Федеральное государственное бюджетное учреждение науки

 **Институт систем информатики им. А.П. Ершова**

Сибирского отделения Российской академии наук

УТВЕРЖДАЮ

Директор ИСИ СО РАН

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

« 2 » сентября 2015 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

 **«Математические основы программирования»**

**Направление подготовки:** 09.06.01 «Информатика и вычислительная техника»

**Специальность:** 05.13.17 «Теоретические основы информатики»

**Уровень образования:** подготовка кадров высшей квалификации

**Квалификация выпускника:** Исследователь. Преподаватель-исследователь

Составители рабочей программы

 Д.ф.-м.н., профессор, \_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_ Касьянов В.Н.

 (должность, ученое звание, ученая степень) (подпись) (ФИО)

Рабочая программа утверждена на заседании Ученого совета Института

«07» июля 2015 г., протокол № 5-2015

Председатель Ученого совета \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_ Марчук А.Г.\_\_

 (подпись) (ФИО)

СОГЛАСОВАНО:

Зам. директора \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_Мурзин Ф.А.\_\_

 (подпись) (ФИО)

Зав. аспирантурой
и докторантурой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_Воронко Н.Ф.\_

 (подпись) (ФИО)

# 1. Цели освоения дисциплины

Целью освоения дисциплины «Математические основы программирования» является обеспечение уровня знаний в области теоретических основ программирования соответствующего квалификационным требованиям.

*(Указываются цели освоения дисциплины)*

# 2. Место дисциплины в структуре основной профессиональной образовательной программы послевузовского профессионального образования (аспирантура)

Данная дисциплина «Математические основы программирования» (Б1.В.ОД.1) относится к группе обязательных дисциплин по специальности 05.13.17.

# 3. Требования к уровню подготовки аспиранта, завершившего изучение данной дисциплины

Аспиранты, завершившие изучение данной дисциплины, должны:

* **знать:** теоретические основы программирования
* **уметь:** разрабатывать и исследовать алгоритмы решения дискретных задач
* **владеть:** математическим аппаратом моделирования программ

Компетенции, формируемые у обучающихся, в соответствии с ООП по направлению 09.06.01 «Информатика и вычислительная техника» и профилю (специальности) 05.13.17 «Теоретические основы информатики»:

**Универсальные компетенции:** УК1, УК2.

**Общепрофессиональные компетенции:** ОПК1, ОПК3, ОПК4, ОПК5, ОПК7

**Профессиональные компетенции:** ПК1, ПК2, ПК3, ПК4, ПК5, ПК6

# 4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет \_\_2\_\_ зачетных единицы \_\_72\_\_ часов.

|  |  |
| --- | --- |
| **Вид учебной работы** | Объем часов / зачетных единиц |
| **Обязательная аудиторная учебная нагрузка (всего)** | **24** |
| в том числе: |  |
|  лекции | 20 |
|  семинары |  |
|  практические занятия |  |
|  Контроль самостоятельной работы | 4 |
| **Самостоятельная работа аспиранта (всего)** | **48** |
| **Вид контроля по дисциплине** | экзамен |

# 5. Разделы дисциплины и виды занятий

|  |  |  |
| --- | --- | --- |
| №п/п | Название раздела дисциплины | Объем часов / зачетных единиц |
|  |  | Всего ауд. часов | из них | Самост. работа |
|  |  |  | лекции | семинары | практ. занятия | КСР |  |
| 1 | Понятие алгоритма и его уточнения | 1,65 | 1,5 |  |  | 0,15 | 4 |
| 2 | Понятие сложности алгоритмов | 1,7 | 1,5 |  |  | 0,2 | 4 |
| 3 | Примеры эффективных (полиномиальных) алгоритмов | 1,65 | 1,5 |  |  | 0,15 | 4 |
| 4 | Автоматы. Эксперименты с автоматами | 1,65 | 1,5 |  |  | 0,15 | 4 |
| 5 | Алгебра логики | 1,65 | 1,5 |  |  | 0,15 | 4 |
| 6 | Исчисление предикатов первого порядка | 1,7 | 1,5 |  |  | 0,2 | 4 |
| 7 | Отношения и функции | 1,65 | 1,5 |  |  | 0,15 | 4 |
| 8 | Формальные языки и способы их описания | 1,65 | 1,5 |  |  | 0,15 | 4 |
| 9 | -исчисление, правила редукции, единственность нормальной формы и правила ее достижения, представление рекурсивных функций | 2,15 | 2 |  |  | 0,15 | 4 |
| 10 | Основы комбинаторного анализа | 2,2 | 2 |  |  | 0,2 | 4 |
| 11 | Коды с исправлением ошибок | 2,15 | 2 |  |  | 0,15 | 4 |
| 12 | Основы криптографии | 2,15 | 2 |  |  | 0,15 | 4 |

