|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**  **«МОСКОВСКИЙ АВИАЦИОННЫЙ ИНСТИТУТ**  **(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)»** | | | | |
| **Журнал практики** | | | | |
| Институт № 8 | «Компьютерные науки и прикладная математика» | | | |
|  |  | | | |
| Кафедра | \_\_\_806\_\_\_\_\_\_\_\_\_\_\_ | | Учебная группа | \_\_М8О-411Б-19\_\_\_ |
|  |  | |  |  |
| ФИО обучающегося | | \_\_Тришин Дмитрий Александрович\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | |
|  | |  | | |
| Направление подготовки/  специальность | | 02.03.02 "Фундаментальная информатика и информационные технологии\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | |
|  | | *шифр, наименование направления подготовки/специальности* | | |
|  | |  | | |
| Вид практики | | \_\_\_\_\_\_преддипломная\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | |
|  | | *учебная, производственная, преддипломная или другой вид практики* | | |
| Оценка за практику | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Плотникова Н.О. | | |

Москва

2023

|  |  |  |
| --- | --- | --- |
| 1. **Место и сроки проведения практики:** | | |
| Наименование организации: | \_\_Кафедра 806\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| Сроки проведения практики |  | |
| дата начала практики: | \_\_09.02.2023\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| дата окончания практики: | \_\_09.05.2023\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| 1. **Инструктаж по технике безопасности:** | | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ | \_\_\_09 \_февраля\_\_\_ 2023г. |
| *подпись проводившего* | *расшифровка подписи* | *дата проведения* |
| 1. **Индивидуальное задание обучающегося:** | | |
| Разработать программное обеспечение, состоящие из распределенной системы, использующей криптографические алгоритмы шифрования на основе эллиптических кривых и способной обрабатывать поступающие запросы пользователей, и приложения для ПК, реализующего функционал онлайн-чата для общения в сети. | | |
| 1. **План выполнения индивидуального задания обучающегося:** | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Место проведения** | **Тема** | **Период выполнения** |
|  | Кафедра 806 | Инструктаж. | 09.02.2023 – 01.03.2023 |
|  | Кафедра 806 | Анализ литературы и существующих решений в предметной области для формулировки задачи | 09.02.2023 – 4.03.2023 |
|  | Кафедра 806 | Разработка подхода и выбор методов и технологий для решения задачи с обоснованием их применимости. | 05.03.2023 – 10.04.2023 |
|  | Кафедра 806 | Результаты решения поставленной задачи и их оценка. | 11.04.2023 – 18.04.2023 |
|  | Кафедра 806 | Введение (автореферат работы). | 19.04.2023 – 25.04.2023 |
|  | Кафедра 806 | Заключение (краткие выводы и перспективы дальнейшей разработки). | 26.04.2023 – 03.05.2023 |
|  | Кафедра 806 | Оформление отчета. Подведение итогов. | 03.05.2023 – 09.05.2023 |

|  |  |  |
| --- | --- | --- |
| **Утверждаю** | | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ | \_\_\_09 \_февраля\_\_\_ 2023г. |
| *подпись руководителя от МАИ* | *расшифровка подписи* | *дата утверждения\** |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ | \_\_\_09 \_февраля\_\_\_ 2023г. |
| *подпись руководителя от организации/предприятия* | *расшифровка подписи* | *дата утверждения\** |
| **Ознакомлен** | | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ | \_\_\_09 \_февраля\_\_\_ 2023г. |
| *подпись обучающегося* | *расшифровка подписи* | *дата ознакомления\** |
| 1. **Отзыв руководителя практики от организации/предприятия:** | | |
| Студент Тришин Д. А. из группы М8О-411Б-19 прошел преддипломную практику на кафедре 806 МАИ в объеме 108 часов, из которых контактная работы составляла 30 часов. Целью практики студента Тришина Д. А. была работа над выпускной квалификационной работой бакалавра по теме «Распределенная система криптографической защиты данных на основе эллиптических кривых».  При прохождении практики Тришин Д. А. продемонстрировал усвоение знаний, умений и навыков планируемых компетенций. Студент Тришин Д. А. выполнил все поставленные задачи, закрепил теоретические знания, провел анализ полученных данных, научился применять современный математический инструментарий для решения различных задач и использовать современное программное обеспечение для их решения. Также студент Тришин Д. А. научился обосновывать актуальность, теоретическую и практическую значимость темы научного исследования, проводить самостоятельные исследования в соответствии с разработанной программой и представлять результаты проведенного исследования в виде статьи или доклада.  В ходе практики Тришиным Д. А. были изучены современные методы разработки программного обеспечения в сфере веб-разработки и криптографии. Проведена самостоятельная разработка серверного приложения онлайн-чата, которое использует алгоритмы шифрования данных на основе эллиптических кривых, а также клиентское приложение для работы с распределенной системы, позволяющее безопасно обмениваться информацией между пользователями. Разработанное студентом Тришиным Д. А. программное обеспечение в полной мере решает все поставленные задачи.  При прохождении практики Тришин Д. А. продемонстрировал усвоение знаний, умений и навыков планируемых компетенций. Студент Тришин Д. А. выполнил все поставленные задачи, посетил лекции, выполнил практическую работу, выполнил индивидуальные задания. Материалы, изложенные в отчете студента Тришина Д. А., полностью соответствуют индивидуальному заданию.  Считаю возможным оценить преддипломную практику студента Тришина Д. А. на «отлично». | | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ | \_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_ 20\_\_г. |
| *подпись руководителя от организации/предприятии* | *расшифровка подписи* | *дата* |
| 1. **Отчет обучающего по практике:** | | |

