искусственном интеллекте ЕС, а также с учетом концепции Закона РК «Об искусственном интеллекте» от 12 мая 2025 года № 6-18-12-119.

Таким образом, на основе проведенного в этой части параграфа анализа отечественного правового регулирования применения ИИ в сфере здравоохранения можно сделать следующий вывод.

Поскольку ИИ продолжает проникать в здравоохранение, существует объективная потребность в разработке и внедрении требований, которые отдадут приоритет правам и интересам пациентов, одновременно способствуя росту и развитию технологий ИИ. Разработав надежную нормативную базу, мы сможем использовать возможности ИИ для улучшения ухода за пациентами и развития медицинских исследований, обеспечив при этом ответственное и справедливое использование данной технологии. ГОСТы и постановление Правительства Российской Федерации от 30 ноября 2024 г. № 1684 «Об утверждении Правил

государственной регистрации медицинских изделий» направлены на регулирование использования ИИ, однако механизм комплексного правового регулирования применения ИИ остается нерешенным. Вопросы юридической ответственности за вред, причиненный ИИ, также требуют внимания, особенно в контексте медицинской помощи.

Необходимость гарантирования прозрачности в работе ИИ и учета прав человека являются ключевыми аспектами для успешного внедрения данных технологий в здравоохранение. Разработка общего федерального закона об ИИ, учитывающего опыт разработки Закона об искусственном интеллекте ЕС и Закона РК «Об искусственном интеллекте», может помочь обеспечить правовое регулирование применения информационных технологий в России и решить многие проблемы, связанные с его применением.

2.5. Телемедицинские технологии

Стоит отметить, что на данный момент в законодательстве Российской Федерации не закреплено конкретное определение понятия «телемедицина». Однако указание на телемедицинские технологии имеется. Оно впервые было введено Федеральным законом от 29 июля 2017 года № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам применения информационных технологий в сфере охраны здоровья»³⁴³.

В соответствии с пунктом 22 ст. 2 Федерального закона от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» под телемедицинскими технологиями понимаются «информационные технологии, обеспечивающие дистанционное взаимодействие медицинских работников между собой, с пациентами и (или) их законными представителями, идентификацию и аутентификацию указанных лиц, документирование совершаемых ими действий

³⁴³ Федеральный закон от 29 июля 2017 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам применения информационных технологий в сфере охраны здоровья» // «Собрание законодательства РФ», 31.07.2017, № 31 (Часть I), ст. 4791.

при проведении консилиумов, консультаций, дистанционного медицинского наблюдения за состоянием здоровья пациента»³⁴⁴. Ввиду отсутствия легальной дефиниции телемедицины целесообразно далее использовать определение понятия «телемедицинские технологии» в контексте оказания медицинской помощи гражданам, как это установлено законодательством Российской Федерации.

Телемедицинские технологии считаются одним из важнейших нововведений в сфере здравоохранения не только с технологической, но и с культурной и социальной точки зрения. Они способствуют доступности медицинских услуг и повышению организационной эффективности. Их роль заключается в решении проблем, вызванных социально-экономическими изменениями в XXI веке (более высокие требования к здравоохранению, старение населения, возросшая мобильность граждан, необходимость управления большими объемами информации, потребность повышения глобальной конкурентоспособности и улучшение предоставления медицинских услуг) в среде с ограниченными бюджетными расходами.

Использование телемедицинских технологий позволяет, например, оказывать консультативные медицинские услуги в тех районах, где у пациентов нет возможности получить помощь узких специалистов напрямую в медицинском учреждении. Но и в огромных мегаполисах и развитых странах телемедицинские технологии имеют не меньшее значение. Благодаря им значительно сокращаются расходы на лечение, повышается качество диагностики и реализуется возможность удаленного мониторинга состояния здоровья. Это особенно важно для пациентов с хроническими заболеваниями и для пожилых людей.

³⁴⁴ Федеральный закон от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» // «Собрание законодательства РФ», 28.11.2011, № 48, ст. 6724.

В третьем квартале 2023 года объем сегмента телемедицинских технологий в России составил 3,76 млрд рублей: на 50% больше, чем годом ранее, и на 12% больше, чем во втором квартале³⁴⁵.

Российское законодательство в части применения телемедицинских технологий обширно и включает в себя как законы, так и подзаконные акты. М.С. Варюшин выделяет два блока нормативных правовых актов в области телемедицинских технологий в здравоохранении: «первый блок связан с регулированием отношений врача (медицинской организации) и пациента, а второй блок устанавливает формы оказания медицинской помощи при передаче данных, составляющих врачебную тайну, регулирует отношения медицинской организации, пациента и оператора (провайдера)»³⁴⁶. М.А. Винокурова и Т.В. Пашнина устанавливают 6 групп правовых актов, регулирующих оказание телемедицинских услуг³⁴⁷.

Несмотря на обширное законодательство по регулированию применения телемедицинских технологий, многие авторы выделяют различные проблемы, связанные с ними. В частности, поднимается проблема отсутствия возможности постановки диагноза посредством использования телемедицинских технологий³⁴⁸. Это означает, что если человек заболел и нуждается в медицинских услугах, он должен сначала нужно пройти очную диагностику³⁴⁹.

М.А. Коваленко отметил отсутствие стандартизации в области телемедицинских технологий и предложил создать стандарт оказания

³⁴⁵ Прилуков М.Д. О современном состоянии правового регулирования телемедицины в Российской Федерации // Вестник Нижегородского университета им. Н.И. Лобачевского. 2024. № 5. С. 148-154.

³⁴⁶ Варюшин М. С. Правовое регулирование телемедицины в России и ЕС: два шага впереди один назад // Закон. 2018. № 1. С. 165-174.

³⁴⁷ Винокурова М. А., Пашнина Т. В. О применении системного подхода в правовом регулировании телемедицинских технологий // Журнал российского права. 2022. Т. 26, № 6. С. 126-139.

³⁴⁸ Базина О. О., Сименюра С. С. Телемедицина: достоинства, недостатки, реалии (правовой анализ и практическое применение) // Медицинское право. 2020. № 3. С. 32—38.

³⁴⁹ Yi, Z. and Chenguang, W. (2024) “‘Internet Plus Health Care’ as an Impetus for China’s Health System Reform”. *Digital Health Care outside of Traditional Clinical Settings: Ethical, Legal, and Regulatory Challenges and Opportunities*. Cambridge: Cambridge University Press, pp. 156–168.

телемедицинской помощи, который «сможет учесть особенности диагностирования в зависимости от характера обращения, заболевания, состояния пациента и других обстоятельств, которые могут повлиять на достоверность диагноза»³⁵⁰.

Е.Н. Карягина и А.Р. Еникеев в качестве еще одного пробела отмечают «отсутствие временного интервала после очного приема пациента, в течение которого он может обратиться за дистанционной консультацией»³⁵¹.

Также К.Е. Лукичев упомянул проблему отсутствия регулирования заключения договора на оказание платных медицинских услуг в форме электронного документа в случае применения телемедицинских технологий³⁵².

Иными учеными изучаются проблемы невозможности оказания медицинской помощи с применением телемедицинских технологий вне помещения медицинской организации³⁵³, невозможности пользоваться телемедицинскими технологиями по обязательному медицинскому страхованию³⁵⁴.

Некоторые ученые поднимали проблему отсутствия права пациента на выбор консультирующего врача при оказании медицинской помощи через телемедицинские технологии³⁵⁵.

³⁵⁰ Коваленко М.А. О правовой возможности постановки диагноза при дистанционном консультировании // Юридические исследования. 2024. № 4. С. 87-97.

³⁵¹ Карягина Е.Н., Еникеев А.Р. Назначение лекарственных средств посредством применения телемедицинских технологий: правовое регулирование в России и США (сравнительно-правовой анализ) // Медицинское право: теория и практика. Т. 5. № 2(10). 2020. С. 183-189.

³⁵² Лукичев К. Е. Нормативное обеспечение процесса внедрения телемедицинских технологий в российском здравоохранении // Управленческие науки в современном мире : сборник докладов научной конференции, Москва, 13–15 ноября 2019 года / Финансовый университет при Правительстве Российской Федерации. – Москва: Издательский дом "Реальная экономика", 2020. С. 157-161.

³⁵³ Ковалевский С. М. Отдельные проблемы правового регулирования использования телемедицинских технологий в Российской Федерации // Медицина и право в XXI веке : Сборник трудов XV ежегодной научно-практической конференции с международным участием, Санкт-Петербург, 22–23 декабря 2023 года. – Санкт-Петербург: Центр современной литературы и книги на Васильевском, 2024. С. 228-237.

³⁵⁴ Чилилов А. М., Кадыров Ф. Н., Мамаев М. Г. Баланс прав и обязанностей медицинских работников и пациентов при оказании медицинской помощи с применением телемедицинских технологий // Экономика, предпринимательство и право. 2023. Т. 13. № 6. С. 2041-2054.

³⁵⁵ Коваленко М. А. Медицинский работник как субъект оказания телемедицинской помощи: вопросы законодательной регламентации // Евразийский юридический журнал. 2024. №

Подчеркнем, что по состоянию на 2026 год многие из вышеуказанных проблем были решены в результате принятия двух экспериментальных правовых режимов в сфере применения телемедицинских технологий, рассмотренных в начале параграфа 2 главы 2, поэтому здесь мы не будем останавливаться на вышеуказанных вопросах подробно.

При этом, несмотря на принятые экспериментальные правовые режимы, все еще остро стоит проблема сохранения врачебной тайны и защиты персональных данных при использовании телемедицинских технологий³⁵⁶.

Многие авторы единогласны во мнении, что вопросы соблюдения в цифровой среде врачебной тайны урегулированы недостаточно³⁵⁷, не сформированы надежные гарантии неразглашения сведений, которые относятся к врачебной тайне, а также персональных данных пациента³⁵⁸. Очевидно, что для снижения рисков нарушения врачебной тайны, требуется разработка комплексного решения обозначенной проблемы³⁵⁹, включающего правовые меры³⁶⁰.

Несмотря на то, что проблемы врачебной тайны могут рассматриваться в рамках применения иных информационных технологий, помимо телемедицинских, изначально в России получили развитие именно телемедицинские технологии. Беря начало с 1990 и впоследствии получив законодательное закрепление в 2017 году, телемедицинские технологии в период с 2016 и по настоящее время получили

1(188). С. 184-186; *Кадыров Ф. Н., Куракова Н. Г., Чилилов А. М.* Правовые проблемы применения телемедицинских технологий в условиях борьбы с распространением коронавируса COVID-19 // *Врач и информационные технологии.* 2020. № 2. С. 45-51.

³⁵⁶ *Третьякова Е. П.* Правовые аспекты регулирования телемедицины // *Цифровое право.* 2020. Т. 1, № 2. С. 53-66.

³⁵⁷ *Акулин И. М., Чеснокова Е. А., Смирнова К. М., Пресняков Р. А.* Трансформация института врачебной тайны в эпоху электронного здравоохранения // *Закон.* 2019. № 9. С. 179–189.

³⁵⁸ *Иншакова А. О., Тымчук Ю. А.* Охрана персональных данных пациентов при оказании медицинской помощи (услуг) с применением телемедицинских технологий // *Lex Russica (Русский закон).* 2024. Т. 77, № 7(212). С. 19-29.

³⁵⁹ *Буянова А. В.* Телемедицинские проблемы регулирования и правоприменения // *Социально-политические науки.* 2018. № 2. С. 235–238.

³⁶⁰ *Ковалева Н. Н., Новикова Е. А.* Особенности правового регулирования телемедицинских технологий в условиях цифровизации // *Право и государство: теория и практика.* 2021. № 7 (199). С. 150–152

широкое развитие, поскольку появились мобильные специализированные системы и телемедицинские комплексы (PACS-системы, электронные медицинские карты, электронные банки данных и т.п.)³⁶¹.

Поэтому целесообразно рассмотреть вопрос соблюдения врачебной тайны на примере телемедицинских технологий, поскольку для их использования необходимы совершенно особые условия, отличные от других видов информационных технологий. Например, техническое состояние оборудования, отсутствие врачей, которые имеют право оказывать медицинскую помощь и проводить консультации с использованием телемедицинских технологий в связи с необходимостью получения ими соответствующей лицензии. Как отмечает А.В. Попова, «право на использование телемедицинских технологий возникает только у медицинских работников, зарегистрированных в Федеральном реестре, и при условии регистрации медицинской организации, в которой они работают, в соответствующем реестре Единой государственной информационной системы в сфере здравоохранения»³⁶².

Иначе говоря, вопрос о соблюдении врачебной тайны с учётом политики цифровизации и развития информационных технологий становится всё более актуальным. Конституционный Суд Российской Федерации рассматривал проблему разглашения врачебной тайны, например, в постановлении № 1-П от 13 января 2020 «По делу о проверке конституционности частей 2 и 3 ст. 13, пункта 5 части 5 ст. 19 и части 1 ст. 20 Федерального закона «Об основах охраны здоровья граждан в Российской Федерации» в связи с жалобой Р.Д. Свечниковой», где затрагивался вопрос ее разглашения, в том числе после смерти человека. Данная информация является информацией с ограниченным доступом, но в случае смерти пациента возникает вопрос: насколько содержание этой медицинской информации может быть доступно третьим лицам (в частности, родственникам). Пациент имеет

³⁶¹ Шепель Р. Н. Кутчер, А. В., Ваховская, Т. В., Дряпкина, О. М. История развития телемедицины в Российской Федерации // Неотложная кардиология и кардиоваскулярные риски. 2025. Т. 3. №. 2. С. 765–771.

³⁶² Попова А.В. Телемедицина в России и за рубежом: к вопросу о правовом регулировании // Вестник МГПУ. Серия: Юридические науки. 2019. № 1 (33). С. 53 – 60.

право сохранить свой медицинский диагноз в тайне как при жизни, так и после нее³⁶³. Приведённая позиция Суда позволяет сделать вывод о том, что врачебная тайна как особый правовой режим информации относится к тому человеку, которого она касается, и у нее есть особый порядок разглашения.

Диссертант в одной из своих научных публикаций отмечает, что личная, врачебная и профессиональная тайны в рамках изучаемой проблематики часто рассматриваются вместе, образуя комплекс серьезных правовых проблем. Профессиональная тайна может относиться к сведениям конфиденциального характера в различных сферах деятельности. Врачебная тайна, с другой стороны, характерна для медицинской практики и касается сведений пациента, при этом она, как подчеркивает А.А. Фатьянов, относится к «сфере профессиональных тайн, направленных на обеспечение защиты личной и семейной тайны граждан»³⁶⁴. Личная тайна, в свою очередь, связана с частной жизнью человека, его убеждениями и другими личными аспектами³⁶⁵.

Также врачебная тайна является специальным институтом, производным от права на неприкосновенность частной жизни. Врачебная тайна - конкретное проявление тайны частной жизни в сфере здравоохранения, поскольку объект врачебной тайны установлен более точно - это акты обращения пациентов к врачу, диагноз, состояние здоровья, иная информация пациента, полученная при обследовании и лечении (включая личные сведения, сообщенные врачу), а не просто любые сведения о частной жизни лица (личные, семейные, переписка и т.д.), не подлежащие разглашению без согласия.

³⁶³ Постановление Конституционного Суда Российской Федерации № 1-П от 13 января 2020 "По делу о проверке конституционности части первой статьи 111 и части первой статьи 112 Уголовного кодекса Российской Федерации, а также пункта 3 Правил определения степени тяжести вреда, причиненного здоровью человека, в связи с жалобой гражданина Б." // "Собрание законодательства РФ ", 22.01.2024, № 4, ст. 591.

³⁶⁴ *Фатьянов А.А.* Проблемы защиты конфиденциальной информации, не составляющей государственную тайну // Информационное общество. 1997. № 1. С. 49 - 56

³⁶⁵ *Федотов Н. Е.* Отдельные аспекты защиты врачебной тайны при использовании телемедицинских технологий в здравоохранении. Сравнительное конституционное обозрение // Сравнительное конституционное обозрение. 2024. №. 1. С. 40-59.

В следующем параграфе будет затронут вопрос соотношения тайны частной жизни и защиты персональных данных, а также будут рассмотрены создаваемые информационными технологиями риски для тайны частной жизни, в том числе и проблемы конфиденциальности персональных данных в здравоохранении при использовании информационных технологий.

Передача данных пациента с помощью телемедицинских устройств происходит через поставщика телемедицинских услуг, что может повлечь за собой раскрытие врачебной тайны. Личная информация о пациентах может оказаться на незащищённых устройствах или в облачных хранилищах, которые не обеспечены достаточными мерами защиты. Персональные медицинские данные могут оказаться в свободном доступе также в результате использования информационных систем, предназначенных для удаленного мониторинга состояния здоровья пациента.

В таких случаях злоумышленники могут получить доступ к этой информации и использовать её во вред пациенту. В итоге это может привести к негативным последствиям, таким, например, как утечка конфиденциальной интимной информации о здоровье пациента, которую бы он не хотел разглашать.

В доктрине отмечается, что одним из пробелов в обеспечении конфиденциальности медицинских данных, полученных при использовании телемедицинских услуг, является отсутствие закреплённого принципа соблюдения врачебной тайны при обращении к телемедицинским технологиям «в целях обеспечения конфиденциальности сведений, полученных и (или) разработанных субъектом, участвующим в предоставлении телемедицинских услуг в рамках медицинской деятельности»³⁶⁶.

Действительно, в положениях Порядка организации и оказания медицинской помощи с применением телемедицинских технологий, утверждённого приказом Минздрава России от 11 апреля 2025 г. № 193н, отсутствует важный принцип

³⁶⁶ Буланова В.С. Правовое обеспечение телемедицинских услуг и цифровая трансформация: теоретико-методологические вопросы // Мониторинг правоприменения. 2021. № 2 (39). С. 5964.

сохранения врачебной тайны, который предполагает, что коммуникация между пациентом и врачом, связанная с раскрытием конфиденциальных сведений, носит доверительный характер³⁶⁷. Любой представитель медицинской организации, допущенный к подобной информации, несет обязательство по соблюдению правил, направленных на защиту персональных данных пациентов.

Установление данного принципа позволит обеспечить баланс интересов субъектов телемедицинских услуг и корректные отношения между врачом и пациентом, которые будут способствовать уменьшению случаев компрометации личной информации пациентов со стороны медицинских сотрудников во время проведения телемедицинских консультаций.

Следовательно, законодательство Российской Федерации на данный момент не предусматривает, каким образом должна соблюдаться врачебная тайна при передаче персональной информации пациентов врачу в случае использования телемедицинских технологий.

Полагаем, что для решения данной проблемы целесообразно внести изменения в вышеуказанный приказ Минздрава России и установить требования и стандарты безопасности технологий, используемых для проведения телемедицинских консультаций. Кроме того, в данном приказе для поставщиков медицинских услуг, предоставляющих с помощью телемедицинских технологий медицинскую помощь, необходимо закрепить нормы о соблюдении требований конфиденциальности данных, включая уведомление пациентов о том, как будет обрабатываться их защищённая медицинская информация, а также информация об их правах в отношении обработки такой информации. В качестве основы могут послужить положения ранее рассмотренного в разделе 3.3. параграфа 3 главы 1 исследования постановления Правительства Германии по применению цифровых технологий в здравоохранении (DiGAV), раздел 2 которого содержит требования к

³⁶⁷ Приказ Минздрава России от 11 апреля 2025 г. № 193н «Об утверждении Порядка организации и оказания медицинской помощи с применением телемедицинских технологий». URL: <http://publication.pravo.gov.ru/document/0001202505150033> (дата обращения: 28.11.2025)

безопасности, функциональности, конфиденциальности и безопасности информации, а также к качеству приложений для цифрового здравоохранения³⁶⁸.

Таким образом, на основе проведенного в этой части параграфа анализа отечественного правового регулирования применения телемедицинских технологий можно сделать следующий вывод.

В настоящее время проблема сохранения врачебной тайны и обеспечения информационной безопасности в целях защиты персональных данных при использовании информационных технологий, в том числе телемедицинских, остается актуальной. В законодательстве Российской Федерации не предусмотрено, каким образом должна соблюдаться врачебная тайна при передаче персональной информации пациентов врачу в случае использования телемедицинских технологий. Целесообразным представляется внесение соответствующих изменений в отечественное законодательство для решения данной проблемы и определения необходимых мер, которые позволят обеспечить безопасное применение телемедицинских технологий врачами для оказания качественной медицинской помощи пациентам, на примере опыта Германии.

§ 3. Проблемы реализации отдельных конституционных прав человека в России в условиях применения информационных технологий в здравоохранении

Рассмотрев подробно российское правовое регулирование применения технологий обработки первичных данных, технологий анализа больших данных, технологий Интернета вещей, технологий искусственного интеллекта и телемедицинских технологий и выявив соответствующие пробелы, можно отметить, что все они также непосредственно влияют на реализацию

³⁶⁸ Verordnung über das Verfahren und die Anforderungen zur Prüfung der Erstattungsfähigkeit digitaler Gesundheitsanwendungen in der gesetzlichen Krankenversicherung (Digitale Gesundheitsanwendungen-Verordnung - DiGAV). URL: <https://www.gesetze-im-internet.de/digav/BJNR076800020.html> (дата обращения: 28.11.2024)

конституционных прав российских граждан. В этой связи необходимо рассмотреть наиболее важные современные проблемы реализации отдельных конституционных прав в условиях применения вышеуказанных информационных технологий в отечественном здравоохранении.

Использование информационных технологий стало частью государственной политики в России. В соответствии с пунктом 57 Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 2 июля 2021 г. № 400, достижение цели обеспечения информационной безопасности осуществляется путем реализации государственной политики, направленной на обеспечение защиты конституционных прав и свобод человека и гражданина при обработке персональных данных, в том числе с использованием информационных технологий³⁶⁹.

Задача Российской Федерации заключается в создании всех необходимых правовых условий и гарантий, в числе которых упоминается комплексное, систематизированное и непротиворечивое регулирование общественных отношений, складывающихся по вопросам использования информации и информационных технологий, гарантирующее реализацию прав на доступ к информации, на охрану здоровья и медицинскую помощь, на неприкосновенность частной жизни и создающее условия для развития и внедрения информационных технологий.

Рассматривая реализацию прав и свобод человека в условиях развития информационных технологий, Я.К. Чепенко указывает, что информатизация общества несет не только блага, но и негативные последствия для прав человека³⁷⁰.

³⁶⁹ Указ Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // "Собрание законодательства РФ", 05.07.2021, № 27 (часть II), ст. 5351.

³⁷⁰ Чепенко Я.К. Механизм реализации прав и свобод человека и гражданина в условиях развития современных информационных технологий // Исторический путь России: из прошлого в будущее: Мат-лы Междунар. науч. конф., посвященной 800-летию со дня рождения великого князя Александра Невского: В 3 т. / Под ред. С.И. Бугашева, А.С. Минина. Т. 1. СПб.: Санкт-

И.В. Гончаров аналогично отмечал, что использование цифровых технологий при реализации прав человека не всегда дает позитивный эффект³⁷¹. Оценивая защиту прав человека, Ю.А. Чернышева справедливо подчеркивает тот факт, что в России отсутствует концепция противодействия посягательствам на права человека в условиях информационного общества³⁷².

Следовательно, с учетом текущей ситуации в правовом поле и распространением политики цифровизации под угрозой могут оказаться различные права граждан. Иначе говоря, использование информационных технологий в здравоохранении порождает различные проблемы в сфере прав человека.

Их применение может нарушать несколько основных прав. К числу прав, которые будут рассмотрены в рамках настоящего исследования, относятся: конституционное право на охрану здоровья и медицинскую помощь (ст. 41 Конституции Российской Федерации), право на неприкосновенность частной жизни (ст. 23 Конституции Российской Федерации), право на доступ к информации (часть 2 ст. 24 Конституции Российской Федерации). Выбор указанных прав обусловлен наличием рассмотренной в параграфе 3 главы 1 исследования общей проблематики зарубежных стран и России, связанной с влиянием информационных технологий на права на неприкосновенность частной жизни, права на доступ к медицинским технологиям и права на наивысший достижимый уровень здоровья граждан, которые изначально были закреплены в международных стандартах и были впоследствии установлены в конституциях многих стран в различных формулировках и получили свое развитие в отраслевом и межотраслевом национальном законодательстве.

В дополнение к вышесказанному стоит обратить внимание на содержание положений, содержащихся в Концепции информационной безопасности в сфере

Петербургский государственный университет промышленных технологий и дизайна, 2021. С. 645 – 649.

³⁷¹ Гончаров И. В. Современные подходы к реализации прав человека в условиях цифровизации общественных отношений // Вестник Университета имени О.Е. Кутафина. 2019. №. 9 (61). С. 97-102.

³⁷² Чернышева Ю.А. Права человека в условиях цифровизации общества // Психология и право. 2019. Т. 9. № 4. С. 90 - 102.

здравоохранения, утвержденной протоколом президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 10.03.2022 № 7. По результатам анализа применения информационных технологий в сфере здравоохранения, проектов по цифровизации здравоохранения, а также основных типов угроз безопасности информации в информационных системах в сфере здравоохранения в данном системообразующем документе был выделен ряд следующих негативных последствий, связанных с реализацией угроз безопасности, имеющих критически опасный характер с учетом специфики сферы здравоохранения:

1. Невозможность точного определения диагноза и назначения лечения, а также невозможность обеспечения преемственности оказания медицинской помощи (*ошибочные результаты диагностических исследований, проводимых с помощью информационных систем и (или) автоматизированных систем управления технологическим процессом*). Указанные проблемы относятся к риску нарушения права на охрану здоровья и медицинскую помощь при использовании информационных технологий, например технологий искусственного интеллекта.

2. Невозможность предоставления медицинских услуг и оказания медицинской помощи (*недоступность (блокировка), длительные прерывания, нарушения штатного функционирования работы информационных систем в сфере здравоохранения, а также автоматизированных систем управления технологическим процессом, эксплуатируемых организациями в сфере здравоохранения*). Указанные проблемы относятся к риску нарушения права на доступ к информации при использовании информационных технологий, а именно технологий обработки первичных данных и анализа больших данных.

3. Неправомерное использование конфиденциальной информации, обрабатываемой в информационных системах в сфере здравоохранения (*разглашение персональных данных граждан, включая специальную категорию персональных данных; разглашение сведений, составляющих врачебную тайну;*

разглашение сведений конфиденциального характера; нарушение неприкосновенности частной жизни)³⁷³. Указанные проблемы относятся к риску нарушения права на неприкосновенность частной жизни при использовании информационных технологий, в частности технологий Интернета вещей и телемедицинских технологий.

Проблематика нарушений указанных прав отличается значительной сложностью. Например, объем защиты, предоставляемый правом, может быть не окончательно определен законодательством и доктриной, что затрудняет оценку того, нарушено ли право. Права могут быть нарушены в разной степени. Если та или иная технология нарушает конституционное право гражданина, то такое нарушение в связи с использованием цифровых технологий может быть сочтено еще более серьезным при определенных обстоятельствах (причинение вреда здоровью пациенту в результате применения врачом искусственного интеллекта). Выделяется и множество других интересных для науки постановок вопроса. Однако в силу ограниченности объема работы обратимся далее лишь к наиболее актуальным в настоящее время с практической точки зрения аспектам реализации указанных выше конституционных прав российских граждан.

3.1. Конституционное право на охрану здоровья и медицинскую помощь

В России право на охрану здоровья и медицинскую помощь в настоящее время реализуется в условиях активной цифровизации в сфере здравоохранения³⁷⁴. Согласно ст. 41 Конституции Российской Федерации каждый имеет право на

³⁷³ Протокол Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 10.03.2022 № 7 «Об утверждении концепции информационной безопасности в сфере здравоохранения». URL: <https://regulhub.kaspersky.ru/upload/iblock/86f/0x0rk2olahwno02qxyw7sn6c6anrbj7g.pdf> (дата обращения: 28.01.2025)

³⁷⁴ Комарова В. В. Социальная государственность России и право на охрану здоровья, медицинскую помощь // Право и государство: теория и практика. 2014. № 2(110). С. 32-38.

охрану здоровья и медицинскую помощь³⁷⁵. Данное право должно обеспечиваться оказанием доступной и качественной медицинской помощи, которая все больше начинает оказываться пациентам с применением информационных технологий.

Внедрение информационных технологий в здравоохранение должно соответствовать праву на наивысший достижимый уровень здоровья, о чем говорилось в параграфе 2 главы 1 исследования.

Согласно международным стандартам, информационные технологии в здравоохранении должны стать шагом к поддержке государствами реализации права на охрану здоровья и медицинскую помощь, что означает: медицинские услуги должны быть приемлемыми для всех и качественными.

