На правах рукописи

Чемусов Артем Александрович

Программный комплекс для защищенного хранения данных с использованием биометрической аутентификации в ОС Android

Направление подготовки
09.04.01 Информатика и вычислительная техника
направленность – Инженерия программного обеспечения и информационных систем
программа академической магистратуры

АВТОРЕФЕРАТ
магистерской диссертации
на соискание квалификации (степени) магистра

Екатеринбург 2025

Работа выполнена в Федеральном государственном бюджетном образовательном учреждении высшего образования «Сибирский государственный университет телекоммуникаций и информатики» Уральский технический институт связи и информатики (филиал) в г. Екатеринбурге (УрТИСИ СибГУТИ)

Научный руководитель **Долинер Леонид Исаевич**
Доктор педагогических наук,
профессор
кафедры ИСТ УрТИСИ СибГУТИ

Рецензент **Шестаков Иван Игоревич**
Кандидат технических наук, доцент
кафедры МЭС УрТИСИ СибГУТИ

Защита состоится «30» 06 2025 г. в 9 00 часов в Федеральном государственном бюджетном образовательном учреждении высшего образования «Сибирский государственный университет телекоммуникаций и информатики» Уральский технический институт связи и информатики (филиал) в г. Екатеринбурге (УрТИСИ СибГУТИ), г. Екатеринбург, ул. Репина, д. 15.

Секретарь Государственной аттестационной комиссии

Общая характеристика работы

В современном мире, который становится все более взаимосвязанным, безопасность личных и конфиденциальных данных стала критической проблемой. С быстрым развитием цифровых услуг и облачных платформ пользователи генерируют и хранят огромные объемы информации на различных устройствах и в различных средах. В то же время киберугрозы стали более сложными и частыми, нацеленными на все: от корпоративных сетей до персональных компьютеров и мобильных устройств. В этой среде обеспечение конфиденциальности, целостности и доступности данных — это не просто техническая проблема, это фундаментальная необходимость.

Одним из ключевых аспектов современной кибербезопасности является предоставление людям возможности контролировать свои собственные данные. Это включает в себя предоставление безопасных, удобных для пользователя инструментов, которые позволяют надежно шифровать и хранить файлы. Шифрование остается одним из наиболее эффективных методов защиты данных от несанкционированного доступа, особенно в сочетании с надежными механизмами аутентификации. Биометрическая аутентификация, такая как сканирование отпечатков пальцев, стала мощной альтернативой традиционным паролям, предлагая как высокую безопасность, так и удобство за счет использования уникальных физических характеристик пользователя.

В статье проанализированы такие статьи как: «Designing a Secure, Scalable, and Cost-Effective Cloud Storage Solution: A Novel Approach to Data Management using NextCloud, TrueNAS, and QEMU/KVM», «Revolutionizing Healthcare Record Management: Secure Documentation Storage and Access through Advanced Blockchain Solutions», «Two Fish Encryption Based Blockchain Technology for Secured Data Storage», «EtrusChain: File Storage with DNA and Blockchain», «dabih -- encrypted data storage and sharing platform», «Portable Trust: biometric-based authentication and blockchain storage for self-sovereign identity systems», «Разработка программного обеспечения безопасного хранения конфиденциальной информации на устройствах под управлением Android» и другие.

Как можно видеть, степень разработанности темы включает в себя ряд существующих работ посвященных разработке систем защищенного хранения данных, криптографии и биометрии. Однако, существует пробел в исследованиях, которые предлагают решение, направленное на домашнее использование и защиту личных данных. Большинство исследований сосредоточены на создании систем защиты данных для предприятий и медицинских организаций. Исследований же, которые предлагают систему защиты и шифрования данных для домашнего использования мало и в них используется другой подход к реализации архитектуры приложения, а также в них не предусмотрена такая защита ключа, которая используется в архитектуре данного исследования.

Архитектура, предлагаемая в данном исследовании, позволяет пользователю зашифровать любые файлы на компьютере с помощью своего смартфона на системе Android используя биометрическую аутентификацию.

Обычно механизмы биометрической аутентификации используются только приложениями внутри системы Android, предлагаемое в данном исследовании решение позволяет пользователю использовать надежные механизмы хранения ключей и биометрической аутентификации в ОС Android для шифрования любых файлов на ПК. Надежность этой системы обусловлена тем, что для расшифровки данных пользователь должен подтвердить свою личность, а ключ шифрования не хранится в открытом виде и никогда не передается внутрь приложения.

