На правах рукописи

ШУМИЛИН АЛЕКСАНДР СЕРГЕЕВИЧ

МЕТОД ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В РАСПРЕДЕЛЕННОЙ МЕДИЦИНСКОЙ ОБЛАЧНОЙ СИСТЕМЕ

Специальность 2.3.6 – Методы и системы защиты информации, информационная безопасность

Автореферат
диссертации на соискание ученой степени
кандидата технических наук

Таганрог 2024

Работа выполнена в ФГАОУ ВО «Южный федеральный университет» на кафедре безопасности информационных технологий имени Олега Борисовича Макаревича Института компьютерных технологий и информационной безопасности.

Научный руководитель:	**Бабенко Людмила Клементьевна** доктор технических наук, профессор, ФГАОУ ВО «Южный федеральный университет», г. Таганрог
Официальные оппоненты:	**Ажмухамедов Искандар Маратович** доктор технических наук, профессор, ФГБОУ ВО «Астраханский государственный университет имени В. Н. Татищева», г. Астрахань, декан Факультета цифровых технологий и кибербезопасности, профессор кафедры информационной безопасности
	Тебуева Фариза Биляловна доктор физико-математических наук, доцент, ФГАОУ ВО «Северо-Кавказский федеральный университет», г. Ставрополь, заведующая кафедрой компьютерной безопасности

Защита состоится «16» мая 2024 г. в 14:00 часов на заседании диссертационного совета ЮФУ801.02.02 Федерального государственного автономного образовательного учреждения высшего образования «Южный федеральный университет» по адресу: Ростовская обл., г. Таганрог, ул. Шевченко, 2, «Точка кипения» ИТА ЮФУ.

С диссертацией можно ознакомиться в зональной научной библиотеке ЮФУ по адресу: г. Ростов-на Дону, ул. Зорге, 21-ж и на сайте ФГАОУ ВО «Южный федеральный университет» по адресу: https://hub.sfedu.ru/diss.

Отзывы на автореферат в двух экземплярах, заверенные печатью учреждения, просьба направлять по адресу: 347922, Ростовская обл., г. Таганрог, ГСП-17А, пер. Некрасовский, 44, к. 302, Диссертационный совет ЮФУ801.02.02.

Автореферат разослан «___» марта 2024 г.

Ученый секретарь
диссертационного совета ЮФУ801.02.02,
кандидат технических наук, доцент  Ельчанинова Н.Б.

Общая характеристика работы

Актуальность темы исследования. В современном мире ежедневно миллионы людей используют компьютерные технологии для решения различных задач, а возможность свободного доступа в интернет сделала популярными такие активности, как поиск информации, обучение, разработку программного обеспечения, а также возможность предоставления широкого спектра услуг для населения, в том числе оказание медицинской помощи. Ситуацию с актуальностью и повсеместным развитием информационных технологий обострила пандемия COVID-19, из-за которой большинство сфер деятельности и бизнеса пришлось адаптировать под новые реалии работы. Процессы оказания услуг населению, удаленный формат работы сотрудников и проведение обучения, а также многие другие факторы активно способствовали масштабной информатизации и цифровизации тысяч предприятий и муниципальных организаций. В условиях современного информационного общества медицинская сфера стала более зависимой от цифровых технологий. Облачные медицинские системы, в которых выполняется обработка больших объемов данных, предоставляют возможность эффективного управления циркулирующей информацией и повышают качество медицинских услуг. Однако существенно возрастают риски утечки конфиденциальных данных, представляющих высокую ценность, как для пользователей информационных систем, так и для злоумышленников ввиду увеличения количества потенциальных угроз. В связи с этим становится актуальной проблема обеспечения информационной безопасности, так как небезопасное хранение и передача медицинских данных в информационных системах может являться источником различных угроз, например, стать причиной неправомерного доступа или утечки конфиденциальной информации или кибератаки.

Интеграция информационных технологий в медицинскую сферу позволила автоматизировать и повысить качество процессов управления медицинскими данными, что способствовало улучшению эффективности работы медицинских учреждений. Облачные медицинские информационные системы на сегодняшний день позволяют получать доступ к медицинским данным, позволяют сократить время обработки информации, повышают точность диагностики и эффективность лечения. Однако возрастает необходимость обеспечивать безопасность данных в таких медицинских системах, чтобы предотвратить несанкционированный доступ и защитить права пациентов на конфиденциальность.

Одним из основных рисков при использовании облачных медицинских систем является возможность несанкционированного доступа к медицинской информации. Утечка конфиденциальных данных может привести не только к негативным последствиям для пациентов, но и к имиджевым и юридическим проблемам для медицинских учреждений. Кроме того, облачные системы подвержены кибератакам, которые могут привести к нарушению доступности данных и нарушению работы приложений, используемых в медицинских целях. Поэтому, обеспечение информационной безопасности является критически важным аспектом при построении облачных медицинских систем. В доменной области, связанной с медициной, утечки данных являются одной из самых актуальных

проблем. Ситуация осложняется тем, что в руки злоумышленников помимо персональных данных пациентов попадают и результаты обследований, диагнозы, рекомендации к лечению, что усугубляет ситуацию и дает возможность злоумышленникам действовать более эффективно, имея большой информационный ресурс для воздействия на жертву и достижения своих корыстных целей.

Степень разработанности темы. Для обеспечения информационной безопасности в облачных медицинских информационных системах используются методы разграничения прав доступа и классические способы шифрования, в частности симметричное шифрование при работе с отдельными файлами и ассиметричное при шифровании ключей, а также применение комбинированных методов. Использование существующих методов обеспечения безопасности данных в информационных системах, рассмотренных среди работ авторов Rohan J., Jeeva S., Wen-Cheng L., Dr. Anua S., Sharma Y., Batra M., Chowdary D., Chandra P., Patel R., Maha T., Said El H., Ruba A., Azman S., Izang A., Mehsa Y., Omotosh O., Obioma C., Acar A., Aksu H., Conti M., Крейтова М.Р., Малыш В.Н., Бойченко И.В., Кривошеевой Д., Лаврова Д. Н., опубликованных в научной литературе, содержат различные недостатки, такие как:

1. Проблема распределения ключей для симметричного шифрования.
2. Строгие требования ко времени работы алгоритмов, потреблению памяти и вычислительным ресурсам.
3. Асимметричное шифрование работает медленно в информационных системах.
4. Потеря секретного ключа при использовании асимметричных алгоритмов приводит к потере данных.
5. Перехват ключа шифрования приводит к компрометации данных.

Отсылка на использование алгоритмов шифрования была отражена в научной работе Котяшичева Ильи и Бырыловой Елены, которые исследовали возможность применения облачных технологий для повышения эффективности интеграции информационных систем в области здравоохранения. Работы научных коллективов, предлагающих использовать гомоморфное шифрование (Maha Tebaa, Said El Hajii и Juan Luis López Delgado, Ruba Awadallah и Azman Samsudin) для решения поставленной научной задачи по обеспечению безопасности медицинских данных, выглядят не применимыми с точки зрения скорости работы таких алгоритмов, потому что операции выполняются медленно и проигрывают классическим алгоритмам в десятки и сотни раз, а передача ключа шифрования выполняется по открытому каналу связи.

Цифровые платформы, которые предлагают свои вычислительные мощности для развертывания медицинских систем, рассматривают процедуру авторизации пользователей и алгоритмы шифрования как наиболее зарекомендованные технологии для обеспечения защиты конфиденциальных данных от неправомерного использования. Однако, в случае с ассиметричным шифрованием это приводит к тому, что операции выполняются медленно.

