УДК 004

Карпун Дмитрий Алексеевич

магистрант

1 курс, факультет «Информатика и вычислительная техника»

Донской государственный технический университет

Россия, г. Ростов-на-Дону

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СРЕДЕ МЕДИЦИНСКОЙ ОРГАНИЗАЦИИ

Аннотация. *В данной работе рассматриваются актуальные вопросы обеспечения информационной безопасности в специфических условиях современной медицинской организации. В условиях активной цифровизации здравоохранения и перехода на электронные медицинские карты, защита конфиденциальных данных пациентов и обеспечение отказоустойчивости информационных систем становятся критически важными задачами.*

Ключевые слова: *информационная безопасность, медицинская организация, персональные данные, защита информации, электронная медицинская карта, киберугрозы в медицине.*

Abstract. *This paper examines current issues of information security in the specific conditions of a modern medical organization. With the rapid digitalization of healthcare and the transition to electronic medical records, protecting confidential patient data and ensuring the resilience of information systems are becoming critically important.*

Keywords: *information security, medical organization, personal data, information protection, electronic medical records, cyber threats in medicine.*

Введение

Цифровая трансформация российского здравоохранения — процесс необратимый и динамичный. Единая государственная информационная система (ЕГИСЗ), медицинские информационные системы (МИС) в поликлиниках и больницах, телемедицина и мобильные приложения — все эти инструменты призваны сделать медицинскую помощь более доступной и эффективной. Однако вместе с удобствами информационная среда медицинских организаций порождает серьезные риски. Данные пациентов относятся к специальным категориям персональных данных и имеют высокую

стоимость на теневом рынке. Цель данной работы — комплексный анализ состояния информационной безопасности в российских медицинских организациях, включающий нормативно-правовую базу, ключевые угрозы, реальные инциденты, практические меры защиты и перспективы развития этой сферы.

Нормативно-правовая база информационной безопасности в здравоохранении РФ

Обеспечение информационной безопасности (ИБ) медицинских организаций в России регулируется многоуровневой системой нормативно-правовых актов. На вершине этой системы находятся федеральные законы, устанавливающие общие правила и требования.

Федеральный закон «О персональных данных» №152-ФЗ — фундаментальный акт, определяющий основные принципы обработки ПД. В соответствии с его требованиями при сборе ПД организации обязаны обеспечить запись, систематизацию, накопление и хранение персональных данных граждан РФ с использованием баз данных, находящихся на территории России. Для медицинских организаций это требование имеет особое значение, поскольку они работают со специальной категорией ПД, требующей повышенного уровня защиты.

Для сферы здравоохранения ключевым законом является **Федеральный закон №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (КИИ)**. Этот закон распространяется на все медицинские организации, за исключением частных кабинетов — индивидуальных предпринимателей. В рамках исполнения требований закона медицинские организации обязаны присвоить своим информационным системам категории значимости с учетом их подверженности взлому и потенциальным рискам для пациентов. Категорирование информационных систем позволяет определить необходимый уровень защиты и объем мер безопасности для каждой системы.

Важным подзаконным актом является **Приказ Минздрава России №911н от 24 декабря 2018 года**, который утверждает требования к государственным информационным системам в сфере здравоохранения субъектов РФ, медицинским информационным системам медицинских организаций и информационным системам фармацевтических организаций. Данный приказ устанавливает минимальные требования к защите информации при использовании медицинских информационных систем, включая организационные и технические меры.

В апреле 2025 года был принят **Федеральный закон №58-ФЗ**, который обновил требования к субъектам КИИ, в число которых входят все медицинские организации. Закон закрепил необходимость использования на значимых объектах КИИ только того программного обеспечения, которое входит в единый реестр российских программ. Кроме того, все клиники обязали подключиться к государственной системе защиты от кибератак, что является важным шагом в создании единого защищенного информационного пространства в здравоохранении.

Таким образом, нормативно-правовая база в сфере информационной безопасности медицинских организаций в России сформирована достаточно полно и постоянно совершенствуется с учетом актуальных вызовов и угроз. Наличие четких требований и законодательных актов создает основу для построения эффективной системы защиты информации.

Текущее состояние информационной безопасности в медицинских организациях РФ: статистика и анализ

Несмотря на развитую нормативную базу, реальное положение дел с информационной безопасностью в российских медицинских организациях вызывает серьезную обеспокоенность. Статистические данные за 2024–2025 годы демонстрируют тревожную картину.

