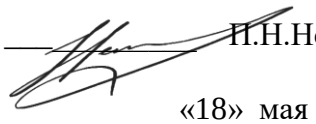
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ

Декан математического факультета


П.Н.Нестеров

«18» мая 2021 г.

Рабочая программа дисциплины
«Теория алгоритмов и сложность вычислений»

Направление подготовки
10.06.01 Информационная безопасность

Направленность (профиль)
«Методы и системы защиты информации,
информационная безопасность»

Форма обучения очная

Программа рассмотрена
на заседании кафедры компьютерной безопасности
и математических методов обработки информации
от «16» апреля 2021 года, протокол № 8

Ярославль

1. Цели освоения дисциплины

Дисциплина «Теория алгоритмов и сложность вычислений» обеспечивает приобретение фундаментальных и профессиональных знаний, умений и навыков, содействует дальнейшей фундаментализации образования, развитию логического 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 программы аспирантуры

Дисциплина «Теория алгоритмов и сложность вычислений» является дисциплиной по выбору вариативной части. Она играет важную роль для общематематической и общепрофессиональной подготовки специалиста. При ее изучении используются знания, полученные при изучении таких математических дисциплин, как “Алгебра”, "Теория чисел", "Дискретная математика", "Информатика" и "Математическая логика и теория алгоритмов".

3. Планируемые результаты обучения по дисциплине – знания, умения, навыки и (или) опыт деятельности, характеризующие этапы формирования компетенций и обеспечивающие достижение планируемых результатов освоения программы аспирантуры, и критерии их оценивания

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Профессиональные компетенции:

- способностью разрабатывать методы проектирования и анализа алгоритмов, программ, языков программирования, исследовать и создавать методы анализа, оценки качества, стандартизации и сопровождения программных систем (ПК-3);

Результаты обучения выпускника формулируются в следующих категориях:
«знать» – означает способность выпускника воспроизводить учебный материал с требуемой степенью научной точности (формулировать определение, с достаточной полнотой описывать процесс и явление);
«уметь» – означает способность выпускника решать типовые (адаптированные) задачи на основе воспроизведения алгоритма решения и его применения в конкретных стандартных условиях;
«владеть» – означает способность выпускника решать усложненные, в том числе комплексные задачи. Задачи данного уровня решаются на основе ранее приобретенных знаний и умений, с их трансформацией и применением в новых нетиповых условиях.

Код компетенции	**Планируемые результаты обучения**	**Критерии оценивания результатов обучения**		
		Пороговый уровень	**Продвинутый уровень**	**Высокий Уровень**
Способностью	**Знать:**	**Знает:**	**Знает:**	**Знает:**

разрабатывать методы проектирования и анализа алгоритмов, программ, языков программирования, исследовать и создавать методы анализа, оценки качества, стандартизации и сопровождения программных систем (ПК-3)	методы проектирования и анализа алгоритмов, программ, языков программирования, **Уметь:** исследовать и создавать методы анализа, оценки качества и стандартизации, **Владеть:** Навыками сопровождения программных систем.	методы проектирования и анализа алгоритмов, программ, языков программирования.	методы проектирования и анализа алгоритмов, программ, языков программирования. **Умеет:** исследовать и создавать методы анализа, оценки качества и стандартизации.	методы проектирования и анализа алгоритмов, программ, языков программирования. **Умеет:** исследовать и создавать методы анализа, оценки качества и стандартизации. **Владеет:** Навыками сопровождения программных систем.

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 акад.часов

Дисциплина изучается в течение второго семестра. Формой итоговой промежуточной аттестации по дисциплине является зачет.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий и их трудоемкость (в академических часах)					Формы текущего контроля успеваемости Форма промежуточной аттестации *(по семестрам)*
			лекции	практические	лабораторные	консультации	самостоятельная работа	
	Теория алгоритмов							
1	Введение. История развития теории алгоритмов.	2					1	
2	Машины Тьюринга.	2		1			3	
3	Частично рекурсивные, рекурсивные и примитивно рекурсивные функции.	2					3	
4	Примитивно рекурсивные и	2				0,5	3	Собеседование на консультации

	рекурсивные предикаты, отношения и множества, операции над ними.							
5	Задание функций и предикатов.	2					3	
6	Нумерация.	2					3	
7	Рекурсивно перечислимые множества, отношения и предикаты.	2		1			3	
8	Операции над машинами Тьюринга.	2					3	
9	Вычислимость функций по Тьюрингу**.**	2					3	
10	Арифметизация теории машин Тьюринга.	2		1		0,5	3	Собеседование на консультации
11	Нормальная форма Клини.	2					3	
12	Алгоритмическая неразрешимость	2					3	
13	Тьюрингов предикат вычислимости.	2					3	
14	Нумерация Клини частично рекурсивных функций.	2					3	
15	Теорема Райса для частично рекурсивных функций.	2		1			3	
16	Нумерация Поста рекурсивно перечислимых множеств.	2					3	
17	Сводимость по Тьюрингу. *m*-сводимость.	2					3	
18	Нормальные алгорифмы А.А.Маркова.	2					3	
19	Алгоритмическая разрешимость и неразрешимость.	2					4	
	Сложность вычислений							
1	Детерминированные	2		1			3	

