DOI: 10.15514/ISPRAS-2024-36(5)-14

Аналитический обзор методов проектирования систем безопасности в телемедицинских системах

[1] *М.А. Лапина, ORCID: 0000-0001-8117-9142 <mlapina@ncfu.ru>*
[2] *Е.А. Максимова, ORCID: 0000-0001-8788-4256 <maksimova@mirea.ru>*
[3] *В.Г. Лапин, ORCID: 0000-0002-0611-7002 <vitl@skkdc.ru>*
[1] *Н.С. Бойков, ORCID: 0009-0003-4038-0474 <nikitaboickov4@gmail.com>*

[1] *Северо-Кавказский федеральный университет,*
355017, Россия, г. Ставрополь, ул. Пушкина, д. 1.
[2] *МИРЭА – Российский технологический университет,*
119454, Россия, г. Москва, пр-т Вернадского, д. 78.
[3] *Ставропольский краевой клинический консультативно-диагностический центр,*
355000, Россия, г. Ставрополь, ул. Ленина, д. 304.

Аннотация. В статье исследуются методы проектирования систем безопасности при обеспечении конфиденциальности данных в телемедицине. Рассмотрены подходы к аутентификации пациентов, используемые в телездравоохранении с учетом их эффективности и безопасности. Проведен анализ методов аутентификации, включая биометрическую идентификацию, двухфакторную аутентификацию и использование уникальных идентификационных кодов. Выявлены преимущества и недостатки каждого из этих методов, что дает медицинским организациям возможность принимать управленческие решения, наиболее соответствующие структуре информационных систем и уровням риска.

Ключевые слова: телемедицина; информационная безопасность; информационная система; система безопасности; конфиденциальность; персональные данные; врачебная тайна; аутентификация; шифрование; медицинские информационные системы.

Для цитирования: Лапина М. А., Максимова Е. А., Лапин В. Г., Бойков Н. С. Аналитический обзор методов проектирования систем безопасности в телемедицинских системах. Труды ИСП РАН, том 36, вып. 5, 2024 г., стр. 191–218. DOI: 10.15514/ISPRAS–2024–36(5)–14.

Analytical Review of Methods for Designing E-Health Security Systems

[1] *M.A. Lapina, ORCID: 0000-0001-8117-9142 <norra7@yandex.ru>*
[2] *E.A. Maksimova, ORCID: 0000-0001-8788-4256 <maksimova@mirea.ru>*
[3] *V.G. Lapin, ORCID: 0000-0002-0611-7002 <vitlx@yandex.ru>*
[1] *N.S. Boikov, ORCID: 0009-0003-4038-0474 <nikitaboickov4@gmail.com>*

[1] *North Caucasus Federal University,*
1, Pushkina St., Stavropol, 355017, Russia.
[2] *MIREA - Russian Technological University,*
78, Vernadsky ave, Moscow, 119454, Russia.
[3] *Stavropol Regional Clinical Advisory and Diagnostic Center,*
304, Lenina St, Stavropol, 355000, Russia.

Abstract. The article explores the methods of designing security systems to ensure data confidentiality in telemedicine. The approaches to patient authentication used in tele-health care are considered, with an emphasis on their effectiveness and safety. The analysis of authentication methods, including biometric identification, two-factor authentication and the use of unique identification codes, was carried out. The advantages and disadvantages of each of these methods have been identified, which gives medical organizations the opportunity to make management decisions that best match the structure of information systems and acceptable levels of risk.

Keywords: telemedicine; information security; information system; security system; confidentiality; personal data; medical secrecy; authentication; encryption; medical information systems.

For citation: Lapina M.A., Maksimova E.A., Lapin V.G., Boikov N.S. Analytical review of methods for designing e-health security systems. Trudy ISP RAN/Proc. ISP RAS, vol. 36, issue 5, 2024. pp. 191-218 (in Russian). DOI: 10.15514/ISPRAS-20124-36(5)-14.

1. Введение

Телемедицина стала неотъемлемой частью медицинской практики, при этом конфиденциальность продолжает оставаться основополагающим принципом медицинской этики, и ее нарушение может привести к серьезным негативным последствиям. Защита конфиденциальности пациентов – важная этическая и юридическая обязанность медицинских учреждений. Несанкционированный доступ к персональным данным пациентов или утечки таких данных в информационном пространстве могут нанести ущерб репутации пациентов, привести к мошенничеству и злоупотреблению информацией, а также нарушить их право на личную жизнь. Телемедицина подразумевает доступ пациентов к медицинским услугам из удаленных и труднодоступных регионов. Такой подход нашел особое применение в условиях пандемий, что подчеркивает важность обеспечения безопасной передачи и хранения медицинских данных. С развитием перечня и методов угроз безопасности данным, таких как несанкционированный доступ, фишинг, кибератаки, уровень угроз для конфиденциальности данных значительно возрастает. Возникает также необходимость во внедрении эффективных методов аутентификации пользователей телемедцинских систем.

В настоящее время **м**ногие страны принимают законы и нормативно-правовые акты, обязывающие организации соблюдать высокие стандарты конфиденциальности медицинских данных. Нарушение этих норм может привести к серьезным последствиям для организаций. Дополнительную сложность представляет тот факт, что различные медицинские учреждения и пациенты имеют разные потребности и допускают для себя разные уровни риска. Выбор подходящего метода аутентификации становится критически важным для удовлетворения возникающих потребностей.

За последние десятилетия телемедицина претерпела значительное развитие, предоставляя пациентам доступ к медицинским услугам и консультациям через цифровые платформы. Развитие в этой области привело к увеличению объема электронных медицинских данных, которые передаются по каналам связи и хранятся в информационных системах. Безопасность и конфиденциальность таких данных стали одними из главных вопросов в телемедицине. Работа с этой информацией несет риск разглашения и нарушения ее защиты. В России закон устанавливает, что врачебная тайна включает информацию о том факте, что человек обратился за медицинской помощью, о состоянии его здоровья, об установленном диагнозе, а также другую информацию, полученную в процессе обследования и лечения (ч. 1 ст. 13 Федерального закона от 21 ноября 2011 г. № 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации", далее - Закон № 323-ФЗ) [1]. Лица, получившие доступ к такой информации (например, в рамках обучения или исполнения служебных обязанностей), не могут ее разглашать, кроме случаев, которые установлены законом (ч. 2 ст. 13 Закона № 323-ФЗ) [1]. Международный кодекс медицинской этики обязывает любого врача уважать право пациента на конфиденциальность и этично раскрывать конфиденциальную информацию при согласии пациента или при наличии реальной и непосредственной угрозы причинения вреда здоровью пациента или другим лицам, причем только в тех случаях, когда эта угроза может быть устранена только путем нарушения конфиденциальности [2]. Использование телемедицинских технологий при оказании медицинской помощи также осуществляется с соблюдением требований, установленных законодательством Российской Федерации в области персональных данных и врачебной тайны [3].

Необходимость неукоснительного соблюдения требований о неразглашении сведений, составляющих врачебную тайну, непосредственно закреплена в части 1 статьи 23 Конституции Российской Федерации, где указано, что «каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну» [4, 5].

Врачебная тайна в соответствии с Конституцией Российской Федерации относится к частной жизни человека, и ее суть заключается в защите прав граждан на личную и семейную тайну от необоснованного и незаконного вмешательства со стороны государственных органов, органов местного самоуправления, государственных и негосударственных организаций, органов власти и частных лиц. Врачебная тайна – относится к сведениям, непосредственно связанным с профессиональной деятельностью медицинских работников, доступ к которой ограничен [4].

Сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении, как раз и составляют врачебную тайну (Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»), а именно его статья 13, содержание которой отражает особое отношение государства к охране врачебной тайны, а именно, врачебную тайну составляют «сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении» [1, 5].

Важно отметить, что врачебная тайна играет ключевую роль в защите частной жизни пациента. Однако в настоящее время, с развитием цифровых технологий и электронных медицинских карт, обеспечение безопасности и аутентификации пользователей в медицинской сфере стало более актуальным, для него выработаны методы, позволяющие сбалансировать конфиденциальность медицинской информации и обеспечить надежную защиту.

Цель исследования – проанализировать современные результаты в области обеспечения конфиденциальности и безопасности данных в телемедицинских системах, а также провести сравнительную характеристику методов аутентификации пациентов для выявления лучших практик в области защиты медицинской информации и аутентификации пациентов.

Телемедицинские технологии (телемедицина) представляют собой информационные технологии, которые обеспечивают дистанционное взаимодействие медицинских работников между собой и с пациентами, а также идентификацию указанных лиц и документирование действий при проведении консультаций, консилиумов и дистанционного медицинского наблюдения (п. 22 ст. 2 Закона № 323-ФЗ) [6].

Рассмотрим виды конфиденциальной информации в медицинских учреждениях.

- Персональные данные пациентов: ФИО, место рождения и проживания, контактная информация, номер медицинского полиса и прочее. Этот вид данных наиболее подвержен утечкам.
- Медицинская (врачебная) тайна. Включает сведения, иллюстрирующие состояние здоровья пациента, наличие заболеваний, диагнозы, результаты лечения.
- Коммерческая тайна: сведения о базе клиентов, планы развития организации, методология лечения болезней, способы проведения качественных исследований и проверок.
- Статистические сведения: информация из карт пациентов, сведения о собственных работниках (например, зарплаты), работе с бюджетными средствами и прочее.
- Иная служебная информация: результаты служебных проверок по исполнению требований по работе и служебным обязанностям.

Особое внимание при обеспечении безопасности уделяется персональным данным пациентов и сведениям, составляющим врачебную тайну.

В статье 3 Федерального закона «О персональных данных» от 27.07.2006 №152-ФЗ содержится определение термина «персональные данные», под которыми понимается любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу. Целью указанного закона является обеспечение защиты прав и свобод человека и гражданина при обращении с его персональными данными, в том числе защита права на неприкосновенность частной жизни, личную и семейную тайну.

