**МИНИСТЕРСТВО 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 и компьютерные науки

**Квалификация**  **бакалавр**

**УТВЕРЖДАЮ**

Заведующий кафедрой 806 \_\_\_\_\_\_\_\_\_ С.С. Крылов

(№ каф.) (подпись) (инициалы, фамилия)

\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_ 2023г.

**ЗАДАНИЕ**

**на выпускную квалификационную работу бакалавра**

**Обучающийся** Тришин Дмитрий Александрович

(фамилия, имя, отчество полностью)

**Руководитель** Романенков Александр Михайлович

(фамилия, имя, отчество полностью)

доцент, кандидат технических наук, доцент кафедры 806

ученая степень, ученое звание, должность и место работы)

**1. Наименование темы** Распределенная система криптографической защиты данных на основе эллиптических кривых

**2. Срок сдачи обучающимся законченной работы** 24.05.2023

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

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

**Перечень иллюстративно-графических материалов:**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование** | **Количество листов** |
| 1 | Раздаточный материал |  |

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| п/п | Наименование раздела или этапа | Трудоёмкость в % от полной трудоёмкости ВКРБ | Срок выполнения | Примечание |
| 1 | Разработка библиотеки исходного кода для работы с эллиптическими кривыми | 9 | 09.02.2023 – 18.02.2023 |  |
| 2 | Проектирование архитектуры распределенной системы | 5 | 19.02.2023 – 23.02.2023 |  |
| 3 | Разработка сервиса мессенджера | 25 | 24.02.2023 – 21.03.2023 |  |
| 4 | Разработка сервиса хранения документов | 10 | 22.03.2023 – 02.04.2023 |  |
| 5 | Разработка сервиса электронной подписи документа | 14 | 03.04.2023 – 17.04.2023 |  |
| 6 | Разработка приложения для ПК | 14 | 17.04.2023 – 01.05.2023 |  |
| 7 | Оформление текста ВКРБ | 23 | 01.05.2023 – 24.05.2023 |  |

**5. Исходные материалы и пособия**

Н. Смарт, Криптография/ Н. Смарт- Москва: Изд-во ТЕХНОСФЕРА, 2005. – 525 с.

Б. Шнайер, Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер – Москва: Изд-во Триумф, 2002. -816 с.

Ричардсон К. Микросервисы. Паттерны разработки и рефакторинга / К. Ричардсон. – Санкт-Петербург: Питер, 2019. – 544 с.

Амундсен, М. RESTful Web APIs / М. Амундсен. – Sebastopol: O’Reilly Media, 2013. – 373 с.

**6. Дата выдачи задания** 09.02.2023

Руководитель Романенков А. М.

(подпись)

Задание принял к исполнению Тришин Д. А.

(подпись)