В связи с вышеупомянутыми фактами существует актуальная научная задача, которая заключается в следующем: в условиях увеличения количества попыток несанкционированных вторжений со стороны злоумышленников на данные, находящиеся в медицинских информационных системах, необходимо в пределах имеющихся ресурсов

разработать такой метод защиты медицинских данных, который позволит обеспечить безопасность при условии отсутствия снижения производительности работы информационной системы.

Для решения задачи предлагается разработать новый метод обеспечения безопасности, который позволит использовать подход на основе схемы разделения секрета. Секрет, представляющий собой файл медицинского обследования, разделяется на определенное количество частей, затем каждая часть зашифровывается и отправляется на отдельный сервер, входящий в состав облачной инфраструктуры медицинской системы. Такой подход гарантирует восстановление исходного медицинского файла в том случае, когда заданное пороговое значение частей файла собирается воедино. До тех пор, пока менее, чем заданное пороговое значение серверов не «вступают в сговор» с целью нарушения конфиденциальности, они не могут восстановить секрет, даже при условии успешной компрометации каждой из долей секрета. Более того, такой подход обеспечивает избыточность данных для повышения доступности: некоторые доли могут быть утеряны, не препятствуя восстановлению исходного секрета уполномоченными лицами.

Целью диссертационного исследования является повышение эффективности обеспечения безопасности медицинских информационных систем за счет использования метода обеспечения защиты конфиденциальных медицинских данных на основе протокола разделения секрета.

Научная задача, решаемая в диссертации, заключается в разработке метода обеспечения безопасности медицинских данных в условиях несанкционированных вторжений со стороны злоумышленников на данные, находящиеся в медицинских информационных системах. Необходимо в пределах имеющихся ресурсов разработать метод защиты конфиденциальных данных, который позволит обеспечить безопасность при условии отсутствия снижения производительности работы МИС.

Достижение поставленной цели предполагает необходимость решения следующих задач:

1. Анализ существующих медицинских информационных систем, их архитектурных решений, а также способов обеспечения защиты данных в таких системах.
2. Разработка архитектуры распределенной облачной платформы хранения и систематизации конфиденциальных данных медицинских обследований, позволяющей получать и обрабатывать данные различных аппаратных средств диагностики. Универсальность архитектуры должна позволять оперировать различными типами медицинских данных, зарегистрированных с использованием различных аппаратных средств, работающих на основе протокола HL7.
3. Разработка метода обеспечения безопасности с использованием протокола разделения секрета, для защиты медицинских данных пациентов, циркулирующих в облачной медицинской информационной системе.
4. Программная реализация разработанного метода обеспечения безопасности конфиденциальных медицинских данных.
5. Выполнение экспериментальных исследований и тестирование разработанного метода защиты путем получения практических результатов.

Объектом исследования являются технологии хранения, передачи и защиты конфиденциальной информации, находящейся в распределенной медицинской информационной системе, реализованной на основе облачной архитектуры.

Предметом исследования являются методы и схемы разделения секрета, обеспечивающие конфиденциальность медицинских данных пациентов.

Методы исследования: теория шифрования, методы математического численного моделирования, математическая статистика, алгоритмы шифрования и разделения секрета.

Теоретической основой исследования являются методы работы с данными, а также теоретические основы математической логики, основ алгоритмизации, методов программирования, криптографических методов защиты информации, методы оптимизации, методы теории реализации математических моделей с использованием прикладных программ.

Научная новизна. **В работе получены следующие новые научные результаты.**

1. Метод обеспечения безопасности конфиденциальной информации в распределенной медицинской облачной системе (МИС), **отличающийся** использованием схемы разделения секрета Шамира, позволяющий повысить безопасность МИС путем усложнения процесса компрометации файла с конфиденциальными данными. Файл разделяется на фрагменты, которые затем передаются и хранятся на разных серверах, что усложняет процедуру доступа к исходному файлу со стороны злоумышленников, потому что для восстановления исходных данных требуется собрать части воедино.

2. Алгоритм оценки времени работы протокола разделения секрета на основе схемы Шамира, **отличающийся** применением библиотеки MPI, позволяющей производить обработку и взаимодействие параллельных процессов. Получены результаты сокращения времени для разделения файлов медицинского обследования на фрагменты и восстановления фрагментов файла в исходное состояние.

3. Архитектура облачной медицинской распределенной системы, **отличающаяся** возможностью функционировать с использованием разработанного метода, включающего определенную конфигурацию серверов, каналов связи, алгоритмы и способы формирования ключей шифрования, процедуру разделения на части и объединения воедино конфиденциальных данных согласно схеме Шамира. Архитектура медицинской системы позволяет работать как с классическими форматами представления файлов, так и с медицинскими файлами (DICOM, Nifti, NRRD).

Теоретическая значимость исследования заключается в формировании новых подходов к построению систем защиты медицинских данных на основе использования схем разделения секрета, теоретических знаний о процессе интеграции механизмов защиты в системы обеспечения конфиденциальности медицинских информационных систем, имеющих облачную архитектуру. Полученные результаты могут служить основой для исследований в различных областях и направлениях информационной безопасности: исследование свойств безопасности криптографических средств и алгоритмов защиты информации, разработка, оценка и анализ алгоритмов защиты информации в облачных вычислениях. Кроме того, полученные результаты могут быть использованы при проектировании новых или улучшении действующих распределенных медицинских систем

с целью повышения уровня защищенности данных пациентов (полученных результатов медицинских обследований: ЭЭГ, ЭМГ, ЭКГ, ФПГ, КГР и др.), что играет ключевую роль для улучшения сферы отечественной медицины.

Практическая значимость работы состоит в том, что полученные в ходе исследования результаты могут быть использованы при проектировании и разработке медицинских информационных систем с учетом обеспечения безопасного хранения данных. Использование разработанного метода позволяет снизить количество угроз со стороны злоумышленников и обеспечить защиту информации, циркулирующей в распределенной медицинской системе, построенной на основе современных криптографических протоколов, что играет важную роль в обеспечении информационной безопасности.

В ходе разработки метода защиты конфиденциальных данных и проведенных экспериментальных исследованиях получены новые научные результаты, подтверждающие эффективность применения предложенного метода на основе схемы разделения секрета по сравнению с использованием защиты без использования разработанного метода. Количество угроз в рамках медицинской системы может быть снижено на 45% по сравнению с состоянием системы до внедрения предлагаемого метода.

Полученные практические результаты и универсальность метода обеспечения безопасности медицинских данных позволяют использовать предлагаемый метод и программно-технические решения, основанные на нем, при разработке новых алгоритмов и подходов к защите информации в текущих условиях активной цифровизации сферы здравоохранения и импортозамещения в отечественной медицине.

Научные положения, выносимые на защиту:

1. Метод обеспечения безопасности, использующий протокол разделения секрета на основе схемы Шамира, позволяет распределить фрагменты секрета (файла медицинского обследования) между серверами и как следствие усложнить процедуру компрометации файла, поскольку для восстановления исходного файла требуется собрать фрагменты секрета в единый файл. Использование разработанного метода защиты медицинских данных позволяет снизить количество угроз безопасности в медицинской системе на 45%.
2. Архитектура облачной медицинской распределенной системы имеет возможность функционировать с использованием разработанного метода обеспечения безопасности, включающего в себя: определенную конфигурацию серверов, необходимых для распределения фрагментов файла, алгоритмы и способы формирования ключей, а также процедуру разделения и объединения конфиденциальных файлов согласно схеме Шамира. Архитектура позволяет работать как с классическими форматами представления файлов, так и с медицинскими файлами (DICOM, Nifti, NRRD). Имеется возможность интеграции с различными медицинскими информационными системами посредством использования протокола HL7 – health level 7.
3. Алгоритм оценки времени работы протокола разделения секрета с применением библиотеки MPI позволяет получить результаты сокращения времени для процедуры разделения файла на фрагменты и восстановления фрагментов файла в исходное состояние.