# ПОСТАНОВКА ЗАДАЧИ

Темой данной работы во время преддипломной практики было создание распределенной системы криптографической защиты данных на основе эллиптических кривых.

Данные имеют огромное значение, потому что они могут дать нам важную информацию о нашем мире, помочь нам принимать решения, оптимизировать процессы и увеличивать эффективность наших действий. Однако существуют также определенные ограничения и проблемы, связанные с их использованием. Одна из главных проблем заключается в защите данных и приватности. С постоянным увеличением объема данных и их значимости, возрастает их уязвимость, и проблема безопасности данных становится все более актуальной. В результате безопасность данных становится ключевой проблемой, требующей серьезного внимания и многогранного подхода.

Для защиты данных используются криптографические методы, такие как шифрование. Одним из наиболее эффективных методов шифрования является криптография на основе эллиптических кривых. Этот метод обеспечивает высокую стойкость к взлому, что делает его идеальным для защиты конфиденциальных данных в распределенной среде. Таким образом, разработка распределенной системы криптографической защиты данных на основе эллиптических кривых является актуальной темой, которая может помочь обеспечить безопасность данных в распределенных системах и защитить конфиденциальные данные от несанкционированного доступа.

Цель работы – создание математической библиотеки исходного кода для работы с эллиптическими кривыми и разработка распределенной системы клиент-серверного приложения. Для достижения поставленной цели в работе были решены следующие задачи:

1) изучение теоретического материала по эллиптическим кривым над полями конечной характеристики;

2) написание математической библиотеки исходного кода для работы с эллиптическими кривыми над полями конечной характеристики;

3) реализация симметричного и асимметричного алгоритма шифрования на основе эллиптических кривых для создания гибридной криптосистемы;

4) разработка с учетом вопрос балансировки нагрузки клиент-серверного приложения, применяющего разработанную криптосистему.

# АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ

Криптографические алгоритмы шифрования — это методы преобразования информации из открытого вида в зашифрованный, защищенный от несанкционированного доступа и вмешательства.

Эллиптическая криптография — это метод криптографии, который использует свойства эллиптических кривых для защиты данных. Она основывается на трудности вычисления дискретного логарифма в конечном поле, который используется для генерации ключей. Ключевым элементом эллиптической криптографии является эллиптическая кривая над полем конечной характеристики.

Эллиптические кривые – это кривые, которые задаются кубическим уравнением третьей степени с использованием переменных из поля k и точкой на бесконечной прямой. Эллиптические кривые представляют собой график уравнения вида

, (1.1)

где a и b – константы, определяющие форму эллиптической кривой. Примеры эллиптических кривых приведены на рисунке 1.