Федеральный закон о персональных данных РФ № 152-ФЗ устанавливает правила для обработки персональных данных, включая медицинскую информацию. Он требует, чтобы медицинские организации обеспечивали конфиденциальность и безопасность данных пациентов, а также предусматривает строгие санкции за нарушение этих норм [7]. Важно, что соблюдение этих правил не просто законное требование, но и ключевой фактор поддержания доверия со стороны пациентов. В сфере телемедицины, где данные передаются через неконтролируемые информационные сети, конфиденциальность данных играет критическую роль в выборе медицинской услуги. Соблюдение законодательства о персональных данных помогает не только избежать юридических последствий, но также улучшить репутацию медицинских учреждений и обеспечить долгосрочное доверие пациентов [6].

Понятие врачебной тайны является более широким, нежели персональные данные. И ряд сведений, не относящихся к персональным данным, все равно относятся к врачебной тайне. Например, исключительно данные о диагнозе пациента или методе лечения не позволят идентифицировать лицо [5, 7].

С письменного согласия гражданина или его законного представителя могут быть разглашены сведения, составляющие врачебную тайну в целях медицинского обследования и лечения пациента, проведения научных исследований, их опубликования в научных изданиях, использования данных сведений в учебном процессе.

Законодательством установлены случаи, при которых возможно предоставление сведений, составляющих врачебную тайну, без согласия гражданина (его законного представителя).

Разглашение сведений, составляющих врачебную тайну, может выражаться несколькими способами, а именно:

- Устное распространение сведений, составляющих врачебную тайну. Такое

разглашение может совершаться как умышленно, так и по неосторожности. Особенно часто такая информация передается по телефону третьим лицам, представляющимся родственниками пациента;

- Разглашение сведений, составляющих врачебную тайну возможно при непосредственном общении врача и пациента в общественных местах при сообщении информации о состоянии здоровья в присутствии третьих лиц;
- Указание в научных текстах, исследованиях и иной литературе информации о состоянии здоровья пациента, его диагнозе, течении болезни и прочее без предварительного письменного согласия больного;
- Небрежное отношение с медицинской документацией, в том числе, амбулаторной картой, историей болезни, листками нетрудоспособности.

Важным фактором является постоянный рост объема медицинской информации, передаваемой и хранимой в рамках телемедицины. Электронные медицинские записи и обмен данными стали неотъемлемой частью современной медицины. В этом контексте, нарушение конфиденциальности данных может иметь серьезные последствия. Утечка чувствительной медицинской информации может привести к серьезным репутационным и финансовым последствиям, как для пациентов, так и для медицинских организаций. Соблюдение правил и нормативов в области здравоохранения очень важно. Несоблюдение этих требований может привести к серьезным правовым последствиям.

В случае разглашения сведений, составляющих врачебную тайну, действующим законодательством предусмотрена как административная, так и уголовная ответственность. Ответственности подлежат лица, которым сведения, составляющие врачебную тайну, стали известны при обучении, исполнении трудовых, должностных, служебных и иных обязанностей. Согласно законодательству РФ, к нарушителю, допустившему раскрытие врачебной тайны, персональных данных пациента и другой информации, охраняемой законом, могут быть применены следующие виды наказаний:

- Дисциплинарное. Выражается в вынесении виновнику замечания, выговора. В крайних случаях не исключено увольнение.
- Гражданское. Назначается судом в виде штрафа или возмещения убытков согласно степени нанесенного вреда. Характерно для случаев, где пострадавшей стороне нанесен материальный или моральный ущерб.
- Административное. Заключается в назначении штрафа на сумму 1000-5000 рублей для физических и должностных лиц (статья 13.14 КоАП).
- Уголовное. Назначается штраф в размере 100 000-300 000 рублей, принудительные работы продолжительностью до 4 лет или арест продолжительностью до 6 месяцев с отзывом права занимать отдельные должности. В тяжелых и исключительных случаях в качестве наказания назначается лишение свободы сроком до 4 лет, ограничение заниматься профессиональной деятельностью на срок 2-5 лет (статья 137 УК РФ «Нарушение неприкосновенности частной жизни»).

Так, за разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), в отношении лица, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, может быть возбуждено дело об административном правонарушении по ст. 13.14 Кодекса Российской Федерации об административных правонарушениях (далее – КоАП РФ). Санкция данной статьи предусматривает наказание для граждан в размере от 500 до 1 тысячи рублей; для должностных лиц - от 4 тысяч до 5 тысяч рублей [5, 8].

Максимальное наказание за совершение данного деяния предусмотрено в виде штрафа в размере от 150 тысяч до 350 тысяч рублей или в размере заработной платы или иного дохода осужденного за период от 18 месяцев до 3 лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от 3 до 5 лет, либо принудительными работами на срок до 5 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 6 лет или без такового, либо арестом на срок до 6 месяцев, либо лишением свободы на срок до 5 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 6 лет.

Кроме того, согласно ст. 1068 Гражданского кодекса Российской Федерации юридическое лицо возмещает вред, причиненный его работником при исполнении трудовых (служебных, должностных) обязанностей. Это означает, что медицинское учреждение (должностные лица) в данной ситуации также может быть привлечено к гражданско-правовой ответственности [5, 9].

Защита данных – это не только юридическое требование, но и этическая обязанность медицинских учреждений. Пациенты доверяют им свою глубоко личную информацию о здоровье, и поддержание этого доверия является фундаментальным аспектом эффективной телемедицины.

Важность сохранения доверия и конфиденциальности пациентов в области телемедицины и здравоохранения не должна быть недооценена. Аспекты обеспечения конфиденциальности медицинских данных представлены на рис. 1.

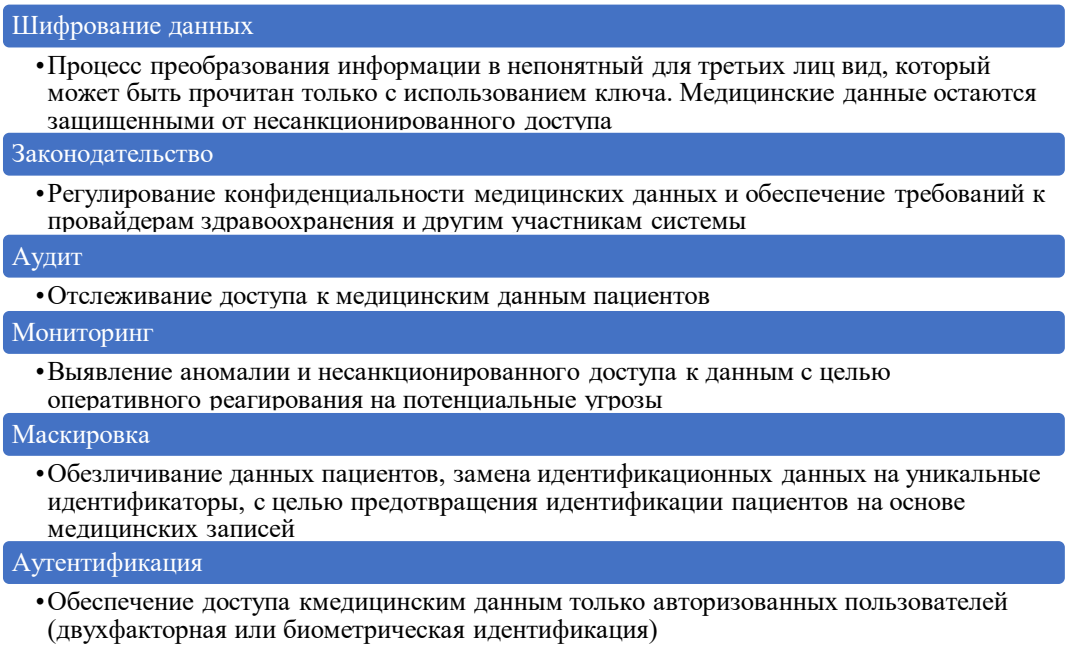

Рис. 1. Аспекты конфиденциальности медицинских данных.
Fig. 1. Aspects of medical data privacy.

С развитием технологий, включая широкополосный интернет и смартфоны, телемедицина стала еще более доступной и распространенной. Пациенты могут получать консультации и медицинские советы прямо из дома, что особенно важно в отдаленных и малонаселенных районах. Многие страны разрабатывают законы и нормативы, которые регулируют использование телемедицины. Это включает в себя вопросы безопасности данных,

лицензирование медицинских профессионалов, и другие аспекты, чтобы обеспечить качество и безопасность телемедицинских услуг.

2. Этапы развития телемедицины

Телемедицина представляет собой использование компьютерных и телекоммуникационных технологий в здравоохранении для лечения, диагностики и предотвращения заболеваний, а также для организационного управления в этой области. Часто этот термин сопровождается словами "современный", "инновационный", "впервые разработанный" и другими подобными. Телемедицина, несмотря на свое современное развитие, имеет свои корни еще в XIX веке. Ее инструменты и технологии продолжают меняться с течением времени. Например, в 1940-х годах актуальным средством был телеграфный аппарат, созданный Жаном Бодо, а в 2010-х годах – смартфоны и облачные программные средства [10, 11].

Развитие дистанционного предоставления медицинской помощи и услуг тесно связано с прогрессом в телекоммуникационных средствах. На разных этапах истории телемедицины применялись передовые технологии для достижения ее целей. История телемедицины – это постепенная эволюция средств связи и удаленного обмена медицинской информацией. Прямо на сущность телемедицины развитие систем здравоохранения и отдельных областей медицины не влияет, так как ее основная цель – передача медицинской информации, остается постоянной, независимо от конкретной области медицины. Более того, в определенные моменты истории телемедицина становилась мощным инструментом для получения существенных новых медицинских знаний, например, через использование радиотелеметрии [12, 13].

- Первая волна включает в себя изобретение телеграфа, радио и телефона.
- Вторая волна охватывает развитие телевидения, включая кабельное и беспроводное телевидение, переход от медленной развертки к цветному изображению.
- Третья волна связана с разработкой инструментов модуляции и демодуляции для передачи данных по телефонным линиям связи.
- Четвертая волна характеризуется развитием спутниковой связи.
- Пятая волна включает в себя создание локальных и распределенных сетей, а также развитие интернет-протокола.

В период с 1850 по нынешние годы можно выделить несколько "волн" в развитии телекоммуникационных технологий. В соответствии с исследованиями Максимова И.Б. и др. [14] временные периоды в развитии телемедицины представлена в табл. 1.

