**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: *Фамилия Имя Отчество* (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)

Консультант: *Фамилия Имя Отчество* (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)

Рецензент: *Фамилия Имя Отчество* (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)

**К защите допустить**

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

*ХХ* мая 2023 года

Москва 2023

*!!!!!!!!!!!!!!!!!!!!!!!!!! Все слова, набранные не полужирным курсивом (наклонным тонким шрифтом), в данном шаблоне подлежат замене или удалению, включая данное примечание. При замене курсив изменяется на обычный шрифт (без наклона).*

**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](#_Toc133275170)

[ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ 7](#_Toc133275171)

[ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ 8](#_Toc133275172)

[ВВЕДЕНИЕ 9](#_Toc133275173)

[1 АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ 13](#_Toc133275174)

[1.1 Криптографические алгоритмы шифрования 13](#_Toc133275175)

[1.1.1 Симметричные алгоритмы шифрования 13](#_Toc133275176)

[1.1.2 Асимметричные алгоритмы шифрования 13](#_Toc133275177)

[1.1.3 Алгоритмы шифрования на эллиптических кривых 13](#_Toc133275178)

[1.2 Обзор существующих решений 13](#_Toc133275179)

[1.2.1 Telegram 13](#_Toc133275180)

[1.2.2 WhatsApp 13](#_Toc133275181)

[1.3 Постановка задач 13](#_Toc133275182)

[2 ПРОЕКТИРОВАНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ 14](#_Toc133275183)

[2.1 Описание решения поставленной задачи 14](#_Toc133275184)

[2.1.1 Математическая библиотека 14](#_Toc133275185)

[2.1.2 Криптосистема 14](#_Toc133275186)

[2.1.3 Распределенная система 14](#_Toc133275187)

[2.1.3.1 REST API сервис 14](#_Toc133275188)

[2.1.3.2 Сервис баз данных 14](#_Toc133275189)

[2.1.3.3 Сервис файлового хранилища 14](#_Toc133275190)

[2.2 Выбор программных средств разработки 14](#_Toc133275191)

[2.2.1 C# 14](#_Toc133275192)

[2.2.2 ASP.NET 14](#_Toc133275193)

[2.2.3 WPF 14](#_Toc133275194)

[2.2.4 PostgreSQL 14](#_Toc133275195)

[2.2.5 Docker и Docker Compose 14](#_Toc133275196)

[2.3 Описание программной разработки 15](#_Toc133275197)

[3 РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ 16](#_Toc133275198)

[3.1 Характеристика условий и места применения разработки 16](#_Toc133275199)

[3.2 Результаты работы разработанного программного кода 16](#_Toc133275200)

[3.2.1 Серверное приложение 16](#_Toc133275201)

[3.2.2 Клиентское приложение 16](#_Toc133275202)

[3.3 Технические характеристики разработанного приложения 16](#_Toc133275203)

[ЗАКЛЮЧЕНИЕ 17](#_Toc133275204)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 18](#_Toc133275205)

[ПРИЛОЖЕНИЕ А Наименование приложения 19](#_Toc133275206)

# **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* |
|  | *– определение* |

# **ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ**

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

|  |  |
| --- | --- |
| *Аббревиатура* | *– детальная расшифровка* |
| *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**

## **Симметричные алгоритмы шифрования**

Текст второго параграфа первой главы.

## **Асимметричные алгоритмы шифрования**

Текст второго параграфа первой главы.

## **Алгоритмы шифрования на эллиптических кривых**

Текст второго параграфа первой главы.

## **Обзор существующих решений**

## **Telegram**

Текст второго параграфа первой главы.

## **WhatsApp**

Текст второго параграфа первой главы.

## **1.3 Постановка задач**

Текст главы.

*Рекомендуемый объем первой главы – 10–12 страниц*

# **2 ПРОЕКТИРОВАНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ**

## **Описание решения поставленной задачи**

## **2.1.1 Математическая библиотека**

Текст второго параграфа первой главы.

## **Криптосистема**

Текст второго параграфа первой главы.

## **Распределенная система**

## **REST API сервис**

Текст второго параграфа первой главы.

## **Сервис баз данных**

Текст второго параграфа первой главы.

## **Сервис файлового хранилища**

Текст второго параграфа первой главы.

## **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 РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ**

## **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.*