МЕТОД ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В МЕДИЦИНСКОЙ ОБЛАЧНОЙ СИСТЕМЕ

Шумилин А.С.[1]

Задача обеспечения безопасного хранения и передачи данных в информационных системах становится актуальнее с каждым днем, поскольку процессы цифровизации активно внедряются во все сферы деятельности человека. Особое внимание требует медицинская отрасль, а именно – задача обеспечения безопасности данных пациентов, которые являются пользователями медицинских информационных систем (МИС).

Цель работы: *разработка метода обеспечения безопасности при передаче, обработке и хранении персональных данных (ПД) пациентов МИС, построенной по принципу распределенной облачной архитектуры.*

Метод исследования: *анализ возможных способов обеспечения безопасности персональных данных в распределенных информационных системах с использованием протокола разделения секрета. Анализ существующих проблем при реализации методов защиты в облачных системах. Анализ модели злоумышленника и способов атак.*

Результаты: *в рамках проведенного исследования было обосновано использование протокола разделения секрета в качестве основы метода обеспечения защиты персональных данных пациентов в рамках облачной медицинской информационной системы. Среди нескольких кандидатов с аналогичным набором функций была определена оптимальная схема разделения секрета с учетом особенностей поставленной задачи. Выбор схемы был обоснован наличием таких преимуществ, как свойства совершенности, идеальности, а также скорость выполнения основных операций перед другими кандидатами. Проведены эксперименты и получены результаты, которые подтверждают правильность выбора схемы разделения секрета (Шамира). На основе выбранной схемы разделения секрета предложена реализация метода обеспечения безопасности персональных данных пациентов для облачных МИС. Для проверки работы предлагаемого метода авторами предложена архитектура облачной МИС, которая позволяет выполнить интеграцию механизмов защиты.*

Ключевые слова: *шифрование, криптография, безопасность облачных вычислений, защита персональных данных, протокол разделения секрета, информационные системы.*

DOI:10.21681/2311-3456-2023-4-53-64

Введение

Ежедневно во всем мире люди используют компьютерные технологии для достижения различных целей и решения множества сложных задач, а возможность свободного доступа в интернет сделала популярными такие активности, как общение в социальных сетях, поиск практически любой информации, образовательные и развлекательные услуги, выполнение сложных математических расчетов, создание программного обеспечения, а также различные медицинские услуги. Ситуацию с актуальностью и галопирующим развитием информационных технологий обострила, в том числе, пандемия новой коронавирусной инфекции COVID-19 из-за которой большинство сфер деятельности и бизнеса пришлось адаптировать под новые реалии работы и оказания услуг и проводить информатизацию и цифровизацию предприятий [1].

В связи с такими действиями, в настоящее время процессы создания, накопления и обработки информации в различных сферах становятся все более актуальными, но особое внимание стоит уделить именно отрасли здравоохранения, потому что активно начали развиваться медицинские информационные системы, построенные на основе распределенных облачных архитектур. Факт того, что эффективность оказываемой медицинской помощи полностью зависит от оперативности и удобства использования имеющейся у специалистов информации, в рамках медицинских организаций, является лежащим на поверхности и не требует обсуждений. Наличие задач, связанных с

1 Шумилин Александр Сергеевич, аспирант, Южный федеральный университет, Таганрог, Россия. E-mail: ashumilin@sfedu.ru

хранением, систематизацией и обработкой больших объемов данных обуславливает актуальность разработки и интеграции в медицинские учреждения медицинских информационных систем (МИС). Данные в электронном виде позволяют врачам оперативно получать необходимую информации о пациенте, что увеличивает скорость принятия решения, а как следствие процесс постановки диагноза и выбор методов лечения также производятся быстрее.

Медицинские организации в силу законодательства[2] являются операторами персональных данных своих пациентов, поскольку принимают активное участие в сборе, накоплении, хранении, изменении, распространении и уничтожении такой информации.

В рамках исследования ставится задача разработки метода обеспечения безопасности данных пациентов таких медицинских систем, обоснование выбора способа защиты информации, который ляжет в основу предлагаемого метода и проведение экспериментальных исследований.

Актуальность проблемы

Основная проблема при проектировании МИС заключается в необходимости интеграции надёжных систем защиты конфиденциальной информации, поскольку задача обеспечения безопасности составляет основу любой современной медицинской системы. В эпоху популяризации информационных систем, утечки данных вследствие атак хакеров стали одной из главных проблем по отношении к персональным данным пользователей таких систем. Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ регламентирует отношения, связанные с обработкой персональных данных в том числе и в рамках работы внутри МИС. Проблема обеспечения надежной защиты персональных данных в МИС является актуальной как в мировом масштабе, так и в рамках Российской Федерации [2-3], что особенно важно в современных условиях импортозамещения и разработки отечественных систем безопасности.

Статистика за 2020 год демонстрирует, что Россия вышла в лидеры по количеству умышленных утечек из различных информационных систем в рамках мировых инцидентов, а показатель составил 79,7%. Уже в 2022 году в нашей стране атакам подверглись такие крупные компании, как «Яндекс», «1С», «СДЭК», «Ozon», «Инфотекс», «Вкусно и точка», а последствиями стала публикация в открытом доступе сотен миллионов строк с персональными данными граждан страны. Общий рост утечек данных россиян вырос в 40 раз по сравнению с показателями 2021 года[3]. Кроме того, Роскомнадзор подтвердил утечки 600 млн записей о соотечественниках, которые были опубликованы в общий доступ. Суммарно более 140 утечек персональных данных было зафиксировано за период с февраля по декабрь 2022 года.

В доменной области, связанной с медициной, к сожалению, утечки данных тоже являются одной из актуальных проблем. Ситуация осложняется тем, что в руки злоумышленников помимо личных 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. Поскольку популяризация информационных систем для работы в рамках медицинских задач в России еще не так актуальна и только набирает обороты, то объемы утечек [5] в данной области кажутся не сильно большими на фоне аналогичных проблем зарубежных компаний.