# 6. Содержание дисциплины:

*(Раздел, тема учебного курса, содержание лекции)*

Понятие алгоритма и его уточнения: машины Тьюринга, нормальные алгоритмы Маркова, рекурсивные функции. Эквивалентность данных формальных моделей алгоритмов. Понятие об алгоритмической неразрешимости. Примеры алгоритмически неразрешимых проблем.

Понятие сложности алгоритмов. Классы P и NP. Полиномиальная сводимость задач. Теорема Кука об NP-полноте задачи выполнимости булевой формулы. Примеры NP-полных задач, подходы к их решению. Точные и приближенные комбинаторные алгоритмы.

Примеры эффективных (полиномиальных) алгоритмов: быстрые алгоритмы поиска и сортировки; полиномиальные алгоритмы для задач на графах и сетях (поиск в глубину и ширину, о минимальном остове, о кратчайшем пути, о назначениях).

Конечные автоматы и их свойства. Регулярные языки и регулярные выражения. Теорема Клини о регулярных языках.

Алгебра логики. Булевы функции, канонические формы задания булевых функций. Понятие полной системы. Критерий полноты Поста. Минимизация булевых функций в классах нормальных форм.

Исчисление предикатов первого порядка. Понятие интерпретации. Выполнимость и общезначимость формулы первого порядка. Понятие модели. Теорема о полноте исчисления предикатов первого порядка.

Отношения и функции. Отношение эквивалентности и разбиения. Фактор множества. Отношения частичного порядка. Теоретико-множественное и алгебраическое определения решетки, их эквивалентность. Свойства решеток. Булевы решетки. Полные решетки.

Формальные языки и способы их описания. Классификация формальных грамматик. Их использование в лексическом и синтаксическом анализе.

-исчисление, правила редукции, единственность нормальной формы и правила ее достижения, представление рекурсивных функций.

Основы комбинаторного анализа. Метод производящих функций, метод включений и исключений. Примеры применения.

Коды с исправлением ошибок. Алфавитное кодирование. Методы сжатия информации.

Основы криптографии. Задачи обеспечения конфиденциальности и целостности информации. Теоретико-информационный и теоретико-сложностный подходы к определению криптографической стойкости. Американский стандарт шифрования DES и российский стандарт шифрования данных ГОСТ 28147-89. Системы шифрования с открытым ключом (RSA). Цифровая подпись. Методы генерации и распределения ключей.

# 7. Самостоятельная работа аспирантов

Изучение основной и дополнительной литературы по вопросам программы.
*(Приводятся виды самостоятельной работы обучающегося, порядок их выполнения
и контроля, учебно-методическое обеспечение (возможно в виде ссылок) самостоятельной работы по отдельным видам дисциплин)*

# 8. Учебно-методическое и информационное обеспечение дисциплины

### 8.1. Основная и дополнительная литература

а) основная литература:

1. Алферов А.П. Зубов А.Ю. Кузьмин А.С. Черемушкин А.В. Основы криптографии. М.: Гелиос АРВ, 2002.
2. Касьянов В.Н. Лекции по теории формальных языков, автоматов и сложности вычислений. Новосибирск: НГУ, 1995.
3. Новиков Ф.А. Дискретная математика для программистов. СПб: Питер, 2000.
4. Яблонский С.В. Введение в дискретную математику. М.: Наука, 2001.