Достоверность результатов диссертационной работы подтверждается результатами проведенных экспериментов, корректным использованием математического аппарата, а также большим количеством научных публикаций и обсуждением основных положений со специалистами на научных конференциях.

Внедрение результатов работы. Результаты диссертационных исследований, подтвержденные соответствующими актами, используются в:

1. Научно-производственной деятельности ООО «СиВижинЛаб» (г. Таганрог), а именно: выполнена апробация метода обеспечения безопасности конфиденциальной информации в рамках собственной МИС, разработанной в организации;
2. Научно-производственной деятельности ООО «Нейротех» (г. Таганрог), а именно выполнена интеграция авторского метода в подсистему безопасности в рамках информационной системы одного из пилотных проектов компании.
3. Научно-производственной деятельности ООО «Инженерный центр Интегра» (г. Таганрог), а именно апробация результатов проведенных исследований в рамках внутренних задач компании.
4. В учебно-исследовательском процессе на кафедре безопасности информационных технологий имени О.Б. Макаревича ИКТИБ ЮФУ.

Апробация результатов

Основные результаты работы докладывались и обсуждались на 9 научных конференциях:

1. VIII всероссийская молодежная школа-семинар по проблемам информационной безопасности «ПЕРСПЕКТИВА-2019», 12 октября 2019 г., г. Таганрог;
2. Всероссийская научно-практическая конференция «Синтез науки и образования в решении глобальных проблем современности», 29 мая 2020 г., г. Таганрог;
3. Международная научно-практическая конференция «Совершенствование методологии и организации научных исследований в целях развития общества», 29 декабря 2020 г., г. Новосибирск;
4. Международная научно-практическая конференция «Внедрение результатов инновационных разработок: проблемы и перспективы», 12 января 2021 г., г. Челябинск;
5. LIV международная научно-практическая конференция «World science: problems and innovations», 30 мая 2021 г., г. Пенза.
6. SinConf 2021 the 14th International Conference on Security of Information and Networks, декабрь 2021 г., г. Эдинбург;
7. III международная научно-практическая конференция «Информационно-психологическая безопасность личности», 15 апреля 2022 г., г. Махачкала.
8. XII всероссийская научно-практическая конференция «Проблемы передачи информации в инфокоммуникационных системах», май 2022 г., г. Волгоград.
9. XIII всероссийская научно-практическая конференция «Проблемы передачи информации в инфокоммуникационных системах», май 2023 г., г. Волгоград.

Публикации. Основные положения диссертации опубликованы в 20 научных печатных работах, в том числе: 4 – в ведущих рецензируемых научных журналах,

входящих в перечень ВАК РФ (1 из которых входит в базу RSCI), 3 – в научных рецензируемых изданиях, индексируемых в базе Scopus, 13 – в материалах конференций и других изданиях. Получено 1 свидетельство о государственной регистрации программы для ЭВМ.

Соответствие паспорту специальности. Диссертация соответствуют паспорту научной специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность»: п. 5 «Методы, модели и средства (комплексы средств) противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет» и п. 15 «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности».

Личный вклад автора. Основные научные результаты, в том числе разработка метода обеспечения безопасности конфиденциальной информации в распределенной медицинской облачной системе на основе схемы Шамира, рекомендации и обоснование выбора схемы разделения секрета, а также проведенные экспериментальные исследования получены автором лично. Вклад соавторов ограничивался постановкой задач на исследования и обсуждением полученных результатов.

Связь работы с научными программами, темами, грантами.

Исследования выполнялись при поддержке РФФИ в рамках научного проекта № 20-37-90138 – «Аспиранты 2020» на тему «Разработка и реализация алгоритмов обеспечения безопасности конфиденциальной информации в распределенной медицинской облачной системе».

Объем и структура диссертационной работы. Диссертация написана на русском языке, состоит из введения, пяти глав, заключения, списка используемой литературы из 94 наименований и 3 приложений. Полный объём диссертации составляет 146 страниц (в том числе приложения 28 стр.), включая 11 рисунков и 18 таблиц.

Содержание работы

Во введении обоснована актуальность темы диссертации, определен объект исследования, сформулированы цель и задачи работы, показаны методы исследования, определена научная новизна, практическая и теоретическая ценность полученных результатов, приведены научные результаты, выносимые на защиту.

В первой главе представлен обзор подходов к обеспечению защиты конфиденциальных данных в распределенных информационных системах, а также направления развития таких подходов. В первую очередь проведен анализ исследований других авторов в рассматриваемой предметной области. Отмечены преимущества и недостатки наиболее известных методов и алгоритмов, использующихся для обеспечения безопасности данных в информационных системах. Продемонстрирована целесообразность использования протоколов разделения секрета при разработке метода обеспечения безопасности конфиденциальных данных с целью улучшения защиты информации, повышения защищенности результатов медицинских исследований от угроз несанкционированного доступа со стороны злоумышленников.

Обоснована разработка метода обеспечения безопасности с использованием протокола разделения секрета и проведен обзор наиболее эффективных схем, которые могут быть использованы для разделения файла на фрагменты и восстановления исходного файла в рамках предлагаемого метода защиты данных.

Сформулированы частные задачи, решением которых достигается цель исследования.

Во второй главе представлена архитектура медицинской облачной информационной системы, которая выступает в качестве объекта защиты.

Общая схема облачной информационной системы продемонстрирована на рисунке 1. Данные, которые находятся в экосистеме могут использоваться как медицинскими, так и исследовательскими организациями, а платформа способна выполнять задачу цифровизации бизнес-процессов за счет упрощения доступа специалистов к информации (сервисы телемедицины, SaaS-сервисы, автоматизированные системы поддержки принятия решения) и научно-исследовательскую задачу (исследование алгоритмов обеспечения защиты информации, анализ больших объемов данных различных типов обследований).

Функционал облачной информационной системы включает следующие возможности:

1. Предоставление удобных инструментов для передачи данных между пользователями системы.
2. Наличие графического интерфейса для упрощения процесса коммуникации между компонентами системы.
3. Общая база данных для исследовательской системы анализа.
4. Возможность создания интерфейсов для интеграции в существующие медицинские информационные системы.
5. Облачный сервис (SaaS) для хранения, классификации и обработки данных, созданных с помощью различного оборудования с поддержкой множества популярных форматов данных.
6. Подсистема обеспечения защиты результатов обследований с использованием разработанного метода обеспечения безопасности данных.

