ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ УЧРЕЖДЕНИЕ
«ФЕДЕРАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
ИНСТИТУТ ПРИКЛАДНОЙ МАТЕМАТИКИ ИМ. М.В. КЕЛДЫША
РОССИЙСКОЙ АКАДЕМИИ НАУК»

Утверждена
Ученым советом
ИПМ им. М.В. Келдыша РАН,
протокол № 14-22 от «10» ноября 2022 г.

РАБОЧАЯ ПРОГРАММА

УЧЕБНОЙ ДИСЦИПЛИНЫ:
«Математические основы программирования»

Научная специальность:
2.3.5 – «Математическое обеспечение вычислительных систем, комплексов икомпьютерных сетей»

Форма обучения:
очная

Москва, 2022

Дисциплина: Математические основы программирования
Научная специальность:
2.3.5 – «Математическое обеспечение вычислительных систем, комплексов и компьютерных сетей»
Форма обучения: очная

ИСПОЛНИТЕЛЬ (разработчик программ):
Бондаренко А.А., ИПМ им. М.В. Келдыша, научный сотрудник, к.ф.-м.н.

РЕЦЕНЗЕНТ:
Якобовский Михаил Владимирович, ИПМ им.М.В. Келдыша РАН, член-корреспондент РАН

РАБОЧАЯ ПРОГРАММА РЕКОМЕНДОВАНА
Ученым советом ИПМ им. М.В. Келдыша РАН,
протокол № 14/22 от «10» ноября 2022 г.

Заведующий аспирантурой_____/ Меньшов И.С. /

Оглавление

АННОТАЦИЯ

Рабочая программа дисциплины «Математические основы программирования» разработана и составлена на основании ФГТ - «Федеральные государственные требования к структуре программ подготовки научных и научно-педагогических кадров в аспирантуре (адъюнктуре), условиям их реализации, срокам освоения этих программ с учетом различных форм обучения, образовательных технологий и особенностей отдельных категорий аспирантов (адъюнктов)» (Приказ Минобрнауки № 951 от 20.10.2021г.), в соответствии с учебными планами подготовки аспирантов ФГУ «Федеральный исследовательский центр «Институт прикладной математики им. М.В. Келдыша РАН (ИПМ им. М.В. Келдыша РАН) по научным специальностям: 2.3.5 «Математическое обеспечение вычислительных систем, комплексов и компьютерных сетей»

Дисциплина «Математические основы программирования» реализуется в рамках Блока «Образовательный компонент программы подготовки научных и научно - педагогических кадров в аспирантуре ИПМ им. М.В. Келдыша РАН.

Основным источником материалов для формирования содержания программы являются: научные издания и монографические исследования и публикации, материалы конференций, симпозиумов, семинаров и Интернет-ресурсы.

Общая трудоемкость дисциплины по учебному плану составляет 2 зач.ед. (72 часа), из них лекций – 4 часа, семинарских занятий – 10 часов, практических занятий – 0 часов и самостоятельной работы – 58 часа. Дисциплина реализуется на 1-м курсе, в 1-м семестре, продолжительность обучения – 1 семестр.

Текущая аттестация проводится не менее 2 раз в соответствии с заданиями и формами контроля, предусмотренными настоящей программой.

Промежуточная оценка знания осуществляется в период зачётно-экзаменационной сессии в форме зачета.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели и задачи дисциплины «Математические основы программирования»

Цель: освоение фундаментальных знаний и компетенций, которые позволят представлять и разрабатывать алгоритмы (решения поставленной задачи) в удобном для проблемной области виде, а также владеть математическим аппаратом, позволяющим выбрать наиболее эффективный алгоритм, согласно критериям проблемной области.

Задачи:

- освоить основной математический аппарат, позволяющий описывать алгоритмы и анализировать их эффективность;
- практическое освоение накопленных по дисциплине знанийпри решении профессиональных проблем в реальных (смоделированных) условиях;
- стимулирование к самостоятельной деятельности по освоению дисциплины и формированию необходимых компетенций.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс изучения дисциплины «Математические основы программирования» направлен на формирование определенных знаний, умений и компетенций.

