**Министерство науки и высшего образования Российской Федерации**

**Федеральное государственное автономное образовательное учреждение**

**высшего образования**

**«КАЗАНСКИЙ (ПРИВОЛЖСКИЙ) ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»**

Институт вычислительной математики и информационных технологий

Кафедра системного анализа и информационных технологий

Направление подготовки: 10.03.01 – Информационная безопасность

Профиль: Безопасность компьютерных систем

**КУРСОВАЯ РАБОТА**

**Настольный мессенджер с элементами защиты данных**

Студент 3 курса

группы 09-142

«\_\_\_» \_\_\_\_\_\_\_ 2024 г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Малышев Р.Е.

Научный руководитель

старший преподаватель КСАИТ

«\_\_\_» \_\_\_\_\_\_\_ 2024 г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Еникеев Р.Р.

Казань-2024



# **ВВЕДЕНИЕ**

В современное время обеспечение конфиденциальности и безопасности данных в интернете становится все более и более актуальной задачей. С быстрым развитием цифровых технологий и увеличением объема обмена информацией в сети растет и число угроз, нацеленных на данные пользователей, имеющие какую-либо ценность, будь то личная информация, пароли или ПИН-коды от банковских карт. В таких условиях необходимо постоянно совершенствовать механизмы защиты данных для разработки безопасных средств обмена сообщениями.

Мессенджеры играют ключевую роль в жизни современного человека и используются практически повсеместно, как для личного общения, так и для корпоративных целей. Но многократно участившиеся случаи кражи аккаунтов или персональной информации пользователей, а также случаи получения несанкционированного доступа к данным, подчеркивают важность создания мессенджеров, которые бы смогли обеспечить должный уровень безопасности.

Разработка настольного мессенджера с элементами защиты данных представляет собой практически значимый шаг в обеспечении приватности и безопасности пользователей при общении онлайн. Предложенное исследование может привести к созданию эффективного инструмента для безопасного обмена сообщениями, которое позволит забыть о рисках утечки информации.

Целью данной работы является разработка и анализ настольного мессенджера с элементами защиты данных. Для достижения поставленной цели необходимо выполнение следующих задач:

1. Обзор существующих мессенджеров и выявление основных проблем безопасности;
2. Изучение методов защиты данных и выбор наиболее подходящих методов для внедрения в создаваемый мессенджер;
3. Разработка модели настольного мессенджера с встроенными механизмами защиты;
4. Анализ результатов и формулирование выводов о применимости и эффективности выбранных способов обеспечения безопасности в мессенджере;

# **Глава 1**

**1.1** **Обзор популярных мессенджеров**

Мессенджеры играют важную роль в современной коммуникации, и среди них можно выделить несколько популярных приложений, которые широко используются по всему миру. Рассмотрим основные особенности таких мессенджеров, как Telegram, WhatsApp и Signal.

Telegram — это облачный мессенджер с поддержкой мгновенных сообщений, мультимедиа и документов. Одной из ключевых особенностей Telegram является его система шифрования, которая включает в себя серверное шифрование для стандартных чатов и клиент-клиентское шифрование для секретных чатов. Telegram также предлагает функции самоуничтожающихся сообщений и поддержку ботов для автоматизации задач.

WhatsApp — один из самых популярных мессенджеров, принадлежащий компании Meta (ранее Facebook). WhatsApp использует сквозное шифрование (end-to-end encryption) по умолчанию для всех чатов и звонков, обеспечивая высокий уровень конфиденциальности и безопасности сообщений. Кроме того, приложение предлагает функции групповых чатов, голосовых и видеозвонков, а также обмена мультимедийными файлами.

Signal — это мессенджер с открытым исходным кодом, известный своим акцентом на безопасность и конфиденциальность. Signal использует собственный протокол Signal Protocol для сквозного шифрования сообщений и звонков. Приложение поддерживает как текстовые сообщения, так и голосовые и видеозвонки, а также имеет функции самоуничтожающихся сообщений и анонимной регистрации с помощью номера телефона.

Эти мессенджеры являются лидерами в своей области и демонстрируют различные подходы к обеспечению безопасности данных. Изучение их характеристик и методов защиты позволяет понять современные стандарты и лучшие практики в области разработки защищенных коммуникационных приложений.

