**Изображение выглядит как логотип

Автоматически созданное описаниеМИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ   
«МОСКОВСКИЙ АВИАЦИОННЫЙ ИНСТИТУТ**(национальный исследовательский университет)»

**Институт (Филиал)** № 8 «Компьютерные науки и прикладная математика» **Кафедра** 806

**Группа** М8О-411-19 **Направление подготовки** 02.03.02 Фундаментальная информатика и информационные технологии

**Профиль** Информатика и компьютерные науки

**Квалификация: бакалавр**

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА БАКАЛАВРА**

на тему: «Распределенная система криптографической защиты данных на основе эллиптических кривых»

Автор ВКРБ: Тришин Дмитрий Александрович (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)

Руководитель: Романенков Александр Михайлович (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)

Консультант: (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)

Консультант: (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)

Рецензент: (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)

**К защите допустить**

Заведующий кафедрой № 806 «Вычислительная математика  
и программирование» Крылов Сергей Сергеевич (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)

*ХХ* мая 2023 года

Москва 2023

**Изображение выглядит как логотип

Автоматически созданное описаниеМИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ   
«МОСКОВСКИЙ АВИАЦИОННЫЙ ИНСТИТУТ**(национальный исследовательский университет)»

**Институт (Филиал)** № 8 «Компьютерные науки и прикладная математика» **Кафедра** 806

**Группа** М8О-411Б-19 **Направление подготовки** 02.03.02 Фундаментальная информатика и информационные технологии

**Профиль** Информатика

**Квалификация**  **бакалавр**

**УТВЕРЖДАЮ**

Заведующий кафедрой № 806 «Вычислительная   
математика и программирование» (\_\_\_\_\_\_\_\_\_\_\_\_) С.С. Крылов

14 октября 2022 года

**ЗАДАНИЕ   
на выпускную квалификационную работу бакалавра**

**Обучающийся** Тришин Дмитрий Александрович

**Руководитель** Романенков Александр Михайлович, *ученая степень, ученое звание, должность и место работы*

**1. Наименование темы:** *Формулировка темы в соответствии с приказом – буква в букву, символ в символ, без каких-либо изменений*

**2. Срок сдачи обучающимся законченной работы:** 24 апреля 2023 года

**3. Задание и исходные данные к работе**

* *Нормативные документы, в соответствии с которыми выполнена работа (перечень)*
* *Данные и источники данных*
* *Условия и ограничения на разработку*
* *Требования по функциональности и их основания*

**Перечень иллюстративно-графических материалов**

| **№ п/п** | **Наименование** | **Количество листов (слайдов)** |
| --- | --- | --- |
| 1 | *Обоснование актуальности темы работы* | 1 |
| 2 | *Логика работы (структура – разделы и их взаимосвязи)* | 1 |
| 3 | *Характеристика стека используемых технологий* | 1 |
| 4 | *Архитектура решения, алгоритм решения задачи* | 1 |
| 5 | *Описание программной разработки* | 1 |
| 6 | *Содержание выполненных работ, связанных с подготовкой, использованием/обработкой данных* | 1 |
| 7 | *Характеристика и демонстрация результатов разработки* | 1 |
| 8 | *Оценка полученных результатов по метрикам (исходя из специфики разработанного решения)* | 1 |

**4. Перечень подлежащих разработке разделов и этапы выполнения работы:**

| № п/п | Наименование раздела или этапа | Трудоемкость в % от полной трудо­емкости квалифи­кационной работы | Срок выполнения | Примечание |
| --- | --- | --- | --- | --- |
| 1 | *Анализ публикаций и практики деятельности в предметной области для обоснования постановки задачи, подлежащей разработки* | 15 | 18.12.2022 |  |
| 2 | *Разработка подхода к решению задачи, подлежащей разработке с обоснованием выбора технологий для реализации* | 35 | 13.02.2023 |  |
| 3 | *Результаты решения поставленной задачи и их оценка* | 25 | 27.03.2023 |  |
| 4 | Введение *(автореферат работы)* | 15 | 10.04.2023 |  |
| 5 | Заключение (краткие выводы и перспективы дальнейшей разработки темы) | 10 | 17.04.2023 |  |

**5. Исходные материалы и пособия:**

– Список литературы (основные работы, 25-30% от приведенного в работе списка)

**6. Дата выдачи задания:** 14 октября 2022 года

Руководитель (\_\_\_\_\_\_\_\_\_\_\_\_\_) И. О. Фамилия

Задание принял к исполнению (\_\_\_\_\_\_\_\_\_\_\_\_\_) И.О. Фамилия

## **РЕФЕРАТ**

Выпускная квалификационная работа бакалавра состоит из 00 страниц, 00 рисунков, 00 таблиц, 00 использованных источников, 00 приложений.

РАСПРЕДЕЛЕННАЯ СИСТЕМА КРИПТОГРАЧИСЕКОЙ ЗАЩИТЫ ДАННЫХ НА ОСНОВЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Целью данной работы является исследование применения криптографических алгоритмов шифрования на основе эллиптических кривых для защиты данных и реализация распределенной системы криптографической защиты данных с использованием разработанных инструментов для работы с эллиптическим кривыми. Были использованы материалы о существующих алгоритмах шифрования и о применении этих алгоритмов в существующих системах, использующих эти криптографические алгоритмы для шифрования и дальнейшего хранения данных. Для реализации был использован язык программирования C#, фреймворки ASP.NET и WPF. В результате было разработана библиотека исходного кода для работы с эллиптическими кривыми и клиент-серверное приложение мессенджера, состоящее из распределенной системы, использующей алгоритм шифрования на основе эллиптических кривых для защиты данных пользователей, и приложения для персональных компьютеров для взаимодействия с распределенной системой. Разработанное приложение может использоваться для обеспечения безопасности общения и хранения данных компаний.