После начала кампании по вакцинации населения Российской Федерации от новой коронавирусной инфекции, спустя несколько месяцев, в сети уже были опубликованы данные о 300 тысяч переболевших жителей Москвы. Вслед за этим еще одна утечка – база QR-кодов вакцинированных, а уже в 2023 году в открытый доступ попала база данных с информацией о сотне тысяч клиентов из лабораторий «Ситилаб». По общим подсчетам за 2022 год в нашей стране было похищено более 31 млн записей о пациентах из различных медицинских организаций[4], что составляет более 20% от общего населения России.

Что касается инцидентов в других странах, то подобные ситуации не является исключением. В 2022 году Организация «Shields Health Care Group», которая занимается визуализацией МРТ, КТ, радиологии и амбулаторных хирургических услугах, была подвергнута хакерской атаке, что позволило злоумышленником обойти слабую систему безопасности, вследствие чего была допущена утечка персональных данных более двух миллионов пациентов[5].

2 Федеральный закон «Об основах охраны здоровья граждан в РФ» от 21.11.2011 №323-ФЗ

3 Статистика Роскомнадзора по утечкам данных // https://www.tadviser.ru/index.php/Статья:Роскомнадзор

4 Утечки данных в медицинских учреждениях [Электронный ресурс] // https://zdrav.expert/index.php/Статья:Утечки_данных_в_медицинских_учреждениях

5 Утечка данных Shields Health Care Group // https://xakep.ru/2022/06/08/shields-leak

В мае 2023 года компания «MCNA Denta»l (Managed Care of North America), сообщила о взломе своей информационной инфраструктуры. Киберпреступники украли данные приблизительно о 8,9 млн пациентов[6].

Стоит отметить, что помимо информации, которую можно использовать в качестве шантажа и вымогательств, есть еще один вид полезных данных – медицинские снимки, представляющие огромную ценность для разработчиков алгоритмов машинного обучения. Например, датасеты содержащие снимки компьютерной томографии, рентген и другие способы визуализации крайне сложно найти в открытом доступе. Поэтому, наличие базы данных в несколько миллионов изображений позволяет получить дополнительный канал заработка для злоумышленников и продавать такие изображения заинтересованным компаниям, а сопутствующая информация о персональных данных будет являться подтверждением того факта, что злоумышленник является правообладателем.

Таким образом, проблема безопасности персональных данных в информационных системах, является актуальной на сегодняшний день, в особенности при работе с медицинскими данными [6]. В связи с тем, что требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» установлена необходимость защиты персональных данных пациентов медицинских организаций, важной задачей в МИС является обеспечение безопасности хранимой и передаваемой информации. Среди множества МИС часто встречаются такие системы, в которых вовсе не используются механизмы обеспечения безопасности или используются неподходящие способы, такие как симметричное шифрование данных, основная особенность которого – проблема распределения ключей. Стоит отметить и тот факт, что некоторые компании используют для хранения данных сервера, находящиеся не на территории Российской Федерации (Amazon, Google, Azure и т. д.), что создает брешь в информационной безопасности. Наиболее защищенные системы, в которых применяется асимметричное шифрование, тоже являются уязвимыми, поскольку данные в таких системах шифруются на локальных серверах, а попадают туда по каналу связи в незашифрованном виде.

Что касается распределенных информационных систем, то на сегодняшний день они являются наиболее актуальными для решения задач медицинского обследования населения, поскольку нет необходимости иметь единый сервер и централизованное управление данных, что в домене медицины является весьма важным фактором, ведь централизованное управление может накладывать определенные ограничения на пропускную способность, тем самым замедляя процесс обработки данных, а также считается менее безопасным с точки зрения обработки и хранения персональных данных.

Целью данного исследования является разработка метода обеспечения защиты персональных данных, представляющих конфиденциальную медицинскую информацию, на основе протокола разделения секрета для облачной распределенной системы хранения и систематизации результатов обследований. Преимущества данного метода заключаются в том, что передача данных между серверами будет осуществляться в виде фрагментов секрета (за секрет принимается состоящий на N частей файл обследования), каждый из которых по отдельности не представляет интереса. В качестве криптографического протокола выбран протокол Диффи-Хеллмана, с помощью которого решается проблема выработки общего секретного ключа при использовании незащищенного канала связи.

В основе протокола разделения секрета лежит схема Шамира, которая позволяет реализовать (k, n) — пороговое разделение секретного сообщения (файла медицинского обследования) между n сторонами так, чтобы только любые k и более сторон ($k \leq n$) могли восстановить секрет. При этом любые $k-1$ и менее сторон не смогут восстановить секрет. Визуализация процесса разделения секрета представлена на рисунке 1. Процесс сбора частей секрета в единый фрагмент продемонстрирован на рисунке 2.

В рамках предложенного метода абоненты представляют собой сервера, на которых в последующем будут храниться фрагменты секрета (файла обследования).

Схема Шамира предполагает реализацию на основе полиномиальной интерполяции. Это означает следующее: для того, чтобы обеспечить разделение секрета на n частей, так чтобы его в последующем могли восстановить k абонентов, следует реализовать решение через многочлен степени $k-1$. Процесс восстановления такого многочлена выполняется по k точкам [7].