а) универсальные (УК): не предусмотрено

б) общепрофессиональные (ОПК): Владение методологией теоретических и экспериментальных исследований в области профессиональной деятельности (ОПК-1)

в) профессиональных (ПК): Способность использовать языки программирования и системы программирования (ПК-1), Способность создавать модели и алгоритмы проектирования

программных систем (ПК-2), Способность владеть моделями и методами создания программ и программных систем для параллельного программирования (ПК-3).

В результате освоения дисциплины обучающийся должен:

Знать:

- основные понятия теории множеств, математической логики, (булевой) логики высказываний, теории автоматов, теории алгоритмов, элементы теория формальных языков, криптографии, алфавитного кодирования;
- основные методы оценки сложности алгоритмов, сжатия информации и шифрования;
- основные математические методы формализации решения прикладных задач;

Уметь:

- вычислять оценки сложности алгоритмов;
- применять математический аппарат при решении типовых задач, а также применять аппарат математической логики, теории алгоритмов, теории автоматов, теории кодирования для решения задач в различных областях науки и ее приложениях;

Владеть:

- теоретико-множественными подходами к постановке и решению задач;
- навыками расчёта сложности алгоритмов и выбора наиболее эффективного алгоритма согласно критериям проблемной области;
- навыками моделирования прикладных задач методами математической логики,теории алгоритмов, теории автоматов, теории кодирования.

Приобрести опыт:

- для естественнонаучных задач построения математической формулировки;
- построения алгоритма решения формализованной задачи и его анализ

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1. Структура дисциплины

Распределение трудоемкости дисциплины по видам учебных работ

Вид учебной работы	Трудоемкость общая	
	зач.ед.	час.
ОБЩАЯ ТРУДОЕМКОСТЬ по Учебному плану	**2**	**72**
Лекции (Л)		**4**
Практические занятия (ПЗ)	-	-
Семинары (С)		**10**
Самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к семинарским и практическим занятиям)		***58***
и самостоятельное изучение тем дисциплины		
Вид контроля: зачет		

3.2. Содержание разделов дисциплины

Общее содержание дисциплины

№ раздела	Наименование раздела	Содержание раздела	Форма текущей аттестации
1.	Алгебра и исчисление высказываний	Алгебра логики. Булевы функции, канонические формы задания булевых функций. Понятие полной системы. Критерий полноты Поста. Минимизация булевых функций в классах нормальных форм. Исчисление предикатов. Понятие интерпретации. Выполнимость и общезначимость формулы. Понятие модели. Теорема о полноте исчисления предикатов. Отношения и функции. Отношение эквивалентности и разбиения. Фактор множества.	О, ДЗ

		Отношения частичного порядка. Теоретико-множественное и алгебраическое определения решетки, их эквивалентность. Свойства решеток. Булевы решетки.	
2.	Общие вопросы теории алгоритмов	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)	О, ДЗ
3.	Теория формальных языков	Формальные языки и способы их описания. Классификация формальных грамматик. Их использование в лексическом и синтаксическом анализе. Лямбда-исчисление,правила редукции, единственность нормальной формы и правила ее достижения, представление рекурсивных функций. Автоматы. Эксперименты с автоматами. Алгебры регулярных выражений. Теорема Клини о регулярных языках.	О, ДЗ
4.	Кодирование	Коды с исправлением ошибок. Алфавитное кодирование. Методы сжатия информации	О, ДЗ
5.	Основы криптографии	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	О, ДЗ
		ГОСТ 28147-89. Системы шифрования с открытым ключом (RSA). Цифровая подпись. Методы генерации и распределения ключей.	

Примечание: О – опрос, Д – дискуссия (диспут, круглый стол, мозговой штурм, ролевая игра), ДЗ – домашнее задание (эссе и пр.). Формы контроля не являются жесткими и могут быть заменены преподавателем на другую форму контроля в зависимости от контингента обучающихся. Кроме того, на занятиях семинарских может проводится работа с нормативными документами, изданиями средств информации и прочее, что также оценивается преподавателем.

