ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЗДРАВООХРАНЕНИИ: СОВРЕМЕННЫЕ УГРОЗЫ И МЕТОДЫ ЗАЩИТЫ

О. В. Соколова[1] ✉, О. В. Желткевич[1], С. В. Калабекова[2]

[1] Ярославский государственный медицинский университет, Ярославль, Россия

[2] Северо-Кавказская государственная академия, Черкесск, Россия

Статья посвящена анализу проблем информационной безопасности в здравоохранении России в условиях цифровой трансформации. Цифровизация сферы здравоохранения, включая интеграцию информационных систем медицинских и фармацевтических организаций с ЕГИСЗ, повышает качество оказания медицинской и лекарственной помощи населению. При этом увеличиваются риски утечек персональных данных пациентов и угрозы компьютерных атак на информационные системы организаций. Цель исследования — формирование комплексного подхода к обеспечению информационной безопасности в медицинских и фармацевтических организациях. В ходе исследования использованы контент-анализ, логический и структурный анализ научных трудов и нормативно-правовых актов в области применения информационных технологий в здравоохранении. Авторами выделены этапы регулирования информационной безопасности от защиты врачебной тайны к категорированию критической информационной инфраструктуры и применению отечественного программного обеспечения. Приведена классификация угроз безопасности цифровых систем по расположению источника угроз относительно организации по внешним и внутренним критериям. Предложены направления и критерии оценки для повышения информационной безопасности на основе современных методов и технологий защиты информации, включая технические средства защиты, юридические механизмы, а также организационно-управленческие методы.

Ключевые слова: здравоохранение, информационная безопасность, компьютерные атаки, защита информации, ЕГИСЗ, медицинские персональные данные, критическая информационная инфраструктура, медицинские и фармацевтические организации

✉ **Для корреспонденции:** Ольга Вячеславовна Соколова
ул. Революционная, д. 5, г. Ярославль, 150014, Россия; sova293@yandex.ru

Статья поступила: 10.04.2026 **Статья принята к печати:** 15.04.2026 **Опубликована онлайн:** 27.04.2026

DOI: 10.24075/medet.2026.009

INFORMATION SECURITY IN HEALTHCARE: MODERN THREATS AND PROTECTION METHODS

Sokolova OV[1] ✉, Zheltkevich OV[1], Kalabekova SV[2]

[1] Yaroslavl State Medical University, Yaroslavl, Russia

[2] North Caucasus State Academy, Cherkessk, Russia

The paper analyzes information security issues in Russian healthcare in the context of digital transformation. Digitalization of the healthcare sector, including integration of information systems of medical and pharmaceutical organizations with the Uniform State Health Information System (EGISZ), improves the quality of medicines and healthcare provided to the population. Meanwhile, the risk of patient personal data leakage and computer attacks on healthcare organizational information systems is increasing. The purpose of the study is to develop an integrated approach to information security in medical and pharmaceutical organizations. The research uses content analysis, logical and structural analysis of scientific papers and regulatory legal acts in the field of information technology in healthcare. The authors identify the stages of information security regulation from protecting medical secrets to categorizing critical information infrastructure and using domestic software. The classification of security threats to digital systems is provided based on the location of the threat source depending on whether they originate outside or inside the organization's network perimeter. The directions and evaluation criteria for improving information security are provided based on modern methods and technologies of information protection, including technical means of protection, legal mechanisms, as well as organizational and managerial methods.

Keywords: healthcare, information security, medical personal data, computer attacks, information protection, EGISZ, critical information infrastructure, medical and pharmaceutical workers

✉ **Correspondence should be addressed:** Olga V. Sokolova
Revolutsionnaya Str., 5, Yaroslavl, 150014, Russia; sova293@yandex.ru

Received: 10.04.2026 **Accepted:** 15.04.2026 **Published online:** 27.04.2026

DOI: 10.24075/medet.2026.009

Цифровизация и информатизация системы здравоохранения, реализуемая в рамках стратегии развития информационного общества и национального проекта «Здравоохранение», связана с внедрением и использованием информационных систем в медицинских и фармацевтических организациях для оказания качественной медицинской и лекарственной помощи. Информационные системы, предназначенные для автоматизации бизнес-процессов деятельности, предусматривают совокупность информационных, программных и технических, а также организационных средств [1, 2]. При этом в информационных системах объединены данные о финансовой, экономической, административной и организационной информации; медицинские сведения о пациентах; результаты исследований, мониторингов и др. Применение

информационных систем позволяет сокращать ошибки при заполнении отчетной документации, осуществлять быстрый доступ к медицинской информации больших объемов и др. [3].

