

УДК: 61, 57.016.3, 355.343.18

ОТВЕТСТВЕННОСТЬ ЗА УТЕЧКИ МЕДИЦИНСКИХ ДАННЫХ: ПРАВОВЫЕ ПОСЛЕДСТВИЯ И СПОСОБЫ МИНИМИЗАЦИИ РИСКОВ

Абилкайрова Милана Бахтжановна¹,

Ртищева Юлия Борисовна¹

Саляхова Лилия Якуповна¹

к.м.н, доцент

¹Казанский институт (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Все-российский государственный университет юстиции (РПА Минюста России)»

Аннотация. В представленной статье рассматривается насущная проблема ответственности, возникающей при несанкционированном раскрытии медицинских сведений в контексте современной цифровизации сферы здравоохранения. Исследуются юридические последствия, наступающие при нарушении принципов конфиденциальности медицинской информации, и предлагаются стратегии для снижения соответствующих рисков. Основная цель исследования – всесторонний анализ существующих механизмов привлечения к ответственности за нарушение врачебной тайны и разработка рекомендаций, направленных на предотвращение утечек медицинских данных. Методология исследования включает в себя изучение нормативно-правовой базы, анализ судебной практики, а также исследование современных методов защиты информации.

Ключевые слова: здравоохранение, цифровизация, медицинские данные, врачебная тайна, ответственность.

LIABILITY FOR MEDICAL DATA LEAKS: LEGAL CONSEQUENCES AND RISK MITIGATION

Abilkayrova Milana Bakhtzhanovna¹,

Rtishcheva Julia Borisovna¹

Liliya Yakupovna Salyakhova

Cand. Sc. (Medicine), Associate Professor

¹Kazan Institute (branch) of the Federal State Budgetary Educational Institution of Higher Education “All-Russian State University of Justice (RPA of the Ministry of Justice of Russia)”

Abstract. This article addresses the pressing issue of liability arising from the unauthorized disclosure of medical information in the context of

modern digitalization in the healthcare sector. It explores the legal consequences of violating the principles of medical information confidentiality and proposes strategies to mitigate these risks. The primary objective of this research is to provide a comprehensive analysis of existing mechanisms for prosecuting violations of medical confidentiality and to develop recommendations for preventing medical data breaches. The research methodology involves examining the legal framework, analyzing court cases, and exploring current methods of information protection.

Keywords: *healthcare, digitalization, medical data, medical confidentiality, and responsibility.*

Введение. Обеспечение информационной безопасности в медицинской сфере становится приоритетным направлением развития, поскольку утечка конфиденциальных данных может иметь серьезные последствия как для пациентов, так и для медицинских учреждений.

В России проблема утечек медицинских данных обусловлена сочетанием нескольких факторов: уязвимостью устаревшей ИТ-инфраструктуры, человеческим фактором и масштабной цифровизацией здравоохранения, что привлекает внимание киберпреступников. Публикация баз данных с медицинской и персональной информацией в последние годы вызвала широкий общественный резонанс: для многих учреждений демонстрация масштабов уязвимости стала стимулом для пересмотра подходов к обеспечению информационной безопасности. Утечка медицинской информации может привести к серьезным последствиям: дискриминации пациентов, шантажу, финансовым потерям и репутационному ущербу.

Научная значимость данной работы определяется необходимостью системного подхода к проблеме защиты медицинских данных и разработки эффективных механизмов предотвращения утечек информации. Результаты исследования могут быть использованы как в практической деятельности медицинских организаций, так и в научных исследованиях по совершенствованию законодательства в области информационной безопасности.

Методы. В соответствии с положениями Федерального закона № 323-ФЗ от 21.11.2011 “Об основах охраны здоровья граждан в Российской Федерации” и Федерального закона № 152-ФЗ от 27.07.2006 “О персональных данных”, утечка медицинских данных

определяется как незаконный доступ, передача или разглашение информации о факте обращения гражданина за медицинской помощью, о состоянии его здоровья и диагнозе, а также других сведений, полученных в ходе медицинского обследования и лечения. Одним из основных способов обеспечения права каждого человека на неприкосновенность частной жизни является запрет на разглашение информации, составляющей врачебную тайну, которая охраняется бессрочно, может быть раскрыта другим лицам, в том числе должностным, например, для проведения специальных обследований и лечения пациентов, а также в процессе осуществления научной или учебной деятельности, но только при условии предварительного согласия пациента или его законного представителя.

Серьёзной проблемой остаётся баланс между необходимостью обмена данными и сохранением конфиденциальности информации между медицинскими организациями для оказания качественной помощи при передаче пациента в рамках трехуровневой модели оказания медицинской помощи. Человеческий фактор остается одним из основных источников нарушений. Небрежность сотрудников, оставление документов без надзора, обсуждение пациентов в общественных местах – все это может привести к разглашению конфиденциальной информации. Цифровизация медицины, приносящая множество преимуществ, одновременно увеличивает риски кибератак и утечек данных из электронных медицинских систем.