Телемедицинский период начался в 1905 году, когда впервые была передана электрокардиограмма на расстояние, представляя собой важный этап в развитии этой области.

В 1920-х годах морская телемедицина стала активно развиваться, особенно в ситуациях, когда моряки нуждались в медицинской помощи во время длительных плаваний, а медицинских специалистов на борту судов не всегда хватало. В таких ситуациях использовалась морская телемедицина, позволяя обмениваться медицинской информацией на расстоянии и получать консультации узких специалистов [15].

С развитием технологий появилась возможность проводить видеоконференции. Это открыло новые возможности для обмена информацией и консультирования, в том числе в сфере телемедицины. Важным моментом стал 1949 год, когда была проведена первая цветная видеоконференцсвязь между медицинскими специалистами, что стало важным шагом в развитии телемедицинских консультаций [15].

Активно развивалась телемедицина в СССР. С 1960-х по 1990-е годы прошли множество дистанционных консультаций в разнообразных областях, с фокусом на передаче ЭКГ и ее

активном использовании в космических исследованиях. Многие инновации, включая технологии телемедицины, свое начало брали из таких дисциплин, как военная, космическая и морская индустрия, которым практически повсюду придавали приоритетное значение. В стремлении каждой страны занять лидирующую позицию в конкретной сфере, активно развивались промышленные технологии, придавая существенное движение в развитии телемедицинских практик.

Табл. 1. Важные события в области телемедицины.
Table 1. Results for different strategies.

Год	Период / волна	Важные события в телемедицине
1920	I	Первые эксперименты с использованием радио и телефона для консультаций между врачами.
1960	II	Применение спутниковых связей в телемедицине для связи с отдаленными лечебными учреждениями и кораблями.
1990	III	Развитие интернета и мобильной связи способствует распространению телемедицинских консультаций и мониторинга. Появление телемедицинских компаний.
2010	IV	Внедрение мобильных приложений и сенсорных устройств для мониторинга здоровья. Значительное развитие телемедицины в онкологии и диагностике.
2020	V	Бурное развитие телемедицины в связи с пандемией COVID-19 и расширением онлайн-консультаций. Использование искусственного интеллекта и аналитики данных в телемедицине.

В частности, в СССР, в момент исторического полета первого космонавта Юрия Гагарина, телемедицинские инновации уже играли важную роль. Гагарин был подключен к разнообразным устройствам, передающим медицинские данные на Землю, и на планете работало множество медицинских специалистов, бдительно следивших за его здоровьем. Развитие технологий в настоящее время свидетельствует о непрерывном развитии телемедицины. Например, на борту Международной космической станции (МКС), где астронавты проводят продолжительное время, регулярно проводят медицинские осмотры. На станции находится обширное медицинское оборудование, которое выполняет функции диагностики и передает информацию о состоянии здоровья астронавтов на Землю, где эти данные анализируются высококвалифицированными медицинскими специалистами [10].

Если рассматривать эволюцию телемедицины, то она началась с простых технологий передачи данных. На протяжении нескольких лет формируется нормативно-правовое поле регламентации оказания услуг с помощью технологий телемедицины [16].

В будущем технологии телемедицины продолжат развиваться. Этот процесс будет способствовать дальнейшему совершенствованию и улучшению доступности медицинской помощи на расстоянии.

3. Этапы обеспечения конфиденциальности в телемедицине

С развитием технологий и интернета, телемедицина стала широко распространенной практикой, которая позволяет проводить медицинские консультации и лечение пациентов удаленно. Конфиденциальность данных в области телемедицины является одним из ключевых аспектов ее функционирования, что обеспечивает защиту личной и медицинской информации пациентов [17].

Рассмотрим основные этапы обеспечения конфиденциальности в телемедицине.

- Защита данных. Этап включает в себя создание и использование безопасных систем

хранения и передачи данных пациентов. Это может быть реализовано путем использования защищенных интернет-протоколов и программного обеспечения, включающего механизмы шифрования и аутентификации.

- Верификация пациента. Для обеспечения конфиденциальности могут использоваться различные методы идентификации пациента, такие как проверка по электронным документам, биометрическая аутентификация или проверка с помощью одноразовых кодов.
- Контроль доступа. Для предотвращения несанкционированного доступа к медицинской информации пациентов, провайдеры телемедицины должны разработать строгие политики и процедуры, регулирующие доступ персонала к данным. Это включает ограничение доступа к информации только для авторизованного медицинского персонала и использование паролей или других средств аутентификации для входа в систему.
- Обучение персонала. Образование и обучение медицинского персонала в области конфиденциальности является неотъемлемой частью обеспечения безопасности данных пациентов. Провайдеры телемедицины должны предоставить своему персоналу обучение по темам, связанным с конфиденциальностью, этикой и соблюдением HIPAA (Закон о портативности и ответственности в медицинском страховании), если это применимо.
- Согласие пациента. Пациенты должны давать согласие на использование и передачу своей медицинской информации при получении телемедицинской консультации или лечения. Провайдеры телемедицины должны разработать и использовать ясные и понятные политики сбора и использования данных пациентов, а также получать письменное согласие пациента перед обработкой их данных.
- Аудит и мониторинг. Важным аспектом обеспечения конфиденциальности телемедицины является проведение регулярных аудитов и мониторинга системы для выявления и предотвращения любых нарушений безопасности. Это включает проверку журналов доступа, мониторинг сетевого трафика и реагирование на любые подозрительные активности.

4. Принципы обеспечения информационной безопасности для обеспечения конфиденциальности данных в телемедицинских системах

Телемедицина представляет собой важную область медицинской практики, которая использует информационные технологии для предоставления медицинских услуг на расстоянии с использованием информационно-коммуникационных технологий. С увеличением популярности телемедицины становится критически важным обеспечение конфиденциальности данных пациентов.

Анализ современных достижений в области обеспечения конфиденциальности и безопасности данных в системах телемедицины имеет важное значение в современном мире, где цифровизация здравоохранения стала неотъемлемой частью медицинской практики. Это обеспечивает более удобное и доступное обслуживание пациентов, однако также поднимает ряд важных вопросов, связанных с безопасностью данных и аутентификацией пациентов [18].

Рассмотрим методы применения фундаментальных принципов безопасности данных в телемедицине, на основы которых достигается высокий уровень обеспечения конфиденциальности данных пациентов.

4.1 Методология управления идентификацией FAIDM

Методология федеративного анонимного управления идентификацией (Federated Anonymous Identity Management, FAIDM) используется в системах телемедицины для обеспечения конфиденциальности медицинских данных. Методика включает в себя несколько ключевых компонентов:

- GW – "Шлюзовой узел" (Gateway).
- CNi – локальный узел (Constrained Node) в контексте Интернета вещей (IoT).

Система, построенная на базе методологии FAIDM, включает в себя удаленный серверный узел, шлюзовой узел (GW), и локальный узел (CNi). Ограниченный узел приближен к источникам сенсорной информации, собираемой в системе мониторинга пациентов, и может быть интегрирован в устройства, например, в датчики или в носимые устройства, имеющиеся у пациентов [17].

Обычно эти устройства служат для мониторинга окружающей среды и собирают соответствующие данные, которые передаются шлюзовым узлам. В сфере здравоохранения такие датчики могут быть размещены внутри или на теле пациентов для сбора медицинских данных. Шлюзовые узлы расположены на сетевом или коммуникационном уровне структуры системы мониторинга пациентов и, предположительно, обладают достаточными ресурсами по энергопотреблению, производительности процессора и объему памяти [19].

Шлюзы выполняют обработку данных, собранных различными ограниченными узлами, и передают их на удаленный серверный узел, который находится в структуре системы мониторинга пациентов уровнем выше и, скорее всего, не имеет ограничений по вычислительным ресурсам. Медицинский персонал на этом уровне имеет возможность непрерывно мониторить состояние здоровья пациентов на основе получаемых данных [20].

Безопасность взаимодействия между связующими узлами и основным уровнем архитектуры является настолько важной, что для ее обеспечения создается комплекс базовых сетевых функций, в частности, функция сервера аутентификации (Authentication Server Function, AUSF), хранилище и функция обработки учетных данных аутентификации (Authentication Credential Repository and Processing Function, ARPF), функция разглашения идентификатора подписки (Subscription Identifier De-concealing Function, SIDF) и функция закрепления безопасности (Security Anchor Function, SEAF). Однако, несмотря на всю важность этих средств обеспечения безопасности связи между уровнями системы, в описываемой авторами схеме они подробно не рассматриваются [19].

Ключевую роль в инициализации системы и формировании ее параметров играет удаленный серверный узел. Все шлюзовые узлы для обеспечения собственной легитимности должны проходить процедуру регистрации на удаленном сервере. Аналогичным образом каждый ограниченный узел должен зарегистрироваться на одном из легальных шлюзовых узлов.

Когда пациенту вручается носимое медицинское устройство, и он возвращается домой после лечения в больнице, устройство начинает передавать собранные медицинские данные через шлюз IoT (GW), который находится в другом домене, отличающемся от домена больницы. Рассмотрим алгоритм работы метода.

- Инициализации системы.

На начальном этапе удаленного серверного узла удаленный серверный узел S, который предоставляет телемедицинские услуги и сертифицирован органом сертификации здравоохранения, настраивает параметры

- Регистрации узла шлюза.

Шлюзовой узел GWi взаимодействует с удаленным серверным узлом S для регистрации

- Регистрации локального узла

В фазе регистрации локального узла, ограниченный узел $CNij$ отправляет регистрационную информацию на шлюзовой узел GWi.

- Взаимной аутентификации и согласования ключей

После присоединения локального узла к альянсу удаленных серверных узлов в качестве члена удаленного серверного узла, он получает доступ к услугам, предоставляемым не только зарегистрированным поставщиком услуг, но и другими поставщиками услуг в том же альянсе удаленных серверных узлов

- Анонимная подпись и этап проверки

Узел шлюза GWt (верификатор) получает и проверяет сообщение с подписью, которая была создана анонимным закрытым ключом $aSij$, с использованием функции проверки подписи. Это позволяет удостовериться, что сообщение было подписано анонимным узлом, связанным с закрытым ключом $aSij$, и подтвердить его подлинность

4.2 Технология блокчейн

Блокчейн технология (технология распределенного реестра) в телемедицине представляет собой подход к обеспечению безопасности и конфиденциальности медицинских данных и транзакций. Эта концепция позволяет создать два уровня блокчейна [21], что повышает качество системы телемедицины.