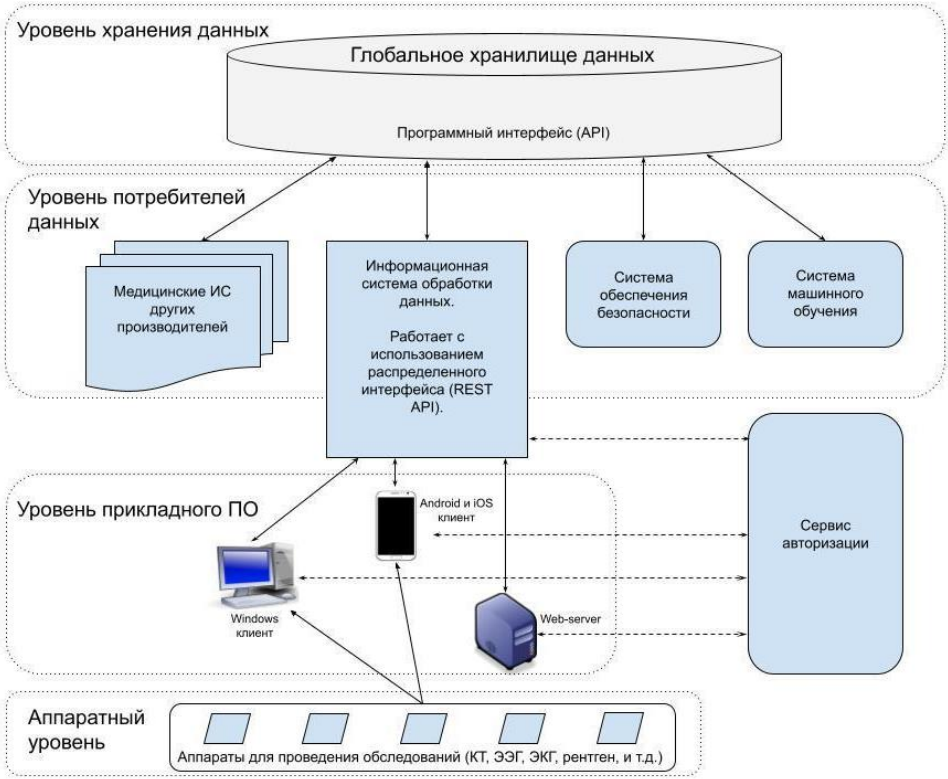

Рисунок 1 – Общая схема организации модулей платформы

Архитектура медицинской системы состоит из четырех основных уровней, которые используются для обработки данных. Иерархическое разделение потоков данных на уровни, стандартизация протоколов передачи данных и форматы их хранения обеспечивают создание универсальной и гибкой медицинской информационной системы.

Уровень хранения данных – представляет собой глобальное хранилище конфиденциальных данных, которое включает в себя базу данных для хранения необработанных обследований и отчетов, а также диагностическую, информацию о пациентах с учетом персональных данных. Таким образом хранилище содержит полный объем информации для исследований, а идентификация пациентов выполняется по защищенному идентификатору.

Уровень потребителей данных включает системы, которые принимают и обрабатывают данные из глобального хранилища или передают в него новые данные. Этот уровень связан с уровнем хранения данных через стандартизированный программный интерфейс. Ядром платформы является *информационная система обработки данных*, которая реализует управление потоками информации, логику групп и ролей, обеспечивает взаимодействие с клиентскими приложениями, используя распределенный интерфейс (REST API). Важной особенностью на данном уровне является подсистема защиты, которая

представляет собой выполнение предложенного в диссертации метода обеспечения защиты медицинских данных.

Уровень прикладного ПО содержит программные средства клиентов, где формируются и отображаются медицинские данные (обследования в виде сигналов, отчетные и персональные данные пациента). Сюда входит программное обеспечение для ОС семейства Windows, Linux, клиенты на базе мобильных устройств, веб-сервисы.

Уровень аппаратных средств включает в себя физические устройства, используемые для проведения медицинских обследований: электроэнцефалографы, кардиографы, портативные устройства и т. д.

Являясь ядром платформы, *информационная система обработки данных* взаимодействует с прикладными приложениями с помощью REST API запросов. Доступ пользователей к системе осуществляется с помощью модуля авторизации, который получает шифрованный токен от внешнего сервиса авторизации и сравнивает его с токеном, полученным от пользователя. Информационная система обработки данных в общем случае может состоять из параллельно работающих виртуальных узлов, обеспечивающих работу со своим пулом пользователей. Центральным элементом информационной системы обработки данных является *менеджер управления*, который отрабатывает запросы пользователей и запросы интерфейсных модулей. Менеджер управления также обеспечивает подготовку данных к сохранению в глобальном хранилище данных.

Третья глава посвящена обоснованию выбора схемы разделения секрета, а также описанию проведенных экспериментальных исследований.

Используя различные схемы разделения секрета: Шамира, Асмута-Блума, Блэкли и Карнин-Грин-Хеллмана, были проведены эксперименты для выбора подходящей схемы для дальнейшего использования в предлагаемом методе обеспечения безопасности. В главе также рассматривается основная идея схемы Шамира и фазы.

Схема Шамира позволяет реализовать (k, n) пороговое разделение секрета между n сторонами так, чтобы только любые k и более сторон ($k < n$) могли восстановить секрет. При этом любые ($k-1$) и менее сторон не смогут восстановить секрет.

Идея схемы заключается в том, что для интерполяции многочлена степени $k-1$ необходимо k точек. Интерполяция невозможна если известно меньшее число точек. Если требуется разделить секрет между n людьми таким образом, чтобы восстановить его могли только k человек ($k \leq n$), он скрывается в формулу многочлена степени $k-1$. Восстановить этот многочлен и исходный секрет можно только по k точкам.

Важным достоинством схемы Шамира является то, что она легко масштабируема. Чтобы увеличить число пользователей, необходимо добавить соответствующее число несекретных элементов к существующим. В то же время компрометация одной части секрета переводит схему из (k, n) пороговой в $(k-1, n-1)$ пороговую. Реализация алгоритма по схеме Шамира состоит из трех фаз:

1. *Подготовительная фаза.*

Доверенный сервер определяет коэффициенты $a_{k-1}, a_{k-2}, \ldots, a_1$ случайным образом, а также выбирается p – простое число, которое больше, чем m. Число p доступно всем участникам, оно задает конечное поле размера p. Над этим полем строится многочлен степени $k-1$ (случайно выбираются все коэффициенты многочлена кроме m):

$$f(x) = (m + a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots + a_1 x)\ mod\ p\ ,$$

где m – разделяемый секрет (файл с обследованием), $a_{k-1}, a_{k-2}, \ldots, a_1$- некоторые случайные числа.

2. *Генерация долей секрета.*

Каждый участник получает свою долю секрета (значения построенного многочлена в *n* различных точках, важно отметить, что $x \neq 0$).

$$k_1 = f(1) = (m + a_{k-1}1^{k-1} + a_{k-2}1^{k-2} + \cdots + a_1 1)\ mod\ p$$
$$k_2 = f(2) = (m + a_{k-1}2^{k-1} + a_{k-2}2^{k-2} + \cdots + a_1 2)\ mod\ p$$
$$\ldots$$
$$k_n = f(n) = (m + a_{k-1}n^{k-1} + a_{k-2}n^{k-2} + \cdots + a_1 n)\ mod\ p$$

Каждой стороне, участвующей в разделении секрета, выдаётся доля секрета k_i вместе с номером *i*. Помимо этого, всем сторонам сообщается степень многочлена *k-1* и размер поля *p*. Случайные коэффициенты $a_{k-1}, a_{k-2}, \ldots, a_1$и сам секрет *m* далее не требуются.

3. *Восстановление секрета.*

Любые *k* участников, зная координаты *k* различных точек многочлена, смогут восстановить многочлен и все его коэффициенты, включая последний из них — разделяемый секрет.