СОДЕРЖАНИЕ

[РЕФЕРАТ 4](#_Toc133831417)

[ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ 7](#_Toc133831418)

[ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ 8](#_Toc133831419)

[ВВЕДЕНИЕ 9](#_Toc133831420)

[1 АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ 13](#_Toc133831421)

[1.1 Криптографические алгоритмы шифрования 13](#_Toc133831422)

[1.1.1 Симметричные алгоритмы шифрования 14](#_Toc133831423)

[1.1.2 Асимметричные алгоритмы шифрования 16](#_Toc133831424)

[1.1.3 Алгоритмы шифрования на эллиптических кривых 18](#_Toc133831425)

[1.2 Распределенные системы 19](#_Toc133831426)

[1.2.1 Сведения о распределенных системах 19](#_Toc133831427)

[1.3 Исследование существующих распределенных криптосистем 23](#_Toc133831428)

[2 РАЗРАБОТКА РЕШЕНИЯ 24](#_Toc133831429)

[2.1 Описание решения поставленной задачи 24](#_Toc133831430)

[2.1.1 Математическая библиотека 24](#_Toc133831431)

[2.1.2 Криптосистема 25](#_Toc133831432)

[2.1.3 Распределенная система 27](#_Toc133831433)

[2.1.3.1 REST API сервис 28](#_Toc133831434)

[2.1.3.2 Сервис баз данных 29](#_Toc133831435)

[2.1.3.3 Сервис файлового хранилища 30](#_Toc133831436)

[2.2 Выбор программных средств разработки 30](#_Toc133831437)

[2.2.1 C# 30](#_Toc133831438)

[2.2.2 ASP.NET 31](#_Toc133831439)

[2.2.3 WPF 31](#_Toc133831440)

[2.2.4 PostgreSQL 31](#_Toc133831441)

[2.2.5 Docker и Docker Compose 31](#_Toc133831442)

[2.3 Описание программной разработки 31](#_Toc133831443)

[3 РЕЗУЛЬТАТЫ РАБОТЫ 32](#_Toc133831444)

[3.1 Характеристика условий и места применения разработки 32](#_Toc133831445)

[3.2 Результаты работы разработанного программного кода 32](#_Toc133831446)

[3.2.1 Серверное приложение 32](#_Toc133831447)

[3.2.2 Клиентское приложение 32](#_Toc133831448)

[3.3 Технические характеристики разработанного приложения 32](#_Toc133831449)

[ЗАКЛЮЧЕНИЕ 33](#_Toc133831450)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 34](#_Toc133831451)

[ПРИЛОЖЕНИЕ А Наименование приложения 35](#_Toc133831452)

# **ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ**

В настоящей выпускной квалификационной работе бакалавра применяют следующие термины с соответствующими определениями:

|  |  |
| --- | --- |
| *C#* | *– определение* |
| *.NET* | *– определение* |
| *ASP.NET* | *– определение* |
| *WPF* | *– определение* |
| *Docker* | *– определение* |
| *Docker Compose* | *– определение* |
| *REST API* | *– определение* |
| *Entity Framework* | *– определение* |

# **ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ**

В настоящей выпускной квалификационной работе бакалавра применяют следующие сокращения и обозначения:

|  |  |
| --- | --- |
| *ЭП* | *– Электронная подпись* |
| *Аббревиатура* | *– детальная расшифровка* |
| *Аббревиатура* | *– детальная расшифровка* |
| *Аббревиатура* | *– детальная расшифровка* |
| *Обозначение* | *– детальная расшифровка* |
| *Обозначение* | *– детальная расшифровка* |
| *Обозначение* | *– детальная расшифровка* |
| *Обозначение* | *– детальная расшифровка* |
| *Обозначение* | *– детальная расшифровка* |
| *Обозначение* | *– детальная расшифровка* |
| *Обозначение* | *– детальная расшифровка* |
| *Обозначение* | *– детальная расшифровка* |

# **ВВЕДЕНИЕ**

В современном мире, который быстро и неумолимо изменяется, данные играют все более важную роль. Мы живем в эпоху, когда объем данных, которые мы производим, растет экспоненциально. Не только компьютерные системы и интернет генерируют огромные объемы данных, но и мобильные устройства, социальные сети, онлайн-торговые платформы и другие технологии собирают и хранят данные о нас и нашем окружении.

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. Данные используются в различных сферах деятельности, таких как экономика, медицина, наука, технологии, государственное управление, и многие другие.

Одним из ключевых аспектов данных является их количественная и качественная характеристика. В современном мире существует огромное количество данных, их обработка и интерпретация требуют высококвалифицированных специалистов и современных технологий. Правильно обработанные данные могут помочь нам принимать более обоснованные решения, оптимизировать бизнес-процессы, повышать эффективность производственных и научных процессов, а также создавать новые продукты и услуги.

Важным аспектом данных является их интерпретация и использование. Данные могут быть использованы для обнаружения закономерностей и тенденций, которые могут помочь нам принимать более обоснованные решения. Однако, неправильное использование данных или неправильная их интерпретация может привести к ошибкам и нежелательным последствиям. Поэтому, правильная обработка и интерпретация данных является критически важным элементом в их значимости для нашей жизни.

Несмотря на значимость данных в нашей жизни, 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.

Данные могут быть украдены, изменены или уничтожены злоумышленниками, что может привести к серьезным последствиям, включая финансовые потери, утечку конфиденциальной информации и нарушение прав человека. Поэтому безопасность данных становится ключевой проблемой, требующей серьезного внимания и многогранного подхода.

Актуальность темы данной работы связана с увеличивающейся необходимостью защиты данных в интернете. В современном мире большинство процессов осуществляется через компьютеры и Интернет, и большое количество конфиденциальных данных передается по сети. Однако это также означает, что данные могут быть украдены или скомпрометированы злоумышленниками.

Для защиты этих 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.

Кроме того, в современном мире распределенные системы становятся все более популярными. Эти системы включают в себя несколько компьютеров, которые работают вместе для выполнения задач. Криптографическая защита данных в распределенных системах также становится все более важной, так как она может быть наиболее уязвимой точкой в системе.

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.

Таким образом, выполненная работа актуальна и с научно-методической/теоретической, и с практической точек зрения.

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.

Работа основывалась на следующих инструментах и методах. Для разработки был выбран язык программирования C#. C# *–* это объектно-ориентированный язык общего назначения, разработанный компанией Microsoft в 2001 году. Клиент-серверное приложения задействует в себе два фреймворка. ASP.NET - платформа разработки веб-приложений, в состав которой входят: веб-сервисы, программная инфраструктура, модель программирования. ASP.NET используется для создания REST API приложения, отвечающего за основную логику приложения. Для хранения данных была выбрана реляционная база данных PostgreSQL. Для разработки клиентского приложения была выбрана система для построение приложений под систему Windows под названием Windows Presentation Foundation, сокращенно WPF. Для развертывания распределенной системы на серверной инфраструктуре был использован Docker – программное обеспечение для автоматизации развертывания и управления приложениями в средах и Docker Compose – инструментальное средство, входящее в состав утилиты Docker.