**1.2. Методы защиты данных в мессенджерах**

Защита данных в мессенджерах является ключевым аспектом их функциональности и популярности. Существует несколько основных методов защиты данных, которые используются в современных мессенджерах:

**1. Сквозное шифрование (End-to-End Encryption)** Сквозное шифрование обеспечивает защиту данных на всем пути от отправителя к получателю. Это означает, что только отправитель и получатель могут расшифровать сообщения, а все промежуточные серверы видят лишь зашифрованный текст. Этот метод используется в таких мессенджерах, как WhatsApp и Signal.

**2. Транспортное шифрование (Transport Layer Security, TLS)** TLS защищает данные во время их передачи между устройством пользователя и сервером. Это предотвращает атаки типа "человек посередине" (Man-in-the-Middle) и обеспечивает целостность данных при их передаче. Telegram, например, использует TLS для защиты стандартных чатов.

**3. Управление ключами** Эффективное управление ключами является критически важным для обеспечения безопасности шифрования. Методы управления ключами включают в себя генерацию, распределение, хранение и обновление криптографических ключей. В Signal используется протокол Double Ratchet для регулярного обновления ключей, что повышает безопасность.

**4. Аутентификация пользователей** Аутентификация пользователей позволяет удостовериться в подлинности собеседника. Способы аутентификации включают в себя использование паролей, биометрических данных, а также двухфакторную аутентификацию (2FA). WhatsApp, например, предлагает двухфакторную аутентификацию для дополнительной защиты учетной записи.

**5. Самоуничтожающиеся сообщения** Эта функция позволяет пользователям отправлять сообщения, которые автоматически удаляются через заданный промежуток времени. Это помогает сохранить конфиденциальность информации, даже если устройство попадает в чужие руки. Telegram и Signal предлагают такую функциональность в своих секретных чатах.

**6. Защита на устройстве** Защита данных на устройстве пользователя включает в себя шифрование локально хранящихся данных и использование безопасных хранилищ для ключей. Это предотвращает доступ к данным, даже если устройство было потеряно или украдено.

Эти методы защиты данных демонстрируют современные подходы к обеспечению безопасности в мессенджерах и служат основой для разработки надежных и защищенных коммуникационных приложений.

**1.3. Проблемы безопасности в существующих мессенджерах**

Несмотря на использование современных методов защиты, многие популярные мессенджеры сталкиваются с различными проблемами безопасности, которые могут ставить под угрозу конфиденциальность и целостность данных пользователей.

**1. Уязвимости в реализации шифрования** Даже при использовании сквозного шифрования возможны ошибки в его реализации. Примеры включают неправильное управление ключами или использование устаревших алгоритмов. Такие ошибки могут привести к тому, что злоумышленники смогут расшифровать сообщения. Например, в прошлом были случаи, когда уязвимости в протоколах шифрования позволяли перехватывать сообщения в WhatsApp и Telegram.

**2. Атаки на серверную инфраструктуру** Многие мессенджеры хранят часть данных на своих серверах, включая метаданные, которые могут быть использованы для анализа пользовательской активности. Атаки на серверную инфраструктуру, такие как DDoS-атаки или взлом серверов, могут привести к утечке данных. В 2019 году произошел инцидент, когда серверы Telegram подверглись DDoS-атаке, что вызвало сбои в работе сервиса.

**3. Социальная инженерия** Злоумышленники могут использовать методы социальной инженерии для получения доступа к учетным записям пользователей. Это включает в себя фишинговые атаки, подделку идентификационных данных или убеждение пользователя предоставить свои учетные данные. В WhatsApp были случаи, когда пользователи становились жертвами фишинговых атак, что приводило к компрометации их аккаунтов.

**4. Угрозы конфиденциальности на уровне устройства** Даже если данные защищены при передаче, уязвимости на уровне устройства могут поставить под угрозу конфиденциальность сообщений. Вредоносные программы, получившие доступ к устройству, могут читать сообщения до их шифрования или после расшифровки. Например, шпионские программы, установленные на смартфонах, могут перехватывать данные из мессенджеров.