	многоленточные машины Тьюринга.							
2	Сложность алгоритмов и вычислений.	2					3	
3	Недетерминированные многоленточные машины Тьюринга**.**	2				0,5	3	Собеседование на консультации
4	Временная и емкостная меры сложности (недетерминированный случай).	2		1			3	
5	Свойства функций сложности.	2					3	
6	Сложность проблемы разрешимости систем линейных уравнений.	2					3	
7	**NP-полные** проблемы для уравнений в свободных полугруппах и для регулярных языков.	2					3	
8	**NP-полные** проблемы в теории графов.	2					3	
9	**NP-полные проблемы** из различных разделов математики.	2		1			3	
10	Алгоритмически неразрешимые проблемы в области защиты информации.	2		1			3	
11	Сложностная классификация языков.	2				0,5	3	Собеседование на консультации
12	Сложность описания нормального алгорифма А.А.Маркова.	2					3	
13	Теория алгоритмов и задачи использования ЭВМ.	2					3	
14	Сложность конечных объектов по А.Н.Колмогорову.	2					3	
		2						Зачет
	Всего			**8**		**2**	**98**	

Содержание разделов дисциплины.

Раздел "Теория алгоритмов"

Тема 1. Введение. История развития теории алгоритмов.
Теория алгоритмов и принципиальные возможности компьютеров.
Оценки сложности алгоритмов и их значение для практики.

Тема 2. Машины Тьюринга.
Интуитивное понятие "алгоритма" и его характерные черты. Задачи, приводящие к необходимости уточнения понятия "алгоритм".
Вычислимые в интуитивном смысле функции.
Два подхода к уточнению понятия "алгоритм".
Машины Тьюринга-Поста: внешний и внутренний алфавиты, программы и команды. Конфигурации. Композиция и ветвление машин Тьюринга. Вычислимость и правильная вычислимость функций по Тьюрингу. Принцип Тьюринга- Поста-Черча.
Правильная вычислимость исходных функций и сложения.

Тема 3. Частично рекурсивные, рекурсивные и примитивно рекурсивные функции.
Тезис Черча.
Примитивная рекурсивность теоретико-числовых функций.
Операции суммирования и мультиплицирования.

Тема 4. Примитивно рекурсивные и рекурсивные предикаты, отношения и множества, операции над ними.
Соотношения между классами примитивно рекурсивных, общерекурсивных и частично рекурсивных функций.

Тема 5. Задание функций и предикатов.
Задание функций кусочными схемами.
Ограниченный оператор минимизации.
Примитивная рекурсивность функций, связанных с каноническим представлением натуральных чисел и с делением с остатком.

Тема 6. Нумерация.
Канторовские нумерационные функции, их примитивная рекурсивность.
Примитивная рекурсивность функции Геделя.

Тема 7. Рекурсивно перечислимые множества, отношения и предикаты.
Рекурсивно перечислимые множества, отношения и предикаты, операции над ними.
Теорема о графике функции. Ее следствия.

Тема 8. Операции над машинами Тьюринга.
Транспозиция, удвоение, циклический сдвиг, копирование

Тема 9. Вычислимость функций по Тьюрингу.
Правильная вычислимость по Тьюрингу любой частично рекурсивной функции.

Тема 10. Арифметизация теории машин Тьюринга.
Частичная рекурсивность любой вычислимой по Тьюрингу функции.

Тема 11. Нормальная форма Клини.
Универсальные частично рекурсивные функции.

Тема 12. Алгоритмическая неразрешимость.
Неразрешимость проблемы самоприменимости и применимости для машин Тьюринга.

Тема 13. Тьюрингов предикат вычислимости.
Существование рекурсивно перечислимого, но не рекурсивного множества.

Тема 14. Нумерация Клини частично рекурсивных функций. Универсальные функции Клини.
Теорема о неподвижной точке для частично рекурсивных функций.

Тема 15. Теорема Райса для частично рекурсивных функций.

Тема 16. Нумерация Поста рекурсивно перечислимых множеств.
Теорема о неподвижной точке для рекурсивно перечислимых множеств.
Теорема Райса для рекурсивно перечислимых множеств.

Тема 17. Сводимость по Тьюрингу. *m*-сводимость.
m-универсальные, креативные и продуктивные множества.

