Вестник РУДН. Серия: Юридические науки 2025 Т. 29. № 1. 235–254
RUDN JOURNAL OF LAW. ISSN 2313-2337 (Print), ISSN 2408-9001 (Online) http://journals.rudn.ru/law

https://doi.org/10.22363/2313-2337-2025-29-1-235-254
EDN: RYZIXU

Научная статья / Research Article

Компаративный анализ: надлежащие практики защиты данных в здравоохранении России и за рубежом

Д.А. Лебедева

Национальный исследовательский университет «Высшая школа экономики», *г. Москва, Российская Федерация*
lebedevady@yandex.ru

Аннотация. Проведен сравнительно-правовой анализ законодательства и практики защиты персональных данных пациентов в системе здравоохранения России, США, ЕС, Китая и ряда других азиатских стран. Основными методами исследования явились сравнительно-правовой, формально-юридический, экспертно-аналитический, методы визуализации и структурного анализа. Целью исследования является проведение анализа законодательства в сфере защиты персональных данных пациентов в системе здравоохранения в разных странах и выявление рекомендаций для России. Доказано, что лидерами в этой сфере являются США и ЕС, где действуют специальные законы о защите персональных данных в сфере здравоохранения, устанавливающие строгие требования к операторам медицинских данных и предусматривающие серьезные санкции за их нарушение. Отмечается, что российская законодательство в сфере защиты персональных данных в сфере здравоохранения соответствует мировым тенденциям цифровизации и защиты персональных данных, однако имеются проблемы правоприменения, связанные с недофинансированием IT-инфраструктуры медицинских организаций, дефицитом квалифицированных кадров, низкой цифровой грамотностью медицинского персонала. Полученные результаты формируют основу для дальнейших научных изысканий по проблемам трансформации систем охраны медицинской тайны в контексте развития технологий больших данных, ИИ, интернета вещей. В работе обоснована целесообразность дифференциации правового регулирования в зависимости от категорий информации (генетических и биометрических данных), аргументирована необходимость усиления ответственности за нарушения, предложены конкретные законодательные новеллы.

Ключевые слова: персональные данные, информационная безопасность, здравоохранение, электронные медицинские карты, HIPAA, GDPR, сравнительный анализ, медицинские информационные системы

Конфликт интересов. Автор заявляет об отсутствии конфликта интересов.

Поступила в редакцию: 18 апреля 2024 г.
Принята к печати: 15 января 2025 г.

Для цитирования:

Лебедева Д.А. Компаративный анализ: надлежащие практики защиты данных в здравоохранении России и за рубежом // RUDN Journal of Law. 2025. Т. 29. № 1. С. 235–254. https://doi.org/10.22363/2313-2337-2025-29-1-235-254

Comparative analysis of effective data protection practices in healthcare: Russia and international standards

Diana A. Lebedeva

National Research University "Higher School of Economics", *Moscow, Russian Federation*
✉lebedevady@yandex.ru

Abstract. A comparative legal analysis has been conducted on the legislation and practices regarding the protection of patients' personal data in the healthcare systems of Russia, the USA, the EU, China, and several other Asian countries. The main research methods employed include comparative-legal analysis, formal-legal analysis, expert-analytical methods, visualization techniques, and structural analysis. The aim of the study is to analyze the legislation related to the protection of patients' personal data in healthcare across different countries and to identify recommendations for Russia. The findings indicate that the USA and the EU are leaders in this area, with specific laws governing the protection of personal data in healthcare that impose strict requirements on medical data operators and significant penalties for violation. It is noted that Russian legislation on data protection in healthcare aligns with global trends toward digitalization and personal data protection. However, challenges remain in law enforcement due to underfunding of IT infrastructure in medical organizations, a shortage of qualified personnel, and low digital literacy among medical staff. The results of this study provide a foundation for further scientific research into the transformation of medical privacy protection systems in light of advancements in big data technologies, AI, and the Internet of Things. The paper advocates for a differentiated legal regulation based on categories of information (such as genetic and biometric data), argues for strengthened liability for violations, and proposes specific legislative innovations.

Key words: personal data, information security, healthcare, electronic health records, HIPAA, GDPR, comparative analysis, medical information systems

Conflict of interest. The author declares no conflict of interest.

Received: 18th April 2024
Accepted: 15th January 2025

For citation:

Lebedeva, D.A. (2025) Comparative analysis of effective data protection practices in healthcare: Russia and international standards. *RUDN Journal of Law.* 29 (1), 235–254. (in Russian). https://doi.org/10.22363/2313-2337-2025-29-1-235-254

Введение

Защита персональных данных граждан в эпоху цифровизации становится одной из ключевых задач государства и общества. Особую важность эта проблема приобретает в сфере здравоохранения, где обрабатываются «сверхчувствительные» данные о здоровье людей. Утечка медицинской информации может не только нанести психологический ущерб пациенту, но и привести к его дискриминации, шантажу,

финансовым потерям (Edemekong & Haydel, 2024). На макроуровне низкий уровень защиты данных подрывает доверие населения к системе здравоохранения, что негативно влияет на готовность людей обращаться за медицинской помощью и следовать рекомендациям врачей[1].

Актуальность вопросов информационной безопасности в медицине резко возросла в период пандемии COVID-19. Массовый перевод части услуг в дистанционный формат, развитие телемедицины, внедрение искусственного интеллекта для диагностики заболеваний – все эти тренды повышают риски утечки данных из-за роста объемов обрабатываемой информации и появления новых уязвимостей в IT-системах (Gurtsko & Smirnov, 2024).

Сравнительно-правовой анализ регулирования защиты медицинских данных в разных странах позволяет выявить лучшие законодательные практики и подходы к обеспечению безопасности критической информационной инфраструктуры здравоохранения (Bradford, Aboy & Liddell, 2019). Наработанный за рубежом опыт может быть полезен и для совершенствования российского законодательства в области защиты прав субъектов персональных данных в медицинской сфере.

Цель исследования – проведение анализа законодательства в сфере защиты персональных данных пациентов и медицинских работников в системе здравоохранения в разных юрисдикциях и выявление рекомендаций на их основе для России.

Материалы и методы исследования.

1. Сравнительно-правовой анализ – изучение и сопоставление законодательства о защите медицинских персональных данных в разных странах (США, ЕС, Китай, Россия, Япония, Корея, Сингапур и др.) для выявления общих черт и национальных особенностей регулирования.

2. Формально-юридический метод – рассмотрение конкретных правовых норм, правоприменительной практики, прецедентов и инцидентов в сфере безопасности медицинской информации для понимания особенностей функционирования правовых механизмов защиты данных в различных юрисдикциях.

3. Экспертно-аналитический метод – изучение и обобщение оценок ведущих экспертов, аналитических центров, профильных ассоциаций относительно состояния систем защиты медицинских данных в исследуемых государствах, ключевых проблем и перспектив их развития.

4. Кейс-стади (case study) – детальный разбор показательных случаев утечек данных, кибератак на медицинские организации в разных странах для иллюстрации особенностей практического применения законодательства о персональных данных и выявления типовых факторов уязвимости.