6 Утечка данных Managed Care of North America // https://zdrav.expert/index.php/Компания:MCNA_Dental

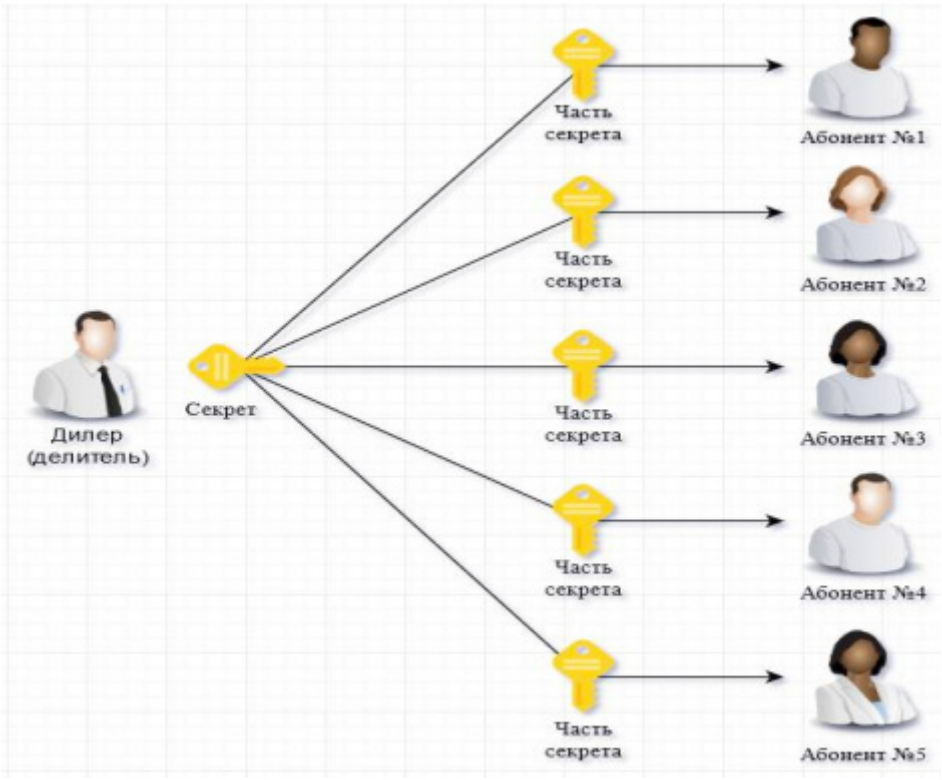

Рис. 1. Процесс разделения секрета на части по схеме Шамира

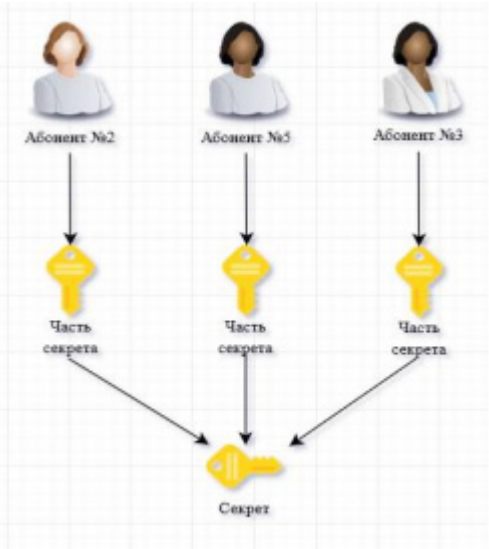

Рис. 2. Процесс сбора частей секрета в единый фрагмент по схеме Шамира

Математическая реализация этапа разделения секрета выглядит следующим образом:

1. На первом шаге выбирается случайное простое число (p).
2. Затем выбирается такое количество коэффициентов k-1, которое необходимо для построения полинома над полем Z_p (размерность простого модуля кольца целых числе)
3. На данном шаге происходит процесс вычисления теней, при котором количество повторений равно n. Каждая новая итерация представлена в виде цикла, который выполняет проход по k-1 координатам.
4. Все абоненты получают доли секрета.

Этап восстановление секрета представляет собой процесс, при котором необходимо построить интерполяционный полином Лагранжа [8].

На пороговые системы существуют атаки, однако лишь при условии, что, в числе k участников имеется нарушитель.

В таком случае возможности обойти пороговую схему могут выглядеть следующим образом:

1. Использование неверной части секрета – в таком случае абоненты не смогут восстановить секрет. Установить, кто именно предоставляет неверную часть невозможно.

2. Нарушитель имеет возможность инициировать процесс разделения секрета, если он сможет доказать, что он является одним из абонентов.

3. В пороговой схеме типа k, n злоумышленник может выдать себя за k+1 участника. Поскольку k участников будет достаточно для восстановления секрета, то нарушитель может выдать под видом своего секрета случайный набор символов. В итоге злоумышлен-

ник получит части секрета остальных абонентов, а затем воссоздаст секрет полностью.

Перечисленные способы атак присущи неидеальным схемам разделения секрета, а также схемам, с низкой ресурсоемкостью.

Обоснование необходимости использования протокола разделения секрета, реализованного по схеме Шамира, в качестве основы метода обеспечения безопасности в рамках медицинских информационных систем обусловлено наличием нерешенной научной задачи, которая была выявлена при анализе работ других авторов.

Использование существующих способов защиты данных в ИС, среди работ авторов [9-11], опубликованных в научной литературе, содержат различные недостатки, такие как: проблема распределения ключей для симметричного шифрования, обеспечение дополнительной безопасности канала связи, а также достаточно строгие требования к времени работы алгоритмов, потреблению памяти и вычислительным ресурсам в целом. Работы авторов, предлагающих подходы с использованием гомоморфного шифрования [12] для решения задачи обеспечения безопасности данных выглядят не применимыми с точки зрения скорости работы алгоритмов, потому что операции выполняются медленно и значительно проигрывают классическим алгоритмам по времени обработки данных. В научной работе [13] автор акцентирует внимание на том факте, что использование только гомоморфного шифрования будет недостаточным для обеспечения безопасности зашифрованного текста, например, при адаптивных атаках с выбранным зашифрованным текстом.

Сама по себе проблема безопасности — основная причина, по которой многие организации не спешат внедрять облачные вычисления, поскольку поставщики облачных услуг сталкиваются с тремя важными юридическими проблемами:

1) Конфиденциальность данных связана с защитой данных клиента, предоставляемых третьей стороной. Нарушение любого письменного договора с третьей стороной может повлиять на конфиденциальность данных клиента.

2) Целостность данных связана с сохранением исходных данных, которые хранятся в различных физических местах на серверах, эксплуатируемых и организациями по всему миру. Ввиду того, что поставщики облачных услуг не могут гарантировать ни защиту данных, которые в некоторых случаях хранятся в их центрах обработки данных, расположенных по всему миру, ни сам процесс выбора данных поставщиками облачных услуг – это серьёзная проблема.