Тема 18. Нормальные алгоритмы А.А. Маркова.
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 19. Алгоритмическая разрешимость и неразрешимость. Нумерация слов в счетном алфавите и арифметизация алгоритмов. Примеры алгоритмически разрешимых и неразрешимых задач из математической логики, теории алгоритмов, алгебры, теории чисел, теории формальных грамматик, теории обыкновенных дифференциальных уравнений, топологии, математического анализа и теории конечных автоматов. Теорема Черча о неразрешимости логики предикатов.
Значение существования алгоритмически неразрешимых проблем для обще математической практики, приложений в компьютерных науках и в области обеспечения информационной безопасности.

Раздел "Сложность вычислений":

Тема 1. Детерминированные многоленточные машины Тьюринга.
Внешний и внутренний алфавиты k-ленточной детерминированной машины Тьюринга. Программа и команды. Конфигурации. Описание выполнения команд в терминах преобразования конфигураций. Языки, принимаемые (допускаемые, распознаваемые) k-ленточными детерминированными машинами Тьюринга.

Тема 2. Сложность алгоритмов и вычислений. 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 3. Недетерминированные многоленточные машины Тьюринга.
Внешний и внутренний алфавиты k-ленточной недетерминированной машины Тьюринга. Программа и команды недетерминированной машины Тьюринга. Их особенность.

Конфигурации. Описание выполнения команд в терминах преобразования конфигураций. Языки, принимаемые (допускаемые) недетерминированными k-ленточными машинами Тьюринга.

Тема 4. 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).

Тема 5. Свойства функций сложности.
Нижние оценки. Сложность распознавания функциональной полноты системы булевых функций, сложность проблем вхождения в классы самодвойственных, монотонных и линейных функций. Существование сколь угодно сложно вычислимых функций.

Тема 6. Сложность проблемы разрешимости систем линейных уравнений.
Решение систем целочисленных линейных уравнений в целых, натуральных и 0-1 числах.

Тема 7. NP-полные проблемы для уравнений в свободных полугруппах и для регулярных языков.

Тема 8. NP-полные проблемы в теории графов.

Тема 9. NP-полные проблемы из различных разделов математики.

Тема 10. Алгоритмически неразрешимые проблемы в области защиты информации.
Дискреционная политика управления доступом - неразрешимый и разрешимые варианты.

Тема 11. Сложностная классификация языков. Классы TIME(f(n)) и SPACE(f(n)).
Классы TIME(n^k), P-TIME и TIME(2^n).
Сложностные иерархии.
Элементарные и неэлементарные задачи (языки).
Сложность разрешимости элементарной теории поля действительных чисел и арифметики Пресбургера.

Тема 12. Сложность описания нормального алгоритма А.А. Маркова.

Тема 13. Теория алгоритмов и задачи использования ЭВМ. Вычислительные возможности современных ЭВМ. Модель ЭВМ – машина произвольного доступа (МПД). МПД - вычислимые функции и их связь с частично рекурсивными функциями.

Тема 14. Сложность конечных объектов по А.Н.Колмогорову.

5. Образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

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

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения и информационных справочных систем (при необходимости).

В процессе осуществления образовательного процесса используются:

– для формирования текстов материалов для промежуточной и текущей аттестации – программы Microsoft Office, издательская система MikTex;

– для поиска учебной литературы библиотеки ЯрГУ – Автоматизированная библиотечная информационная система "БУКИ-NEXT" (АБИС "Буки-Next").

7. Перечень основной и дополнительной учебной литературы, необходимых для освоения дисциплины

а) основная литература

1. Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов. М.: Мир, 1983.
2. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи.М.: Мир, 1979.
3. Дурнев, В. Г., Материалы по дисциплине "Теория алгоритмов и сложность вычислений" : метод. указания / В. Г. Дурнев ; Яросл. гос. ун-т, Ярославль, ЯрГУ, 2010, 40с
4. Дурнев, В. Г., Элементы теории алгоритмов : учеб. пособие для вузов / В. Г. Дурнев ; Яросл. гос. ун-т, Ярославль, ЯрГУ, 2008, 247с
5. Дурнев, В. Г., Элементы теории множеств и математической логики : учеб. пособие для вузов / В. Г. Дурнев ; Яросл. гос. ун-т, Ярославль, ЯрГУ, 2009, 411с
6. Кормен, Т., Алгоритмы : построение и анализ : учеб. пособие / Т. Кормен, Ч. Лейзерсон, Р. Ривест, М., МЦНМО, 2001, 955с
7. Мальцев, А.И. Алгоритмы и рекурсивные функции / А.И. Мальцев. М.: Наука, 1986.
8. Марков, А.А., Нагорный Н.М. Теория алгорифмов / А.А. Марков, М.: Наука, 1984.
9. Глухов М.М. Задачи и упражнения по математической логике, дискретным функциям и теории алгоритмов: учеб. пособие для вузов / М. М. Глухов, О. А. Козлитин, В. А. Шапошников, А. Б. Шишков. СПб., Лань, 2008, 111 с.
10. Лавров И.А. Задачи по теории множеств, математической логики и теории алгоритмов / И.А. Лавров, Л.Л. Максимова. М.: Наука. 1984. 287 с.