Особенностью схемы является то, что вероятность раскрытия секрета в случае произвольных *k-1*долей оценивается как p^{-1}. То есть в результате интерполяции по *k-1* точке секретом может быть любой элемент поля с равной вероятностью. Попытка полного перебора всех возможных долей не позволит злоумышленникам получить дополнительную информацию о секрете. Чтобы восстановить секрет, можно воспользоваться интерполяционной формулой, например формулой Лагранжа.

В таблице 1 продемонстрированы результаты проведенного эксперимента по анализу ресурсоемкости в процессе вычислений для файла, состоящего из 256 символов. В качестве рабочей станции использовался персональный компьютер на ОС Ubuntu 20.04 с характеристиками: Intel Core i7-11800H, ядра: 8 x 2.3 ГГц, ОЗУ 16 ГБ, SSD 500 Гб.

Таблица 1 – Анализ ресурсоемкости в процессе вычислений

Схема разделения секрета	**Шамира**	**Асмута-Блума**	**Карнин–Грин Хелмана**	**Блэкли**
Разделение секрета на доли	*24 Кб*	*56 Кб*	*80 Кб*	*1 Мб*
Восстановление долей секрета	*112 Кб*	*319 Кб*	*82 Кб*	*1 Мб*

Под ресурсоемкостью понимается количество потребляемой оперативной памяти при выполнении операций разделения и восстановления секрета. Оперативная память серверов является одним из нагруженных ресурсов (в контексте использования ресурсов

различными потребителями), потому что любой процесс, запущенный на сервере, обращается к памяти и использует некоторую ее часть в своих целях. Именно поэтому важно выбрать такую схему, которая потребляла бы минимальное количество оперативной памяти, но в то же время без ущерба в контексте безопасности.

Измерения представленные в таблице 2 демонстрируют сравнение времени быстродействия среди трех основных схем разделения секрета при выполнении операций для параметра *N*, который определяет возможное количество участников в пороговой схеме разделения (количество серверов) и параметра *K*, который используется для операции восстановления секрета и задает необходимое пороговое количество участников коалиции. Параметр *K* представляет собой численное значение фрагментов файла, которое достаточно собрать воедино для восстановления исходного состояния файла. Важно учесть, что условие $K \leq N$ всегда выполнимо.

Таблица 2 – Сравнение характеристик схем (DICOM 8192 Кб)

	Параметры												
Схемы	**Пар-ры схем**	**N = 5**	**K = 4**	**M = 8192**	**N = 10**	**K = 8**	**M = 8192**	**N = 25**	**K = 20**	**M = 8192**	**N = 50**	**K = 40**	**M = 8192**
Шамира	Разделение (мс)	7,32			7,5			9,2			21,9		
	Восстановление (мс)	1,26			1,72			2,76			7,2		
Асмута-Блума	Разделение (мс)	150,7			221,82			1206,11			1653,58		
	Восстановление (мс)	1,33			2,29			4,56			25		
Карнин – Грин - Хелмана	Разделение (мс)	21,95			260,81			1333,32			6933,1		
	Восстановление (мс)	1,18			134,32			776,3			4039,78		

Результаты проведенного эксперимента на примере DICOM файла показали, что использование схемы Шамира является наилучшим решением, поскольку при разделении файла на различное количество частей и восстановлении частей в единый файл для данной схемы потребовалось меньше времени. Также схема Шамира зарекомендовала себя при оценке времени в случае использовании различных типов и размеров файлов.

В таблице 3 приведено сравнение времени основных операций на примере текстового файла размером 1024 Кб. Такое сравнение было необходимо чтобы убедиться в том, что время выполнения основных операций (разделение файла на фрагменты и восстановление фрагментов обратно) имеет зависимость от размера исходного файла.

Таблица 3 – Сравнение характеристик (TXT 1024 Кб)

Схемы	Пар-ры схем	Параметры											
		N = 5	K = 4	M = 8192	N = 10	K = 8	M = 8192	N = 25	K = 20	M = 8192	N = 50	K = 40	M = 8192
Шамира	Разделение (мс)	2,96			2,95			3,86			8,99		
	Восстановление (мс)	Менее 1			Менее 1			Менее 1			2,93		
Асмута-Блума	Разделение (мс)	61,85			84,96			475,56			681,2		
	Восстановление (мс)	Менее 1			Менее 1			1,82			9,67		
Карнин – Грин - Хелмана	Разделение (мс)	8,43			104,9			548,7			2891,71		
	Восстановление (мс)	Менее 1			55,66			313,26			1696,9		

Визуализация различий во времени выполнения операций наглядно демонстрируется на рисунке 2. Стоит отметить, что на рисунке 2 отражена ситуация для разделения файла на 10 фрагментов. Случай, рассмотренный в эксперименте с разделением файла на 50 фрагментов, демонстрирует еще большую разницу по времени (по схеме Шамира операции выполняются в десятки раз быстрее, чем по схеме Асмута-Блума и в сотни раз быстрее, чем по схеме Карнин-Грин-Хеллмана).

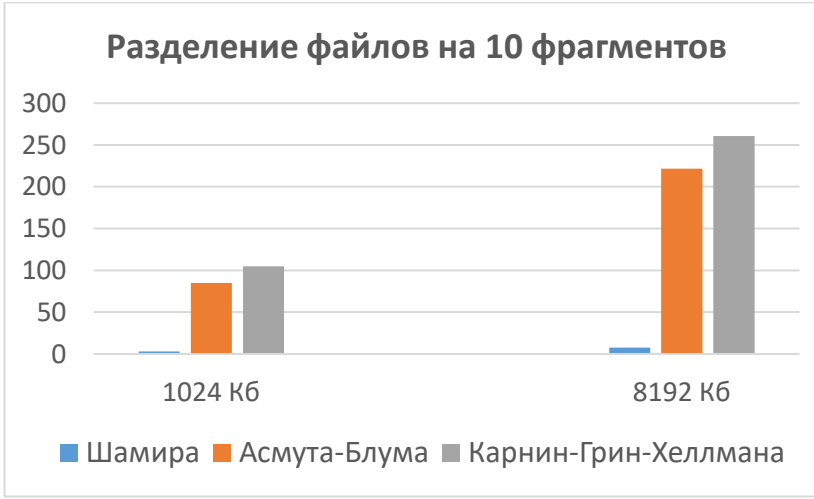

Рисунок 2 – Время (мс) выполнения операции разделения файла на 10 фрагментов для различных схем

Помимо экспериментов, посвященных замерам времени работы, был проведен анализ безопасности предлагаемого метода с помощью анализатора безопасности криптографических протоколов Avispa, при использовании различных схем разделения секрета. Метод, реализованный на основе протокола разделения секрета Шамира, был протестирован в программной среде анализатора с применением формализованного языка интерпретации протоколов. В процессе эксперимента анализировались следующие основные действия:

1. Отправка исходного медицинского файла на сервер.
2. Хранение файла на сервере.
3. Разделение файла на фрагменты по схеме Шамира.
4. Передача фрагментов файла на распределенные сервера.
5. Восстановление исходного файла из фрагментов.
6. Получение исходного медицинского файла и скачивание на рабочую станцию пользователя.

Для того, чтобы получить количественное значение параметра безопасности и определить эффективность системы защиты до и после внедрения метода защиты были выполнены следующие действия:

1. С помощью анализатора подсчитано общее количество шагов от момента передачи сообщения (файла) между всеми сторонами (получателями) до конечного адресата.
2. Подсчитано количество unsafe ответов (небезопасных шагов) с точки зрения анализатора безопасности протоколов.
3. Найдено процентное соотношение количества небезопасных шагов к общему количеству. Выполнено сравнение значений до и после применения предлагаемого метода защиты.

