АНАЛИЗ ТРЕБОВАНИЙ К КОНФИДЕНЦИАЛЬНОСТИ И ОБМЕНУ ДАННЫМИ ЦИФРОВОГО ЗДРАВООХРАНЕНИЯ

А. К. Алзубаиди ✉

Елецкий государственный университет им. И. А. Бунина, Елец, Россия

Статья отвечает на насущные вопросы, связанные с государственным регулированием конфиденциальности информации и обмена данных в эпоху цифрового здравоохранения. Институт врачебной тайны, зародившийся в Древнем мире, продолжает эволюционировать на протяжении всего развития медицинского права. Однако в наше время, в эпоху глобальной цифровизации, вопросы, связанные с конфиденциальностью информации, стали более актуальными, чем когда-либо. С развитием современных технологий и цифровых платформ здравоохранения возникают новые вызовы в области защиты данных пациентов. Врачи и медицинские учреждения сталкиваются с необходимостью соблюдения стандартов безопасности данных, чтобы обеспечить надежную защиту личной и медицинской информации пациентов. С увеличением объема электронных медицинских записей и цифровых обменов данными становится жизненно важным разработать эффективные стратегии и механизмы для предотвращения несанкционированного доступа и утечек информации. Одним из ключевых аспектов в этой области является установление строгих нормативов и законов, которые регулируют сбор, хранение и передачу медицинских данных. В Российской Федерации активно работают над созданием законодательства, которое защищало бы права пациентов и обязывало медицинские учреждения соблюдать высокие стандарты конфиденциальности, а также разработать технические средства, которые обеспечивают шифрование данных и защиту от хакерских атак.

Ключевые слова: врачебная тайна, закон, этика, раскрытие данных, вопросы защиты, медицина, пациент, эксперт, цифровое здравоохранение, государственный контроль, цифровые права, защита персональных данных, информационная безопасность, электронные госуслуги

✉ **Для корреспонденции:** Азхар Кхудхаир Алзубаиди
ул. Коммунаров, д. 10А, г. Елец, Россия; azhrstar90@gmail.com

Статья поступила: 14.10.2023 **Статья принята к печати:** 25.11.2023 **Опубликована онлайн:** 05.12.2023

DOI: 10.24075/medet.2023.030

ANALYSIS OF REQUIREMENTS FOR CONFIDENTIALITY AND EXCHANGE OF DIGITAL HEALTH DATA

Alzubaidi AK ✉

Yelets State University named after Bunin IA, Yelets, Russia

The article provides answers to immediate questions associated with the state regulation of confidentiality of information and exchange of data in the era of digital healthcare. The institute of medical confidentiality which originated in the ancient world is still evolving throughout the development of medical law. In the current era of global digitalization, however, the issues related to data confidentiality have become more relevant than ever. With all the modern technologies and digital health care platforms on the rise, new challenges associated with protection of these patients are emerging. To ensure the reliable protection of patient's personal and medical information, doctors and medical institutions have to meet data security standards. It becomes vital to develop effective strategies and mechanisms to prevent unauthorized access and data leakage due to a larger volume of electronic medical records and digital data exchange. Strict rules and standards regulating collection, storage and transfer of medical data belong to a key aspect in this area. The Russian Federation is making great efforts to create the legislation which could protect the rights of patients and made medical establishments to follow the high standards of confidentiality, and to develop technical aids that provide data encryption and protection against hacker attacks.

Keywords: medical secrecy, law, ethics, data disclosure, protection issues, medicine, patient, expert, digital health care, state control, digital rights, personal data protection, digital security, online state services

✉ **Correspondence should be addressed:** Azkhar K. Alzubaidi
Kommunarov Str., 10A, Yelets, Russia; azhrstar90@gmail.com

Received: 14.10.2023 **Accepted:** 25.11.2023 **Published online:** 05.12.2023

DOI: 10.24075/medet.2023.030

На сегодняшний день мы наблюдаем стремительное развитие цифровых медицинских сервисов, которые осуществляют анализ результатов обследований на основе обширных данных. В связи с этим вопрос о врачебной тайне и конфиденциальности информации остается крайне актуальным.