Несомненно, информационные технологии оказывают позитивное влияние на реализацию права на охрану здоровья и медицинскую помощь. Применение информационных технологий приводит к снижению количества ошибок, уменьшает бумажную работу для врачей, автоматизирует рутинные задачи, такие как оформление документов, запись на прием, выписка рецептов, ускоряет обработку страховых случаев. Роботы могут использоваться для проведения операций, реабилитации, а также для ухода за пациентами, что повышает точность и эффективность медицинских процедур.

Тем не менее применение информационных технологий в здравоохранении создает необходимость изменения подходов к правовому регулированию отношений в области здравоохранения.

Использование информационных технологий в качестве основной системы или стратегии в сфере здравоохранения может повлиять на доступность и непреднамеренно усугубить неравенство граждан, способствуя цифровому разрыву среди населения. Возникает вопрос: не нарушается в таком случае принцип равной доступности медицинской помощи?

³⁷⁵ Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // «Российская газета», № 237 (853).

О.В. Фадеева провела исследование деятельности 3323 медицинских организаций (44,7 % от числа проверенных) и выявила 4252 нарушения прав граждан в сфере охраны здоровья, в том числе:

низкая доступность и качество медицинской помощи – 2029 случаев;
медицинское вмешательство без получения добровольного информированного согласия гражданина – 1118 случаев;

нарушение права на медицинскую помощь в гарантированном объеме, оказываемую без взимания платы в соответствии с программой государственных гарантий бесплатного оказания гражданам медицинской помощи – 555 случаев;

отказ в оказании медицинской помощи – 446 случаев;

отказ в предоставлении информации о состоянии здоровья – 40 случаев;

непредоставление информации о факторах, влияющих на здоровье – 41 случай;

нарушение права выбора врача и медицинской организации – 15 случаев;

несоблюдение врачебной тайны – 8 случаев³⁷⁶.

Таким образом, большое число данных проблем связано с применением информационных технологий, в частности по непредоставлению информации о факторах, влияющих на здоровье.

Статистика демонстрирует широкий спектр нарушений прав пациентов. Хотя прямая связь с информационными технологиями прослеживается не во всех случаях, сам масштаб проблем с доступностью и качеством помощи указывает на системные сбои, которые могут усугубляться при некорректном внедрении цифровых технологий, влияя на право на охрану здоровья и медицинскую помощь, а также на принцип равной доступности медицинской помощи, когда информация о состоянии здоровья не предоставляется.

³⁷⁶ Фадеева О. В. Проблемы реализации права граждан на охрану здоровья и медицинскую помощь, гарантированного ст. 41 Конституции Российской Федерации // Вестник Кемеровского государственного университета. Серия: Гуманитарные и общественные науки. 2019. Т. 3. №. 1 (9). С. 97-103.

Более того, в связи с тем, что было выявлено 2029 случаев низкой доступности и качества медицинской помощи, что является самым большим по количеству зафиксированных случаев в приведенной статистической подборке, мы приходим к выводу, что проблема оказания некачественной медицинской помощи является наиболее важной из числа актуальных проблем, связанных с влиянием информационных технологий на реализацию права на охрану здоровья и медицинскую помощь в России.

Проблема некачественного оказания медицинской помощи с использованием информационных технологий приводит к фактическому или потенциальному вреду для пациента, что было зафиксировано учеными в различных исследованиях, как российских, так и зарубежных³⁷⁷.

К примеру, среди инцидентов, раскрытых в зарубежных исследованиях, зафиксированы случаи смерти пациентов, которые связаны с неправильной идентификацией пациента, невыполнением лечения, неправильной процедурой из-за ошибок в использовании программного обеспечения, передозировкой из-за плохой функциональности программного обеспечения³⁷⁸.

Также в другом исследовании отмечается, что случаи смерти пациента связаны с невозможностью лечения из-за ошибок в использовании программного обеспечения, задержкой лечения после госпитализации, поскольку ожидаемые

³⁷⁷ *Magrabi, F., Baker, M., Sinha, I., Ong, M. S., Harrison, S., Kidd, M. R., ... & Coiera, E.* (2015). Clinical safety of England's national programme for IT: a retrospective analysis of all reported safety events 2005 to 2011. *International journal of medical informatics*, 84(3), pp. 198-206; *Cheung, K. C., van der Veen, W., Bouvy, M. L., Wensing, M., van den Bemt, P. M., & de Smet, P. A.* (2014). Classification of medication incidents associated with information technology. *Journal of the American Medical Informatics Association*, 21(e1), pp. 63-70 и др.

³⁷⁸ *Magrabi, F., Ong, M. S., Runciman, W., & Coiera, E.* (2011). Patient safety problems associated with healthcare information technology: an analysis of adverse events reported to the US Food and Drug Administration. In *AMIA Annual Symposium Proceedings*. Vol. 2011, P. 853; *Magrabi, F., Ong, M. S., Runciman, W., & Coiera, E.* (2012). Using FDA reports to inform a classification for health information technology safety problems. *Journal of the American Medical Informatics Association*, 19(1), pp. 45-53.

результаты теста из предыдущей госпитализации не были видны соответствующим врачам³⁷⁹.

Ошибки при использовании, мешающие получению информации о пациенте, были отмечены в большинстве указанных исследований и обычно связаны с плохим обучением и незнанием информационной системы. Плохой пользовательский интерфейс также способствовал возникновению ошибок при ее использовании, а иногда их усугубляли машинные ошибки. Например, врачи игнорировали все предупреждения со стороны программного обеспечения³⁸⁰, учитывая количество предупреждений и чрезмерное оповещение об ошибке, также имели место случаи использования информационной системы, связанные с ошибочным отклонением предупреждений.

Доступность и качество медицинской помощи являются элементами права на охрану здоровья, а также принципами охраны здоровья, закрепленными в ст. 4 Федерального закона от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации». Более того, в пункте 21 ст. 2 данного Федерального закона установлены критерии качества медицинской помощи: «правильность выбора методов профилактики, диагностики, лечения и реабилитации при оказании медицинской помощи, степень достижения запланированного результата»³⁸¹.

Как отметил И.В. Тимофеев: «доступность и качество медицинской помощи затрагивают само существо соответствующего конституционного права, поскольку непосредственно касаются того социального блага, которое опосредуется

³⁷⁹ *Magrabi, F., Baker, M., Sinha, I., Ong, M. S., Harrison, S., Kidd, M. R., ... & Coiera, E.* (2015). Clinical safety of England's national programme for IT: a retrospective analysis of all reported safety events 2005 to 2011. *International journal of medical informatics*, 84(3), pp. 198-206.

³⁸⁰ *Meeks, D. W., Smith, M. W., Taylor, L., Sittig, D. F., Scott, J. M., & Singh, H.* (2014). An analysis of electronic health record-related patient safety concerns. *Journal of the American Medical Informatics Association*, 21(6), pp. 1053-1059; *Ash, J. S., Berg, M., & Coiera, E.* (2004). Some unintended consequences of information technology in health care: the nature of patient care information system-related errors. *Journal of the American Medical Informatics Association*, 11(2), pp. 104-112.

³⁸¹ Федеральный закон от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» // «Собрание законодательства РФ», 28.11.2011, № 48, ст. 6724.

конституционными нормами»³⁸². А.А. Громова под качественной медицинской помощью понимает «совокупность характеристик медицинской помощи с учетом целенаправленности такой помощи, уровня ее оказания, а также степени позитивного влияния на здоровье человека и гражданина»³⁸³. Вышеуказанные позиции ученых подчеркивают тот факт, что некачественно оказанная медицинская помощь негативно отражается на человеке и приводит к возникновению существенного вреда здоровью пациента, вплоть до летального исхода.

Более того, право на охрану здоровья и медицинскую помощь, по мнению В.В. Власенковой, предполагает требование пациентом от врачей и других медицинских работников предоставления квалифицированной медицинской помощи, проведения диагностических исследований³⁸⁴.

Врач обязан оказать медицинскую помощь надлежащим образом и верно поставить диагноз пациенту, в особенности если для этого был использован искусственный интеллект. Поэтому проблема некачественного оказания медицинской помощи распространяется и на информационные технологии.

Любые информационные технологии влияют на право на охрану здоровья и медицинскую помощь, когда применяются в здравоохранении, однако в большей мере в настоящее время именно технологии искусственного интеллекта используются чаще всего в здравоохранении в силу их популяризации и повсеместного распространения.

В научной доктрине значительное внимание уделяется проблемам нарушения конституционных прав граждан именно при применении

³⁸² Тимофеев И. В. К вопросу о содержании права на охрану здоровья и медицинскую помощь в конституционно-правовом аспекте // Ученые записки юридического факультета. 2015. № 39(49). С. 109-115.

³⁸³ Громова А. А. Реализация конституционного права на медицинскую помощь в Российской Федерации // Проблемы права. 2022. № 4(87). С. 59-63.

³⁸⁴ Власенкова В. В. Право на охрану здоровья и медицинскую помощь в Российской Федерации: Автореф. дис.....канд. юрид. наук 12.00.05. Власенкова Вероника Викторовна. - М., 2007. 21 с.

искусственного интеллекта³⁸⁵, поэтому целесообразно в рамках исследования более пристально в настоящем разделе рассмотреть вопрос о проблемах использования искусственного интеллекта при реализации права на охрану здоровья и медицинскую помощь.

Рассмотрим данный вопрос в связи с применением искусственного интеллекта врачом. Какие новые вызовы применение искусственного интеллекта создает в здравоохранении для реализации конституционного права на охрану здоровья?

Если медицинские работники при принятии решений о вариантах лечения пациента будут опираться на ошибочные результаты диагностики, предложенные алгоритмами искусственного интеллекта, и не проверят, не убедятся в их правильности, то это создает системную проблему, приводящую к некачественному оказанию медицинской помощи и создающую реальную угрозу причинения вреда здоровью пациентов.

Одним из главных факторов существования проблемы, связанной с некачественным оказанием медицинской помощи при применении искусственного интеллекта, можно признать отсутствие информированности пациента о его использовании врачом. Критерии информированности пациента предполагают, что он заранее должен получить информацию о цели и характере медицинского вмешательства, а также о его последствиях и рисках. Решение пациент должен принять до момента медицинского вмешательства.

В условиях развития цифровизации, искусственный интеллект все чаще стал использоваться врачами при оказании пациенту медицинской помощи. Однако врачи часто не информируют пациента о применении искусственного интеллекта, что противоречит принципу получения информированного добровольного согласия в целях соблюдения интересов пациента. В результате чего и возникают

³⁸⁵ *Stoica, A. A. (2025). Artificial Intelligence and the Fundamental Constitutional Rights and Freedoms. Legis. Info. Bull., pp. 30; H., Subramanian; Kansal, Shivamm. (2023). Artificial Intelligence and Constitutional Rights: Assessing an Imaginable Unimaginable Future. LawFoyer Int'l J. Doctrinal Legal Rsch., 1, pp. 98.*

вышеуказанные случаи неинформирования, которую Т.А. Ковелина, А.В. Собянин и В.М. Марухно характеризуют как проблему «включения сведений в информированное добровольное согласие пациента о медицинском вмешательстве с помощью искусственного интеллекта»³⁸⁶.

Прежде чем проанализировать названную проблему, стоит отметить следующее. Мы придерживаемся позиции тех ученых, которые считают, что право на информированность отличается от права на информацию, выражающегося в том, что это право, активное по своей направленности, напрямую связано с инициативными действиями самого субъекта. Упомянутые действия могут выражаться в поиске, получении, передаче, распространении сведений, а информированность носит пассивный характер и зависит от воли другого лица (врача). Данный подход разделяет, в частности, Р.А. Осипов, указывающий, что право на информирование имеет пассивный, «выжидательный» характер, а его реализация во многом зависит от действий противоположного субъекта³⁸⁷. Поэтому в исследовании рассматривается проблема информированности пациента об использовании искусственного интеллекта в рамках права на охрану здоровья и медицинскую помощь.

При этом стоит учесть, что рассматриваемая проблема имеет тесную связь с правом на доступ к информации, поскольку последний означает, что пациенты могут осуществлять своё право на выбор работников здравоохранения, предоставляющих лечение или консультацию, место проведения лечения или получения консультаций, а также методов лечения. После получения информации о возможных вариантах пациент имеет право дать своё согласие на медицинское вмешательство.

³⁸⁶ Ковелина Т.А., Собянин А.В., Марухно В.М. К вопросу о правовом регулировании применения искусственного интеллекта в медицине // Гуманитарные, социально-экономические и общественные науки. 2022. № 2. С. 149.

³⁸⁷ Осипов Р. А. Право на информированность: понятие и соотношение с правом на информацию // Вестник Саратовской государственной юридической академии. 2016. №. 3 (110). С. 163-167.

Актуальность данной проблемы подтверждается практикой. Согласно статистике, только в Москве врачи московских поликлиник поставили более 17 миллионов диагнозов с помощью искусственного интеллекта, который анализирует данные пациента, результаты исследований, а также подтверждает или предлагает альтернативный диагноз³⁸⁸.

Указанная проблема актуальна не только для России, но и обсуждается в США. Так, ряд ученых на основании проведенного исследования в США установили, что пациентов не информируют и не просят дать согласие на использование искусственного интеллекта в их лечении³⁸⁹.

Отсутствие раскрытия информации об его применении может привести к тому, что пациенты могут быть никогда не проинформированы о любых ошибках, допущенных какой-либо моделью искусственного интеллекта, а это является одной из причин, по которым они могут быть лишены необходимой помощи или подвергнуты ненужным, дорогостоящим или даже вредным вмешательствам. Упоминание в информированном согласии искусственного интеллекта, который применяется в лечении пациента, повлияет на его решение о медицинском вмешательстве, так как в рамках информированного добровольного согласия пациент получает от врача необходимые сведения о здоровье, рисках, связанных с вмешательством, характере самого вмешательства и его последствиях.

В другом исследовании, проведенным П. Эсмаилзаде, Т. Мирзаем и С. Дхараникотой, установлено, что пациенты с острыми заболеваниями чаще беспокоились о вопросах ответственности в сценариях как чисто клинического применения искусственного интеллекта, так и взаимодействия искусственного интеллекта с врачом, а также были обеспокоены использованием услуг, основанных исключительно на искусственном интеллекте и искусственного

³⁸⁸ Врачи московских поликлиник поставили более 17 миллионов диагнозов с помощью искусственного интеллекта. URL <https://www.mos.ru/news/item/145399073/> (дата обращения: 23.01.2024).

³⁸⁹ An invisible hand: Patients aren't being told about the AI systems advising their care. URL: <https://www.statnews.com/2020/07/15/artificial-intelligence-patient-consent-hospitals/> (дата обращения: 23.01.2024).

интеллекта-приложения под непосредственным руководством врачей³⁹⁰. Это свидетельствует о том, что люди с хроническими заболеваниями могут быть более склонны доверять прямому взаимодействию пациента и врача для контроля и лечения своих симптомов, поэтому врачам следует оценивать соответствующие риски при использовании искусственного интеллекта при лечении пациентов. Отсутствие информирования пациента о применении искусственного интеллекта при оказании медицинской помощи связано с доктриной информированного добровольного согласия. Речь идет о применении информационных технологий в самой процедуре лечения пациента. При этом неясно, когда врачи должны сообщать пациентам о том, что в принятии решения о назначении лечения участвовал искусственный интеллект. Если считать, что такое уведомление пациента уместно, то насколько подробно они должны рассказывать о рекомендациях искусственного интеллекта и о том, как врач принял решение о назначении лечения и постановке диагноза с учетом таких рекомендаций? Пациентам также могут не рассказывать о том, что в процессе оказания медицинской помощи применяется искусственный интеллект в качестве инструмента для медицинского вмешательства, а не для постановки диагноза.

Для решения соответствующей проблемы необходимо проанализировать доктрину информированного согласия. Это позволит определить, может ли такое согласие включать информацию об использовании искусственного интеллекта.

В соответствии со ст. 20 Федерального закона от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» информированное добровольное согласие гражданина на медицинское вмешательство дается «на основании предоставленной медицинским работником в доступной форме полной информации о целях, методах оказания медицинской помощи, связанном с ними риске, возможных вариантах медицинского вмешательства, о его последствиях, а также о предполагаемых результатах

³⁹⁰ *Esmailzadeh, P., Mirzaei, T., & Dharanikota, S. (2021). Patients' perceptions toward human-artificial intelligence interaction in health care: experimental study. Journal of medical Internet research, 23(11), pp 1-21.*

оказания медицинской помощи»³⁹¹. Важно, что пациент имеет право получить в доступной для него форме имеющуюся в медицинской организации указанную выше информацию.

Анализ данной нормы позволяет выделить следующие признаки информированного добровольного согласия, а именно доступность, осведомленность и добровольность, которые проявляются при даче согласия пациента на определенное медицинское вмешательство. Информированное добровольное согласие «обеспечивает юридическую чистоту события оказания медицинской помощи, давая пациенту понимание того, с чем он столкнется, а для врача и медицинского учреждения — верифицируя данное понимание»³⁹².

Законодательство России предусматривает использование информационных технологий в здравоохранении. Например, как установлено в Федеральном законе от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», «специализированная медицинская помощь включает в себя профилактику, диагностику и лечение заболеваний и состояний, требующих использования специальных методов и сложных медицинских технологий»³⁹³.

При этом высокотехнологичная медицинская помощь, которая является частью специализированной медицинской помощи, «включает в себя применение новых сложных и (или) уникальных методов лечения, а также ресурсоемких методов лечения с научно доказанной эффективностью, в том числе клеточных технологий, роботизированной техники, информационных технологий...»³⁹⁴. Авторы также подтверждают, что информационные технологии внедрены в здравоохранение и предусмотрены законодательством, например, М.А.

³⁹¹ Федеральный закон от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» // «Собрание законодательства РФ», 28.11.2011, № 48, ст. 6724.

³⁹² *Алексеева С.С., Стародубцев М. Э.* Информированное добровольное согласие на медицинское вмешательство: фигура и роль врача // Российский кардиологический журнал. 2021. № 9. С. 69.

³⁹³ Федеральный закон от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» // «Собрание законодательства РФ», 28.11.2011, № 48, ст. 6724.

³⁹⁴ Там же.

Липчанская и Т.В. Заметина относят к высокотехнологичной медицинской помощи системы искусственного интеллекта³⁹⁵.

Из вышесказанного можно сделать вывод, что пациент имеет право принять предложенное лечение или отказаться от него на основании предоставленной информации и дать соответствующее информированное согласие на медицинское вмешательство, осуществляемое с использованием информационных технологий. Классическая доктрина информированного согласия, закрепленная в ст. 20 Федерального закона от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», не была адаптирована к эпохе алгоритмического принятия решений. В результате этого возникла правовая неопределенность: порождает ли использование искусственного интеллекта новые, специфические риски, о которых врач обязан сообщить?

В зарубежных странах в настоящее время доктрина информированного согласия включает в себя принцип, ориентированный на автономию личности, и требует, чтобы при обсуждении лечения врач раскрывал такие риски, которые пациент ожидал бы узнать в определенной ситуации. Т. Бошам считает, что данный принцип предполагает, что сознательные пациенты, обладающие способностью принимать разумные решения, вправе принимать их относительно собственного медицинского ухода³⁹⁶.

Современные условия в области развития информационных технологий привели к тому, что сейчас значительное внимание уделяется праву человека на охрану здоровья и медицинскую помощь. Однако до недавнего времени принципу автономии личности не уделялось должного внимания также, как и необходимости усиления потенциала личности (пациента) в принятии решений по отношению к патерналистской системе.

³⁹⁵ Липчанская М. А., Заметина Т. В. Социальные права граждан в условиях использования искусственного интеллекта: правовые основы и пробелы законодательного регулирования в России // Журнал российского права. 2020. № 11. С. 78-96.

³⁹⁶ Beauchamp T.L., Childress J.F. Principles of Biomedical Ethics // 5th ed. New York. NY: Oxford University Press. 2001. P. 454.

Принцип автономии личности в сфере здравоохранения подразумевает, что пациент имеет право на информированный выбор относительно своего лечения. Как отмечает Э.В. Барбашина, автономия пациента предполагает самостоятельность в принятии решений, их дальнейшую реализацию в соответствии с жизненными планами и целями пациента. Врач обязан предоставить объективную и полную информацию для того, чтобы пациент принял решение. После этого задача врача - выполнять решение пациента³⁹⁷.

Запрет на неправомерное вмешательство в автономию личности необходим для обеспечения среды, которая способствует полноценному развитию личности и установлению демократического устройства в обществе, что неоднократно отмечал Конституционный Суд Российской Федерации³⁹⁸. Тем самым принцип индивидуальной автономии возлагает на государство позитивную обязанность: обеспечивать каждому человеку реальные шансы на свободное самопроявление и самоопределение³⁹⁹.

Также согласимся с мнением А.А. Троицкой, отметившей, что автономия пациента может возникнуть и проявить себя лишь по итогам целого ряда корректных действий, совершённых врачами, которые в свою очередь нуждаются в адекватной их задачам организации труда, что предполагает позитивные действия органов публичной власти⁴⁰⁰. А в части регулирования применения информационных технологий в сфере здравоохранения может произойти

³⁹⁷ Барбашина Э. В. Принцип автономии пациента: возможное и действительное // Вестник Томского государственного университета. 2019. №. 449. С. 64-70.

³⁹⁸ Постановление Конституционного Суда Российской Федерации от 22.03.2005 № 4-П «По делу о проверке конституционности ряда положений Уголовно-процессуального кодекса Российской Федерации, регламентирующих порядок и сроки применения в качестве меры пресечения заключения под стражу на стадиях уголовного судопроизводства, следующих за окончанием предварительного расследования и направлением уголовного дела в суд, в связи с жалобами ряда граждан» // «Российская газета», № 66, 01.04.2005.

³⁹⁹ Постановление Конституционного Суда Российской Федерации от 23.09.2014 № 24-П «По делу о проверке конституционности части 1 статьи 6.21 Кодекса Российской Федерации об административных правонарушениях в связи с жалобой граждан Н.А. Алексева, Я.Н. Евтушенко и Д.А. Исакова» // «Российская газета», № 226, 03.10.2014.

⁴⁰⁰ Троицкая А.А. Автономия личности как принцип оказания медицинской помощи: между патернализмом и (мнимой) свободой выбора // Сравнительное конституционное обозрение. Т.33. 2024. №1(158). С.25–39.

установление чрезмерных ограничений и контроля со стороны государственной власти, что приведет к нарушению принципа автономии пациента. В результате верно утверждение, что «цифровая среда может быть использована в различных целях государственными органами и государствами, в том числе и для «цифровой кабалы», а не «цифровой свободы»»⁴⁰¹.

В настоящее время автономия пациента включает в себя способность пациентов обладать контрольной информацией относительно состояния своего здоровья, целей, методов оказания медицинской помощи, связанных с ними рисков в порядке их выбора⁴⁰². Поэтому принцип автономии пациента тесно связан с информированным добровольным согласием и включает в себя риски при выборе определенных методов лечения.

Кроме того, А.А. Шутова и И.Р. Бегишев справедливо отмечают, что «доктрина добровольного информирования согласия пациентов должна строиться на следующих принципах:

- предоставление достоверных сведений о медицинской манипуляции (вмешательстве);
- раскрытие объективных сведений о здоровье пациента и о его состоянии;
- добровольное согласие пациента;
- обеспечение информированного раскрытия информации;
- предоставление информации о соответствующих рисках и потенциально вредных последствиях»⁴⁰³.

Диссертантом в отдельной научной публикации проведено исследование зарубежной и российской судебной практики в части информированного добровольного согласия при использовании информационных технологий, по

⁴⁰¹ *Кравец И.А.* Цифровизация, право и конституция // Право цифровой среды: Монография / Под ред. Т.П. Подшивалова, Е.В. Титовой, Е.А. Громовой. М.: Общество с ограниченной ответственностью «Перспект», 2022. С. 185-200.

⁴⁰² *Юдин Е.В.* Принцип автономии пациента и право на информированное добровольное согласие при оказании медицинской помощи: некоторые правовые и биоэтические аспекты // Вопросы российского и международного права. 2021. Т. 11. № 1-1. С. 241.

⁴⁰³ *Шутова А. А., Бегишев И. Р.* Этические принципы создания и применения технологий искусственного интеллекта в здравоохранении // Правоприменение. 2024. Т. 8, № 1. С. 34-43.

итогах которого автор приходит к выводу, что современная доктрина информированного согласия в России, как и в зарубежных странах, в частности, в Великобритании основывается на автономии личности пациента⁴⁰⁴.

А.С. Белов задавался вопросом: информированное согласие предполагает участие пациента в принятии решения о выборе методов лечения, оценке рисков или же роль пациента сводится исключительно к согласию с тем, что предлагает ему врач?⁴⁰⁵.

Отвечая на указанный вопрос исследователя, подчеркнем, что если искусственный интеллект используется под руководством врача и тем самым не несет рисков для пациента, не вносит существенный вклад, то такой случай может расцениваться как незначительный для информирования пациента. Но если искусственный интеллект выполняет операции самостоятельно без участия человека или ставит диагноз пациенту, то в таком случае пациенты должны быть проинформированы об использовании искусственного интеллекта, поскольку это связано с различными проблемами.

Если искусственный интеллект не поддается объяснению, у медицинских работников могут возникнуть проблемы с предоставлением достаточной информации о причинах классификаций и предлагаемых методов лечения, чтобы пациенты могли осознанно принять решение и воспользоваться своим правом на автономию. Адекватное информирование пациента требует, чтобы врачи не только указывали на медицинскую пользу применения искусственного интеллекта, но и подчеркивали потенциальный риск, связанный с ней (при условии, что он является значимым с точки зрения его характера и вероятности). В противном случае решение пациента в пользу медицинского вмешательства будет односторонним и ущербным.

⁴⁰⁴ Федотов Н. Е. Отдельные конституционно-правовые аспекты оказания высокотехнологичной медицинской помощи с применением искусственного интеллекта // Конституционное и муниципальное право. 2024. № 11. С. 36-41.

⁴⁰⁵ Белов С. А. Автономия личности и врачебный патернализм // Юридический мир. 2023. № 4. С. 19-23

Кроме того, если мы не хотим получить вред от использования искусственного интеллекта в здравоохранении, он должен применяться для принятия оптимального решения на основе всей имеющейся информации о конкретном пациенте. Уровень риска или оптимальный вариант лечения могут зависеть от таких факторов, как возраст, пол или этническое происхождение. Если не принимать во внимание эти факторы, когда это возможно, это может привести к дискриминационным результатам, поскольку игнорируются известные (или неизвестные) факторы риска и уязвимые группы оказываются в невыгодном положении.

Существует реальная опасность того, что искусственный интеллект может обучаться и тестироваться на этически неприемлемом наборе данных или что в данных, используемых для разработки искусственного интеллекта, может присутствовать другая предвзятость. Также существуют опасения по поводу феномена «галлюцинаций» в искусственном интеллекте, когда он не может объяснить свои собственные рассуждения. Указанные факторы, в первую очередь непрозрачность алгоритмов и вытекающий из нее риск дискриминации, подрывают саму основу информированного согласия. Если врач в силу непонятности работы искусственного интеллекта не может предоставить пациенту адекватную информацию о рисках и обосновании предлагаемого лечения, то согласие, данное пациентом, не может считаться в полной мере информированным. Эту точку зрения разделяет А.Ю. Киселева, справедливо отмечая, что непрозрачность и автономность решений искусственного интеллекта затрудняет соблюдение требования получения информированного согласия пациента перед осуществлением медицинского вмешательства⁴⁰⁶.

Ключевым аспектом является то, что в научной доктрине авторы часто поднимают вопрос непрозрачности искусственного интеллекта, именуемый «черным ящиком» - непрозрачность и неподотчетность алгоритмов

⁴⁰⁶ Киселева А.Ю. Применение искусственного интеллекта в здравоохранении: аспекты медицинского права // Медицинское право: теория и практика. 2020. Т. 6. № 2(12). С. 30.

искусственного интеллекта⁴⁰⁷. Термин «черный ящик» используется для описания сложного и непрозрачного способа работы автономной системы искусственного интеллекта с технической точки зрения, а также связан с трудностями автономной системы в предоставлении подходящего объяснения о средствах и обосновании конкретного принятого ею решения на языке, понятном человеку⁴⁰⁸.

Эта проблема в здравоохранении связана с тем, что механизмы принятия решений искусственным интеллектом обычно непрозрачны и сложны для понимания врачами и пациентами.