Следует отметить о возможности интеграции информационных систем медицинских и фармацевтических организаций с Единой государственной информационной системой в сфере здравоохранения (ЕГИСЗ), одной из задач которой стоит информационное обеспечение государственного регулирования в сфере здравоохранения. ЕГИСЗ включает информацию о данных федеральной электронной регистратуры, электронных медицинских карт пациентов (ЭМК), электронных медицинских документов и др. Также в состав информации ЕГИСЗ входят и федеральные реестры. Федеральный регистр медицинских работников (ФРМР) — это централизованная база данных, которая содержит информацию о всех медицинских и фармацевтических работниках России. Федеральный регистр медицинских организаций (ФРМО), который содержит сведения о структуре, профилях деятельности, адресах и оснащении каждого медицинского учреждения. Подсистемы ЕГИСЗ представлены специализированным регистром пациентов по отдельным заболеваниям и/или состояниям, реестром лекарственных препаратов для медицинского применения, а также информационно-аналитической подсистемой мониторинга и контроля в сфере закупок лекарственных препаратов [4].

Следовательно, объединенная цифровая среда здравоохранения содержит актуальную информацию о техническом, лекарственном, кадровом обеспечении сферы здравоохранения и личных данных пациентов о состоянии их здоровья. Однако, как показывает практика, цифровая трансформация сопровождается ростом рисков, среди которых ведущее место занимают угрозы информационной безопасности. Поэтому необходимо обеспечение безопасности информационных систем для сохранности личных данных пациентов, специалистов путем разработки направлений защиты данных и оборудования от компьютерных атак [5–8].

Таким образом, актуальность темы определяется несколькими факторами. Во-первых, медицинские данные относятся к специальной категории персональных данных, их утечка влечет за собой нарушение права пациента на врачебную тайну. Во-вторых, медицинские и фармацевтические организации признаны субъектами критической информационной инфраструктуры (КИИ), что налагает на них повышенные требования к защите информации. В-третьих, рост числа компьютерных атак на сектор здравоохранения свидетельствует о высокой уязвимости отрасли (за первое полугодие 2025 г. их количество увеличилось на 24% по сравнению с аналогичным периодом 2024 г.). В-четвертых, уровень цифровой грамотности медицинских и фармацевтических работников и подготовки в сфере информационной безопасности нередко оказывается недостаточным.

Вышеизложенное определило цель настоящей работы — формирование комплексного подхода к обеспечению информационной безопасности в медицинских и фармацевтических организациях.

Достижение поставленной цели включало решение последовательных задач.

1. Анализ этапов развития защиты информационной безопасности в сфере здравоохранения.
2. Выделение и структурирование угроз информационной безопасности в здравоохранении.
3. Проведение анализа современных методов и технологий защиты информации.
4. Разработку рекомендаций и предложений по обеспечению информационной безопасности в медицинских и фармацевтических организациях.

МАТЕРИАЛЫ И МЕТОДЫ

Основой исследования явились научные публикации, как отечественных, так и зарубежных ученых в рамках применения информационных технологий при оказании медицинской и лекарственной помощи. Изучались нормативно-правовые акты в области цифровой трансформации здравоохранения. В процессе исследования использовались методы: логический, структурный, контент-анализ.