С одной стороны, врачебная тайна защищается государством через установление запретов и механизмов защиты. С другой стороны, на этот вопрос влияет этическая сторона, которая регулируется специальными нормами медицинского права, как отмечает Александра Дронова, статс-секретарь и заместитель Министра здравоохранения Российской Федерации. «С развитием информационных технологий обеспечение врачебной тайны в процессе обработки и защиты информации, собранной от пациентов, становится чрезвычайно важным», — подчеркивает эксперт. Обработка такой информации сопряжена с рисками ее раскрытия, поэтому вопросы надежной защиты данных стоят на новом уровне [1].

Согласно Федеральному закону от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» [2], врачебная тайна охватывает разнообразные сведения, включая информацию о факте обращения гражданина за медицинской помощью, его состоянии здоровья, диагнозе и данных, полученных в процессе медицинского обследования и лечения [3]. Закон строго запрещает раскрытие этих данных лицам, которые стали их обладателями, за исключением случаев, предусмотренных законодательством [4].

Во-первых, при наличии письменного согласия гражданина (или его законного представителя) возможна передача сведений, составляющих врачебную тайну, другим гражданам и должностным лицам для проведения медицинского обследования, лечения и связанных процедур [5].

Во-вторых, в случае отсутствия письменного согласия допускаются следующие случаи (ч. 4 ст. 13 Закона № 323-ФЗ) [2]:

- в целях проведения медицинского обследования и лечения гражданина, который в результате своего состояния не способен выразить свою волю;
- при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;
- по запросу государственных органов в определенных законом случаях — например, по запросу органов дознания и следствия, суда в связи с проведением расследования или судебным разбирательством;
- в целях контроля за исполнением лицами, признанными больными наркоманией, возложенной на них при назначении административного наказания судом обязанности пройти лечение от наркомании;
- в случае оказания медицинской помощи несовершеннолетнему;
- в целях информирования органов внутренних дел в определенных случаях — например, о поступлении пациента, в отношении которого имеются достаточные основания полагать, что вред его здоровью причинен в результате противоправных действий;
- для проведения военно-врачебной экспертизы;
- для расследования несчастного случая на производстве и профессионального заболевания;
- при обмене информацией медицинскими организациями;
- для осуществления учета и контроля в системе обязательного социального страхования;
- для осуществления контроля качества и безопасности медицинской деятельности.

Эти строгие ограничения предназначены для обеспечения надежной защиты врачебной тайны и конфиденциальности пациентов в Российской Федерации. Термин «врачебная тайна» не отражает полный круг лиц, которые должны эту тайну соблюдать, — она относится не только к врачам, но и ко всему персоналу медицинского учреждения, куда обратился пациент, а также к любым людям, которым такие сведения стали доступны (например, фармацевты или юристы). Врачебная тайна включает не только медицинскую информацию, характеризующую состояние здоровья пациента, но и другие данные, такие как информация о местонахождении пациента, факт обращения за медицинской помощью, госпитализация, проведение обследований и т.д. [6, 7].

Эта концепция подчеркивает, что соблюдение врачебной тайны является обязанностью для всех, кто имеет доступ к медицинской информации пациентов, и несет важное значение для поддержания доверия пациентов к медицинской системе.

Законодательством Российской Федерации, а именно Основами законодательства о здоровье граждан от 22.07.93 № 5488-1 (Постановление № 5488-1), устанавливаются права граждан на сохранение конфиденциальности информации о том, что они обратились за медицинской помощью, и других сведениях, предоставляемых им при обращении за медицинской помощью. Эти права включают в себя требование информированного и добровольного согласия на медицинское вмешательство и право отказа от него. Подобные нормы и правила обращения с медицинской информацией также регулируются «Этическим кодексом российского врача» (Кодекс, 1994) [8].

Согласно статье 30 «Права пациента» Основ, при обращении за медицинской помощью и ее получении пациент имеет право на сохранение конфиденциальности информации о своем обращении за медицинской помощью, своем состоянии здоровья, поставленном диагнозе и других данных, полученных в процессе обследования и лечения, согласно статье 61 Основ. Кроме того, у него есть право выбирать лиц, которым можно разрешить доступ к информации о его состоянии здоровья (пункт 6.9 статьи 30) [8].

