Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования

Московский государственный университет имени М.В. Ломоносова

Механико-математический факультет

Кафедра теоретической информатики

УТВЕРЖДАЮ

Заведующий кафедрой

\_\_\_\_\_\_\_\_\_\_\_\_\_\_/А.В.Михалев /

«22» января 2019 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**Наименование дисциплины :**

специальный курс по выбору студента

**Эллиптические кривые в алгоритмах**

**Уровень высшего образования:**

**аспирантура**

**Направление подготовки (специальность):**

**01.06.01 Математика и механика**

**Направленность (профиль) ОПОП:**

**Математика**

Форма обучения:

очная

Рабочая программа рассмотрена и одобрена

на заседании кафедры Теоретической информатики

(протокол №2а, «22» января 2019 года)

Москва 2019

Рабочая программа дисциплины разработана в соответствии с самостоятельно установленным МГУ образовательным стандартом (ОС МГУ) для реализуемых основных профессиональных образовательных программ высшего образования по специальности «Математика и механика» (программы аспирантуры) в редакции приказа МГУ от 30 декабря 2016 г.

Год (годы) приема на обучение\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**1.** Место дисциплины в структуре ОПОП ВО. **Вариативная часть ОПОП ВО***.*

**2.** Входные требования для освоения дисциплины , предварительные условия: знание основ статистики, линейной алгебры и программирования.

**3.** Результаты обучения по дисциплине , соотнесенные с требуемыми компетенциями выпускников*.*

|  |  |
| --- | --- |
| **Компетенции выпускников (коды)** | **Планируемые результаты обучения по дисциплине , соотнесенные с компетенциями** |
| *ПК-1, ПК-5* | ***Знать:*** *стандартные методы построения эффективных алгоритмов используя эллиптические кривые.****Уметь*** *ориентироваться в современных методах и алгоритмах компьютерной математики, уметь решать стандартные задачи по изученным темам.****Владеть:*** *прикладными методами решения практических задач по изученным темам.* |
| *ОПК-1, ОПК-2, ОПК-4* | ***Уметь*** *решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий****\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_******Иметь опыт*** *использования на практике математических алгоритмов, в том числе с применением современных вычислительных систем**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* |
| *УК-1* | ***Уметь*** *формулировать научно обоснованные гипотезы, создавать теоретические модели явлений и процессов, применять методологию научного познания в профессиональной деятельности****\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_******Владеть*** *специальными разделами фундаментальной математики, методами анализа и решения задач**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* |

**4.** Формат обучения очный.

**5.** Объем дисциплины составляет  **1** з.е., в том числе **38**  академических часов, отведенных на контактную работу обучающихся с преподавателем, **20**  академических часов на самостоятельную работу обучающихся.

**6.** Содержание дисциплины , структурированное по темам (разделам) с указанием отведенного на них количества академических часов и виды учебных занятий

|  |  |  |
| --- | --- | --- |
| **Наименование и краткое содержание разделов и тем дисциплины ,****Форма промежуточной аттестации по дисциплине**  | **Всего****(часы**) | В том числе |
| **Контактная работа (работа во взаимодействии с преподавателем)****Виды контактной работы, часы** | **Самостоятельная работа обучающегося,** **часы**  |
| Занятия лекционного типа\* | Занятия семинарского типа\* | **Всего** |  |
| Тема 1. Основы теории эллиптических кривых. Арифметика эллиптических кривых. ТеоремыХассе, Дойринга и Ленстры.  | 6 | 4 |  | 4 | 2 |
| Тема 2. Диофантовые задачи, приводящие к нахождению рациональных точек на эллиптической кривой. | 6 | 4 |  | 4 | 2 |
| Тема 3. Эллиптические кривые над конечными полями и их порядок. Базовый алгоритм ECM.  | 6 | 4 |  | 4 | 2 |
| Тема 4. Подсчет числа точек на эллиптической кривой. Методы Шенкса-Местре, Шуфа и Аткина-Морейна  | 6 | 4 |  | 4 | 2 |
| Текущий контроль успеваемости | 4 |  | 2 | 2 | 2 |
| Тема 5. Тесты на простоту Гольдвассер-Килиана и Аткина-Морейна.  | 6 | 4 |  | 4 | 2 |
| Тема 6. Быстрое доказательство простоты при помощи эллиптических кривых  | 6 | 4 |  | 4 | 2 |
| Тема 7. Факторизация больших чисел используя эллиптические кривые. | 6 | 4 |  | 4 | 2 |
| Промежуточная аттестация – контрольная работа | 4 |  |  | 2 | 2 |
| Консультации | 4 | 2 | 2 |
| Экзамен | 4 | 4 |  |
| **Итого** | 58 | 38 | 20 |