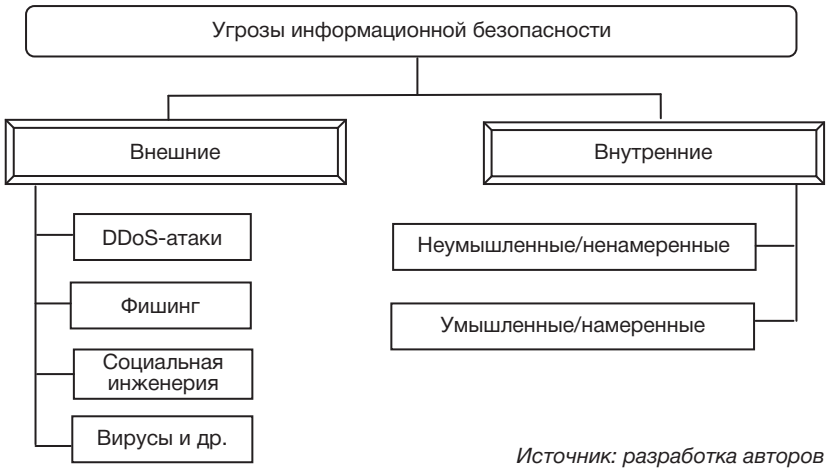
РЕЗУЛЬТАТЫ И ОБСУЖДЕНИЯ

На основе анализа нормативных документов показано, что информация как медицинская, так и фармацевтическая в российской правовой системе относится к категории «сведения, составляющие врачебную тайну» (ст. 13, ст. 20 Федерального закона № 323-ФЗ) [9] и одновременно к «специальным категориям персональных данных» (ст. 10 Федерального закона № 152-ФЗ) [10]. Такой двойной правовой статус предопределяет особый режим ее обработки. Сбор, хранение и передача таких данных требуют согласия субъекта или наличия законных оснований.

Формирование правового поля информационной безопасности российского здравоохранения происходит постепенно. Основное внимание, прежде всего, уделено соблюдению врачебной тайны и защите персональных данных в соответствии с Федеральным законом № 152-ФЗ [10]. В 2017 г. принят Федеральный закон № 187-ФЗ, который изменил подходы к защите информации. Так, медицинские информационные системы (МИС) и фармацевтические системы (ФС) отнесены к объектам критической информационной инфраструктуры (КИИ), что повлекло за собой обязанность по их категорированию [11]. В рамках выполнения требований закона о КИИ, оказывающие медицинскую и лекарственную помощь обязаны провести категорирование не только информационных систем, но и автоматизированных систем управления технологическими процессами (АСУ ТП), к которым относится и медицинское оборудование. Также необходимо создание ведомственных центров мониторинга и применение сертифицированных средств защиты.

В 2021 г. вступили в силу поправки к Указу Президента РФ № 250 [12], предписывающие руководителям организаций КИИ создать структурные подразделения по информационной безопасности. Это требование распространяется на организации федерального, регионального и муниципального уровней.

В 2022 г. Правительство РФ определило задачи Единой государственной системы здравоохранения (ЕГИСЗ), ее структуру, порядки и сроки предоставления информации, участников информационного взаимодействия, порядок защиты информации, содержащейся в единой системе, а также требования к программно-техническим



Источник: разработка авторов

Рис. Классификация угроз информационной безопасности в здравоохранении по источнику возникновения

средствам. Следующим важным этапом стало повышение требований к использованию иностранного программного обеспечения. С 2025 г. субъектам КИИ запрещено применять средства защиты информации иностранного производства [13].

Таким образом, на государственном уровне решаются вопросы защиты информационной безопасности в здравоохранении.

Проведенный анализ выявленных рисков цифровизации здравоохранения в рамках цифровой информационной безопасности показал, что наиболее вероятными представляются угроза утраты персональных данных пациента и компьютерные атаки на цифровые базы медицинских и фармацевтических организаций [14–17].

Установлено, что угрозы безопасности цифровых систем классифицируются по различным критериям. Следовательно, для дальнейшего изучения данного вопроса целесообразно использовать классификацию угроз информационной безопасности, адаптированную для медицинских и фармацевтических организаций. В связи с тем что угрозы исходят не только извне, но и изнутри организации нами представлена классификация по расположению источника угроз относительно организации (рис.).