Статья 31 «Права граждан на информацию о состоянии здоровья» утверждает, что информация, содержащаяся в медицинских документах гражданина, является врачебной тайной и может быть раскрыта без согласия гражданина только в определенных случаях, предусмотренных статьей 61 Основ. Также гарантируется право каждого гражданина получить информацию о своем состоянии здоровья в удобной для него форме, включая сведения о результатах обследования, наличии заболевания, прогнозе, методах лечения, связанных рисках, возможных вмешательствах и их последствиях, а также результатах лечения [8].

Согласно статье 61 «Врачебная тайна», информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе и другие сведения, полученные при его обследовании и лечении, считаются врачебной тайной [8].

Право граждан на конфиденциальность передаваемой ими информации при получении медицинской помощи и другой информации, составляющей врачебную тайну, влечет за собой ответственность медицинских работников и других лиц за разглашение такой информации. Эта ответственность может включать административные, дисциплинарные или уголовные меры в соответствии с законодательством Российской Федерации и республик в составе Российской Федерации.

Проводя анализ регламентации правового статуса врачебной тайны, заведующая отделом социального законодательства Института законодательства и сравнительного правоведения при Правительстве РФ Наталья Путило заметила тенденцию на рост исключений из понятий того, что относится к врачебной тайне. Так, Основы законодательства Российской Федерации об охране здоровья граждан (утв. ВС РФ 22 июля 1993 г. № 5487-1, в настоящее время утратили силу) в первоначальной редакции содержало пять позиций об исключениях в отношении разглашения врачебной тайны, в то время как текущий закон в первоначальной редакции содержал 10 позиций, а в текущей редакции — 14. При этом следует учитывать решения КС РФ, который установил, что российское законодательство несовершенно в части медицинской тайны и требуется установление дополнительных оснований в части раскрытия врачебной тайны родственникам умерших пациентов в определенных случаях — разработка соответствующего законопроекта уже ведется, отметила эксперт. Все это говорит об увеличении исключений в части раскрытия информации, составляющей врачебную тайну [2].

Отдельного обсуждения заслуживает также вопрос о законодательном регулировании телемедицинских услуг [2]. Телемедицинские технологии представляют собой средства дистанционного взаимодействия медицинских специалистов с пациентами, идентификации участников и документирования медицинских консультаций и наблюдения. Существует два противоположных мнения в юридическом сообществе относительно необходимости дальнейшего регулирования телемедицинских технологий. Одни эксперты считают, что существующее регулирование недостаточно и требует ужесточения и детализации, включая вопросы врачебной тайны. Другие же считают, что текущие нормы достаточны и чрезмерное регулирование препятствует развитию новых информационных технологий [9].

В свете цифровизации медицинского сектора множество процессов обработки информации переходят в электронный формат. Вместе с увеличением объема информации возрастает ответственность за ее безопасность. Поэтому информационная безопасность в медицине требует соблюдения трех принципов: целостности, доступности и конфиденциальности. Защита необходима не только для информации, но и для инфраструктуры, обеспечивающей ее обработку. Кроме того, медицинская сфера является частью критической информационной структуры, и субъекты этой сферы обязаны обеспечивать защиту информации и соответствовать требованиям по безопасности [1].

Медицинские учреждения обладают множеством персональных данных сотрудников и пациентов, многие из которых относятся к врачебной тайне [10, 11]. Из-за этого они становятся всё более уязвимыми к различным киберугрозам, каждая из которых представляет уникальные вызовы и риски. Особую озабоченность вызывают атаки с использованием вымогательского ПО, что подтверждается атакой WannaCry в 2017 г., серьезно затронувшей Национальную службу здравоохранения Великобритании (NHS) и подчеркнувшей уязвимость медицинских систем к подобным угрозам [12].

Персональная медицинская информация (PMI) очень ценится на черном рынке. Поэтому кража данных также представляет значительные риски. Наглядным примером является утечка данных в Anthem в 2015 г., когда хакеры получили доступ к конфиденциальным данным 79 миллионов человек [13].