5. Диахронный (исторический) анализ – рассмотрение генезиса и эволюции систем защиты медицинских персональных данных в их связи с развитием нормативной базы, ИТ-технологий и вызовов цифровой эпохи. Этот метод позволил проследить трансформацию подходов и выявить ключевые тренды.

6. Синхронный (структурный) анализ – изучение актуального состояния механизмов защиты данных в здравоохранении на определенном временном срезе в совокупности правовых, организационных и технических компонентов как в страновом разрезе, так и в международной компаративистике.

7. Метод визуализации – представление ключевых результатов исследования в виде структурированной сравнительной таблицы для более наглядной демонстрации сходств и различий национальных моделей регулирования по ряду критериев.

[1] Snell, E. (2015) A Breakdown of HIPAA Security Rule. HealthITSecurity, 3–6.

В работе использовался мультимодальный методологический аппарат, сочетающий общенаучные и специальные методы юридического исследования, что позволило провести комплексный анализ проблематики и сформулировать практические рекомендации.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Проанализировать нормативные акты США, регулирующие защиту медицинских персональных данных.
2. Изучить соответствующее законодательство ЕС, КНР и других зарубежных стран.
3. Сравнить практику применения законов о защите медицинских персональных данных за рубежом.
4. Выявить лучшие зарубежные практики обеспечения безопасности персональных данных в сфере здравоохранения.
5. Предложить возможные пути совершенствования законодательства РФ с учетом релевантного международного опыта.

Работа имеет практическую значимость для законотворческой деятельности, формирования государственной политики в области здравоохранения и информационной безопасности. Результаты исследования могут быть интересны как представителям органов власти, так и руководству медицинских и IT-организаций.

Выбор стран для сравнительно-правового анализа защиты персональных данных пациентов обусловлен стремлением охватить ключевые модели регулирования, существующие в современном мире. США и ЕС являются признанными лидерами в этой сфере, задающими глобальные стандарты в виде законов HIPAA и GDPR, на которые ориентируются многие государства. Китай представляет интерес как крупнейшая экономика Азии, активно внедряющая передовые технологии в здравоохранение, но имеющая специфическую модель регулирования с приоритетом государственных интересов. Япония, Южная Корея и Сингапур демонстрируют опыт развитых азиатских стран, успешно сочетающих прогрессивное законодательство и масштабные проекты цифровизации медицины. Индия и Таиланд, напротив, показывают проблемы и перспективы становления системы защиты данных в развивающихся странах региона. Наконец, Россия анализируется как основной объект исследования, чье законодательство и практика сопоставляются с мировыми трендами для выявления возможностей совершенствования. Такая комбинация стран позволяет провести разносторонний анализ универсальных закономерностей и национальной специфики защиты персональных данных пациентов, обобщить лучшие практики, применимые для оптимизации регулирования в России.

Основы регулирования персональных данных в сфере здравоохранения в Российской Федерации

Основу правового регулирования защиты персональных данных в России, включая сферу здравоохранения, составляет Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (Закона о ПД)[2]. Данный закон устанавливает принципы и условия обработки персональных данных, права субъектов персональных данных, обязанности операторов персональных данных, а также механизмы государственного контроля и надзора в этой области.

[2] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства РФ. 31.07.2006. № 31 (1 ч.). Ст. 3451.

Медицинские сведения о пациентах относятся к специальной категории персональных данных[3]. Их обработка допускается только в случаях, предусмотренных, в частности, при наличии письменного согласия субъекта ПД либо в медико-профилактических целях, для установления медицинского диагноза и оказания медицинских услуг, при условии, что обработку осуществляет лицо, профессионально занимающееся медицинской деятельностью и обязанное сохранять врачебную тайну.

Операторы персональных данных обязаны принимать необходимые правовые, организационные и технические меры для защиты ПД от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий[4]. Конкретные требования к обеспечению безопасности ПД при их обработке в информационных системах устанавливаются Правительством РФ[5].

Более детально вопросы защиты информации в системе здравоохранения регламентируются подзаконными нормативными актами. Приказ № 911н закрепляет правила информационного взаимодействия МИС с иными информационными системами в сфере здравоохранения, такими как Единая государственная информационная система в сфере здравоохранения (далее – ЕГИСЗ), Единый портал государственных и муниципальных услуг (далее – ЕПГУ), Государственная информационная система обязательного медицинского страхования (далее – ГИС ОМС) и др[6]. При этом устанавливается прямой запрет на размещение и обработку сведений, составляющих врачебную тайну, с использованием интернет-сайтов и иных общедоступных информационных ресурсов[7].

Сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении, составляют врачебную тайну[8]. Их разглашение допускается только с письменного согласия гражданина или его законного представителя, а также в случаях: угрозы распространения инфекционных заболеваний, расследования преступления, оказание медпомощи несовершеннолетнему и др.[9]

---

[3] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства РФ. 31.07.2006. № 31 (1 ч.). Ст. 10.

[4] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства РФ. 31.07.2006. № 31 (1 ч.). Ст. 7.

[5] Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Собрание законодательства РФ. 05.11.2012. № 45. Ст. 6257.

[6] Приказ Минздрава России от 24.12.2018 № 911н «Об утверждении Требований к государственным информационным системам в сфере здравоохранения субъектов Российской Федерации, медицинским информационным системам медицинских организаций и информационным системам фармацевтических организаций» // Официальный интернет-портал правовой информации. Режим доступа: http://www.pravo.gov.ru (дата обращения: 26.03.2024).

[7] Приказ Минздрава России от 24.12.2018 № 911н «Об утверждении Требований к государственным информационным системам в сфере здравоохранения субъектов Российской Федерации, медицинским информационным системам медицинских организаций и информационным системам фармацевтических организаций» // Официальный интернет-портал правовой информации. Режим доступа: http://www.pravo.gov.ru (дата обращения: 26.03.2024).

[8] Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» // Собрание законодательства РФ. 28.11.2011. № 48. Ст. 6724.

[9] Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» // Собрание законодательства РФ. 28.11.2011. № 48 (ч. 4). Ст. 13.

Сведения, составляющие врачебную тайну, относятся к информации ограниченного доступа, для которой устанавливается особый правовой режим[10]. Ее распространение без согласия субъекта не допускается, а обладатели такой информации обязаны принимать меры по ее защите, в том числе путем установления системы защиты информации, препятствующей неправомерному доступу, уничтожению или модификации.

Надзор за соблюдением законодательства РФ в области персональных данных, включая их обработку в медицинских информационных системах, осуществляет Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее – Роскомнадзор)[11]. В рамках своих полномочий он проводит плановые и внеплановые проверки операторов персональных данных, рассматривает обращения граждан, выносит обязательные для исполнения предписания об устранении нарушений, составляет протоколы об административных правонарушениях.