3.3. Лекционные занятия

№ занятия	№ Раздела	Краткое содержание темы занятия	Кол-во часов
1.	2	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.	2
2.	3	Формальные языки и способы их описания. Классификация формальных грамматик. Их использование в лексическом и синтаксическом анализе. Лямбда-исчисление, правила редукции, единственность нормальной формы и правила ее достижения, представление рекурсивных функций.	2
ВСЕГО			**4**

3.4. Семинарские занятия

	№ Раздела (темы)	Краткое содержание темы занятия	Кол-во часов
3.	1	Задачи по темам: алгебра логики, исчисление предикатов.	2
4.	2	Задачи по темам: формальные модели алгоритмов, сложность и эффективность алгоритмов.	2
5.	3	Задачи по темам: формальные языки, лямбда-исчисление, автоматы	2
6.	4	Задачи по темам: кодирование и методы сжатия информации	2
7.	5	Задачи по теме криптография, повторение предыдущих тем.	2
ВСЕГО			**10**

4. ТЕКУЩАЯ И ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Текущая аттестация аспирантов. Текущая аттестация аспирантов проводится в соответствии с локальным актом ИПМ им. М.В. Келдыша РАН - Положением о текущей, промежуточной и итоговой аттестации аспирантов ИПМ им. М.В. Келдыша РАН по программам высшего образования – программам подготовки научно-педагогических кадров в аспирантуре и является обязательной.

Текущая аттестация по дисциплине проводится в форме опроса, а также оценки вопроса-ответа в рамках участия обучающихся в дискуссиях и различных контрольных мероприятиях по оцениванию фактических результатов обучения, осуществляемых преподавателем, ведущим дисциплину. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины см. ниже.

Объектами оценивания выступают:

- учебная дисциплина – активность на занятиях, своевременность выполнения различных видов заданий, посещаемость занятий;
- степень усвоения теоретических знаний и уровень овладения практическими умениями и навыками по всем видам учебной работы, проводимых в рамках семинаров, практических занятий и самостоятельной работы.

Оценивание обучающегося на занятиях осуществляется с использованием нормативных оценок по 4-х бальной системе (5-отлично, 4-хорошо, 3-удовлетворительно, 2- не удовлетворительно).

Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

Форма контроля знаний	Вид аттестации	Примечание
проверочные работы в течение всего курса	текущая	Ниже приведены перечни рекомендуемых задач и контрольных вопросов
зачет	итоговая	

Примерный перечень рекомендуемых контрольных вопросов для оценки **текущегоуровня** успеваемости студента:

1. Высказывания: простые, сложные, примеры высказываний. Истинностное значение высказывания.
2. Дать определение конъюнкции, импликации, дизъюнкции и эквиваленции.
3. Свойство коммутативности и дистрибутивности. Какие логические связки им удовлетворяют
4. Свойство ассоциативности и идемпотентности. Какие логические связки им удовлетворяют?
5. Отрицание высказывания. Снятие двойного отрицания. Правила де Моргана.
6. Равносильные формулы. Формулы поглощения и расщепления.
7. Тавтология и противоречие. Свойства констант.

8. Двойственная формула. Принцип двойственности.
9. Проблема разрешимости в логике высказываний. Определение КНФ. Как проверить, что формула является тавтологией с помощью КНФ?
10. Проблема разрешимости в логике высказываний. Определение ДНФ. Как проверить, что формула является противоречием с помощью ДНФ?
11. Определение аксиоматической теории.
12. Определение вывода формулы.
13. Правила подстановки и m.p.
14. Теорема дедукции.
15. Правила силлогизма и разъединения посылок.
16. Правила перестановки и соединения посылок.
17. Полнота и непротиворечивость аксиоматической теории.
18. Размещения с повторениями и без повторений. Перестановки.
19. Сочетания с повторениями и без повторений.
20. Нормальный алгоритм Маркова: алфавит, подстановка, правила очередности применения подстановок.
21. Тезисы Черча, Тьюринга, Маркова.
22. Общие черты алгоритмов.
23. Временная и пространственная сложность. Классы сложности. Проблемы классов P и NP.
24. Определение ориентированного и неориентированного графа
25. Определение цепи, цикла, пути, контура в графе. Определение подграфа. Связность в графах.
26. Алфавит, слово, язык над данным алфавитом.
27. Пустое слово, конкатенация слов, степень слова, длина слова, количество вхождений данного символа.
28. Способы конечного задания формального языка.
29. Автоматы, соответствующие праволинейным грамматикам
30. Понятия конечного автомата, недетерминированного конечного автомата
31. Язык распознаваемый конечным автоматом.
32. Свойства замкнутости класса всех автоматных языков относительно итерации, конкатенации, объединения, дополнения и пересечения.
33. Неавтоматность формального языка
34. Регулярные выражения.
35. Применение регулярных выражений.