Результаты. Компрометация данных пациентов может приводить к волнам мошенничества, шантажа и другим негативным последствиям. Экспертно-аналитический центр InfoWatch (ЭАЦ) подготовил обзор утечек информации в сфере здравоохранения за 2024 год. На долю отрасли здравоохранения приходится 6,5% от общего числа утечек конфиденциальной информации в мире. В 2024 году ЭАЦ зафиксировал 601 утечку из медицинских организаций по всему миру. Это на 36,3% меньше, чем в 2023 году. Количество утекших из медицинских учреждений записей персональных данных в 2024 году составило 341 млн, что на 28,7% меньше, чем в 2023 году. Около 92% всех зарегистрированных утечек из медицинских организаций в 2024 году произошли в результате действий хакеров и других внешних злоумышленников.

Экспертно-аналитический центр InfoWatch провел исследование «Утечки конфиденциальных данных из медицинских организаций. Мир – Россия, I полугодие 2025 года». Исследование показало, что количество таких проблем в РФ увеличилось на 16,7% по сравнению со второй половиной 2024 года. За первые шесть месяцев текущего года в стране было официально зарегистрировано 14 крупных инцидентов, связанных с кражей данных из клиник, что составляет 8,1% от всех подобных случаев в мире. С этим показателем Россия заняла второе место в глобальном антирейтинге, уступив США (где было зафиксировано 55,8% случаев утечек).

За первые шесть месяцев 2025 года в разных странах утекло 58,4 млн записей с персональными данными, а в России – более 3 млн. В InfoWatch уточнили, что причиной каждого пятого инцидента (21,4%) в российских медицинских организациях стали действия внутренних нарушителей, что на 2,3% выше, чем в среднем по миру. Как правило, такие злоумышленники похищают данные “точечно и на заказ”, поэтому речь идет о небольшом количестве записей персональных данных. В России вдвое чаще стали утекать коммерческие секреты клиник и лабораторий, а утечки платежной информации, наоборот, сократились. Однако темпы роста числа утечек данных медицинских организаций в России в 2025 году все же ускорились. Так, в одной из районных больниц Республики Татарстан в 2025 г. произошла утечка данных пациентов, по данным расследования, их выставили на продажу в “даркнете”.

Российское законодательство предусматривает несколько видов ответственности за нарушение врачебной тайны: административная ответственность регламентируется статьей 13.14 КоАП РФ в виде штрафа; уголовная ответственность наступает по статье 137 УК РФ за незаконное собирание или распространение сведений о частной жизни лица без его согласия, предусматривает штраф от 100 до 300 тысяч рублей, принудительные работы на срок до четырех лет, арест на срок до шести месяцев, лишение свободы на срок до четырех лет с лишением права занимать определенные должности на срок от двух до пяти лет; гражданско-правовая ответственность, которая предусматривает возможность взыскания компенсации морального вреда через суд.

Обсуждение. Особое значение приобретает превентивная работа по предотвращению утечек данных: формирование культуры ин-

формационной безопасности в медорганизациях, регулярное обучение и повышение осведомленности персонала о последствиях нарушений.

Эффективная защита медицинских данных требует внедрения в медорганизациях: 1) организационных мер: разработка и внедрение политики обработки персональных данных; определение ответственных за безопасность персональных данных; обучение сотрудников правилам работы с медицинской информацией; регламентирование доступа к медицинским данным (кто, к какой информации имеет доступ и на каких условиях) и т. д.; 2) технических мер: использование надежных средств защиты информации (антивирусы, файерволы, системы обнаружения вторжений); шифрование данных при хранении и передаче; регулярное обновление программного обеспечения; использование надежных паролей и многофакторной аутентификации; обеспечение физической безопасности серверов и рабочих мест; внедрение систем аудита и мониторинга действий пользователей; использование безопасных каналов связи для передачи данных; удаление или обезличивание данных, когда они больше не требуются; 3) юридических мер: регулярный аудит соответствия требованиям законодательства в области защиты персональных данных; актуализация локальных нормативных актов; консультирование с юристами по вопросам защиты персональных данных.

Таким образом, в современных условиях необходимо продолжать совершенствование комплексных механизмов защиты медицинских данных, развивать технологии безопасности и укреплять правовую базу.

Список литературы

1. Федеральный закон от 21.11.2011 №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» (ред. от 23.07.2025) // Собрание законодательства РФ, 28.11.2011, №48, ст. 6724.
2. Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных» (ред. от 24.06.2025) // Собрание законодательства РФ, 31.07.2006, №31 (часть I), ст. 3451.
3. Гукемухов Р.М. Сохранность медицинских данных // Наука и Просвещение. 2023. 309–311 с. URL: <https://www.elibrary.ru/item.asp?id=55174871> (дата обращения: 29.11.2025).
4. Исафилов Анар КИБЕРБЕЗОПАСНОСТЬ В МЕДИЦИНЕ: ЗАЩИТА ЭЛЕКТРОННЫХ МЕДИЦИНСКИХ ДАННЫХ // Холодная наука. 2024. №6. URL: <https://cyberleninka.ru/article/n/kiberbezopasnost->

v-meditsine-zaschita-elektronnyh-meditsinskih-dannyh (дата обращения: 30.11.2025).

5. Горбунов Н.А. Уязвимости безопасности информации медицинских информационных систем / Н. А. Горбунов // Международный научно-исследовательский журнал. – 2025. – №5 (155). – URL: <https://research-journal.org/archive/5-155-2025-may/10.60797/IRJ.2025.155.102> (дата обращения: 30.11.2025).