7. Фонд оценочных средств (ФОС) для оценивания результатов обучения по дисциплине

7.1. Типовые контрольные задания или иные материалы для проведения текущего контроля успеваемости.

Примеры задач для самостоятельного решения.

1. Вычислить количество точек на кривой $y^{2}=x^{3}-x$ над $Z\_{p}$, p=17 и p=19.

2. Найти порядок эллиптической кривой $y^{2}=x^{3}-5x+3$ над $Z\_{p},$ р=23.

3. Доказать простоту числа 89 используя эллиптические кривые.

4.Разложить на множители n=1363 используя эллиптические кривые.

7.2. Типовые контрольные задания или иные материалы для проведения промежуточной аттестации.

Эллиптические кривые.

Приведение к форме Вейрштрасса.

Сложение на эллиптической кривой.

ТеоремыХассе, Дойринга и Ленстры.

Диофантовые задачи, приводящие к нахождению рациональных точек на кривой.

Эллиптические кривые над конечным полем и их порядок.

Базовый алгоритм ЕСМ.

Методы подсчета числа точек на эллиптической кривой.

Тесты на простоту.

Доказательства простоты.

Алгоритм факторизации.

|  |
| --- |
| **ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ результатов обучения (РО) по дисциплине (модулю)**  |
| ОценкаРО исоответствующие виды оценочных средств  | 2 | 3 | 4 | 5 |
| **Знания***(виды оценочных средств: устные и письменные опросы и контрольные работы, тесты, и т.п. )* | Отсутствие знаний | Фрагментарные знания | Общие, но не структурированные знания | Сформированные систематические знания |
| **Умения***(виды оценочных средств: практические контрольные задания, написание и защита рефератов на заданную тему и т.п.)*  | Отсутствие умений | В целом успешное, но не систематическое умение | В целом успешное, но содержащее отдельные пробелы умение (допускает неточности непринципиального характера) | Успешное и систематическое умение |
| **Навыки (владения, опыт деятельности)***(виды оценочных средств: выполнение и защита курсовой работы, отчет по практике, отчет по НИР и т.п.)*  | Отсутствие навыков (владений, опыта) | Наличие отдельных навыков (наличие фрагментарного опыта) | В целом, сформированные навыки (владения), но используемые не в активной форме | Сформированные навыки (владения), применяемые при решении задач |

8.  Перечень основной и дополнительной учебной литературы:

А. Основная литература

 1. Р. Крендал, К. Померанс. Простые числа. Криптографические и вычислительные аспекты.

 2. Henry Cohen. Number Theory/ Volume 1, Volume 11.

Б. Дополнительная литература

 3. Henry Cohen and / Handbook of Elliptic and Hyperelliptic curve Cryptography.

 4. А.А. Болотов, С.Б. Гашков, А.Б. Фролов. Элементарное введение в эллиптическую криптографию.

 5. А.А. Болотов, С.Б. Гашков, А.Б. Фролов. Протоколы криптографии на эллиптических кривых.

9. Язык преподавания.

Русский

10. Преподаватель

Айдагулов Р.Р.

11. Автор программы.

Айдагулов Р.Р.