За нарушение порядка обработки персональных данных, в том числе медицинских, предусмотрена административная ответственность по ст. 13.11 КоАП РФ (административный штраф до 18 млн рублей) и по ст. 13.14 КоАП РФ (за разглашение информации ограниченного доступа, штрафы до 40 тыс. руб. для граждан и до 500 тыс. руб. для юридических лиц)[12]. В случае незаконного собирания или распространения сведений о частной жизни (включая медицинские) возможно и уголовное преследование по ст. 137 УК РФ (до 2 лет лишения свободы)[13].

Несмотря на достаточно обширную нормативную основу, на практике в российском здравоохранении нередки случаи утечек персональных данных пациентов и иных нарушений информационной безопасности (Gurtsko & Smirnov, 2024). Среди причин в доктрине называется недофинансирование IT-инфраструктуры медицинских учреждений, нехватка квалифицированных IT-специалистов (Okishev, 2022), низкая цифровая грамотность медицинского персонала (Poduzova, 2023). Распространены случаи несоблюдения медицинскими работниками базовых правил кибербезопасности: использование простых паролей, передача логинов и паролей другим лицам, работа на зараженных вирусами компьютерах, подключение к МИС личных мобильных устройств.

Также серьезную угрозу создает сохраняющаяся практика обработки медицинских персональных данных без средств автоматизации, то есть в бумажном виде. По экспертным оценкам, доля электронного документооборота в российских медицинских организациях составляет всего 20 %. Бумажные медицинские карты и иные документы, содержащие врачебную тайну, зачастую хранятся без соблюдения элементарных мер физической защиты (в незапертых шкафах и кабинетах). Это создает риски несанкционированного доступа и копирования, краж и потерь данных.

---

[10] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. 31.07.2006. № 31. Ст. 3448.

[11] Постановление Правительства РФ от 16.03.2009 № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» // Собрание законодательства РФ. 23.03.2009. № 12. Ст. 1431.

[12] Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ // Собрание законодательства РФ. 07.01.2002. № 1 (ч. 1). Ст. 1.

[13] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Собрание законодательства РФ. 07.01.2002. № 1 (ч. 1). Ст. 1.

Таким образом, обеспечение безопасности персональных данных в сфере российского здравоохранения представляет собой комплексную проблему, требующую усилий как в плане совершенствования правового регулирования, так и в плане повышения уровня оснащенности медицинскими организациями современными IT-системами, наращивания кадрового потенциала и формирования культуры информационной безопасности среди медицинских работников. При этом надзорным органам следует уделять больше внимания не только контрольно-карательным мерам, но и профилактической и консультативной работе с операторами медицинских персональных данных.

Основы регулирования персональных данных в сфере здравоохранения в США

В США защита персональных данных пациентов регулируется, прежде всего, Законом о переносимости и подотчетности медицинского страхования (Health Insurance Portability and Accountability Act – HIPAA) 1996 г. (Edemekong, Annamaraju & Haydel, 2024) HIPAA устанавливает национальные стандарты для электронных транзакций в сфере здравоохранения и защиты конфиденциальности индивидуально идентифицируемой медицинской информации (Evans, 2016).

Закон применяется к так называемым «покрываемым организациям» (covered entities), которые включают в себя медицинские страховые компании, клиринговые центры и поставщиков медицинских услуг (больницы, клиники, врачи, фармацевты и т.д.), которые передают информацию в электронном виде.

Также под действие HIPAA подпадают бизнес-партнеры указанных организаций, получающие доступ к охраняемым данным.

HIPAA предъявляет детальные требования к обеспечению безопасности и конфиденциальности электронных персональных медицинских данных (electronic protected health information – ePHI)[14]. Закон обязывает покрываемые организации внедрять административные, физические и технические меры защиты ePHI от несанкционированного доступа, уничтожения, изменения, раскрытия.

В частности, Правило безопасности HIPAA (HIPAA Security Rule) предусматривает такие требования, как:

- назначение сотрудника, ответственного за соблюдение процедур обеспечения безопасности ePHI;
- ограничение использования и разглашения ePHI случаями, разрешенными Правилами приватности HIPAA или санкционированными субъектом данных;
- внедрение правил доступа и разграничение прав пользователей информационных систем на основе ролей;
- проведение оценки рисков и регулярных аудитов безопасности ИТ-инфраструктуры;
- шифрование ePHI при передаче и хранении;
- заключение письменных соглашений с бизнес-партнерами о конфиденциальности;
- обучение персонала политикам и процедурам защиты ePHI;
- уведомление пациентов и регуляторов о случаях компрометации ePHI.

[14] HIPAA Journal. Healthcare Ransomware Attacks Increased by 123% in 2021. Режим доступа: https://www.hipaajournal.com/healthcare-ransomware-attacks-increased-by-123-in-2021/ (дата обращения: 26.03.2024).

HIPAA предусматривает серьезные санкции для организаций, допустивших нарушение требований безопасности или приватности. Размеры штрафов варьируются от $100 до $50 000 за нарушение и могут достигать $1,5 млн в год для случаев злонамеренного пренебрежения установленными правилами. За умышленные нарушения из корыстных побуждений виновным должностным лицам грозит уголовная ответственность вплоть до 10 лет лишения свободы.

Контроль за соблюдением HIPAA возложен на Министерство здравоохранения и социальных служб США (Department of Health and Human Services – HHS) и его подразделение – Офис по гражданским правам (Office for Civil Rights – OCR). Они проводят периодические проверки покрываемых организаций, расследуют жалобы граждан, накладывают штрафы на нарушителей.

Помимо HIPAA определенные нормы о защите медицинской информации содержатся в Законе о технологиях и клинической медицине в области экономики и здравоохранения (Health Information Technology for Economic and Clinical Health Act – HITECH) 2009 г.[15], Законе о недискриминации на основе генетической информации (Genetic Information Nondiscrimination Act – GINA) 2008 г.[16], некоторых других федеральных и местных актах[17].

Законодательные требования и усиление контроля со стороны государства стимулировали повсеместное внедрение в США электронных медицинских карт (Electronic Health Records – EHR) (Adler-Milstein & Jha, 2017). По данным Управления национального координатора по ИТ в здравоохранении (Office of the National Coordinator for Health IT – ONC), в 2017 г. EHR использовали уже 86 % врачей и более 96 % больниц. Это позволяет поставщикам медицинских услуг эффективно собирать, хранить и обмениваться информацией о пациентах, одновременно обеспечивая надежную защиту персональных данных.

Провайдеры EHR-систем, чтобы иметь право работать с покрываемыми HIPAA организациями, обязаны проходить добровольную сертификацию ONC на соответствие требованиям безопасности, функциональности и интероперабельности. Сертификация проводится аккредитованными лабораториями по утвержденной методологии и включает тестирование таких функций как идентификация/аутентификация пользователей, управление доступом, аудит, шифрование, электронная подпись.

Несмотря на строгое регулирование и высокий уровень цифровизации, в американском здравоохранении случаются громкие утечки персональных данных. Например, в 2015 г. из-за хакерской атаки на страховую компанию Anthem была скомпрометирована информация почти 79 млн человек (Wikina, 2014). В последние годы основной причиной инцидентов стали атаки программ-вымогателей типа WannaCry, Ryuk, Conti. Так, в 2021 г. от действий шифровальщика Ryuk пострадала сеть Universal Health Services, управляющая 400 больницами.