б) дополнительная литература

1. Адян С.И. Алгоритмическая неразрешимость проблем распознавания некоторых свойств групп // Докл. АН СССР. 1955. Т. 103. С.533-535.
2. Адян С.И., Дурнев В.Г. Алгоритмические проблемы для групп и полугрупп //Успехи матем. наук. 2000. Том 55.С.3-94.
3. Булос Дж., Джеффри Р. Вычислимость и логика. М.: Мир, 1994.
4. Дурнев В.Г. О позитивных формулах на свободных полугруппах //Сиб. матем. журн. 1974. Т. 25. С.1131-1137.
5. Дурнев В.Г. Неразрешимость позитивной $\forall\exists^3$-теории свободной полугруппы //Сиб. матем. журн. 1995. Т. 36. С.1067-1080.
6. Дурнев В.Г. Об уравнениях на свободных полугруппах и группах //Матем. заметки. 1974. Т. 16. С.717-724.

7. Катленд Н. Вычислимость. Введение в теорию рекурсивных функций. М.: Мир, 1983.
8. Колмогоров А.Н., Успенский В.А. К определению понятия алгоритма //Успехи мат. наук. 1958. Т. 13. Вып. 4. С.3-28.
9. Маканин Г.С. К проблеме тождества в конечно-определенных полугруппах //Докл. АН СССР. 1966. Т. 171. С.285-287.
10. Маканин Г.С. Проблема разрешимости уравнений в свободной полугруппе //Мат. сб. 1977. Т. 103(145). С.147-236.
11. Манин Ю.И. Вычислимое и невычислимое. М.: Советское радио, 1979.
12. Марков А.А. Невозможность некоторых алгоритмов в теории ассоциативных систем // ДАН СССР. 1947. Том55. С.587-590.
13. Марков А.А. Неразрешимость проблемы гомеоморфии //Докл. АН СССР. 1958. Т. 121. С.218-220.
14. Марков А.А. К проблеме представимости матриц //Z. Math. Log. und Grundl. Math. 1958. Т. 4. С.157-168.
15. Марченков С.С. Неразрешимость позитивной $\forall\exists$ - теории свободной полугруппы //Сиб. мат. журн. 1982. Т. 32. С.196-198.
16. Матиясевич Ю.В. Простые примеры неразрешимых ассоциативных исчислений //Докл. АН СССР. 1967. Т. 173. С.1264-1266.
17. Матиясевич Ю.В. Диофантовость перечислимых множеств //Докл. АН СССР. 1970. Т. 130. С.495-498.
18. Мендельсон Э. Введение в математическую логику. М.: Наука, 1976.
19. Новиков П.С. Об алгоритмической неразрешимости проблемы тождества теории групп //Докл. АН СССР. 1952. Т. 85. С.709-712.
20. Семенов А.Л. Интерпретация свободных алгебр в свободных группах //ДАН СССР. 1980. Том252. С.1326-1332.
21. Трахтенброт Б.А. Алгоритмы и вычислительные автоматы. М.: Советское радио, 1974.
22. Цейтин Г.С. Относительно проблемы распознавания свойств ассоциативных исчислений //Докл. АН СССР. 1956. Т. 107. С.209-212.
23. Цейтин Г.С. Ассоциативное исчисление с неразрешимой проблемой эквивалентности //Труды матем. ин-та. АН СССР. 1958. Т. 52. С.172-189.
24. Эббинхауз Г.Д., Якобс К., Ман Ф.К., Хермес Г. Машины Тьюринга и рекурсивные функции. М.: Мир, 1972.
25. Churh A. An unsolvable problem of elementary number theory //Amer. J. Math. 1936. Vol.58. P.345-363.
26. Churh A. A note on the Entscheidungsproblem // J. SymbolicLogic. 1936. Vol.1. P.40-41.
27. Dehn M. Uber unendliche diskontinuerliche Gruppen //Math.Ann. 1911. Bd. 71. S.116-144.
28. Post, E. Intoduction to a general theory of elementary propositions //Amer. J. Math. 1921. Vol.43.P.163-185.
29. Post E.L. Finite combinatory processes - formulation 1 //Journal of Symbolic Logic. 1936. Vol.1. P.103-105.
30. Post E.L. A variant of a recursively unsolvable problem //Bull. Amer. Math. Soc. 1946. Vol.52. P.264-268.
31. Post E.L. Recursive unsolvability of a problem of Thue //J. Symbol Log. 1947. Vol.12. P.1-11.
32. Rado T. On non-computable functions //Bell System Technical Journal. 1962. P.877-884.
33. Quine W. Concatenation as a basis for arithmetic //J. Symbol Log. 1946. Vol.11. P.105-114.