Процедура передачи конфиденциальной информации от исходного пользователя системы (роль – лаборант) к другому пользователю (роль – специалист) без использования предлагаемого метода состоит из 6 основных шагов (авторизация пользователя посредством логина и пароля с последующей передачей файла медицинского обследования на сервер), а при использовании предложенного метода, с учетом применения схемы Шамира, количество шагов увеличивается до 14 в виду необходимости выполнения дополнительных операций, таких как шифрование файла, разделение на фрагменты, пересылка фрагментов, расшифрование. В результате получены следующие результаты. До внедрения метода на 4 из 6 шагов были определены угрозы. Исходя из описанного алгоритма формализованной оценки эффективности системы защиты получено значение: $\left(1 - \frac{4}{6}\right) * 100\% = 33\%$.

Аналогичный анализ системы после внедрения предлагаемого метода продемонстрировал 3 угрозы. Учитывая общее количество шагов получено следующее значение: $\left(1 - \frac{3}{14}\right) * 100\% = 78.5\%$.

По результатам экспериментов определено, что после внедрения метода защиты данных количество возможных угроз системы снижается на 45%. Таким образом, предлагаемый метод обеспечения безопасности данных с использованием схемы Шамира может быть применен в качестве основы системы защиты данных в облачной медицинской

информационной системе.

Четвертая глава посвящена разработке метода обеспечения защиты конфиденциальных данных в облачной медицинской информационной системе.

Конфиденциальная информация поступает в МИС на этапе проведения медицинского обследования пациентов при помощи различного оборудования. После этого появляется файл, содержащий интерпретацию проведенного обследования в машиночитаемом формате. Иными словами, происходит формирование файла с «сырыми данными», например серия снимков компьютерной томограммы внутренних органов человека в формате DICOM. Затем файл передается от одного пользователя системы к другому на рабочий компьютер для дальнейшего анализа. Таких итераций может быть множество, в зависимости от количества назначенных процедур.

Существует промежуточный этап, когда файл с обследованием отправлен от одного пользователя, но еще не получен другим. В таком случае информация находится на серверах в виде зашифрованных фрагментов файла, полученных посредством применения протокола разделения секрета. Файл, содержащий конфиденциальную информацию, подвергается разделению на фрагменты, каждый из которых шифруется, а затем отправляется на сервера для хранения до получения запроса на скачивание от какого-либо участника МИС. После того, как пользователь делает запрос на получение обследования он устанавливает сеанс с одним из серверов, на котором лежит фрагмент файла и далее собирает воедино исходный файл с обследованием. Таким образом у специалиста появляется возможность скачать файл на свой локальный компьютер для дальнейшей работы (изучения/постановки диагноза и т.д.).

Общая схема процесса перемещения данных в рамках МИС (для существующих ролей) представлена на рисунке 3.

Предлагаемый метод обеспечения защиты медицинских данных охватывает все шаги, представленные на схеме, и может применяться для любого количества шагов. То есть при добавлении в систему дополнительных пользователей (ролей) использование метода остается полностью целесообразным.

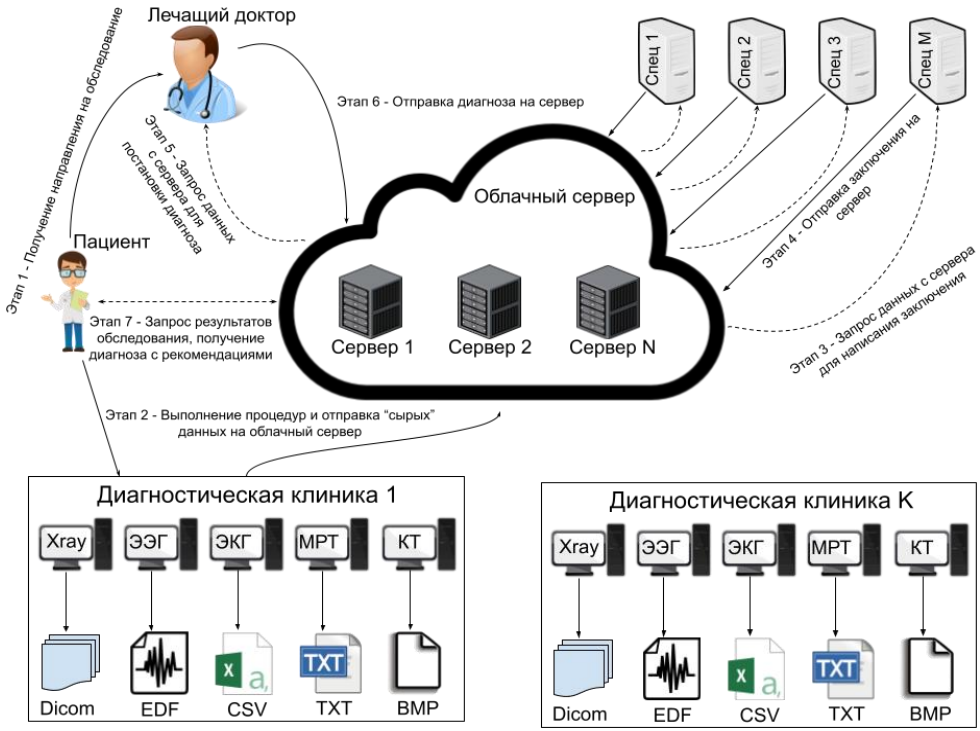

Рисунок 3 – Общая схема циркулирования данных в облачной МИС

Предлагаемый метод направлен на выполнение определенной последовательности действий, одним из которых является выполнение протокола разделения секрета, работающего по схеме Шамира, которая была определена как наиболее эффективная по результатам экспериментальных исследований, представленных в главе 3.

Метод обеспечения защиты медицинских данных состоит из этапов шифрования и расшифрования файла, а также выполнения операций по разделению файла на фрагменты для их хранения на серверах и восстановлению исходного файла при обращении со стороны пользователя.

Шифрование файла обследования и передача частей файла на сервера для последующего хранения:

1. Присвоение уникального идентификатора каждому пациенту для анонимизации.
2. Шифрование результатов обследования и загрузка на сервер. Отправитель результатов обследования формирует отдельный файл **F** (DICOM, JSON, DOC, CSV, EDF, BMP и т.д.) с «сырыми данными» обследования и осуществляет его шифрование, а затем отправляет на сервер в соответствии с определенным алгоритмом:

2.1. Формируется общий ключ (одноразовый сеансовый) отправителя с одним из серверов, выбранным **случайным образом**. Выработка общего ключа производится каждой из сторон по протоколу Диффи-Хеллмана.

2.2. Локально выполняется шифрование файла обследования на общем ключе отправителя и случайно выбранного сервера, а затем передача этого файла в зашифрованном виде на этот сервер.

2.3. Случайный сервер, используя общий с отправителем ключ, осуществляет расшифрование файла, полученного от отправителя. Затем расшифрованный файл разделяется на фрагменты по схеме Шамира.

$$F = F_1 + F_2 + ... + F_N$$

2.4. Случайный сервер зашифровывает своим секретным симметричным ключом и оставляет для хранения у себя один из фрагментов файла. Остальные фрагменты файла передаются всем оставшимся свободным серверам: устанавливается связь с оставшимися серверами, осуществляя процедуру верификации (проверка подлинности на предмет «свой-чужой») по протоколу взаимного рукопожатия.