По данным InfoWatch, по итогам первого полугодия 2025 года Россия сохранила **второе место в мире по количеству утечек данных из медицинских организаций**, увеличив долю до 8,1% против 4,1% в

аналогичный период 2024 года. Лидером по-прежнему остаются США (55,8%), за Россией следуют Индия (4,1%), Австралия (3,5%) и Аргентина (2,9%). Всего за январь-июнь 2025 года в стране зафиксировано 14 крупных инцидентов, связанных с кражей и потерей данных из учреждений здравоохранения — это на 12,5% меньше, чем годом ранее, но **на 16,7% больше, чем во втором полугодии 2024 года** (для сравнения: во II полугодии 2024 г. было 12 инцидентов). Таким образом, темпы роста числа утечек ускоряются, что свидетельствует об обострении проблемы.

Настораживает и **качественный состав** утекших данных. Согласно отчету InfoWatch, 100% утечек включали персональные данные пациентов, что является критически важной информацией. При этом доля утечек аутентификационных сведений (логинов, паролей и иных данных доступа) выросла с 27,2% до 33,3%. В InfoWatch подчеркивают, что рост числа утечек аутентификационной информации «вселяет тревогу за состояние защиты данных». Такие данные позволяют злоумышленникам не только получить доступ к конфиденциальной информации, но и скомпрометировать целые информационные системы, что может привести к каскадным последствиям для всей медицинской организации.

Говоря о мотивации атакующих, следует особо подчеркнуть, что **кража данных становится основной целью**. По данным исследования компании «Информзащита», в 37% случаев именно кража данных является главной целью злоумышленников — этот показатель значительно превышает другие мотивы. Еще в 33% атак основной мотив связан с вымогательством, а остальные случаи приходится на промышленный и государственный шпионаж. Важно отметить, что даже если изначально злоумышленники преследовали иные цели, большинство успешных атак всё равно приводит к утечке или потере контроля над корпоративной информацией.

Аналитики обращают внимание на то, что сегмент здравоохранения в России входит в число главных целей кибератак, причем **на долю медицинских организаций приходится около 15% всех инцидентов** в

стране. Это свидетельствует о высокой концентрации угроз именно в этой отрасли. Особую тревогу вызывает тот факт, что согласно исследованию «Лаборатории Касперского», в 2024 году здравоохранение стало отраслью, наиболее зараженной вредоносными программами, обогнав даже госсектор — каждая четвертая компания, имеющая вирусы и шпионские программы, работает именно в медицинской сфере.

Наконец, важным аспектом является **экономический ущерб** от утечек медицинских данных. По данным исследования аналитической компании Kept, объем рынка медицинских данных в РФ уже почти достиг 4,2 млрд рублей. При этом 90% сделок по покупке медицинских данных приходится на фармацевтические компании, а также ими интересуются страховые службы, разработчики нейросетей и промышленные предприятия. Однако значительная часть этого рынка находится в «серой зоне», что создает дополнительные стимулы для нелегального оборота медицинской информации.

Таким образом, текущее состояние информационной безопасности в российских медицинских организациях характеризуется высоким уровнем угроз, растущим числом инцидентов и значительным объемом утечек конфиденциальных данных.

Основные угрозы информационной безопасности в медицинских организациях

Комплексный анализ ситуации позволяет выделить несколько основных категорий угроз, с которыми сталкиваются медицинские организации в России. Каждая из этих угроз имеет свои особенности и требует специфических мер противодействия.

Внешние кибератаки. Внешние злоумышленники представляют наиболее масштабную угрозу. По данным экспертов, за 2025 год каждая медицинская организация в России подвергалась в среднем более 3 миллионов попыток взлома. Количество попыток взлома систем продолжает расти, что создает высокую нагрузку на системы защиты. В августе 2025 года число

кибератак на компании из сферы здравоохранения России выросло на треть по сравнению с прошлым годом, особенно затронув клиники и аптеки.

В третьем квартале 2025 года специалисты зафиксировали волну целевых вредоносных рассылок, организованных через почтовые системы: на российские медицинские учреждения приходили письма от имени известных страховых компаний и больниц. Эти рассылки содержали вредоносные вложения с троянами, причем письма были подделаны настолько качественно, что обманывали даже опытных сотрудников.

Внутренние угрозы со стороны персонала. Исследование, проведенное компанией «СёрчИнформ» в 2025 году, показало, что с утечками данных по вине сотрудников сталкивались 38% медицинских организаций. Причем в 84% случаев нарушения допускались неумышленно, что свидетельствует о низком уровне цифровой грамотности медицинского персонала.

Основными каналами, через которые сотрудники организаций здравоохранения сливали информацию, в 2025 году были: мессенджеры (62%), почта (41%) и различные устройства хранения (29%). При этом самым распространенным типом утекающих данных стали персональные данные пациентов и служебная документация.

Крайне тревожным является тот факт, что только четверть медицинских организаций оснащены средствами защиты от внутренних информационных угроз. Такое положение дел создает серьезные риски для конфиденциальности пациентских данных, поскольку внутренние нарушители могут действовать целенаправленно, имея легитимный доступ к информационным системам.