Внешние угрозы проявляются в целенаправленных компьютерных атаках. Используются вредоносные программы для заражения систем и блокировки доступа к данным; DDoS-атаки на телемедицинские сервисы затрудняют работу информационных систем МО и ФО; фишинг и социальная инженерия, в виде рассылки писем от имени руководителей организации с просьбой сообщить пароль, направлены на получение конфиденциальной информации от пользователей. Устаревшие ИТ-системы нами также отнесены к внешним угрозам, потому что содержат уязвимости и могут использоваться злоумышленниками для несанкционированного доступа.

Внутренние угрозы информационной безопасности по источнику возникновения распределены на неумышленные и умышленные действия сотрудников организации. Угрозы, входящие в первую группу, связаны с потерей USB-флеш-накопителя (флешки), содержащего базы данных; с отправкой конфиденциальной информации в мессенджеры, с личной электронной почты (e-mail); с использованием простых паролей для аутентификации. Умышленные/намеренные действия могут сопровождаться продажей данных о пациентах конкурентам, копированием информации перед увольнением, нарушения регламентов работы с информационными системами и т.д.

Таким образом, понимание конкретных угроз информационной безопасности способствует формированию комплексной защиты от рисков.

Теоретические основы информационной безопасности в медицинских и фармацевтических организациях предполагают использование различных методов и технологий, включая технические средства защиты, юридические механизмы, а также организационно-управленческие методы.

Технические средства защиты охватывают: системы обнаружения и блокировки вторжений, программно-аппаратные решения (DLP-системы) против утечек данных, антивирусное программное обеспечение (ПО) и файерволы (межсетевой экран и др.). Для обеспечения безопасности данных применяются криптографические методы (алгоритмы шифрования данных и электронная цифровая подпись). Контроль доступа к данным обеспечивается системой аутентификации, предусматривающей использование паролей, сертификатов и биометрических данных.

На современном этапе развития общества правительство РФ поставило задачу создания программ по разработке отечественного ПО. Переход на отечественное ПО, предписанный законодательством, имеет не только политическое, но и практическое значение. Продукты российских разработчиков не уступают зарубежным аналогам по функциональности, а в ряде аспектов (интеграция с государственными системами мониторинга, адаптация к специфике российского законодательства) превосходят их [13].

Соблюдение требований в области обработки, хранения и передачи персональных данных в сфере здравоохранения регулируется комплексом нормативных правовых актов, а юридические механизмы правоприменения предусматривают ответственность за нарушение правил информационной безопасности в виде возмещения нанесенного пациенту ущерба и оплаты штрафа согласно ст. 13.11 КоАП РФ.

Технические средства и юридические механизмы защиты информации будут эффективны только в том случае, если они встроены в систему организационно-управленческих инструментов, которые используются для достижения целей и выполнения задач организации.

По результатам исследования нами предложен подход к обеспечению информационной безопасности в здравоохранении для оказания качественной медицинской и лекарственной помощи, состоящий из основных направлений и критериев оценки информационной безопасности.

Одним из направлений является категорирование объектов КИИ в соответствии с законодательством. В зависимости от требований к средствам защиты объекту присваивается категория значимости — первая, вторая или третья. Медицинские и фармацевтические организации включены в реестр значимых объектов КИИ [11].

Следующее направление предполагает создание системы реагирования на инциденты, связанные с несанкционированным доступом к информации: «разработка стандартной операционной процедуры (СОП) для четкого регламента действий при обнаружении взлома или утечки информации». Это позволяет понимать, кто принимает решение об отключении системы, кто взаимодействует с правоохранительными органами, кто уведомляет пациентов. Регулярные учения (например, имитация фишинговой атаки) помогают отработать эти действия на практике.

Важным направлением в обеспечении информационной безопасности является непрерывное обучение персонала. Изучение основ защиты информации следует начинать уже на этапе подготовки студентов вузов, с последующим повышением квалификации в рамках системы дополнительного профессионального образования.

Предложенные критерии оценки информационной безопасности для организаций медицинского и фармацевтического профиля включают:

1) регулярность обновления антивирусного ПО;
2) наличие структурного подразделения, отвечающего за информационную безопасность, наличие утвержденной СОП в этой области;
3) долю сотрудников, прошедших инструктаж по информационной безопасности;
4) отсутствие зафиксированных нарушений в области защиты информации.