**5. Проблемы с аутентификацией и авторизацией** Небезопасные методы аутентификации и авторизации могут стать причиной несанкционированного доступа к учетным записям. Если злоумышленники получают доступ к аккаунту, они могут читать все сообщения, отправленные и полученные пользователем. В прошлом у некоторых мессенджеров были обнаружены уязвимости, связанные с недостаточной защитой аутентификации.

**6. Уязвимости в клиентском приложении** Уязвимости в клиентском приложении мессенджера могут быть использованы для выполнения вредоносного кода на устройстве пользователя. Это может привести к утечке данных, установке вредоносного ПО или другим атакам. В Signal и других мессенджерах периодически обнаруживаются и устраняются такие уязвимости.

Эти проблемы безопасности подчеркивают необходимость постоянного совершенствования методов защиты данных в мессенджерах и внимательного подхода к их реализации и тестированию.

# **2. Проектирование настольного мессенджера**

**2.1 Требования к системе**

Для разработки настольного мессенджера с элементами защиты данных необходимо определить требования к системе, которые включают в себя как функциональные, так и нефункциональные аспекты.

**1. Функциональные требования**

1.1. **Регистрация и аутентификация пользователей**

* Пользователь должен иметь возможность зарегистрировать новую учетную запись с использованием уникального идентификатора (например, адрес электронной почты или номер телефона).
* Система должна поддерживать методы аутентификации, такие как логин и пароль, а также двухфакторную аутентификацию (2FA).

1.2. **Отправка и получение сообщений**

* Пользователь должен иметь возможность отправлять текстовые сообщения другим пользователям.
* Система должна поддерживать отправку мультимедийных файлов, таких как изображения, аудио и видео.
* Сообщения должны передаваться в зашифрованном виде с использованием сквозного шифрования.

1.3. **Управление контактами**

* Пользователь должен иметь возможность добавлять, удалять и управлять своими контактами.
* Система должна предоставлять функции для поиска и добавления новых контактов.

1.4. **Групповые чаты**

* Пользователь должен иметь возможность создавать и управлять групповыми чатами.
* Сообщения в групповых чатах должны быть защищены аналогично личным сообщениям.

1.5. **Самоуничтожающиеся сообщения**

* Пользователь должен иметь возможность отправлять сообщения, которые автоматически удаляются через заданный промежуток времени.
* Настройки самоуничтожающихся сообщений должны быть гибкими и настраиваемыми.

**2. Нефункциональные требования**

2.1. **Безопасность**

* Система должна обеспечивать высокий уровень безопасности данных как при передаче, так и при хранении.
* Все сообщения и мультимедийные файлы должны быть защищены сквозным шифрованием.
* Данные пользователей, хранящиеся на серверах, должны быть зашифрованы.

2.2. **Производительность**

* Система должна обеспечивать быструю отправку и получение сообщений, даже при высокой нагрузке.
* Время отклика системы должно быть минимальным, чтобы обеспечить удобство использования.

2.3. **Надежность**

* Система должна быть устойчивой к сбоям и обеспечивать сохранность данных в случае непредвиденных ситуаций.
* Должны быть предусмотрены механизмы резервного копирования и восстановления данных.

2.4. **Удобство использования (юзабилити)**

* Интерфейс пользователя должен быть интуитивно понятным и удобным для пользователей с различным уровнем технической подготовки.
* Система должна поддерживать различные языки и адаптироваться к нуждам пользователей.

2.5. **Масштабируемость**

* Система должна быть способна обрабатывать увеличение количества пользователей и объема данных без потери производительности.
* Архитектура системы должна поддерживать горизонтальное и вертикальное масштабирование.

Эти требования обеспечат создание защищенного и надежного настольного мессенджера, который будет удовлетворять потребности пользователей в безопасной коммуникации.

**2.2. Архитектура системы**

Архитектура настольного мессенджера с элементами защиты данных должна быть гибкой, масштабируемой и обеспечивать высокий уровень безопасности. Рассмотрим основные компоненты и принципы архитектуры такой системы.

**1. Клиентское приложение**

* Клиентское приложение представляет интерфейс пользователя для отправки и приема сообщений, управления контактами, создания групповых чатов и других функций.
* Оно должно обеспечивать шифрование сообщений на уровне устройства и передачу зашифрованных данных на сервер.