34. 36 Hall M.Jr. The word problem for semi-groups with two generators //J. Symbolic Logic, 1949. V. 14. P.115-118.
35. A.Thue. Problem uder Veranderungen von Zeichenreihen nach gegebehen Regeln //Vid. Skr. Math.-natur. KI. 1914.
36. Tietze H. \"Uber topologischen Invarianten mehrdimensionaler Mannigfaltigkeiten //Monatsh. Math. Phys. 1908. Vol.19. P.1-118.
37. Turing A.M. On computable numbers, with an application to the Entscheidugsproblem //Proceedings of London Mathematical Society. Ser. 2. 1936. Vol.42. P.230-265.
38. Scott D. A short recursively unsolvable problem (abstract) //J. Symbol. Log. 1956. Vol. 21. P.11-112.

в) ресурсы сети «Интернет»

1.Электронные каталоги НБ ЯрГУ

(http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php) содержат библиографические записи всех видов документов, составляющих фонд библиотеки, на русском и иностранных языках.

2. Личный кабинет (http://lib.uniyar.ac.ru/opac/bk_login.php) возможность получения on-line доступа к списку выданной в автоматизированном режиме литературы, просмотра и копирования электронных версий изданий сотрудников университета (учеб. и метод. пособия, тексты лекций и т.д.) Для работы в «Личном кабинете» необходимо зайти на сайт Научной библиотеки ЯрГУ с любой точки, имеющей доступ в Internet, в пункт меню *«Электронный каталог»*; пройти процедуру авторизации, выбрав вкладку *«Авторизация»*, и заполнить представленные поля информации.

3.Электронная библиотека учебных материалов ЯрГУ

(http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php) содержит более 2500 полных текстов учебных и учебно-методических материалов по основным изучаемым дисциплинам, изданных в университете. Доступ в сети университета, либо по логину/паролю.

4.Электронный архив ЯрГУ

(http://elar.uniyar.ac.ru/jspui/community-list**)** представляет собой коллекцию полнотекстовых электронных публикаций в области научных исследований. База данных предназначена для использования в учебных и научных целях, облегчая доступ к информации о научных работах и их содержанию.

5. Электронная картотека «Книгообеспеченность»

(http://www.lib.uniyar.ac.ru/opac/bk_bookreq_find.php**)**

раскрывает учебный фонд научной библиотеки ЯрГУ, предоставляет оперативную информацию о состоянии книгообеспеченности дисциплин основной и дополнительной литературой, а также цикла дисциплин и специальностей. Электронная картотека «Книгообеспеченность» доступна в сети университета и через Личный кабинет.

Русскоязычные электронные ресурсы (внешние)

1. Научная электронная библиотека (НЭБ) (http://elibrary.ru) – это крупнейший российский информационный портал, содержащий рефераты и полные тексты более 12 млн. научных статей и публикаций. **ЯрГУ выписывает в электронном виде 66 журналов,** более 2 500 наименований журналов на английском и русском языках находятся в свободном доступе. Для работы с полными текстами необходимо зарегистрироваться. Доступ к полным текстам журналов в сети университета.

2. Электронная библиотека диссертаций Российской государственной библиотеки (http://diss.rsl.ru) содержит более 580 000 полных текстов диссертаций и авторефератов. Доступ осуществляется в сети университета.

8. 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 практических занятий (семинаров); групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации;
-помещения для самостоятельной работы;
-помещения для хранения и профилактического обслуживания оборудования.

Специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления информации большой аудитории.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

Число посадочных мест в аудитории для практических занятий (семинаров) больше либо равно списочному составу группы обучающихся.

Автор(ы) :

Зав. кафедрой компьютерной безопасности и математических методов обработки информации, д.ф.-м.н. Дурнев В.Г.

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

Оценочные средства
для проведения текущей и/или промежуточной аттестации аспирантов
по дисциплине

1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Раздел "Теория алгоритмов"

Домашние задания по теме № 2 "**Машины Тьюринга.**"

Задания для самостоятельного решения № 1 - 12 из параграфа 2 части III сборника задач Лавров И.А. Задачи по теории множеств, математической логики и теории алгоритмов / И.А. Лавров, Л.Л. Максимова. М.: Наука. 1984. 287 с.

Домашние задания по теме № 3 "**Частично рекурсивные, рекурсивные и примитивно рекурсивные функции.**"

Задания для самостоятельного решения № 1 - 15 из параграфа 1 части III сборника задач Лавров И.А. Задачи по теории множеств, математической логики и теории алгоритмов / И.А. Лавров, Л.Л. Максимова. М.: Наука. 1984. 287 с.