Основными результатами, полученными в работе, являются:

1. Библиотека исходного кода для работы с эллиптическими кривыми над конечными полями
2. Распределенная система, состоящая из основного REST API приложения, сервера баз данных и сервера хранилища документов, использующее разработанную криптосистему для защиты данных;
3. Приложение для ПК под управлением ОС Windows, реализующее функционал онлайн-чата

Результаты работы предназначены для использования как в бизнес-сфере, так и в государственном управлении для обеспечения безопасности и конфиденциальности данных.

Использование разработки позволяет обеспечить высокий уровень защиты данных в распределенной среде. Система использует алгоритмы криптографической защиты данных на основе эллиптических кривых, которые обеспечивают высокую степень безопасности и эффективности при обработке больших объемов данных.

Кроме того, система обеспечивает возможность распределения данных между различными узлами сети, что позволяет обеспечить высокую отказоустойчивость и надежность при хранении и передаче данных. В целом, разработанная распределенная система позволяет обеспечить безопасное и эффективное хранение и передачу данных в распределенной среде.

# **1 АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ**

## **Криптографические алгоритмы шифрования**

Криптографические алгоритмы шифрования — это методы преобразования информации из открытого вида в зашифрованный, защищенный от несанкционированного доступа и вмешательства. Они являются неотъемлемой частью современных систем безопасности и используются для защиты конфиденциальной информации в различных областях, таких как банковское дело, электронная коммерция, государственная безопасность, медицинские записи и многих других.

Криптографические алгоритмы шифрования позволяют обеспечить конфиденциальность, целостность и доступность данных. Они защищают данные от несанкционированного доступа и изменения, обеспечивая конфиденциальность передачи информации от отправителя к получателю. Также они обеспечивают аутентификацию, т.е. проверку подлинности отправителя и получателя информации.

Одним из основных принципов криптографии является использование ключей шифрования и дешифрования. Криптографический ключ — это секретный код или последовательность символов, используемая в криптографических алгоритмах для защиты конфиденциальности и целостности данных. Он служит для шифрования и дешифрования информации, а также для создания электронной подписи и проверки подлинности сообщения. Ключ может быть симметричным, когда используется один и тот же ключ для шифрования и дешифрования данных, или асимметричным, когда используется пара ключей — открытый и закрытый — для шифрования и дешифрования информации. Криптографический ключ является критически важным элементом в обеспечении безопасности данных и защите от несанкционированного доступа к информации. Ключи могут быть симметричными (когда один и тот же ключ используется для шифрования и дешифрования) и асимметричными (когда разные ключи используются для шифрования и дешифрования). Шифрование происходит с помощью алгоритма, который осуществляет преобразование исходной информации (открытого текста) в зашифрованный вид (шифрованный текст). Зашифрованный текст может быть передан по открытым каналам связи или храниться на ненадежных устройствах без риска несанкционированного доступа к информации.

Криптографические алгоритмы шифрования постоянно совершенствуются и обновляются, чтобы усилить защиту данных от новых видов атак и взломов. Без использования криптографических алгоритмов шифрования информация может быть легко украдена или изменена, что может привести к серьезным последствиям для людей, компаний и государств.

## **Симметричные алгоритмы шифрования**

Симметричный алгоритм шифрования — это метод шифрования данных, при котором используется один и тот же ключ как для зашифровки, так и для расшифровки сообщения. То есть, если отправитель и получатель используют один и тот же ключ для шифрования и расшифровки сообщения, то такой алгоритм называется симметричным.

В симметричном шифровании данные передаются в виде шифрованного текста, который можно расшифровать только при помощи ключа, известного только отправителю и получателю сообщения. Примерами симметричных алгоритмов шифрования являются AES (Advanced Encryption Standard), DES (Data Encryption Standard) и IDEA (International Data Encryption Algorithm).

В настоящее время для симметричного шифрования используются четыре разных виды шифров:

* Поточные шифры – это шифры, которые преобразуют один байт данных за раз. Они используют один ключ для генерации псевдослучайной последовательности, которая затем комбинируется с сообщением для получения зашифрованного сообщения. Примерами поточных шифров являются RC4, Salsa20 и ChaCha20;
* Блочные шифры – это разновидность шифров, где данные преобразуются блоками фиксированного размера (обычно 64 или 128 бит). Каждый блок данных заменяется на зашифрованный блок данных с использованием ключа. Примерами блочных шифров являются AES, Blowfish и DES;
* Сети Фейстеля — один из методов построения блочных шифров. Преобразования в таком шифре состоят из раундов, в каждом из которых блок данных разбивается на две половины, которые затем преобразуются с использованием ключа. Примерами сетей Фейстеля являются алгоритмы шифрования DES и Blowfish;
* Шифры с заменой и перестановкой – это шифры, которые используют операции замены и перестановки для шифрования данных. Они состоят из раундов, в каждом из которых происходят операции замены и перестановки данных. Примерами шифров с заменой и перестановкой являются AES и Serpent;

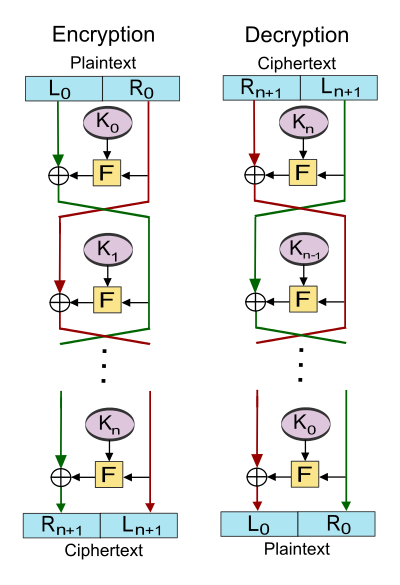


Рисунок 1. Сеть Фейстеля

Каждый из этих типов шифров имеет свои преимущества и недостатки, и выбор шифра зависит от конкретной задачи и уровня безопасности, который требуется достичь. Характеристиками алгоритмов симметричного шифрования являются:

* Стойкость
* Длина ключа
* Число раундов
* Длина шифруемого блока
* Сложность реализации
* Сложность преобразований

## **Асимметричные алгоритмы шифрования**

Асимметричное шифрование — это метод криптографии, в котором для шифрования и дешифрования используются два ключа: открытый и закрытый. Открытый ключ шифрования может быть передан по открытому каналу связи и использован для зашифрования сообщения или проверки цифровой подписи. Закрытый ключ же используется для расшифровки сообщения или создания цифровой подписи.