Примерный перечень рекомендуемых контрольных задач для оценки **текущего уровня** успеваемости студента:

1. Приведением к КНФ(ДНФ) установить является ли формула тавтологией (противоречием)
$$\Phi = (B \vee \overline{C}) \to (A \sim \overline{B}).$$
2. Доказать вывод формулы, используя алгоритм методарезолюций
$B \to (A \to C), A \vdash (B \to C)$
3. Записать программу машины Тьюринга, вычисляющую функцию:

$$f(x) = \left[\frac{4}{3-x}\right] = \begin{cases} 1, & \text{при } x = 0 \\ 2, & \text{при } x = 1 \\ 4, & \text{при } x = 2 \\ \text{не определено}, & \text{при } x > 2 \end{cases}$$

4. Найдите функцию временной сложности следующего фрагмента алгоритма, написанного на псевдокоде, подсчитав количество операторов присваивания x := x + 1, которые в нем выполняются

```
begin
    for i := 1 to 2n do
        for j := 1 to n do
            for k := 1 to j do
                x := x + 1;
end
```

5. Опишите условный оператор в Лямбда-исчислении.
6. Опишите язык, получаемый в алфавите x_1 грамматикой A : $G = \langle A, V, S, P \rangle$ x_2

$$A = \{a, b, c\}, \qquad V = \{S, A, B, C\},$$

$$P: 1)\ S \to A, \quad 2)\ A \to aA, \quad 3)\ A \to a, \quad 4)\ A \to AB,$$
$$5)\ S \to B, \quad 6)\ B \to bB, \quad 7)\ B \to b, \quad 8)\ B \to BC,$$
$$9)\ S \to C, \quad 10)\ C \to cC, \quad 11)\ C \to c, \quad 12)\ S \to \Lambda,$$

7. Для зашифровки сообщения на русском языке, записанного без знаков препинания и пробелов, используется последовательность натуральных чисел x_1, x_2, K, удовлетворяющая соотношению: $x_k = b \cdot 8^{a(k-1)}$, $k = 1,2,\text{K}$. Здесь a и b – фиксированные (но неизвестные) натуральные числа. Зашифрование производится следующим образом. Первую букву сообщения заменяют числом согласно таблице 1 и складывают с x_1. Потом также заменяют вторую букву и складывают с x_2 и т. д.

Затем все суммы заменяют остатками от деления на 31, а остатки заменяют буквами согласно таблице

А	Б	В	Г	Д	Е	Ё	Ж	З	И,Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь,Ъ	Э	Ю	Я
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

В результате получился текст

ОЯФПРПЯФБКПЩСЬИЖЬИЯЫСЯЗТХЖУТНАЖБСЁНФВГМНУТУЁШЖФН

Найдите исходное сообщение, представляющее собой отрывок известного стихотворения,если известно , что в нем есть слово РАВНИНЫ

8. Все 16 городов Криптоландии в качестве названий имеют различные четырехразрядные комбинации, состоящие из нулей и единиц (например, «0011»). Все города попарно соединены непересекающимися дорогами , причем проезд из одного города в другой стоит столько криптов , в скольких разрядах различаются их имена (например, из «0011» в «1001» – 2 крипта). Путешественник, находящийся в «0000», хочет объехать все города страны и вернуться назад за минимальную цену. Как ему это сделать ?