Домашние задания по теме № 4 "**Примитивно рекурсивные и рекурсивные предикаты, отношения и множества, операции над ними.**"

Задания для самостоятельного решения № 16 - 30 из параграфа 1 части III сборника задач Лавров И.А. Задачи по теории множеств, математической логики и теории алгоритмов / И.А. Лавров, Л.Л. Максимова. М.: Наука. 1984. 287 с.

Домашние задания по теме № 5 "**Задание функций и предикатов.**"

Задания для самостоятельного решения № 31 - 44 из параграфа 1 части III сборника задач Лавров И.А. Задачи по теории множеств, математической логики и теории алгоритмов / И.А. Лавров, Л.Л. Максимова. М.: Наука. 1984. 287 с

Домашние задания по теме № 6 "**Нумерация.**"

Задания для самостоятельного решения № 31 - 44 из параграфа 1 части III сборника задач Лавров И.А. Задачи по теории множеств, математической логики и теории алгоритмов / И.А. Лавров, Л.Л. Максимова. М.: Наука. 1984. 287 с

Домашние задания по теме № 7 "**Множества, отношения и предикаты.**"

Задания для самостоятельного решения № 16 - 30 из параграфа 1 части III сборника задач Лавров И.А. Задачи по теории множеств, математической логики и теории алгоритмов / И.А. Лавров, Л.Л. Максимова. М.: Наука. 1984. 287 с.

Домашние задания по теме № 8 "**Машины Тьюринга.**"

Задания для самостоятельного решения № 13 - 25 из параграфа 2 части III сборника задач Лавров И.А. Задачи по теории множеств, математической логики и теории алгоритмов / И.А. Лавров, Л.Л. Максимова. М.: Наука. 1984. 287 с.

Домашние задания по теме № 12 "**Алгоритмическая неразрешимость**"

Задания для самостоятельного решения № 1 - 48 из параграфа 3 части III сборника задач Лавров И.А. Задачи по теории множеств, математической логики и теории алгоритмов / И.А. Лавров, Л.Л. Максимова. М.: Наука. 1984. 287 с.

Домашние задания по теме № 14 **"Нумерация Клини частично рекурсивных функций"** и по теме № 15 "**Нумерация Поста рекурсивно перечислимых множеств.** "

Задания для самостоятельного решения № 1 - 43 из параграфа 4 части III сборника задач Лавров И.А. Задачи по теории множеств, математической логики и теории алгоритмов / И.А. Лавров, Л.Л. Максимова. М.: Наука. 1984. 287 с.

Контрольная работа

Задания для контрольной работы по теме № 9 **"Вычислимость функций"**

1) Доказать примитивную рекурсивность теоретико-числовой функции.

2) Написать программу для машины Тьюринга, вычисляющей заданную функцию.

3) Написать программу для машины Тьюринга, решающей проблему вхождения в заданный язык.

4) Как связаны между собой вычислимость, вычислимость по Тьюрингу и частичная рекурсивность?

Примечание. Каждый вариант задания определяется выбором конкретной теоретико-числовой функции и языка.

Раздел "Сложность вычислений"

Домашние задания по теме № 2 **"Детерминированные многоленточные машины Тьюринга."**

Задания для самостоятельного решения № 1 - 8 из параграфа 2 части III сборника задач Лавров И.А. Задачи по теории множеств, математической логики и теории алгоритмов / И.А. Лавров, Л.Л. Максимова. М.: Наука. 1984. 287 с.

Домашние задания по теме № 3 "**Сложность алгоритмов и вычислений"**

Задания для самостоятельного решения № 16.1 - 16.12 из параграфа 16 главы 3 сборника задач Глухов М.М. Задачи и упражнения по математической логике, дискретным функциям и теории алгоритмов: учеб. пособие для вузов / М. М. Глухов, О. А. Козлитин, В. А. Шапошников, А. Б. Шишков. СПб., Лань, 2008, 111 с.

Домашние задания по теме № 4 **"Недетерминированные многоленточные машины Тьюринга."**

Задания для самостоятельного решения № 9 - 25 из параграфа 2 части III сборника задач Лавров И.А. Задачи по теории множеств, математической логики и теории алгоритмов / И.А. Лавров, Л.Л. Максимова. М.: Наука. 1984. 287 с.

Домашние задания по теме № 5 **"Временная и емкостная меры сложности"**

Задания для самостоятельного решения № 16.13 - 16.25 из параграфа 16 главы 3 сборника задач Глухов М.М. Задачи и упражнения по математической логике, дискретным функциям и теории алгоритмов: учеб. пособие для вузов / М. М. Глухов, О. А. Козлитин, В. А. Шапошников, А. Б. Шишков. СПб., Лань, 2008, 111 с.