Использование двух ключей позволяет решить проблему безопасного обмена ключами, которая возникает при использовании симметричного шифрования. При симметричном шифровании обе стороны должны знать один и тот же секретный ключ, который может быть использован как для шифрования, так и для расшифровки сообщений. Однако, передача секретного ключа по открытому каналу является небезопасной, так как любой злоумышленник может перехватить ключ и использовать его для расшифровки сообщений.

Системы с открытым ключом решают эту проблему, позволяя каждому участнику создать свою пару ключей. Открытый ключ может быть передан любому, кто хочет отправить сообщение, и использован для шифрования, но только владелец закрытого ключа может расшифровать сообщение. Кроме того, владелец закрытого ключа может использовать его для создания цифровой подписи, которая может быть проверена с помощью соответствующего открытого ключа.

Таким образом, системы с открытым ключом позволяют создавать безопасный канал связи между двумя участниками, используя открытый канал для передачи открытых ключей, которые могут быть свободно распространены. Это делает асимметричное шифрование очень удобным для использования в сетях, таких как интернет, где коммуникации происходят между несколькими участниками, которые не имеют заранее согласованных секретных ключей.

Схема шифрования и дешифрования выглядит следующим образом. Пусть – пространство ключей, а и – это ключи шифрования и дешифрования. - функция шифрования для произвольного ключа такая, что , где – пространство шифротекстов, а –пространство сообщений. Функция дешифрования позволяет расшифровать шифротекст и найти исходное сообщение : – набор шифрования, – набор для расшифрования. Каждая пара имеет свойство: зная , невозможно решить уравнение , то есть для данного произвольного шифротекста невозможно найти сообщение . Это означает, что по данному невозможно определить ключ дешифрования .

Ниже представлена схема шифрования информации, передаваемой лицом А лицу Б. Это могут быть как физические лица, так и организации, но для простоты восприятия принято отождествлять участников передачи информации. В таком случае А – это собеседник по имени Алиса, а Б – собеседник по имени Боб.

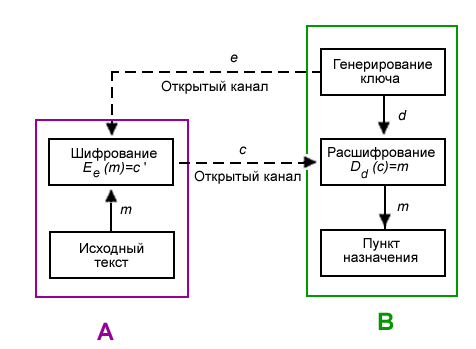


Рисунок 2. Схема передачи информации между участниками беседы

## **Алгоритмы шифрования на эллиптических кривых**

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, которая представляет собой график уравнения вида , где *a* и *b* – константы, определяющие форму кривой, а x и y – координаты точки на кривой. Поля конечной характеристики 2 () отличаются от бесконечных полей тем, что они содержат только конечное число элементов. Это означает, что на эллиптической кривой над полем конечной характеристики существует только конечное число точек.

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.

Кроме того, эллиптическая криптография считается более безопасной, поскольку существующие алгоритмы взлома сложнее, чем в традиционных методах криптографии. Существуют методы атаки на эллиптическую криптографию, но они требуют намного больше вычислительных ресурсов и времени, чем атаки на другие криптографические системы.

Однако, несмотря на все преимущества, эллиптическая криптография требует более сложных математических вычислений, чем традиционные методы, что делает ее более медленной и требовательной к вычислительным ресурсам.

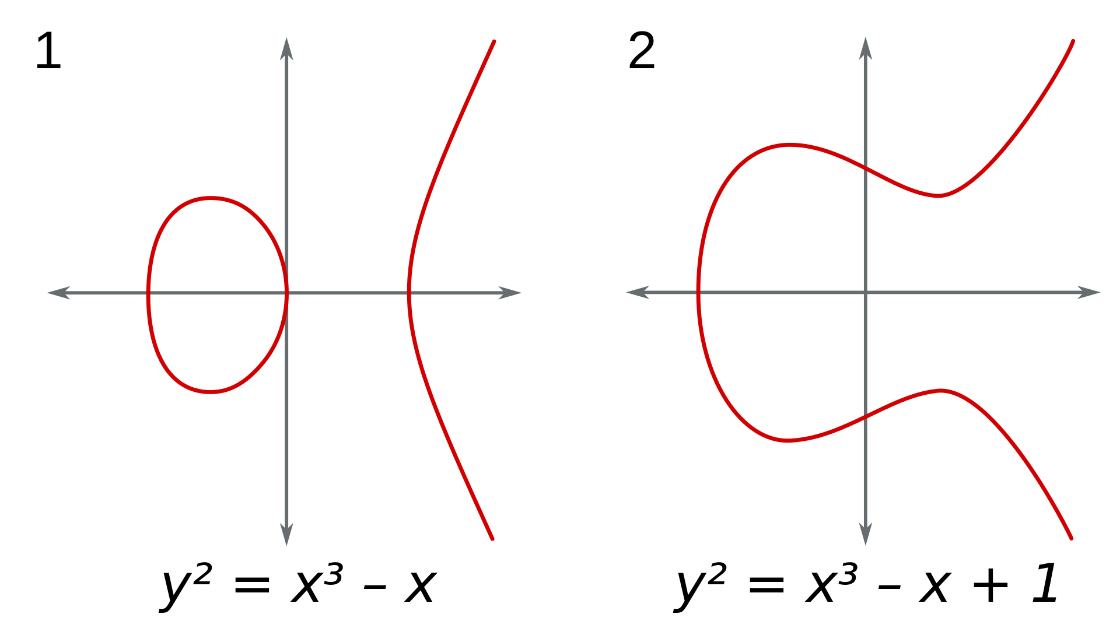


Рисунок 3. Примеры эллиптических кривых.