3) На конфиденциальность данных также влияет функция взаимосвязи нескольких сервисов в облаке, как указано в [14], [15]. Поэтому такие проблемы влияют на облачную инфраструктуру с точки зрения администрирования.

Чтобы обеспечить конфиденциальность и целостность данных, многие исследователи указали, что шифрование и протоколы разделения секрета является одним из лучших безопасных методов для облачных вычислений и информационных систем [16 - 18].

Метод обеспечения безопасности

Предлагаемый подход в рамках исследования направлен на устранение указанных недостатков в работах авторов по данной тематике за счет применения метода на основе схемы разделения секрета, ключевой особенностью которой является повышение уровня безопасности персональных данных, возможность работы с облачными МИС, а также высокая скорость выполнения операций при разделении секрета на фрагменты, что безусловно важно при работе в распределенных системах.

Для решения задач хранения и обработки информации была разработана архитектура медицинской информационной системы (МИС), которая позволяет автоматизировать процессы взаимодействия и обеспечивает защиту систематизированных данных на основе предлагаемого метода разделения секрета. Для МИС предъявляются высокие требования к уровню безопасности, а также реализуется масштабируемость в условиях увеличения количества получаемых данных. Предполагается, что система не должна обеспечивать прозрачность местоположения ресурса (скрывать его физическое расположение). Ресурсы должны иметь только логические имена, такие как указатель URL ресурса, не имеющий информации о местоположении файла.

В рамках исследования предложена архитектура распределенной платформы сбора, хранения, обработки и защиты конфиденциальных медицинских данных, которая состоит из нескольких уровней. Общая схема представлена на рисунке 3. Данные, находящиеся внутри МИС могут использоваться как медицинскими, так и исследовательскими организациями, а платформа может выполнять задачу цифровизации бизнес-процессов за счет упрощения доступа специалистов к информации (телемедицина, SaaS сервисы, автоматизированные системы поддержки принятия

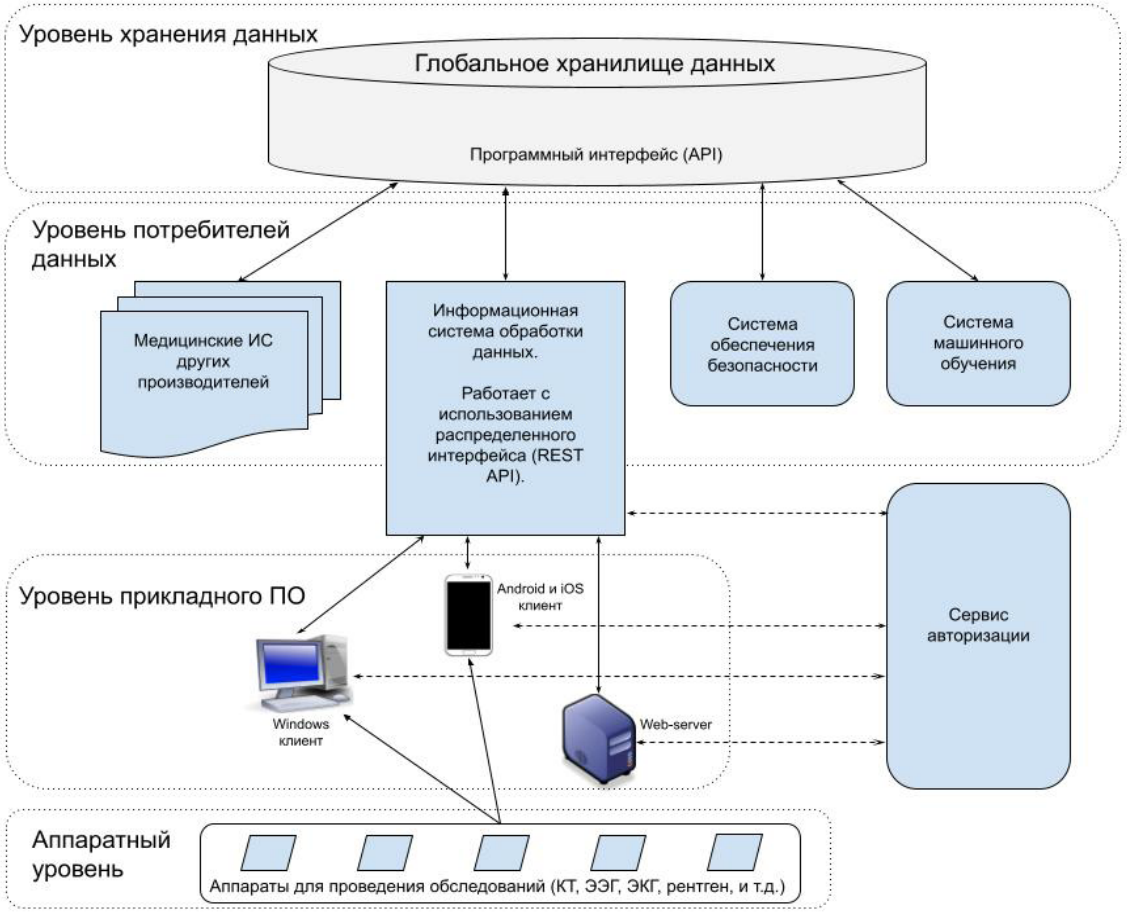

Рис. 3. Общая схема организации модулей МИС

решения, локально развернутые системы и т.д.) и научно-исследовательскую задачу (исследование алгоритмов обеспечения защиты информации, фармакологические исследования, анализ больших объемов данных различных типов обследований, разработку алгоритмов машинного обучения для автоматизированного анализа исследований).

Облачная платформа обладает следующим функционалом: предоставление удобных инструментов для передачи данных между пользователями системы; создание интерфейса и обширной базы данных для исследовательской системы анализа (в том числе, с использованием алгоритмов машинного обучения); создание интерфейсов для интеграции в существующие медицинские информационные системы (МИС); создание облачного сервиса (SaaS) для хранения, классификации и обработки данных, полученных с помощью медицинского оборудования (с поддержкой множества форматов хранения данных); создание подсистемы обеспечения защиты результатов обследований с использованием предложенного автором метода.