Фишинговые атаки — еще одна распространенная угроза, направленная на сотрудников медицинских учреждений с целью извлечения конфиденциальной информации или установки вредоносного ПО. Это произошло во время фишинговой атаки на Медицинский университет Вашингтона в 2019 г., которая затронула данные почти миллиона пациентов [14].

Внутренние угрозы, будь то намеренные или случайные, также являются проблемой в медицине. Примером может служить инцидент в 2018 г., когда медсестра в одной из больниц Нью-Йорка незаконно получила доступ к медицинским записям пациентов, нарушив конфиденциальность [15].

Растущее использование подключенных медицинских устройств или Интернета медицинских вещей (IoMT) влечет за собой новые уязвимости. Например, сообщение FDA о безопасности кардиостимуляторов в 2017 г. подчеркивает потенциальные риски, связанные с IoMT [16].

Атаки на цепочки поставок представляют собой еще один вектор киберугроз, где злоумышленники нацеливаются на сторонних поставщиков, связанных с медицинскими учреждениями. В 2020 г. крупная американская госпитальная система испытала нарушение безопасности через поставщика, что затронуло миллионы пациентов [17].

Атаки типа Distributed Denial of Service (DDoS) могут парализовать ИТ-системы здравоохранения, как это было показано во время DDoS-атаки на Бостонскую детскую больницу в 2014 г., что значительно нарушило работу больницы [18].

Поэтому информационная безопасность в медицине становится всё более важной. Искусственный интеллект (ИИ) является важным союзником в этом направлении, предлагая передовые решения для укрепления безопасности данных и сохранения конфиденциальности. Способность ИИ быстро анализировать огромные массивы данных, обнаруживать аномалии и реагировать на угрозы в реальном времени революционизирует подход к защите данных. От предиктивного анализа угроз до сложных методов шифрования, технологии на основе ИИ переформатируют способы, которыми мы защищаем и обрабатываем конфиденциальную информацию, обеспечивая более высокий стандарт безопасности в нашем взаимосвязанном мире [19, 20]. Системы ИИ превосходно справляются с анализом шаблонов и аномалий в больших объемах данных, что делает их более эффективными, чем традиционное программное обеспечение, в области выявления продвинутых угроз. Они могут изучать нормальное поведение сети и быстро определять отклонения, которые могут указывать на нарушение безопасности, такие как несанкционированный доступ или попытки эксфильтрации данных. Такое раннее обнаружение жизненно важно для предотвращения или минимизации последствий нарушений безопасности данных [21].

В ответ на угрозы ИИ может действовать быстрее, чем человеческие операторы. Как только угроза обнаружена, ИИ может немедленно предпринять действия, такие как изоляция затронутых систем, блокировка подозрительного сетевого трафика или активация других протоколов безопасности для предотвращения дальнейшего ущерба. Кроме того, способность ИИ проводить предиктивный анализ на основе исторических данных позволяет организациям заранее предвидеть и предотвращать потенциальные угрозы безопасности [22].

ИИ также повышает безопасность данных за счет улучшения методов шифрования. Оптимизируя шифрование, ИИ усложняет несанкционированным пользователям доступ к конфиденциальным данным. Эти методы шифрования на основе ИИ постоянно эволюционируют, опережая попытки злоумышленников взломать коды безопасности [23].

Еще одной областью, в которой ИИ вносит значительный вклад, являются системы биометрической аутентификации. ИИ улучшает распознавание лиц, сканирование отпечатков пальцев и распознавание голоса, обеспечивая более высокий уровень безопасности доступа к конфиденциальной информации по сравнению с традиционными паролями [24].

В области сохранения конфиденциальности при анализе данных ИИ может извлекать ценные данные из больших массивов данных, одновременно защищая отдельные точки данных. Техники, такие как дифференциальная конфиденциальность, обеспечивают, чтобы результаты анализа данных не нарушали индивидуальную конфиденциальность. Более того, инструменты ИИ имеют решающее значение для обеспечения соответствия

требованиям законов о защите данных, таких как Федеральный закон № 152-ФЗ «О персональных данных», автоматически оценивая, соответствуют ли практики обработки данных в организации необходимым юридическим стандартам [25].