ВЫВОДЫ

В ходе исследования установлено, что регулирование информационной безопасности в здравоохранении прошло последовательные этапы, которые отражают планомерное усиление государственных требований к защите информации. Угрозы информационной безопасности медицинских и фармацевтических организаций подразделяются на внешние и внутренние. Анализ методов защиты информации выявил три взаимодополняющие группы: технические, юридические и организационно-управленческие, при этом применение каждой группы в отдельности не обеспечивает достаточного уровня защиты. Для повышения информационной безопасности в медицинских и фармацевтических организациях предложен комплексный подход, содержащий основные направления и критерии оценки.

Литература

1. Соколова О. В., Исаева И. Ю., Куликова О. А., Алексеева К. С., Кузнецова Е. А. Применение цифровых инструментов в медицинской организации для оптимизации лекарственного обеспечения. Кардиоваскулярная терапия и профилактика. 2024; 23 (S6): 150–151.
2. Соколова О. В., Куликова О. А., Алексеева К. С., Исаева И. Ю. Значимость информационных систем в деятельности аптечной организации. Вопросы обеспечения качества лекарственных средств. 2025; 1 (47): 54–58. DOI 10.34907/JPQAI.2025.63.82.008.
3. Шандора Н. И. Информационная безопасность в сфере здравоохранения. В сборнике: Материалы VI Международной научно-практической конференции, посвященной 25-летию экономического факультета БГУ: Тенденции экономического развития в XXI веке. Минск. 2024; (1): 529–531.
4. Постановление Правительства РФ от 09.02.2022 № 140 «О единой государственной системе в сфере здравоохранения» (вместе с «Положением о единой государственной информационной системе в сфере здравоохранения»).
5. Платонова Н. И., Устиленцев К. А., Устиленцева Т. А. Информационная безопасность в сфере здравоохранения: проблемы и перспективы развития. 2022; 33 (2): 124–136. DOI 10.20410/2073-7815-2022-33-2-124-136.
6. Удальцов К. Р. Кибербезопасность в здравоохранении: стратегии защиты медицинских данных и оборудования. Международный журнал информационных технологий и энергоэффективности. 2024; 9 (5): 18–22.
7. CODE RED 2026 Актуальные киберугрозы российских организаций. Режим доступа: https://ptsecurity.com/research/analytics/russia-cyberthreat-landscape-2026/#id1 (дата обращения: 27.03.2026).
8. Средствами защиты от внутренних информационных угроз оснащены меньше 25% медорганизаций РФ. Режим доступа: https://medvestnik.ru/content/news/sredstvami-zashity-ot-vnutrennih-informacionnyh-ugroz-osnasheny-menshe-25-medorganizacii-rf.html (дата обращения: 27.03.2026).
9. Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации».
10. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
11. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
12. Указ Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».
13. Кочергина М. О., Чугунова С. А. Роль медицинского программного обеспечения в цифровизации здравоохранения. В сборнике: Новые технологии в учебном процессе и производств: Материалы XXIII научно-технической конференции с международным участием, 16–18 апреля 2025 г. Рязань. 2025; 1: 347–350.
14. Соловьев Н. В. Цифровая безопасность в медицине: вызовы и угрозы цифровой трансформации. В сборнике: Материалы международной научно-практической конференции. 20 ноября 2025 г. Волгоград. 2025; 1: 40–44.
15. Лапина М. А., Максимова Е. А., Лапин В. Г., Бойков Н. С. Аналитический обзор методов проектирования систем безопасности в телемедицинских системах. Труды ИСП РАН. 2024;5. Режим доступа: https://cyberleninka.ru/article/n/analiticheskiy-obzor-metodov-proektirovaniya-sistem-bezopasnosti-v-telemeditsinskih-sistemah (дата обращения: 27.03.2026).
16. Дубовсков М. В., Фот Ю. Д. Информационная безопасность в сфере здравоохранения. В сборнике: Актуальные вопросы обеспечения комплексной безопасности: Материалы национальной научно-практической конференции с международным участием, посвященной 35-летию МЧС России и 95-летию Оренбургского ГАУ. 23 мая 2025 г. Оренбург. 2025; 1: 1041–1044.
17. Кодекс Российской Федерации об административных нарушениях от 30.12.2001 № 195-ФЗ.