1. Основной блокчейн (Main Blockchain):
   - Первый уровень блокчейна, называемый основным, содержит общие медицинские данные, такие как истории болезни, диагнозы, рецепты и другие медицинские записи.
   - Этот уровень отвечает за устойчивость и надежность данных, он также обеспечивает прозрачность доступа к медицинской информации в рамках медицинской сети.
2. Вторичный блокчейн (Secondary Blockchain):
   - Второй уровень блокчейна, известный как вторичный, используется для построения дополнительных слоев безопасности и конфиденциальности.
   - На этом уровне хранятся более чувствительные медицинские данные, такие как биометрические данные, генетические сведения и другие приватные информационные элементы.

При каждой медицинской транзакции, данные записываются одновременно на оба уровня блокчейна. Основной блокчейн гарантирует доступность данных для медицинских работников и организаций, которым такой доступ разрешен. Вторичный блокчейн используется для хранения наиболее конфиденциальных данных и доступен только при наличии соответствующих дополнительных разрешений и аутентификации.

Преимущества двойного блокчейна в телемедицине представлены на рис. 2.

Таким образом, двойной блокчейн в телемедицине помогает сбалансировать доступность и конфиденциальность данных, создавая более безопасную и эффективную систему передачи и хранения медицинской информации.

4.3 Технология радиочастотной идентификации RFID

Применение технологии радиочастотной идентификации (Radio-Frequency Identification, RFID) позволяет идентифицировать, отслеживать и управлять удаленными объектами и связанной с ними информацией [22]. В телемедицине технология RFID играет важную роль, предоставляя ряд преимуществ и способов применения.

Для идентификации пациентов и медицинского персонала могут быть использованы RFID метки. Каждый пациент может иметь индивидуальную RFID-метку, которая содержит его уникальные идентификационные данные. Это позволяет медицинскому персоналу быстро и точно идентифицировать пациентов [22, 23].

На рис. 3 представлена методика работы технологии двойного блокчейна.

Усиленная безопасность данных

- Медицинские данные находятся на вторичном блокчейне

Конфиденциальность данных

- Пациенты могут быть уверены в сохранении конфиденциальности данных, так как доступ к вторичному блокчейну строго ограничен

Совместимость с нормативно-правовым регулированием

- Соответствие законодательству и стандартам в области защиты медицинских данных.

Рис. 2. Преимущества двойного блокчейна в телемедицине.
Fig. 2. Benefits of dual blockchain in telemedicine.

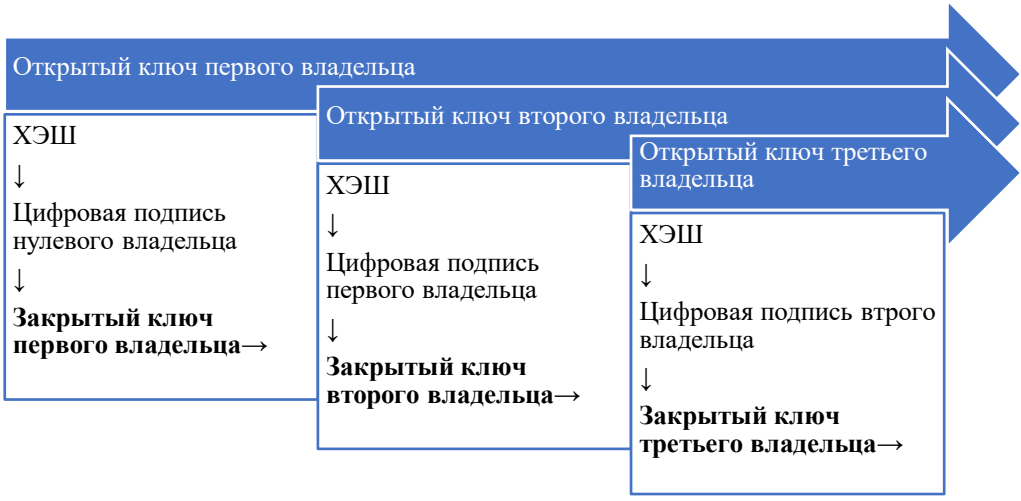

Рис. 3. Методика работы технологии двойного блокчейна.
Fig. 3. The methodology of the dual blockchain technology.

Технология RFID также может использоваться для контроля доступа в медицинских учреждениях, гарантируя, что только уполномоченные сотрудники имеют доступ к определенным зонам.

Рассмотрим механизмы обеспечения контроля доступа и безопасность медицинского оборудования.

- **Управление медицинским оборудованием.** Множество медицинских устройств и инструментов может быть маркировано RFID-метками. Это позволяет медицинским учреждениям отслеживать местонахождение и состояние оборудования. Например, хирургические инструменты могут быть помечены RFID-метками, что облегчает их учет и предотвращает утерю

- **Мониторинг запасов медикаментов и медицинского оборудования.** Процесс позволяет медицинским учреждениям управлять своими ресурсами более эффективно
- **Безопасность пациентов.** RFID-браслеты и карточки могут быть применены для обеспечения безопасности пациентов. Устройства содержат информацию о хронических заболеваниях и медицинских рецептах. В случае неотложной медицинской помощи, медицинский персонал может быстро получить доступ к этой информации
- **Отслеживание медицинских процедур.** В операционных и процедурных залах RFID может использоваться для отслеживания хода операций и медицинских процедур. Это может помочь предотвратить ошибки и обеспечить точное выполнение медицинских рецептов
- **Управление медицинскими записями.** Медицинские записи пациентов могут быть связаны с RFID-метками, что делает их доступными и обновляемыми в реальном времени. Это особенно полезно в системах телемедицины, где медицинские данные могут передаваться и обновляться удаленно
- **Телемониторинг и носимые устройства.** Носимые медицинские устройства, такие как мониторы сердечного ритма или измерители уровня сахара в крови, могут использовать RFID для передачи данных на мобильные устройства для мониторинга в реальном времени. Это позволяет врачам и семейным участникам отслеживать состояние пациентов на расстоянии
- **Системы контроля доступа и безопасности.** RFID-технология может быть использована для обеспечения безопасности в медицинских учреждениях. Это включает в себя контроль доступа в определенные зоны, мониторинг перемещения пациентов и документов, а также обеспечение безопасности в критических ситуациях

На рис. 4 показаны этапы применения технологии RFID в медицине.

Таким образом, RFID играет важную роль в телемедицине, обеспечивая идентификацию пациентов, отслеживание медицинского оборудования, управление медицинскими записями и обеспечение безопасности и безопасности данных в здравоохранении, помогает улучшить эффективность и качество медицинского обслуживания.

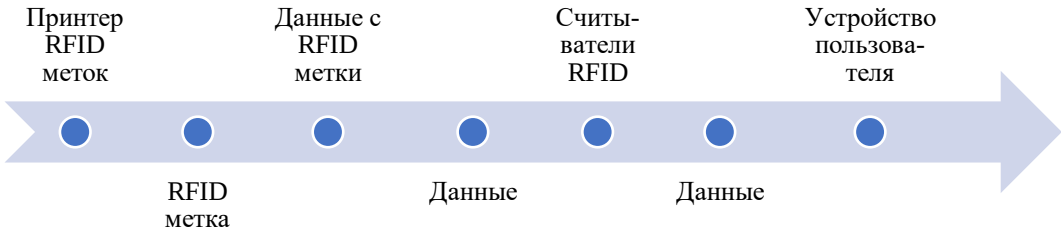

Рис. 4 Этапы применения технологии RFID в медицине.
Fig. 4. RFID technology in medicine.

4.4 Технология бесконтактной связи NFC

Технология бесконтактной связи (Near Field Communication, NFC) может быть полезной в телемедицине для ряда задач и приложений. В технологию NFC входят следующие компоненты:

- **Идентификация пациентов**: для идентификации пациентов в медицинских учреждениях могут быть использованы NFC-метки. Каждый пациент может иметь NFC-метку с уникальным идентификационным номером, которая может быть считана при посещении врача или госпиталя для быстрой и точной идентификации [24].
- **Доступ к медицинской истории**: Пациенты могут использовать NFC-метки, чтобы предоставить врачам доступ к своей медицинской истории и данным о заболеваниях, лекарствах и диагнозах. Это делает процесс консультации более эффективным.
- **Мониторинг пациентов**: Устройства для мониторинга состояния пациентов, такие как носимые медицинские устройства, могут использовать NFC для передачи данных на смартфоны или другие устройства для мониторинга. Например, NFC может быть использовано для передачи данных о сердечном ритме или уровне сахара в крови.
- **Управление лекарствами**: NFC-метки могут быть прикреплены к упаковке лекарств, чтобы предоставить информацию о дозировке, сроках годности и рецепту. Пациенты могут использовать смартфоны для сканирования меток и получения рекомендаций по приему лекарств.
- **Системы контроля доступа**: NFC может быть использовано для ограничения доступа к чувствительной медицинской технике и данным. Только уполномоченный персонал или пациенты с правильными разрешениями могут получить доступ к этой информации.
- **Отслеживание медицинского оборудования**: NFC может быть применено для отслеживания и учета медицинского оборудования, такого как инструменты, медикаменты и медицинские приборы [25].
- **Безопасный обмен медицинскими данными**: NFC может обеспечить безопасный и шифрованный обмен медицинскими данными между устройствами, что критически важно для сохранения конфиденциальности пациентов [25].

Технология NFC предоставляет удобный и безопасный способ обмена и доступа к медицинским данным, улучшая эффективность и безопасность телемедицинских процессов и систем (рис. 5).