ИИ также улучшает системы управления безопасностью информации и событий (SIEM), коррелируя и анализируя сигналы безопасности из различных источников, что обеспечивает более полное понимание потенциальных угроз безопасности. Наконец, ИИ неоценим в выявлении шаблонов, указывающих на мошенническую деятельность в критически важных секторах, таких как финансы и здравоохранение, защищая учреждения и их клиентов от потенциального мошенничества [26].

ЗАКЛЮЧЕНИЕ

Одним из главных требований к системе является обеспечение конфиденциальности информации, которая в больших объемах сосредотачивается в медицинских организациях. Низкий уровень защиты конфиденциальной информации существующих медицинских информационных систем формирует риски хакерских атак на системы данных и использования персональных данных пациентов и работников отрасли в неприемлемых целях.

Интеграция ИИ в медицинские информационные системы значительно улучшает анализ и решение распространенных проблем, в частности, конфиденциальности и безопасности данных. ИИ имеет решающее значение для уменьшения этих проблем, предлагая сложные решения, которые традиционные методы могут не предоставить.

Алгоритмы ИИ могут мониторить и обнаруживать любые необычные действия или потенциальные угрозы в медицинских информационных системах. Анализируя паттерны и выявляя аномалии, ИИ может предоставить систему раннего предупреждения против хакерских атак, которые представляют значительный риск из-за низкого уровня защиты в существующих медицинских информационных системах.

Кроме того, ИИ может сократить рабочую нагрузку на ИТ-персонал в медицинских учреждениях, автоматизируя рутинные задачи, такие как резервное копирование данных, шифрование и процессы восстановления после катастроф. Эта автоматизация позволяет сократить расходы и минимизировать человеческие ошибки, которые могут быть дорогостоящими и вредными при обработке чувствительных медицинских данных.

Наконец, ИИ может способствовать повышению общей надежности медицинских информационных систем. Использование ИИ с передовыми алгоритмами для обнаружения угроз и реагирования на них может обеспечить более высокую безопасность и надежность, что имеет решающее значение при обработке чувствительной медицинской информации.