Результатом данной проблемы в сфере здравоохранения является дискриминация искусственным интеллектом людей, которая была выявлена из-за случая применения алгоритмов для прогнозирования объема необходимой медицинской помощи. Данный вывод содержится в результатах исследования ряда авторов, которые установили, что «несмотря на единую методику расчета для всех пациентов, алгоритм считал чернокожего пациента менее нуждающимся в медицинской помощи, чем белого, даже если у первого больше объективных причин получить медпомощь. Это произошло в результате заложенной идеи о том, что расходы на медпомощь свидетельствуют об одинаковой потребности в ней, поэтому алгоритм рассчитывал рекомендации на основании расходов пациентов на медпомощь в прошлом»⁴⁰⁹.

Термин «прозрачность» указан в стратегии развития искусственного интеллекта в Российской Федерации, утвержденной Указом Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации», который означает «объяснимость работы

⁴⁰⁷ Кутейников Д. Л., Ижаев О. А., Зенин С. С., Лебедев В. А. Алгоритмическая прозрачность и подотчетность: правовые подходы к разрешению проблемы «черного ящика» // *Lex russica*. 2020. Т. 73. № 6. С. 139–148.

⁴⁰⁸ Zednik, C. (2021). Solving the black box problem: A normative framework for explainable artificial intelligence. *Philosophy & technology*, 34(2), pp. 265-288; Adadi, A., & Berrada, M. (2018). Peeking inside the black-box: a survey on explainable artificial intelligence (XAI). *IEEE access*, 6, pp. 52138-52160.

⁴⁰⁹ Харитонова Ю. С., Савина В. С., Паньини Ф. Предвзятость алгоритмов искусственного интеллекта: вопросы этики и права // *Вестник пермского университета. Юридические науки*. 2021. №. 53. С. 488-515.

искусственного интеллекта и процесса достижения им результатов, недискриминационный доступ пользователей продуктов, которые созданы с использованием технологий искусственного интеллекта, к информации о применяемых в этих продуктах алгоритмах работы искусственного интеллекта»⁴¹⁰. В Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года, утвержденной распоряжением Правительства Российской Федерации от 19 августа 2020 г. № 2129-р, проблема алгоритмической прозрачности систем искусственного интеллекта – «использование для принятия решений системами искусственного интеллекта вероятностных оценок и невозможность в ряде случаев полного объяснения принятого ими решения»⁴¹¹ - признается в качестве основного направления, где сохраняются существенные пробелы.

Иначе говоря, в законодательстве России еще не решена проблема прозрачности алгоритмов искусственного интеллекта. Согласимся с мнением ряда ученых в том, что автоматизированная обработка персональных данных, упоминаемая в положениях Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»⁴¹², «определяет не саму технологию, а процесс, т.е. означает только определенную деятельность. Алгоритмы же представляют собой не процесс, а технологию, применение которой и требует правового регулирования»⁴¹³. Более того, субъект персональных данных не будет знать, как именно было принято решение, поскольку ему может не быть предоставлена информация относительно логики принятого этого решения.

⁴¹⁰ Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» // «Собрание законодательства РФ», 14.10.2019, № 41, ст. 5700.

⁴¹¹ Распоряжение Правительства Российской Федерации от 19 августа 2020 г. № 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года» // "Собрание законодательства РФ", 31.08.2020, № 35, ст. 5593

⁴¹² Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // "Собрание законодательства РФ", 31.07.2006, № 31 (1 ч.), ст. 3451.

⁴¹³ Кутейников Д. Л., Ижаев О. А., Зенин С. С., Лебедев В. А. Алгоритмическая прозрачность и подотчетность: правовые подходы к разрешению проблемы «черного ящика» // Lex russica. 2020. Т. 73. № 6. С. 139–148.

Аналогичные пробелы содержатся в положениях ст. 10.2-2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»⁴¹⁴. Как отмечает А.Н. Мочалов, указанные нормы не предусматривают такого критерия, как понятность описания алгоритма, а также не позволяет пользователю отказаться от использования рекомендательной технологии или ограничить (отключить) использование в ней тех или иных характеристик, которые относятся к его личности⁴¹⁵. Под рекомендательной технологией в данной статье Федерального закона понимается «информационная технология предоставления информации на основе сбора, систематизации и анализа сведений, относящихся к предпочтениям пользователей сети «Интернет», находящихся на территории Российской Федерации»⁴¹⁶. Дополним: рекомендательные технологии относятся только к сети «Интернет», что следует из их определения, поэтому речь идет только об алгоритмах в данной информационной сети, что существенно ограничивает сферы действия алгоритмов искусственного интеллекта.

При этом в указанной статье не говорится об автоматизированной обработке персональных данных искусственным интеллектом, решение которого было принято по таким данным, которые не относятся к персональным.

Вышесказанное подтверждает тот факт, что граждане лишены права знать, как устроен алгоритм и на основе каких принципов работает искусственный интеллект, какие исходные данные используются при принятии им решений. И.А. Пибаяев и С.В. Симонова, подчеркнули, что в подобных условиях полноценное обеспечение прав человека возможно лишь в случае наделения граждан особыми правами, направленными на объяснение механизма и особенностей работы

⁴¹⁴ Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // «Собрание законодательства РФ», 31.07.2006, № 31 (1 ч.), ст. 3448

⁴¹⁵ Мочалов А.Н. Прозрачность алгоритмов как правовой принцип автоматизированной обработки данных о человеке // Юридические исследования. 2023. № 12. С. 77-88.

⁴¹⁶ Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // «Собрание законодательства РФ», 31.07.2006, № 31 (1 ч.), ст. 3448

используемых систем, именно на объяснение условий решения, в которых оно принималось, и его исходных данных⁴¹⁷.

Однако не все авторы согласны с тем, что необходимо человеку объяснять логику принятия решения искусственным интеллектом. Так, А.К. Жарова считает, что, если человек поймет его логику, он не сможет изменить алгоритм, поскольку это потребует пересмотра всего заложенного в него математического инструментария⁴¹⁸. Полагаем, в случае если человеку будет предоставлена информация относительно логики принятого решения искусственным интеллектом, то он сможет отказаться от его использования или ограничить его использование в той ситуации, которые относятся к его личности и затрагивают его права и свободы. Поэтому суть информированности человека в использовании искусственного интеллекта и решениях, принимаемым им, не заключается в изменении заложенного в него инструментария.

Также Ю.С. Харитоновна выражает мнение, что «риск необъяснимых предвзятых решений искусственного интеллекта нужно исключать путем обучения с подкреплением и аудита полученного результата, так как не видится целесообразности в юридической значимости раскрытия алгоритмов искусственного интеллекта»⁴¹⁹.

А.Н. Мочалов справедливо в противовес данному мнению указывает, что установление механизмов контроля и аудита в отношении алгоритмов и принимаемых ими решений не должно заменять или отменять действие принципа прозрачности, предполагающего объяснимость и понятность алгоритма пользователям, сведения о которых используются в работе такого алгоритма⁴²⁰.

⁴¹⁷ Пубаев И.А., Симонова С.В. Алгоритмы в механизме реализации конституционных прав и свобод: вызовы цифровой эпохи // Сравнительное конституционное обозрение. 2020. № 6(139). С. 31-50.

⁴¹⁸ Zharova, A. K. (2023). Achieving algorithmic transparency and managing risks of data security when making decisions without human interference: legal approaches. *Journal of Digital Technologies and Law*, 1(4), pp. 973-993.

⁴¹⁹ Харитоновна Ю.С. Правовые средства обеспечения принципа прозрачности искусственного интеллекта // *Journal of Digital Technologies and Law*. 2023. Т. 1. №. 2. С. 337-358.

⁴²⁰ Мочалов А.Н. Прозрачность алгоритмов как правовой принцип автоматизированной обработки данных о человеке // *Юридические исследования*. 2023. № 12. С. 77-88.

Кроме того, Ю.С. Харитонова относительно закрепления права на информированность применения технологии искусственного интеллекта при автоматизированной обработке данных для принятия решений высказывает отрицательную позицию, аргументируя тем, что «защита прав граждан не достигается, входя в противоречие с методами работы искусственного интеллекта, и прежде всего «черного ящика»»⁴²¹.

Не можем согласиться с данным утверждением, поскольку информированность о решениях, принимаемых искусственным интеллектом, предоставляет пострадавшему лицу право на получение четкой и содержательной информации о решении непосредственно от лица, принимающего решение, осуществление этой возможности не предполагает вступления в какое-либо судебное разбирательство. Право на осведомленность о применении технологии искусственного интеллекта применимо в тех ситуациях, где входные данные направлены не на персональные данные, а на другие данные, и в результате было принято решение искусственным интеллектом.

В качестве успешной правовой модели решения обозначенной проблемы прозрачности алгоритмов искусственного интеллекта может рассматриваться ранее рассмотренный Закон об искусственном интеллекте ЕС, в ст. 86 которого закреплено право на разъяснение индивидуальных решений, а в ст. 50 установлена обязанность проектирования искусственного интеллекта таким образом, чтобы можно было информировать пациентов о том, что они взаимодействуют с искусственным интеллектом⁴²². Право на информирование защищает право отдельных лиц быть свободными от произвольного использования алгоритмов

⁴²¹ Харитонова Ю.С. Правовые средства обеспечения принципа прозрачности искусственного интеллекта // *Journal of Digital Technologies and Law*. 2023. Т. 1. №. 2. С. 337-358

⁴²² Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng> (дата обращения: 28.11.2024)

искусственного интеллекта⁴²³. Кроме того, Закон о защите прав потребителей Калифорнии предлагает шаг к большей прозрачности данных и контролю со стороны потребителей, требуя от компаний раскрывать категории собираемой ими личной информации и цели, для которых они используют эту информацию.

Следовательно, в законодательстве передовых западных стран закреплено право на разъяснение индивидуальных решений искусственным интеллектом и предусматривает возможность четкого объяснения того, как система искусственного интеллекта участвовала в процессе принятия решения. Это право имеет значение как крайняя мера для получения важной информации, необходимой для реализации права на эффективное средство правовой защиты. Указанное подтверждает, что искусственный интеллект, применяемый в здравоохранении, должен гарантировать высокую точность и при этом сохранять прозрачность, ведь это в значительной степени способствует укреплению доверия между медицинскими работниками и пациентами. Поэтому если врачи или пациенты не получают ответы на свои вопросы об искусственном интеллекте, который может принимать решения, меняющие жизнь, то отношения доверия сложно будет поддерживать.

В части решения проблемы прозрачности алгоритмов искусственного интеллекта можно обратить внимание, что действующее национальное законодательство в области здравоохранения в странах-членах ЕС, в КНР и др. не предоставляет пациентам прямых правовых средств для отказа от медицинских процедур, основанных на решениях, принятых с помощью искусственного интеллекта (диагностика или выбор лечения), и медицинских процедур, использующих частично или полностью автоматизированное принятие решений (искусственный мониторинг сердца).

Однако, как мы выяснили в разделе 3.2. параграфа 3 главы 1 исследования, в штате Массачусетс США находится на рассмотрении законопроект о

⁴²³ *Shany Y.* (2023). Digital rights and the outer limits of international human rights law. *German Law Journal*, 24(3), pp. 461-472.

регулировании использования искусственного интеллекта при оказании услуг в области психического здоровья, который требует, чтобы любой лицензированный специалист в области психического здоровья, желающий использовать искусственный интеллект для оказания услуг в данной области, должен сообщать своим пациентам об использовании искусственного интеллекта и предоставлять им информированное согласие. Кроме того, в рассмотренной в параграфе 2 главы 1 настоящего исследования Рекомендации об этических аспектах искусственного интеллекта указано, что странам рекомендуется внедрить в национальное законодательство процедуру получения согласия от пациента на использование искусственного интеллекта.

Целесообразно было бы учесть положения вышеуказанного законопроекта штата Массачусетс США в совершенствовании российского законодательства и предусмотреть в Федеральном законе от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» возможность включения в дополнение ко всей стандартной требуемой информации об информированном согласии упоминания искусственного интеллекта и любых соответствующих рисках, если таковые имеются. Риски могут быть связаны с характером оказания медицинской помощи при использовании искусственного интеллекта и вероятностью нанесения вреда пациенту в зависимости от того, каким образом был применен искусственный интеллект, т.е. вносил ли он существенный вклад в лечение пациента.

Альтернативным вариантом решения представляется установление в проекте федерального закона об искусственном интеллекте, предложенном в разделе 2.4 параграфа 2 главы 2 данного исследования, отдельной статьи, посвященной информированности пациента о применении искусственного интеллекта. В связи с риск-ориентированным подходом информированное согласие может быть запрошено в отношении систем искусственного интеллекта, относящихся к высокому и ограниченному риску, поскольку такие системы непосредственно влияют на безопасность и могут нарушить основные права человека, причинить

вред здоровью пациента.

Таким образом, на основе проведенного в этой части параграфа анализа рисков нарушения права на охрану здоровья и медицинскую помощь в результате влияния технологий искусственного интеллекта можно сформулировать следующие выводы.

1. Проблема неинформирования пациента о применении искусственного интеллекта до сих пор не получила должного нормативно-правового регулирования и не располагает достаточной правоприменительной практикой. Требуется дальнейшее развитие правовой базы в данной области, что, учитывая значимость рассматриваемой проблемы, в свою очередь, повлияет на правовую доктрину информированного добровольного согласия.

Предполагается, что врач должен информировать пациента о том, что в его лечении используется искусственный интеллект в зависимости от рисков для самого пациента и последствий в отношении его здоровья. Ключевым фактором, ведущим к врачебным ошибкам и причинению вреда пациенту, выступает использование нерепрезентативных, неполных или смещенных данных в диагнозе, поставленном пациенту искусственным интеллектом. Врачи должны говорить своим пациентам, что даже лучшая и точная персонализированная оценка риска в отношении искусственного интеллекта не является непогрешимой.

В результате анализа доктрины информированного согласия в ее текущем состоянии в России можно отметить, что пациент должен получить право принять предложенное лечение или отказаться от него на основании предоставленной информации и дать соответствующее информированное согласие на медицинское вмешательство, осуществляемое с использованием информационных технологий, исходя из принципа автономии пациента.

Для решения проблемы было предложено обратиться к правовой модели, примененной в законопроекте о регулировании использования искусственного интеллекта при оказании услуг в области психического здоровья штата Массачусетс США.

2. Было установлено, что в законодательстве России не решена проблема прозрачности алгоритмов искусственного интеллекта. Граждане не имеют возможности знать, на основе каких принципов работает искусственный интеллект, какие исходные данные используются при принятии им решений в отношении диагностики состояния их здоровья и лечения.

Чтобы решить данную проблему, можно было бы обратиться к положениям Закона о защите прав потребителей Калифорнии и Закона об искусственном интеллекте ЕС (ст. 50 и 86), которые являются подходящей платформой для регулирования применения искусственного интеллекта.

3.2. Конституционное право на доступ к информации

В соответствии с частью 4 ст. 29 Конституции Российской Федерации каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом⁴²⁴. Часть 2 ст. 24 Конституции Российской Федерации гарантирует право каждого на ознакомление с документами и материалами, непосредственно затрагивающими его права и свободы, за исключением случаев, предусмотренных законом (с соблюдением ограничений, предусмотренных частью 3 ст. 55 Конституции Российской Федерации⁴²⁵).

В научной доктрине существует дискуссия по поводу соотношения права на информацию и права на доступ к информации.

Один из подходов предполагает, что право на информацию носит самостоятельный характер, не связанный со свободой слова и печати (ст. 29 Конституции Российской Федерации). С.Н. Шевердяев отметил, что самостоятельное субъективное право в области информации на основе ч. 4 ст. 29 Конституции Российской Федерации не образуется, при этом право на

⁴²⁴ Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // «Российская газета», № 237 (853).

⁴²⁵ Там же.

информацию является прямым следствием развития теории свободы слова и печати⁴²⁶.

Другой подход основан на том, что право на доступ к информации является частью общего конституционного субъективного права на информацию. Е.С. Лисицына в своем исследовании подчеркивает: «Исследуя механизм реализации права на информацию, следует исходить из того, что право на информацию состоит из права на доступ к информации»⁴²⁷.

Третий подход подразумевает, что право на доступ к информации является самостоятельным правом. А.А. Задков выделяет два направления исследований, одно из которых связано с разработкой «права на информацию» как комплексного субъективного права свободно искать, получать, передавать, производить и распространять информацию, а другое предполагает понимание «права на доступ к информации» как права специального, увязывает его рассмотрение с проблематикой открытости деятельности органов государственной власти⁴²⁸.

Законодатель, в свою очередь, в Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» закрепил право человека на доступ к информации, под которым понимается возможность получения информации и ее использования, при этом граждане (физические лица) и организации (юридические лица) вправе осуществлять поиск и получение любой информации в любых формах и из любых источников⁴²⁹.

Применительно только к гражданам часть 2 ст. 8 данного Федерального закона предоставляет право на получение информации от государственных

⁴²⁶ *Шевердяев С.Н.* Право на информацию: к вопросу о конституционно-правовой сущности // Право и политика. 2001. № 10. С. 91.

⁴²⁷ *Лисицына Е.С.* Право на информацию и информационную деятельность в Российской Федерации: конституционно-правовые аспекты : Дис..... канд. юрид. наук : 12.00.02/ Лисицына Елена Сергеевна - Москва, 2003, 214 с.

⁴²⁸ *Задков А.А.* Конституционное право на доступ к информации в Российской Федерации : Дис. ... канд. юрид. наук : 12.00.02/ Задков Александр Алексеевич - Москва, 2006, 180 с.

⁴²⁹ Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // «Собрание законодательства РФ», 31.07.2006, № 31 (1 ч.), ст. 3448.

органов, органов местного самоуправления, их должностных лиц информации, непосредственно затрагивающей права и свободы граждан⁴³⁰.

Е.Ф. Усманова и В.В. Данилов, основываясь на буквальном толковании термина, определяют получение информации как ее приобретение от лица, владеющего данными сведениями. Сбор информации представляет собой процесс, который является более продолжительным и более широким по охвату, поскольку он включает в себя наблюдение за явлениями, событиями или получением разнообразных данных, которые позже подвергают анализу и обобщению⁴³¹. Как отмечает А.К. Дубень, право на доступ к информации может рассматриваться в более широком смысле, то есть как возможность доступа к любой информации, а не только той, что запрашивается у органов публичной власти и касается их деятельности⁴³².

Таким образом, многие авторы рассматривают право на информацию как самостоятельное право вне свободы мысли и печати, другие считают право на доступ к информации основным элементом права на информацию, а третьи считают право на доступ к информации самостоятельным правом.

В целях настоящего исследования представляется целесообразным рассматривать право на доступ к информации как элемент права на информацию и заострить внимание на проблемах реализации данного права в условиях применения информационных технологий в сфере здравоохранения.

В условиях активного развития информационных технологий и сбора больших объемов электронной информации в медицине значительно возросло использование технологии анализа «больших данных» для обмена данными и их анализа⁴³³.

⁴³⁰ Там же.

⁴³¹ Усманова Е.Ф., Данилов В.В. Правовое регулирование права на доступ к информации // Проблемы права. 2018. № 4(68). С. 30-34.

⁴³² Дубень А.К. Право на доступ к информации как составная часть конституционного права Российской Федерации // Наукосфера. 2022. № 7-1. С. 282-286.

⁴³³ K. M. Kingsford, F. Zhang, M. D. N. Ayeh and A. MaryMargaret, (2017) A Mathematical Model for a Hybrid System Framework for Privacy Preservation of Patient Health Records, IEEE 41st Annual Computer Software and Applications Conference (COMPSAC), pp. 119-124.

Установлено, что именно «большие данные» связаны с правом на доступ к информации, поэтому целесообразно в рамках настоящего исследования рассмотреть их влияние на данное право. Более того, Е.А. Войниканис отметила, что регулирование «больших данных» основано на приоритете свободного доступа к информации⁴³⁴.

Медицинские учреждения обязаны предоставлять информацию в понятном для пациента виде. Разнообразие потребностей в информации означает, что системы, поддерживаемые искусственным интеллектом в здравоохранении, должны быть объяснимы с различными уровнями конкретности, на разных стадиях внедрения, чтобы быть понятными для различных субъектов или аудиторий⁴³⁵. Это может означать, что сначала нужно предоставить объяснения для всех соответствующих пациентов.

Могут быть случаи, когда немедленный доступ к определенной медицинской информации может нанести вред. Поэтому государства для защиты пациента вводят в законодательство нормы о постепенном предоставлении доступа к данным, чтобы определённые медицинские сведения о состоянии здоровья пациента предоставлялись ему только после того, как лечащий врач объяснил пациенту соответствующую медицинскую информацию и ее последствия.

Например, к таким медицинским сведениям могут относиться результаты лабораторных исследований, подтверждающие, что у пациента имеется угрожающее жизни состояние здоровья.

Для защиты пациента может быть целесообразно, чтобы он узнал об этом во время консультации с лечащим врачом, который затем сможет объяснить ему диагноз, прогноз и варианты лечения.

⁴³⁴ *Войниканис Е. А.* Регулирование больших данных и право интеллектуальной собственности: общие подходы, проблемы и перспективы развития // Закон. 2020. №. 7. С. 135-156.

⁴³⁵ *Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., ... & Herrera, F.* (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information fusion*, 58, pp. 82-115.

После этого объяснения информация также станет доступной в электронной форме для скачивания и сохранения.

Медицинская этика и правовая база требуют предоставления значимой информации, контекстуальной прозрачности и объяснимости, чтобы оказывающие помощь могли выполнять свои обязанности и удовлетворять права пациентов на доступ к информации.

В условиях цифровизации общественных отношений происходит трансформация права на доступ к информации, в связи с чем, по мнению Т.А. Поляковой и Г.Г. Камаловой, оно имеет межотраслевой характер и приобретает особую актуальность, что обусловлено не только социально-экономическим значением информации, но и экспоненциальным усилением трансформирующего воздействия цифровых технологий⁴³⁶. Право на получение информации о своем здоровье является важным элементом политики повышения медицинской грамотности населения, поскольку информированный пациент способен к более осознанному участию в профилактике заболеваний, следованию предписаниям врача и, как следствие, к достижению лучших результатов лечения, что в целом повышает эффективность системы здравоохранения. Право на доступ к медицинской информации пациента может быть связано с его текущим состоянием здоровья и прогнозом на будущее. Это дополнение к праву на автономию пациента, которое, помимо информированного согласия (включая согласие на передачу медицинских данных из одного медицинского учреждения в другое) предполагает информационное право на доступ к медицинской информации.

В настоящее время отмечаются различные проблемы, связанные с правом на доступ к информации в сфере здравоохранения в России. Например, в связи с использованием информационных технологий в здравоохранении возникает риск неравного доступа к информации, который зависит от технологических возможностей человека и его способности взаимодействовать с инструментами

⁴³⁶ Полякова Т. А., Камалова Г. Г. Концептуальные основания развития института доступа к информации в Российской Федерации при применении цифровых технологий // Мониторинг правоприменения. 2020. № 4(37). С. 22-27.

электронного здравоохранения. В результате нарушаются конституционные принципы равенства и справедливости, возникает неравенство в доступе, неравное обращение, дискриминация, стигматизация. Это касается и электронных медицинских карт пациентов, которые составляются и хранятся в автоматизированной информационной базе данных медицинского учреждения, а также федеральной интегрированной электронной медицинской карты⁴³⁷.

Поэтому необходимо рассмотреть в контексте права на доступ к информации технологии анализа больших данных и их влияние на данное право на примере электронных медицинских карт, поскольку пациенты имеют доступ к своим электронным медицинским картам, что подразумевает наличие у них права на доступ к информации, содержащейся в таких электронных медицинских картах.

Актуальной проблемой при использовании электронных медицинских карт остается отсутствие у пациента права на внесение дополнительной информации в свою электронную медицинскую карту. О.В. Романовская, Г.Б. Романовский указывали на тот факт, что минимизированы возможности самого гражданина по заполнению личных медицинских данных. Кроме того, пациент не может в электронную медицинскую карту вносить коррективы, отсутствует и обратная связь⁴³⁸.

Данная проблема подтверждается не только в научной доктрине, но и в средствах массовой информации.

Москва и Санкт-Петербург — лидеры с развитыми региональными системами (ЕМИАС, ЕГИСЗ), где жители могут самостоятельно добавить дополнительные медицинские сведения в электронную медицинскую карту. Через Госуслуги не предусмотрена такая возможность в настоящее время.

⁴³⁷ Постановление Правительства Российской Федерации от 9 февраля 2022 г. №140 «О единой государственной информационной системе в сфере здравоохранения» // "Собрание законодательства РФ", 21.02.2022, № 8, ст. 1152.

⁴³⁸ Романовская О. В., Романовский Г. Б. Право и цифровизация современного здравоохранения // Вестник Российского университета дружбы народов. Серия: Юридические науки. 2024. Т. 28. №. 3. С. 565-583.

Как отмечается в СМИ, этот уровень в Москве и Санкт-Петербурге стал возможен благодаря устойчивому финансированию, развитой ИТ-инфраструктуре и системному подходу к внедрению технологий. В других субъектах РФ ситуация существенно отличается. Главным фактором в этом является отсутствие финансирования. В отличие от Москвы и Санкт-Петербурга, обладающими большими бюджетами и развитыми ИТ-экосистемами, которые могут реализовывать масштабные проекты, регионы имеют ограниченные ресурсы, расставляя следующие приоритеты: «сначала — ремонт больниц, закупка оборудования, обеспечение кадрами. Поэтому цифровые платформы зачастую отходят на второй план»⁴³⁹.

Представляется целесообразным предусмотреть возможность вносить пациентами в электронную медицинскую карту дополнительную информацию о своем здоровье: (оценка динамики (улучшения или ухудшения) состояния, оценка влияния лекарств, данные о давлении, количестве выполненных физических упражнений, определенных болевых ощущениях и т. д.). Пациент мог бы дополнить электронную медицинскую карту информацией, полученной в частных медицинских учреждениях (если у последних нет доступа), консультациями, полученными за границей, а также другими данными (давление, температура и т. д.). Окончательное решение о применении такой информации в лечебном процессе должно оставаться в компетенции лечащего врача.

Правовое регулирование данного вопроса в субъектах Российской Федерации, как отмечают ученые, отличается неоднородностью, например, в Москве через единую медицинскую информационно-аналитическую систему (ЕМИАС) ведется электронная медицинская карта. На официальном портале Москвы пациенты наделены возможностью самостоятельного внесения сведений в свою медицинскую карту, в частности в разделе «Прививки», в разделе «Моя семья, в разделе «Дневник здоровья» можно указать температуру тела, уровень

⁴³⁹ Электронные медкарты: где доступ, а где — цифровая пропасть. URL: <https://eur-http://pravo-med.ru/articles/18736/> (дата обращения: 18.01.2026)

кислорода, пульс, уровень сахара в крови, показатели артериального давления и др.⁴⁴⁰. Вышеуказанное право закреплено приказом Департамента здравоохранения города Москвы, Департамента информационных технологий города Москвы и Комитета государственных услуг города Москвы от 13.01.2020 № 7/64-16-6/20/01-05-1/20 «Запрос, изменение и отмена доступа к электронной медицинской карте». В других субъектах Российской Федерации не имеется такая возможность, за исключением Санкт-Петербурга.

Следует предусмотреть данную возможность во всех субъектах России, а не только в Москве и Санкт-Петербурге, учитывая, что с 1 января 2024 появилась обязательная система электронных медицинских карт в медицинских организациях. Доступ к личным данным ЭМК и их дополнение в Москве происходит через медицинскую информационно-аналитическую систему на официальном портале города Москвы.

Для решения обозначенной проблемы представляется перспективным обращение к рассмотренному в разделе 3.3. параграфа 3 главы 1 исследования Закону об обработке данных клиентов в здравоохранении и социальном обеспечении Финляндии.

Как мы выяснили, уникальность реализации цифрового здравоохранения Финляндии состоит в том, что данные в систему Kanta могут вносить сами граждане на добровольной основе. Это способствует формированию более полной картины здоровья пациента и усиливает его вовлеченность. Учитывая схожую централизованную архитектуру (Kanta является аналогом ЕГИСЗ), представляется целесообразным рассмотреть возможность реализации аналогичного функционала в рамках сервиса «Мое здоровье» на Едином портале государственных услуг как подраздела ЕГИСЗ, чтобы такая возможность была не только в Москве, а во всей России, внося соответствующие изменения в постановление Правительства

⁴⁴⁰ Акулин И. М., Чеснокова Е. А., Пресняков Р. А., Прядко А.Е., Гурьянова Н. Е. Электронная медицинская карта: опыт правового регулирования стран ЕАЭС // Врач и информационные технологии. 2022. № 1. С. 72-83.

Российской Федерации от 9 февраля 2022 г. № 140 «О единой государственной информационной системе в сфере здравоохранения»⁴⁴¹.

В дополнение к вышеуказанному подчеркнем, что в соответствии со ст. 5 Регламента ЕС по использованию и обмену электронными данными о здоровье пациент имеет право добавлять информацию в свои электронные медицинские записи через службу доступа к медицинским данным, включая данные из приложения для поддержания здоровья (технологии Интернета вещей)⁴⁴².