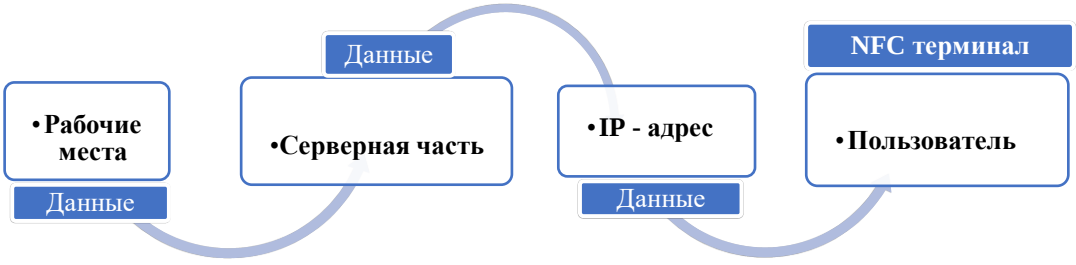

Рис. 5. Технология NFC.
Fig. 5. NFC technology.

Сравнительная характеристика методов аутентификации пациентов позволяет определить направления для повышения уровня защиты медицинской информации и обеспечения безопасности в системах телемедицины [26-28]. Результаты проведенного анализа представлены в табл. 2.

Табл. 2. Сравнительная характеристика принципов безопасности данных для обеспечения конфиденциальности в телемедицине.
Table 2. Comparative Characteristics of Data Security Principles for Ensuring Confidentiality in Telemedicine.

Характеристика	FAIDM	NFC	Двойной блокчейн	RFID
Применение	Используется для идентификации пациентов, доступа к медицинским данным и обеспечения безопасности данных	Может использоваться для идентификации пациентов и доступа к медицинской информации	Может использоваться для обеспечения безопасности и целостности медицинских записей	Беспроводная технология для идентификации и отслеживания объектов
Безопасность	Высокий уровень безопасности с использованием идентификаторов и шифрования данных	Уровень безопасности зависит от применяемых мер безопасности	Высокий уровень безопасности благодаря двум блокчейнам, что делает его более надежным	Уровень безопасности зависит от применяемых мер безопасности
Дальность связи	Средний или длинный диапазон, в зависимости от используемой технологии (например, Bluetooth, WiFi)	Короткий диапазон, обычно менее 4 см	Не применимо, так как это не беспроводная технология	Короткий или средний диапазон, в зависимости от типа RFID (активный или пассивный)
Определение	Передача данных с использованием различных идентификаторов на удаленных устройствах	Беспроводная технология для ближней связи, используемая для идентификации и обмена данными	Технология, которая использует два блокчейна для обеспечения дополнительной безопасности	Беспроводная технология для идентификации и отслеживания объектов

Анализ полученных результатов исследований показывает, что выбор метода аутентификации зависит от конкретных требований проекта и уровня безопасности, необходимого для защиты данных. Но независимо от выбранного метода, для обеспечения безопасности передачи данных необходимо использовать протокол безопасных передач данных HTTPS или другие меры шифрования. Более безопасной альтернативой базовой аутентификации является дайджест-аутентификация, но даже она не обеспечивает абсолютной безопасности и требует дополнительных мер безопасности.

5. Методы обеспечения конфиденциальности на основе аутентификации пользователей

С развитием телемедицины и увеличением числа онлайн-консультаций и рецептов была поставлена задача усиления безопасности пациентов и предотвращения мошеннических действий. Методы аутентификации, такие как пароли и PIN-коды, оказались уязвимыми для вредоносных атак и не всегда обеспечивают надежную защиту данных. Выбор других, более надежных методов аутентификации, зависит от нужного уровня безопасности, удобства для пациентов и нормативных требований.

5.1 Язык управления доступом XACML

Язык управления доступом (eXtensible Access Control Markup Language, XACML) – это стандартный язык и формат для определения политик управления доступом. Он широко используется в области информационной безопасности и управления доступом, включая телемедицину. Применение языка XACML в телемедицине состоит из следующих компонентов:

- **Управление доступом к медицинским данным.** Важно обеспечивать доступ к медицинским данным только тем лицам, которые имеют на это право. XACML позволяет создать гибкие политики управления доступом, которые определяют, кто, как и когда может получать доступ к медицинской информации.
- **Ролевая аутентификация.** XACML может использоваться для определения ролей и привилегий различных пользователей в системе телемедицины. Например, врачи, медсестры и пациенты могут иметь разные уровни доступа к медицинским данным. XACML позволяет настраивать правила доступа в соответствии с этими ролями.
- **Многоуровневые политики доступа.** В системах телемедицины могут существовать различные уровни доступа к данным в зависимости от чувствительности информации. XACML позволяет определять многоуровневые политики, где определенные данные доступны только определенным пользователям или ролям.
- **Динамическое управление доступом.** Врачи и медицинский персонал могут временно требовать доступа к медицинским данным пациента для диагностики и лечения. XACML поддерживает динамическое изменение политик доступа, что позволяет предоставлять доступ при необходимости и отзывать его по завершении процедуры.
- **Аудит доступа.** XACML позволяет регистрировать все попытки доступа к медицинским данным. Это важно для соблюдения законов и нормативных актов в области конфиденциальности медицинских данных.
- **Гибкость и настраиваемость.** XACML обладает высокой степенью гибкости и настраиваемости. Политики доступа могут быть адаптированы к конкретным потребностям медицинских организаций, что позволяет учитывать специфические требования в области безопасности и конфиденциальности данных.

Использование языка XACML в телемедицине помогает обеспечить безопасность, конфиденциальность и целостность медицинских данных, а также эффективное управление доступом медицинского персонала и пациентов к этим данным. Особенно это важно в свете растущей востребованности телемедицины и необходимости соблюдения нормативных актов в области защиты данных.

Язык XACML в телемедицине используется для последовательного достижения следующих целей [23-29]:

- Создание политик контроля доступа для медицинских данных. Политики определяют, кто может иметь доступ к каким данным.
- Аутентификация пользователей и запросов на доступ к данным.
- Применение политик XACML для принятия решений о предоставлении или ограничении доступа к медицинским данным.

5.2 Схема шифрования PEKS

Схема частичного гомоморфного шифрования (Partially Homomorphic Encryption Key Scheme, PEKS) является криптографической техникой, которая может использоваться в

телемедицине для обеспечения конфиденциальности и безопасности медицинских данных, предоставляя средства шифрования и дешифрации данных, которые могут быть полезны в телемедицине [30].

Схема PEKS описывает частично гомоморфное шифрование. Это означает, что она поддерживает выполнение некоторых операций над зашифрованными данными без их предварительной расшифровки. Это может быть полезно, например, при выполнении вычислений над медицинскими данными без раскрытия самих данных. PEKS также может быть настроена для выполнения поиска в зашифрованных данных, не раскрывая самого секретного содержания [21]. PEKS является сложной криптографической схемой и требует внимательной настройки и управления ключами. Использование этой схемы требует больших вычислительных затрат, что следует учитывать при ее применении в системах телемедицины.

Рассмотрим особенности применения схемы PEKS в телемедицине. Для обеспечения безопасности.

- **Конфиденциальность медицинских данных.** Алгоритм PEKS может быть использован для шифрования медицинских записей и данных пациентов. Это обеспечивает конфиденциальность информации и предотвращает несанкционированный доступ к медицинским данным.
- **Управление доступом.** Алгоритм PEKS позволяет контролировать доступ к медицинской информации. Только авторизованные лица с доступом к соответствующим ключам могут расшифровать зашифрованные данные.
- **Безопасная передача данных.** Алгоритм PEKS может быть использован для безопасной передачи медицинских данных между сторонами, обеспечивая шифрование данных в процессе передачи.
- **Подпись и аутентификация.** Алгоритм PEKS может быть интегрирован с механизмами аутентификации и подписи, что помогает подтвердить подлинность медицинских данных и их источника.

В телемедицине схема PEKS работает следующим образом [30, 31]:

- **Шаг 1**: Создание индекса ключевых слов для медицинских документов.
- **Шаг 2**: Шифрование медицинских данных с использованием открытых ключей и индексированных ключевых слов.
- **Шаг 3**: Поиск медицинских данных, по ключевым словам, выполняемый в зашифрованных данных без их расшифровки.

Алгоритм метода PEKS представлен на рис. 6.

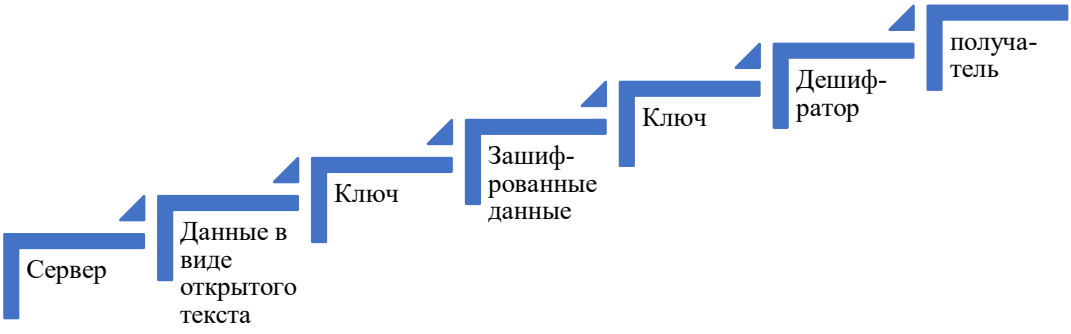

Рис. 6. Алгоритм работы со схемой PEKS.
Fig. 6. PEKS algorithm.

5.3 Прокси-подпись и групповая подпись

Прокси-подпись (Proxy Signature) и групповая подпись (Group Signature) – это два различных метода криптографической подписи, которые могут иметь применение в телемедицине [32].

- **Прокси-подпись** – это механизм, который позволяет одному пользователю (заместителю, прокси) создавать подпись от имени другого пользователя (основного). В контексте телемедицины это может быть полезно, например, когда врач действует от имени пациента для подписания медицинских документов или запросов. Такой механизм может упростить процесс подписания медицинских соглашений и обмена данными, при этом сохраняя право пациента на контроль над своими данными [32].
- **Групповая подпись** – это метод, который позволяет группе пользователей подписывать сообщение так, что внешние наблюдатели могут убедиться в том, что сообщение было подписано представителем группы, но не могут определить, кем именно. В телемедицине это может быть полезно для обеспечения анонимности пациентов или для подписания сообщений от имени медицинских групп или организаций [33].

Рассмотрим применение прокси-подписей и групповых подписей в телемедицине.