Литература

1. Сазонова М. Врачебная тайна и цифровизация: как защитить информацию о пациенте. Режим доступа: [Электронный ресурс] URL: https://www.garant.ru/news/1465292/ (дата обращения: 30.03.2023).
2. Федеральный закон от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» Режим доступа: [Электронный ресурс] URL: https://base.garant.ru/12191967/(дата обращения 31.03.2023).
3. Иванов А. В., Петров В. С. Особенности врачебной тайны в контексте медицинского права. Журнал медицинского права. 2016; 2: 35–40.
4. Смирнов Е. П. Защита персональных медицинских данных в России. Журнал права и интернета. 2018; 10(1): 45–60.
5. Петрова Л. Л. Правовые аспекты передачи медицинской информации. Журнал медицинского права. 2017; 4: 120–135.
6. Васильев Д. И. Раскрытие медицинской информации без согласия пациента: законодательство и практика. Журнал здравоохранения и медицинского права. 2019; 15(2): 200–210.
7. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» Режим доступа: [Электронный ресурс] URL: https://base.garant.ru/12148567/ (дата обращения 31.03.2023).
8. Назаренко Г. И., Гулиев Я. И., Ермаков Д. Е. Медицинкие Информационные системы: теория и практика. Под ред. Г. И. Назаренко, Г. С. Осипова. М.: ФИЗМАТЛИТ. 2005; 320 с.
9. Сазонова М. Здоровье и технологии: правовые проблемы взаимодействия. Режим доступа: [Электронный ресурс] URL: https://www.garant.ru/article/1453970/ (дата обращения 30.03.2023).
10. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» Режим доступа: [Электронный ресурс] URL: https://base.garant.ru/71730198/ (дата обращения 31.03.2023).
11. Иванов А., Петрова М. Повышение безопасности данных в медицине с помощью решений на основе искусственного интеллекта. Журнал медицинской информатики. 2022; 33(4): 207–219. https://doi.org/10.1080/medinf.2022.207219
12. CBS News. Massive ransomware attack hits 74 countries. 2017, May 14.
13. Husted E. T., Jaffe M. Big Health Care Data Breaches Like Anthem's Are Common. NPR. 2015, February 6.
14. Clarridge C. Data breach at UW Medicine exposes information of nearly 1 million patients. The Seattle Times. 2019, February 20.
15. United States Department of Health and Human Services. Conduent Community Health Solutions of New York. OCR Breach Portal. 2018.
16. U. S. Food and Drug Administration. Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication. 2017, August 29.
17. Whittaker Z. Millions of Americans' medical images and data are left 'unprotected' online. TechCrunch. 2019, September 18.
18. Heimes J. The 10 Biggest Healthcare Data Breaches of 2020, So Far. HealthITSecurity. 2020, June 24.
19. Ellement JR. At first, a hacker was convicted of RICO charges for using a 'botnet.' Boston Globe. 2018, October 1.
20. Смит Дж., Джонсон К. ИИ и сетевая безопасность: обнаружение угроз с помощью машинного обучения. Журнал кибербезопасности. 2022; 18(2):123–135. https://doi.org/10.1080/12345678.2022.1234567.
21. Ли М., Ким Ю. Быстрый отклик и устранение киберугроз с помощью систем на базе ИИ. Международный журнал информационной безопасности. 2023; 22(1): 67–79. https://doi.org/10.1007/s10207-022-00555-4.
22. Патель Р., Гупта С. Улучшение методов шифрования данных с помощью техник ИИ. Журнал прикладной криптографии. 2022; 9(4): 301–317. https://doi.org/10.1016/j.jappcry.2022.03.001.
23. Томпсон А., Чжан Б. ИИ в биометрической аутентификации: новая эра безопасности. Сегодняшние биометрические технологии. 2023; (1): 14–22. https://doi.org/10.1016/j.btt.2023.01.003.
24. Дэвис Е., Кумар В. Сохранение конфиденциальности данных в эпоху ИИ. Журнал защиты данных и конфиденциальности. 2022; 5(2): 210–225. https://doi.org/10.1016/j.jdpp.2022.04.002.

25. Грин Ф., Браун Л. ИИ в системах СИЕМ: усиление управления безопасностью событий. Журнал сетевой безопасности. 2022; 17(3): 134–147. https://doi.org/10.1080/15733021.2022.1189072.

26. Нгуен Х., Чанг Дж. Обнаружение финансового и медицинского мошенничества с помощью ИИ. Журнал управления мошенничеством. 2022; 11(4): 32–45. https://doi.org/10.1080/jfm.2022.11223344.