Таким образом, актуальность этой темы исследования заключается в необходимости создания новых подходов к системам защищенного хранения данных, которые будут направлены на домашнее использование, а не на предприятия. Среди пользователей растет потребность в доступных и эффективных решениях по защите данных. Поскольку люди все больше полагаются на цифровые устройства для управления своей личной и профессиональной жизнью, становится критически важным предлагать средства защиты информации, которые являются как безопасными, так и простыми в использовании с понятным интерфейсом.

Этот проект вносит вклад в область кибербезопасности, предоставляя пользователю новый способ защиты любых своих данных с помощью личного смартфона — позволяя ему использовать надежные методы шифрования с современной биометрической аутентификацией внутри системы Android через ПК. Традиционных методов аутентификации на основе паролей уже недостаточно, поскольку они уязвимы для кражи, атак методом подбора и социальной инженерии. Напротив, биометрические данные, уникально привязанные к человеку, обеспечивают более высокий уровень надежности и по своей сути устойчивы ко многим формам атак. Позволяя пользователю применять личное Android-устройство с биометрической аутентификацией для защиты любых данных, этот проект направлен на усиление защиты цифровых активов таким образом, чтобы это было и безопасно, и доступно.

Объект исследования – методы защиты данных, биометрическая аутентификация.

Предмет исследования – ПО, позволяющее использовать систему биометрии и хранилища секретных ключей системы Android для шифрования любых данных на ПК.

Целью исследования является разработка программного комплекса для защищенного хранения данных с использованием биометрической аутентификации в ОС Android.

Для достижения поставленной цели были сформулированы и решены следующие **задачи**:

1) Анализ аналогов и исследований в данной предметной области.
2) Изучение работы биометрической системы в ОС Android.
3) Изучение работы хранилища ключей в ОС Android.
4) Изучение средств, подходящих для реализации практической части.
5) Реализация алгоритма шифрования и дешифрования данных с использованием хранилища ключей и биометрической аутентификации в ОС Android.

6) Создание полноценного мобильного приложения, которое будет служить в качестве сервера и принимать данные от клиента, производить шифрование/дешифрование с помощью созданного алгоритма и возвращать обработанные данные клиенту.
7) Создание клиентского приложения для ПК, которое позволит пользователю выбирать файлы для шифрования/дешифрования, подключаться к серверу, передавать ему данные для обработки и принимать их обратно для сохранения по выбранному пользователю пути.
8) Проведение тестов реализованного программного решения и фиксирование полученных результатов.

Научная новизна:

- предложен новый оригинальный подход к шифрованию данных;
- разработан новый алгоритм для системы защиты данных, который не применялся ранее в аналогах;
- на основе созданного алгоритма разработано ПО, которое направлено на индивидуальное использование и не имеет аналогов.

Теоретическая значимость исследования заключается в следующем:

- Развитие теории защиты данных в мобильных системах. Исследование вносит вклад в теоретические основы информационной безопасности, в частности — в контексте мобильных операционных систем. Оно расширяет существующие представления о возможностях безопасного хранения данных с использованием биометрических факторов, которые всё чаще применяются в мобильных устройствах, но остаются слабо интегрированными в персонализированные системы защиты на уровне пользовательских приложений;
- Системный подход к объединению биометрической аутентификации и криптографической защиты. Работа предлагает новый теоретический подход к построению программной архитектуры, объединяющей биометрию и хранилище ключей в Android. Это усиливает существующие модели безопасной аутентификации, демонстрируя их применимость к задаче индивидуального шифрования данных;
- Анализ и классификация существующих решений. Теоретическая значимость проявляется и в том, что в работе выполнен глубокий анализ существующих методов защиты данных, что позволяет классифицировать текущие подходы, выявить их недостатки и систематизировать проблемы. Это формирует основу для последующего теоретического моделирования более эффективных решений.

Таким образом, исследование теоретически обосновывает необходимость комплексного подхода к защите данных, основанного на синергии криптографических и биометрических механизмов, и предлагает системную

модель, которую можно использовать в дальнейших научных и прикладных разработках.