- **Подпись медицинских документов.** Врачи или медицинские организации могут использовать прокси-подписи для подписания медицинских отчетов, рецептов и другой медицинской документации от имени пациентов
- **Анонимное обращение пациентов.** Групповые подписи могут использоваться для обеспечения анонимности пациентов при обращении в медицинские учреждения. Это может быть полезно в случаях, когда пациенты хотят обсудить свои медицинские вопросы, не раскрывая свою личность
- **Защита конфиденциальности данных.** Прокси-подписи могут использоваться для защиты медицинских данных пациентов при обмене информацией между медицинскими учреждениями
- **Подписание договоров и соглашений.** Прокси-подписи могут облегчить процесс подписания медицинских соглашений и соглашений о лечении, например, когда пациент не может подписать документы лично

На рис. 7 представлен алгоритм работы Proxy Signature Group Signature (Групповая подпись через доверенного посредника) в телемедицине [33]:

- **Шаг 1**: Группа медицинских работников создает ключи для групповой подписи.
- **Шаг 2**: При создании медицинского отчета или документа, каждый медицинский работник подписывает его групповой подписью.

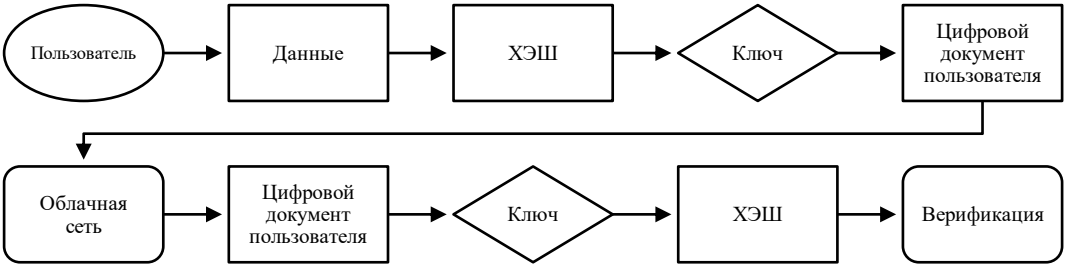

Рис. 7. Механизм групповой прокси-подписи.
Fig. 7. Proxy Signature Group Signature.

- **Шаг 3**: Подписанный документ может быть проверен как подписанный группой, но анонимность отдельных работников сохраняется.

Оба метода подписи предоставляют инструменты для обеспечения конфиденциальности, аутентификации и управления доступом в области телемедицины, однако, учитывая требования к безопасности и конфиденциальности медицинских данных и соблюдение нормативных актов.

5.4 Методы двойных векторных представлений и k-ближайших соседей

Двойные векторные представления (Dual Word Embeddings) и схема k-ближайших соседей (k-Near Neighbors, kNN) – это методы анализа данных и классификации, которые могут быть применены в телемедицине для обработки и классификации медицинских текстов и данных [34].

Алгоритм двойных векторных представлений состоит из следующих шагов [34]:

- **Шаг 1**: Создание двух наборов векторов для каждого слова в медицинском тексте: общих (общих для всех текстов) и специфических (уникальных для данного текста).
- **Шаг 2**: Преобразование медицинского текста в вектор, объединяя оба набора векторов.
- **Шаг 3**: Использование векторов для анализа текста, классификации или извлечения информации.

Схема k-ближайших соседей – это метод классификации объектов на основе их близости к другим объектам в пространстве признаков. В настоящее время он достаточно часто используется в системах нейронных сетях, предполагающих проведение предварительного машинного обучения. В контексте телемедицины схема может быть применена для классификации пациентов, диагнозов или других медицинских данных.

- **Применение метода kNN в телемедицине, диагностика и классификация**: метод kNN может быть использован для диагностики различных состояний или заболеваний на основе медицинских данных и симптомов.
- **Прогнозирование результатов лечения**: kNN может помочь в прогнозировании результатов лечения пациентов на основе данных о предыдущих случаях.

Комбинирование двойных векторных представлений с методом kNN может быть полезным при анализе и классификации медицинских текстов и данных, а также при решении различных задач в области телемедицины. Эти методы помогают улучшить понимание и обработку медицинской информации, что может привести к повышению качества диагностики и ухода за пациентами [34].

Схема k-ближайших соседей работает следующим образом [34]:

- **Шаг 1**: Для каждого пациента создается набор признаков на основе его медицинских данных (например, симптомы, результаты тестов).
- **Шаг 2**: Пациент, для которого требуется классификация (например, диагноз), сравнивается с ближайшими k пациентами на основе их признаков.
- **Шаг 3**: Пациенту присваивается класс или диагноз на основе большинства классов среди k ближайших пациентов.

Сравнительная характеристика рассмотренных методов представлена в табл. 3.

6. Методы анализа защищенности информационных систем

Обеспечение информационной безопасности представляет собой сложный процесс, требующий непрерывного анализа ситуации, который позволяет обнаруживать уязвимости и слабые места в системах безопасности. В [25] рассмотрены методы анализа защищенности информационных систем.

Табл. 3. Сравнительная характеристика методов обеспечения конфиденциальности данных в телемедицине.
Table 3. Comparative characteristics of data privacy methods in telemedicine.

Метод	Описание	Особенности	Преимущества	Недостатки
XACML	Язык управления доступом для определения прав доступа и политик безопасности Декларативный подход	Широко используется в корпоративных информационных системах	• Гибкая система прав доступа • Декларативный подход • Широко применяется в корпоративных системах	• Требует конфигурации и управления политиками • Сложность в больших и сложных системах
Public Encryption with Keyword Search	Технология шифрования данных с возможностью поиска ключевых слов	Обеспечивает конфиденциальность данных и поиск ключевых слов в зашифрованных данных без дешифрации	• Конфиденциальность и поиск в зашифрованных данных. • Подходит для безопасного облачного хранения	• Вычислительная сложность. • Ограниченный поиск ключевых слов
Group Signature	Позволяет создавать подписи, которые могут быть верифицированы как от группы, не раскрывая личность конкретного участника	Защищает анонимность участников группы и используется в приложениях, где требуется подпись от одной из нескольких участников группы	• Анонимность участников группы. • Подпись от группы	• Возможность злоупотребления. • Ограничения в управлении
Dual Word Embeddings, kNN Scheme	Метод представления слов в векторной форме, учитывающий семантику	Улучшает качество анализа текста и задачи обработки естественного языка	• Улучшенный анализ текста. • Семантические ассоциации	• Требует больше вычислительных ресурсов. • Не всегда эффективен на коротких текстах
Proxy Signature	Метод, позволяющий одной стороне подписать сообщение от имени другой стороны	Поддерживает анонимность отправителя, используется для делегирования подписи	• Анонимность отправителя. • Делегирование подписи	• Возможность злоупотребления. • Дополнительная сложность

Один из методов – проведение испытаний на проникновение (penetration test, пентест), которые представляют собой процедуру, заключающуюся в поиске уязвимостей в

информационных системах и использовании этих уязвимостей для проверки защищенности. Тест на проникновение проводится как для выявления "слабых" мест в инфраструктуре и оценки возможных атак, так и для оценки эффективности системы безопасности и получения рекомендаций по повышению ее устойчивости к внешним воздействиям.

Анализ проводится на внутренней и внешней инфраструктуре. При анализе внутренней инфраструктуры специалисты ищут уязвимости в сетевых сервисах и серверах внутри сети компании. При анализе внешних ресурсов проверяются уязвимости веб-сайтов, серверов электронной почты и других сервисов, доступных из глобальной информационной сети.

Еще один метод анализа – анализ беспроводных сетей. Он включает в себя проверку устойчивости внутренней сети к атакам по протоколам на канальном уровне, а также анализ сетевого трафика на наличие критической информации, передаваемой в открытом виде.

Полезным является проведение стресс-тестирования, которое позволяет выявить устойчивость инфраструктуры при повышении нагрузки на нее.

Кроме того, анализ защищенности может быть проведен с использованием методов социальной инженерии, которые проверяют сотрудников на невнимательность и излишнюю доверчивость.

Методы анализа часто называют методами черных, белых или серых ящиков. К методам «черного ящика» относят те методы, при использовании которых заказчик не предоставляет никакой информации о системе, и специалист вынужден собирать ее самостоятельно, моделируя действия злоумышленника. Методами «белого (или прозрачного) ящика» называются методы, применяя которые заказчик предоставляет специалисту всю информацию о системе. Методы «серого ящика» – это компромиссные методы, которые предполагают, что заказчик передает специалистам некоторую, возможно неполную информацию заранее.

7. Информационные системы для решения задач телемедицины

Стандарты обеспечения информационной безопасности и защиты медицинских данных играют критически важную роль в обеспечении конфиденциальности, целостности и доступности медицинской информации особенно с развитием технологий и увеличением объема данных, хранящихся и передаваемых в электронном виде. Рассмотрим основные направления защиты медицинской информации при обеспечении безопасного обмена данными в телемедицинских системах [35-37]:

- Федеральная государственная информационная система в сфере здравоохранения (ЕГИСЗ);
- Медицинская информационная система здравоохранения ("МИС здравоохранения");
- Электронная медицинская карта (ЭМК).

7.1 Информационное пространство ЕГИСЗ

Единая государственная информационная система в сфере здравоохранения (ЕГИСЗ) представляет собой комплексную информационную систему, охватывающую все уровни здравоохранения, с целью совершенствования предоставления медицинских услуг и управления здравоохранением в России [35]. Система имеет три уровня информатизации и три категории пользователей, которые обеспечивают более эффективное и качественное предоставление здравоохранения. На рис. 8 показаны основные категории медицинских организаций РФ.

Рассмотрим основные категории пользователей единого пространства здравоохранения РФ.