## **Распределенные системы**

## **Сведения о распределенных системах**

Распределенная система — это система, которая состоит из множества компьютеров (узлов), связанных между собой сетью и работающих вместе как единое целое. В такой системе каждый узел выполняет свою задачу и обменивается информацией с другими узлами. Распределенная система может располагаться на нескольких физических узлах или же на нескольких компьютерах внутри одного физического узла.

Распределенные системы используются во многих областях, где требуется координация децентрализованных процессов и обработка больших объемов данных. Например, в области интернета вещей, облачных вычислений, сенсорных сетей, блокчейн-технологий, машинного обучения, игровой индустрии, распределенных баз данных, вычислительных кластерах и т.д. Распределенные системы также широко используются для решения задач высокопроизводительных вычислений, таких как моделирование климата, анализ геномных данных, расчет физических процессов и т.д

Криптография играет важную роль в защите распределенных систем от различных угроз и атак. Распределенные системы обычно состоят из множества узлов, которые обмениваются данными и информацией между собой. Криптографические методы и протоколы используются для обеспечения конфиденциальности, целостности и аутентификации данных, передаваемых между узлами. Например, алгоритмы шифрования и дешифрования, цифровые подписи, протоколы аутентификации, ключевое управление — все это является необходимым для обеспечения безопасности в распределенных системах. Кроме того, криптография может использоваться для реализации различных механизмов защиты от атак, таких как атаки на отказ в обслуживании (DoS-атаки), атаки на перехват и изменение данных, атаки на подмену узлов, и многих других.

Таким образом, криптография является важным компонентом в области распределенных систем и играет ключевую роль в обеспечении их безопасности и защите.

## **Структура распределенной системы**

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 4.

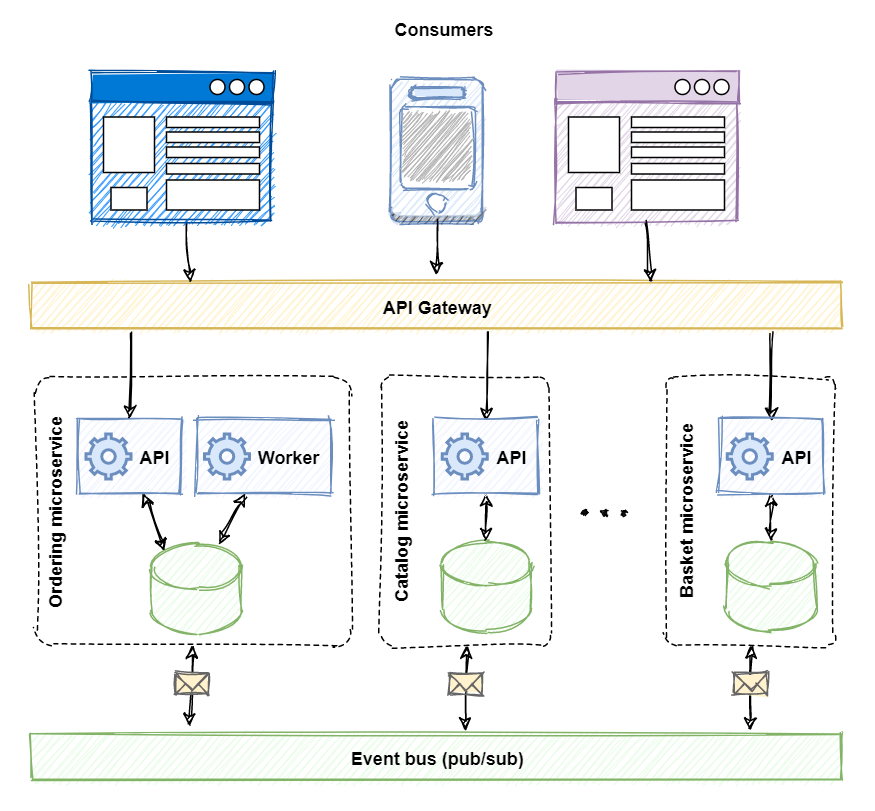


Рисунок 4. Пример распределенной системы

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

* 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.;
* 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;
* Распределенная сеть требует протоколов для установления соединений между узлами, обработки запросов и ответов, передачи данных, обеспечения безопасности и т.д.;
* Распределенная сеть может использовать распределенные ресурсы, такие как хранилище данных, процессорное время, пропускная способность каналов связи и т.д.;
* Топология сети описывает структуру связей между узлами в сети. Распределенная сеть может использовать различные топологии, такие как полная сеть, дерево, кольцо, шина, P2P сеть и т.д.
* Распределенная сеть может использовать различные алгоритмы для решения задач, таких как маршрутизация, репликация данных, консенсус и т.д.;

В целом, структура распределенной сети может быть очень сложной и зависеть от конкретного применения. Однако, понимание основных компонентов и принципов ее работы позволяет разработчикам создавать более эффективные и надежные распределенные системы.

## **Виды распределенных систем**

Распределенные системы могут быть различных видов в зависимости от архитектуры и способа организации взаимодействия между узлами. Ниже приведены некоторые примеры распределенных систем и компаний, которые используют их:

* Клиент-серверная архитектура – это архитектура, в которой существует сервер, который обслуживает несколько клиентов. Клиент-серверная архитектура используется, к примеру, в компании Google, Facebook, Amazon в онлайн-сервисах;
* Peer-to-Peer архитектура – архитектура, все узлы которой имеют равные возможности и работают независимо друг от друга, без централизованного управления. Skype — это программа для видео- и голосовой связи, использующая P2P технологии;
* Кластеризованная архитектура – вид архитектуры, в которой несколько узлов объединяются в кластер, который работает как единый узел. Компании, использующие кластеризованную архитектуру, - Apache и Google;
* Grid-системы: это сеть из географически распределенных компьютеров, которые работают вместе для решения одной задачи.
* Cloud-системы: это сеть из удаленных серверов, которые предоставляют вычислительные ресурсы, хранилище данных и другие услуги через интернет. Используется в таких продукатх, как Amazon Web Services, Microsoft Azure и Google Cloud. Все эти компании предоставляют облачные сервисы для хранения данных, разработки приложений и т.д.

## **1.3 Исследование существующих распределенных криптосистем**

Текст главы.