Для противодействия угрозам Министерство здравоохранения США рекомендует учреждениям здравоохранения внедрять передовые методы обеспечения кибербезопасности, такие как многофакторная аутентификация, сегментация сети,

[15] U.S. Department of Health & Human Services. Health Information Privacy: Enforcement Process. Режим доступа: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-process/index.html (дата обращения: 26.03.2024).

[16] Genetic Information Nondiscrimination Act of 2008 (GINA), Pub. L. 110-233, 122 Stat. 881.

[17] HIPAA Journal. What Are the Penalties for HIPAA Violations? Режим доступа: https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/ (дата обращения: 26.03.2024).

платформы анализа и визуализации событий (SIEM), программы выявления и предотвращения вторжений (IDS/IPS). Большое значение имеет регулярное обучение сотрудников правилам кибергигиены и реагирования на инциденты.

Таким образом, США являются одним из мировых лидеров в сфере защиты медицинских персональных данных. Строгое законодательство, активный надзор со стороны регуляторов, высокий уровень цифровизации здравоохранения, развитая культура информационной безопасности – все эти факторы в совокупности обеспечивают надежную защиту прав американских пациентов. Опыт США заслуживает внимательного изучения и может быть полезен для совершенствования системы защиты медицинских данных в других странах.

Основы регулирования персональных данных в сфере здравоохранения в Европейском Союзе

В Европейском союзе защита персональных данных, включая медицинскую информацию, регулируется Общим регламентом по защите данных (General Data Protection Regulation – GDPR). Этот документ вступил в силу 25 мая 2018 г. и заменил собой Директиву о защите данных 95/46/EC. GDPR устанавливает единые правила обработки персональных данных на всей территории ЕС и имеет прямое действие во всех странах-членах[18].

Согласно GDPR медицинские сведения относятся к специальной категории персональных данных (sensitive data) наряду с информацией о расовой и этнической принадлежности, политических и религиозных взглядах, генетическими и биометрическими данными. Обработка таких данных по общему правилу запрещена, кроме определенных случаев, когда субъект дал явное согласие на обработку или она необходима для целей здравоохранения.

Регламент предъявляет строгие требования к операторам ПД (контролерам и процессорам данных) по обеспечению безопасности обрабатываемой информации. В частности, они обязаны:

- применять шифрование и псевдонимизацию персональных данных;
- обеспечивать конфиденциальность, целостность, доступность и отказоустойчивость систем обработки;
- восстанавливать доступность данных в случае инцидентов;
- регулярно тестировать и оценивать эффективность мер безопасности.

Медицинские учреждения ЕС также должны вести учет всех действий с персональными данными пациентов, включая сбор, хранение, изменение, раскрытие, удаление. При этом ПД разрешено хранить в форме, позволяющей идентифицировать субъектов, не дольше, чем это необходимо для целей обработки.

Контролеры данных обязаны документировать факты утечек персональных данных и сообщать о серьезных инцидентах в надзорный орган в течение 72 часов с момента обнаружения. Если инцидент может создать высокий риск для прав и свобод пациентов, затронутых утечкой, их необходимо проинформировать напрямую без промедления[19].

[18] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[19] European Union Agency for Cybersecurity (ENISA). (2020) ENISA Threat Landscape 2020 – The year in review. October 2020.

За несоблюдение требований GDPR предусмотрены значительные штрафы – до 20 млн евро или, в случае предприятия, до 4 % его общего годового оборота за предыдущий финансовый год, в зависимости от того, какой параметр больше. Кроме того, любое лицо, которому причинен ущерб из-за нарушения Регламента, имеет право получить от контролера или процессора компенсацию за причиненный ущерб[20].

Практика применения GDPR в здравоохранении пока неоднозначна. С одной стороны, крупные медицинские организации, особенно в западноевропейских странах, существенно усилили меры защиты данных, опасаясь репутационных рисков и многомиллионных штрафов. Значительные средства инвестируются во внедрение передовых ИТ-решений для обеспечения кибербезопасности (шифрование, анонимизация, СЗИ, SIEM, SOC и пр.). Регулярно проводится обучение персонала правилам обработки персональных данных.

С другой стороны, многие небольшие клиники и лаборатории, особенно в Восточной Европе, пока не в полной мере выполняют требования GDPR из-за нехватки финансовых и кадровых ресурсов. Остаются распространенными такие проблемы, как передача медицинских данных по незащищенным каналам связи, использование устаревших версий программного обеспечения с уязвимостями, несанкционированный доступ сотрудников к информации. Как показывает статистика, именно человеческий фактор является причиной большинства утечек персональных данных в медицинском секторе ЕС.

Для контроля за соблюдением GDPR в каждой стране ЕС созданы уполномоченные органы по защите данных (Data Protection Authorities). Они принимают жалобы граждан, проводят расследования, налагают штрафы, дают официальные разъяснения по вопросам толкования и применения Регламента. Также на уровне ЕС действует Европейский совет по защите данных (EDPB), в который входят главы национальных надзорных органов. EDPB призван обеспечивать единообразное применение GDPR по всему Евросоюзу.

Наднациональные структуры ЕС помогают медицинским организациям эффективно выполнять требования по защите данных. Разработаны подробные руководства и рекомендации, адаптированные под специфику здравоохранения Еврокомиссия финансирует исследовательские проекты по таким направлениям как конфиденциальные вычисления над большими медицинскими данными, федеративное машинное обучение, многосторонние вычисления. Их цель – найти баланс между приватностью пациентов и потребностями медицинской науки в обработке деперсонализированных массивов данных для создания инноваций (Greenleaf, 2019).

Определенные коррективы в правила GDPR внесла пандемия COVID-19. Регуляторы признали допустимым использование персональных данных граждан (в частности, сведений о локации, контактах, результатах тестов), если это необходимо для борьбы с коронавирусной инфекцией и при условии соблюдения принципов законности, минимизации данных, ограничения цели и хранения. Применение GDPR не должно препятствовать экстренным мерам по охране здоровья населения.

В целом, несмотря на отдельные трудности и национальные различия, GDPR оказывает положительное влияние на уровень защиты медицинских данных в Евро-

[20] European Data Protection Board. (2020) Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak. Adopted on 21 April 2020.

пейском Союзе. Закон способствует гармонизации норм на общеевропейском пространстве, внедрению передовых практик информационной безопасности, повышению прозрачности и подконтрольности обработки персональных данных. При этом важно найти разумный баланс между защитой прав граждан и интересами развития медицинских технологий на основе анализа больших данных.

Основы регулирования персональных данных в сфере здравоохранения в Китае

Правовое регулирование защиты персональных данных в Китае носит комплексный характер и основывается на нескольких ключевых нормативных актах. Базовым документом является Закон КНР о кибербезопасности, вступивший в силу 1 июня 2017 г.[21] Он устанавливает общие принципы и требования к сетевой безопасности, включая защиту персональной информации.