- **Граждане/пациенты.** Граждане имеют доступ к удобным средствам взаимодействия с медицинскими организациями, такими как запись на прием и

получение результатов анализов через онлайн-платформы. Они также могут оперативно получать доступ к своей медицинской документации, что повышает уровень информированности и участие в управлении своим здоровьем

- **Врачи/медицинские работники.** Для медицинских работников ЕГИСЗ сокращает необходимость вручную вести отчетность и дает возможность оперативно получать информацию о пациентах.
- **Органы управления.** Органы управления здравоохранением могут оперативно получать агрегированную информацию о состоянии здравоохранения в регионе или стране. Это помогает им разрабатывать более эффективные стратегии и политики, а также быстро реагировать на изменения в здравоохранении

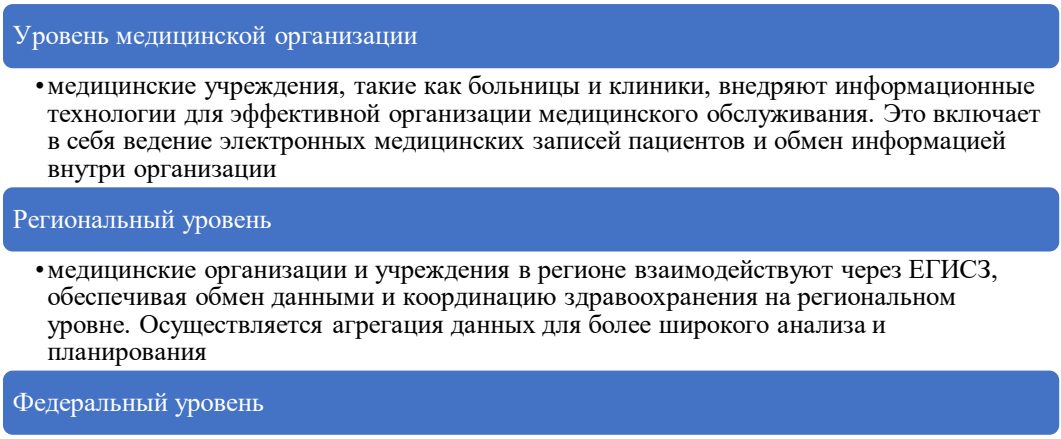

Рис. 8. Основные категории медицинских организаций РФ.
Fig. 8. The main categories of medical organizations in the Russian Federation.

7.2 Медицинская информационная система здравоохранения

Медицинская информационная система (МИС) – это совокупность информационных, организационных, программных и технических средств, предназначенных для автоматизации медицинских процессов [36, 38, 39]. Приведем основные функции и назначение МИС.

- **Повышение качества обслуживания пациентов.** МИС улучшает координацию медицинских процессов, что способствует более точной диагностике и лечению. Это позволяет повысить уровень ухода и комфорта для пациентов
- **Удобный и быстрый доступ к медицинской информации.** МИС позволяет медицинским работникам быстро получать доступ к истории пациента, медицинским данным и другой важной информации, что ускоряет процессы принятия решений
- **Снижение организационных и временных издержек при подготовке отчетов.** МИС автоматизирует процесс создания отчетов, что позволяет сократить время, затрачиваемое на административные задачи, и снизить риски ошибок в документации
- **Сокращение ошибок при составлении медицинских документов.** МИС предотвращает ошибки и упрощает процесс ведения медицинской документации,

что повышает точность и надежность записей о пациентах

- **Организация работы медицинского персонала.** МИС устраняет лишние бумажные процессы, оптимизирует прием и учет пациентов, и упрощает задачи административного характера, что позволяет медицинскому персоналу более эффективно использовать свое время и ресурсы

7.3 Электронные медицинские карты

Электронные медицинские карты (ЭМК) представляют собой электронные версии медицинских карт пациентов [37]. ЭМК могут включать информацию о медицинской истории, данные о здоровье, диагнозы, назначенные лекарства, результаты лабораторных исследований, основные показатели состояния здоровья пациентов, информацию о прививках и выводы из диагностических обследований [40, 41].

Рассмотрим преимущества использования ЭМК.

- **Повышение качества медицинской помощи.** Внедрение ЭМК облегчит врачам обмен информацией о здоровье, что способствует предоставлению медицинской помощи.
- **Безопасное хранение данных.** ЭМК обеспечивают резервное копирование данных, что позволяет восстановить медицинскую информацию о пациентах.
- **Доступ в чрезвычайных ситуациях.** В случае несчастного случая, больницы, работающие с ЭМК, смогут получить неотложные данные о здоровье пациента, что ускорит принятие медицинских решений
- **Эффективное медицинское обслуживание.** Врачи, использующие ЭМК, смогут более быстро отслеживать результаты лабораторных исследований. Обмен информацией между медицинскими учреждениями позволит избежать повторных анализов, что уменьшит расходы на медицинское обслуживание

8. Заключение

Исследование методов проектирования систем безопасности в телемедицинских системах с целью обеспечения конфиденциальности информации показало важность применения соответствующих мер и политик для организации безопасности данных пациентов. С увеличением направлений использования телемедицины возникает необходимость обеспечения высокого уровня защиты информации и предотвращения возможности несанкционированного доступа к ней или ее утечки.

В статье рассмотрены основные понятия в области конфиденциальной информации, на которую в большей степени ориентированы системы обеспечения безопасности при построении телемедицинских систем. Определено, что основными объектами защиты являются персональные данные и данные, содержащие врачебную тайну. Приведены этапы развития технологий в области телемедицины.

На основе приведенных принципов обеспечения информационной безопасности для обеспечения конфиденциальности данных в телемедицинских системах (FAIDM, NFC, блокчейн, RFID) проведена их сравнительная характеристика. Это позволит определить направления использования технологий в телемедицинских системах

Рассмотрены подходы к аутентификации пациентов, используемые в телездравоохранении с учетом их эффективности и безопасности: XACML, Public Encryption with Keyword Search, Group Signature, Dual Word Embeddings, kNN Scheme, Proxy Signature. Проведена их сравнительная характеристика. Выявлены преимущества и недостатки каждого из этих методов**.**

Исследование методов анализа защищенности информационных систем, таких как проведение испытаний на проникновение, методы «черного», «белого» и «серого» ящиков показало их успешную применимость и для телемедицинских систем.

Определены основные направления хранения и обработки медицинской информации при обеспечении безопасного обмена данными в телемедицинских системах, такие как Федеральная государственная информационная система в сфере здравоохранения (ЕГИСЗ), Медицинская информационная система здравоохранения ("МИС здравоохранения"), Электронная медицинская карта (ЭМК), для которых возможно применение рассмотренных выше механизмов обеспечения безопасности конфиденциальной информации.

Таким образом, обеспечение конфиденциальности и безопасности данных является важной частью эффективного функционирования телемедицинских систем. Развитие новых технологий и стандартов обеспечения безопасности данных позволит реализовать эффективную защиту конфиденциальной информации, включая персональные данные и информацию, содержащую врачебную тайну.

Безопасность данных в телемедицине должна быть обеспечена по всем направлениям, включая передачу, хранение и доступ к ней. Несоблюдение требований в сфере обеспечения безопасности в телемедицине может иметь серьезные последствия для всех сторон: пациентов, врачей, медицинские организации и операторов информационных систем, что подчеркивает важность исследования для обеспечения безопасности и эффективности функционирования телемедицинских систем.

Список литературы / References

[1]. Федеральный закон от 21.11.2011 № 323-ФЗ (с изменениями от 24.07.2023) "Об основах охраны здоровья граждан в Российской Федерации" (с изменениями и дополнениями, вступ. В силу с 01.09.2023) Статья 13. Соблюдение врачебной тайны – URL: https://www.consultant.ru/document/cons_doc_LAW_121895/9f906d460f9454a8a0d290738d9fc2798c1e865a/.

[2]. Международный кодекс медицинской этики. Принят 3-й Генеральной Ассамблеей Всемирной медицинской ассоциации, дополнен 22-й Всемирной медицинской ассамблеей 1968 г., 35-й Всемирной медицинской ассамблеей 1983 г., 57-й Всемирной медицинской ассамблеей 2006 г. – URL: https://www.wma.net/policiespost/wma-international-code-of-medical-ethics/.

[3]. Министерство здравоохранения Самарской области: Конфиденциальность: защита и предоставление информации: официальный сайт [https://minzdrav.samregion.ru] – URL: https://minzdrav.samregion.ru/category/vazhnoe/komissiya-po-meditsinskoj-etike/konfidentsialnost-zashhita-i-predostavlenie-informatsii/.

[4]. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ) // СПС «КонсультантПлюс» – URL: https://www.consultant.ru/document/cons_doc_LAW_28399/.

[5]. Прокуратура Ставропольского края: Врачебная тайна и право пациента на информацию о своем здоровье: официальный сайт [https://epp.genproc.gov.ru] – URL: https://epp.genproc.gov.ru/ru/web/proc_26/activity/legal-education/explain?item=59782102 .

[6]. Федеральный закон от 21.11.2011 N 323 ФЗ (ред. от 06.03.2019) «Об основах охраны здоровья граждан в Российской Федерации» // Собрание законодательства РФ, 28. 11. 2011, №48. Ст. 6724. // СПС «КонсультантПлюс» – URL: https://www.consultant.ru/document/cons_doc_LAW_121895/.

[7]. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 08.08.2024) «О персональных данных» // СПС «КонсультантПлюс» – URL: https://www.consultant.ru/document/cons_doc_LAW_61801/

[8]. «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 N 195-ФЗ (ред. от 14.10.2024) (с изм. и доп., вступ. в силу с 21.10.2024) // СПС «КонсультантПлюс» – URL: https://www.consultant.ru/document/cons_doc_LAW_34661/

[9]. «Гражданский кодекс Российской Федерации» (ГК РФ) от 30 ноября 1994 года N 51-ФЗ // СПС «КонсультантПлюс» – https://www.consultant.ru/document/cons_doc_LAW_5142/

[10]. Günter Burg / Telemedicine and Teledermatology / 1.2 The History of Telemedicine – URL: https://books.google.com.mm/books?id=F2gyQlDgptgC&lpg=PA6&dq=history%20of%20telemedicine&lr&hl=ru&pg=PA6#v=onepage&q&f=false

[11]. Владзимирский А.В. История телемедицины: люди, факты, технологии. Донецк: «Цифровая типография», 2008.

[12]. Леванов В.М., Переведенцев О.В., Сергеев Д.В., Никольский А.В. Нормативное обеспечение телемедицины: 20 лет развития. Журнал телемедицины и электронного здравоохранения. 2017; 3(5):160-170.

[13]. Леванов В.М. От телемедицины до электронного здравоохранения: эволюция терминов. Медицинский альманах. 2012; 2(21):16-19.

