

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

Сложность вычислений

Направление подготовки (специальности)
10.04.01 Информационная безопасность

Направленность (профиль)
«Управление информационной безопасностью»

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 "Сложность вычислений" обеспечивает приобретение фундаментальных знаний и умений в соответствии с Федеральным государственным образовательным стандартом направления "10.04.01-Информационная безопасность" (уровень магистратуры), 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 "Сложность вычислений" относится к части образовательной программы, формируемой участниками образовательных отношений. Она играет исключительно важную роль для общематематической и общепрофессиональной подготовки специалиста. При ее изучении существенно используются знания, полученные при изучении математических дисциплин "Алгебра", "Теория чисел", "Дискретная математика", "Информатика", "Математическая логика и теория алгоритмов" и "Теория алгоритмов". Знания, умения и навыки, полученные при изучении дисциплины "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 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
Универсальные компетенции		
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	И-УК-1.7 Знает методы и современные средства и технологии поиска информации; методы и способы фильтрации, критического анализа И-УК-1.8 Умеет анализировать задачу применять методы и современные средства поиска информации; И-УК-1.6 Владеет навыками поиска	Знать: - методы и современные средства и технологии поиска информации; - методы и способы фильтрации, критического анализа Уметь: - анализировать задачу; - применять методы и современные средства поиска информации; Владеть: навыками поиска информации с использованием современных средств и технологий

	информации с использованием современных средств и технологий	
Профессиональные компетенции		
ПК-1 Способен разрабатывать математические модели систем обеспечения информационной безопасности, математически доказывать их соответствие выбранным политикам безопасности	И-ПК-1.10 Знает различные подходы к определению понятия алгоритма, методы доказательства алгоритмической неразрешимости и методы построения эффективных алгоритмов И-ПК-1.11 Умеет оценивать сложность алгоритмов и вычислений	Знать: определение детерминированной и недетерминированной k-ленточной машины Тьюринга: внешний и внутренний алфавиты, команды и программа, конфигурация, описание выполнения команд в терминах преобразования конфигураций, языки, принимаемые (допускаемые, распознаваемые) k-ленточными детерминированными и недетерминированными машинами Тьюринга, подходы к оценкам сложности алгоритмов и вычислений, временная и емкостная меры сложности (детерминированный и недетерминированный случаи), полиномиально ограниченные машины Тьюринга, классы языков P-TIME и P-SPACE , NP-TIME , пример языка, не входящего в класс P-TIME , проблема NP = P? Полиномиальная сводимость, NP-полнота проблемы распознавания выполнимости для булевых функций (The satisfiability problem for boolean functions, SAT-problem, SAT), сложность проблемы распознавания функциональной полноты системы булевых функций, сложность проблем вхождения в классы самодвойственных, монотонных и линейных функций, проблемы распознавания и проблемы вхождения в языки, NP-трудные и NP-полные языки (задачи, проблемы), NP-полные проблемы из различных разделов математики, сложностная классификация языков: классы TIME(f(n)) и SPACE(f(n)) , классы TIME(n^k) , P-TIME и TIME(2ⁿ) , сложностные иерархии, элементарные и неэлементарные задачи (языки), сложность разрешимости элементарной теории поля действительных чисел и арифметики Пресбургера, теорема Рабина-Фишера, алгоритмически неразрешимые проблемы в области защиты информации, дискреционная политика управления доступом, модель HRU - неразрешимый и разрешимые варианты, нормальные алгорифмы А.А.Маркова, сложность его описания как мера сложности алгоритма, РАМ-машины (МПД) . Уметь:

		разрабатывать алгоритмы и оценивать сложность его реализации и сложной решаемой задачи.
ПК-2 Способен анализировать математические модели систем обеспечения информационной безопасности, а также проводить тестирование средств защиты информации на соответствие этим моделям	И-ПК-2.12 Владеет навыками применения методов и фактов теории алгоритмов для разработки алгоритмов И-ПК-2.13 Умеет оценивать сложность алгоритмов и вычислений	Владеть навыками: оценки временной и емкостной сложности алгоритмов, получения верхних оценок Уметь: разрабатывать алгоритмы и оценивать сложность его реализации и сложной решаемой задачи.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет **3** зачетных единицы, **108** 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						
			лекции	практические	лабораторные	консультации	аттестационные испытания		
1	Вводная лекция	2	1					2	Устный опрос
2	Детерминированные многоленточные машины Тьюринга	2	2	1		1		4	Задания для самостоятельной (домашней) работы Устный опрос
3	Сложность алгоритмов и вычислений.	2	2	1		1		4	Задания для самостоятельной (домашней) работы Устный опрос
4	Недетерминированные многоленточные машины Тьюринга.	2	2	1				4	Задания для самостоятельной (домашней) работы Устный опрос
5	Временная и емкостная меры сложности	2	2	2		1		4	Задания для самостоятельной (домашней) работы Устный опрос
6	Свойства функций сложности	2	2	2		1		4	Задания для самостоятельной (домашней) работы