Регламент не устанавливает перечень элементов данных, которые могут быть вставлены. Однако цель состоит в том, чтобы дать пациентам возможность дополнять данные в приоритетных категориях данных. Любая информация, добавленная пациентом, будет четко отличаться от информации, введенной медицинскими работниками.

Это право касается только добавления информации, оно не позволяет изменять информацию, предоставленную медицинскими работниками. Тем не менее пациент может самостоятельно внести дополнительную информацию в свою электронную медицинскую карту через портал, позволяющий пациенту получить электронный доступ к документам с медицинскими данными: онлайн-службы предоставят пациентам панель управления, с помощью которой они внесут данные.

Кроме того, нельзя не упомянуть об особенностях внесения изменений в электронные медицинские карты самими врачами.

В судебных разбирательствах по делам о медицинской халатности возникают вопросы, касающиеся точности медицинских записей врача. Иногда это происходит потому, что пациент решительно оспаривает содержание записей. Были случаи, когда эта проблема становилась настолько серьезной в деле или жалобе, что ИТ-экспертам поручали проверить журнал аудита

⁴⁴¹ Постановление Правительства Российской Федерации от 9 февраля 2022 г. № 140 «О единой государственной информационной системе в сфере здравоохранения» // «Собрание законодательства РФ», 21.02.2022, № 8, ст. 1152.

⁴⁴² Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847. URL: <https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng> (дата обращения: 28.11.2024)

компьютеризированных записей, чтобы определить, когда они были созданы и были ли они впоследствии изменены.

Например, в российской судебной практике имеется решение Октябрьского районного суда г. Архангельска от 7 марта 2017 года по делу № 2-1180/2017 ~ М-9858/2016, в рамках которого истец обратился в суд с исковым заявлением в отношении ГАУЗ «Архангельская областная клиническая стоматологическая поликлиника» о признании записи недействительной и обязанности заменить ее на иную запись.

Суд отказал в удовлетворении иска на том основании, что истцом материалы дела не представлены, а судом не добыты какие-либо доказательства, подтверждающие ошибочность внесения работниками ответчика рассматриваемой записи в медицинскую карту истца, исходя из того обстоятельства, что данная запись вносится со слов пациента. Суд счел необходимым обратить внимание и на то обстоятельство, что сама по себе рассматриваемая запись, по мнению суда, не свидетельствует о нарушении каких-либо прав истца, так как фактически не несет на себе правовой нагрузки. Данная запись также не свидетельствует и об оказании истцу некачественной медицинской услуги, за получением которой он обратился к ответчику⁴⁴³.

В научной доктрине отмечается, что предоставление пациентам возможности просматривать свои медицинские записи может быть полезно по ряду причин, в том числе для расширения их прав и возможностей — более активного участия в лечении и лучшего понимания своего лечения⁴⁴⁴, а также для уменьшения количества ошибок, когда пациенты выявляют ошибки, которые впоследствии

⁴⁴³ Решение Октябрьского районного суда г. Архангельска от 7 марта 2017 года по делу № 2-1180/2017 ~ М-9858/2016. URL: https://oktsud--arh.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=285308532&case_u_id=70829744-c194-45e0-b8a9-03d52ce992c8&delo_id=1540005&new= (дата обращения: 28.01.2025).

⁴⁴⁴ *Demiris, G., Afrin, L. B., Speedie, S., Courtney, K. L., Sondhi, M., Vimarlund, V., & Lynch, C. (2008). Patient-centered applications: use of information technology to promote disease management and wellness. A white paper by the AMIA knowledge in motion working group. Journal of the American Medical Informatics Association, 15(1), pp. 8-13.*

могут быть исправлены⁴⁴⁵. Этот подход к повышению точности записей, ориентированный на пациента, был признан важным способом улучшения качества лечения⁴⁴⁶, а опросы показали, что пациенты заинтересованы в просмотре своих записей для выявления и исправления ошибок, если им предоставляется такая возможность⁴⁴⁷.

Если необходимо внести какие-либо пояснения или исправления в медицинскую карту, это должно быть четко обозначено как ретроспективная дополнительная запись с указанием даты внесения изменений и личности автора. В идеале также следует указать причину уточнения (исправления). Эти требования применяются как к электронным, так и к физическим медицинским картам. Любому, кто просматривает запись, должно быть абсолютно ясно, что она была сделана не во время события или консультации, а добавлена позже. Это обеспечит прозрачность медицинских карт и позволит показать, что речь идет о подлинном последующем уточнении, без намерения ввести в заблуждение какое-либо другое лицо.

Также врачам может быть разрешено изменять демографические данные, такие как дата рождения, после проверки, тогда как все запросы на внесение клинических изменений должны быть отправлены обратно поставщику медицинских услуг для обновления. Независимо от типа изменения, любые изменения в содержании медицинской карты должны быть одобрены поставщиком медицинских услуг.

⁴⁴⁵ Ross, S. E., & Lin, C. T. (2003). The effects of promoting patient access to medical records: a review. *Journal of the American Medical Informatics Association*, 10(2), pp. 129-138; Siteman, E., Businger, A., Gandhi, T., Grant, R., Poon, E., Schnipper, J., & Middleton, B. (2006). Clinicians recognize value of patient review of their electronic health record data. In *AMIA Annual Symposium Proceedings* (Vol. 2006, P. 1101).

⁴⁴⁶ Baker, A. (2001). Crossing the quality chasm: a new health system for the 21st century. *British Medical Journal Publishing Group*. Vol. 323, No. 7322, P. 1192.

⁴⁴⁷ Bhavnani, V., Fisher, B., Winfield, M., & Seed, P. (2011). How patients use access to their electronic GP record—a quantitative study. *Family Practice*, 28(2), pp. 188-194; Fowles, J. B., Kind, A. C., Craft, C., Kind, E. A., Mandel, J. L., & Adlis, S. (2004). Patients' interest in reading their medical record: relation with clinical and sociodemographic characteristics and patients' approach to health care. *Archives of Internal Medicine*, 164(7), pp.793-800.

В соответствии с ранее рассмотренным в исследовании Общим регламентом ЕС о защите данных пациенты имеют право требовать исправления фактически неточной информации (ст. 16)⁴⁴⁸. Также на основании положений ст. 6, 13 Регламента ЕС по использованию и обмену электронными данными о здоровье пациент может запросить исправление ошибочных данных в своей электронной медицинской карте с помощью функций, предоставляемых службами доступа к медицинским данным. Такие запросы будут затем направлены врачу, который оценит их и исправит в случае необходимости. Однако важно отметить, что пациент не сможет самостоятельно изменить данные, которые считает неверными⁴⁴⁹.

Врачам следует помнить о различии между простой фактической неточностью (например, неверно указанная дата рождения пациента в медицинской карте) и, отдельно, спором о медицинском заключении врача, содержащемся в медицинской карте (например, о том, что у пациента наблюдались психотические симптомы или он выглядел встревоженным во время консультации). Рассмотрение спора пациента в последнем случае должно осуществляться в индивидуальном порядке. Один из подходов заключается в добавлении в карту дополнительной записи, например, о несогласии пациента с диагнозом. Однако оригинал записи, сделанной врачом, должен оставаться в силе, если врач убежден, что это была актуальная запись его клинического заключения на тот момент.

Из вышеизложенного следует, что поскольку электронные медицинские карты становятся все более популярным механизмом предоставления пациентам удобного доступа к их медицинским записям, возможно увеличение количества запросов со стороны пациентов на внесение изменений, что может создать дополнительную нагрузку на и без того занятых врачей, особенно если многие

⁴⁴⁸ General Data Protection Regulation. URL: <https://gdpr-info.eu/> (дата обращения: 28.11.2024)

⁴⁴⁹ Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847. URL: <https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng> (дата обращения: 28.11.2024)

запросы клинически необоснованны. С другой стороны, если многие из запросов действительно обоснованны, это может подчеркнуть важность предоставления пациентам расширенного доступа к их записям для обеспечения большей точности информации, так как расширение доступа пациентов к своим медицинским записям может привести к более эффективному выявлению и исправлению потенциальных ошибок. Для повышения эффективности такого подхода, основанного на участии пациентов, важно информировать их о праве на просмотр и изменение записей, а также о процедуре, позволяющей это делать. Это будут важные шаги на пути к повышению точности и полноты медицинских записей за счет вовлечения пациентов, являющихся конечными владельцами данных.

Таким образом, на основе проведенного в этой части параграфа анализа рисков нарушения права на доступ к информации в сфере здравоохранения в результате влияния технологий анализа «больших данных» можно сформулировать следующий вывод.

Трансформация права на доступ к информации в сфере здравоохранения носит двойственный характер: с одной стороны, оно получает беспрецедентные инструменты для реализации ЭМК, с другой — сталкивается с новыми системными правовыми рисками.

Актуальной остается проблема внесения дополнительной информации пациентами в электронную медицинскую карту. Не все субъекты России имеют такую возможность.

В качестве ключевой меры по преодолению выявленных пробелов предлагается в личном сервисе «Мое здоровье», доступном в Госуслугах через ЕГИСЗ, предусмотреть возможность вносить самостоятельно сведения в свою медицинскую карту всеми гражданами страны, а не только гражданами Москвы, которые могут в разделе «Прививки», в разделе «Моя семья, в разделе «Дневник здоровья» указать температуру тела, уровень кислорода, пульс, уровень сахара в крови, показатели артериального давления и др. через ЕМИАС.

Чтобы такая возможность появилась на уровне федеральной государственной информационной системы полезно было бы использовать опыт Финляндии, которая смогла закрепить такую возможность на уровне общегосударственной платформы Kanta, являющейся аналогом отечественной ЕГИСЗ и содержащей несколько подразделов.

3.3. Конституционное право на неприкосновенность частной жизни

Одним из первых конституционных прав, подвергшихся активному обсуждению в связи с цифровизацией, и одним из наиболее актуальных в контексте применения информационных технологий является право на неприкосновенность частной жизни. При этом следует согласиться с тем, что данное конституционное право предопределяет неизбежность его столкновения с другими правами и свободами человека и гражданина, в частности, с правом на доступ к информации, представляющим общественный интерес⁴⁵⁰.

Актуальность научной дискуссии о реализации права на неприкосновенность частной жизни возрастает из-за повсеместного внедрения информационных технологий, поскольку некоторые авторы придерживаются мнения, что право на неприкосновенность частной жизни может стать декларативным, превратиться в атавизм конституционного права и полностью раствориться в цифровой среде⁴⁵¹. Полагаем, что данное утверждение не в полной мере учитывает природу конституционных прав человека, которые не могут рассматриваться как декларативные, поскольку «каждое право человека – это, прежде всего, свод требований, предъявляемых к государству, что и отличает их от иных

⁴⁵⁰ Гриценко Е.В., Должиков А.В., Дудко И.А., Егорова О., Кененова И.П., Красиков Д.В., Кряжкова О.Н., Кузнецова И.С., Сыченко Е.В., Третьяк И.А., Троицкая А.А., Храмова Т.М., Чирнинов А.М., Шилова А.И. Конституционные права в России: судебная практика и сравнительные материалы / Е– Москва : Центр конституционных исследований, 2024. 582 с.

⁴⁵¹ Волкова Г. Е. Трансформация права на неприкосновенность частной жизни в условиях цифровизации общества // Цифровые технологии и право : Сборник научных трудов I Международной научно-практической конференции. В 6-ти томах, Казань, 23 сентября 2022 года. Казань: Издательство "Познание", 2022. С. 78-82.

категорий»⁴⁵². Право на неприкосновенность частной жизни относится к естественным и неотчуждаемым правам человека, которое налагает на государство обязанность по принятию конкретных мер для защиты персональных данных. Это конституционное право, поддерживаемое законами, механизмами правоприменения и глобальным сообществом, стремящимся к созданию цифровой среды, которая уважает и защищает частную жизнь отдельных людей. Важным представляется и тот факт, что ВОЗ в глобальной стратегии по цифровому здравоохранению на 2020–2025 гг. ставит на первый план создание прочной правовой и нормативной базы для защиты конфиденциальности, целостности и доступности данных и обработки персональных данных о здоровье⁴⁵³. Без закрепленного и гарантированного в конституции государства права на неприкосновенность частной жизни невозможно создать требуемую нормативно-правовую базу.

Конституция Российской Федерации в ст. 23 устанавливает, что каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени⁴⁵⁴. Также согласно части 1 ст. 24 Конституции Российской Федерации сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются⁴⁵⁵.

В этих статьях закреплено право на неприкосновенность частной жизни и содержатся положения, способствующие его реализации, такие как запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия. Этих основополагающих специальных норм Конституции Российской Федерации достаточно, чтобы создать надежную основу для защиты

⁴⁵² Романовский Г. Б., Романовская О. В. Право и современная медицина: проблемы и перспективы // Известия высших учебных заведений. Поволжский регион. Общественные науки. 2024. № 1 (69). С. 96-110.

⁴⁵³ Global strategy on digital health 2020-2025. URL: <https://www.who.int/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf> (дата обращения: 28.01.2025)

⁴⁵⁴ Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // «Российская газета», № 237 (853).

⁴⁵⁵ Там же.

частной жизни даже в условиях повсеместного внедрения информационных технологий. Однако гарантии реализации данных правомочий должны исходить от самого государства, его положительных действий: государству необходимо создавать инфраструктуру для реализации права и формировать дополнительные механизмы для его осуществления. Поэтому перед государством стоит множество задач, на которые ему следует обратить внимание. Одной из таких задач государства является развитие правовых механизмов защиты права на неприкосновенность частной жизни в новых условиях цифровизации⁴⁵⁶.

Несмотря на создаваемые информационными технологиями риски для тайны частной жизни, эти же технологии обладают потенциалом для ее защиты. К их преимуществам можно отнести следующее.

Информационные технологии позволяют создавать более совершенные системы шифрования, средства защиты от несанкционированного доступа, а также системы безопасного хранения данных, что может способствовать повышению уровня защиты личной информации от неправомерного доступа и использования. Информационные технологии дают возможность автоматизировать многие процессы, связанные с защитой частной жизни, такие как обнаружение и предотвращение утечек данных, мониторинг доступа к информации и т.д.

В целом информационные технологии позволяют управляющим органам и оказывающим медицинские услуги организациям создавать удобные онлайн-инструменты, через которые граждане могут:

- запрашивать доступ к своим персональным данным, хранящимся у организации;
- требовать исправления неточных данных;
- подавать запросы на удаление данных (право на забвение);
- отзываться согласие на обработку данных.

⁴⁵⁶ Белова А.Р. Трансформация права на неприкосновенность частной жизни в условиях информатизации общественных отношений // Евразийский юридический журнал. 2022. № 10(173). С. 157-159.

Однако вне зависимости от преимуществ информационных технологий в области неприкосновенности частной жизни актуальной остается проблема конфиденциальности сведений, составляющих тайну частной жизни и персональных данных.

А.В. Преснякова, обратила внимание на тот факт, что право на неприкосновенность частной жизни оказалось особо уязвимым под воздействием новых информационных технологий, которые проникают во все сферы человеческой жизни; особой угрозой подвергаются такие составляющие права на неприкосновенность частной жизни, как неприкосновенность персональных данных⁴⁵⁷.

В научной литературе выделяют три подхода по вопросу соотношения понятий «персональные данные» и «частная жизнь».

Так, представители первого подхода считают, что частная жизнь рассматривается шире, чем персональные данные. Е. А. Миндрова отмечает, что персональные данные являются по своему содержанию сегментом информации о частной жизни лица⁴⁵⁸. Э.А. Цадыкова доказывает, что «информация о частной жизни» — понятие более широкое, чем понятие «персональные данные», поскольку персональные данные — это лишь информация, позволяющая идентифицировать личность⁴⁵⁹. М. Н. Малеина рассматривает тайну частной жизни как общую родовую категорию, включающую тайну персональных данных — одну из видов тайн⁴⁶⁰.

⁴⁵⁷ *Преснякова А. В.* Конституционное право на неприкосновенность частной жизни в условиях информатизации общества : современный зарубежный опыт : диссертация ... кандидата юридических наук : 12.00.02 / Преснякова Анна Викторовна; [Место защиты: Моск. гос. юрид. акад. им. О.Е. Кутафина].- Москва, 2010. 196 с.

⁴⁵⁸ *Миндрова Е.К.* Коллизия права граждан на доступ к информации и права на неприкосновенность частной жизни в условиях информационного общества: Автореф. дис. ... канд. юрид. наук. М., 2007. 24 с.

⁴⁵⁹ *Цадыкова Э. А.* Гарантии охраны и защиты персональных данных человека и гражданина // Конституционное и муниципальное право. 2007. № 14. С. 15—18.

⁴⁶⁰ *Малеина М. Н.* Право на тайну и неприкосновенность персональных данных // Журнал российского права. 2010. №. 11 (167). С. 18-28

Второй подход предполагает, что персональные данные, в свою очередь, шире, чем понятие «частная жизнь». Е.В. Климович подчеркивает, что «персональные данные не являются однородными и в их структуре, помимо идентифицирующей информации, следует выделять и информацию о конкретном человеке, к которой относится информация о частной жизни»⁴⁶¹. Д.М. Ветров относит сведения о частной жизни к одной из составляющих персональных данных⁴⁶².

Сторонники третьего подхода полагают, что указанные понятия не являются тождественными, но во многом пересекаются. Н.И. Пикуров, комментируя данный подход, установил, что «сведения о частной жизни лица и персональные данные не совпадают по содержанию, хотя и в значительной своей части пересекаются по объему»⁴⁶³. По мнению В.В. Вабищевича, «не все случаи использования персональных данных можно отнести к частной жизни, а элементы частной жизни могут составлять персональные данные»⁴⁶⁴.

В рамках настоящего исследования следует отдать предпочтение второму подходу, в котором частная жизнь непосредственно связана с персональными данными, которые шире ее, и поэтому сведения о частной жизни лица (личные, семейные, переписка и т.д.) являются частью персональных данных, так что целесообразно рассматривать персональные данные в контексте права на неприкосновенность частной жизни.

Проблема конфиденциальности персональных данных в сфере здравоохранения связана с тем, что персональные данные могут попасть к третьим лицам и быть раскрыты посторонним людям помимо врача без согласия пациента.

⁴⁶¹ *Климович Е. В.* О сущности понятия «персональные данные» как конфиденциальной информации особой категории // Международные юридические чтения : материалы ежегодной международной научно-практической конференции (14 апреля 2005 г.). — Омск : Изд-во Омск. юрид. ин-та, 2005. С. 21—30.

⁴⁶² *Ветров Д.М.* Защита персональных данных и защита информации на предприятии. Некоторые спорные вопросы применения // Проблемы права. Челябинск, 2010. № 1. С. 119

⁴⁶³ *Пикуров Н.И.* Проблемы квалификации преступных посягательств на частную жизнь: теория и судебная практика // Уголовное право. 2019. № 2. С. 51-58.

⁴⁶⁴ *Вабищевич, В. В.* О некоторых вопросах совершенствования уголовно-правовой охраны персональных данных и информации о частной жизни // Право.by. 2023. № 4. С. 89–96.

Даже если пациент случайно или добровольно раскрыл свои персональные данные, третье лицо при получении их без согласия самого пациента и использования в своих целях, будет нести ответственность, предусмотренную законом. Информационные технологии в здравоохранении часто собирают информацию, касающуюся медицинских показаний, симптомов и дозировок, и делятся этой информацией с третьими лицами. Для нормального функционирования информационных технологий в данной сфере требуется медицинская информация, которая является высокочувствительной по своей природе и связана с многочисленными категориями риска. К медицинской информации относятся любые сведения, касающиеся здоровья человека, истории болезни, лечения, диагнозов, принимаемых лекарств и общего самочувствия.

Среди медицинской информации можно выделить «чувствительные» данные о здоровье, которые должны быть классифицированы как конфиденциальные персональные данные⁴⁶⁵. Они нуждаются в особой защите на уровне законодательства государства, поскольку затрагивают такую информацию, которая наиболее тесно связана с пациентом и которую он не хотел бы раскрывать в принципе.

В этой связи растет значимость информационных технологий, поскольку их применение непосредственно влияет на медицинскую информацию и чувствительные данные о здоровье, так как, например, искусственным интеллектом или технологиями анализа больших данных обрабатываются персональные данные, в том числе в автоматизированном режиме. В результате возникают вопросы, связанные с обработкой таких типов данных и их регулированием на законодательном уровне.

В контексте данной проблемы важно рассмотреть вопрос об утечке персональных данных. В российском законодательстве утечка персональных

⁴⁶⁵ *Карицкая А.А.* Информационно-правовое обеспечение цифровой экосистемы здравоохранения // Правовая информатика. 2021. № 1. С. 13-23.

данных закреплена как угроза безопасности персональных данных в пункте 11 ст. 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»⁴⁶⁶.

Утечки персональных данных нарушают право человека на неприкосновенность частной жизни и подрывают доверие к системе здравоохранения. Согласно отчету корпорации International Business Machines, средняя стоимость утечки данных в здравоохранении составляет 7,1 миллиона долларов⁴⁶⁷. Кроме того, в России, по данным Роскомнадзора, за два года почти в 40 раз выросло количество утечек персональных данных пользователей. Если в 2021-м таких инцидентов было четыре, то в 2022-м — свыше 140, а за первые семь месяцев 2023-го — уже свыше 150⁴⁶⁸.

Сведения о состоянии здоровья и медицинские данные относятся к персональным данным. В соответствии с пунктом 1 ст. 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)⁴⁶⁹. Статья 10 указанного Федерального закона относит данные о состоянии здоровья к специальным персональным данным⁴⁷⁰.

Европейский суд по правам человека, несомненно, называет данные о здоровье одним из видов данных, заслуживающих защиты в соответствии с правом на уважение частной жизни. В отношении них Европейский суд по правам человека часто подчеркивает важность «защиты данных». Например, дело Z против

⁴⁶⁶ Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // "Собрание законодательства РФ", 31.07.2006, N 31 (1 ч.), ст. 3451.

⁴⁶⁷ Average cost of healthcare data breach rises to \$7.1M, according to IBM report. URL: <https://www.fiercehealthcare.com/tech/average-cost-healthcare-data-breach-rises-to-7-1m-according-to-ibm-report#:~:text=A%20healthcare%20data%20breach%20comes,2020%20data%20breach%20cost%20report.> (дата обращения: 28.11.2024)

⁴⁶⁸ Личное делят: в РФ в 40 раз выросло количество утечек персональных данных. URL: <https://iz.ru/1554402/alena-nefedova/lichnoe-deliat-v-rf-v-40-razvyroslo-kolichestvo-utechek-personalnykh-dannykh> (дата обращения: 29.11.2023).

⁴⁶⁹ Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // "Собрание законодательства РФ", 31.07.2006, № 31 (1 ч.), ст. 3451.

⁴⁷⁰ Там же.

Финляндии (*Z v. Finland*) в 1997 году касалось раскрытия информации о состоянии здоровья заявителя с ВИЧ в ходе разбирательства по делу о сексуальном нападении.

Суд подчеркнул в своем решении, что защита персональных данных, не в последнюю очередь медицинских, имеет фундаментальное значение для осуществления человеком своего права на уважение частной и семейной жизни, гарантированного ст. 8 Европейской конвенции по правам человека. Суд обосновал необходимость защиты раскрытой информации не тем, что она представляет собой «персональные данные» по смыслу Европейской конвенции по правам человека, а тем, что она относится к чувствительным данным. Суд постановил, что раскрытие такой информации может существенно повлиять на личную и семейную жизнь человека. Кроме того, Европейский суд по правам человека связал соответствующую защиту с принципом «конфиденциальности» и охарактеризовал ее как защиту от определенных видов передачи или раскрытия информации⁴⁷¹.

Применительно к российской правовой системе, как отмечает А.С. Федосин в диссертационном исследовании, «право на защиту персональных данных является элементом структуры права на неприкосновенность частной жизни, сформировавшимся в условиях кардинального изменения способа обработки информации»⁴⁷². С.Н. Алямкин также относит защиту персональных данных человека к одной из главных составляющих права человека на неприкосновенность частной жизни⁴⁷³. Кроме того, Конституционный Суд Российской Федерации

⁴⁷¹ *Z v. Finland*. URL: <https://hudoc.echr.coe.int/eng#%7B%22itemid%22%3A%5B%22002-9432%22%5D%7D> (дата обращения: 28.11.2024)

⁴⁷² *Федосин А.С.* Защита конституционного права человека и гражданина на неприкосновенность частной жизни при автоматизированной обработке персональных данных в Российской Федерации : автореферат дис. кандидата юридических наук : 12.00.14 / Федосин Алексей Сергеевич. - Саранск, 2009. 27 с.

⁴⁷³ *Алямкин С.Н.* Персональные данные как объект правового регулирования: понятие и способы защиты // Мир науки и образования. 2016. № 4 (8). С. 4.

неоднократно связывал защиту персональных данных с обеспечением права на неприкосновенность частной жизни⁴⁷⁴.

Использование технологий искусственного интеллекта создает прямые риски для конфиденциальности данных. Одной из проблем, связанных с применением искусственного интеллекта для отслеживания и анализа действий людей, является нарушение конфиденциальности и защиты данных, что может представлять угрозу для личной свободы и неприкосновенности частной жизни⁴⁷⁵. Случаи нарушения конфиденциальности данных в здравоохранении участились во многих национальных юрисдикциях, включая США⁴⁷⁶ и Европу⁴⁷⁷. И в настоящее время искусственный интеллект и другие программные средства и алгоритмы вносят свой вклад в растущую неспособность защитить медицинскую информацию⁴⁷⁸.

Сфера здравоохранения также несет самые высокие расходы, связанные с обеспечением конфиденциальности личных данных, которые более чем в три раза превышают расходы в других отраслях. Мировая практика изобилует случаями незаконной продажи данных о здоровье, незаконного распространения, использования в новых и неожиданных целях или несправедливой коммерциализации.

⁴⁷⁴ См: Определение от 16 июля 2013 г. № 1176-О об отказе в принятии к рассмотрению жалобы гражданина Круглова Александра Геннадьевича на нарушение его конституционных прав пунктом 4 части 2 ст. 10 Федерального закона «О персональных данных»; постановление от 26 октября 2017 г. № 25-П по делу о проверке конституционности пункта 5 ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации» в связи с жалобой гражданина А.И. Сушкова и др.

⁴⁷⁵ *Петроченков И. А.* Перспективы защиты прав человека в контексте принятия Евросоюзом регламента об искусственном интеллекте. *Гражданин. Выборы // Власть.* 2024. Т. 2. С. 104-115.

⁴⁷⁶ HIPAA Journal. Healthcare data breach statistics. URL: <https://www.hipaajournal.com/healthcare-data-breach-statistics/> (дата обращения: 28.11.2024)

⁴⁷⁷ European Union Agency for Cybersecurity. From January 2019 to April 2020 Data breach ENISA Threat Landscape. 2020. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-data-breach/at_download/fullReport (дата обращения: 28.11.2024)

⁴⁷⁸ Artificial intelligence advances threaten privacy of health data. URL: <https://www.sciencedaily.com/releases/2019/01/190103152906.htm> (дата обращения: 28.11.2024); Your Data Were ‘Anonymized’? These Scientists Can Still Identify You (Published 2019). URL: <https://www.ncbi.nlm.nih.gov/search/research-news/4173/> (дата обращения: 28.11.2024)

Так, в деле Ю.Г. против России (Y.G. v. Russia) Европейского суда по правам человека (№ 8647/12) от 30 августа 2022 г. выяснилось, что данные о здоровье, в том числе о здоровье заявителя, который был ВИЧ-инфицирован и страдал от гепатита, содержащиеся в базе данных, оказались доступны для продажи на рынке. Заявитель также утверждал, что правоохранительные органы незаконно собирали, хранили и вносили его медицинские данные в базу данных, а также что они не обеспечили конфиденциальность его данных и не провели эффективного расследования по факту их разглашения.

Суд постановил, что имело место нарушение ст. 8 Европейской конвенции о защите прав человека и основных свобод, установив, что российские власти не выполнили свое позитивное обязательство по обеспечению надлежащей защиты права заявителя на уважение его частной жизни. В контексте данного дела не существует иного объяснения, кроме того, что государственные органы, имевшие доступ к данным, не смогли предотвратить нарушение конфиденциальности. В результате эти данные стали общедоступными, что повлекло за собой ответственность государства-ответчика. Обстоятельства этого серьезного нарушения неприкосновенности частной жизни так и не были выяснены. В этой связи Суд напомнил, что он неоднократно подчеркивал важность надлежащих гарантий для предотвращения передачи и раскрытия данных о здоровье⁴⁷⁹.