References

1. Sazonova M. Vrachebnaya tayna i tsifrovizatsiya: kak zashchitit' informatsiyu o patsiyente. Available from URL: https://www.garant.ru/news/1465292/ (data obrashcheniya: 30.03.2023). Russian.
2. Federal'nyy zakon ot 21 noyabrya 2011 g. № 323-FZ «Ob osnovakh okhrany zdorov'ya grazhdan v Rossiyskoy Federatsii» Available from URL: https://base.garant.ru/12191967/ (data obrashcheniya 31.03.2023). Russian.
3. Ivanov AV, Petrov VS. Osobennosti vrachebnoy tayny v kontekste meditsinskogo prava. Zhurnal meditsinskogo prava. 2016; 2: 35–40. Russian.
4. Smirnov Ye P. Zashchita personal'nykh meditsinskikh dannykh v Rossii. Zhurnal prava i interneta. 2018; 10(1): 45–60. Russian.
5. Petrova LL. Pravovyye aspekty peredachi meditsinskoy informatsii. Zhurnal meditsinskogo prava. 2017; 4: 120–135. Russian.
6. Vasil'yev DI. Raskrytiye meditsinskoy informatsii bez soglasiya patsiyenta: zakonodatel'stvo i praktika. Zhurnal zdravookhraneniya i meditsinskogo prava. 2019; 15(2): 200–210. Russian.
7. Federal'nyy zakon ot 27 iyulya 2006 g. № 152-FZ «O personal'nykh dannykh» Rezhim dostupa: [Elektronnyy resurs] URL: https://base.garant.ru/12148567/ (data obrashcheniya 31.03.2023). Russian.
8. Nazarenko GI, Guliyev YaI, Yermakov DYe. Meditsinkiye Informatsionnyye sistemy: teoriya i praktika. Pod red. G. I. Nazarenko, G. S. Osipova. M.: FIZMATLIT. 2005; 320 s. Russian.
9. Sazonova M. Zdorov'ye i tekhnologii: pravovyye problemy vzaimodeystviya. Available from URL: https://www.garant.ru/article/1453970/ (data obrashcheniya 30.03.2023). Russian.
10. Federal'nyy zakon ot 26 iyulya 2017 g. № 187-FZ «O bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii Available from URL: https://base.garant.ru/71730198/ (data obrashcheniya 31.03.2023). Russian.
11. Ivanov A, Petrova M. Povysheniye bezopasnosti dannykh v meditsine s pomoshch'yu resheniy na osnove iskusstvennogo intellekta. Zhurnal meditsinskoy informatiki. 2022; 33(4): 207–219. https://doi.org/10.1080/medinf.2022.207219 Russian.
12. CBS News. Massive ransomware attack hits 74 countries. 2017, May 14.
13. Husted ET, Jaffe M. Big Health Care Data Breaches Like Anthem's Are Common. NPR. 2015, February 6.
14. Clarridge C. Data breach at UW Medicine exposes information of nearly 1 million patients. The Seattle Times. 2019, February 20.
15. United States Department of Health and Human Services. Conduent Community Health Solutions of New York. OCR Breach Portal. 2018.
16. U. S. Food and Drug Administration. Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication. 2017, August 29.
17. Whittaker Z. Millions of Americans' medical images and data are left 'unprotected' online. TechCrunch. 2019, September 18.
18. Heimes J. The 10 Biggest Healthcare Data Breaches of 2020, So Far. HealthITSecurity. 2020, June 24.
19. Ellement JR. At first, a hacker was convicted of RICO charges for using a 'botnet.' Boston Globe. 2018, October 1.
20. Smit Dzh., Dzhonson K. II i setevaya bezopasnost': obnaruzheniye ugroz s pomoshch'yu mashinnogo obucheniya. Zhurnal kiberbezopasnosti. 2022; 18(2):123–135. https://doi.org/10.1080/12345678.2022.1234567. Russian.
21. Li M., Kim YU. Bystryy otklik i ustraneniye kiberugroz s pomoshch'yu sistem na baze II. Mezhdunarodnyy zhurnal informatsionnoy bezopasnosti. 2023; 22(1): 67–79. https://doi.org/10.1007/s10207-022-00555-4. Russian.
22. Patel' R, Gupta S. Uluchsheniye metodov shifrovaniya dannykh s pomoshch'yu tekhnik II. Zhurnal prikladnoy kriptografii. 2022; 9(4): 301–317. https://doi.org/10.1016/j.jappcry.2022.03.001. Russian.
23. Tompson A, Chzhan B. II v biometricheskoy autentifikatsii: novaya era bezopasnosti. Segodnyashniye biometricheskiye tekhnologii. 2023; (1): 14–22. https://doi.org/10.1016/j.btt.2023.01.003. Russian.
24. Devis Ye, Kumar V. Sokhraneniye konfidentsial'nosti dannykh v epokhu II. Zhurnal zashchity dannykh i konfidentsial'nosti. 2022; 5(2): 210–225. https://doi.org/10.1016/j.jdpp.2022.04.002. Russian.
25. Grin F, Braun L. II v sistemakh SIYEM: usileniye upravleniya bezopasnost'yu sobytiy. Zhurnal setevoy bezopasnosti. 2022; 17(3): 134–147. https://doi.org/10.1080/15733021.2022.1189072. Russian.
26. Nguyen KH, Chang Dzh. Obnaruzheniye finansovogo i meditsinskogo moshennichestva s pomoshch'yu II. Zhurnal upravleniya moshennichestvom. 2022; 11(4): 32–45. https://doi.org/10.1080/jfm.2022.11223344. Russian.