Ботовые атаки и автоматизированные угрозы. В первом полугодии 2025 года число значимых ботовых атак на компании из сектора медицинских технологий в России увеличилось на 26% по сравнению с аналогичным периодом прошлого года и достигло 339 тысяч инцидентов. Самой уязвимой категорией стали онлайн-лаборатории, на которые пришлось 60% всех

зафиксированных ботовых атак, 25% атак пришлось на телемедицинские платформы, и 15% — на мобильные приложения клиник.

Ботовые атаки представляют особую опасность тем, что они имитируют действия реальных пользователей — вход в личный кабинет, запись к врачу, регистрацию на сайте. Такие атаки сложнее обнаружить, поскольку трафик выглядит нормальным. Их последствия могут быть весьма серьезными: от утечки персональных данных до блокировки реальным пациентам возможности записаться к врачу из-за автоматизированных регистраций ботами и роста расходов на связь при попытках защитить доступ к личным кабинетам.

Угрозы, связанные с использованием мобильных приложений. В эпоху цифровизации здравохранения все больше пациентов пользуются мобильными приложениями для записи к врачу, получения результатов анализов и телемедицинских консультаций. Однако, согласно совместному исследованию Центра цифровой экспертизы Роскачества и группы компаний «Солар», онлайн-аптеки и медицинские приложения оказались среди самых уязвимых к утечкам категорий мобильных сервисов. Проверка 14 популярных приложений с совокупной аудиторией более 26 млн пользователей выявила уязвимости, позволяющие перехватывать трафик и получать доступ к персональным и финансовым данным.

Меры и средства обеспечения информационной безопасности

Действующее законодательство и регуляторные требования определяют комплекс мер, которые должны реализовывать медицинские организации для обеспечения информационной безопасности.

Организационные меры. Категорирование информационных систем медицинской организации является ключевым организационным мероприятием. В учреждении должна быть создана специальная комиссия по категорированию, в состав которой входит главный врач, заместитель по кибербезопасности и другие сотрудники. Состав комиссии, порядок ее работы, сбора и хранения документов должны быть оформлены локальным актом.

Важным является разработка и утверждение политики в отношении обработки персональных данных. В соответствии с требованиями Федерального закона №152-ФЗ, оператор персональных данных обязан опубликовать документ, определяющий его политику в отношении обработки ПД, к сведениям о реализуемых требованиях к защите ПД. Политика оператора — это документ, в котором раскрываются концептуальные основы, принципы обеспечения безопасности ПД субъектов.

Технические меры защиты. Субъектам КИИ с 2025 года запрещено использовать импортные средства защиты информации (СЗИ). Переход на российское системное и прикладное ПО часто требует внедрения новых или обновления имеющихся средств ИБ. Это требование направлено на обеспечение технологического суверенитета в критически важной сфере здравоохранения.

Медицинские организации всех форм собственности должны использовать средства антивирусной защиты, межсетевые экраны и системы обнаружения вторжений. Многофакторная аутентификация становится обязательным требованием для доступа к критически важным информационным системам, особенно с учетом роста числа атак на парольную защиту.

Меры по защите от внутренних угроз. Учитывая, что 38% медицинских организаций сталкиваются с утечками по вине собственного персонала, особое значение приобретают меры по минимизации внутренних рисков. К ним относятся: разграничение доступа к данным по принципу минимальной необходимости, мониторинг действий пользователей в информационных системах, применение DLP-систем, способных фиксировать подозрительные операции с конфиденциальными данными, контроль передачи данных через съемные носители, электронную почту и мессенджеры.

Меры по повышению квалификации персонала. В 84% случаев нарушения информационной безопасности в медицинских организациях совершаются неумышленно. Поэтому регулярное обучение персонала

правилам работы с конфиденциальной информацией, проведение тренингов по выявлению фишинговых писем и других социально-инженерных атак становится критически важным направлением работы.

Перспективы развития и рекомендации

Дальнейшее развитие информационной безопасности в российских медицинских организациях должно идти по нескольким ключевым направлениям.

Во-первых, необходимо **дальнейшее совершенствование нормативной базы** с учетом специфики медицинской отрасли. Минздрав России в 2024 году разработал и согласовал с ФСТЭК перечень типовых систем, которые должны категорироваться. В этот перечень вошли ЕГИСЗ, медицинские информационные системы организаций, программное обеспечение клинико-диагностических лабораторий, аппаратов для лучевой терапии, анестезии и хирургии, а также системы для телемедицины. На полную реализацию этих нормативных требований потребуется время, однако их внедрение должно повысить уровень защищенности критической информационной инфраструктуры здравоохранения на системном уровне.

Во-вторых, **планомерный переход на отечественное программное и аппаратное обеспечение** должен сопровождаться обеспечением соответствующего уровня защищенности. Особое внимание следует уделять совместимости различных информационных систем, чтобы меры безопасности не приводили к снижению доступности и качества медицинской помощи.