Информация, собираемая медицинскими организациями, часто содержит личные данные пациентов, а также медицинскую информацию, и в случае утечки данных вся эта информация может быть скомпрометирована. Учитывая этот аспект, можно говорить о необходимости эффективной защиты данных в сфере здравоохранения, которая должна детально регулировать все аспекты работы с медицинскими данными — от хранения и передачи до защиты, — а также однозначно определять пределы доступа различных организаций к конкретным массивам медицинской информации.

⁴⁷⁹ Y.G. v. Russia. URL: [https://hudoc.echr.coe.int/fre#{%22itemid%22:\[%22002-13761%22\]}](https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-13761%22]}) (дата обращения: 28.11.2024)

В России обработка персональных данных регулируется Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Однако на не все случаи обработки медицинских данных с помощью информационных технологий распространяется законодательство России о защите персональных данных, поскольку темпы роста внедрения информационных технологий в здравоохранение возрастают с каждым годом, в связи с чем законодатель не успевает реагировать на появляющиеся угрозы со стороны информационных технологий относительно обработки персональных данных человека.

Например, Л.А. Бердегулова обращает внимание на тот факт, что в Федеральном законе от 27 июля 2006 г. № 152-ФЗ «О персональных данных» не рассматривается отдельная специфика предоставления охраны персональных данных, в частности, не урегулирован «вопрос хранения сведений для аутентификации и идентификации пользователей электронных порталов»⁴⁸⁰, то есть речь идет о вопросе аутентификации и идентификации через федеральные государственные информационные системы, к которой можно отнести Единую государственную информационную систему в сфере здравоохранения.

Дополнительно отметим, что Европейский суд по правам человека подчеркивает важность национального законодательства, направленного на защиту персональных данных гражданина и права на неприкосновенность частной жизни. Более подробно в этой связи мы анализировали дело С. и Марпер против Соединенного Королевства от 4 декабря 2008 года (*S. and Marper v. the United Kingdom*) и другие судебные дела в рамках отдельной научной публикации⁴⁸¹.

Если проблемы использования искусственного интеллекта в основном лежат в плоскости совершенствования существующих правовых механизмов, то технологии Интернета вещей ставят принципиально новые вызовы для

⁴⁸⁰ Бердегулова, Л.А. Проблемы правового регулирования института защиты персональных данных в системе правовой защиты права на неприкосновенность частной жизни, личную и семейную тайну в России // Актуальные проблемы государства и общества в области обеспечения прав и свобод человека и гражданина. 2021. № 1. С. 65-73.

⁴⁸¹ Федотов Н.Е. Право на неприкосновенность частной жизни в условиях цифровизации здравоохранения: некоторые законодательные пробелы в свете судебных решений // Конституционное и муниципальное право. 2025. № 6. С. 24 - 28.

гарантирования неприкосновенности частной жизни, обусловленные масштабом, скрытностью и децентрализованностью сбора данных подобными устройствами. Технологии Интернета вещей широко используются в сфере здравоохранения для сбора медицинской информации, поэтому в рамках данного исследования целесообразно подробнее рассмотреть влияние указанных технологий на право на неприкосновенность частной жизни.

В настоящее время практически у каждого человека есть мобильный телефон (смартфон), в котором может быть установлено медицинское приложение, многие пациенты используют переносимые медицинские устройства. Это позволяет следить за состоянием здоровья дистанционно. Появилась возможность диагностировать состояние здоровья пациента на расстоянии и отправлять данные врачу. Благодаря системе датчиков, расположенных, например, дома, а также на переносимых медицинских устройствах, можно отслеживать основные параметры здоровья, такие как кровяное давление, температура тела, уровень глюкозы и частота сердечных сокращений. Все данные, собранные датчиками, могут быть быстро переданы врачу. Все чаще в приложениях можно найти историю болезней пациентов и прочее. Интеграция технологий Интернета вещей сделала системы управления данными более уязвимыми⁴⁸². Устройства технологий Интернета вещей представляют угрозу с точки зрения нарушения безопасности и конфиденциальности данных. Расширенные полномочия по сбору и обработке данных означают, что стало проще, чем когда-либо, выводить, извлекать и прогнозировать конфиденциальные персональные данные, а также продавать и распространять эти данные третьим лицам.

Как показало исследование, проведенное в США, 29 из 36 приложений для борьбы с депрессией и курением передают данные сервисам, принадлежащим компаниям, таким как Facebook или Google, но только 12 точно указывают это в

⁴⁸² *Abouzakhar N.S., A. Jones, O. Angelopoulou (2017) Internet of things security: A review of risks and threats to healthcare sector, in: 2017 IEEE International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE, pp. 373–378.*

политике конфиденциальности⁴⁸³. В другом исследовании, в котором изучались 10 приложений, результат показал, что они передавали данные о действиях пользователей в приложении 70 различным субъектам (третьим сторонам), занимающимся рекламой и профилированием, без явного согласия пользователей⁴⁸⁴. Иные специализированные исследования показывают, что некоторые медицинские приложения оставляют остаточные данные о защищенной медицинской информации на аппаратном обеспечении используемого устройства⁴⁸⁵.

Все это подчеркивает главную проблему, которая заключается в нарушении конфиденциальности данных пациента и защиты права на неприкосновенность частной жизни в связи с применением технологий Интернета вещей.

Преобладающая модель защиты конфиденциальности в вышеуказанных технологиях Интернета вещей предполагает, что компании уведомляют людей об использовании и раскрытии их данных и предоставляют им право на согласие. Однако такие действия с их стороны в отношении персональных данных обычно содержатся в Политике конфиденциальности и Условиях предоставления услуг, и потребители должны подтвердить, что они прочитали и согласились с этими документами, прежде чем им разрешат пользоваться приложением или переносимым устройством.

⁴⁸³ *Huckvale K, Torous J, Larsen ME. (2019) Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation. JAMA Netw Open. 2(4), pp. 1-10*

⁴⁸⁴ Nutrition And Health Applications Do Not Respect Privacy. URL: <https://www.test-achats.be/action/espace-presse/communiqués-de-presse/2020/food-and-health-apps#> (дата обращения: 29.02.2025).

⁴⁸⁵ *Miller, S., Glisson, W. B., Campbell, M., & Sittig, S. (2019). Risk analysis of residual protected health information of android telehealth apps. Twenty-fifth Americas Conference on Information Systems, Cancun, pp. 1-10; McGowan, A. H., Sittig, S., & Menard, P. (2019). mHealth Cross-Contamination of User Health Data: Android Platform Analysis. Twenty-fifth Americas Conference on Information Systems, Cancun, pp. 1-5.*

Однако такая модель уведомления и согласия, по общему признанию многих зарубежных ученых, сама по себе является недостаточной для защиты права на неприкосновенность частной жизни⁴⁸⁶.

Уведомления о конфиденциальности и условия предоставления услуг, как известно, слишком объемны и трудны для понимания, а часто и вовсе отсутствуют. В эпоху цифровизации зачастую трудно предугадать все будущие варианты использования данных на момент их сбора. Опора на уведомление и согласие также перекладывает бремя защиты права на неприкосновенность частной жизни на человека, вместо того чтобы возложить на организации и держателей персональных данных ответственность за прозрачное и ответственное обращение с данными. Кроме того, организации могут менять свою политику согласия, а потребители могут не знать об этих изменениях или не иметь особого выбора, кроме как согласиться с ними, чтобы продолжать пользоваться услугами.

Организации, собирающие персональные данные, все равно должны быть обязаны быть прозрачными в отношении использования и раскрытия персональных данных. Хотя уведомление и согласие не должны быть единственным способом защиты персональных данных, люди по-прежнему хотят и должны иметь уведомление и некоторый выбор относительно сбора, использования и раскрытия информации, касающейся здоровья. Даже когда данные собираются с согласия отдельных лиц, возникают риски нарушения конфиденциальности, если данные используются в целях, выходящих за рамки изначально раскрытых. В связи с этим возникает риск чрезмерного сбора данных, выходящего за рамки того, что необходимо, то есть «на всякий случай», с использованием чрезмерно широких уведомлений о сборе и политик конфиденциальности в попытке «охватить все». Такая практика позволяет организациям заявлять о техническом соответствии своим обязательствам по

⁴⁸⁶ *Cate, F. H., & Mayer-Schönberger, V. (2013). Notice and consent in a world of Big Data. International Data Privacy Law, 3(2), pp. 67-73; Nissenbaum, H. (2011). A contextual approach to privacy online. Daedalus, 140(4), pp. 32-48; Pasquale, F. (2014). Redescribing health privacy: the importance of information policy. Hous. J. Health L. & Pol'y, 14, pp. 95.*

конфиденциальности данных, но это не соответствует основной цели принципа ограничения сбора. Кроме того, это подрывает возможность людей осуществлять значимый контроль над своей личной информацией.

На важность вопроса чрезмерного сбора конфиденциальных данных пациента указал Европейский суд по правам человека в деле Л.Х. против Латвии (L.H. v. Latvia) (№ 52019/07) от 29 апреля 2014 г. Заявительница, в частности, утверждала, что сбор ее личных медицинских данных государственным органом - в данном случае Инспекцией по контролю качества медицинского обслуживания и профессиональной пригодности («МАДЕККИ») - нарушил ее право на уважение частной жизни.

В этом решении Суд напомнил о важности защиты медицинских данных для осуществления права на уважение частной жизни. Он постановил, что в деле заявителя имело место нарушение права на частную жизнь, сочтя, что применимое законодательство не указало с достаточной ясностью объем дискреционных полномочий, предоставленных компетентным органам, и порядок их осуществления. Суд, в частности, отметил, что латвийское законодательство никак не ограничивало объем частных данных, которые могли быть собраны МАДЕККИ, что привело к сбору медицинских данных заявителя, относящихся к семилетнему периоду, без разбора и без предварительной оценки того, могут ли эти данные быть потенциально решающими, значимыми или важными для достижения какой-либо цели, которую могло преследовать рассматриваемое расследование⁴⁸⁷.

В российском законодательстве отсутствуют реально действующие механизмы обеспечения права личности на неприкосновенность персональных данных в сфере здравоохранения в случае использования технологий Интернета вещей. Чтобы решить проблему возможной угрозы раскрытия персональных данных пациента при использовании информационных технологий, необходимо перспективное и более совершенное правовое регулирование в данной области.

⁴⁸⁷ L.H. v. Latvia - 52019/07. URL: [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22002-9365%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22002-9365%22]}) (дата обращения: 29.02.2025).

В этой связи целесообразно обратиться к ранее рассмотренным в диссертации положениям Закона о защите персональной информации КНР, Общего регламента ЕС о защите данных и новых законов штатов США о защите частной жизни, таких как Закон Калифорнии о защите персональных данных потребителей и Закон о конфиденциальности медицинской информации штата Нью-Йорк и др., которые закрепляют либо согласие на сбор, либо отказ от сбора и согласие на использование данных, особенно коммерческими компаниями.

Представляется, что следовало бы, в первую очередь, внедрить в Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» подходы, примененные в Законе о защите персональной информации КНР, касающиеся сбора личной информации, которая должна быть ограничена минимальным объемом для целей обработки, притом, что чрезмерный сбор личной информации не допускается. Это необходимо для регулирования обработки персональных данных организациями, собирающими такие данные через технологии Интернета вещей в здравоохранении. На практике мобильные приложения настроены собирать избыточное количество информации, и по-прежнему сложно определить, какие типы информации необходимы для конкретной обработки⁴⁸⁸.

Как отмечено в разделе 3.3. параграфа 3 главы 1 исследования, в целях ограничения получения избыточного количества информации, получаемой с мобильных медицинских приложений, было выпущено Положение об объеме необходимой личной информации для общих типов мобильных приложений КНР, в результате любой сбор личной информации за пределами установленного объема может считаться незаконным.

Целесообразно по аналогии предусмотреть такое положение в России, чтобы норма об объеме необходимой личной информации для общих типов мобильных

⁴⁸⁸ Procuratorial Organs Actively Maintain Personal Information Security, Handling More than 2,000 Public Interest Litigation Cases in the Field of Personal Information Protection in 2021'. URL: https://www.spp.gov.cn/spp/xwfbh/wsfbh/202202/t20220227_545967.shtml (дата обращения: 29.02.2025).

приложений перечисляла различные категории мобильных приложений и предоставляла операторам мобильных приложений практические рекомендации о том, какие типы данных будет разумно собирать. Необходимо подобное руководство, чтобы определить, какие типы данных считаются необходимыми для медицинских приложений. В связи с быстрым появлением мобильных медицинских приложений представляется разумным создать перечень приложений, поддерживающих различные медицинские функции.

Кроме того, пациенты, использующие технологии Интернета вещей, как правило, не знают, что технологии постоянно отслеживают их сферу интересов, а персональные данные продаются организациям для целей рекламы или слежения. Большинство пользователей также не понимают, какой объем информации собирается, хранится и продается в интересах третьих лиц. Как правило, пациенты в полной мере не владеют информацией о том, где содержатся их персональные данные, какая медицинская информация собирается и монетизируется⁴⁸⁹, и практически не имеют возможности по своему усмотрению распоряжаться ими, изменить или исключить их из свободного доступа, а с учетом развития технологий Интернета вещей встает вопрос их надлежащего регулирования, в том числе и в целях защиты права на неприкосновенность частной жизни.

Следовательно, следует соблюсти принцип информированности и рассмотреть возможность в законодательстве России в сфере персональных данных, например, в главе 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» установить право субъектов персональных данных на согласие или несогласие при продаже его обработанных персональных данных оператором третьим лицам. Аналогичные нормы закрепляют право отказаться от продажи своих данных в Законе Калифорнии о защите персональных данных потребителей и в Законе о конфиденциальности медицинской информации штата Нью-Йорк.

⁴⁸⁹ Grande, D., Marti, X. L., Feuerstein-Simon, R., Merchant, R. M., Asch, D. A., Lewson, A., & Cannuscio, C. C. (2020). Health policy and privacy challenges associated with digital technology. *JAMA network open*, 3(7), pp. 1-11.

Это подразумевает соблюдение требований прозрачности оператора в отношении того, каким образом персональные данные оператор продал или передал третьим лицам, тем самым предоставив субъектам персональных данных больший контроль над своими данными, в том числе медицинскими персональными данными.

Данная норма необходима для установления запрета продажи персональных данных оператором третьим лицам в коммерческих целях, которые основаны исключительно на личной информации пациента при использовании мобильных медицинских приложений без предварительного явного согласия⁴⁹⁰.

При этом стоит отметить, что норма ст. 15 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» не относится к вышеуказанному случаю, поскольку данная норма была принята в целях регулирования таких отношений под влиянием Директивы 2002/58/ЕС Европейского парламента и Совета ЕС от 12.07.2002 об обработке персональных данных и защите информации о частной жизни в сфере электронных коммуникаций и не относится к информации, собираемой технологиями Интернета вещей⁴⁹¹.

Таким образом, на основе проведенного в этой части параграфа анализа рисков нарушения права на неприкосновенность частной жизни в сфере здравоохранения в результате влияния технологий Интернета вещей можно сформулировать следующий вывод.

Право на неприкосновенность частной жизни в условиях цифровизации и внедрения информационных технологий, особенно в сфере здравоохранения, становится всё более уязвимым.

Чтобы решить проблему возможной угрозы раскрытия персональных данных пациента при использовании информационных технологий, необходимо

⁴⁹⁰ Под термином «продажа» можно понимать передачу устно, письменно или с помощью электронных или других средств оператором персональных данных субъекта третьему лицу за денежное или иное ценное вознаграждение.

⁴⁹¹ *Амелин Р.В., Богатырева Н.В., Волков Ю.В., Марченко Ю.А., Федосин А.С.* Комментарий к Федеральному закону от 27.07.2006 N 152-ФЗ "О персональных данных" (постатейный) // СПС "КонсультантПлюс".

перспективное и более совершенное правовое регулирование в данной области, особенно в части технологий Интернета вещей.

Для этой цели следовало бы внедрить в Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» подходы, примененные в Законе о защите персональной информации КНР, касающиеся сбора личной информации, который должна быть ограничен минимальным объемом для целей обработки. Также предложено на основе Положения об объеме необходимой личной информации для общих типов мобильных приложений КНР разработать аналогичное регулирование в России.

Кроме того, поскольку пациенты, использующие технологии Интернета вещей, как правило, не знают, что персональные данные продаются организациям для целей рекламы или слежения, важно было бы рассмотреть возможность в законодательстве России в сфере персональных данных, например, в главе 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» установить право субъектов персональных данных на предварительное согласие при продаже его обработанных персональных данных оператором третьим лицам в коммерческих целях, в том числе с использованием правовой модели, примененной в Законе Калифорнии о защите персональных данных потребителей и Законе о конфиденциальности медицинской информации штата Нью-Йорк.

ЗАКЛЮЧЕНИЕ

Проведенное исследование подтверждает, что цифровая трансформация здравоохранения представляет собой не просто технологический сдвиг, но и глубокий конституционно-правовой вызов, затрагивающий фундаментальные основы взаимоотношений личности, общества и государства. Внедрение информационных технологий в сферу здравоохранения, будучи объективно необходимым для повышения эффективности и доступности медицинской помощи, одновременно порождает комплекс новых проблем для реализации конституционных прав граждан и требует формирования адекватной правовой среды.

Анализ международных стандартов и зарубежных моделей регулирования (ЕС, США, КНР) применения информационных технологий в здравоохранении демонстрирует, что правовые ответы на технологические вызовы варьируются в зависимости от особенностей национального правового регулирования, государственного устройства и социально-экономических приоритетов. Однако общим трендом является осознание необходимости построения целостных правовых рамок, основанных на балансе между стимулированием инноваций и обеспечением надежных гарантий прав человека. Европейский риск-ориентированный подход, американская гибкость в сочетании с активным регулированием на уровне штатов и китайская модель с акцентом на государственный контроль представляют ценный опыт для осмысления, но не могут быть механически перенесены в российскую правовую систему.

Конституционные поправки 2020 года, закрепившие информационные технологии в исключительном ведении Российской Федерации, заложили важную правовую основу для централизованного построения политики цифровизации. Это создало необходимый фундамент. Тем не менее исследование выявило, что правовое регулирование применения ключевых информационных технологий в российском здравоохранении (технологий искусственного интеллекта, Интернета

вещей, анализа больших данных, обработки первичных данных и телемедицинских технологий) носит пробельный характер.

В целом можно отметить следующее.

1. Основой для многих выводов в части совершенствования концепции профильного российского законодательства в данной работе стал сравнительный анализ законодательства ЕС, КНР и США, который был разделен на рамочное правовое регулирование применения информационных технологий в сфере здравоохранения, фрагментированное правовое регулирование вопросов здравоохранения в части применения информационных технологий и специализированное правовое регулирование применения информационных технологий в сфере здравоохранения. Данное компаративистское исследование законодательства ЕС, КНР и США проведено для того, чтобы выявить проблемы в области реализации конституционных прав, возникающие в результате цифровизации (рассматриваемые во второй главе), а также оценить соответствие российского законодательства современным вызовам. Проведенный сравнительный анализ позволил идентифицировать конкретные нормативные правовые акты зарубежных стран, релевантные для решения проблем российской практики.

Выбор национального законодательства Швейцарии, Германии, Австрии, Франции, Великобритании, Финляндии для более глубокого исследования обусловлен их лидирующим опытом в области регулирования применения различных видов информационных технологий: этот факт может быть использован для решения аналогичных проблем в России.

2. В России в целом сформирована неплохая законодательная основа применения информационных технологий, более того, поправки 2020 г. в Конституцию России ознаменовали процесс конституционализации, связанный с цифровизацией и вызванной ею трансформацией конституционных прав и свобод.

Однако конституционализация применения информационных технологий пока не привела к должной защите прав граждан в этой области. Государство, взяв

на себя исключительные полномочия по обеспечению безопасности в цифровой сфере, должно реализовать их через создание комплексной системы гарантий, которая:

- устанавливала бы четкие, конституционные принципы и нормы, определяющие особенности делегирования полномочий органов государственной власти в части правового регулирования применения информационных технологий;

- определяла бы требования к внедрению информационных технологий в сферу здравоохранения, обеспечивая соблюдение законности и защиту прав и свобод граждан, а также соответствующие правовые механизмы и меры, направленные на балансирование потенциальных рисков и преимуществ новых технологий и на обеспечение прозрачности и ответственности в их использовании;

- наделяла бы пациентов действенными инструментами контроля за своими медицинскими данными.

3. Российская сфера здравоохранения трансформируется в результате воздействия технологий обработки первичных данных, которые внедрены для управления ею, в том числе совершенствования процесса принятия медицинских решений (на примере ЕГИСЗ).

Несмотря на рост административной эффективности и очевидные успехи в повышении доступности медицинских услуг, подтверждаемые растущей активностью пользователей, ЕГИСЗ создаёт новые риски. Они связаны с потенциальным ограничением автономии пациента и необходимости получения его информированного согласия в условиях сквозного обмена данными. Для их устранения представляется целесообразным обратиться к соответствующим правовым и организационным подходам, разработанным в ЕС.

Отсутствие надлежащего способа правового регулирования технологий Интернета вещей является одним из ключевых факторов, сдерживающих их внедрение в здравоохранение.

В законодательстве России отсутствует классификация и требования к

регистрации технологий Интернета вещей в силу того, что фитнес-браслеты, смарт-часы, портативные приборы и иные носимые устройства не относятся к медицинским устройствам согласно классификации Росздравнадзора. Для решения данной проблемы предложено заимствовать подходы к регулированию приложений и устройств на базе технологий Интернета вещей, применяемые во Франции и Великобритании, и даны рекомендации по совершенствованию отечественного законодательства.

Поскольку искусственный интеллект продолжает проникать в здравоохранение, представляется необходимым разработать и внедрить требования, которые отдадут приоритет правам и интересам пациентов, одновременно способствуя росту и развитию технологий искусственного интеллекта. Механизм правового регулирования применения искусственного интеллекта остается несформированным. Разработка надежной нормативно-правовой базы позволит использовать возможности искусственного интеллекта для улучшения ухода за пациентами и развития медицинских исследований, обеспечив при этом ответственное и справедливое использование технологии.

В целом правовое регулирование искусственного интеллекта в здравоохранении представляет собой нелегкую задачу. В работе предложено применить подход по общему регулированию искусственного интеллекта с использованием риск-ориентированного подхода. Также в диссертации даны рекомендации по разработке федерального закона об искусственном интеллекте в России на основе положений Закона об искусственном интеллекте ЕС и опыта Казахстана, разработавшего аналогичный Закон об искусственном интеллекте.

В части отечественного правового регулирования применения технологий анализа больших данных на примере электронных медицинских карт выявлена проблема отсутствия прямого закрепления права пациента на ограничение доступа к своей электронной медицинской карте. Для устранения этого недостатка рекомендовано обратиться к опыту Австрии и Швейцарии. В этих странах пациенты обладают правом ограничивать доступ третьих лиц к своей медицинской

карте, включая возможность выборочно предоставлять разрешение определённым медработникам и вводить запрет на доступ для других лиц.

Действующее российское законодательство не содержит конкретных норм, регламентирующих обеспечение врачебной тайны в процессе передачи персональных данных пациента врачу с применением телемедицинских технологий. В связи с этим были выдвинуты предложения по совершенствованию отечественной правовой базы на основе опыта Германии.

4. Исследование показало, что сохраняется ряд проблем, возникающих в связи с нарушением отдельных конституционных прав человека в результате применения информационных технологий в здравоохранении и ее цифровизацией.

Так, право на неприкосновенность частной жизни сталкивается с системными угрозами, связанными с масштабным сбором и потенциальной монетизацией чувствительных медицинских данных, особенно через устройства технологий Интернета вещей. Существующая модель «уведомления и согласия» оказывается неэффективной в условиях сложности и непрозрачности процессов обработки данных.

Право на охрану здоровья и медицинскую помощь трансформируется под влиянием искусственного интеллекта. Возникает парадокс: технологии, призванные повысить качество помощи, могут его снизить из-за ошибок алгоритмов искусственного интеллекта, эффекта «черного ящика» и размывания персональной ответственности врача. Классическая доктрина информированного согласия требует адаптации к ситуациям, когда значимый вклад в диагноз или план лечения вносит искусственный интеллект.

Право на доступ к информации приобретает новые особенности, связанные с контролем пациента над собственной электронной медицинской картой. Отсутствие у граждан возможности не только получать, но и активно дополнять, а в некоторых случаях – ограничивать доступ к своим медицинским данным, свидетельствует о недостаточной реализации принципа автономии пациента.

Кроме того, технологические риски, связанные с информационными технологиями, актуализируют вопрос возникновения в национальном законодательстве новых правомочий. Эти правомочия — такие как право на прозрачность решений, принимаемых искусственным интеллектом, ограничение пациентом доступа к электронной медицинской карте или информированность пациента о применении искусственного интеллекта в его лечении, — являются необходимым элементом конституционных прав человека в цифровой среде. В случае отсутствия их закрепления в отечественном законодательстве применение информационных технологий приведет к еще более явным нарушениям конституционных прав человека, а также - к увеличению количества правовых проблем.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Международные акты

1. Американская декларация прав и обязанностей человека (обзор). URL: <https://hrlib.kz/document/199513> (дата обращения: 28.03.2025)
2. Всеобщая декларация о биоэтике и правах человека. URL: https://www.un.org/ru/documents/decl_conv/declarations/bioethics_and_hr.shtml (дата обращения: 28.03.2025).
3. Всеобщая декларация прав человека. URL: https://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml (дата обращения: 28.03.2025).
4. Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Заключена в г. Страсбурге 28.01.1981) // "Собрание законодательства РФ", 03.02.2014, № 5, ст. 419.
5. Конвенция о защите прав и достоинства человека в связи с применением достижений биологии и медицины: Конвенция о правах человека и биомедицине. URL: <http://hrlibrary.umn.edu/russian/euro/Rz37.html> (дата обращения: 28.03.2025).
6. Конвенция о здравоохранении и медицинском обслуживании моряков. URL: https://www.ilo.org/sites/default/files/wcmsp5/groups/public/@ed_norm/@normes/documents/normativeinstrument/wcms_c164_ru.htm (дата обращения: 28.03.2025)
7. Международный пакт о гражданских и политических правах. URL: https://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml (дата обращения: 28.03.2025).
8. Международный пакт об экономических, социальных и культурных правах. URL: https://www.un.org/ru/documents/decl_conv/conventions/pactecon.shtml (дата обращения: 28.03.2025).
9. Протокол к Конвенции о защите прав человека и основных свобод. URL: <http://hrlibrary.umn.edu/russian/euro/Rz20prot1.html> (дата обращения: 28.03.2025).

10. Протокол о внесении изменений в Соглашение о сотрудничестве государств - участников СНГ в создании совместимых национальных телемедицинских систем и дальнейшем их развитии и использовании от 19 ноября 2010 года. URL: https://www.mid.ru/ru/foreign_policy/international_contracts/international_contracts/multilateral_contract/62714/ (дата обращения: 28.03.2025).
11. Хартия Европейского союза об Основных правах. URL: <https://eulaw.ru/treaties/charter/> (дата обращения: 15.09.2024).
12. Additional protocol to the American convention on human rights in the area of economic, social and cultural rights "Protocol of San Salvador". URL: <https://www.oas.org/juridico/english/treaties/a-52.html> (дата обращения: 28.03.2025).
13. Committee on Artificial Intelligence (CAI) - Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. URL: [https://search.coe.int/cm#{%22CoEIdentifier%22:\[%220900001680afb11f%22\],%22sort%22:\[%22CoEValidationDate%20Descending%22\]}](https://search.coe.int/cm#{%22CoEIdentifier%22:[%220900001680afb11f%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}) (дата обращения: 28.03.2025).

Нормативные правовые акты Российской Федерации

14. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Российская газета, № 237 (853).
15. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // «Собрание законодательства РФ», 31.07.2006, № 31 (1 ч.), ст. 3448.
16. Федеральный закон от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» // «Собрание законодательства РФ», 28.11.2011, № 48, ст. 6724.
17. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // «Собрание законодательства РФ», 31.07.2006, № 31 (1 ч.), ст. 3451.

18. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // «Собрание законодательства РФ», 31.07.2017, № 31 (Часть I), ст. 4736.
19. Федеральный закон от 29 июля 2017 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам применения информационных технологий в сфере охраны здоровья» // «Собрание законодательства РФ», 31.07.2017, № 31 (Часть I), ст. 4791.
20. Федеральный закон от 24 апреля 2020 г. № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в ст. 6 и 10 Федерального закона «О персональных данных» // "Собрание законодательства РФ", 27.04.2020, № 17, ст. 2701.
21. Федеральный закон от 31 июля 2020 г. № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых и технологических инноваций в Российской Федерации» // «Собрание законодательства РФ», 03.08.2020, № 31 (часть I), ст. 5017.
22. Федеральный закон от 8 июля 2024 г. № 169-ФЗ «О внесении изменений в Федеральный закон «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» // «Собрание законодательства РФ», 15.07.2024, № 29 (Часть II), ст. 4098.
23. Федеральный закон от 20 марта 2025 г. № 33-ФЗ «Об общих принципах организации местного самоуправления в единой системе публичной власти» // "Собрание законодательства РФ", 28.11.2011, № 48, ст. 6724.
24. Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» // «Собрание законодательства РФ», 15.05.2017, № 20, ст. 2901.
25. Указ Президента Российской Федерации от 8 декабря 2025 г. № 896 «О Стратегии развития здравоохранения в Российской Федерации на период до 2030 года» // «Собрание законодательства РФ», 15.12.2025, № 50, ст. 7826.

26. Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» // «Собрание законодательства РФ», 14.10.2019, № 41, ст. 5700.
27. Указ Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // «Собрание законодательства РФ», 05.07.2021, № 27 (часть II), ст. 5351.
28. Указ Президента Российской Федерации от 15 февраля 2024 г. № 124 «О внесении изменений в Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» и в Национальную стратегию, утвержденную этим Указом» // «Собрание законодательства РФ», 19.02.2024, № 8, ст. 1102.
29. Указ Президента Российской Федерации от 7 мая 2024 г. № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» // «Собрание законодательства РФ», 13.05.2024, № 20, ст. 2584.
30. Постановление Правительства Российской Федерации от 15 декабря 2020 г. № 2110 «Об утверждении Правил предоставления из федерального бюджета субсидии на проведение повышения квалификации преподавателей высшего и среднего профессионального образования по новым программам для ИТ-специальностей и различных предметных отраслей и обеспечение достижения отдельных результатов федерального проекта «Кадры для цифровой экономики» на базе автономной некоммерческой организации высшего образования «Университет Иннополис» // «Собрание законодательства РФ», 28.12.2020, № 52 (Часть I), ст. 8808.
31. Постановление Правительства Российской Федерации от 9 февраля 2022 г. № 140 «О единой государственной информационной системе в сфере здравоохранения» // «Собрание законодательства РФ», 21.02.2022, № 8, ст. 1152.
32. Постановление Правительства Российской Федерации от 9 декабря 2022 г. № 2276 «Об установлении экспериментального правового режима в сфере цифровых

инноваций и утверждении Программы экспериментального правового режима в сфере цифровых инноваций по направлению медицинской деятельности с применением технологий сбора и обработки сведений о состоянии здоровья и диагнозов граждан в отношении реализации инициативы социально-экономического развития Российской Федерации «Персональные медицинские помощники» // «Собрание законодательства РФ», 19.12.2022, № 51, ст. 9237.

33. Постановление Правительства Российской Федерации от 18 июля 2023 года № 1164 «Об установлении экспериментального правового режима в сфере цифровых инноваций и утверждении Программы экспериментального правового режима в сфере цифровых инноваций по направлению медицинской деятельности, в том числе с применением телемедицинских технологий и технологий сбора и обработки сведений о состоянии здоровья и диагнозах граждан» // «Собрание законодательства РФ», 24.07.2023, № 30, ст. 5693.

34. Постановление Правительства Российской Федерации от 30 ноября 2024 г. № 1684 «Об утверждении Правил государственной регистрации медицинских изделий» // «Собрание законодательства РФ», 09.12.2024, № 50, ст. 7744.

35. Распоряжение Правительства Российской Федерации от 19 августа 2020 г. № 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года» // «Собрание законодательства РФ», 31.08.2020, № 35, ст. 5593

36. Распоряжение Правительства Российской Федерации от 16 марта 2024 г. № 637-р «Об утверждении стратегического направления в области цифровой трансформации государственного управления» // "Собрание законодательства РФ", 25.03.2024, № 13, ст. 1837.

37. Приказ Минздрава России от 11 ноября 2013 года № 18-1/1010 «Основные разделы электронной медицинской карты». URL: <https://www.garant.ru/products/ipo/prime/doc/70425516/> (дата обращения: 28.11.2024).

38. Приказ Минкомсвязи России от 23 апреля 2020 г. № 195 «Об утверждении методик расчета показателей федерального проекта "Цифровые технологии" национальной программы "Цифровая экономика Российской Федерации». URL: <https://base.garant.ru/74858195/> (дата обращения: 28.11.2024)

39. Приказ Минздрава России от 7 сентября 2020 г. № 947н «Об утверждении Порядка организации системы документооборота в сфере охраны здоровья в части ведения медицинской документации в форме электронных документов». URL: <http://publication.pravo.gov.ru/Document/View/0001202101120007> (дата обращения: 28.11.2024).

40. Приказ Минздрава России от 11 апреля 2025 г. № 193н «Об утверждении Порядка организации и оказания медицинской помощи с применением телемедицинских технологий». URL: <http://publication.pravo.gov.ru/document/0001202505150033> (дата обращения: 28.11.2025)

Зарубежные нормативные правовые акты

41. Конституция Соединенных Штатов Америки. URL: <https://www.wipo.int/wipolex/ru/legislation/details/21129> (дата обращения: 15.09.2024)

42. Конституция КНР 1982 г. (с изм. 1988, 1993, 1999, 2004 гг.). URL: https://chinalawinfo.ru/constitutional_law/constitution (дата обращения: 15.09.2024)

43. Act on the Electronic Processing of Client Data in Healthcare and Social Welfare. URL: <https://www.kanta.fi/en/legislation> (дата обращения: 28.11.2024)

44. An Act regulating the use of artificial intelligence (AI) in providing mental health services. URL: <https://malegislature.gov/Bills/193/H1974> (дата обращения: 28.11.2024)

45. AB-3030 Health care services: artificial intelligence. URL: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB3030

- (дата обращения: 28.11.2025) Bundesgesetz über das elektronische Patientendossier. URL: <https://www.fedlex.admin.ch/eli/cc/2017/203/de> (дата обращения: 28.11.2024)
46. Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Gesundheitstelematikgesetz 2012. URL: <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20008120> (дата обращения: 28.11.2024)
47. Concerning consumer protections in interactions with artificial intelligence systems. URL: https://leg.colorado.gov/sites/default/files/2024a_205_signed.pdf (дата обращения: 28.11.2024)
48. Code de la santé publique. URL: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006072665/LEGISCTA000038841870/#LEGISCTA000038841870 (дата обращения: 28.11.2024).
49. ССРА Text. URL: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 (дата обращения: 15.09.2024)
50. Digital-Gesetz (DigiG). URL: <https://www.bundesgesundheitsministerium.de/service/gesetze-und-verordnungen/detail/digital-gesetz.html> (дата обращения: 28.11.2024)
51. D.C. Law 22-126. Telehealth Medicaid Expansion Amendment Act of 2018. URL: <https://code.dccouncil.gov/us/dc/council/laws/22-126> (дата обращения: 28.11.2024)
52. General Data Protection Regulation. URL: <https://gdpr-info.eu/> (дата обращения: 28.11.2024)
53. Gesetzgebung Elektronisches Patientendossier (EPDG). URL: <https://www.bag.admin.ch/bag/de/home/gesetze-und-bewilligungen/gesetzgebung/gesetzgebung-mensch-gesundheit/gesetzgebung-elektronisches-patientendossier.html> (дата обращения: 28.11.2024)
54. IoT Cybersecurity Improvement Act of 2020. URL: <https://www.congress.gov/bill/116th-congress/house-bill/1668> (дата обращения: 28.11.2024)

55. Healthy Technology Act of 2025. URL: <https://www.congress.gov/bill/119th-congress/house-bill/238> (дата обращения: 28.01.2026)
56. 21st Century Cures Act. URL: <https://www.congress.gov/bill/114th-congress/house-bill/34> (дата обращения: 28.11.2024)
57. Telemental Health Expansion Act of 2020, H.R.5201, 116th Cong. (2020). URL: <https://www.congress.gov/bill/116th-congress/house-bill/5201/text> (дата обращения: 28.11.2024)
58. Health Insurance Portability and Accountability Act of 1996. URL: <https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996> (дата обращения: 15.09.2024)
59. HITECH Act Summary. URL: <https://www.hipaasurvivalguide.com/hitech-act-summary.php> (дата обращения: 15.09.2024)
60. Law of the People's Republic of China on Basic Medical and Health Care and Promotion of Health. URL: http://en.moj.gov.cn/2021-06/26/c_636455.htm (дата обращения: 28.11.2024)
61. Office for Civil Rights (OCR), 2002. Standards for privacy of individually identifiable health information. Final rule. Federal Register, 67(157), p.53181, §164.514 (a).
62. Personal Information Protection Law of the People's Republic of China. URL: <https://personalinformationprotectionlaw.com/PIPL/category/general-provisions/definitions/> (дата обращения: 28.11.2024)
63. Provisions on the Scope of Necessary Personal Information for Common Types of Mobile Internet Applications. URL: <https://www.chinalawtranslate.com/en/necessary-app-info/> (дата обращения: 28.11.2024)
64. Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space COM/2022/197 final. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0197> (дата обращения: 28.11.2024)

65. Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847. URL: <https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng> (дата обращения: 28.11.2024)
66. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0745> (дата обращения: 28.11.2024)
67. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng> (дата обращения: 28.11.2024)
68. Regulation on medical records management in medical institutions. URL: https://english.www.gov.cn/policies/latest_releases/2014/08/23/content_281474983027052.htm (дата обращения: 28.11.2024)
69. S.2333 - Pandemic and All-Hazards Preparedness and Response Act. URL: <https://www.congress.gov/bill/118th-congress/senate-bill/2333/text> (дата обращения: 28.01.2026)
70. Senate Bill S929. New York Health Information Privacy Act. URL: <https://www.nysenate.gov/legislation/bills/2025/S929> (дата обращения: 02.05.2025)
71. Senate Bill No. 1120. «Health care coverage: utilization review» URL: https://custom.statenet.com/public/resources.cgi?mode=show_text&id=ID:bill:CA2023000S1120&verid=CA2023000S1120_20240928_0_CH& (дата обращения: 28.11.2024)

72. Senate Bill No. 327. The Security of Connected Devices URL: https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327 (дата обращения: 28.11.2024)
73. Improving the Nation's Cybersecurity. URL: <https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity> (дата обращения: 28.11.2024)
74. Verordnung über das Verfahren und die Anforderungen zur Prüfung der Erstattungsfähigkeit digitaler Gesundheitsanwendungen in der gesetzlichen Krankenversicherung (Digitale Gesundheitsanwendungen-Verordnung - DiGAV). URL: <https://www.gesetze-im-internet.de/digav/BJNR076800020.html> (дата обращения: 28.11.2024)
75. Washington my health my data Act. URL: <https://app.leg.wa.gov/RCW/default.aspx?cite=19.373&full=true> (дата обращения: 28.11.2024)
76. Executive Order on Improving the Nation's Cybersecurity. URL: <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/> (дата обращения: 28.11.2024).
77. Образец профессионального кодекса для врачей, работающих в Германии – (МВО-Ä 1997)-, сформулированный на основании решения 114-го съезда врачей в г. Киль 2011. URL: <https://nacmedpalata.ru/?action=show&id=8962> (дата обращения: 28.11.2024)
78. Положение о надзоре и управлении медицинскими изделиями. URL: <https://www.nmpa.gov.cn/xxgk/fgwj/flxzhfg/20210319202057136.html> (дата обращения: 28.11.2024)

Судебные акты

79. Постановление Конституционного Суда Российской Федерации от 26 октября 2017 г. № 25-П «По делу о проверке конституционности пункта 5 статьи 2 Федерального закона «Об информации, информационных технологиях и о защите

информации» в связи с жалобой гражданина А.И. Сушкова» // «Собрание законодательства РФ», 06.11.2017, № 45, ст. 6735

80. Постановление Конституционного Суда Российской Федерации от 22.03.2005 № 4-П «По делу о проверке конституционности ряда положений Уголовно-процессуального кодекса Российской Федерации, регламентирующих порядок и сроки применения в качестве меры пресечения заключения под стражу на стадиях уголовного судопроизводства, следующих за окончанием предварительного расследования и направлением уголовного дела в суд, в связи с жалобами ряда граждан» // «Российская газета», № 66, 01.04.2005.

81. Постановление Конституционного Суда Российской Федерации от 23.09.2014 № 24-П «По делу о проверке конституционности части 1 статьи 6.21 Кодекса Российской Федерации об административных правонарушениях в связи с жалобой граждан Н.А. Алексеева, Я.Н. Евтушенко и Д.А. Исакова» // «Российская газета», № 226, 03.10.2014.

82. Постановление Конституционного Суда Российской Федерации № 1-П от 13 января 2020 "По делу о проверке конституционности части первой статьи 111 и части первой статьи 112 Уголовного кодекса Российской Федерации, а также пункта 3 Правил определения степени тяжести вреда, причиненного здоровью человека, в связи с жалобой гражданина Б." // "Собрание законодательства РФ ", 22.01.2024, № 4, ст. 591.

83. Решение Октябрьского районного суда г. Архангельска от 7 марта 2017 года по делу № 2-1180/2017 ~ М-9858/2016. URL: https://oktsud--arh.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=285308532&case_uid=70829744-c194-45e0-b8a9-03d52ce992c8&delo_id=1540005&new= (дата обращения: 28.01.2025)

84. Dobbs v. Jackson Women's Health Organization. URL: <https://www.oyez.org/cases/2021/19-1392> (дата обращения: 02.05.2025)

85. I v. FINLAND. URL: [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-87510%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-87510%22]}) (дата обращения: 14.01.2025)

86. L.H. v. Latvia - 52019/07. URL: [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22002-9365%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22002-9365%22]}) (дата обращения: 29.02.2025).
87. Y.G. v. Russia. URL: [https://hudoc.echr.coe.int/fre#{%22itemid%22:\[%22002-13761%22\]}](https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-13761%22]}) (дата обращения: 28.11.2024)
88. Z v. Finland. URL: [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22002-9432%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22002-9432%22]}) (дата обращения: 28.11.2024)

Монографии, сборники статей, учебная литература

89. Баранов А. А. Интернет вещей: теоретико-методологические основы правового регулирования. Т.1: Сферы применения, риски и барьеры, проблемы правового регулирования: монография / О.А. Баранов; НИИ ИП НАПрН Украины – К.: Издательский дом «АртЕк». 2018. 344 с.
90. Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право: учебник / Под ред. Топорнина Б.Н. – Спб.: Юрид. центр Пресс, 2001. 789 с.
91. Богдановская И.Ю. Правовое регулирование телемедицины: опыт США // Материалы конференции «Информатизация здравоохранения и социальной сферы в регионах России: проблемы координации и информационного обмена». М., 2007. № 3. С. 64–68.
92. Волкова Г. Е. Трансформация права на неприкосновенность частной жизни в условиях цифровизации общества // Цифровые технологии и право : Сборник научных трудов I Международной научно-практической конференции. В 6-ти томах, Казань, 23 сентября 2022 года. Казань: Издательство "Познание", 2022. С. 78-82.
93. Вороньжева И. И., Федотова Г. В. Единый цифровой контур здравоохранения (ЕГИСЗ) // Актуальные тренды цифровой трансформации промышленных предприятий: сборник статей Всероссийской научно-практической конференции, Казань, 30–31 октября 2024 года. Курск: ЗАО «Университетская книга», 2024. С. 70-74.

94. Владзимирский А. В., Морозов С. П., Урванцева И. А., Коваленко Л. В., Воробьев А. С. Применение телемедицинских технологий в кардиологии : учеб. пособие; Сургут. гос. ун-т. Сургут : Изд-во СурГУ, 2019. 115 с.
95. Государство и право в новой цифровой реальности : монография / под общ. ред. д-ра юрид. наук, проф. И.А. Умновой-Конюховой и д-ра техн. наук, проф. Д.А. Ловцова. – М.: РАН. ИНИОН, 2020. 259 с.
96. Камалова Г. Г. Перспективы правового регулирования применения искусственного интеллекта и робототехники в здравоохранении // Исследование и практика в социально-экономической и гуманитарной сфере: сборник избранных статей Всероссийской (национальной) научно-практической конференции, Санкт-Петербург, 13 января 2022 года. – Санкт-Петербург: ГНИИ «Нацразвитие», 2022. С. 55-58.
97. Климович Е. В. О сущности понятия «персональные данные» как конфиденциальной информации особой категории // Международные юридические чтения : материалы ежегодной международной научно-практической конференции (14 апреля 2005 г.). — Омск : Изд-во Омск. юрид. ин-та, 2005. С. 21—30.
98. Колонтаевская, И. Ф. Правовое регулирование цифровой медицины в Российской Федерации // Новое в науке и образовании : Материалы Международной ежегодной научно-практической конференции, Москва, 04 апреля 2023 года / Отв. редактор Е.В. Дмитриев, сост. Э.Н. Замега. – Ростов-на-Дону: Общество с ограниченной ответственностью «Манускрипт», 2023. С. 177-181.
99. Костоломова К.К, Николенко Т.А. К вопросу классификации информационных технологий // Математические методы и модели в управлении, экономике и социологии : Сборник научных трудов. Том Выпуск 7. – Тюмень : Тюменский государственный нефтегазовый университет. 2013. С. 167-170.
100. Кравец И.А. Цифровизация, право и конституция // Право цифровой среды: Монография / Под редакцией Т.П. Подшивалова, Е.В. Титовой, Е.А. Громовой. Москва, 2022. С. 185-200.

101. Мещеряков А. Н. Искусственный интеллект в предмете конституционного права // Право в эпоху искусственного интеллекта: перспективные вызовы и современные задачи : сборник научных статей по материалам Международного научно-практического форума «VI Сибирские правовые чтения», г. Тюмень, 17-19 октября 2024 г. / гл. ред. С. С. Зенин ; отв. ред. Л. В. Иванова ; Министерство науки и высшего образования Российской Федерации, Тюменский государственный университет, Институт государства и права. - Тюмень : ТюмГУ-Press, 2024. С. 36–40.
102. Минько Н.С., Курилович М. П Перспективы развития правовых отношений в области здравоохранения в условиях внедрения систем искусственного интеллекта // Правовое регулирование в сфере здравоохранения в условиях новых вызовов: вопросы теории и практики : Материалы Всероссийской научно-практической конференции с международным участием, Тамбов, 25–26 марта 2022 года / Отв. редактор Р.В. Зелепукин. Тамбов: Издательский дом "Державинский", 2022. С. 102-117.
103. Роуз К., Элдридж С., Чапин Л. Интернет вещей: краткий обзор // Вопросы и проблемы использования сети Интернет в более глобальном масштабе. ICOS. 2015. С. 1-75.
104. Сорокин Д.А., Гречушкина Н.В. Цифровые технологии в медицине // Актуальные проблемы физики и технологии в образовании, науке и производстве: материалы IV Всероссийской научно-практической конференции, посвященной 120-летию Александра Васильевича Пёрышкина. Рязань, 2022. С. 173-175.
105. Титоренко Г. А. Информационные системы в экономике: учебник для студентов вузов, обучающихся по специальностям «Финансы и кредит», «Бухгалтерский учет, анализ и аудит» и специальностям экономики и управления / Под ред. Г. А. Титоренко. – 2-е изд., перераб. и доп. – М.: ЮНИТИ-ДАНА. 2008. 463 с.
106. Федотов Н. Е. Искусственный интеллект и его правосубъектность: философско-правовая интерпретация // Традиции и новации в системе

современного российского права : Материалы XX Международной конференции молодых ученых. В 3-х томах, Москва, 09–10 апреля 2021 года. Том 3. Москва: Московский государственный юридический университет имени О.Е. Кутафина (МГЮА), 2021. С. 399-401

107. Хай Г.А. Информатика для медиков: учебное пособие. СПб.: СпецЛит, 2009. 223 с.

108. Чепенко Я.К. Механизм реализации прав и свобод человека и гражданина в условиях развития современных информационных технологий // Исторический путь России: из прошлого в будущее: Мат-лы Междунар. науч. конф., посвященной 800-летию со дня рождения великого князя Александра Невского: В 3 т. / Под ред. С.И. Бугашева, А.С. Минина. Т. 1. СПб.: Санкт-Петербургский государственный университет промышленных технологий и дизайна, 2021. С. 645 – 649.

109. Шокина Д. И. Влияние поправок к конституции 2020 на повышение роли информационных технологий в избирательном процессе // Стабильность и динамизм Российской Конституции : Материалы XII Международного Конституционного Форума, посвященного 15-летию возрождения юридического факультета СГУ имени Н.Г.: сборник научных статей, Саратов, 16–18 декабря 2020 года. Том Часть 1. – Саратов: Издательство "Саратовский источник", 2021. С. 243-248.

Статьи в периодических изданиях

110. Авакьян С.А. Конституционная реформа 2020 и российский парламентаризм: реальность, решения, ожидания // Вестник Моск. гос. обл. университета. Сер. Юриспруденция. 2020. № 3. С. 8

111. Авдеева О. А. Право на здоровье в международном праве: от аморфного архетипа к синтетической концепции // Российское право: образование, практика, наука. 2023. №. 4. С. 45-52.

112. Авдулов А.Н., Кулькин А.М. Классификация информационных технологий // Вестник Российского фонда фундаментальных исследований. 2004. № 1(35). С. 36-

45.

113. Аксенова Е. И., Горбатов С. Ю. Применение технологий Интернета вещей в здравоохранении // Здоровье мегаполиса. 2021. Т. 2, № 4. С. 101-113.

114. Акулин И. М., Чеснокова Е. А., Смирнова К. М., Пресняков Р. А. Трансформация института врачебной тайны в эпоху электронного здравоохранения // Закон. 2019. № 9. С. 179–189.

115. Акулин И. М., Чеснокова Е. А., Пресняков Р. А., Прядко А.Е., Гурьянова Н. Е. Электронная медицинская карта: опыт правового регулирования стран ЕАЭС // Врач и информационные технологии. 2022. № 1. С. 72-83.

116. Акулин И. М., Чеснокова Е.А., Пресняков Р.А., Прядко А.Е. Телемедицина: правовой опыт регулирования субъектов Российской Федерации, перспективы развития // Проблемы стандартизации в здравоохранении. 2020. №. 5-6. С. 15-22.

117. Алексеева С.С., Стародубцев М. Э. Информированное добровольное согласие на медицинское вмешательство: фигура и роль врача // Российский кардиологический журнал. 2021. № 9. С. 69.

118. Алешкова И. А. Искусственный интеллект и его взаимосвязь с правами человека // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4, Государство и право. 2021. №. 1. С. 70-78.

119. Аликперова Н.В. Искусственный интеллект в здравоохранении: риски и возможности // Здоровье мегаполиса. 2023. № 3. с. 41–49.

120. Алямкин С.Н. Персональные данные как объект правового регулирования: понятие и способы защиты // Мир науки и образования. 2016. № 4 (8). С. 4.

121. Амадаев А.А., Начхоев И.И. Понятие и классификация информационных технологий // Вопросы устойчивого развития общества. 2021. № 12. С. 869-873.

122. Амелин Р. В., Бессонов Л. В. О некоторых вопросах правового регулирования телемедицинских технологий // Информационное право. 2019. № 2. С. 21-25.

123. Амелин Р.В., Богатырева Н.В., Волков Ю.В., Марченко Ю.А., Федосин А.С. Комментарий к Федеральному закону от 27.07.2006 № 152-ФЗ "О персональных данных" (постатейный) // СПС "КонсультантПлюс". 013.

124. Архипов В.В., Грачева А.В., Наумов В.Б., Полякова Т.А., Минбалеев А.В. Определение искусственного интеллекта в контексте российской правовой системы: критический подход // Государство и право. 2022. № 1. С. 168–178.
125. Архирейская Т.Ю. Поправка-2020: обеспечение безопасности личности, общества и государства при применении информационных технологий, обороте цифровых данных // Труды Оренбургского института (филиала) Московской государственной юридической академии. 2021. № 1(47). С. 6.
126. Базина О. О., Сименюра С. С. Телемедицина: достоинства, недостатки, реалии (правовой анализ и практическое применение) // Медицинское право. 2020. № 3. С. 32—38.
127. Балгутите И. В. Правовые проблемы использования искусственного интеллекта в сфере здравоохранения // Правовая парадигма. 2022. Т. 21, № 2. С. 140-148.
128. Барбашина Э. В. Принцип автономии пациента: возможное и действительное // Вестник Томского государственного университета. 2019. №. 449. С. 64-70.
129. Бачило И. Л. Понятийный аппарат информационного права и система обеспечения информационной безопасности // Труды Института государства и права Российской академии наук. 2016. №. 3 (55). С. 5-16.
130. Бегишев И.Р., Хисамова З.И. Искусственный интеллект и робототехника: теоретико-правовые проблемы разграничения понятийного аппарата // Вестник Удмуртского университета. Серия Экономика и право. 2020. Т. 30. № 5. С. 706–713.
131. Белов С. А. Автономия личности и врачебный патернализм // Юридический мир. 2023. № 4. С. 19-23
132. Белова А.Р. Трансформация права на неприкосновенность частной жизни в условиях информатизации общественных отношений // Евразийский юридический журнал. 2022. № 10(173). С. 157-159.
133. Бердегулова, Л.А. Проблемы правового регулирования института защиты персональных данных в системе правовой защиты права на неприкосновенность частной жизни, личную и семейную тайну в России // Актуальные проблемы

государства и общества в области обеспечения прав и свобод человека и гражданина. 2021. № 1. С. 65-73.

134. Бондарь Н.С. Информационно-цифровое пространство в конституционном измерении: из практики Конституционного суда Российской Федерации // Журнал российского права. 2019. № 11. С. 25—42.

135. Буланова В.С. Правовое обеспечение телемедицинских услуг и цифровая трансформация: теоретико-методологические вопросы // Мониторинг правоприменения. 2021. № 2 (39). С. 5964.

136. Буянова А. В. Телемедицинские проблемы регулирования и правоприменения // Социально-политические науки. 2018. № 2. С. 235–238.

137. Вабищевич, В. В. О некоторых вопросах совершенствования уголовно-правовой охраны персональных данных и информации о частной жизни // Право.by. 2023. № 4. С. 89–96.

138. Варюшин М. С. Правовое регулирование телемедицины в России и ЕС: два шага впереди один назад // Закон. 2018. №. 1. С. 165-174.

139. Ванько В. В., Артемова О. Р., Карпов О. Э., Матвиенко А. В., Гусев А. В., Еникеев И. М., Костина Е. В. Итоги внедрения искусственного интеллекта в здравоохранении России // Врач и информационные технологии. 2024. № 3. С. 32-43.

140. Венгеров А. Б. Научно-технический прогресс и применение права // Правоведение : научный журнал. 1983. № 3. С. 21—28.

141. Ветров Д.М. Защита персональных данных и защита информации на предприятии. Некоторые спорные вопросы применения // Проблемы права. Челябинск, 2010. № 1. С. 119

142. Винокурова М. А., Пашнина Т. В. О применении системного подхода в правовом регулировании телемедицинских технологий // Журнал российского права. 2022. Т. 26, № 6. С. 126-139.

143. Вичева А. А. Обеспечение доступности медицинской помощи как новый уровень конституционных полномочий органов местного самоуправления в России

- // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2022. Т. 8. №. 1. С. 54-61.
144. Владзимирский А.В. Телемедицина: Curatio Sine Temporaet Distantia. М.: Aegitas, 2016, С. 662.
145. Волкова В. Н. и др. Классификация информационных технологий // Прикладная информатика. 2015. №. 5 (59). С. 124-141.
146. Володченко В.С., Ланцова Д.С., Миронова Т.А. Понятие и классификация информационных технологий // Достижения науки и образования. 2020. №. 12 (66). С. 41-43.
147. Воротилина Т. В., Коротченко А. В. Место искусственного интеллекта в правовой системе России // Юридический вестник Дагестанского государственного университета. 2024. Т. 49. №. 1. С. 166-172.
148. Войниканис Е. А. Регулирование больших данных и право интеллектуальной собственности: общие подходы, проблемы и перспективы развития // Закон. 2020. №. 7. С. 135-156.
149. Гончаров И. В. Современные подходы к реализации прав человека в условиях цифровизации общественных отношений // Вестник Университета имени О.Е. Кутафина. 2019. №. 9 (61). С. 97-102.
150. Горovenko С. В., Бородинa О. Л. Актуальные вопросы правового регулирования применения электронной медицинской карты пациента как элемента процедуры оказания телемедицинских услуг // Вестник Уральского финансово-юридического института. 2019. № 1(15). С. 14-16.
151. Григонис В.П., Немова Н.Ю., Одинокaвa Е.Ю. Местное самоуправление в России: развитие законодательства и вопросы соотношения полномочий с государственными органами публичной власти // Государственная власть и местное самоуправление. 2024. № 1. С. 27 - 31.
152. Григорьев И. В. Международно-правовая регламентация медицинской помощи с применением телемедицинских технологий // Право и политика. 2024. №. 12. С. 132-142.