*Рекомендуемый объем первой главы – 10–12 страниц*

# **2 РАЗРАБОТКА РЕШЕНИЯ**

## **Описание решения поставленной задачи**

## **Математическая библиотека**

В первую очередь для работы с эллиптическими кривыми и алгоритмами, которые их используют, необходимо разработать библиотеку исходного кода для работы с эллиптическими кривыми над полями конечной характеристики. Библиотека состоит из набора основных сущностей, необходимых для дальнейшей работы, а также реализует набор операций над эллиптическими кривыми, а именно:

* Сложение точек — это операция, при которой две точки на кривой складываются, чтобы получить третью точку, которая также лежит на кривой. Сумма точек используется для шифрования и подписывания сообщений в криптографии на эллиптических кривых.
* Умножение точки на скаляр — это операция, при которой точка на кривой умножается на целое число, чтобы получить новую точку на кривой. Эта операция используется для генерации ключей в криптографии на эллиптических кривых.
* Вычисление порядка точки — это операция, при которой вычисляется количество точек на кривой, которые можно получить, складывая выбранную точку на кривой себя саму многократно. Знание порядка точки важно для безопасности в криптографии на эллиптических кривых.
* Вычисление дискретного логарифма — это операция, при которой вычисляется целое число, которое является степенью известной точки на кривой, чтобы получить другую заданную точку на кривой. Эта операция служит основой для создания криптографических протоколов на эллиптических кривых, таких как протокол Диффи-Хеллмана на эллиптических кривых.

## **Криптосистема**

Для обеспечения защиты системы необходимо разработать систему криптографической защиты. Криптографическая система будет использовать как симметричные алгоритмы шифрования, так и асимметричные.

В первую очередь всеми участниками распределенной системы согласуется эллиптическая кривая, которая будет использоваться для шифрования данных. Для решения поставленной задачи была выбрана эллиптическая кривая под названием SECP256R1, также известная как P-256.

Эта эллиптическая кривая определяется уравнением , где *a* и *b* – константы, определенные стандартом ANSI X9.62, а *x* и *y* - координаты точки на кривой. Одним из основных достоинств эллиптической кривой SECP256R1 является ее безопасность. Благодаря размеру поля и параметрам кривой, она обеспечивает высокую стойкость к криптоанализу и предотвращает возможность атак с использованием известных алгоритмов. Также эллиптическая кривая SECP256R1 хорошо подходит для использования в различных приложениях благодаря своей эффективности. Она позволяет производить операции шифрования и подписи данных с высокой скоростью и использовать меньшее количество ресурсов, чем при использовании других криптографических алгоритмов.

Для шифрования данных, прежде всего, необходимо создать ключи шифрования. Эллиптическая кривая определяет следующие параметры:

* *p* – простое число, задающее размер конечного поля
* *a* и *b* – коэффициенты уравнения эллиптической кривой
* *G* – базовая точка, генерирующая подгруппу
* *n* – порядок подгруппы
* *h* – кофактор подгруппы.

Алгоритмы эллиптических кривых будут работать в циклической подгруппе эллиптической кривой над конечным полем. В результате параметрами области определения для алгоритмов является шестёрка (p, a, b, G, n, h). В результате будет сгенерировано два ключа – приватный и публичный. Приватный ключ – это случайное большое число, а публичный ключ – точка (X, Y) на эллиптической кривой.

Для обмена ключами используется алгоритм ECDH — это криптографический протокол, используемый для обмена ключами шифрования между участниками общения в сети с целью обеспечения безопасности передачи данных. Он обеспечивает безопасный обмен ключами, так как любой несанкционированный пользователь, который пытается перехватить данные, не сможет получить секретный ключ без знания закрытого ключа. Данный алгоритм основан на криптографических алгоритмах эллиптических кривых и является аналогом алгоритма Диффи-Хеллмана для классической криптографии.

Для шифрования данных используется алгоритм шифрования AES — это симметричный алгоритм блочного шифрования, который шифрует данные блоками размером 128 бит, используя ключи длиной 128, 192 или 256 бит. AES работает в несколько раундов, где каждый раунд состоит из различных этапов, таких как замена байтов, перемешивание столбцов и смещение строк. В результате каждого раунда получается новый блок данных, который используется для следующего раунда. Число раундов зависит от размера ключа - для ключей длиной 128 бит используется 10 раундов, для ключей длиной 192 бит - 12 раундов, а для ключей длиной 256 бит - 14 раундов. В начале процесса шифрования, исходный текст разбивается на блоки по 128 бит, которые затем проходят через начальный раунд шифрования, в котором каждый байт заменяется на другой байт из предопределенной таблицы замен. Затем происходит перемешивание столбцов и смещение строк, чтобы получить новый блок данных, который подвергается следующему раунду шифрования. После нескольких раундов шифрования, получается зашифрованный блок данных, который можно отправлять по сети или сохранять на диске. Для дешифрования данных, процесс применяется в обратном порядке, начиная с последнего раунда и заканчивая начальным раундом. В процессе дешифрования, каждый блок данных проходит через обратные этапы, чтобы получить исходный текст.

Для создания и проверки электронных подписей используется алгоритм ECDSA — это метод создания электронной подписи, который использует эллиптические кривые. Для создания электронной подписи необходимы закрытый и открытый ключи шифрования. Закрытый ключ хранится только у владельца и используется для создания электронной подписи. Открытый ключ может быть распространен публично и используется для проверки электронной подписи. Во время создания электронной подписи сообщения вычисляется хеш-функцию, которая сжимает сообщение до фиксированной длины и в конечном счете возвращает фиксированный результат. Затем используется закрытый ключ шифрования для создания электронной подписи, которая включает информацию о сообщении и публичном ключе. Любой пользователь может убедиться в подлинности подписи, используя открытый ключ и сравнивая результат с хеш-значением исходного сообщения.

## **Распределенная система**

Распределенная система состоит из нескольких компонентов, приведенных на рисунке ниже.