									Устный опрос
7	Сложность проблемы разрешимости систем линейных уравнений	2	2	1		1		4	Задания для самостоятельной (домашней) работы Устный опрос
8	NP-полные проблемы для уравнений в свободных полугруппах и для регулярных языков.	2	2					2	Устный опрос
9	NP-полные проблемы в теории графов.	2	2	1				2	Устный опрос
10	NP-полные проблемы из различных разделов математики.	2	2	1		1		4	Контрольная работа
11	Алгоритмически неразрешимые проблемы в области защиты информации	2	2	1				2	Устный опрос
12	Сложностная классификация языков	2	2	2		1		4	Задания для самостоятельной (домашней) работы Устный опрос
13	Сложность описания нормального алгорифма А.А.Маркова	2	3	1				2	Устный опрос
14	Теория алгоритмов и задачи использования компьютеров	2	3	1		1		2	Устный опрос
15	Сложность конечных объектов по А.Н.Колмогорову	2	3	1				2	Устный опрос
							0,3	5,7	зачет
	Всего		32	16		8	0,3	51,7	

Содержание разделов дисциплины:

Тема 1. Вводная лекция.

История развития теории алгоритмов. Теория алгоритмов и принципиальные возможности вычислительных машин. Оценка сложности алгоритмов и ее значение для практики.

Тема 2. 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 3. 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 4. 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 5. Временная и емкостная меры сложности (недетерминированный случай).

Класс языков **NP-TIME**. Проблема **NP = P?**

Полиномиальная сводимость.

Сложность (**NP-полнота**) проблемы распознавания выполнимости для булевых функций (The satisfiability problem for boolean functions, SAT-problem, SAT). Сложность проблемы распознавания функциональной полноты системы булевых функций, сложность проблем вхождения в классы самодвойственных, монотонных и линейных функций. Проблемы распознавания и проблемы вхождения в языки.

NP-трудные и **NP-полные** языки (задачи, проблемы).

Тема 6. Свойства функций сложности.

Нижние оценки. Сложность разрешимости арифметики Пресбургера и элементарной теории поля действительных чисел. Теорема Рабина - Фишера.

Существование сколь угодно сложно вычислимых функций.

Тема 7. Сложность проблемы разрешимости систем линейных уравнений.

Решение систем целочисленных линейных уравнений в целых, натуральных и 0-1 числах.

Тема 8. NP-полные проблемы для уравнений в свободных полугруппах и для регулярных языков.

Тема 9. NP-полные проблемы в теории графов.

Тема 10. NP-полные проблемы из различных разделов математики.

Тема 11. Алгоритмически неразрешимые проблемы в области защиты информации.

Дискреционная политика управления доступом - неразрешимый и разрешимые варианты. Модель HRU.

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

Тема 13. Теория алгоритмов и задачи использования компьютеров.

Вычислительные возможности современных компьютеров. Математическая модель компьютера – машина произвольного доступа (МПД). RAM-A machine with random access to memory. МПД - вычислимые функции и их связь с частично рекурсивными функциями.

Тема 14. 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;
- MikTeX (свободно распространяемое ПО).

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>

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

а) основная литература

1. М. М. Глухов, А. Б. Шишков Математическая логика. Дискретные функции. Теория алгоритмов: учебное пособие — Санкт-Петербург: Лань, 2021.
<https://matematika76.ru/fm/глухов.pdf>
2. М. М. Глухов, О. А. Козлитин, В. А. Шапошников, А. Б. Шишков Задачи и упражнения по математической логике, дискретным функциям и теории алгоритмов: учебное пособие — Санкт-Петербург: Лань, 2021.
<https://reader.lanbook.com/book/167678>

3. Дурнев В. Г. Элементы теории алгоритмов: учеб. пособие для вузов - Ярославль, ЯрГУ, 2008 <http://www.lib.uniyar.ac.ru/edocs/iuni/20080230.pdf>
4. С. В. Судоплатов, Е. В. Овчинникова Математическая логика и теория алгоритмов: учебник и практикум для вузов — Москва: Издательство Юрайт, 2022. <https://urait.ru/viewer/matematicheskaya-logika-i-teoriya-algoritmov-447321>

б) дополнительная литература

1. Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов. - М.: Мир, 1979.
2. М. О. Асанов, В. А. Баранский, В. В. Расин Дискретная математика: графы, матроиды, алгоритмы: учебное пособие — Санкт-Петербург: Лань, 2010 <https://reader.lanbook.com/book/536>
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>
4. Дурнев В. Г., Элементы теории множеств и математической логики: учеб. пособие для вузов - Ярославль, ЯрГУ, 2009 <http://www.lib.uniyar.ac.ru/edocs/iuni/20090231.pdf>
5. М. Гэри, Д. Джонсон Вычислительные машины и труднорешаемые задачи. - М.: Мир, 1979
6. И. А. Лавров, Л. Л. Максимова Задачи по теории множеств, математической логики и теории алгоритмов - М.: Физматлит. 2006. <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 и 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 в электронную информационно-образовательную среду организации.