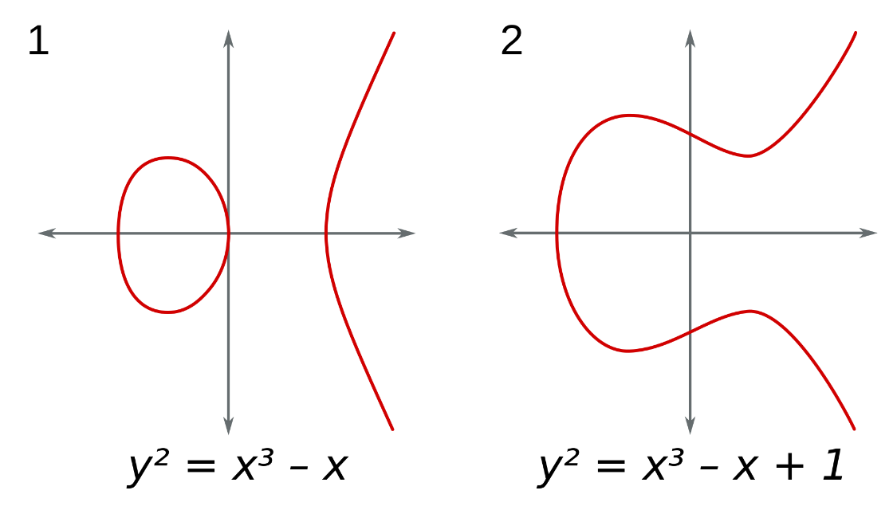


Рисунок 1 - Примеры эллиптических кривых

Одним из основных преимуществ эллиптической криптографии является то, что она обеспечивает такой же уровень безопасности при более коротких ключах, чем традиционные методы криптографии. Это делает ее особенно полезной для мобильных устройств, где ограниченный объем памяти и скорость работы являются ограничениями.

Распределенная система — это сеть, в которой узлы не централизованы и не зависят от единого управления. Она состоит из множества узлов, которые могут обмениваться информацией и ресурсами между собой напрямую. Пример распределенной системы приведен на рисунке 2.

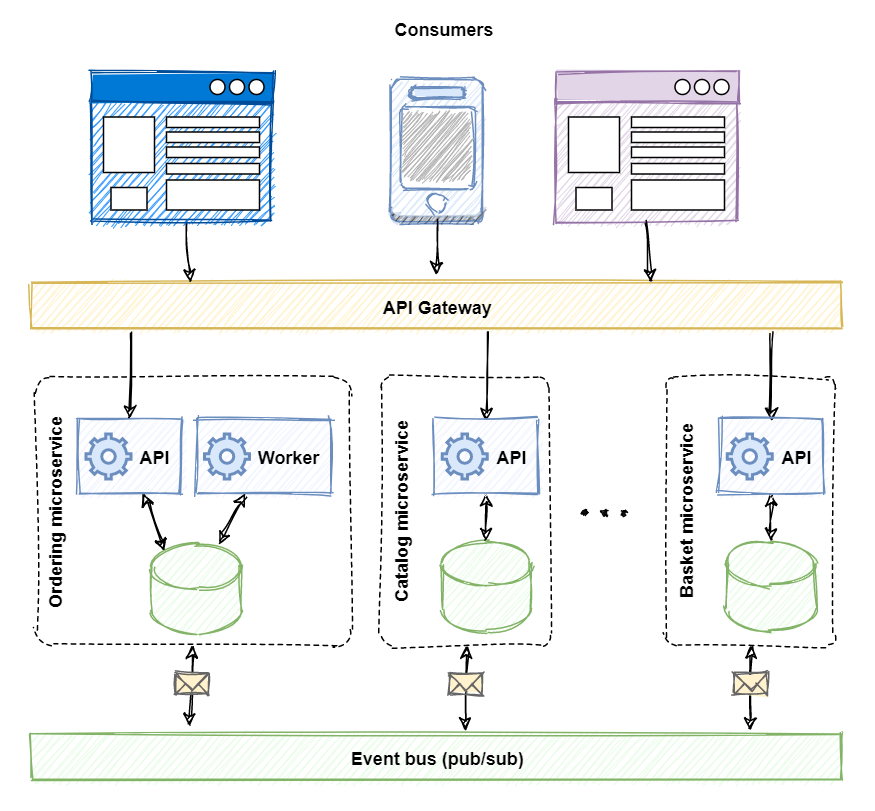


Рисунок 2 - Пример распределенной архитектуры

Структура распределенной сети зависит от конкретной реализации и ее целей. Однако, в общем случае, можно выделить следующие компоненты.