[14]. История, анализ состояния и перспектив развития телемедицины: [https://jtelemed.ru/] Российский журнал телемедицины и электронного здравоохранения – URL: https://jtelemed.ru/node/3739.

[15]. Wu He, Justin Zhang, Huanmei Wu / A Unified Health Information System Framework for Connecting Data, People, Devices, and Systems – URL: https://www.researchgate.net/publication/363425208_A_Unified_Health_Information_System_Framework_for_Connecting_Data_People_Devices_and_Systems.

[16]. Поспелова С.И., Сергеев Ю.Д., Павлова Ю.В., Каменская Н.А. Правовой режим применения телемедицинских технологий и внедрения электронного документооборота: современное состояние правового регулирования и перспективы развития. Медицинское право. 2018, №5. с.24- 33.

[17]. SearchInform: информационная безопасность / официальный сайт [https://searchinform.ru/] – URL: https://searchinform.ru/informatsionnaya-bezopasnost/.

[18]. Kaspersky: Кибербезопасность в здравоохранении: где болезнь, где болезнь роста / официальный сайт: [https://www.kaspersky.ru] – URL: https://www.kaspersky.ru/blog/healthcare-safeguarding-data/4474/.

[19]. Tzu Wei Lin / FAIDM for Medical Privacy Protection in 5G Telemedicine Systems – URL: https://www.researchgate.net/publication/348816986_FAIDM_for_Medical_Privacy_Protection_in_5G_Telemedicine_Systems.

[20]. Кучуков, Р. А. Теория и практика государственного регулирования экономических и социальных процессов: учебное пособие для студентов, обучающихся по специальностям: "Финансы и кредит", "Бухгалтер. учет, анализ и аудит", "Мировая экономика", "Налоги и налогообложение" / Р. А. Кучуков; Р. А. Кучуков. – Москва: Гардарики, 2004. – 287 с. – (Disciplinae). – ISBN 5-8297-0201-0. – EDN QQEXOB.

[21]. Abdelkader Laouid, Mohammad Hammoudeh, Kara Mostefa /A MultiKey with Partially Homomorphic Encryption Scheme for Low End Devices Ensuring Data Integrity – URL: https://www.researchgate.net/publication/370392930_A_MultiKey_with_Partially_Homomorphic_Encryption_Scheme_for_LowEnd_Devices_Ensuring_Data_Integrity.

[22]. Yang Xiao; Xuemin Shen; BO Sun; Lin Cai / Security and privacy in RFID and applications in telemedicine: – URL: https://ieeexplore.ieee.org/abstract/document/1632651.

[23]. Encryption Scheme for Low End Devices Ensuring Data Integrity – URL: https://www.researchgate.net/publication/370392930_A_MultiKey_with_Partially_Homomorphic_Encryption_Scheme_for_LowEnd_Devices_Ensuring_Data_Integrity

[24]. Yasir Iqbal, Shahzaib Tahir, Abdullah M. Almuhaideb, Adeel M. Syed / A Novel Homomorphic Approach for Preserving Privacy of Data in Telemedicine – URL: https://www.mdpi.com/1424-8220/22/12/4432.

[25]. Yonghang Tai; Bixuan Gao; Qiong Li; Zhengtao Yu; Chunsheng Zhu; Victor Chang / Trustworthy and Intelligent COVID-19 Diagnostic IoMT Through XR and Deep-Learning-Based Clinic Data Access – URL: https://ieeexplore.ieee.org/abstract/document/9343340.

[26]. Иванов В.В., аутентификация и авторизация / Иванов В. В., Лубова Е. С., Черкасов Д. Ю. Текст :электронный // Компьютерные и информационные науки: https://cyberleninka.ru/ 2017 – URL: https://cyberleninka.ru/article/n/autentifikatsiya-i-avtorizatsiya.

[27]. Утечка медицинских данных: как они происходят и как их предотвратить:[https://www.itsec.ru/] Information security журнал /– URL: https://lib.itsec.ru/articles2/control/utechki-meditsinskih-dannyh-kak-oni-proishodyat-i-kak-ih-predotv.

[28]. Hitesh Gupta / Management Information System: – URL: https://books.google.ru/books?hl=ru&lr=&id=PWRYwOJ8FmgC&oi=fnd&pg=PA1&dq=Description+of+the+procedure+and+regulations+for+personnel+actions+during+the+operation+of+MIS&ots=wvVUGCMb-

0&sig=YFhrCauvEg4skq2_TQTy2hqlHxE&redir_esc=y#v=onepage&q=Description%20of%20the%20procedure%20and%20regulations%20for%20personnel%20actions%20during%20the%20operation%20of%20MIS&f=false

[29]. Carroline Dewi Puspa Kencana Ramli, Hanne Riis Nielson, Flemming / The logic of XACML – URL: https://www.sciencedirect.com/science/article/pii/S0167642313001238.

[30]. Sun-Moon Jo, Kyung-Yong Chung / Design of access control system for telemedicine secure XML documents – URL: https://link.springer.com/article/10.1007/s11042-014-1938-x.

[31]. Kaspersky: Что такое шифрование? / официальный сайт: [https://www.kaspersky.ru] – URL: https://www.kaspersky.ru/resource-center/definitions/encryption (дата обращения 17.10.2024).

[32]. Byoungcheon Lee / Strong Proxy Signature and Applications – URL: https://www.researchgate.net/publication/2410948_Strong_Proxy_Signature_and_its_Applications.

[33]. Yuping Zhou, Yu Hu,1Jianneng Chen, Zengjie Huang, Hui Huang, Yi Fan Zhang / Identity Based Designated-Verifier Proxy Signature Scheme with Information Recovery in Telemedicine System https://www.hindawi.com/journals/wcmc/2022/1580444/

[34]. Robert P. Bostrom and J. Stephen Heinen / MIS Problems and Failures: A Socio-Technical Perspective. Part I: The Causes – URL: https://www.sci-hub.ru/10.2307/248710.

[35]. ЕГИСЗ / официальный сайт: – URL: https://egisz.rosminzdrav.ru/.

[36]. Белышев Д.В., Гулиев Я.И., Михеев А.Е. / Место МИС медицинской организации в методологии информатизации здравоохранения – URL: https://cyberleninka.ru/article/n/mesto-mis-meditsinskoy-organizatsii-v-metodologii-informatizatsii-zdravoohraneniya.

[37]. Зингерман Б.В., Шкловский-Корди Н.Е. / Электронная медицинская карта и принципы ее организации – URL: https://cyberleninka.ru/article/n/elektronnaya-meditsinskaya-karta-i-printsipy-ee-organizatsii.

[38]. Когаленок В.Н., Царева З.Г., Тараканов С.А. / Проблемы внедрения медицинских информационных систем автоматизации здравоохранения. Комплекс программных средств «Система автоматизации медикострахового обслуживания населения» – URL: https://cyberleninka.ru/article/n/problemy-vnedreniya-meditsinskih-informatsionnyh-sistem-avtomatizatsii-uchrezhdeniy-zdravoohraneniya-kompleks-programmnyh-sredstv.

[39]. Кошкаров А. А. / Структурная адаптация федеральных требований к медицинским информационным системам на региональном уровне – URL: https://cyberleninka.ru/article/n/strukturnaya-adaptatsiya-federalnyh-trebovaniy-k-meditsinskim-informatsionnym-sistemam-na-regionalnom-urovne.

[40]. Зарубина Т.В., Швырев С.Л., Соловьев В.Г., Раузина С.Е., Родионов В.С. / Интегрированная медицинская карта: состояние дел и перспективы – URL: https://cyberleninka.ru/article/n/integrirovannaya-elektronnaya-meditsinskaya-karta-sostoyanie-del-i-perspektivy.

[41]. Швырев С.Л. / Опыт разработки электронной медицинской документации на основе архитектуры клинических документов CDA 2. 0 HL7 – URL: https://cyberleninka.ru/article/n/opyt-razrabotki-elektronnoy-meditsinskoy-dokumentatsii-na-osnove-arhitektury-klinicheskih-dokumentov-cda-2-0-hl7.

Информация об авторах / Information about authors

Мария Анатольевна ЛАПИНА – кандидат физико-математических наук, доцент, доцент кафедры информационной безопасности автоматизированных систем Северо-Кавказского федерального университета. Сфера научных интересов: цифровые технологии, киберфизические системы, анализ данных, управление информационной безопасностью, доверенный искусственный интеллект, криптография, анализ программного кода.

Maria Anatolyevna LAPINA – Cand. Sci. (Phys.-Math.), Associate Professor, Associate Professor of the Department of Information Security of Automated Systems of the North Caucasus Federal University. Research interests: digital technologies, cyber-physical systems, data analysis, information security management, trusted artificial intelligence, cryptography, program code analysis.

Елена Александровна МАКСИМОВА – доктор технических наук, доцент, заведующий кафедрой «Интеллектуальные системы информационной безопасности» РТУ МИРЕА –

Российский технологический университет. Сфера научных интересов: цифровые технологии, киберфизические системы, анализ данных, управление информационной безопасностью, криптография, критическая информационная инфраструктура.

Elena Alexandrovna MAKSIMOVA – Dr. Sci. (Tech.), Associate Professor, Head of the Department "Intelligent Information Security Systems" of RTU MIREA – Russian University of Technology. Research interests: digital technologies, cyber-physical systems, data analysis, information security management, cryptography, critical information infrastructure.

Виталий Геннадьевич ЛАПИН – кандидат физико-математических наук, начальник отдела АСУ Ставропольского краевого клинического консультативно-диагностического центра. Сфера научных интересов: цифровые технологии, киберфизические системы, анализ данных, управление информационной безопасностью, анализ программного кода.

Vitaly Gennadevich LAPIN – Cand. Sci. (Phys.-Math.), Head of the Automated Control System Department of the Stavropol Regional Clinical Advisory and Diagnostic Center. Research interests: digital technologies, cyber-physical systems, data analysis, information security management, program code analysis.

Никита Сергеевич БОЙКОВ – студент кафедры информационной безопасности Северо-Кавказского федерального университета. Сфера научных интересов: цифровые технологии, анализ данных, управление информационной безопасностью, анализ программного кода.

Nikita Sergeevich BOIKOV – a student of the Department of Information Security of the North Caucasus Federal University. Research interests: digital technologies, data analysis, information security management, program code analysis.