Практическая значимость исследования заключается в создании программного комплекса, который построен на новом алгоритме защиты данных. В основе данного алгоритма лежит соединение двух систем: секретного хранилища ключей и биометрической системы в ОС Android. Обе системы выполняют свои операции в защищенном и отделенном от основной системы месте, что делает их безопасными и надежными. Созданная клиентская программа для ПК позволяет пользователю шифровать данные с помощью серверного Android приложения, используя биометрическую аутентификацию. Надежность системы заключается в том, что ключ шифрования хранится в защищенном пространстве и никогда не передается в приложение, а все операции по шифрованию/дешифрованию выполняются так же, в защищенном пространстве, а приложение получает только обработанные данные.

Данное решение предлагает надежную защиту пользовательских данных и направлено на индивидуальное использование, а также имеет простой и понятный интерфейс.

Методология и методы исследования.

Решение поставленных задач осуществлялось с использованием следующих методов:

- Анализ существующих решений и методов защиты данных;
- Синтез знаний для разработки новых методов защиты данных;
- Поиск нового решения, которое будет закрывать пробелы в данной предметной области;
- Разработка алгоритма нового решения;
- Анализ средств реализации нового решения и выбор наилучших;
- Реализация нового решения с помощью выбранных средств;
- Тестирование нового решения, выявление плюсов и недостатков.

Основные этапы и элементы работы клиентской программы приведены на рисунке 1.

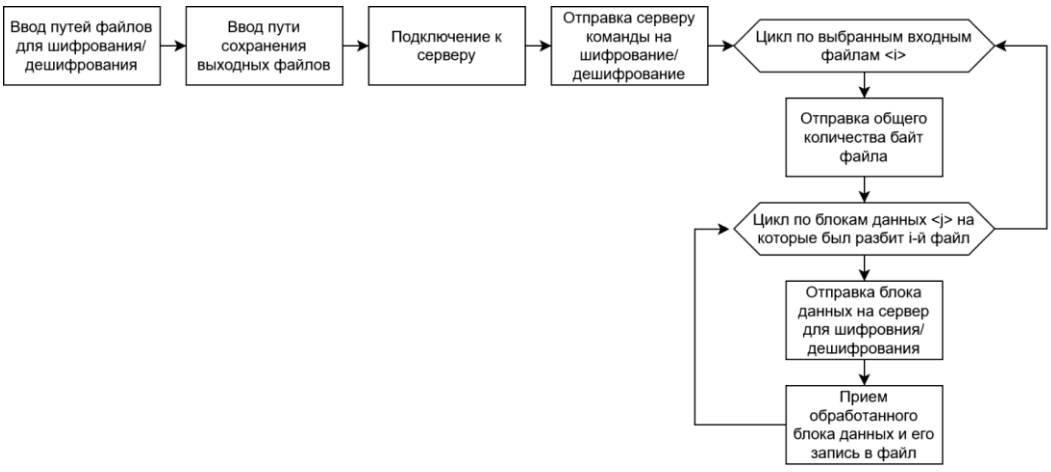

Рисунок 1 – Основные этапы работы программы-клиента

Основные этапы и элементы работы мобильного приложения, на котором запускается сервер приведены на рисунке 2.

