

МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ

Декан математического факультета



Нестеров П.Н.

21 мая 2024 г.

Рабочая программа дисциплины
Теория алгоритмов и сложность вычислений

Направление подготовки (специальности)
02.04.01 Математика и компьютерные науки

Направленность (профиль)
«Компьютерная математика»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 26 апреля 2024 г., протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 3 мая 2024 г.

1. Цели освоения дисциплины

Дисциплина «Теория алгоритмов и сложность вычислений» обеспечивает приобретение фундаментальных знаний и умений в соответствии с Федеральным государственным образовательным стандартом направления подготовки 02.04.01 «Математика и компьютерные науки», содействует фундаментализации образования, развитию логического и алгоритмического мышления и формированию математического и общенаучного мировоззрения. Целью изучения дисциплины является овладение базовыми понятиями и методами теории алгоритмов, ознакомление с их применениями в области обеспечения информационной безопасности, установление существования алгоритмически неразрешимых проблем и значение этого фундаментального факта теории алгоритмов для алгоритмической практики, компьютерных наук и защиты информации, ознакомление с базовыми подходами к оценке сложности алгоритмов и задач и некоторыми приемами построения эффективных алгоритмов.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Теория алгоритмов и сложность вычислений» относится к части образовательной программы, формируемой участниками образовательных отношений. Она играет исключительно важную роль для общематематической и общепрофессиональной подготовки выпускников. При ее изучении используются знания, полученные при изучении математических дисциплин «Алгебра», «Теория чисел», «Дискретная математика», «Информатика» и «Математическая логика и приложения в информатике и компьютерных науках». Знания, умения и навыки, полученные при изучении дисциплины «Теория алгоритмов и сложность вычислений», используются обучаемыми при изучении общепрофессиональных и специальных дисциплин.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих элементов компетенций в соответствии с ФГОС ВО, ООП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	Индикатор достижения компетенции (код и формулировка)	Перечень планируемых результатов обучения
Профессиональные компетенции		
ПК-1 Способен создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники.	И-ПК-1.3 Обладает фундаментальными знаниями, полученными в области математического моделирования.	Знать: основные понятия, принципиальные результаты и методы алгоритмов и сложности вычислений. Уметь: Решать стандартные задачи теории алгоритмов и сложности вычислений. Владеть навыками: Написания программ для машин Тьюринга, оценки временной и емкостной сложности алгоритмов.

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет **5** зачетных единиц, **180** акад. часов.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости Форма промежуточной аттестации (по семестрам)
			Контактная работа					самостоятельная работа	
			лекции	практические	лабораторные	консультации	аттестационные испытания		
1	Вводная лекция	3	1						Устный опрос.
2	Частично рекурсивные, рекурсивные и примитивно рекурсивные функции. Алгоритмическая теория множеств.	3	10	6		1		16	Задания для самостоятельной работы, устный опрос, контрольная работа №1
3	Машины Тьюринга.	3	6	6		1		8	Задания для самостоятельной работы, устный опрос
4	Арифметизация теории машин Тьюринга. Эквивалентность класса частично рекурсивных функций и класса вычислимых по Тьюрингу функций.	3	8			1		8	Задания для самостоятельной работы, устный опрос
5	Теорема Райса	3	6	4		1		16	Задания для самостоятельной работы, устный опрос, контрольная работа №2
6	m-сводимость	3	2			1		4	устный опрос
7	Алгоритмически неразрешимые проблемы	3	2			1		6	Задания для самостоятельной работы, устный опрос
8	Введение в сложность вычислений. Классы сложности.	3	2			1		2	устный опрос
9	NP-полные проблемы. Теорема Кука.	3	6			1		8	Задания для самостоятельной работы, устный опрос
10	Нормальные алгорифмы А.А. Маркова. Сложность описания нормального алгорифма.	3	2					2	устный опрос
11	Сложность конечных объектов по А.Н. Колмогорову.	3	3					2	устный опрос

						2	0,5	33,5	Экзамен
		Всего	48	16		10	0,5	105,5	

Содержание разделов дисциплины:

Тема 1. Вводная лекция.

История развития теории алгоритмов. Теория алгоритмов и принципиальные возможности компьютеров. Оценки сложности алгоритмов и их значение для практики. Интуитивное понятие «алгоритм». Необходимость математического уточнения понятия «алгоритм». Два подхода к уточнению понятия «алгоритм».