Закон обязывает операторов сетей соблюдать принципы законности, правомерности и необходимости при сборе и использовании персональных данных, получать согласие субъектов, обеспечивать безопасность и конфиденциальность информации[22]. За нарушение этих норм предусмотрена административная и уголовная ответственность.

Более детально вопросы защиты персональных данных в Интернете регламентирует Положение о защите личной информации в сети, принятое в 2012 г. Оно определяет состав личной информации, общие и специальные правила ее сбора и использования, права субъектов, обязанности операторов. В частности, операторы должны публиковать политику конфиденциальности, хранить собранную информацию не дольше необходимого срока, применять шифрование и другие меры безопасности, уведомлять пользователей об утечках данных.

На практике эти общие нормы дополняются отраслевыми стандартами и правилами. Так, в сфере здравоохранения действует национальный стандарт по безопасности личной информации пациентов (Dai, Zheng & Zhang, 2019). Он предписывает медучреждениям получать письменное согласие граждан на обработку информации об их здоровье, обеспечивать анонимизацию и шифрование медицинских данных, использовать их только для заявленных целей.

Особенностью китайского подхода является широкий доступ государства к персональным данным, объясняемый приоритетом национальной безопасности и общественных интересов. По закону операторы сетей обязаны предоставлять необходимую информацию по запросу полиции, органов госбезопасности и прокуратуры в целях защиты национальной безопасности или расследования преступлений. На практике спецслужбы имеют доступ к различным базам данных, включая медицинские (Cheng, Liu & Yao, 2017).

Китайский рынок здравоохранения переживает цифровую трансформацию, активно внедряя такие технологии, как большие данные, искусственный интеллект, интернет медицинских вещей. С одной стороны, это помогает улучшить качество медицинских услуг, оптимизировать управление ресурсами, развивать персонализированную медицину. Анализ обезличенных массивов медицинских данных позволяет

[21] Cybersecurity Law of the People's Republic of China. Режим доступа: http://www.npc.gov.cn/englishnpc/c23934/202012/32/ content_2511499.shtml (дата обращения: 26.03.2024).
[22] Cybersecurity Law of the People's Republic of China, Article 28.

выявлять закономерности в распространении заболеваний, оценивать эффективность лечения, прогнозировать эпидемии.

С другой стороны, концентрация огромных объемов чувствительной информации в государственных системах создает дополнительные риски утечек данных. В Китае уже происходили громкие инциденты, связанные с компрометацией медицинских данных граждан из-за небрежности администраторов или действий злоумышленников. Поэтому обеспечение надежной защиты больших медицинских данных является приоритетной задачей как для государства, так и для бизнеса.

Заслуживает внимания опыт города Яньтай провинции Шаньдун, где в 2019 г. была создана единая муниципальная платформа обмена медицинскими данными. Она объединяет информацию из электронных медкарт жителей, поступающую из больниц, клиник, лабораторий и страховых компаний города. При этом данные деперсонализируются с помощью новейших методов анонимизации и шифруются перед загрузкой в систему (Zhang, et al., 2018).

Платформа используется для выявления групп риска, профилактики хронических заболеваний, мониторинга назначений лекарств, анализа эффективности работы медучреждений. Доступ к обезличенным данным предоставляется муниципальным управленцам, эпидемиологам, медицинским экспертам. При этом к конфиденциальности информации предъявляются повышенные требования в соответствии со стандартами информационной безопасности в здравоохранении.

Яньтайский проект демонстрирует потенциал использования больших медицинских данных на благо общества при условии надежной защиты личной информации граждан. Он привлек внимание китайского правительства, которое рассматривает возможность масштабирования этой модели на другие регионы страны (Dai, Zheng & Zhang 2019).

В целом, несмотря на наличие солидной правовой базы, говорить о высоком уровне защиты медицинских персональных данных в Китае пока преждевременно. Имеются проблемы с практической реализацией законодательных норм, особенно в небольших медучреждениях. Серьезную озабоченность вызывает чрезмерно широкий доступ государства к личной информации граждан под предлогом защиты безопасности.

Вместе с тем Китай активно инвестирует в развитие передовых ИТ-решений для безопасности данных в здравоохранении, таких как блокчейн, федеративное машинное обучение, конфиденциальные вычисления, гомоморфное шифрование. В условиях стремительной цифровизации отрасли это позволяет надеяться на постепенное выстраивание эффективной и сбалансированной системы защиты медицинских данных в КНР.

Основы регулирования персональных данных в сфере здравоохранения в странах Азии

Страны Азиатско-Тихоокеанского региона демонстрируют разнообразие подходов к регулированию защиты персональных данных, в том числе в сфере здравоохранения. Наиболее развитое законодательство в этой области имеют Япония, Южная Корея и Сингапур. Эти государства уже давно приняли специальные законы о персональных данных, которые во многом схожи с европейскими нормами.

Так, в Японии действует Закон о защите персональной информации (APPI), первая редакция которого была принята еще в 2003 г. Закон распространяется на всех операторов ПД, обрабатывающих данные более 5000 субъектов. Он устанавливает принципы законной и добросовестной обработки, ограничения на сбор и использование ПД, требования к обеспечению их безопасности. Контроль за исполнением закона возложен на Комиссию по защите персональной информации.

В 2017 г. в APPI были внесены поправки, сблизившие японское законодательство с GDPR. В частности, введено требование получать согласие субъектов на передачу их ПД третьим лицам за рубеж. Ужесточены санкции за нарушения – максимальный штраф увеличен до 1 млн иен. Отдельные нормы APPI конкретизированы в отраслевых руководствах, таких как Руководство по защите медицинской информации.

В Южной Корее основным законом в сфере ПД является Закон о защите персональной информации (PIPA), принятый в 2011 г. Как и японский APPI, он налагает на операторов ПД обязанности по сбору минимально необходимых данных, получению согласия субъектов, обеспечению безопасности ПД, уведомлению об утечках. За нарушения предусмотрены серьезные штрафы и даже тюремное заключение.

В 2020 г. корейский парламент принял поправки к PIPA, которые существенно ужесточили требования к операторам, сблизив местные нормы с GDPR. Были усилены права субъектов ПД, ограничены возможности для профилирования и автоматизированного принятия решений, введена обязанность назначать сотрудника, ответственного за защиту данных. Особо чувствительные ПД, включая медицинскую информацию, теперь можно передавать за рубеж только с явного согласия субъекта[23].

В Сингапуре защита персональных данных регулируется Законом о защите персональных данных (PDPA) 2012 г. Его нормы во многом аналогичны японскому и корейскому законодательству. В 2020 г. в PDPA также были внесены изменения в русле сближения с GDPR – усилены штрафы, ограничено профилирование, разрешено обрабатывать данные для законных интересов без согласия.