Домашние задания по теме № 8 **"Алгоритмические модели. Элементы теории алгоритмов"**

Задания для самостоятельного решения № 1 - 44 из параграфа 1 части III сборника задач Лавров И.А. Задачи по теории множеств, математической логики и теории алгоритмов / И.А. Лавров, Л.Л. Максимова. М.: Наука. 1984. 287 с.

Задания для самостоятельного решения № 1 - 25 из параграфа 2 части III сборника задач Лавров И.А. Задачи по теории множеств, математической логики и теории алгоритмов / И.А. Лавров, Л.Л. Максимова. М.: Наука. 1984. 287 с.

Задания для самостоятельного решения № 15.1 - 15.19 из параграфа 15 главы 3 сборника задач Глухов М.М. Задачи и упражнения по математической логике, дискретным функциям и теории алгоритмов: учеб. пособие для вузов / М. М. Глухов, О. А. Козлитин, В. А. Шапошников, А. Б. Шишков. СПб., Лань, 2008, 111 с.

Домашние задания по теме № 11 **" Алгоритмически неразрешимые проблемы в области защиты информации. "**

Задания для самостоятельного решения № 1 - 48 из параграфа 3 части III сборника задач Лавров И.А. Задачи по теории множеств, математической логики и теории алгоритмов / И.А. Лавров, Л.Л. Максимова. М.: Наука. 1984. 287 с.

Задания для самостоятельного решения № 1 - 43 из параграфа 4 части III сборника задач Лавров И.А. Задачи по теории множеств, математической логики и теории алгоритмов / И.А. Лавров, Л.Л. Максимова. М.: Наука. 1984. 287 с.

Домашние задания по теме № 12 **" Сложность алгоритмов и вычислений"**

Задания для самостоятельного решения № 16.1 - 16.26 из параграфа 16 главы 3 сборника задач Глухов М.М. Задачи и упражнения по математической логике, дискретным функциям и теории алгоритмов: учеб. пособие для вузов / М. М. Глухов, О. А. Козлитин, В. А. Шапошников, А. Б. Шишков. СПб., Лань, 2008, 111 с.

Домашние задания по теме № 12 **"Сложностная классификация переборных задач "**

Задания для самостоятельного решения № 16.1 - 16.26 из параграфа 16 главы 3 сборника задач Глухов М.М. Задачи и упражнения по математической логике, дискретным функциям и теории алгоритмов: учеб. пособие для вузов / М. М. Глухов, О. А. Козлитин, В. А. Шапошников, А. Б. Шишков. СПб., Лань, 2008, 111 с.

Контрольная работа

Задания для контрольной работы по теме № 10 **"NP-полные проблемы"**

1) Основные идеи доказательства **NP-полноты** проблемы функциональной полноты для конечных систем булевых функций.

2) Доказать со**NP-полноту** проблемы вхождения в класс монотонных (самодвойственных, линейных) булевых функций.

3) Построить цепочку полиномиальных сводимостей различных проблем.

Примечание. Каждый вариант задания определяется выбором конкретной системы булевых функций и конкретного класса булевых функций.

1.1 Список вопросов и (или) заданий для проведения промежуточной аттестации

Вопросы к зачету по дисциплине
"Теория алгоритмов и сложность вычислений"
(2 семестр)

Раздел «Теория алгоритмов»

1. Алгоритмы в интуитивном смысле. Примеры алгоритмов из различных разделов математики: алгебры, теории чисел, математической логики, математического анализа, теории обыкновенных дифференциальных уравнений и т. д.

2. Основные свойства алгоритмов. Дискретность, детерминированность, элементарность шагов и массовость алгоритмов.

3. Необходимость математического уточнения интуитивного понятия алгоритма, примеры математических проблем, сформулированных в конце XIX -- начале XX в.в., приведших к уточнению понятия алгоритма.

4. Неразрешимые алгоритмические пробелы в теории алгоритмов, алгебре, математичекой логике, теории чисел, математическом анализе, топологии.

5. Машина Тьюринга. Внешний и внутренний алфавиты, команды и программа машины Тьюринга. Различные варианты машин Тьюринга: многоленточные и одноленточные, с одномерной и многомерной лентой, с потенциально бесконечной в обе стороны лентой, с непродолжаемой влево лентой и т. д.

6. Словарные алгоритмы, реализуемые машинами Тьюринга.

7. Вычислимые по Тьюрингу функции. Правильная вычислимость по Тьюрингу.

8. Вычислимость по Тьюрингу элементарных теоретико-числовых функций. Разрешимые и перечислимые множества слов.

9. Операции над машинами Тьюринга. Композиция машин Тьюринга. Разветвление. Диаграммы машин Тьюринга. Циклический сдвиг, копирование.