Тема 2. Частично рекурсивные, рекурсивные и примитивно рекурсивные функции. Алгоритмическая теория множеств.

Тезис Черча. Определение классов примитивно рекурсивных и частично рекурсивных функций: исходные функции, оператор суперпозиции, оператор примитивной рекурсии, оператор минимизации. Примитивная рекурсивность теоретико-числовых функций. Операции суммирования и мультиплицирования. Задание функций кусочными схемами. Ограниченный оператор минимизации. Канторовские нумерационные функции и их примитивная рекурсивность. Примитивная рекурсивность функции Гёделя. Функция Аккермана и ее свойства. Рекурсивные и рекурсивно перечислимые множества. Теорема о графике. Теорема Поста.

Тема 3. Машины Тьюринга.

Машины Тьюринга-Поста. Вычислимость и правильная вычислимость по Тьюрингу. Операции над машинами Тьюринга: композиция и ветвление. Транспозиция, удвоение, циклический сдвиг, копирование. Правильная вычислимость по Тьюрингу любой частично рекурсивной функции.

Тема 4. Арифметизация теории машин Тьюринга. Эквивалентность класса частично рекурсивных функций и класса вычислимых по Тьюрингу функций.

Частичная рекурсивность любой вычислимой по Тьюрингу функции. Тьюрингов предикат вычислимости. Существование рекурсивно перечислимого, но не рекурсивного множества.

Тема 5. Теорема Райса.

Универсальные функции. Нумерации Клини и Поста. Теорема о трансляторе. Теорема о неподвижной точке. Теорема Райса для частично рекурсивных функций и для рекурсивно перечислимых множеств.

Тема 6. m-сводимость.

m-универсальные, креативные и продуктивные множества.

Тема 7. Алгоритмически неразрешимые проблемы.

Проблемы применимости и самоприменимости. Примеры алгоритмически разрешимых и неразрешимых задач из различных областей математики.

Тема 8. Введение в сложность вычислений. Классы сложности.

Некоторые подходы к оценкам сложности алгоритмов и вычислений. Модели вычислений. Сложность вычисления на детерминированной машине Тьюринга. Временная и емкостная меры сложности (детерминированный случай). Полиномиально ограниченные детерминированные машины Тьюринга. Классы языков P-TIME и P-SPACE. Пример языка, не входящего в класс P-TIME.

Тема 9. NP-полные проблемы. Теорема Кука.

Временная и емкостная меры сложности (недетерминированный случай). Класс языков NP-TIME. Проблема $NP = P$? Полиномиальная сводимость. NP-трудные и NP-полные языки (задачи, проблемы). NP-полнота проблемы выполнимости для формул логики высказываний (булевых функций). Теорема Кука. NP-полные проблемы для уравнений в свободных полугруппах и для регулярных языков. NP-полные проблемы в теории графов. NP-полные проблемы из различных разделов математики.

Тема 10. Нормальные алгорифмы А.А. Маркова. Сложность описания нормального алгорифма.

Нормальные алгорифмы А.А.Маркова: схема алгорифма, заключительные и простые правила подстановки (замены). Примеры нормальных алгорифмов. Принцип нормализации А.А.Маркова. Композиция нормальных алгорифмов. Связь с машинами Тьюринга и частично рекурсивными функциями.

Тема 11. Сложность конечных объектов по А.Н. Колмогорову

5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Вводная лекция – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

Академическая лекция с элементами лекции-беседы – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Элементы лекции-беседы обеспечивают контакт преподавателя с аудиторией, что позволяет привлекать внимание студентов к наиболее важным темам дисциплины, активно вовлекать их в учебный процесс, контролировать темп изложения учебного материала в зависимости от уровня его восприятия.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков по закреплению полученных на лекции знаний.

Консультации – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы студентов. На консультациях по просьбе студентов рассматриваются наиболее сложные моменты при освоении материала дисциплины, преподаватель отвечает на вопросы студентов, которые возникают у них в процессе самостоятельной работы.