1) Узлы в распределенной сети могут выполнять различные функции, например, хранить данные, обрабатывать запросы, передавать сообщения и т.д. Узлы могут быть реализованы на различных устройствах, таких как компьютеры, мобильные устройства, роутеры, и т.д.

2) Обмен информацией между узлами происходит путем передачи сообщений. Сообщения могут содержать данные, запросы или команды. Каждое сообщение обычно содержит информацию о отправителе, получателе и содержании сообщения.

3) Распределенная сеть требует протоколов для установления соединений между узлами, обработки запросов и ответов, передачи данных, обеспечения безопасности и т.д.

4) Распределенная сеть может использовать распределенные ресурсы, такие как хранилище данных, процессорное время, пропускная способность каналов связи и т.д.

6) Распределенная сеть может использовать различные алгоритмы для решения задач, таких как маршрутизация, защита данных и т.д.

# ОБЗОР СОВРЕМЕННЫХ СРЕДСТВ РАЗРАБОТКИ

## C#

C# — это объектно-ориентированный язык программирования, который был разработан Microsoft в 2000 году. C# имеет широкую стандартную библиотеку, которая включает в себя множество функций для работы с файлами, сетью, базами данных, графикой и другими задачами.

## ASP.NET

ASP.NET — это веб-фреймворк, разработанный компанией Microsoft для создания динамических веб-приложений и веб-сайтов. ASP.NET используется для создания серверных приложений на языках программирования C#.

## WPF

Windows Presentation Foundation (WPF) — это технология разработки графических интерфейсов для приложений Windows, которая была представлена компанией Microsoft в 2006 году. WPF позволяет создавать более интерактивные и эффективные пользовательские интерфейсы с помощью визуальных элементов, таких как кнопки, списки, таблицы, графики и другие элементы управления.

## PostgreSQL

PostgreSQL - это свободная реляционная база данных с открытым исходным кодом, которая была создана в 1986 году в Университете Беркли. PostgreSQL поддерживает стандарт SQL, что делает его легко использовать для разработки приложений. SQL — это язык программирования, который используется для работы с реляционными базами данных. SQL позволяет программистам и администраторам баз данных выполнять различные операции с данными, такие как создание, изменение, удаление и извлечение информации из баз данных.

## Docker и Docker Compose

Docker — это платформа для создания, развертывания и управления приложениями в контейнерах. Он использует технологию виртуализации на уровне операционной системы, чтобы разделить приложения и их зависимости от основной операционной системы, что делает их переносимыми и легко развертываемыми на любой системе.

Docker Compose — это инструмент для описания и запуска многоконтейнерных приложений в Docker. Он позволяет описывать зависимости и конфигурации контейнеров в файле YAML, что делает управление множеством контейнеров проще и более эффективным.

# АНАЛИЗ ТРЕБОВАНИЙ И ПРОЕКТИРОВАНИЕ АРХИТЕКТУРЫ ПРИЛОЖЕНИЯ

Для разрабатываемой распределенной системы должны быть выполнение следующие требования.

1. Система должна использовать алгоритмы на эллиптических кривых для обеспечения защиты данных.
2. Система должна реализовывать функционал авторизации.
3. Система должна быть распределенной, то есть компоненты системы должны быть слабосвязанные и независимые.
4. Система должна обрабатывать входящие запросы пользователей данной системы.
5. Пользователь должен взаимодействовать с системой с помощью клиентского приложения: производить авторизацию, обмениваться данными.
6. Данные пользователей должны храниться в объектном хранилище и базе данных

Для выполнения всех требований к разрабатываемой системе была спроектирована архитектура приложения, приведенная на рисунке 3.