153. Гриценко Е.В., Должиков А.В., Дудко И.А., Егорова О., Кененова И.П., Красиков Д.В., Кряжкова О.Н., Кузнецова И.С., Сыченко Е.В., Третьяк И.А., Троицкая А.А., Храмова Т.М., Чирнинов А.М., Шилова А.И. Конституционные права в России: судебная практика и сравнительные материалы / Е– Москва : Центр конституционных исследований, 2024. 582 с.
154. Громова А. А. Реализация конституционного права на медицинскую помощь в Российской Федерации // Проблемы права. 2022. № 4(87). С. 59-63.
155. Гурылева М. Э. История развития медицинских информационных систем // Российская академия медицинских наук. Бюллетень Национального научно-исследовательского института общественного здоровья. 2013. № S1. С. 54-56.
156. Гусев А. В. Медицинские информационные системы: состояние, уровень использования и тенденции // Врач и информационные технологии. 2011. №. 3. С. 6-14.
157. Гусев А. В. Шарова Д. Е. Этические проблемы развития технологий искусственного интеллекта в здравоохранении // Общественное здоровье. 2023. Т. 3, № 1. С. 42-50.
158. Гусев А. В., Артемова О. Р., Васильев Ю. А., & Владимирский А. В. Внедрение медицинских изделий с технологиями искусственного интеллекта в здравоохранении России: итоги 2023 г // Национальное здравоохранение. 2024. Т. 5, № 2. С. 17-24.
159. Гусев А. В., Добридюк С. Л. Искусственный интеллект в медицине и здравоохранении // Информационное общество. 2017. № 4-5. С. 78-93.
160. Гусев А. В., Зингерман Б. В., Тюфилин Д. С., Зинченко В. В. Электронные медицинские карты как источник данных реальной клинической практики // Реальная клиническая практика: данные и доказательства. 2022. Т. 2, № 2. С. 8-20.
161. Гусев А. В., Владимирский, А. В., Шарова, Д. Е., Арзамасов, К. М., Храмов, А. Е. Развитие исследований и разработок в сфере технологий искусственного интеллекта для здравоохранения в Российской Федерации: итоги 2021 года // Digital Diagnostics. 2022. Т. 3. №. 3. С. 178-194.

162. Гуськов Д.Д., Абугалиева Ж. М. Перспективы развития медицинских информационных систем в России // Научный аспект. 2023. Т. 29. № 12. С. 3581-3588
163. Дейнеко А.Г. Информационно-правовой комментарий к поправкам в Конституцию Российской Федерации // Труды по интелл. собственности. 2021. Т. 37, № 1/2. С. 9–10.
164. Демкина А. Е. Эволюция цифровой медицины. Мировой и отечественный опыт // Вестник Московского университета. Серия 21. Управление (государство и общество). 2023. №. 2. С. 3-26.
165. Дубень А.К. Право на доступ к информации как составная часть конституционного права Российской Федерации // Наукосфера. 2022. № 7-1. С. 282-286.
166. Дьякова Е. Г. Переход к электронному правительству как процесс социальной адаптации технологии (на примере информатизации здравоохранения Свердловской области) // Антиномии. 2014. Т. 14. №. 4. С. 78-90.
167. Дятлов С.А. Принципы информационного общества // Информационное общество. 2000. Т. 2. С. 77-85.
168. Емелин И. В., Зингерман Б. В., Лебедев Г. С. Проблемы определения ключевых терминов медицинской информатики // Информационно-измерительные и управляющие системы. 2009. Т. 7. №. 12. С. 15-22.
169. Забайкин Ю. В., Лунькин Д. А. Направления развития права в сфере Интернета вещей // Вопросы российского и международного права. 2023. Т. 13, № 1-2-1. С. 208-214.
170. Заметина Т. В., Комбарова Е. В. Искусственный интеллект и конституционные вопросы его внедрения в современной России // Правовая политика и правовая жизнь. 2021. №. 1. С. 180-189.
171. Зингерман Б. В., Шкловский-Корди Н. Е., Карп В. П., Воробьев А. И. Интегрированная электронная медицинская карта: задачи и проблемы // Врач и информационные технологии. 2015. № 1. С. 24-34.

172. Ильяшенко О. Ю. Караптан, Д. Н., Лукьянченко Е. Л. Архитектура платформенных решений медицинской организации на основе технологии "Интернет вещей": практики, проблемы, инструменты // Вестник Димитровградского инженерно-технологического института. 2021. № 3(25). С. 24-35.
173. Иншакова А. О. Право как основа инфраструктурного обеспечения цифровой экономики и технологии Интернета вещей // Правовая парадигма. 2019. Т. 18, № 3. С. 6-11.
174. Иншакова А. О., Тымчук Ю. А. Охрана персональных данных пациентов при оказании медицинской помощи (услуг) с применением телемедицинских технологий // Lex Russica (Русский закон). 2024. Т. 77, № 7(212). С. 19-29.
175. Исаков И. Н. Новые технологии в праве как высокоэффективное средство реализации конституционного принципа равенства в условиях разноуровневого правового регулирования // Вестник Российского университета дружбы народов. Серия: Юридические науки. 2023. Т. 27. №. 4. С. 919-938.
176. Кадыров Ф. Н., Куракова Н. Г., Чилилов А. М. Правовые проблемы применения телемедицинских технологий в условиях борьбы с распространением коронавируса COVID-19 // Врач и информационные технологии. 2020. № 2. С. 45-51.
177. Казакова В. А., Тюлякова С. А., Шивилов Е. В., Аничкина К. А., Мифтахова А. Л., Юрканова Д. Д. Правовые основы применения технологий искусственного интеллекта в лучевой диагностике // Радиология—практика. 2023. №. 2. С. 63-77.
178. Карцхия А.А. Информационно-правовое обеспечение цифровой экосистемы здравоохранения // Правовая информатика. 2021. № 1. С. 13-23.
179. Карягина Е.Н., Еникеев А.Р. Назначение лекарственных средств посредством применения телемедицинских технологий: правовое регулирование в России и США (сравнительно-правовой анализ) // Медицинское право: теория и практика. Т. 5. № 2(10). 2020. С. 183-189.
180. Кафтанов А. Н., Андрейченко А. Е., Гусев А. В. Обзор методических

- подходов к оценке качества ведения электронных медицинских карт // Врач и информационные технологии. 2024. № 3. С. 6-19.
181. Киричек Е.В. Цифровизация в конституционно-правовом измерении // Вестник Восточно-Сибирского института МВД России. 2020. № 4(95). С. 29-40.
182. Киселев Г. М. К вопросу о понятии «информационные технологии // Научный поиск. 2013. № 4.1. С. 33-34.
183. Киселева А. Ю. Применение искусственного интеллекта в здравоохранении: аспекты медицинского права // Медицинское право: теория и практика. 2020. Т. 6, № 2(12). С. 29-38.
184. Кисель А. А., Нестеренков С. Н. Электронные медицинские карты как представитель big data в медицине // Редакционная коллегия. 2022. С. 378.
185. Климан Ю. А. Правовые проблемы применения искусственного интеллекта в сфере здравоохранения // Теория и практика общественного развития. 2024. № 11(199). С. 237-243.
186. Ковалева Н. Н., Новикова Е. А. Особенности правового регулирования телемедицинских технологий в условиях цифровизации // Право и государство: теория и практика. 2021. № 7 (199). С. 150–152.
187. Коваленко М. А. К вопросу о применении экспериментального правового режима в области телемедицины в России // Пролог: журнал о праве. 2024. № 1(41). С. 43-53.
188. Коваленко М. А. Медицинский работник как субъект оказания телемедицинской помощи: вопросы законодательной регламентации // Евразийский юридический журнал. 2024. № 1(188). С. 184-186.
189. Ковелина Т.А., Собянин А.В., Марухно В.М. К вопросу о правовом регулировании применения искусственного интеллекта в медицине // Гуманитарные, социально-экономические и общественные науки. 2022. № 2. С. 149.
190. Коданева С.И. Цифровые технологии в здравоохранении: зарубежный опыт // Россия: тенденции и перспективы развития. 2020. № 15–1. С. 617–620.

191. Коваленко М.А. О правовой возможности постановки диагноза при дистанционном консультировании // Юридические исследования. 2024. № 4. С. 87-97.
192. Ковалевский С. М. Отдельные проблемы правового регулирования использования телемедицинских технологий в Российской Федерации // Медицина и право в XXI веке : Сборник трудов XV ежегодной научно-практической конференции с международным участием, Санкт-Петербург, 22–23 декабря 2023 года. – Санкт-Петербург: Центр современной литературы и книги на Васильевском, 2024. С. 228-237.
193. Комарова В. В. Социальная государственность России и право на охрану здоровья, медицинскую помощь // Право и государство: теория и практика. 2014. № 2(110). С. 32-38.
194. Коробкова О. К., Воронина Н. В. Промежуточные результаты Федерального проекта «Создание единого цифрового контура в здравоохранении на основе единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ)» // Международный научно-исследовательский журнал. 2024. №. 10 (148). С. 65.
195. Косоруков А.А., Кшеменецкая М.Н. Большие данные в практике управления современным государством // Тренды и управление. 2019. № 1. С. 90.
196. Кравец И.А. Цифровой конституционализм: методологические и правовые аспекты // Государство и право. 2022. № 1. С. 19-33.
197. Купцова А. С. Правовое регулирование использования интернета вещей // Образование и право. 2021. №. 7. С. 225-230.
198. Кутейников Д. Л., Ижаев О. А., Зенин С. С., Лебедев В. А. Алгоритмическая прозрачность и подотчетность: правовые подходы к разрешению проблемы «черного ящика» // Lex russica. 2020. Т. 73. № 6. С. 139–148.
199. Лапина М. А. Организационно-правовые и финансовые аспекты цифровизации и внедрения технологий искусственного интеллекта в области здравоохранения // Финансы: теория и практика. 2022. Т. 26, № 3. С. 169-185.

200. Лаптев В. А. Искусственный интеллект в системе правовых инструментов стабилизации политических режимов мировых держав // Вестник Российского университета дружбы народов. Серия: Политология. 2023. Т. 25. №. 4. С. 831-847.
201. Лебедев, Г. С., Шадеркин, И. А., Фомина, И. В., Лисненко, А. А., Рябков, И. В., Качковский, С. В., Мелаев, Д. В. Интернет медицинских вещей: первые шаги по систематизации // Журнал телемедицины и электронного здравоохранения. 2017. №. 3 (5). С. 128-136.
202. Лебедев, Г. С., Шадеркин, И. А., Фомина, И. В., Лисненко, А. А., Рябков, И. В., Качковский, С. В., Мелаев, Д. В. Эволюция интернет-технологий в системе здравоохранения // Журнал телемедицины и электронного здравоохранения. 2017. №. 2 (4). С. 63-78.
203. Левчegov О. Н. Системы искусственного интеллекта в здравоохранении: текущее состояние, проблемы и перспективы // ЭФО: Экономика. Финансы. Общество. 2023. № 4(8). С. 52-71.
204. Ленъ Л.С., Никулина Т.Н. Управление медицинским учреждением в современных условиях: проблемы и пути решения // Вестник АГТУ. Сер.: Экономика. 2016 г. № 2. С. 73-80.
205. Липчанская М. А., Заметина Т. В. Социальные права граждан в условиях использования искусственного интеллекта: правовые основы и пробелы законодательного регулирования в России // Журнал российского права. 2020. №. 11. С. 78-96.
206. Липчанская М. А., Отставнова Е. А. Конституционно-правовые и нравственные основы использования искусственного интеллекта в реализации социальных прав и свобод человека // Вестник Саратовской государственной юридической академии. 2020. №. 3 (134). С. 69-78.
207. Лолаева А. С. Вопросы цифровизации в новой редакции Конституции Российской Федерации // Международный журнал конституционного и государственного права. 2021. № 1. С. 110-113
208. Лолаева А.С. Электронная демократия в России: юридическая форма и

- доктринальная интерпретация // Журнал российского права. 2023. № 4. С. 37-48
209. Лукичев К. Е. Нормативное обеспечение процесса внедрения телемедицинских технологий в российском здравоохранении // Управленческие науки в современном мире : сборник докладов научной конференции, Москва, 13–15 ноября 2019 года / Финансовый университет при Правительстве Российской Федерации. – Москва: Издательский дом "Реальная экономика", 2020. С. 157-161.
210. Магрицкая А. В. Информационные технологии в управлении предприятием: эволюция развития и классификация // Огарёв-Online. 2023. №. 10 (195). С. 8.
211. Макаров В. О. Этапы развития правового регулирования телемедицины в России // Медицинское право: новые правовые вызовы в работе медицинских организаций : Материалы IV Международного форума по медицинскому праву, Екатеринбург, 25–26 апреля 2024 года. – Екатеринбург: Уральский государственный юридический университет им. В.Ф. Яковлева, 2024. С. 79-85.
212. Макаров В.О., Коваленко М.А. К вопросу об эффективности регулятивных ограничений при проведении телемедицинских консультаций // Право и политика. 2024. № 4. С. 24-35.
213. Малеина М. Н. Право на тайну и неприкосновенность персональных данных // Журнал российского права. 2010. №. 11 (167). С. 18-28
214. Маличенко В. С. Международно-правовые механизмы регулирования доступа к технологиям здравоохранения // Право. Журнал Высшей школы экономики. 2021. №. 5. С. 256-285.
215. Маличенко В. С. Международно-правовые основы регулирования сферы охраны здоровья // Вестник Санкт-Петербургского университета. Право. 2024. Т. 15. №. 4. С. 1098-1117.
216. Мамедова В.Э. Экспериментальные правовые режимы в сфере медицинской деятельности и персонифицированная медицинская информация: снижение уровня защищенности или дополнительные гарантии? // Юридический вестник Самарского университета. 2024. Т. 10, № 3. С. 17-25.
217. Медведев А.И. Когда машинная логика неочевидна: проблема прозрачности

- искусственного интеллекта с точки зрения права // Информационное право. 2023. № 1(75). С. 9-13.
218. Милкова Э. Г. Искусственный интеллект в здравоохранении: к чему приведет цифровизация? // Инновации и инвестиции. 2021. №. 4. С. 353-356.
219. Михеев А. Е. Личный кабинет и расширение полномочий пациентов в цифровых экосистемах медицинской помощи // Менеджер здравоохранения. 2023. №. S1. С. 46-54.
220. Михеев А. Е. Возможности, проблемы и перспективы информационных технологий в сфере клинической безопасности // Менеджер здравоохранения. 2023. №. S1. С. 5-20.
221. Монаков Д. М., Алтунин Д. В. Медицинские информационные системы: современные реалии и перспективы. Литературный обзор // Журнал телемедицины и электронного здравоохранения. 2022. Т. 8. №. 4. С. 46-53.
222. Морозова Н. С. Задачи этико-правового обеспечения технологического развития системы здравоохранения // Lex Genetica. 2024. Т. 3. №. 1. С. 44-56.
223. Мочалов А.Н. Прозрачность алгоритмов как правовой принцип автоматизированной обработки данных о человеке // Юридические исследования. 2023. № 12. С. 77-88.
224. Мухитдинов Ж. Ф. Правовое регулирование Интернет вещей // International Multidisciplinary Research in Academic Science (IMRAS). 2024. №. 7 (9). С. 1-10.
225. Неверов А.Я. О месте и роли конституционно-правового регулирования общественных отношений в условиях развития информационных технологий // Вестник Московского университета МВД России. 2021. № 6. С. 207-214.
226. Несмиянова И. О. Информационные технологии: этапы развития, понятие и классификация // Известия Тульского государственного университета. Экономические и юридические науки. 2020. № 1. С. 149-155.
227. Оленева И.В. Современное состояние проблемы внедрения электронных медицинских карт в единой государственной информационной системе // Медицинский алфавит. 2011 г. № 4 (20). С. 8-10.

228. Осипов Р. А. Право на информированность: понятие и соотношение с правом на информацию // Вестник Саратовской государственной юридической академии. 2016. № 3 (110). С. 163-167.
229. Петроченков И. А. Перспективы защиты прав человека в контексте принятия Евросоюзом регламента об искусственном интеллекте. Гражданин. Выборы // Власть. 2024. Т. 2. С. 104-115.
230. Петроченков И. А. К вопросу о практике реализации конституционных новелл в сфере информационных технологий // Право и государство: теория и практика. 2023. № 6(222). С. 427-432.
231. Пибяев И.А., Симонова С.В. Алгоритмы в механизме реализации конституционных прав и свобод: вызовы цифровой эпохи // Сравнительное конституционное обозрение. 2020. № 6(139). С. 31-50.
232. Пикуров Н.И. Проблемы квалификации преступных посягательств на частную жизнь: теория и судебная практика // Уголовное право. 2019. № 2. С. 51-58.
233. Платонова Н.И. К вопросу об экспериментальном правовом режиме в сфере телемедицинских технологий // Журнал Белорусского государственного университета. Право. 2021. № 3. С. 32-37.
234. Полякова Т. А., Камалова Г. Г. Концептуальные основания развития института доступа к информации в Российской Федерации при применении цифровых технологий // Мониторинг правоприменения. 2020. № 4(37). С. 22-27.
235. Понкин И.В., Редькина А.И. Искусственный интеллект с точки зрения права // Вестник Российского университета дружбы народов. Серия: Юридические науки. 2018. Т. 22. №. 1. С. 91-109.
236. Попова А.В. Телемедицина в России и за рубежом: к вопросу о правовом регулировании // Вестник МГПУ. Серия: Юридические науки. 2019. № 1 (33). С. 53 – 60.
237. Привалов С. А. Технологии искусственного интеллекта в сфере обеспечения права на охрану здоровья, доступную и качественную медицинскую помощь:

перспективы и проблемы регулирования // Вестник Саратовской государственной юридической академии. 2021. № 4(141). С. 34-43.

238. Прилуков М. Д. Проблемы правового регулирования телемедицины. Российский и международный опыт // Вестник Нижегородского университета им. Н.И. Лобачевского. 2018. № 6. С. 136-141.

239. Прилуков М.Д. О современном состоянии правового регулирования телемедицины в Российской Федерации // Вестник Нижегородского университета им. Н.И. Лобачевского. 2024. № 5. С. 148-154.

240. Романовская О. В., Романовский Г. Б. Право и цифровизация современного здравоохранения // Вестник Российского университета дружбы народов. Серия: Юридические науки. 2024. Т. 28. №. 3. С. 565-583.

241. Романовский Г. Б., Романовская О. В. Право и современная медицина: проблемы и перспективы // Известия высших учебных заведений. Поволжский регион. Общественные науки. 2024. №. 1 (69). С. 96-110.

242. Романовский Г. Б. Право на здоровье и право на охрану здоровья в международном и национальном праве // Гражданин и право. 2021. № 5. С. 3-14.

243. Свищева И.В., Пронкина А.Г. Исследование и анализ процессов внедрения информационных технологий в сферу здравоохранения РФ: актуальность и дальнейшие пути развития // Международный журнал гуманитарных и естественных наук. 2022. № 11-2(74). С. 146-152.

244. Собянин С.С., Ракова А. Об электронной медицинской карте, о телемедицине, об искусственном интеллекте // Московская медицина. 2021. № 2(42). С. 26-29.

245. Сивоконева П.С. Защита прав пациентов при использовании персональных медицинских помощников в рамках экспериментального правового режима // Право и практика. 2024. № 4. С. 72-75.

246. Сушильников И.С. Конституционно-правовые основы экспериментальных правовых режимов // Теоретическая и прикладная юриспруденция. 2023. № 1(15). С. 109-121.

247. Тимофеев И. В. К вопросу о содержании права на охрану здоровья и медицинскую помощь в конституционно-правовом аспекте // Ученые записки юридического факультета. 2015. № 39(49). С. 109-115.
248. Третьякова Е. П. Правовые аспекты регулирования телемедицины // Цифровое право. 2020. Т. 1, № 2. С. 53-66.
249. Троицкая А.А. Автономия личности как принцип оказания медицинской помощи: между патернализмом и (мнимой) свободой выбора // Сравнительное конституционное обозрение. Т.33. 2024. №1(158). С.25–39.
250. Троянская М. А., Еременков А. А. Информационные технологии в государственном управлении: понятие, виды, задачи и направления регулирования // Вестник Академии знаний. 2022. № 50(3). С. 331-337.
251. Усенков И. А. Стабильность законодательства о телемедицине: актуальные проблемы // Право и современные государства. 2023. № 6. С. 36-40.
252. Усманова Е.Ф., Данилов В.В. Правовое регулирование права на доступ к информации // Проблемы права. 2018. № 4(68). С. 30-34.
253. Умаров М. Ф., Мирзоджанова М. К. О возможности применения технологии больших данных в медицине и в системе здравоохранения // Информатизация и связь. 2025. № 1. С. 42-49.
254. Умнова И.А. «Лохлин М. Что означает конституционализация? Реф. статьи: Loughlin M. What is constitutionalisation?» // Современный конституционализм: Теория, доктрина и практика. 2013. С. 155-159.
255. Умнова-Конюхова И.А. Трансформация современного права под влиянием научно-технологического развития: общие тенденции и опыт России // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4, Государство и право. 2024. №. 4. С. 9-25.
256. Умнова-Конюхова И. А. Экология человека, биоправо и право биобезопасности: межотраслевые и междисциплинарные взаимосвязи // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4, Государство и право. 2024. №. 2. С. 7-25.

257. Умнова-Конюхова И. А. Право на здоровье: актуальные аспекты природы, содержания и регулирования в международном и национальном праве // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4, Государство и право. 2025. №. 2. С. 7-25.
258. Умнова-Конюхова И. А. Искусственный интеллект и международное право: настоящее и будущее // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4, Государство и право. 2025. №. 3. С. 63-75.
259. Фадеева О. В. Проблемы реализации права граждан на охрану здоровья и медицинскую помощь, гарантированного ст. 41 Конституции Российской Федерации // Вестник Кемеровского государственного университета. Серия: Гуманитарные и общественные науки. – 2019. Т. 3. №. 1 (9). С. 97-103.
260. Фатьянов А.А. Проблемы защиты конфиденциальной информации, не составляющей государственную тайну // Информационное общество. 1997. № 1. С. 49 - 56
261. Федотов Н. Е. Отдельные аспекты защиты врачебной тайны при использовании телемедицинских технологий в здравоохранении. Сравнительное конституционное обозрение // Сравнительное конституционное обозрение. 2024. №. 1. С. 40-59.
262. Федотов Н. Е. Отдельные конституционно-правовые аспекты оказания высокотехнологичной медицинской помощи с применением искусственного интеллекта // Конституционное и муниципальное право. 2024. № 11. С. 36-41.
263. Федотов Н. Е. Электронные медицинские карты и право на доступ к информации: зарубежный опыт и российские реалии // Юридический мир. 2025. №. 8 (343). С. 56-59.
264. Федотов Н.Е. Право на неприкосновенность частной жизни в условиях цифровизации здравоохранения: некоторые законодательные пробелы в свете судебных решений // Конституционное и муниципальное право. 2025. № 6. С. 24 - 28.
265. Филатова А. О. К вопросу о выделении нового поколения прав человека:

цифровые правомочия активного избирательные права // Вестник образовательного консорциума Среднерусский университет. Серия: Юриспруденция. 2021. № 18. С. 56-58.

266. Филипова И. А. Правовое регулирование искусственного интеллекта: опыт Китая // Journal of Digital Technologies and Law. 2024. Т. 2. №. 1. С. 46-73.

267. Филипова, И. А. Искусственный интеллект: европейский подход к регулированию // Журнал зарубежного законодательства и сравнительного правоведения. 2023. Т. 19, № 2. С. 54-65.

268. Фролов С. В. Маковеев С.Н., Семенова С.В., Фареа С.Г. Современные тенденции развития рынка медицинских информационных систем // Вестник Тамбовского государственного технического университета. 2010. Т. 16. №. 2. С. 266-272.

269. Хабриев Р. У., Абашидзе А. Х., Маличенко В. С. Роль развития системы регулирования обращения лекарственных средств в реализации права человека на наивысший достижимый уровень здоровья // Журнал зарубежного законодательства и сравнительного правоведения. 2016. №. 2 (57). С. 16-22.

270. Харитонов Ю. С., Савина В. С., Паньини Ф. Предвзятость алгоритмов искусственного интеллекта: вопросы этики и права // Вестник пермского университета. Юридические науки. 2021. №. 53. С. 488-515.

271. Харитонов Ю.С. Правовые средства обеспечения принципа прозрачности искусственного интеллекта // Journal of Digital Technologies and Law. 2023. Т. 1. №. 2. С. 337-358.

272. Хомяков Э.Г. Современные информационные и цифровые технологии и отдельные направления их использования в правоохранительной деятельности // Вестник Удмуртского университета. Серия «Экономика и право». 2024. Т. 34. №. 5. С. 950-957.

273. Хурматуллина А.М. Конституционно-правовые основы экспериментальных правовых режимов в сфере здравоохранения // Lex russica. 2024. Т. 77. №. 8 (213). С. 65-74.

274. Цадыкова Э. А. Гарантии охраны и защиты персональных данных человека и гражданина // Конституционное и муниципальное право. 2007. № 14. С. 15—18.
275. Цветкова Л. А., Кузнецов П. П., Куракова Н. Г. Оценка перспектив развития мобильной медицины-mHealth на основании данных наукометрического и патентного анализа // Врач и информационные технологии. 2014. №. 4. С. 66-77.
276. Чайка В. К., Вустенко В. В., Морозова Н. А. О рисках цифровизации здравоохранения // Медико-социальные проблемы семьи. 2022. Т. 27, № 4. С. 64-74.
277. Чернышева Ю.А. Права человека в условиях цифровизации общества // Психология и право. 2019. Т. 9. № 4. С. 90 - 102.
278. Чилилов А. М., Кадыров Ф. Н., Мамаев М. Г. Баланс прав и обязанностей медицинских работников и пациентов при оказании медицинской помощи с применением телемедицинских технологий // Экономика, предпринимательство и право. 2023. Т. 13. № 6. С. 2041-2054.
279. Шадеркин, И. А., Цой, А. А., Сивков, А. В., Шадеркина, В. А., Просьянников, М. Ю., Войтко, Д. А., & Зеленский, М. М. (2015). mHealth-новые возможности развития телекоммуникационных технологий в здравоохранении // Экспериментальная и клиническая урология. 2015. №. 2. С. 142-148.
280. Шевердяев С.Н. Право на информацию: к вопросу о конституционно-правовой сущности // Право и политика. 2001. № 10. С. 91.
281. Шевердяев С. Н. Правовое сопровождение развития "электронного правительства" в России: новые идеалы и старые проблемы // Государственная власть и местное самоуправление. 2008. № 11. С. 30-37.
282. Шейкин А. Г. Правовое регулирование искусственного интеллекта в Китайской Народной Республике: состояние, перспективы, сравнительный анализ законопроектных предложений (часть 1) // Пролог: журнал о праве. 2025. №. 1 (45). С. 38-54.
283. Шепель Р. Н. Кутчер, А. В., Ваховская, Т. В., Драпкина, О. М. История развития телемедицины в Российской Федерации // Неотложная кардиология и

кардиоваскулярные риски. 2025. Т. 3. №. 2. С. 765–771.

284. Шутова А. А., Бегишев И. Р. Этические принципы создания и применения технологий искусственного интеллекта в здравоохранении // Правоприменение. 2024. Т. 8, № 1. С. 34-43.

285. Юдин Е.В. Принцип автономии пациента и право на информированное добровольное согласие при оказании медицинской помощи: некоторые правовые и биоэтические аспекты // Вопросы российского и международного права. 2021. Т. 11. № 1-1. С. 241.

286. Якуньков В. В. Проблемы правового регулирования информационнотехнологических систем в сфере охраны здоровья населения // Право и государство: теория и практика. 2024. №. 3 (231). С. 68-73.

287. Abouzakhar N.S., Jones A., Angelopoulou O. (2017) Internet of things security: A review of risks and threats to healthcare sector, in: 2017 IEEE International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE, pp. 373–378.

288. Adadi, A., & Berrada, M. (2018). Peeking inside the black-box: a survey on explainable artificial intelligence (XAI). IEEE access, 6, pp. 52138-52160.

289. Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., & Herrera, F. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. Information fusion, 58, pp. 82-115.

290. Ash, J. S., Berg, M., & Coiera, E. (2004). Some unintended consequences of information technology in health care: the nature of patient care information system-related errors. Journal of the American Medical Informatics Association, 11(2), pp. 104-112.