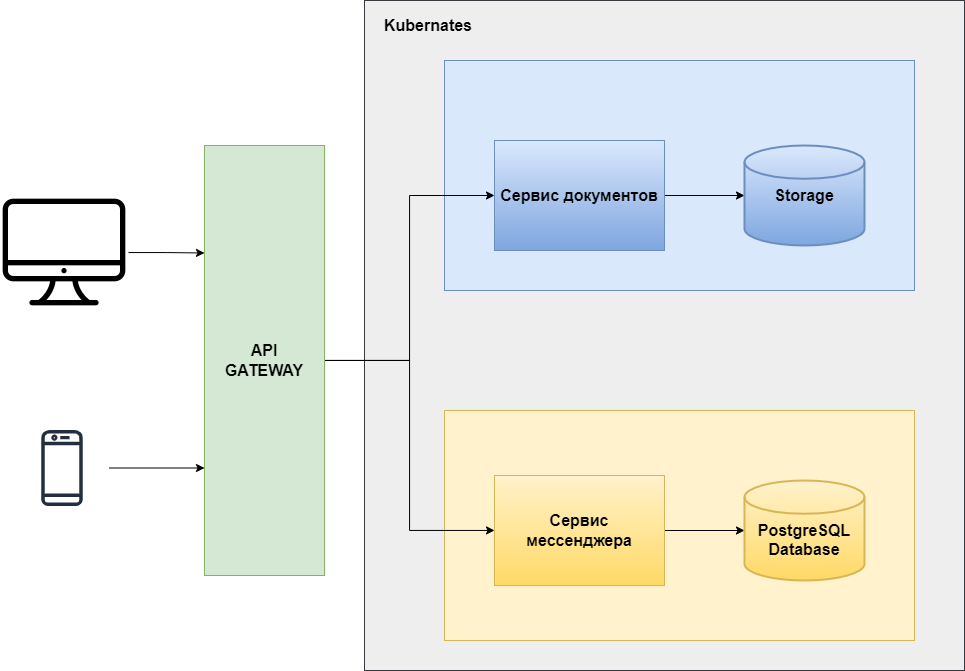


Рисунок 5. Архитектура приложения

Для реализации распределенной системы была выбрана клиент-серверная архитектура. Данная разновидность распределенной архитектуры состоит из сервера, который обслуживает несколько клиентов. Приложение представляет из себя мессенджер, использующий разработанную библиотеку для работы с эллиптическими кривыми и алгоритмами для обеспечения надежной защиты данных пользователей. Приложение имеет микросервисную архитектуру. Микросервисная архитектура — это способ разработки программного обеспечения, в котором приложение разбивается на небольшие самостоятельные блоки, называемые микросервисами. Каждый микросервис выполняет свою специфическую функцию и может взаимодействовать с другими микросервисами, используя API или другие методы коммуникации. Этот подход помогает сделать приложение более масштабируемым, гибким и легко изменяемым, что может упростить его разработку и обслуживание. Кроме того, микросервисы могут быть развернуты и масштабированы независимо друг от друга, что позволяет более эффективно использовать вычислительные ресурсы и повышать отказоустойчивость.

В соответствии с микросервисной архитектурой было спроектировано два самостоятельных сервиса: сервис мессенджера, содержащий основную бизнес-логику, и сервис документов, отвечающий за хранение документов и работу с электронными подписями. Для объединения микросервисов в единый компонент используется паттерн API Gateway — это паттерн проектирования, используемый для создания единой точки входа в микросервисную архитектуру, который облегчает доступ и управление множеством микросервисов. Суть этого паттерна заключается в том, что все запросы к микросервисам проходят через единую точку входа.

## **REST API сервис**

REST — это стиль проектирования, используемый для проектирования веб-сервисов и API. Он основан на принципе организации взаимодействия между клиентом и сервером через стандартные HTTP-методы, такие как GET, POST, PUT, DELETE и т.д., и ресурсы, которые идентифицируются уникальными URI (Uniform Resource Identifier). Основной принцип REST — это разделение клиента и сервера, что позволяет улучшить масштабируемость и гибкость приложений. Клиент и сервер обмениваются данными в формате, общеизвестном как JSON или XML, и общий формат сообщений позволяет легко интегрировать приложения, разработанные на разных платформах. REST также поддерживает кэширование, что может улучшить производительность, и не требует состояния сессии на стороне сервера, что упрощает масштабирование и увеличивает надежность приложения. REST является одним из наиболее распространенных и удобных способов взаимодействия между клиентом и сервером в современном веб-программировании. Он широко используется в различных приложениях, включая социальные сети, мобильные приложения и облачные сервисы.

Данный сервис представляет из себя REST API сервис, содержащий основную бизнес-логику приложения и реализующий CRUD операции с базой данных. Приложение имеет трехуровневую архитектуру, состоящую из следующих уровней:

* Уровень бизнес-логики. Этот слой содержит в себе основную логику приложения и является центральным, независимым слоем, вокруг которого выстраивается приложение;
* Уровень доступа к данных. Этот слой определяет, где и в каком виде хранятся данные, с которыми работает приложение;
* Уровень API. Этот слой реализует REST API для взаимодействия микросервиса с внешним миром.

Выбор трехуровневой монолитной архитектуры решает множество архитектурных проблем небольших приложений. Разделение функциональности на три уровня облегчает масштабирование приложения и улучшает его гибкость. Каждый уровень может быть развернут и масштабирован независимо, что упрощает управление ресурсами. Разделение бизнес-логики и уровня данных помогает обеспечить более высокий уровень безопасности. Бизнес-логика не имеет прямого доступа к данным, что позволяет лучше контролировать доступ к ним и уменьшить риски несанкционированного доступа. Как итог, трехуровневая архитектура повышает читаемость и улучшает поддержку кода. Разделение кода на три уровня позволяет разработчикам работать с более четко определенными участками кода, что упрощает его понимание и поддержку.

## **Сервис баз данных**

Хранением данных пользователей в системе занимается сервер баз данных. Сервер обладает единственной ответственностью - хранением данных, поэтому на сервере располагается единственный объект - реляционная база данных. Вынесение базы данных приложения и связанных с ней компонентов на отдельный сервер является преимуществом, поскольку повышает отказоустойчивость системы. Разбиение основного приложения и базы данных вводит такое понятие, как разделение ответственностей. Сервер основного приложения отвечает за обработку запросов и логику приложения, а сервер баз данных отвечает за хранения информации в системе. Это позволяет повысить отказоустойчивость системы, и в случае сбоя того или иного компонента позволяет сохранить работоспособность системы.