10. Тезис Тьюринга. Замкнутость класса правильно вычислимых по Тьюрингу функций относительно операций суперпозиции, примитивной рекурсии и минимизации.

11. Примитивно рекурсивные, частично рекурсивные и рекурсивные функции. Простейшие (исходные) функции. Операции суперпозиции, примитивной рекурсии и минимизации.

12. Примитивно рекурсивные функции. Примеры примитивно рекурсивных теоретико-числовых функций.

13. Частично рекурсивные и рекурсивные функции, примеры. Операции над примитивными, рекурсивными и частично рекурсивными функциями.
Тезис А. Черча.

14. Нумерация пар и n-ок натуральных чисел. Нумерационные функции.
15. Рекурсивные и рекурсивно перечислимые множества и предикаты.
16. Теорема Э. Поста.

17. Теорема о графике функции.

18. Правильная вычислимость по Тьюрингу любой частично рекурсивной функции.

19. Арифметизация теории машин Тьюринга.

20. Частичная рекурсивность любой вычислимой по Тьюрингу функции.

Раздел "Сложность вычислений"

1. Детерминированные многоленточные машины Тьюринга.
Внешний и внутренний алфавиты k-ленточной детерминированной машины Тьюринга. Программа и команды. Конфигурации. Описание выполнения команд в терминах преобразования конфигураций. Языки, принимаемые (допускаемые, распознаваемые) k-ленточными детерминированными машинами Тьюринга.

2. Сложность алгоритмов и вычислений. 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.

3. Недетерминированные многоленточные машины Тьюринга.
Внешний и внутренний алфавиты k-ленточной недетерминированной машины Тьюринга. Программа и команды недетерминированной машины Тьюринга. Их особенность. Конфигурации. Описание выполнения команд в терминах преобразования конфигураций. Языки, принимаемые (допускаемые) недетерминированными k-ленточными машинами Тьюринга.

4. 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).

5. Свойства функций сложности**.**
Нижние оценки. Сложность распознавания функциональной полноты системы булевых функций, сложность проблем вхождения в классы самодвойственных, монотонных и линейных функций. Существование сколь угодно сложно вычислимых функций.

6. Сложность проблемы разрешимости систем линейных уравнений.
Решение систем целочисленных линейных уравнений в целых, натуральных и 0-1 числах.

7. **NP-полные** проблемы для уравнений в свободных полугруппах и для регулярных языков.

8. **NP-полные** проблемы в теории графов.

9. **NP-полные** проблемы из различных разделов математики.

10. Алгоритмически неразрешимые проблемы в области защиты информации.
Дискреционная политика управления доступом - неразрешимый и разрешимые варианты.

11. Сложность описания нормального алгоритма А.А. Маркова.

12. Теория алгоритмов и задачи использования ЭВМ. Вычислительные возможности современных ЭВМ. Модель ЭВМ – машина произвольного доступа (МПД). МПД - вычислимые функции и их связь с частично рекурсивными функциями.

13. Сложность конечных объектов по А.Н.Колмогорову.

Приложение № 2 к рабочей программе дисциплины
«Теория алгоритмов и сложность вычислений»

Методические указания для аспирантов по освоению дисциплины

Для успешного освоения дисциплины важно самостоятельное изучение теоретического материала, решение достаточно большого набора хорошо подобранных задач, как в аудитории, так и самостоятельно в качестве домашних заданий. Примеры решения задач разбираются на практических занятиях, при необходимости по наиболее трудным темам проводятся дополнительные консультации. Основная цель решения задач – помочь усвоить фундаментальные понятия, методы и теоремы теории алгоритмов, научиться определять сложность вычислений. Для решения задач необходимо не только знать, но и понимать теоретический материал. Поэтому в процессе изучения дисциплины рекомендуется регулярная работа с рекомендованной литературой.

Большое внимание должно быть уделено выполнению домашней работы. В качестве заданий для самостоятельной работы дома аспирантам предлагаются задачи, аналогичные разобранным на практических занятиях или более сложные, которые являются результатом объединения нескольких базовых задач.

Для проверки и контроля усвоения теоретического материала, приобретенных практических навыков работы с основными понятиями в течение обучения проводятся мероприятия текущей аттестации в виде устного опроса на занятиях и консультациях и разбору некоторых заданий для самостоятельной работы.

Аспиранты сдают зачет во втором семестре. Зачет проводится на основании выполнения домашних заданий, контрольной работы и собеседования на основании списка вопросов к зачету, который охватывает полностью всю программу дисциплины.

Учебно-методическое обеспечение самостоятельной работы аспирантов по дисциплине

В качестве учебно-методического обеспечения рекомендуется использовать литературу, указанную в разделе № 7 данной рабочей программы.