Итоговая аттестация аспирантов. Итоговая аттестация аспирантов по дисциплине проводится в соответствии с локальным актом ИПМ им. М.В. Келдыша РАН
– Положением о текущей, промежуточной и итоговой аттестации аспирантов ИПМ им. М.В. Келдыша РАН обучающихся по программам подготовки научных и научно- педагогических кадров в аспирантуре и является обязательной.

Итоговая аттестация по дисциплине осуществляется в форме зачета в период зачетно-экзаменационной сессии в соответствии с Графиком учебного. Обучающийся допускается к зачетув случае выполнения аспирантом всех учебных заданий и мероприятий, предусмотренных настоящей программой. В случае наличия учебной задолженности (пропущенных занятий и (или) невыполненных заданий) аспирант отрабатывает пропущенные занятия и выполняет задания.

Оценивание обучающегося на промежуточной аттестации осуществляется с использованием нормативных оценок на зачете – зачет, незачет.

Оценивание аспиранта на промежуточной аттестации в форме экзамена

Оценка	Требования к знаниям и критерии выставления оценок
Незачет	основное содержание учебного материала не раскрыто; допущеныгрубые ошибка в определении понятий и при использовании терминологии; не даны ответы на дополнительные вопросы.

Зачет	раскрыто содержание материала, даны корректные определенияпонятий; допускаются незначительные нарушения последовательности изложения; допускаются небольшие неточности при использовании терминов илив логических выводах; при неточностях задаются дополнительные вопросы.

Список вопросов к **итоговой** аттестации аспирантов.

1. Понятие сложности алгоритмов.
2. Классы P и NP.
3. Полиномиальная сводимость задач.
4. Теорема Кука об NP-полноте задачи выполнимости булевой формулы.
5. Примеры NP-полных задач, подходы к их решению.
6. Точные и приближенные комбинаторные алгоритмы.
7. Примеры эффективных (полиномиальных) алгоритмов.
8. Формальные языки и способы их описания.
9. Классификация формальных грамматик.
10. Использование в лексическом и синтаксическом анализе.
11. Лямбда-исчисление.
12. Правила редукции.
13. Единственность нормальной формы и правила ее достижения.
14. Представление рекурсивных функций

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

1. Яблонский С.В. Введение в дискретную математику. М., 2001
2. Айзерман М.А. и др. Логика. Автоматы. Алгоритмы. М., 1963.

Дополнительная литература и Интернет-ресурсы

1. Лавров И.А., Максимова Л.Л. Задачи по теории множеств, математической логике итеории алгоритмов. М.: Физматгиз,2001.
2. Д. Сэлмон Сжатие данных, изображений и звука М.: Техносфера, 2004.
3. Верещагин Н. К., Шень А. Лекции по математической логике и теории алгоритмов. Часть 2. Языки и исчисления (4-е издание, исправленное). М.: МЦНМО, 2012.
4. Верещагин Н. К., Шень А. Лекции по математической логике и теории алгоритмов. Часть 3. Вычислимые функции (4-е издание, исправленное). М.: МЦНМО, 2012.
5. Абрамов С.А Лекции о сложности алгоритмов (2-е, переработанное). М.: МЦНМО, 2012.
6. Т.С. Соболева, А.В. Чечкин Дискретная математика. М.: Academia 2014
7. А. Е. Пентус, М. Р. Пентус. Теория формальных языков. М.: Изд-во ЦПИ при механико-математическом ф-те МГУ, 2004 (http://www.mccme.ru/free- books/pentus/pentus.pdf).
8. Шнайер Б. Прикладная криптография. 2-е издание М.: Триумф, 2002.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для обеспечения интерактивных методов обучения для чтения лекций требуется аудитория с мультимедиа (возможен вариант с интерактивной доской).

Для проведения дискуссий и круглых столов, возможно, использование аудиторий со специальным расположением столов и стульев.

ИСПОЛНИТЕЛИ (разработчики программы):
Бондаренко А.А., ИПМ им. М.В. Келдыша, научный сотрудник, к.ф.-м.н.