291. Baker, A. (2001). Crossing the quality chasm: a new health system for the 21st century. British Medical Journal Publishing Group. Vol. 323, No. 7322, P. 1192.

292. Baysari, M. T., & Westbrook, J. I. (2015). Mobile applications for patient-centered

- care coordination: a review of human factors methods applied to their design, development, and evaluation. *Yearbook of medical informatics*, 24(01), pp. 47-54.
293. Beauchamp T.L., Childress J.F. *Principles of Biomedical Ethics* // 5th ed. New York. NY: Oxford University Press. 2001. P. 454.
294. Bhavnani, V., Fisher, B., Winfield, M., & Seed, P. (2011). How patients use access to their electronic GP record—a quantitative study. *Family Practice*, 28(2), pp. 188-194
295. Brown I. (2015). Regulation and the Internet of Things. GSR Discussion Paper, 15th Global Symposium for. Regulators. pp. 1-34.
296. Carmi, L., Zohar, M., & Riva, G. M. (2023). The European General Data Protection Regulation (GDPR) in mHealth: Theoretical and practical aspects for practitioners' use. *Medicine, Science and the Law*, 63(1), pp. 61-68.
297. Cate, F. H., & Mayer-Schönberger, V. (2013). Notice and consent in a world of Big Data. *International Data Privacy Law*, 3(2), pp. 67-73.
298. Cheung, K. C., van der Veen, W., Bouvy, M. L., Wensing, M., van den Bemt, P. M., & de Smet, P. A. (2014). Classification of medication incidents associated with information technology. *Journal of the American Medical Informatics Association*, 21(e1), pp. 63-70.
299. Demiris, G., Afrin, L. B., Speedie, S., Courtney, K. L., Sondhi, M., Vimarlund, V., & Lynch, C. (2008). Patient-centered applications: use of information technology to promote disease management and wellness. A white paper by the AMIA knowledge in motion working group. *Journal of the American Medical Informatics Association*, 15(1), pp. 8-13.
300. Esmaeilzadeh, P., Mirzaei, T., & Dharanikota, S. (2021). Patients' perceptions toward human–artificial intelligence interaction in health care: experimental study. *Journal of medical Internet research*, 23(11), pp 1-21.
301. Fowles, J. B., Kind, A. C., Craft, C., Kind, E. A., Mandel, J. L., & Adlis, S. (2004). Patients' interest in reading their medical record: relation with clinical and sociodemographic characteristics and patients' approach to health care. *Archives of Internal Medicine*, 164(7), pp.793-800.

302. Grande, D., Marti, X. L., Feuerstein-Simon, R., Merchant, R. M., Asch, D. A., Lewson, A., & Cannuscio, C. C. (2020). Health policy and privacy challenges associated with digital technology. *JAMA network open*, 3(7), pp. 1-11.
303. H., Subramanyan; Kansal, Shivamm. (2023). Artificial Intelligence and Constitutional Rights: Assessing an Imaginable Unimaginable Future. *LawFoyer Int'l J. Doctrinal Legal Rsch.*, 1, pp. 98.
304. Huckvale K, Torous J, Larsen ME. (2019) Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation. *JAMA Netw Open*. 2(4), pp. 1-10
305. Kingsford K. M., Zhang F., Ayeh M. D. N. and MaryMargaret A., (2017) A Mathematical Model for a Hybrid System Framework for Privacy Preservation of Patient Health Records, *IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*, pp. 119-124.
306. Kraft, D., Srinivasan, K., & Bieber, G. (2020). Deep learning based fall detection algorithms for embedded systems, smartwatches, and IoT devices using accelerometers. *Technologies*, 8(4), P. 72.
307. Liu, P. R., Lu, L., Zhang, J. Y., Huo, T. T., Liu, S. X., & Ye, Z. W. (2021). Application of artificial intelligence in medicine: an overview. *Current Medical Science*, 41(6), pp. 1105-1115.
308. Malik, P., Pathania, M., & Rathaur, V. K. (2019). Overview of artificial intelligence in medicine. *Journal of family medicine and primary care*, 8(7), pp. 2328-2331.
309. Mantelero, A. (2024). The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template. *Computer Law & Security Review*, 54, pp. 1-18.
310. Mayer, A. H., C. A. da Costa, & R. D. R. Righi. (2020). Electronic Health Records in aBlockchain: A Systematic Review. *Health Informatics Journal*, 26(2), pp. 1273-1288
311. Magrabi, F., Baker, M., Sinha, I., Ong, M. S., Harrison, S., Kidd, M. R., ... & Coiera, E. (2015). Clinical safety of England's national programme for IT: a retrospective

- analysis of all reported safety events 2005 to 2011. *International journal of medical informatics*, 84(3), pp. 198-206.
312. Magrabi, F., Ong, M. S., Runciman, W., & Coiera, E. (2011). Patient safety problems associated with healthcare information technology: an analysis of adverse events reported to the US Food and Drug Administration. In *AMIA Annual Symposium Proceedings*. Vol. 2011, P. 853.
313. Magrabi, F., Ong, M. S., Runciman, W., & Coiera, E. (2012). Using FDA reports to inform a classification for health information technology safety problems. *Journal of the American Medical Informatics Association*, 19(1), pp. 45-53.
314. Magrabi, F., Baker, M., Sinha, I., Ong, M. S., Harrison, S., Kidd, M. R., ... & Coiera, E. (2015). Clinical safety of England's national programme for IT: a retrospective analysis of all reported safety events 2005 to 2011. *International journal of medical informatics*, 84(3), pp. 198-206.
315. McGowan, A. H., Sittig, S., & Menard, P. (2019). mHealth Cross-Contamination of User Health Data: Android Platform Analysis. *Twenty-fifth Americas Conference on Information Systems*, Cancun, pp. 1-5.
316. Meeks, D. W., Smith, M. W., Taylor, L., Sittig, D. F., Scott, J. M., & Singh, H. (2014). An analysis of electronic health record-related patient safety concerns. *Journal of the American Medical Informatics Association*, 21(6), pp. 1053-1059.
317. Mello, M. M., ADLER-MILSTEIN, J. U. L. I. A., Ding, K. L., & Savage, L. (2018). Legal barriers to the growth of health information exchange—boulders or pebbles? *The Milbank Quarterly*, 96(1), pp. 110-143.
318. Mendonça, M., Jerónimo, T., Julião, M., Santos, J., Pombo, N., & Silva, B. M. (2020). An IoT-based healthcare ecosystem for home intelligent assistant services in smart homes. In *IoT Technologies for HealthCare: 6th EAI International Conference, HealthyIoT*, Braga, Portugal, Proceedings 6. pp. 142-155.
319. Miller, S., Glisson, W. B., Campbell, M., & Sittig, S. (2019). Risk analysis of residual protected health information of android telehealth apps. . *Twenty-fifth Americas Conference on Information Systems*, Cancun, pp. 1-10.

320. Mora, H., Gil, D., Terol, R. M., Azorín, J., & Szymanski, J. (2017). An IoT-based computational framework for healthcare monitoring in mobile environments. *Sensors*, 17(10), P. 2302.
321. Nazir, S., Ali, Y., Ullah, N., & García-Magariño, I. (2019). Internet of things for healthcare using effects of mobile computing: a systematic literature review. *Wireless Communications and Mobile Computing*, 2019(1), pp. 593-1315.
322. Nichani A. V., Pistolwala S. T., Deshmukh A. A., Godse M. J. Telemedicine: making health care accessible. In: Vasudevan H., Deshmukh A., Ray K., editors. *Proceedings of International Conference on Wireless Communication* . Vol. 19. Singapore: Springer; 2018. pp. 255–263.
323. Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus*, 140(4), pp. 32-48.
324. Ozdalga, E., Ozdalga, A., & Ahuja, N. (2012). The smartphone in medicine: a review of current and potential use among physicians and students. *Journal of medical Internet research*, 14(5), P.1994.
325. Pasquale, F. (2014). Redescribing health privacy: the importance of information policy. *Hous. J. Health L. & Pol'y*, 14, pp. 95.
326. Pendyala VS, Figueira S. (2017). Automated medical diagnosis from clinical data. *Proceedings of 2017 IEEE 3rd International Conference on Big Data Computing Service and Applications (BigDataService)*; Apr 6–9; Redwood City, CA. p. 185-90.
327. Popescu, C., El-Chaarani, H., El-Abiad, Z., & Gigauri, I. (2022). Implementation of health information systems to improve patient identification. *International Journal of Environmental Research and Public Health*, 19(22), P.15236.
328. Popkova, E.G. (2019). *Ubiquitous Computing and the Internet of Things: Prerequisites for the Development of ICT* (Vol. 826). Springer., P. 1235.
329. Rachas, A., Farmer, A. J., Inzitari, M., & Shepperd, S. (2015). Interactive telemedicine: effects on professional practice and health care outcomes. *Cochrane Database of Systematic Reviews*, (9), pp. 1-512.
330. Reichertz, P. L. (2006). Hospital information systems—Past, present, future.

International journal of medical informatics, 75(3-4), pp. 282-299.

331. Ross, S. E., & Lin, C. T. (2003). The effects of promoting patient access to medical records: a review. *Journal of the American Medical Informatics Association*, 10(2), pp. 129-138.

332. Ross, M. K., Wei, W., & Ohno-Machado, L. (2014). "Big data" and the electronic health record. *Yearbook of medical informatics*, 23(01), pp. 97-104.

333. Rosenbaum, S., & Goldstein, M. M. (2015). Regulation of information technology in behavioral health. *Public Health Reports*, pp.130(4).

334. Sakushima, K., Umeki, R., Endoh, A., Ito, Y. M., & Nasuhara, Y. (2015). Time trend of injection drug errors before and after implementation of bar-code verification system. *Technology and health care*, 23(3), pp. 267-274.

335. Shany Y. (2023). Digital rights and the outer limits of international human rights law. *German Law Journal*, 24(3), pp. 461-472.

336. Shi, X. (2024). Reducing privacy risks of China's healthcare big data through the policy framework. *Frontiers in Public Health*, 12, pp 1-9.

337. Shrank, W. H., Rogstad, T. L., & Parekh, N. (2019). Waste in the US health care system: estimated costs and potential for savings. *Jama*, 322(15), pp. 1501-1509.

338. Singhal K., Azizi S., Tu T., Mahdavi S. S., Wei J., Chung H. W., Natarajan V. (2023). Large language models encode clinical knowledge. *Nature*, 620(7972), pp. 172-180.

339. Siteman, E., Businger, A., Gandhi, T., Grant, R., Poon, E., Schnipper, J., & Middleton, B. (2006). Clinicians recognize value of patient review of their electronic health record data. In *AMIA Annual Symposium Proceedings* (Vol. 2006, P. 1101).

340. Stoica, A. A. (2025). Artificial Intelligence and the Fundamental Constitutional Rights and Freedoms. *Legis. Info. Bull.*, pp. 30.

341. Talwar, Y. K., Karthikeyan, S., Bindra, N., & Medhi, B. (2016). Smartphone-a user-friendly device to deliver affordable healthcare-a practical paradigm. *J Health Med Informat*, 7(7), P. 3.

342. Topol, E.J. (2019) *High-Performance Medicine: The Convergence of Human and*

Artificial Intelligence. *Nature Medicine*, 25, pp. 44-56.

343. Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the general data protection regulation. *International data privacy law*, 7(2), pp. 76-99.

344. Working Party on the Protection of Individuals with Regard to the Processing of Personal Data. Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679. WP251rev.01; 2018.

345. Yi, Z. and Chenguang, W. (2024) “‘Internet Plus Health Care’ as an Impetus for China’s Health System Reform”. *Digital Health Care outside of Traditional Clinical Settings: Ethical, Legal, and Regulatory Challenges and Opportunities*. Cambridge: Cambridge University Press, pp. 156–168.

346. Zednik, C. (2021). Solving the black box problem: A normative framework for explainable artificial intelligence. *Philosophy & technology*, 34(2), pp. 265-288.

347. Zharova, A. K. (2023). Achieving algorithmic transparency and managing risks of data security when making decisions without human interference: legal approaches. *Journal of Digital Technologies and Law*, 1(4), pp. 973-993.

Диссертации, авторефераты диссертаций

348. Буланова В.С. Информационно-правовое обеспечение оказания телемедицинских услуг в условиях цифровой трансформации: дис. канд. юрид. наук. 12.00.13/ Буланова Валерия Сергеевна - М., 2021. 210 с.

349. Власенкова В. В. Право на охрану здоровья и медицинскую помощь в Российской Федерации: Автореф. дис. ... канд. юрид. наук 12.00.05/ Власенкова Вероника Викторовна. - М., 2007. 21 с.

350. Громова А.А. Реализация конституционного права на охрану здоровья и медицинскую помощь в условиях применения биомедицинских технологий в Российской Федерации : Дис. ... канд. юрид. наук : 5.1.2/ Громова Арина Алексеевна - Москва, 2025, 233 с.

351. Задков А.А. Конституционное право на доступ к информации в Российской

Федерации : Дис. ... канд. юрид. наук : 12.00.02/ Задков Александр Алексеевич - Москва, 2006, 180 с.

352. Лисицына Е.С. Право на информацию и информационную деятельность в Российской Федерации: конституционно-правовые аспекты : Дис. канд. юрид. наук : 12.00.02/ Лисицына Елена Сергеевна - Москва, 2003, 214 с.

353. Лопатин В. Н. Информационная безопасность России : специальность 12.00.01 "Теория и история права и государства; история учений о праве и государстве" : диссертация на соискание ученой степени доктора юридических наук 12.00.01/ Лопатин Владимир Николаевич. - Санкт-Петербург, 2000. 433 с.

354. Миндрова Е.К. Коллизия права граждан на доступ к информации и права на неприкосновенность частной жизни в условиях информационного общества: Автореф. дис. канд. юрид. наук. М., 2007. 24 с.

355. Преснякова А. В. Конституционное право на неприкосновенность частной жизни в условиях информатизации общества : современный зарубежный опыт : диссертация ... кандидата юридических наук : 12.00.02 / Преснякова Анна Викторовна; [Место защиты: Моск. гос. юрид. акад. им. О.Е. Кутафина].- Москва, 2010. 196 с.

356. Федосин А.С. Защита конституционного права человека и гражданина на неприкосновенность частной жизни при автоматизированной обработке персональных данных в Российской Федерации : автореферат дис. кандидата юридических наук : 12.00.14 / Федосин Алексей Сергеевич. - Саранск, 2009. 27 с.

Интернет-ресурсы

357. В России готовятся госстандарты для искусственного интеллекта. URL: https://www.cnews.ru/news/top/2023-03-01_v_rossii_gotovyat_standarty (дата обращения: 29.02.2025).

358. В России фиксируют рекордный рост электронных медицинских документов. URL: <https://vmeste-rf.tv/news/v-rossii-fiksiryut-rekordnyy-rost-elektronnykh-meditinskikh-dokumentov/> (дата обращения: 28.11.2024)

359. В Центре инноваций и Интернета вещей в здравоохранении в «Сколково» открылись пять новых терапевтических зон. URL: <https://sk.ru/news/v-centre-innovaciy-i-interneta-veschey-v-zdravoohranenii-v-skolkovo-otkrylis-pyat-novyh-terapevticheskikh-zon/> (дата обращения: 28.02.2025)
360. Врачи московских поликлиник поставили более 17 миллионов диагнозов с помощью искусственного интеллекта. <https://www.mos.ru/news/item/145399073/> (дата обращения: 23.01.2024).
361. Досье на проект Закона Республики Казахстан «Об искусственном интеллекте» (январь 2025 года). URL: https://online.zakon.kz/Document/?doc_id=34868071&pos=133;-54#pos=133;-54 (дата обращения: 28.02.2025)
362. Для чего в российских регионах используют ИИ в медицине. URL: https://rg.ru/2023/10/24/nejroseti-staviat-diagnoz.html?ysclid=lt0d7znqod817828204&utm_referrer=https%3A%2F%2Fwww.elibrary.ru%2F (дата обращения: 28.02.2025)
363. Интернет вещей, IoT, M2M рынок России. URL: [https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9,_IoT_\(%D1%80%D1%8B%D0%BD%D0%BE%D0%BA_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8\)](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9,_IoT_(%D1%80%D1%8B%D0%BD%D0%BE%D0%BA_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8)) (дата обращения: 29.02.2025).
364. Информационные технологии в сфере здравоохранения. URL: <https://mirror-info.ucoz.com/medicine/InfoTecMed.pdf> (дата обращения: 15.08.2024)
365. Искусственный интеллект в российском здравоохранении: информация о последних тенденциях и влиянии на медицинскую практику. URL: <https://med.roche.ru/innovations/blog/ai-russia.html> (дата обращения: 29.02.2025).
366. Кодекс этики в сфере искусственного интеллекта. URL: https://ethics.a-ai.ru/assets/ethics_files/2023/05/12/%D0%9A%D0%BE%D0%B4%D0%B5%D0%BA%D1%81_%D1%8D%D1%82%D0%B8%D0%BA%D0%B8_20_10_1.pdf (дата

обращения: 28.02.2025)

367. Как искусственный интеллект помогает решить задачи здравоохранения. URL: <https://www.rbc.ru/society/11/10/2024/66f681ba9a79471b04d22aaa> (дата обращения: 29.02.2025).

368. Классификация цифровых действий, услуг и приложений в здравоохранении: общий язык для описания использования цифровых технологий в интересах здравоохранения. URL: <https://whodc.mednet.ru/ru/osnovnye-publikaczii/informaczionnye-texnologii-v-zdravooxranenii/4147.html> (дата обращения: 15.09.2024)

369. Личное делят: в РФ в 40 раз выросло количество утечек персональных данных. URL: <https://iz.ru/1554402/alena-nefedova/lichnoe-deliat-v-rf-v-40-razvyroslo-kolichestvo-utechek-personalnykh-dannykh> (дата обращения: 29.11.2023).

370. Минцифры подготовило концепцию регулирования искусственного интеллекта. URL: <https://www.vedomosti.ru/economics/articles/2025/08/20/1132830-mintsifri-podgotovilo-kontseptsiyu-regulirovaniya-iskusstvennogo-intellekta> (дата обращения: 28.08.2025)

371. Мнения о содействии развитию «Интернет + медицина-здоровье». URL: https://www.gov.cn/zhengce/content/2018-04/28/content_5286645.htm (дата обращения: 28.11.2024)

372. На заседании Совета глав правительств СНГ утверждены изменения в Соглашение о сотрудничестве в создании совместимых национальных телемедицинских систем. URL: <https://e-cis.info/news/564/118441/> (дата обращения: 28.03.2025)

373. Открытая концепция «Интернет-вещей: правовые аспекты (Российская Федерация)». URL: <https://www.ifap.ru/pr/2016/160712aa.pdf> (дата обращения: 28.10.2025)

374. «Персональные медицинские помощники» помогли 2,5 тысячам новосибирцев. URL: <https://zdrav.nso.ru/news/9006> (дата обращения: 11.09.2025)

375. Протокол Правительственной комиссии по цифровому развитию,

использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 10.03.2022 № 7 «Об утверждении концепции информационной безопасности в сфере здравоохранения». URL:

<https://regulhub.kaspersky.ru/upload/iblock/86f/0x0rk2olahwno02qxuw7sn6c6anrbj7g.pdf> (дата обращения: 28.01.2025)

376. Рекомендация об этических аспектах искусственного интеллекта. URL: https://unesdoc.unesco.org/ark:/48223/pf0000380455_rus (дата обращения: 28.03.2025)

377. Разговор с экспертом: «Здравоохранение – самая ресурсоемкая отрасль из всех отраслей социальной сферы». URL: <https://mednet.ru/novosti/razgovor-s-ekspertom-zdravooxranenie-%E2%80%93-samaya-resursoemkaya-otrasl-iz-vsex-otraslej-soczialnoj-sferyi> (дата обращения: 15.08.2024)

378. С 1 января 2024 года вступят в силу новые правила посещения поликлиник в РФ. URL: <https://ufafabry.ru/posts/s-1-ianvaria-2024-goda-vstupiat-v-silu-novye-pravila-poseshcheni> (дата обращения: 28.11.2024)

379. Электронные медкарты: где доступ, а где — цифровая пропасть. URL: <https://eur-http://pravo-med.ru/articles/18736/> (дата обращения: 28.11.2025)

380. Центральный комитет Коммунистической партии Китая и Госсовет опубликовали План планирования «Здоровый Китай 2030». URL: https://www.gov.cn/zhengce/2016-10/25/content_5124174.htm (дата обращения: 28.11.2024)

381. Цифровизацию и технологии искусственного интеллекта обсудят на Форуме будущих технологий. URL: <https://minzdrav.gov.ru/news/2024/02/10/20871-tsifrovizatsiyu-i-tehnologii-iskusstvennogo-intellekta-obsudyat-na-forume-buduschih-tehnologiy-2024> (дата обращения: 15.08.2024)

382. Южная Корея станет первой страной в мире, где будет действовать закон об ИИ. URL: <https://rg.ru/2025/12/15/iuzhnaia-koreia-stanet-pervoj-stranoj-v-mire-gde-budet-dejstvovat-zakon-ob-ii.html> (дата обращения: 28.12.2025)

383. An invisible hand: Patients aren't being told about the AI systems advising their care. - 2020. URL: <https://www.statnews.com/2020/07/15/artificial-intelligence-patient-consent-hospitals/> (дата обращения: 23.01.2024).
384. Artificial Intelligence (AI) in Healthcare Market worth \$148.4 billion by 2029 - Exclusive Report by MarketsandMarkets. – 2024. URL: <https://www.prnewswire.com/news-releases/artificial-intelligence-ai-in-healthcare-market-worth-148-4-billion-by-2029---exclusive-report-by-marketsandmarkets-302052956.html> (дата обращения: 28.02.2025)
385. Artificial intelligence advances threaten privacy of health data. URL: <https://www.sciencedaily.com/releases/2019/01/190103152906.htm> (дата обращения: 28.11.2024)
386. Artificial Intelligence Index Report 2023. CHAPTER 6: Policy and Governance. URL: https://aiindex.stanford.edu/wp-content/uploads/2023/04/HAI_AI-Index-Report-2023_CHAPTER_6-1.pdf (дата обращения: 28.11.2024)
387. Availability, Accessibility, Acceptability and Quality framework. URL: <https://gbvguidelines.org/wp/wp-content/uploads/2019/11/AAAQ-framework-Nov-2019-WEB.pdf> (дата обращения: 29.02.2025).
388. Average cost of healthcare data breach rises to \$7.1M, according to IBM report. URL: <https://www.fiercehealthcare.com/tech/average-cost-healthcare-data-breach-rises-to-7-1m-according-to-ibm-report#:~:text=A%20healthcare%20data%20breach%20comes,2020%20data%20breach%20cost%20report.> (дата обращения: 28.11.2024)
389. Big Data. URL: <https://yandex.cloud/ru/docs/glossary/bigdata> (дата обращения: 15.10.2025)
390. Cindy Hu, Jason Gong, Jiaxin Yang. Digital Health Laws and Regulations China 2024. URL: <https://iclg.com/practice-areas/digital-health-laws-and-regulations/china> (дата обращения: 28.11.2024)
391. Considerations for the Use of Artificial Intelligence To Support Regulatory Decision-Making for Drug and Biological Products. URL:

- <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/considerations-use-artificial-intelligence-support-regulatory-decision-making-drug-and-biological> (дата обращения: 28.01.2025)
392. Day, J., Iwańska, K., Simon, E., & Willamo, K. (2024). Packed with loopholes: Why the AI Act fails to protect civic space and the rule of law. URL: https://dq4n3btxmr8c9.cloudfront.net/files/hjoz6a/AI_Act_RoL_Analysis.pdf (дата обращения: 28.11.2024)
393. Digital health - Statistics & Facts. URL: <https://www.statista.com/topics/2409/digital-health/#topicOverview> (дата обращения: 15.09.2024)
394. Digital health innovation action plan. URL: <https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/UCM568735.pdf> (дата обращения: 28.02.2025)
395. Edemekong PF, Annamaraju P, Haydel MJ. Health Insurance Portability and Accountability Act. URL: https://dq4n3btxmr8c9.cloudfront.net/files/hjoz6a/AI_Act_RoL_Analysis.pdf (дата обращения: 28.11.2024)
396. European Union Agency for Cybersecurity. From January 2019 to April 2020 Data breach ENISA Threat Landscape. 2020. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-data-breach/at_download/fullReport (дата обращения: 28.11.2024)
397. FDASIA Health IT Report. Proposed Strategy and Recommendations for a Risk-Based Framework. URL: https://www.healthit.gov/sites/default/files/fdasia_healthitreport_final.pdf (дата обращения: 28.11.2024)
398. Food and Drug Administration (FDA). “Developing Software Precertification Program: A Working Model.” U.S. Food & Drug Administration. Retrieved. URL: <https://www.fda.gov/media/113802/download> (дата обращения: 28.02.2025)
399. Global IoT Market Will Grow to 24.1 Billion Devices in 2030, Generating \$1.5

- Trillion Annual Revenue // PR Newswire. URL: <https://www.prnewswire.com/news-releases/global-iot-market-will-grow-to-24-1-billion-devicesin-2030--generating-1-5-trillion-annual-revenue-301061873.html> (дата обращения: 28.02.2025)
400. Global diffusion of eHealth: Making universal health coverage achievable. URL: <https://www.statista.com/topics/2409/digital-health/#topicOverview> (дата обращения: 15.09.2024)
401. Global strategy on digital health 2020-2025. URL: <https://www.who.int/docs/default-source/documents/g4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf> (дата обращения: 28.01.2025)
402. Good practice guidelines on health apps and smart devices (mobile health or mhealth). URL: https://www.has-sante.fr/jcms/c_2681915/en/good-practice-guidelines-on-health-apps-and-smart-devices-mobile-health-or-mhealth (дата обращения: 28.02.2025)
403. Guidance: Medical device stand-alone software including apps. URL: <https://www.fda.gov/media/113802/download> (дата обращения: 28.02.2025)
404. HIPAA Journal. Healthcare data breach statistics. URL: <https://www.hipaajournal.com/healthcare-data-breach-statistics/> (дата обращения: 28.11.2024)
405. Jana Grieb, Dr. Deniz Tschammler, Dr. Claus Färber, Steffen Woitz. Digital Health Laws and Regulations Germany 2024. URL: <https://iclq.com/practice-areas/digital-health-laws-and-regulations/germany> (дата обращения: 28.11.2024)
406. Karolína Babická, Cristina Giacomini. Understanding the Scope of the Council of Europe Framework Convention on AI. URL: <https://opiniojuris.org/2024/11/05/understanding-the-scope-of-the-council-of-europe-framework-convention-on-ai/> (дата обращения: 28.03.2025)
407. Nutrition And Health Applications Do Not Respect Privacy. URL: <https://www.test-achats.be/action/espace-presse/communiqués-de-presse/2020/food-and-health-apps#> (дата обращения: 29.02.2025).

408. Policy for Device Software Functions and Mobile Medical Applications Guidance for Industry and Food and Drug Administration Staff. URL: <https://www.fda.gov/media/80958/download> (дата обращения: 28.02.2025)
409. Procuratorial Organs Actively Maintain Personal Information Security, Handling More than 2,000 Public Interest Litigation Cases in the Field of Personal Information Protection in 2021'. URL: https://www.spp.gov.cn/spp/xwfbh/wsfbh/202202/t20220227_545967.shtml (дата обращения: 29.02.2025).
410. Roger Kuan, David Wallace. Digital Health Laws and Regulations Introduction 2024. URL: <https://iclg.com/practice-areas/digital-health-laws-and-regulations/01-introduction> (дата обращения: 15.09.2024)
411. TELEMEDICINE: A GLOBAL APPROACH TO TRENDS AND PRACTICES. URL: <https://www.ibanet.org/document?id=Healthcare-Telemedicine-Survey-Germany> (дата обращения: 28.11.2024)
412. The International Medical Device Regulators Forum final document, “Software as a Medical Device (SaMD): Key Definitions. URL: <http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-131209-samd-key-definitions-140901.pdf> (дата обращения: 28.02.2025)
413. IoT in Healthcare Market by Component (Medical Device, Systems & Software, Services, and Connectivity Technology), Application (Telemedicine, Connected Imaging, and Inpatient Monitoring), End User and Region - Global Forecast to 2028. URL: <https://www.marketsandmarkets.com/Market-Reports/iot-healthcare-market-160082804.html?gclid=CjwKCAjw> (дата обращения: 28.02.2025)
414. Your Data Were ‘Anonymized’? These Scientists Can Still Identify You (Published 2019). URL: <https://www.ncbi.nlm.nih.gov/search/research-news/4173/> (дата обращения: 28.11.2024)