Важным аспектом МИС является **механизм защиты**, который представляет собой предлагаемый метод на основе схемы разделения секрета.

Последовательность действий алгоритма представляет собой несколько этапов и описывает шаги метода, который применяется при обработке обследований пациентов всеми участниками МИС (лаборантом, специалистом и доктором), их последующим разделением на части, шифрованием и расшифрованием. Каждый из этапов предлагаемого метода определяет формат взаимодействия между ролями (например, пациент – доктор, пациент – лаборант, лаборант – специалист, специалист – доктор, доктор – пациент).

Ниже на рисунке 4 представлена общая схема взаимодействия между участниками МИС на всех этапах, а также процесс обработки медицинских обследований.

Метод обеспечения защиты конфиденциальных данных представляет собой несколько этапов, которые включают в себя:

1. Присвоение уникального идентификатора каждому пациенту.

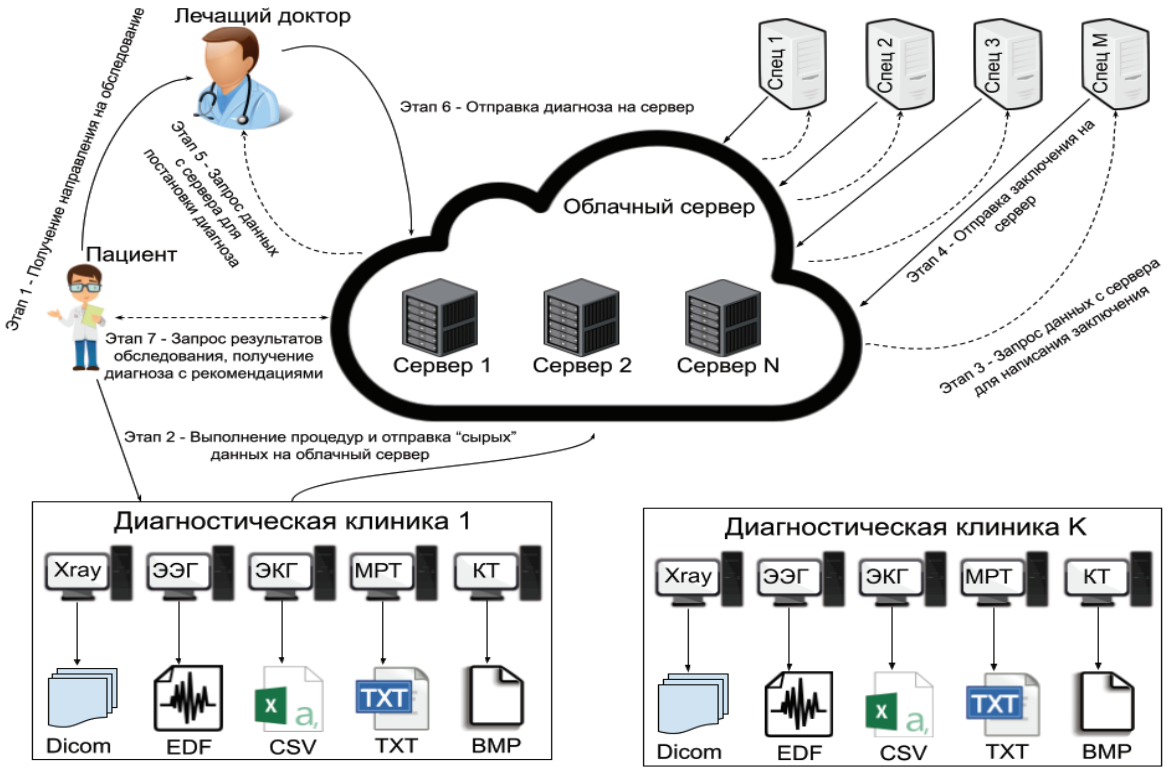

Рис. 4. Общая схема процесса циркулирования данных в облачной МИС

2. Шифрование результатов обследования и загрузка на сервер.

Данный этап описывает процесс прохождения медицинских процедур в клинике, на основании направления доктора. После посещения пациентом медицинского учреждения и выполнения назначенного обследования, для пациента формируется файл (отдельный для каждого обследования) с результатами в виде исходных данных, например снимок компьютерной томографии области грудной клетки, который должен быть отправлен на облачный сервер для последующего анализа специалистом.

3. Расшифрование файла (скачивание с сервера) обследования для анализа и постановки заключения. Выполняется расшифрование файла и скачивание на компьютер специалиста для написания заключения, на основе проведенного обследования. Распределение файлов между специалистами реализовано по принципу очереди: первый файл, отправленный на сервер лаборантом, будет проанализирован специалистом в первую очередь (в рамках своего медицинского профиля).

4. Зашифрование файла обследования (после написания заключения) и загрузка обратно на сервер. Основная цель на данном этапе заключается в отправке на сервер файла с обследованием и заключением (по конкретному медицинскому обследованию) в зашифрованном виде для последующего изучения лечащим врачом.

5. Расшифрование файла (скачивание с сервера) обследования с заключением для постановки диагноза. На данном этапе выполняется скачивание и расшифрование файла обследования с уже написанным заключением для того, чтобы доктор имел возможность поставить диагноз.

6. Зашифрование файла с диагнозом и рекомендациями по лечению, отправка данных на сервер. Цель на данном этапе заключается в отправке на сервер файла с поставленным диагнозом и рекомендациями по лечению в зашифрованном виде. После завершения этого этапа у пациента появится возможность ознакомится с диагнозом в личном кабинете МИС.

7. Получение данных с сервера пациентом и расшифрование файла с диагнозом и рекомендациями по лечению. На данном этапе пациент получает файл с диагнозом и рекомендациями от доктора посредством обращения в личный кабинет МИС.