В-третьих, **развитие государственной системы обнаружения и предотвращения кибератак в сфере здравоохранения**. Все клиники обязаны подключиться к государственной системе защиты от кибератак. Эта мера позволит создать единое защищенное пространство, оперативно выявлять угрозы и координировать действия по их отражению на межорганизационном уровне.

В-четвертых, **усиление работы по повышению цифровой грамотности медицинского персонала**. Каждый медицинский работник должен понимать ценность и конфиденциальность данных, с которыми он работает, а также возможные последствия их утечки. Регулярное обучение должно стать неотъемлемой частью профессиональной деятельности.

В-пятых, **создание эффективной системы мониторинга и реагирования на инциденты**. Медицинские организации должны иметь четкие регламенты действий при обнаружении инцидента, назначенных ответственных лиц и налаженные каналы взаимодействия с государственными органами.

И наконец, критически важным является **адекватное финансирование мероприятий по информационной безопасности**. Как показал опрос, 26% медицинских организаций в 2025 году сократили бюджеты на ИБ, и лишь 23% увеличили. Без должного финансирования невозможно обеспечить требуемый уровень защищенности информационных систем. По прогнозам экспертов, в 2026 году ИБ-бюджеты в сфере здравоохранения продолжат расти, но темпы этого роста должны ускориться.

В перспективе ожидается дальнейшая консолидация усилий государства и бизнеса по защите медицинских данных, внедрение систем на основе искусственного интеллекта для обнаружения аномалий и предиктивной аналитики угроз, а также стандартизация требований к информационной безопасности для всех типов медицинских организаций.

Заключение

Проведенный анализ позволяет сделать ряд итоговых выводов. Информационная безопасность в медицинских организациях России находится на переломном этапе своего развития. С одной стороны, цифровая трансформация здравоохранения открывает новые возможности для повышения качества и доступности медицинской помощи. С другой стороны, она создает серьезные риски, которые уже реализуются в виде множества инцидентов и утечек конфиденциальных данных.

Ключевыми угрозами являются массированные внешние кибератаки, активные действия APT-группировок, ботовые атаки на телемедицинские и лабораторные сервисы, а также внутренние инциденты, связанные с недостаточной квалификацией или злонамеренными действиями персонала. Нормативно-правовая база в этой сфере достаточно развита и продолжает совершенствоваться, однако ее реализация на практике сталкивается с серьезными вызовами — от недостатка финансирования до кадрового голода.

Учитывая, что Россия занимает второе место в мире по числу утечек медицинских данных, а объем теневого рынка этих данных приближается к 4,2 млрд рублей, проблему информационной безопасности в здравоохранении необходимо считать не просто технологической, но и социально значимой. Каждая утечка медицинских данных — это не просто статистическая единица, это реальная угроза приватности и благополучию конкретных людей.

Перспективы развития информационной безопасности в медицинских организациях связаны с дальнейшей консолидацией усилий регуляторов, развитием технологической базы и повышением культуры информационной безопасности среди медицинского персонала. Только комплексный подход, сочетающий совершенствование нормативной базы, внедрение современных технических средств защиты, систематическое обучение персонала и адекватное финансирование, способен обеспечить надежную защиту пациентских данных в эпоху цифровой медицины.

Информационная безопасность в медицинских организациях — это не просто соблюдение формальных требований законодательства. Это вопрос доверия пациентов к системе здравоохранения, вопрос качества оказания медицинской помощи и вопрос стратегической безопасности государства в цифровую эпоху. От того, насколько успешно российское здравоохранение справится с этими вызовами, зависит будущее цифровой медицины в стране.

Использованные источники:

1. Указ Президента РФ от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации».
2. Постановление Правительства РФ от 02.03.2026 № 398-р «Об утверждении стратегического направления в области цифровой трансформации обрабатывающих отраслей промышленности».
3. Постановление Правительства РФ от 01.03.2026 № 1667 «О мерах по обеспечению устойчивого функционирования информационно-телекоммуникационных сетей и суверенного интернета».
4. Приказ ФСТЭК России от 11.02.2014 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных...» (в актуальной редакции 2025-2026 гг.).
5. Единый реестр российской радиоэлектронной продукции (ПП РФ № 878) — как основной источник для выбора оборудования.
6. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. — 6-е изд. — СПб.: Питер, 2023. — 1008 с. (Базовая база по стеку TCP/IP и Ethernet).
7. Кучерявый А. Е. Сети связи следующего поколения. — М.: Медиа Паблишер, 2024. (Перспективные технологии, актуальные для РФ).
8. Таненбаум Э., Уэзеролл Д. Компьютерные сети. — 6-е изд. — СПб.: Питер, 2022.

Информация о себе: grimjoy88@yandex.ru