В отличие от развитых восточноазиатских стран, Индия пока не имеет единого закона о персональных данных. Конституция страны признает право на приватность, а в 2017 г. Верховный суд Индии подтвердил, что оно распространяется и на личную информацию. Отдельные нормы о защите ПД содержатся в Законе об информационных технологиях 2000 г. и подзаконных актах (Edemekong, Annamaraju & Haydel, 2024).

В 2018 г. правительственный комитет подготовил проект закона о защите персональных данных, в 2019 г. парламент представил его доработанную версию. Законопроект предусматривает широкие права граждан в отношении их ПД, дифференцированные обязанности для операторов, включая локализацию критически важных данных, экстерриториальное действие закона и создание регулятора (Data Protection Authority). Однако пока он не принят из-за критики со стороны бизнеса.

В Таиланде в 2019 г. вступил в силу Закон о защите персональных данных, основанный на принципах GDPR. Он дает субъектам ПД права требовать от операторов доступа, исправления, удаления их данных. Операторы обязаны иметь законные основания для обработки ПД (согласие, договор, закон), сообщать об утечках,

[23] Sheng, W. (2019) **万条公民信息在暗网售**卖，大量为医疗信息 (30 million pieces of citizen information sold on darknet, mostly medical information), 12. Xinjing Daily.

назначать DPO и представителя в стране. За нарушения грозит уголовная ответственность – до 1 года тюрьмы. Но полноценно закон пока не работает из-за отсутствия подзаконных актов[24].

Как показывают опросы, жители азиатских стран в целом более терпимо относятся к сбору их персональных данных государством и бизнесом, чем европейцы или американцы. Во многом это связано с культурными особенностями, такими как коллективизм, уважение к власти, готовность жертвовать личными интересами ради общего блага. Кроме того, люди ценят удобство цифровых сервисов и готовы делиться информацией в обмен на их преимущества.

Такие установки создают благоприятную среду для реализации инновационных проектов в сфере здравоохранения. Примером может служить японская инициатива по сбору медицинских big data для развития персонализированной медицины и созданию на их основе новых продуктов и услуг. В рамках проекта данные из электронных медкарт, генетических тестов, носимых устройств, приложений поступают в единую базу данных, обезличиваются и анализируются ИИ[25].

Южная Корея активно развивает удаленный мониторинг здоровья хронических больных с помощью IoMT (Интернета медицинских вещей). Пациенты используют домашние смарт-устройства, передающие данные в реальном времени лечащим врачам. Это позволяет вовремя выявлять угрожающие симптомы, корректировать терапию, избегать осложнений. Власти поддерживают проекты развертывания общенациональной IoMT-платформы, совместимой с системами больниц.

В Сингапуре реализуется проект HealthHub – онлайн-платформа для управления здоровьем, агрегирующая медицинские данные из государственных клиник. Через веб-сайт или приложение пациенты получают доступ к своим электронным медкартам, результатам анализов, назначениям врачей и могут делиться этой информацией с другими поставщиками медуслуг. Платформа также предлагает персонализированные рекомендации по здоровому образу жизни на основе анализа данных пользователей[26].

Подобные инициативы, безусловно, несут в себе риски утечек персональных данных из-за чрезмерной централизации чувствительной информации и недостаточной культуры кибербезопасности. В Сингапуре и Южной Корее уже случались громкие инциденты с компрометацией медицинских данных граждан. Поэтому критически важно, чтобы цифровая трансформация здравоохранения сопровождалась адекватными мерами по защите персональных данных как на уровне законов, так и на уровне технологий и организационных практик.

Рекомендации по совершенствованию законодательства РФ в сфере защиты медицинских персональных данных

«Огораживание» медицинских данных, затрудняющее их вторичное использование для научных и управленческих задач, в конечном счете может негативно

[24]Amended Act on the Protection of Personal Information (Japan). Режим доступа: https://www.ppc.go.jp/en/news/archives/2017/170530/ (дата обращения: 26.03.2024).

[25] Act on the Protection of Personal Information (Japan). Режим доступа: https://www.ppc.go.jp/en/legal/ (дата обращения: 26.03.2024).

[26] Personal Data Protection Act 2012 (Singapore). Режим доступа: https://sso.agc.gov.sg/Act/PDPA2012 (дата обращения: 26.03.2024).

повлиять на интересы самих пациентов. В то же время ослабление контроля чревато нарушениями прав граждан, дискриминацией по медицинскому признаку со стороны работодателей и страховщиков. Отсюда вывод: защита персональных медицинских данных должна быть разумной, сфокусированной на предотвращении неправомерного доступа и противоправного использования, но не препятствующей легальному обмену деперсонализированной информацией для общественного блага.

Наиболее строгими и эффективными системами защиты медицинских персональных данных обладают США и ЕС. Китай, Россия пока отстают как в плане нормативного регулирования, так и практической реализации. Развитые страны Азии (Япония, Корея, Сингапур) занимают промежуточное положение, сочетая достаточно современное законодательство с высоким уровнем цифровизации здравоохранения. Приведена сравнительная таблица правового регулирования защиты медицинских персональных данных по ключевым параметрам в рассмотренных странах.

Правовое регулирование защиты медицинских персональных данных по ключевым параметрам

Критерий	Россия	США	ЕС	Китай	Япония	Юж. Корея	Сингапур
Специальный закон о мед. данных	Нет	HIPAA	GDPR распространяется	Нет	APPI распространяется	PIPA распространяется	PDPA распространяется
Согласие на обработку	Требуется	Требуется	Требуется	Требуется	Требуется	Требуется	Требуется
Ответственность за нарушения	Низкие штрафы, редко применяются	Высокие штрафы, уголовная ответственность	Очень высокие штрафы (до 4% годового оборота)	Есть административная и уголовная	Умеренные штрафы	Высокие штрафы и уголовная ответственность	Умеренные штрафы
Надзорный орган	Роскомнадзор	HHS OCR	Национальные DPA	Нет единого	PPC	PIPC	PDPC
Обязательное уведомление об утечках	Нет	Да, без промедления	Да, в течение 72 часов	Нет	Нет	Да	Да
Требования безопасности ИС	Приказ Минздрава 911н	HIPAA Security Rule	GDPR ст.32	Общие требования кибербезопасности	APPI ст.20	Сетевой закон	Практические коды
Уровень цифровизации мед. организаций	Низкий	Высокий	Средний	Средний	Высокий	Высокий	Высокий
Обучение персонала	Недостаточное	Обязательное регулярное	Обязательное регулярное	Недостаточное	Рекомендуется	Обязательное	Рекомендуется

Legal regulation of medical personal data protection data protection by key parameters

Criterion	Russia	U.S.	EU	China	Japan	South Korea	Singapore
A special act on medical data	No	HIPAA	GDPR applies	No	APPI applies	PIPA applies	PDPA applies
Consent to processing	Required	Required	Required	Required	Required	Required	Required
Liability for violations	Low penalties, rarely enforced	High penalties, criminal liability	Very high penalties (up to 4% of annual turnover)	Administrative and criminal liability	Moderate penalties	High penalties and criminal liability	Moderate penalties
Supervisory body	Roskomnadzor	HHS OCR	National DPAs	No single supervisory body	PPC	PIPC	PDPC
Mandatory notification of data breach	No	Yes, without delay	Yes, within 72 hours	No	No	Yes	Yes
IS security requirements	Ministry of Health Order No. 911n	HIPAA Security Rule	GDPR Art.32	General cybersecurity requirements	APPI Art.20	Network law	Practice Codes
Level of digitalization of medical organizations	Low	High	Medium	Medium	High	High	High
Staff training	Insufficient	Mandatory regular	Mandatory regular	Insufficient	Recommended	Mandatory	Recommended

Проведенный анализ зарубежного опыта правового регулирования защиты персональных данных в здравоохранении позволяет сформулировать ряд рекомендаций по развитию российского законодательства в этой сфере.