3. Каждый из серверов, получив свой фрагмент файла, выполняет расшифрование, используя сеансовый ключ (общий с сервером, выбранным случайным образом на шаге 2.1).

4. Затем, каждый из серверов зашифровывает расшифрованный фрагмент файла своим секретным ключом для дальнейшего хранения.

Соединение частей файла и расшифрование (скачивание с сервера) для последующего анализа и постановки заключения.

1. Получатель файла выполняет запрос к серверу, выбранному случайным образом на получение файла с обследованием.

2. Сервер, получив запрос от пользователя, расшифровывает фрагмент файла обследования своим секретным ключом. Для получения остальных фрагментов файла обследования сервер, выбранный случайным образом на шаге 1, устанавливает связь с оставшимися серверами, осуществляя процедуру верификации (проверка подлинности на предмет «свой-чужой») по протоколу взаимного рукопожатия.

3. Сервер, случайно выбранный на шаге 1, получив оставшиеся фрагменты файлов от остальных серверов, расшифровывает эти фрагменты с помощью одноразовых сеансовых ключей, соответствующих определенным фрагментам файла (и серверам).

4. Затем сервер осуществляет восстановление исходного файла обследования с использованием фрагментов, расшифрованных на предыдущем шаге. Восстановление выполняется по схеме Шамира.

5. Далее выбранный сервер устанавливает связь с получателем для шифрования файла обследования с целью дальнейшей передачи получателю.

6. Получатель, скачав зашифрованный файл обследования, расшифровывает его с использованием общего ключа (своего и сервера).

Таким образом, после выполнения всех шагов описанного метода файл с медицинским обследованием проходит процедуру отправки на сервер, разделение на фрагменты, шифрование фрагментов с последующей передачей на свободные сервера, а затем скачивание на локальный компьютер специалиста для проведения анализа. В конечном итоге файл с медицинским обследованием, а также заключения и рекомендации от врача попадают к пациенту по аналогичному сценарию и являются защищёнными, с точки

зрения информационной безопасности на всех этапах в рамках медицинской информационной системы. При попытке компрометации какой-либо из долей (или нескольких долей) файла – эти данные не представляют никакой ценности, поскольку распределены между N серверами и только при наличии определенного количества (пороговое значение, которое задается на этапе разделения исходного файла на фрагменты) расшифрованных долей секрета можно получить доступ к исходному файлу.

В пятой главе описано моделирование распараллеливания операций разделения и слияния долей секрета по схеме Шамира с использованием библиотеки MPI. Была выполнена оценка времени разделения файла на фрагменты и слияние фрагментов обратно в единый файл. Результаты эксперимента показали, что можно добиться почти линейного ускорения и сократить время генерации 255 долей файла в 1,87 раза, а время восстановления этих долей обратно в единый файл в 1,74 при работе в многопоточном режиме. Эксперимент был проведен на локальном компьютере, имеющем характеристики: 16 ГБ ОЗУ, Intel Core i7 – 11800H: 8-ядер по 2,3 ГГц с гиперпоточностью до 16 потоков.

В таблице 4 показаны результаты масштабирования, при которых время создания долей секрета уменьшается почти вдвое каждый раз, когда удваивается количество потоков.

Таблица 4 – Время, необходимое для генерации 255 долей секрета

Кол-во потоков	**1000 – символьный файл**	**2000 - символьный файл**
1	8.42 мс	17.53 мс
2	4.44 мс	9.02 мс
4	2.35 мс	5.23 мс
8	1.3 мс	2.98 мс
16	0.7 мс	1.58 мс

Были получены аналогичные результаты при объединении долей секрета для восстановления исходного секрета, что демонстрируется в таблице 5. Важно отметить, что при 16 потоках происходит увеличение времени. Это соответствует количеству гиперпотоков ядер на тестовой рабочей станции (восемь ядер с шестнадцатью гиперпотоками). На этом этапе увеличение количества потоков становится контрпродуктивным, поскольку они не могут выполняться параллельно на таком оборудовании, однако тенденция с сокращением времени при увеличении числа потоков также подтверждается.

Таблица 5 – Время, необходимое на восстановление 255 долей секрета

Кол-во потоков	**1000 – символьный файл**	**2000 - символьный файл**
1	1.48 мс	3.02 мс
2	0.75 мс	1.6 мс
4	0.4 мс	0.93 мс
8	0.29 мс	0.69 мс
16	0.33 мс	0.62 мс

В таблице 6 продемонстрированы результаты для «одновременного масштабирования», при котором увеличивалось как количество потоков, так и количество символов тестового файла. В этом эксперименте стоит обратить внимание на время, которое не увеличивается пропорционально.

Таблица 6 – Изменение времени при генерации долей секрета с одновременным удвоением количества символов и потоков

Кол-во потоков	Количество символов	Время
1	500	4.53 мс
2	1000	4.65 мс
4	2000	5.17 мс
8	4000	5.66 мс
16	8000	7.13 мс

Заключение

В результате диссертационного исследования было предложено решение актуальной научной задачи и достигнута поставленная цель, заключающаяся в повышении эффективности обеспечения безопасности распределенных медицинских облачных систем за счет разработки и внедрения метода обеспечения защиты конфиденциальных данных.

1. Разработан метод защиты медицинских данных, использующий протокол разделения секрета на основе схемы Шамира. Метод применяется в рамках облачной информационной системы для обеспечения безопасности файлов обследований. Экспериментально подтверждено, что использование разработанного метода защиты позволяет снизить уровень угроз при обработке файлов медицинских обследований в распределенной информационной системе на величину 45% по сравнению с традиционными способами обеспечения безопасности.

2. Разработана архитектура облачной медицинской распределенной системы, которая может работать с использованием предложенного метода, включающего в себя определенную конфигурацию серверов, каналы связи между пользователями и серверами, способы формирования ключей шифрования для обеспечения безопасности передаваемых фрагментов файла, а также процедуру разделения конфиденциальных данных на фрагменты согласно схеме Шамира с последующим восстановлением фрагментов в исходный файл. Архитектура медицинской системы разработана с учетом поддержки как классических форматов файлов, содержащих информацию об обследовании, так и медицинских файлов в форматах DICOM, Nifti, NRRD.

3. Разработан алгоритм оценки сокращения времени при распараллеливании с применением библиотеки MPI выполнения основных операций – разделение секрета на фрагменты и восстановление фрагментов секрета по схеме Шамира. Результаты экспериментов продемонстрировали, что при параллельной реализации схемы время для разделения файла на 255 частей сократилось в 1,87 раза, а для восстановления долей в 1,74 раза при работе в многопоточном режиме на рабочей станции, имеющей характеристики: 16 ГБ ОЗУ, Intel Core i7 – 11800H (8-ядер по 2,3 ГГц с гиперпоточностью до 16 потоков).

4. Получено свидетельство о государственной регистрации программы для ЭВМ из Роспатента.

5. Результаты проведённых диссертационных исследований могут найти применение:

- при разработке и проектировании распределенных медицинских информационных систем, систем обеспечения безопасного хранения персональных данных;
- при обеспечении защиты информации, в распределенной медицинской системе.

Публикации автора по теме диссертации

В рецензируемых журналах из перечня ВАК РФ

1. Бабенко, Л. К. Использование параллельных вычислений для реализации метода обеспечения безопасности на основе схемы Шамира в медицинской информационной системе / Л. К. Бабенко, А. С. Шумилин // Известия ЮФУ. Технические науки. – 2023. – №4(234). – С. 6-13. – DOI 10.18522/2311-3103-2023-4-6-13

2. Шумилин, А. С. Метод обеспечения защиты персональных данных в медицинской облачной системе / А. С. Шумилин // Вопросы кибербезопасности. – 2023. – № 4(56). – С. 53-64. – DOI 10.21681/2311-3456-2023-4-53-64.

