МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»**

Кафедра теоретических основ компьютерной безопасности и криптографии

**Протоколы открытого распределения ключей**

ОТЧЁТ

ПО ДИСЦИПЛИНЕ

«КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ»

студента 5 курса 531 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Серебрякова Алексея Владимировича

|  |  |  |
| --- | --- | --- |
| Преподаватель  аспирант | \_\_\_\_\_\_\_\_\_\_ | Р. А. Фарахутдинов |
|  | подпись, дата |  |

Саратов 2023

**1 Постановка задачи**

Цель работы:

* Изучение протокола открытого распределения ключей Диффи-Хеллмана и его программная реализация.

Задачи работы:

* Изучить протокол Диффи-Хеллмана, его сильные и слабые стороны;
* Привести программную реализацию протокола.

**2 Теоретические сведения**

**3 Тестирование программы**

**ПРИЛОЖЕНИЕ А**

**Код программы proc.rb**

**ПРИЛОЖЕНИЕ Б**

**Код программы methods.rb**

**ПРИЛОЖЕНИЕ В**

**Код программы units.rb**