1. Представляется целесообразным ужесточить ответственность медицинских организаций за нарушение требований по обеспечению безопасности персональных данных пациентов, в частности, за допущение их утечки. Действующие штрафы по статье 13.11 КоАП РФ (до 50 тыс. руб. для юридических лиц) недостаточны для превенции правонарушений и несопоставимы с многомиллионными санкциями в странах ЕС и США.

Стоит рассмотреть возможность повышения верхнего предела штрафов до нескольких миллионов рублей, а также введения уголовной ответственности для должностных лиц, виновных в массовых утечках медицинских данных. Аналогичные нормы существуют в Южной Корее – до 5 лет лишения свободы и штрафа до $40 тыс. Это будет стимулировать медицинские организации серьезнее относиться к вопросам обеспечения информационной безопасности.

2. По примеру GDPR следует законодательно обязать медучреждения оперативно (в течение 72 часов) сообщать об инцидентах, связанных с утечкой персональных данных, в уполномоченный орган, а в случае высоких рисков – также уведомлять субъектов персональных данных.

Это повысит прозрачность и контроль в отрасли, поскольку сейчас многие утечки скрываются из-за боязни репутационных потерь. Своевременное информирование поможет минимизировать ущерб, оперативно принять меры реагирования. Пациенты смогут скорректировать свое поведение, например, сменить скомпрометированные пароли.

3. Целесообразно утвердить детальные отраслевые требования по безопасности информационных систем в сфере здравоохранения, как это сделано в США стандартом HIPAA Security Rule. Он предписывает проводить оценку рисков, использовать контроль доступа и шифрование, вести аудит событий безопасности, обучать персонал, иметь планы реагирования на инциденты и т.д.

Аналогичный документ, адаптированный под российские реалии, мог бы стать ориентиром для медицинских организаций по внедрению комплекса мер защиты персональных данных. Соответствие таким требованиям должно быть предметом обязательной сертификации МИС – по примеру американской программы сертификации EHR-технологий на соответствие HIPAA.

4. Актуальной задачей является установление специальных правил работы со сверхчувствительными персональными данными, такими как биометрия, геномная информация, психическое здоровье и др. Пока в законе «О персональных данных» они лишь упомянуты как частные случаи специальных категорий ПД и обрабатываются на общих основаниях.

Необходимо закрепить более строгие требования к сбору, хранению и использованию таких данных – в части согласия, безопасности, трансграничной передачи и др. В этом случае целесообразно изучить передовые практики Евросоюза и Китая, уже имеющих подобные нормы.

5. Важным условием обеспечения безопасности медицинских данных является перевод всей документации в защищенный электронный вид. Пока во многих российских клиниках сохраняется бумажный документооборот, что создает риски утечек и затрудняет контроль доступа.

Государству следует стимулировать внедрение МИС, выделять целевое финансирование на закупку медицинскими организациями современного IT-оборудования и программного обеспечения, особенно отечественных разработок. Все электронные медицинские данные должны храниться и передаваться исключительно в шифрованном виде с использованием криптографии по ГОСТам.

6. Одним из ключевых факторов утечек медицинских данных в России остается человеческий фактор, прежде всего низкая компьютерная грамотность медицинского персонала и пренебрежение правилами кибергигиены. Исправить ситуацию можно только путем массового обучения медработников методам безопасной работы с информацией ограниченного доступа.

Целесообразно законодательно закрепить требование о регулярном прохождении медиками курсов повышения квалификации по тематике информационной безопасности и защиты персональных данных. Основы цифровой грамотности и принципы работы с конфиденциальными данными следует включить в образовательные стандарты всех уровней подготовки медицинских кадров – вузов, колледжей, ординатуры.

7. По аналогии с американской системой оперативного реагирования US-CERT имеет смысл создать на базе Минздрава РФ ситуационный центр мониторинга и реагирования на инциденты ИБ в сфере здравоохранения, работающий в круглосуточном режиме.

Важно наладить эффективный обмен информацией об угрозах и уязвимостях между медорганизациями, IT-компаниями, регуляторами (Минздрав, Роскомнадзор, ФСБ, ФСТЭК) и правоохранительными органами. Это позволит быстрее выявлять атаки на МИС, обмениваться успешными практиками защиты, минимизировать ущерб от инцидентов.

Заключение

Подводя итог проведенному анализу правового регулирования и практики защиты персональных данных пациентов в России и за рубежом, можно констатировать наличие как общих проблем, так и особенности каждой из стран в данной сфере.

Наиболее развитые системы обеспечения безопасности медицинской информации созданы в США и Евросоюзе. Специализированные законы (HIPAA в США, GDPR в ЕС) устанавливают жесткие требования к операторам медицинских данных по обеспечению их конфиденциальности, целостности и доступности. Регуляторы ведут активный надзор за соблюдением законодательства, применяя серьезные санкции к нарушителям вплоть до многомиллионных штрафов и уголовного преследования.

Важную роль играет высокий уровень цифровизации системы здравоохранения, в частности, повсеместное внедрение сертифицированных EHR-систем, использующих передовые методы защиты информации (шифрование, многофакторная аутентификация, детализация действий пользователей, проактивное выявление утечек данных и т.д.). Большое внимание уделяется обучению медработников правилам кибергигиены и формированию культуры информационной безопасности.

В то же время угрозы безопасности медицинских данных приобретают транснациональный характер. Во всех странах растет число утечек из-за целенаправленных хакерских атак (в том числе с использованием программ-вымогателей), инсайдерских действий персонала, потери или кражи мобильных устройств. Это требует постоянного совершенствования системы защиты данных, внедрения новых организационных и технических мер контроля, адекватных современному ландшафту угроз.

Российская нормативная база в области защиты медицинских персональных данных в целом сопоставима с передовыми зарубежными практиками. Федеральный закон «О персональных данных», отраслевые требования Минздрава России (приказ № 911н) и другие подзаконные акты налагают на операторов персональных данных обязанности по обеспечению их безопасности, при необходимости – с использованием сертифицированных средств защиты информации. Вместе с тем размеры штрафов несоизмеримы с западными аналогами, а случаи уголовного преследования за незаконные действия с медицинскими персональными данными практически отсутствуют.