3. Бабенко, Л. К. Алгоритм обеспечения защиты конфиденциальных данных облачной медицинской информационной системы / Л. К. Бабенко, А. С. Шумилин, Д. М. Алексеев // Известия ЮФУ. Технические науки. – 2021. – № 5(222). – С. 120-134. – DOI 10.18522/2311-3103-2021-5-120-134.

4. Бабенко, Л. К. Алгоритм обеспечения безопасности конфиденциальных данных медицинской информационной системы хранения и обработки результатов обследований / Л. К. Бабенко, А. С. Шумилин, Д. М. Алексеев // Известия ЮФУ. Технические науки. – 2020. – № 5(215). – С. 6-16. – DOI 10.18522/2311-3103-2020-5-6-16.

В изданиях, индексируемых Scopus и Web of Science

5. Babenko, L. Algorithm of ensuring confidential data security of the cloud medical information system / L. Babenko, A. Shumilin, D. Alekseev // E3S Web of Conferences. – 2020. – Vol. 224. – Article № 03023. – P. 1-8. – DOI 10.1051/e3sconf/202022403023.

6. Development and Testing of the Information Security Protocol in the Medical Cloud Platform / L. Babenko, D. Alekseev, E. Ishchukova, A. Shumilin // CEUR Workshop Proceedings : Advanced in Information Security Management and Applications 2021. 2022. – Vol. 3094. – Article № 3. – P. 35-40.

7. Babenko, L. Development of the algorithm to ensure the protection of confidential data in cloud medical information system / L. Babenko, A. Shumilin, D. Alekseev // Proceedings – 2021 14th International Conference on Security of Information and Networks. – 2021. – P. 1-4. – DOI 10.1109/SIN54109.2021.9699356.

В прочих изданиях

8. Алексеев, Д. М. Обеспечение защиты конфиденциальной информации в медицинской облачной системе с использованием пороговой гомоморфной криптосистемы с открытым ключом / Д. М. Алексеев, А. С. Шумилин // Вестник современных исследований. – 2021. – № 5-9(43). – С. 4-8.

9. Система автоматического поиска участков эпилептической активности в составе облачной платформы хранения, систематизации и обработки медицинских данных /

Д. М. Алексеев, А. Н. Минюк, З. А. Понимаш, А. С. Шумилин // Современные наукоемкие технологии. – 2019. – № 1. – С. 14-19.

10. Ансамбль классификаторов: реализация, оценка эффективности и интеграция в облачную платформу хранения, систематизации и обработки медицинских данных / Д. М. Алексеев, А. Н. Минюк, З. А. Понимаш, А. С. Шумилин // Современные наукоемкие технологии. – 2019. – № 9. – С. 20-25

11. Разработка и описание структуры и функционала облачной платформы хранения, систематизации и обработки медицинских данных: интеграция системы автоматического поиска участков эпилептической активности / Д. М. Алексеев, А. Н. Минюк, З. А. Понимаш, А. С. Шумилин // Системы управления и информационные технологии. – 2019. – № 3(77). – С. 52-55.

12. Шумилин, А. С. Метод обеспечения безопасности конфиденциальной информации в распределенной медицинской облачной системе / А. С. Шумилин // Проблемы передачи информации в инфокоммуникационных системах : сборник докладов и тезисов XIII Всероссийской научно-практической конференции, г. Волгоград, 26 мая 2023 г. – Волгоград : Издательство Волгоградского государственного университета, 2023. – С. 82-86.

13. Шумилин, А. С. Разработка алгоритма для обеспечения защиты конфиденциальных данных в МИС с облачной архитектурой / А. С. Шумилин, Д. М. Алексеев // Проблемы передачи информации в инфокоммуникационных системах : сборник докладов и тезисов XII Всероссийской научно-практической, г. Волгоград, 20 мая 2022 г. – Волгоград : Издательство Волгоградского государственного университета, 2022. – С. 15-19.

14. Алексеев, Д. М. Метод защиты информации в распределенной облачной информационной системе здравоохранения / Д. М. Алексеев, А. С. Шумилин // Развитие правового сознания в образовательном пространстве : материалы Международной 9-ой научно-практической конференции, Махачкала, 22 февраля 2022 г. Ч. 1. – Махачкала : Дагестанский государственный педагогический университет, 2022. – С. 92-103.

15. Алексеев, Д. М. Использование пороговой гомоморфной криптосистемы с открытым ключом для защиты информации в медицинской облачной платформе / Д. М. Алексеев, А. С. Шумилин // Интеграция науки, общества, производства и промышленности: проблемы и перспективы : сборник статей по итогам Международной научно-практической конференции, г. Волгоград, 29 мая 2021 г. – Стерлитамак : Агентство международных исследований, 2021. – С. 86-88.

16. Алексеев, Д. М. Облачная медицинская информационная система: защита конфиденциальной информации с использованием порогового гомоморфного шифрования / Д. М. Алексеев, А. С. Шумилин // Проблемы и перспективы разработки инновационных технологий : сборник статей Международной научно-практической конференции, г. Магнитогорск, 1 июня 2021 г. – Магнитогорск ; Уфа : Аэтерна, 2021. – С. 6-8.

17. Алексеев, Д. М. Обзор методов обеспечения безопасности конфиденциальных данных в медицинских информационных системах / Д. М. Алексеев, А. С. Шумилин // Внедрение результатов инновационных разработок: проблемы и перспективы : сборник статей Международной научно-практической конференции, г. Челябинск, 12 января 2021 г. : [в 2 ч.]. Ч. 1. – Челябинск ; Уфа : МЦИИ Омега Сайнс, 2021. – С. 47-49.

18. Алексеев, Д. М. Методы защиты информации при передаче медицинских обследований в облачной платформе / Д. М. Алексеев, А. С. Шумилин // Совершенствование методологии и организации научных исследований в целях развития общества : сборник статей по итогам Международной научно-практической конференции, г. Новосибирск, 29 декабря 2020 г. : [в 2 ч.]. Ч. 2. – Стерлитамак : Агентство международных исследований, 2020. – С. 117-120.

19. Алексеев, Д. М. Методы и подходы к обеспечению конфиденциальности персональных данных в медицинских информационных системах / Д. М. Алексеев, А. С. Шумилин // Научно-технический прогресс как механизм развития современного общества : сборник статей Всероссийской научно-практической конференции, г. Тюмень, 13 января 2021 г. – Тюмень ; Уфа : Аэтерна, 2021. – С. 19-21.

20. Алексеев, Д. М. Защита конфиденциальной информации в облачной медицинской информационной системе / Д. М. Алексеев, А. Н. Минюк, А. С. Шумилин // Инновационная наука. – 2020. – № 6. – С. 32-33.

Свидетельства о государственной регистрации программы для ЭВМ

21. Свидетельство о государственной регистрации программы для ЭВМ № 2023665287 Российская Федерация. Программа для реализации алгоритма защиты результатов обследований пациентов в медицинской информационной системе на основе схемы разделения секрета: №2023663429 : заявл. 28.06.2023 : опубл. 13.07.2023 / А. С. Шумилин, Д. М. Алексеев, Л. К. Бабенко, В. Д. Салманов ; правообладатель Шумилин А. С.