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

**Алгоритмы в алгебре и теории чисел: основные алгоритмы**

**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 в алгебре и теории чисел.****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, **28**  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. Эффективность алгоритмов. О- большое нотация. Принцип разделяй и властвуй. Сортировка делением пополам и разбиением по значениям.  | 4 | 2 |  | 2 | 2 |
| Тема 2. Китайская теорема об остатках. Алгоритм Евклида. Модулярные и мультимодулярные выяисления. Квадратные корни. | 6 | 4 |  | 4 | 2 |
| Тема 3. Представление больших чисел и умножение по Карацуба. Фильтрованные и градуированные вычисления. Преобразование Фурье и быстрый метод умножения. Умножение матриц методом Штрассена. | 4 | 2 |  | 2 | 2 |
| Тема 4. Групповая и бигрупповая алгебра и изоморфизм последних с алгеброй матриц. Быстрое умножение больших матриц. | 6 | 4 |  | 4 | 2 |
| Тема 5. Основы криптографии RSA. Максимальный порядок в группе Эйлера, Числа и функция Кармайкла. Тесты на простоту Ферма, Эйлера и Рабина-Миллера. | 4 | 2 |  | 2 | 2 |
| Тема 6. Псевдопростые числа Фибоначчи и Люка. Тест Фробениуса. | 4 | 2 |  | 2 | 2 |
| Текущий контроль успеваемости | 4 |  | 2 | 2 | 2 |
| Тема 7. n-1 и n+1 методы доказательства простоты. Критерии простоты чисел Мерсена и чисел Ферма. | 4 | 2 |  | 2 | 2 |
| Тема 8. Полиномиальный алгоритм AKS, доказывающий простоту или составность большого числа. | 6 | 4 |  | 4 | 2 |
| Тема 9. Экспоненциальные методы факторизации. | 4 | 2 |  | 2 | 2 |
| Тема 10. Метод квадратичного решета в задаче факторизации. | 6 | 4 |  | 4 | 2 |
| Тема 11. Методы числового поля NFS. | 6 | 4 |  | 4 | 2 |
| Промежуточная аттестация – контрольная работа | 4 |  |  | 2 | 2 |
| Консультации | 4 | 2 | 2 |
| Экзамен | 4 | 4 |  |
| **Итого** | 66 | 38 | 28 |

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. Сравнить эффективность алгоритмов сортировки слиянием и ранжированием.

2. Сравнить эффективность мультимодулярного вычисления последовательным вычислением остатков и методом бинарного дерева.

3. Найти минимальную мультипликативную образующую по модулю 41.

3.Найти минимальную пару натуральных чисел a,b, удовлетворяющую уравнению 89a-46b=1.

4. Найти x, удовлетворяющую соотношению $x^{2}=17 mod 256\*43$.

5. Разложить на множители 10057 методом Лемана.

6. Разложить на множители 5207 ро методом.

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

О- большое нотация.

Сравнение эффективности разных алгоритмов.

Мастер теорема.

Алгоритмы сортировки.

Китайская теорема об остатках.

Алгоритм Евклида.

Модулярные и мультимодулярные вычисления.

Вычисление произведения больших чисел и матриц.

Криптография RSA.

Тесты на простоту.

Доказательства простоты.

Экспоненциальные алгоритмы факторизации.

Субэкспоненциальные алгоритмы 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. Изд. Либроком 2011г.

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

Б. Дополнительная литература

 3. П. Ноден, К. Китте. Алгебраическая алгоритмика», Москва, «Мир», 1999 г.

 4. Р. Грэхем, Д. Кнут, О. Паташник. «Конкретная математика.» Москва, «Мир», 1998.

5. С. Дасгупта, Х. Пападимитриу, У. Вазирани. «Алгоритмы». Москва, Изд-во МЦНМО, 2014 г.

9. Язык преподавания.

Русский

10. Преподаватель

Айдагулов Р.Р.

11. Автор программы.

Айдагулов Р.Р.