**2. Серверная инфраструктура**

* Серверная инфраструктура состоит из серверов, обеспечивающих обработку и хранение данных, а также обеспечивающих связь между клиентскими приложениями.
* Серверы должны поддерживать высокую доступность и масштабируемость, чтобы обеспечить удобство использования и надежность сервиса.

**3. Шифрование**

* Шифрование данных должно осуществляться на двух уровнях: на уровне клиентского приложения и на сервере.
* Клиентское приложение должно использовать сквозное шифрование (End-to-End Encryption) для защиты сообщений от доступа третьих лиц.
* На сервере должно быть обеспечено хранение зашифрованных данных и обработка их только в зашифрованном виде.

**4. Аутентификация и авторизация**

* Система должна иметь механизмы аутентификации пользователей при входе в систему и авторизации доступа к данным.
* Должны быть предусмотрены механизмы двухфакторной аутентификации и другие методы повышения безопасности аутентификации.

**5. Безопасное хранение данных**

* Данные пользователей, включая сообщения и мультимедийные файлы, должны храниться в зашифрованном виде на серверах.
* Должны быть предприняты меры для защиты данных от несанкционированного доступа и вредоносных атак.

**6. Механизмы резервного копирования и восстановления**

* Должны быть реализованы механизмы резервного копирования данных для предотвращения потери данных в случае сбоев или атак на серверную инфраструктуру.
* Восстановление данных должно быть быстрым и эффективным, чтобы минимизировать перерывы в обслуживании пользователей.

Эта архитектура обеспечит надежное и защищенное функционирование настольного мессенджера, соответствующее требованиям безопасности и производительности.

**2.3. Методы защиты данных**

Эффективная защита данных является ключевым аспектом в разработке настольного мессенджера с элементами конфиденциальности. Рассмотрим основные методы защиты данных, которые могут быть использованы в такой системе.

**1. Сквозное шифрование (End-to-End Encryption)**

* Сквозное шифрование обеспечивает конфиденциальность сообщений, шифруя данные на устройстве отправителя и расшифровывая их только на устройстве получателя.
* Этот метод защиты данных обеспечивает надежную защиту даже в случае компрометации серверов, так как данные остаются зашифрованными на серверах.

**2. Протоколы аутентификации и авторизации**

* Использование современных протоколов аутентификации и авторизации, таких как OAuth 2.0 или OpenID Connect, позволяет обеспечить безопасную и надежную идентификацию пользователей.
* Двухфакторная аутентификация (2FA) может быть использована для дополнительного уровня защиты учетных записей.

**3. Хеширование паролей**

* Хеширование паролей позволяет сохранять пароли пользователей в зашифрованном виде, что обеспечивает защиту от их утечки в случае компрометации базы данных.
* Для увеличения безопасности рекомендуется использовать соль (salt) и алгоритмы хеширования с адаптивными хешами, такие как bcrypt или Argon2.

**4. Защита на уровне сети**

* Использование протоколов безопасности на уровне сети, таких как Transport Layer Security (TLS), обеспечивает шифрование данных во время их передачи между клиентскими приложениями и серверами.
* Настройка правил файрвола и других средств защиты сети помогает предотвратить атаки типа Man-in-the-Middle и другие угрозы безопасности.

**5. Мониторинг и реагирование на инциденты**

* Реализация системы мониторинга безопасности позволяет выявлять подозрительную активность и потенциальные угрозы безопасности в реальном времени.
* Быстрое реагирование на инциденты и применение соответствующих мер безопасности помогает минимизировать последствия атак и утечек данных.

**6. Регулярное обновление и аудит безопасности**

* Регулярное обновление клиентских и серверных компонентов помогает закрывать известные уязвимости и улучшать общую защиту системы.
* Проведение регулярного аудита безопасности позволяет выявлять потенциальные уязвимости и проблемы безопасности и своевременно принимать меры по их устранению.

**Глава 3: Разработка настольного мессенджера**

**3.1. Разработка прототипа**

Разработка прототипа настольного мессенджера является первым этапом создания полноценной системы. В этом модуле мы опишем процесс создания прототипа, который будет включать в себя основные функции и элементы безопасности.