References

1. Sokolova OV, Isaeva IYu, Kulikova OA, Alekseeva KS, Kuznetsova EA. Application of digital tools in a medical organization for optimization of drug provision. Cardiovascular Therapy and Prevention. 2024; 23 (S6): 150–151. Russian.
2. Sokolova OV, Kulikova OA, Alekseeva KS., Isaeva IYu. The Importance of Information Systems in the Activities of a Pharmacy Organization. Issues of Drug Quality Assurance. 2025; 1 (47): 54–58. DOI 10.34907/JPQAI.2025.63.82.008. Russian.
3. Shandora N. I. Information Security in the Healthcare Sector. In the collection: Proceedings of the 6th International Scientific and Practical Conference dedicated to the 25th Anniversary of the Faculty of Economics at BSU: Trends in Economic Development in the 21st Century, February 28–29, 2024. Minsk. 2024; 529–531.
4. Decree of the Government of the Russian Federation No. 140 dated February 9, 2022. "On the Unified State Healthcare System" (together with the "Regulations on the Unified State Healthcare Information System"). Russian.
5. Platonova NI, Ustilentsev KA, Ustilentseva TA. Information Security in the Healthcare Sector: Challenges and Development Prospects. 2022; 33 (2): 124–136. DOI 10.20410/2073-7815-2022-33-2-124-136. Russian.
6. Udaltsov KR. Cybersecurity in Healthcare: Strategies for Protecting Medical Data and Equipment. International Journal of Information Technology and Energy Efficiency. 2024; 9 (5): 18–22. Russian.
7. CODE RED 2026 Current Cyber Threats to Russian Organizations. Available from URL: https://ptsecurity.com/research/analytics/russia-cyberthreat-landscape-2026/#id1 (accessed: 27.03.2026). Russian.
8. Less than 25% of medical organizations in the Russian Federation are equipped with means of protection against internal information threats. Available from URL: https://medvestnik.ru/content/news/sredstvami-zashity-ot-vnutrennih-informacionnyh-ugroz-osnasheny-menshe-25-medorganizacii-rf.html (accessed: 27.03.2026). Russian.
9. Federal Law No. 323-FZ dated November 21, 2011. "On the Fundamentals of Public Health Care in the Russian Federation". Russian.
10. Federal Law No. 152-FZ dated July 27, 2006. "On Personal Data".
11. Federal Law No. 187-FZ dated July 26, 2017. "On the Security of the Critical Information Infrastructure of the Russian Federation". Russian.
12. Presidential Decree No. 250 dated May 1, 2022. "On Additional Measures to Ensure the Information Security of the Russian Federation." Russian.
13. Kochergina MO, Chugunova SA. The Role of Medical Software in the Digitalization of Healthcare. In the collection: New Technologies in the Educational Process and Production: Materials of the XXIII Scientific and Technical Conference with International Participation. Ryazan. April 16–18, 2025; 347–350. Russian.
14. Solovyov NV. Digital Security in Medicine: Challenges and Threats of Digital Transformation. In the collection: Materials of the International Scientific and Practical Conference. Volgograd. November 20, 2025; 40–44. Russian.
15. Lapina MA., Maksimova EA, Lapin VG, Boykov NS. Analytical review of methods for designing security systems in telemedicine systems. Proceedings of ISP RAS. 2024; 5. Available from URL: https://cyberleninka.ru/article/n/analiticheskiy-obzor-metodov-proektirovaniya-sistem-bezopasnosti-v-telemeditsinskih-sistemah (accessed: 27.03.2026). Russian.
16. Dubovskov MV, Fot Yu D. Information Security in the Healthcare Sector. In the collection: Current Issues in Ensuring Comprehensive Security: Proceedings of the National Scientific and Practical Conference with International Participation Dedicated to the 35th Anniversary of the Russian Ministry of Emergency Situations and the 95th Anniversary of the Orenburg State Agrarian University. Orenburg. May 23, 2025; 1041–1044. Russian.
17. Code of Administrative Offenses of the Russian Federation dated 30.12.2001 No. 195-FZ. Russian.