б) дополнительная литература

1. Барендрегт Х. Ламбда–исчисление. Его синтаксис и семантика. М.: Мир, 1985.
2. Булос Дж., Джеффри Р. Вычислимость и логика. М.: Мир, 1994.
3. Введение в криптографию / Под ред. В.В. Ященко. СПб.: МЦНМО, 2001.
4. Гэри М.Р., Джонсон Д.С. Вычислительные машины и тpудноpешаемые задачи. М.: Миp, 1982.
5. Кнут Д. Искусство программирования. Т. 1 – 3. М., СПб., Киев: ИД «Вильямс», 2000.
6. Мальцев А.Н. Алгоритмы и рекурсивные функции. М.: Наука, 1986.
7. Рыбников К.А. Введение в комбинаторный анализ. М.: Изд-во МГУ, 1985.
8. Хопкрофт Дж., Мотвани Р., Ульман Дж. Ведение в теорию автоматов, языков и вычислений. 2-е изд., исправ., М.: Вильямс, 2016.
9. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2002.

в) программное обеспечение и Интернет-ресурсы

### 8.2. Перечень вопросов и заданий (аттестации) и/или тем рефератов

1. Понятие алгоритма и его уточнения: машины Тьюринга, нормальные алгоритмы Маркова, рекурсивные функции. Эквивалентность данных формальных моделей алгоритмов.
2. Понятие об алгоритмической неразрешимости. Примеры алгоритмически неразрешимых проблем.
3. Понятие сложности алгоритмов. Классы P и NP. Полиномиальная сводимость задач и NP-полные задачи.
4. Теорема Кука об NP-полноте задачи выполнимости булевой формулы.
5. Примеры NP-полных задач, подходы к их решению. Точные и приближенные комбинаторные алгоритмы.
6. Примеры эффективных (полиномиальных) алгоритмов, быстрые алгоритмы поиска и сортировки.
7. Полиномиальные алгоритмы для задач на графах и сетях (поиск в глубину и ширину, о минимальном остове, о кратчайшем пути, о назначениях).
8. Конечные автоматы и их свойства.
9. Регулярные языки и регулярные выражения. Теорема Клини о регулярных языках.
10. Алгебра логики. Булевы функции, канонические формы задания булевых функций. Понятие полной системы. Критерий полноты Поста.
11. Минимизация булевых функций в классах нормальных форм.
12. Исчисление предикатов первого порядка. Понятие интерпретации. Выполнимость и общезначимость формулы первого порядка.
13. Понятие модели. Теорема о полноте исчисления предикатов первого порядка.
14. Отношения и функции. Отношение эквивалентности и разбиения. Фактор множества.
15. Отношения частичного порядка. Теоретико-множественное и алгебраическое определения решетки, их эквивалентность.
16. Свойства решеток. Булевы решетки. Полные решетки.
17. Формальные языки и способы их описания. Классификация формальных грамматик.
18. Использование формальных грамматик в лексическом и синтаксическом анализе.
19. -исчисление, правила редукции, единственность нормальной формы и правила ее достижения, представление рекурсивных функций.
20. Основы комбинаторного анализа. Метод производящих функций, метод включений и исключений. Примеры применения.
21. Коды с исправлением ошибок. Алфавитное кодирование.
22. Методы сжатия информации.
23. Основы криптографии. Задачи обеспечения конфиденциальности и целостности информации.
24. Теоретико-информационный и теоретико-сложностный подходы к определению криптографической стойкости.
25. Американский стандарт шифрования DES и российский стандарт шифрования данных ГОСТ 28147-89.
26. Системы шифрования с открытым ключом (RSA). Цифровая подпись. Методы генерации и распределения ключей.

# 9. Материально-техническое обеспечение дисциплины

Для лекций используется класс, оснащённый мультимедийным проектором и имеющий в составе программное обеспечение MS Office и Acrobat Reader. Литература из основного и вспомогательного списков доступна в электронно-библиотечной системе ИСИ СО РАН и в Мемориальной библиотека А.П. Ершова (каб. 265).

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(*Указывается материально-техническое обеспечение данной дисциплины*)

**ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ В РАБОЧЕЙ ПРОГРАММЕ**

за \_\_\_\_/\_\_\_\_ учебный год

В рабочую программу Математические основы программирования

(наименование дисциплины)

Для специальности (тей) 05.13.17

(номер специальности)

Вносятся следующие дополнения и изменения:

Дополнения и изменения внес

(должность, ФИО, подпись)

Рабочая программа пересмотрена и одобрена на заседании Ученого совета Института

Председатель Ученого совета \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (подпись) (ФИО)