6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине

В процессе осуществления образовательного процесса по дисциплине используются:

для формирования материалов для текущего контроля успеваемости и проведения промежуточной аттестации, для формирования методических материалов по дисциплине:

- программы Microsoft Office;
- издательская система LaTeX;
- Adobe Acrobat Reader;

7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)

В процессе осуществления образовательного процесса по дисциплине используются:

- Автоматизированная библиотечно-информационная система «БУКИ-NEXT»
http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php
- Электронная библиотечная система «Лань» <https://e.lanbook.com>
- Электронная библиотечная система «Юрайт» <https://urait.ru>
- Электронная библиотечная система «Консультант студента»
<https://www.studentlibrary.ru>
- Общероссийский портал Math-Net.Ru <http://www.mathnet.ru/>

8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет» (при необходимости), рекомендуемых для освоения дисциплины

а) основная литература

1. Судоплатов С. В., Овчинникова Е. В. Математическая логика и теория алгоритмов: учебник и практикум для вузов. - Москва: Юрайт, 2023. <https://urait.ru/viewer/matematiceskaya-logika-i-teoriya-algoritmov-510826>
2. Скорубский В. И., Поляков В. И., Зыков А. Г. Математическая логика: учебник и практикум для вузов. - Москва: Юрайт, 2023. <https://urait.ru/viewer/matematiceskaya-logika-511996>
3. Крупский, В. Н. Теория алгоритмов. Введение в сложность вычислений : учебное пособие для вузов / В. Н. Крупский. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2024. — 117 с. — (Высшее образование). — ISBN 978-5-534-04817-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/539671>

б) дополнительная литература

1. Дурнев В. Г. Элементы теории алгоритмов: учеб. пособие для вузов - Ярославль, ЯрГУ, 2008 <http://www.lib.uniyar.ac.ru/edocs/iuni/20080230.pdf>
2. Дурнев В. Г., Материалы по дисциплине «Теория алгоритмов и сложность вычислений»: метод. указания - Ярославль, ЯрГУ, 2010 <http://www.lib.uniyar.ac.ru/edocs/iuni/20100268.pdf>
3. Мальцев А. И. Алгоритмы и рекурсивные функции - М.: Наука, 1986.
4. М. М. Глухов, О. А. Козлитин, В. А. Шапошников, А. Б. Шишков Задачи и упражнения по математической логике, дискретным функциям и теории алгоритмов: учеб. пособие для вузов - СПб., Лань, 2022 <https://reader.lanbook.com/book/247400>
5. И. А. Лавров, Л. Л. Максимова Задачи по теории множеств, математической логики и теории алгоритмов - М.: Физматлит, 2002. <https://www.studentlibrary.ru/ru/book/ISBN5922100262.html>

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

- учебные аудитории для проведения занятий лекционного типа;

- учебные аудитории для проведения практических занятий (семинаров);
- учебные аудитории для проведения групповых и индивидуальных консультаций;
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы;
- помещения для хранения и профилактического обслуживания технических средств обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде ЯрГУ.

Автор:

Ассистент кафедры КБиММОИ

Белов А.Р.

**Приложение № 1 к рабочей программе дисциплины
«Теория алгоритмов и сложность вычислений»**

**Фонд оценочных средств
для проведения текущего контроля успеваемости
и промежуточной аттестации студентов
по дисциплине**

**1. Типовые контрольные задания и иные материалы,
используемые в процессе текущего контроля успеваемости**

Контрольная работа № 1

(проверка сформированности ПК-1, индикатор ИД-ПК-1.3)

Примеры заданий:

1. Можно ли с помощью одного применения операции минимизации получить нигде не определенную функцию из всюдуопределенной?
2. Докажите примитивную рекурсивность функций НОД(x, y) и НОК(x, y).
3. Докажите, что существует числовая функция, которая не является частично рекурсивной.
4. Докажите примитивную рекурсивность функции $f(n)$, которая каждому натуральному числу n ставит в соответствие n -ое число Фибоначчи.

Контрольная работа № 2

(проверка сформированности ПК-1, индикатор ИД-ПК-1.3)

Примеры заданий:

1. Докажите примитивную рекурсивность конечного множества
2. Докажите, что бесконечное рекурсивно перечислимое множество содержит бесконечное рекурсивное подмножество.
3. Докажите, что существует множество, которое не является рекурсивно перечислимым.
4. Докажите, что график функции Аккермана рекурсивно перечислим.

2. Список вопросов и (или) заданий для проведения промежуточной аттестации

На экзамене проверяется сформированность компетенции ПК-1 (индикатор ИД-ПК-1.3).

Оценка на экзамене выставляется по результатам собеседования по темам из списка вопросов и по результатам контрольных работ, выполненных в течении семестра.