1. Определение основных функциональных требований

* Определяем основные функции мессенджера, такие как отправка текстовых и мультимедийных сообщений, создание групповых чатов, добавление и управление контактами и другие.
* Обеспечиваем защиту всех сообщений и файлов с помощью сквозного шифрования и других методов безопасности.

2. Проектирование пользовательского интерфейса

* Разрабатываем пользовательский интерфейс, который будет интуитивно понятен и удобен для использования.
* Учитываем в дизайне интерфейса элементы безопасности, такие как индикаторы шифрования сообщений и настройки конфиденциальности.

3. Создание клиентской части приложения

* На основе определенных функциональных требований создаем клиентскую часть приложения с использованием современных технологий разработки программного обеспечения.
* Реализуем функции отправки и приема сообщений, управления контактами и другие основные функции.

4. Разработка серверной части приложения

* Создаем серверную инфраструктуру, которая будет обеспечивать связь между клиентскими приложениями и хранение данных.
* Обеспечиваем защиту данных на сервере с помощью шифрования и других методов безопасности.

5. Интеграция методов защиты данных

* Интегрируем методы защиты данных, такие как сквозное шифрование, хеширование паролей и механизмы аутентификации, в клиентское и серверное приложения.
* Убеждаемся, что все данные пользователя хранятся и передаются в зашифрованном виде.

6. Тестирование и отладка

* Проводим тестирование прототипа для выявления и устранения возможных ошибок и проблем.
* Проверяем работоспособность функциональных аспектов приложения.

7. Демонстрация и обратная связь

* Демонстрируем прототип пользователям для получения обратной связи и предложений по улучшению.
* Используем полученные отзывы для доработки и улучшения функциональности и безопасности мессенджера.

Разработка прототипа настольного мессенджера позволит нам определить ключевые особенности и убедиться в их работоспособности и безопасности перед переходом к созданию полноценной системы.

**3.2. Интеграция механизмов защиты**

Интеграция механизмов защиты данных является важным этапом в разработке настольного мессенджера с учетом конфиденциальности. В данном модуле мы опишем процесс интеграции основных механизмов защиты.

**1. Сквозное шифрование (End-to-End Encryption)**

* Реализуем сквозное шифрование для всех типов сообщений и файлов, передаваемых между клиентскими приложениями.
* Используем современные алгоритмы шифрования, такие как AES (Advanced Encryption Standard), для обеспечения высокого уровня безопасности.

**2. Хеширование паролей и механизмы аутентификации**

* Реализуем механизмы хеширования паролей и солей для сохранения учетных данных пользователей в зашифрованном виде на сервере.
* Интегрируем методы аутентификации, такие как логин и пароль, а также двухфакторная аутентификация (2FA), для защиты учетных записей пользователей.

**3. Защита на уровне сети**

* Обеспечим шифрование данных при передаче между клиентскими приложениями и сервером с использованием протокола TLS.
* Настроим правила файрвола и других средств защиты сети для предотвращения атак типа Man-in-the-Middle и других сетевых угроз.

**4. Мониторинг и реагирование на инциденты**

* Разработаем систему мониторинга безопасности, которая будет отслеживать подозрительную активность и потенциальные угрозы безопасности.
* Настроим механизмы реагирования на инциденты, чтобы своевременно обнаруживать и реагировать на угрозы безопасности.

**5. Регулярное обновление и аудит безопасности**

* Реализуем систему регулярного обновления компонентов приложения, включая клиентские и серверные части, для закрытия известных уязвимостей.
* Проведем регулярный аудит безопасности приложения для выявления потенциальных уязвимостей и проблем безопасности и принятия мер по их устранению.

**6. Тестирование интегрированных механизмов защиты**

* Проведем тестирование интегрированных механизмов защиты для проверки их работоспособности и эффективности.
* Проверим работу сквозного шифрования, механизмов аутентификации, защиты на уровне сети и других аспектов безопасности.

Интеграция механизмов защиты данных обеспечит высокий уровень безопасности настольного мессенджера и защиту конфиденциальности пользователей.

# **ЗАКЛЮЧЕНИЕ**

# **СПИСОК ЛИТЕРАТУРЫ**

# **ПРИЛОЖЕНИЕ**