Главные проблемы связаны с недостаточной реализацией установленных законом требований на практике. Утечки медицинских данных из российских клиник стали почти обыденным явлением. Причины кроются в хроническом недофинансировании IT-инфраструктуры (особенно в регионах), дефиците квалифицированных специалистов по информационной безопасности, низком уровне цифровых компетенций медиков, сохранении архаичных практик работы с информацией на бумажных носителях. Контрольно-надзорная деятельность Роскомнадзора и других регуляторов пока не привела к кардинальному улучшению ситуации.

Для изменения ситуации требуется системный подход, подразумевающий синхронизацию усилий на нескольких направлениях.

1. Совершенствование законодательства в русле гармонизации с лучшими мировыми практиками. Прежде всего, необходимо усиление ответственности за нарушения, дифференциация требований для разных категорий медицинских данных (в т.ч. генетических и биометрических), уточнение правил их трансграничной передачи.

2. Стимулирование цифровой трансформации медорганизаций, выделение целевых бюджетов на внедрение современных средств защиты информации, особенно отечественной разработки. Курс на импортозамещение должен учитывать реалии и не создавать необоснованных барьеров для использования эффективных зарубежных решений.

3. Массовое обучение медицинского персонала базовым правилам кибербезопасности. Необходимо включить соответствующие курсы во все программы подготовки медицинских кадров, а также ввести регулярную аттестацию действующих работников на знание политик информационной безопасности.

4. Построение эффективной системы непрерывного мониторинга и реагирования на инциденты ИБ в медицинских сетях, обмена данными об угрозах между всеми заинтересованными сторонами (регуляторами, медицинскими организациями, IT-компаниями, исследовательскими центрами).

5. Превентивная работа регуляторов с операторами персональных данных – методическая поддержка, информирование о типовых нарушениях и лучших практиках их устранения, стимулирование добровольного аудита и сертификации на соответствие отраслевым стандартам информационной безопасности.

Таким образом, для совершенствования защиты персональных данных в российском здравоохранении целесообразно использовать комплексный подход, включающий законодательные, организационные, технические и образовательные меры. Ориентиром для нас могут служить эффективные практики США, ЕС и других развитых стран, адаптированные к национальной специфике.

Вместе с тем не стоит прямо копировать зарубежный опыт, поскольку в РФ иные правовые реалии, ресурсные возможности, IT-инфраструктура. Кроме того, излишне строгие нормы могут создать барьеры для развития инноваций в медицине (телемедицины, ИИ-диагностики, интернета медицинских вещей). Поиск баланса между конфиденциальностью и прогрессом – главный вызов для законодателей на современном этапе.

References / Список литературы

Adler-Milstein, J. & Jha, A.K. (2017) HITECH Act Drove Large Gains In Hospital Electronic Health Record Adoption. *Health Affairs*. 36(8), 1416–1422. https://doi.org/10.1377/hlthaff.2016.1651

Bradford, L., Aboy, M. & Liddell, K. (2019) International health data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR). *Hum Genet*., 575–582. https://doi.org/10.1007/s00439-018-1919-7

Cheng, L., Liu, F. & Yao, D. (2017) Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery.* 7(5). e1211. https://doi.org/10.1002/widm.1211

Dai, H.N., Zheng, Z. & Zhang, Y. (2019) Blockchain for Internet of Things: A Survey. *IEEE Internet of Things Journal.* 6. 8076–8094. https://doi.org/10.1109/JIOT.2019.2920987

Edemekong, P.F. & Haydel, M.J. (2024) In: *StatPearls*. Health Insurance Portability and Accountability Act. StatPearls Publishing. pp. 18–19.

Edemekong, P.F., Annamaraju, P. & Haydel, M.J. (2024) In: *StatPearls*. Health Insurance Portability and Accountability Act. StatPearls Publishing. pp. 8–12.

Evans, R.S. (2016) Electronic Health Records: Then, Now, and in the Future. *Yearb Med Inform.* Suppl 1(Suppl 1), 48–61. https://doi.org/10.15265/IYS-2016-s006

Greenleaf, G. (2019) Global Tables of Data Privacy Laws and Bills. *6th Ed. Privacy Laws & Business International Report.* (9). https://doi.org/10.2139/ssrn.2280875

Gurtsko, L.D., Smirnov, E.K., Baranova, T.V., Tykyl-Ool, A.C. (2024) Digital competences of medical workers – priority of staffing of the health care system. *Zdorovye megapolisa*. 5(3), 167–172. https://doi.org/10.47619/2713-2617.zm.2024.v.5i3

Гурцкой, Л.Д., Смирнова Е.К., Баранова Т.В., Тыкыл-Оол А.С. Цифровые компетенции медицинских работников – приоритет кадрового обеспечения системы здравоохранения // Здоровье мегаполиса. 2024. Т. 5. № 3. С. 167–172. https://doi.org/10.47619/2713-2617.zm.2024.v.5i3

Okishev, B.A. (2022) Realisation of personal data protection in the field of medicine. *Bulletin of the O.E. Kutafin University (Moscow State Law Academy).* (4). 120–126. https://doi.org/10.17803/2311-5998.2022.92.4.120-126

Окишев, Б.А. Реализация охраны персональных данных в сфере медицины // Вестник Университета имени О.Е. Кутафина (МГЮА). 2022. № 4. С. 120–126. https://doi.org/10.17803/2311-5998.2022.92.4.120-126

Poduzova, E.B. (2023) Personal data of the patient and his legal representative: the specifics of electronic provision in the context of the application of 'artificial intelligence' technologies in digital medicine. *Actual problems of Russian law.* 18(4), 86–92. https://doi.org/10.17803/1994-1471.2023.149.4.086-092

Подузова, Е.Б. Персональные данные пациента и его законного представителя: специфика электронного предоставления в контексте применения технологий «искусственного интеллекта» в digital-медицине // Актуальные проблемы российского права. 2023. Т. 18. № 4. С. 86–92. https://doi.org/10.17803/1994-1471.2023.149.4.086-092

Wikina, S.B. (2014) What Caused the Breach? An Examination of Use of Information Technology and Health Data Breaches. *Perspectives in health information management*. 11(Fall), 1h.

Zhang, X., Liu, S., Chen, X., Wang, L., Gao, B. & Zhu, Q. (2018) Health information privacy concerns, antecedents, and information disclosure intention in online health communities. *Information and Management*. 55(4), 482–493.

Сведения об авторе:

Лебедева Диана Альбертовна – аспирант, Факультет права, Национальный исследовательский университет «Высшая школа экономики»; 101000, Российская Федерация, г. Москва, Б. Трехсвятительский пер., д. 3

ORCID: 0000-0003-0070-8300; SPIN-код: 1985-0155

e-mail: lebedevady@yandex.ru

About the author:

Diana A. Lebedeva – Law faculty, National Research University "Higher School of Economics"; 3 Bolshoy Tryokhsvyatitelsky Per., Moscow, 101000, Russian Federation

ORCID: 0000-0003-0070-8300; SPIN-код: 1985-0155

e-mail: lebedevady@yandex.ru