Эксперименты

Перед проведением экспериментов была поставлена цель – определить наиболее эффективные протоколы разделения секрета среди схожих по функциона-

лу вариантов. Для этого был проведен сравнительный анализ по некоторым основным параметрам, которые наиболее сильно влияют на уровень безопасности.

Для обеспечения эффективности предложенного метода защиты были проанализированы сложность математического алгоритма, ресурсоемкость вычислений, совершенность и идеальность для четырех основных схем, выбранных в качестве наиболее подходящих для решения поставленной задачи. Схемы выбирались исходя из цели решаемой задачи, а также простоты программной реализации и наличии в открытом доступе библиотек, которые можно использовать без каких-либо доработок. В таблице 1 приведено сравнение сложности алгоритма для этапов разделения на доли и восстановление долей секрета.

Для оценки ресурсоемкости были приняты следующие условия:

— Размерность объекта, который будет разделен (секрет) и размерность простого модуля кольца целых чисел Z_p обозначены в качестве общей величины |M|.

— Размерность любого числа из модуля кольца целых чисел следует принимать за |M|, оценив верхний предел размерности.

С учетом допущений, обозначенных выше, можно утверждать, что, одинаковая размерность для больших чисел приводит к небольшому проигрышу в ресурсоемкости вычислений (количество потребляемой оперативной памяти). Это происходит из-за того, что для небольших значений приходится выделять большой объем памяти. Однако происходит значительный выигрыш в производительности. Не требуется контролировать и переопределять максимальный размер чисел.

В таблице 2 представлены результаты проведенного анализа ресурсоемкости. Такой анализ позволяет понять какое количество оперативной памяти требуется при выполнении одного и того же набора действий для различных схем.

В таблице 3 приведены результаты анализа схем по параметрам совершенности и идеальности.

— Совершенность означает, что если бесконечное число нелегитимных абонентов не имеет возможности извлечь информацию о секрете, то такая схема совершенная.

— Идеальность означает, что если размер доли секрета равен размеру секрета, то такая схема идеальна.

Из анализа видно, что единственная схема, обладающая обоими свойствами, является схема Шамира. Дальнейшие эксперименты проведены для трех пороговых схем разделения секрета, а именно:

— схема Шамира,

— схема Асмута-Блума,

— схема Карин-Грин-Хелмана.

Таблица 1

Анализ сложности математического алгоритма

	Шамира	**Асмута-Блума**	**Грин-Хелмана**	**Блэкли**
Разделение секрета на доли	*O(N×K)*	*O(N)*	*O(N)*	*O(K×N)*
Восстановление долей секрета	$O(K^2)$	$O(K^2)$	$O(K^3)$	$O(K^3)$

Таблица 2

Анализ ресурсоемкости в процессе вычислений

	Шамира	**Асмута-Блума**	**Карин–Грин Хелмана**	**Блэкли**
Разделение секрета на доли	*24 Кб*	*57 Кб*	*80 Кб*	*1 Мб*
Восстановление долей секрета	*112 Кб*	*320 Кб*	*82 Кб*	*1 Мб*

Таблица 3

Сравнение параметров идеальности и совершенности для анализируемых схем разделения секрета

	Шамира	**Асмута-Блума**	**Карин–Грин Хелмана**	**Блэкли**
Совершенность	+	+	+	+
Идеальность	+	-	-	-

Схема Блэкли оказалась в десятки раз более ресурсоемкой по сравнению с другими, а также уступает по сложности вычислений. Использование данной схемы в экспериментах не видится целесообразным.

В рамках исследования проведены 9 серий экспериментов, позволяющие оценить зависимость времени разделения и восстановления секрета, а также объем используемой памяти при использовании различных схем разделения секрета на основе анализа параметров. Ниже в таблицах продемонстрированы результаты для некоторых замеров. Параметр *N* – определяет возможное количество серверов в пороговой схеме разделения. Параметр *K* используется для операции восстановления секрета и образует необходимое пороговое количество участников. В таблице 5 приведены результаты, исходя из которых видно преимущества схемы Шамира для различных значений *K* и *N*.

В качестве файла (*M*) был использован обезличенный DICOM (КТ области грудной клетки), полученный в результате компьютерной томографии легких, содержащий серию из 2 слайсов (толщина среза 1 мм) и дополнительную информацию в виде тегов. Размер файла был специально подобран и составил 1048576 байт (1024 кбайт). 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.

Другой эксперимент был проведен с использованием файла большего размера, чтобы убедиться в том, что при увеличении объема файла схема Шамира не становится менее эффективной по сравнению с конкурентами. В таблице 6 показаны результаты эксперимента для DICOM'а размером более 8 Мб.

Таблица 5

Исследование основных параметров схем разделения секрета

	Параметры												
Схемы	Параметры схем	N=5	K=4	M= 1024	N=10	K=8	M= 1024	N=25	K=20	M= 1024	N=50	K=40	M= 1024
Шамира	Разделение (мс)	3,85			3,92			5			11,5		
	Восстановление (мс)	0,73			0,76			1,4			3,8		
Асмута-Блума	Разделение (мс)	71,31			110,75			681,8			778		
	Восстановление (мс)	0,82			1,2			2,4			13,1		
Карнин – Грин - Хелмана	Разделение (мс)	11,55			137,26			700			3648,96		
	Восстановление (мс)	0,7			70,7			408,58			2126,2		

Таблица 6

Исследование влияния размера файла на время восстановления и разделения

	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)	1,4			2,33			4,6			26		
Карнин – Грин - Хелмана	Разделение (мс)	21,95			260,81			1333,32			6933,1		
	Восстановление (мс)	1,18			134,32			776,3			4039,78		

На основе результатов из таблиц 5 и 6 видно, что схема Шамира является наилучшей. Кроме того, было замечено, что при увеличении объема файла схема Асмута-Блума становится более медленной по сравнению с другими схемами, поскольку время разделения секрета выросло в 2,11 раза, а у схемы Шамира в 1,9. Касательно замедления при восстановлении секрета (при увеличении размера файла), то для схемы Асмута-Блума этот показатель увеличился в 2,3 раза, а у Шамира в 2 раза. Если предположить, что работа будет проводится на файлах, размер которых составляет сотни мегабайт, то проигрыш в скорости будет сотни процентов, поскольку на данном этапе мы видим проигрыш в 15%.