Для хранения информации была выбрана реляционная база данных – это тип баз данных, который организует хранение информации в виде таблиц. Каждая таблица представляет собой коллекцию объектов или сущностей, например, пользователей сервиса. В таблице есть столбцы, которые определяют тип данных, хранимых в таблице, и строки, которые содержат фактические данные. Для работы с реляционными базами данных используется язык SQL. Существуют также нереляционные базы данных, именуемые как NoSQL базы данных. Отличие нереляционных баз данных от реляционных заключается в способе хранения информации. Если в реляционных базах данных информация хранится в виде таблиц, то в нереляционных базах данных информация может быть представлена в виде документов, кэша и т.д.

Выбор такого типы баз данных обоснован простотой использования реляционных баз данных. Потому что они имеют простую и интуитивно понятную структуру, которая позволяет легко добавлять, изменять и удалять данные. Это делает их идеальными для широкого круга пользователей, включая разработчиков и конечных пользователей.

## **Сервис файлового хранилища**

Сервис предоставляет пользователю возможность работать с документами. Документами в данном случае называются любые файлы, например, текстовые файлы, архивы, бинарные файлы и т.д. Для хранения этих документов и последующей их обработки необходимо разработать дополнительный микросервис, который помимо хранения будет выполнять и другие функции.

## **Выбор программных средств разработки**

## **2.2.1 C#**

Текст второго параграфа первой главы.

## **ASP.NET**

Текст второго параграфа первой главы.

## **WPF**

Текст второго параграфа первой главы.

## **PostgreSQL**

Текст второго параграфа первой главы.

## **2.2.5 Docker и Docker Compose**

Текст второго параграфа первой главы.

## **2.3 Описание программной разработки**

Текст главы.

*Рекомендуемый объем второй главы – 15–20 страниц.*

# **3 РЕЗУЛЬТАТЫ РАБОТЫ**

## **3.1 Характеристика условий и места применения разработки**

Текст главы.

## **3.2 Результаты работы разработанного программного кода**

## **3.2.1 Серверное приложение**

Текст главы.

## **Клиентское приложение**

Текст главы.

## **3.3 Технические характеристики разработанного приложения**

*Текст третьего параграфа третьей главы.*

*Рекомендуемый объем третьей главы – 12–15 страниц.*

# **ЗАКЛЮЧЕНИЕ**

*Бла-бла бла-бла бла-бла-бла. Бла-бла-бла. Бла-бла бла-бла бла-бла-бла. Бла-бла-бла. Бла-бла бла-бла бла-бла-бла. Бла-бла-бла. Бла-бла бла-бла бла-бла-бла. Бла-бла-бла. Бла-бла бла-бла бла-бла-бла. Бла-бла-бла. Бла-бла бла-бла бла-бла-бла. Бла-бла-бла.*

*Заключение должно содержать:*

*– краткие выводы по результатам выполненной работы или отдельных ее этапов;*

*– оценку полноты решений поставленных задач;*

*– разработку рекомендаций и исходных данных по конкретному использованию результатов работы;*

*– результаты оценки технико-экономической эффективности внедрения;*

*–результаты оценки научно-технического уровня выполненной работы в сравнении с лучшими достижениями в этой области.*

*Рекомендуемый объем заключения 1–2 страницы.*

# **СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

1. Moos, D., Peska, P. et al. Comprehensive wellbore stability analysis using quantitative risk assessment// Knowledge Organization – 2017. – Vol. 34, No. 4 . – P. 97–109.
2. Прогноз научно-технологического развития Российской Федерации на период до 2090 года. – URL: [http://government.ru/media /files/41d4b737638891da2184/pdf](http://government.ru/media%20/files/41d4b737638891da2184/pdf) (дата обращения 15.11.2022).
3. Bradbury, A., McLellan, J. Impact Fluid Solutions Biodegradable shale inhibitor developed for water-based muds, Drilling It Safely, Innovating While Drilling, July/August, Onshore Advances Jul 11, 2013. – URL: [http://www.nlm.nih.gov/ pubs/factsheets/umlsmeta.html](http://www.nlm.nih.gov/%20pubs/factsheets/umlsmeta.html%20) (дата обращения 01.02.2023).
4. Двойников, М.В. Технология бурения нефтяных и газовых скважин модернизированными винтовыми забойными двигателями// Дисс. доктора техн. Наук. – Тюмень, 2021. – 360 с.
5. Хегай, В.К. К вопросу оптимизации режимных параметров бурения с учетом крутильных автоколебаний// Известия Коми НЦ УрО РАН. 2020 . № 07–08. – с. 6–10 .
6. Гуреев, В.Н., Мазов, Н.А. Использование библиометрии для оценки значимости журналов в научных библиотеках (обзор)// Научно-техническая информация. Сер. 1. 2019. № 2. – с. 8–19.
7. Статистические показатели российского книгоиздания в 2006 г.: цифры и рейтинги [Электронный ресурс]. - URL: <http://bookhamber.ru/stat_2006.htm> (дата обращения 12.03.2023).

*Рекомендуемое число источников – около 30, в т.ч. не менее 15% на иностранном языке*

# **ПРИЛОЖЕНИЕ А Наименование приложения**

*В приложения рекомендуется включать материалы, дополняющие текст отчета, если они не могут быть включены в основную часть.*

*Приложения могут включать: графический материал, таблицы, расчеты, описания алгоритмов и программ.*

*В тексте отчета на все приложения должны быть даны ссылки. Приложения располагают в порядке ссылок на них в тексте отчета.*

*Каждое приложение следует размещать с новой страницы с указанием в центре верхней части страницы слова ПРИЛОЖЕНИЕ.*

*Приложение должно иметь заголовок, который записывают с прописной буквы, полужирным шрифтом, отдельной строкой по центру без точки в конце.*

*Приложения обозначают прописными буквами кириллического алфавита, начиная с А, за исключением букв Ё, З, Й, О, Ч, Ъ, Ы, Ь. После слова ПРИЛОЖЕНИЕ следует буква, обозначающая его последовательность. Допускается обозначение приложений буквами латинского алфавита, за исключением букв I и O.*

*В случае полного использования букв кириллического или латинского алфавита допускается обозначать приложения арабскими цифрами.*

*Если в отчете одно приложение, оно обозначается ПРИЛОЖЕНИЕ А".*

*Приложения должны иметь общую с остальной частью отчета сквозную нумерацию страниц.*

*Все приложения должны быть перечислены в содержании отчета с указанием их обозначений, статуса и наименования.*