Список вопросов к экзамену:

1. Понятие «алгоритм» в интуитивном смысле. Необходимость его математического уточнения.
2. Примитивно рекурсивные функции. Всюдуопределенность примитивно рекурсивных функций. Примеры.
3. Частично рекурсивные и рекурсивные функции. Тезис Черча. Операции над примитивно рекурсивными, рекурсивными и частично рекурсивными функциями.
4. Функция Аккермана и ее свойства.

5. Прimitивно рекурсивные предикаты и отношения. Кусочное задание функций. Ограниченный оператор минимизации.
6. Прimitивная рекурсивность некоторых теоретико-числовых функций.
7. Нумерационные функции. Нумерации Кантора и Гёделя. Их прimitивная рекурсивность.
8. Рекурсивные и рекурсивно перечислимые множества. Эквивалентные определения рекурсивной перечислимости.
9. Теорема о графике.
10. Теорема Поста.
11. Машины Тьюринга. Вычислимость и правильная вычислимость по Тьюрингу. Тезис Тьюринга. Операции над машинами Тьюринга.
12. Замкнутость класса правильно вычисляемых по Тьюрингу функций относительно операций суперпозиции, прimitивной рекурсии и минимизации.
13. Арифметизация теории машин Тьюринга.
14. Частичная рекурсивность любой вычисляемой по Тьюрингу функции.
15. Нормальная форма Клини.
16. Универсальные функции.
17. Алгоритмически неразрешимые проблемы. Алгоритмическая неразрешимость проблем останова, самоприменимости и применимости к пустому слову.
18. Нумерация функций и множеств. Нумерация Клини.
19. Теорема о трансляторе.
20. Теорема о неподвижной точке.
21. Теорема Райса.
22. m-сводимость. m-универсальное множество.
23. Сложность алгоритмов. Сложностные характеристики работы машины Тьюринга. Сложностные классы.
24. Недетерминированные машины Тьюринга. Классы P и NP. NP трудные и NP полные проблемы. Примеры.
25. Теорема Кука.
26. Проблема выполнимости k-КНФ. Случай $k=2$ и $k=3$.

3. Правила выставления оценки на экзамене.

В экзаменационный билет включается два теоретических вопроса. На подготовку к ответу дается не менее 1 часа.

По итогам экзамена выставляется одна из оценок: «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Оценка «Отлично» выставляется студенту, который демонстрирует глубокое и полное владение содержанием материала и понятийным аппаратом криптографии; осуществляет межпредметные связи; умеет связывать теорию с практикой. Студент дает развернутые, полные и четкие ответы на вопросы экзаменационного билета и дополнительные вопросы, соблюдает логическую последовательность при изложении материала. Грамотно использует криптографическую терминологию.

Оценка «Хорошо» выставляется студенту, ответ которого на экзамене в целом соответствует указанным выше критериям, но отличается меньшей обстоятельностью, глубиной, обоснованностью и полнотой. В ответе имеют место отдельные неточности (несущественные ошибки), которые исправляются самим студентом после дополнительных и (или) уточняющих вопросов экзаменатора.

Оценка «Удовлетворительно» выставляется студенту, который дает недостаточно полные и последовательные ответы на вопросы экзаменационного билета и

дополнительные вопросы, но при этом демонстрирует умение выделить существенные и несущественные признаки и установить причинно-следственные связи. Ответы излагаются с использованием терминологии принятой в криптографии, но при этом допускаются ошибки в определении и раскрытии некоторых основных понятий, формулировке положений, которые студент затрудняется исправить самостоятельно. При аргументации ответа студент не обосновывает свои суждения. На часть дополнительных вопросов студент затрудняется дать ответ или дает неверные ответы.

Оценка «Неудовлетворительно» выставляется студенту, который демонстрирует разрозненные, бессистемные знания; беспорядочно и неуверенно излагает материал; не умеет выделять главное и второстепенное, не умеет соединять теоретические положения с практикой, не устанавливает межпредметные связи; допускает грубые ошибки при определении сущности раскрываемых понятий, явлений, вследствие непонимания их существенных и несущественных признаков и связей; дает неполные ответы, логика и последовательность изложения которых имеют существенные и принципиальные нарушения, в ответах отсутствуют выводы. Дополнительные и уточняющие вопросы экзаменатора не приводят к коррекции ответов студента. На основную часть дополнительных вопросов студент затрудняется дать ответ или дает неверные ответы.

Оценка «Неудовлетворительно» выставляется также студенту, который взял экзаменационный билет, но отвечать отказался.