Таким образом на основании проведенных экспериментов была выбрана схема разделения секрета Шамира, поскольку оказалась самой оптимальной и обладающая одновременно свойствами совершенности идеальности. Схема легла в основу предложенного метода.

Заключение

В рамках научной работы были исследованы современные методы разделения секрета, в основе которых лежат реализации Шамира, Асмута-Блума и Карин-Грин-Хелмана, а также алгоритмы, применяемые для обеспечения безопасности информации в распределенных МИС. Анализ литературных источников позволил определить основные проблемы в существующих подходах к обеспечению безопасности персональных данных в распределенных системах, к которым относятся проблема распределения ключей, ресурсоемкость вычислений при работе алгоритмов, а также необходимость обеспечения дополнительной защиты канала связи. В результате работы предложен метод обеспечения безопасности персональных данных, а также результатов медицинских обследований на основе схемы разделения секрета, который ляжет в основу системы защиты в облачной медицинской ИС.

Для подтверждения правильности выбора схемы разделения секрета были проведены эксперименты, в ходе которых была определена оптимальная схема - Шамира. По результатам дополнительных серий проведенных исследований, схема Шамира доказала эффективность, в том числе при работе с файлами больших размеров и различных форматов, что подтверждается быстрой работой и малым потреблением памяти, чем обусловлен выбор данной схемы для реализации предложенного в настоящей работе метода защиты. Кроме того, подтверждено, что схема Шамира обладает свойствами совершенности и идеальности, что является важным аспектом в контексте вопросов информационной безопасности. Применение СРС с такими свойствами позволяет обеспечивать безопасность данных на более высоком уровне, поскольку имеется возможность создавать фрагменты секрета такого же размера как и исходный файл.

Исследования, проведенные авторами в процессе разработки метода обеспечения безопасности, нашли свое применение при работе над задачами в рамках организации ООО «СиВижинЛаб», что подтверждается актом об использовании результатов (акт о внедрении) от 7 июля 2022 года.

Работа выполнена при финансовой поддержке РФФИ в рамках проекта № 20-37-90138 – «Аспиранты 2020».

Литература

1. Соловьева И. А., Юрьева Е. А., Кустова Т. В., Беляева А. В., Ткаченко О. В., Наркевич А. Н. Уроки пандемии: тренды цифровизации медицинского образования в эпоху covid-19 // Siberian Journal of Life Sciences and Agriculture. 2022. №6, с 265 – 268.
2. Ваулин Г. Ф., Тихомирова А. А., Котиков П. Е. Защита персональных данных пациентов в медицинских информационных системах // FORCIPE, 2022, № S2, с. 111– 112.
3. Вольская Е., Александрова О. Защита персональных данных пациентов // Ремедиум. 2018. №10, с. 6 – 9.
4. Мирабова Л. Современная защита информации и кибербезопасность // Научный журнал CETERIS PARIBUS, 2023, no 4. с. 56 – 57.
5. Зонова Д. Ю. Исследование кибербезопасности предприятий // Colloquium-journal. 2023. №2 (161), с. 17 – 19.
6. Бабенко Л.К., Шумилин А.С., Алексеев Д.М. Алгоритм обеспечения безопасности конфиденциальных данных медицинской информационной системы хранения и обработки результатов обследований // Известия ЮФУ. Технические науки. 2020. №5 (215), с. 6 – 8.
7. Утешев А.Ю., Маров А.В. Faulty share detection in Shamir's secret sharing // Вестник СПбГУ. Серия 10. Прикладная математика. Информатика. Процессы управления. 2019. №2, с. 274 – 277.
8. Давыдов В. В., Хуцаева А. Ф., Иогансон И. Д., Дакуо Ж.-М. Н., Беззатеев С. В. Усовершенствованная схема пороговой подписи csi-fish со свойством быстрой сборки секрета // Вестник СибГУТИ. 2023. №1 (60), с. 4 – 5.

9. Jeeva Selvaraj, Wen-Cheng Lai, Balasubramanian Prabhu Kavin, Kavitha C. and Gan Hong Seng Cryptographic Encryption and Optimization for Internet of Things Based Medical Image Security // Electronics 2023, №12. – 1636, March 2023, - pp. 42 – 43.
10. Shobana Pritha, Dr. A. Sasi Kumar Healthcare information system using cloud security // International Journal of Engineering & Technology 7 (2.33), 2018.
11. Гриднев В. А., Селиванов А. Ю., Программное обеспечение, реализующее алгоритм Шамира в стойких частных криптосистемах // Правовая информатика. 2021. №3, с. 53 – 57.
12. Maha Tebaa, Said EL Hajii Secure Cloud Computing through Homomorphic Encryption // International Journal of Advancements in Computing Technology, Volume 5, №16, December 2019, pp. 172 –174.
13. Ruba Awadallah, Azman Samsudin Homomorphic Encryption for Cloud Computing and Its Challenges // IEEE 7th International Conference on Engineering Technologies and Applied Sciences (ICETAS), December 2020, pp. 34 – 38.
14. A. A. Izang, Y. A. Mensah, O. J. Omotosho, and C. P. Obioma Overview of Cloud Computing and Recent Addendum // Journal of Communications Technology, Electronics and Computer Science, Vol. 5, 2019.
15. K. Muhammad, and Y. Z. Shao A survey on top security threats in cloud computin // International Journal of Advanced Computer Science and Applications (IJACSA), 2018, Vol. 6, no. 3, pp.109 – 113.
16. A. Acar, H. Aksu, A. S. Uluagac, M. Conti A survey on homomorphic encryption schemes: Theory and implementation // ACM Computing Surveys (CSUR), 2018, vol. 51, no. 4, pp. 1 – 3.
17. X. Liu, K. K. R. Choo, R. H. Deng, R. Lu, and J. Weng Efficient and Privacy-Preserving Outsourced Calculation of Rational Numbers // IEEE Trans. Dependable Secur. Comput., 2018, vol. 15, no. 1, pp. 27 – 39.