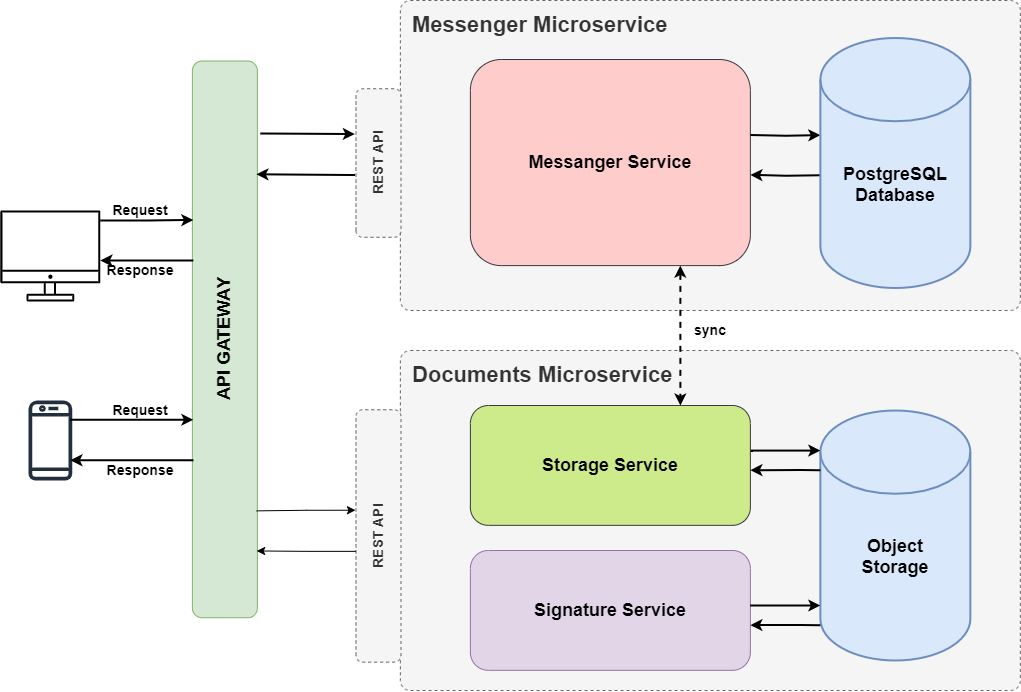


Рисунок 3 - Архитектура приложения

Для хранения данных в БД PostgreSQL была спроектирована схема хранения данных системы, приведенная на рисунке 4.

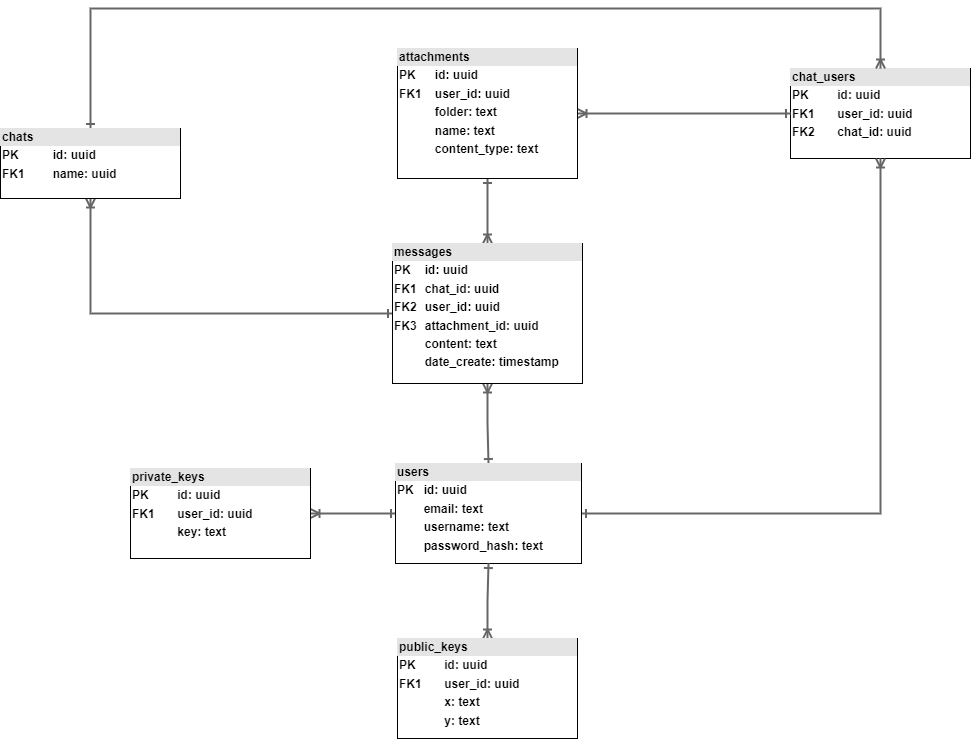


Рисунок 4 - Схема хранения данных

Клиентское приложение должно иметь пользовательский интерфейс с возможность авторизации. Окно авторизации приложения и основное окно проиллюстрированы на рисунках 5 и 6.