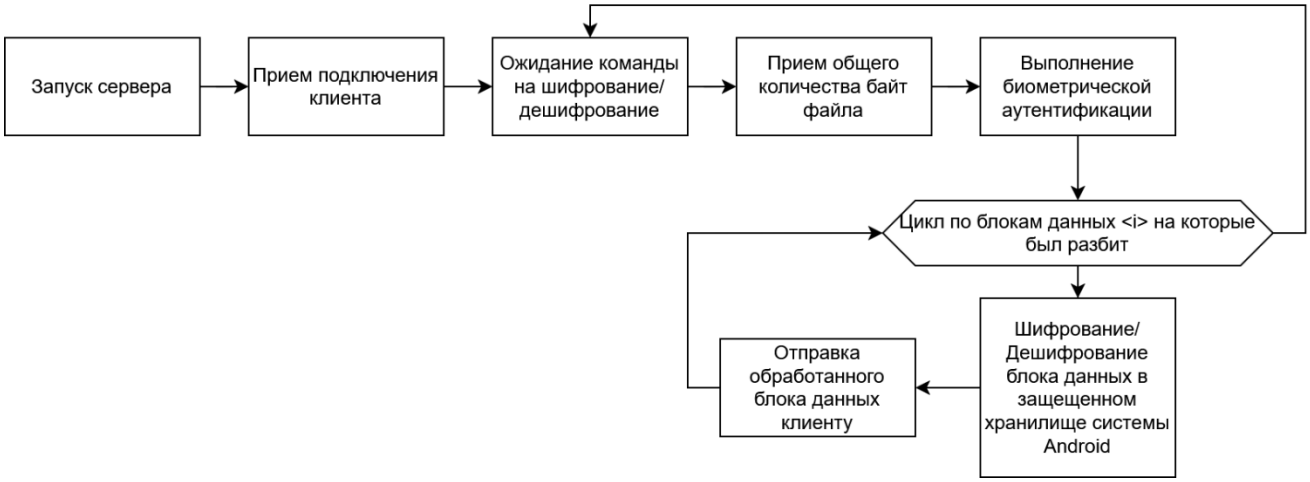

Рисунок 2 – Основные этапы работы мобильного приложения

Положения, выносимые на защиту:

- Технологии хранилища секретных ключей и биометрической системы в ОС Android;
- Алгоритм защиты данных на основе биометрической аутентификации в ОС Android;
- Применение разработанного алгоритма для реализации ПО для защиты данных;
- Оценка эффективности разработанного ПО.

Степень достоверности результатов исследования обеспечивается применением современных технологий для разработки ПО. В работе использованы общепризнанные методики и алгоритмы, которые прошли широкую проверку на практике и в научной среде.

Достоверность результатов также подтверждается тестированием разработанной системы на реальных данных, что позволяет объективно оценить ее эффективность и применимость на различных файлах.

В работе использовались данные, полученные из различных источников, включая научные статьи и исследования, а также официальную документацию средств разработки.

Диссертационная работа включает введение, три главы, заключение, список литературы из 33 наименований. Объем диссертации 100 страниц, включены также 10 рисунков, 1 таблица

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Введение

Во введении обоснована актуальность исследования, сформулированы цель и задачи работы, описаны методологические подходы и методы, использованные для решения поставленных задач, а также изложена научная новизна и практическая значимость работы.

В первой главе «Анализ литературы по теме исследования» рассмотрены существующие исследования по методам и алгоритмам защиты данных. Проанализированы основные подходы к решению разработки систем защиты данных. Представлен обзор литературы, посвященной разработке систем защиты данных. Выявлены основные недостатки существующих решений, а также пробелы в данной области исследований, обоснована необходимость разработки новых подходов, учитывающих направленность на индивидуальное использование и надежную защиту секретного ключа.

Во второй главе «Теоретические сведения по теме исследования» рассмотрены основы работы системы хранилища ключей и биометрической системы в ОС Android. Рассмотрен способ совместной работы данных систем. Описаны ключевые факторы, на которых будет построен новый алгоритм защиты данных и новое программное решение. Так же рассмотрены средства, подходящие для реализации программной части, приведены их преимущества и недостатки. В соответствии с проанализированными средствами разработки, выбраны наилучшие из них.

В третьей главе «Практическая реализация» рассмотрена логика работы клиентского приложения для ПК и мобильного приложения, которое служит сервером и выполняет операции шифрования/дешифрования по запросу клиента. Разобран код и алгоритмы клиентского и мобильного приложений. Разобран код алгоритма шифрования и дешифрования данных, в котором применяется биометрическая аутентификация ОС Android. Рассмотрен пользовательский интерфейс клиентского и мобильного приложений. Описан их функционал и реакция элементов интерфейса на действия пользователя и другие условия. Приведены результаты тестирования программного решения, описаны его плюсы и недостатки.

ЗАКЛЮЧЕНИЕ

В работе исследованы существующие решения систем защиты данных, а также основы работы биометрической системы и хранилища секретных ключей в ОС Android. На основе проанализированных данных предложен новый алгоритм защиты информации.

На основе нового алгоритма для защиты данных, в котором используется биометрическая аутентификация в ОС Android построен программный комплекс для защищенного хранения данных.

Разработанное решение было протестировано и был сделан вывод, что время шифрования данных с использованием данного ПО может быть дольше, чем в аналогичных системах или при простом шифровании алгоритмами шифрования. Но здесь стоит учитывать, что шифрование и дешифрование производится на мобильном устройстве, которое может быть существенно ограничено в производительности и объеме оперативной памяти. Так же, данный минус может быть перекрыт надежностью новой системы, так как секретный ключ не хранится в открытом виде и никогда не передается в приложение. Он находится в защищенном хранилище ключей системы Android и все операции с данными производятся там же, а приложение только получает обработанные данные.