METHOD OF PERSONAL DATA PROTECTION IN A MEDICAL CLOUD SYSTEM

Shumilin A.S.[7]

The task of ensuring secure storage and data transmission in information systems is becoming more relevant nowadays due to digitalization processes that are actively integrating into all areas of people activity. The medical industry requires special attention, especially, the task of ensuring the security of patient data, who are users of medical information systems (MIS).

Purpose of the work: *development of a method for ensuring data security in terms of transferring and storage of personal patients' data who use the MIS which have built based on distributed cloud architecture.*

Research method: *the analysis of possible ways to ensure personal data security in distributed information systems based on a secret sharing protocol. The analysis of existing problems in terms of protection methods implementation in cloud-based systems. Analysis of violator model and attack methods.*

Results: *in terms of this paper, the use of a secret sharing protocol was justified as the basis for a method of ensuring the protection of patients' personal data in a cloud-based medical information system. Among several candidates with a similar functionality, the optimal secret sharing scheme was determined, taking into account the specifics of the task. The choice of the scheme has justified by the presence of such advantages as the properties of perfection, ideality, as well as the speed of execution the basic operations over other candidates. The experiments have been performed and the results have been obtained that have confirmed the correct choice of the secret sharing scheme (Shamir). Based on the chosen scheme, an implementation of the method for ensuring the security of patients' personal data in cloud medical information system has proposed. The authors proposed a cloud medical system architecture that allows to integrate a protection mechanism to be able to test how the proposed method works.*

Keywords: *encryption, cryptography, cloud computing security, personal data protection, secret sharing scheme, information systems.*

7 Alexander S. Shumilin, postgraduate, Southern federal university, Taganrog, Russia. Russia. E-mail: ashumilin@sfedu.ru

References

1. Solov'eva I. A., Jur'eva E. A., Kustova T. V., Beljaeva A. V., Tkachenko O. V., Narkevich A. N. Uroki pandemii: trendy cifrovizacii medicinskogo obrazovanija v jepohu covid-19 // Siberian Journal of Life Sciences and Agriculture. 2022. №6, s 265 – 268.
2. Vaulin G. F., Tihomirova A. A., Kotikov P. E. Zashhita personal'nyh dannyh pacientov v medicinskih informacionnyh sistemah // FORCIPE, 2022, № S2, s. 111– 112.
3. Vol'skaja E., Aleksandrova O. Zashhita personal'nyh dannyh pacientov // Remedium. 2018. №10, s. 6 – 9.
4. Mirabova L. Sovremennaja zashhita informacii i kiberbezopasnost' // Nauchnyj zhurnal CETERIS PARIBUS, 2023, no 4. s. 56 – 57.
5. Zonova D. Ju. Issledovanie kiberbezopasnosti predprijatij // Colloquium-journal. 2023. №2 (161), s. 17 – 19.
6. Babenko L.K., Shumilin A.S., Alekseev D.M. Algoritm obespechenija bezopasnosti konfidencial'nyh dannyh medicinskoj informacionnoj sistemy hranenija i obrabotki rezul'tatov obsledovanij // Izvestija JuFU. Tehnicheskie nauki. 2020. №5 (215), s. 6 – 8.
7. Uteshev A.Ju., Marov A.V. Faulty share detection in Shamir's secret sharing // Vestnik SPbGU. Serija 10. Prikladnaja matematika. Informatika. Processy upravlenija. 2019. №2, c. 274 – 277.
8. Davydov V. V., Hucaeva A. F., Ioganson I. D., Dakuo Zh.-M. N., Bezzateev S. V. Usovershenstvovannaja shema porogovoj podpisi csi-fish so svojstvom bystroj sborki sekreta // Vestnik SibGUTI. 2023. №1 (60), c. 4 – 5.
9. Jeeva Selvaraj, Wen-Cheng Lai, Balasubramanian Prabhu Kavin, Kavitha C. and Gan Hong Seng Cryptographic Encryption and Optimization for Internet of Things Based Medical Image Security // Electronics 2023, №12. – 1636, March 2023, - pp. 42 – 43.
10. Shobana Pritha, Dr. A. Sasi Kumar Healthcare information system using cloud security // International Journal of Engineering & Technology 7 (2.33), 2018.
11. Gridnev V. A., Selivanov A. Ju., Programmnoe obespechenie, realizujushhee algoritm Shamira v stojkih chastnyh kriptosistemah // Pravovaja informatika. 2021. №3, s. 53 – 57.
12. Maha Tebaa, Said EL Hajii Secure Cloud Computing through Homomorphic Encryption // International Journal of Advancements in Computing Technology, Volume 5, №16, December 2019, pp. 172 –174.
13. Ruba Awadallah, Azman Samsudin Homomorphic Encryption for Cloud Computing and Its Challenges // IEEE 7th International Conference on Engineering Technologies and Applied Sciences (ICETAS), December 2020, pp. 34 – 38.
14. A. A. Izang, Y. A. Mensah, O. J. Omotosho, and C. P. Obioma Overview of Cloud Computing and Recent Addendum // Journal of Communications Technology, Electronics and Computer Science, Vol. 5, 2019.
15. K. Muhammad, and Y. Z. Shao A survey on top security threats in cloud computin // International Journal of Advanced Computer Science and Applications (IJACSA), 2018, Vol. 6, no. 3, pp.109 – 113.
16. A. Acar, H. Aksu, A. S. Uluagac, M. Conti A survey on homomorphic encryption schemes: Theory and implementation // ACM Computing Surveys (CSUR), 2018, vol. 51, no. 4, pp. 1 – 3.
17. X. Liu, K. K. R. Choo, R. H. Deng, R. Lu, and J. Weng Efficient and Privacy-Preserving Outsourced Calculation of Rational Numbers // IEEE Trans. Dependable Secur. Comput., 2018, vol. 15, no. 1, pp. 27 – 39.