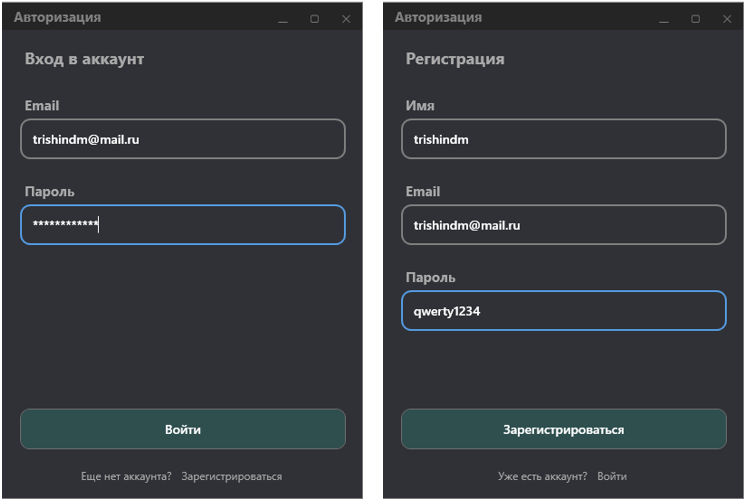


Рисунок 5 - Авторизация в системе

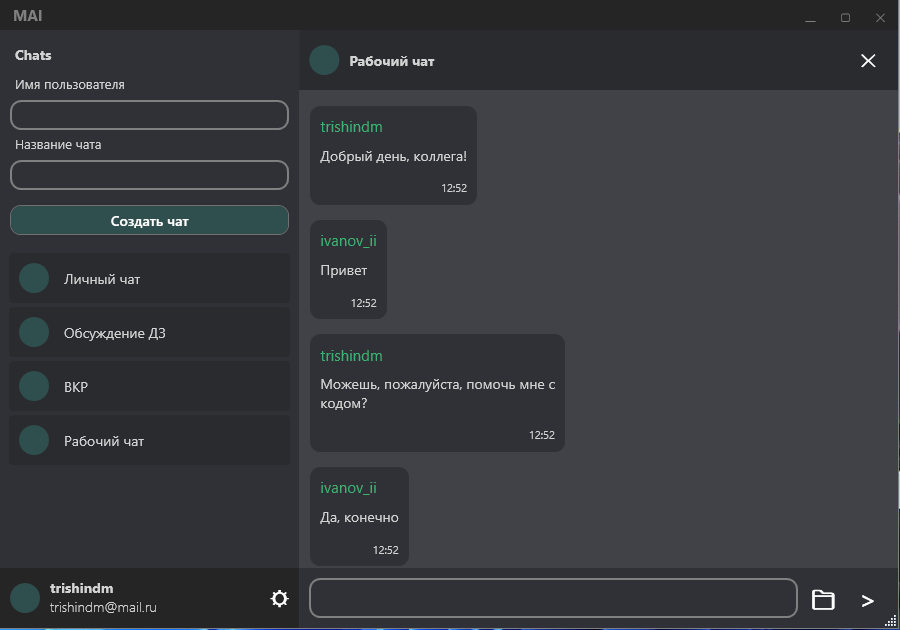


Рисунок 6 - Основное окно приложения

# РЕЗУЛЬТАТ

В результате проделанной работы анализ различных алгоритмов шифрования на основе эллиптических кривых позволил выбрать оптимальные варианты для разработки распределенной системы. Для работы с эллиптическими кривыми была разработана математическая библиотека исходного кода на языке программирования C#, позволяющая в полной мере работать с используемыми алгоритмами. Была спроектирована и разработана распределенная система на языке программирования C#, использующая математическую библиотеку для работы с алгоритмами шифрования и электронной подписи. Для демонстрации работы распределенной системы было разработано приложения для ПК, реализующее функционал онлайн-чата для безопасного общения пользователей в сети Интернет.

|  |  |  |
| --- | --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ | 09 мая 2023 г. |
| *подпись обучающегося* | *расшифровка подписи* | *дата* |