Автор(ы):

Профессор, доктор физ.-матем. наук

Дурнев В.Г.

**Приложение №1 к рабочей программе дисциплины
«Сложность вычислений»**

**Фонд оценочных средств
для проведения текущей и промежуточной аттестации студентов
по дисциплине**

**1. Типовые контрольные задания или иные материалы,
используемые в процессе текущей аттестации**

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 **"Нетерминированные 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 **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.

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

Вопросы к зачету по дисциплине "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.

Сложность (**NP-полнота**) проблемы распознавания выполнимости для булевых функций (The satisfiability problem for boolean functions, SAT-problem, SAT). Сложность проблемы распознавания функциональной полноты системы булевых функций, сложность проблем вхождения в классы самодвойственных, монотонных и линейных функций. Проблемы распознавания и проблемы вхождения в языки.

NP-трудные и **NP-полные** языки (задачи, проблемы).

5. Свойства функций сложности.

Нижние оценки. Сложность разрешимости арифметики Пресбургера и элементарной теории поля действительных чисел. Теорема Рабина - Фишера.

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. Модель HRU.

11. Сложность описания нормального алгорифма А.А.Маркова.

12. Теория алгоритмов и задачи использования компьютеров. Вычислительные возможности современных компьютеров. Математическая модель компьютера – машина произвольного доступа (МПД). RAM-A machine with random access to memory. МПД - вычислимые функции и их связь с частично рекурсивными функциями.

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

3. Перечень компетенций, этапы их формирования, описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкалы оценивания

3.1 Шкала оценивания сформированности компетенций и ее описание

Оценивание уровня сформированности компетенций в процессе освоения дисциплины осуществляется по следующей трехуровневой шкале:

Пороговый уровень - предполагает отражение тех ожидаемых результатов, которые определяют минимальный набор знаний и (или) умений и (или) навыков, полученных студентом в результате освоения дисциплины. Пороговый уровень является обязательным уровнем для студента к моменту завершения им освоения данной дисциплины.

Продвинутый уровень - предполагает способность студента использовать знания, умения, навыки и (или) опыт деятельности, полученные при освоении дисциплины, для решения профессиональных задач. Продвинутый уровень превосходит пороговый уровень по нескольким существенным признакам.

Высокий уровень - предполагает способность студента использовать потенциал интегрированных знаний, умений, навыков и (или) опыта деятельности, полученных при освоении дисциплины, для творческого решения профессиональных задач и самостоятельного поиска новых подходов в их решении путем комбинирования и использования известных способов решения применительно к конкретным условиям. Высокий уровень превосходит пороговый уровень по всем существенным признакам.

**3.2 Перечень компетенций, этапы их формирования,
описание показателей и критериев оценивания компетенций
на различных этапах их формирования**

Код компетенции	Форма контроля	Этапы формирования (№ темы (раздела))	Показатели оценивания	Шкала и критерии оценивания компетенций на различных этапах их формирования		
				Пороговый уровень	Продвинутый уровень	Высокий уровень
Универсальные компетенции						
УК-1 Способность осуществлять критический анализ проблемных ситуаций на основе системы	Зачет	1-4	И-УК-1.7: - знает методы и современные средства и технологии поиска информации; - знает методы и способы фильтрации, критического анализа И-УК-1.8: - умеет анализировать задачу; - умеет применять	Знать: методы и современные средства и технологии поиска информации; методы и способы фильтрации, критического анализа	Знать: методы и современные средства и технологии поиска информации; методы и способы фильтрации, критического анализа Уметь: анализировать задачу; применять методы и современные средства поиска информации;	Знать: методы и современные средства и технологии поиска информации; методы и способы фильтрации, критического анализа Уметь: анализировать задачу; применять методы и современные средства поиска информации; Владеть: навыками поиска информации с использованием современных средств и технологий;

много подхо да, выраб атыва ть strate гию дейст вий			методы и современные средства поиска информации; И-УК-1.6: - владеет навыками поиска информации с использованием современных средств и технологий;			
--	--	--	---	--	--	--

Профессиональные компетенции

ПК-1 Спосо бен разраб атыва ть матем атичес кие модел и систе	Зачет	2 – 8	И-ПК-1.10 знает различные подходы к определению понятия алгоритма, методы доказательства алгоритмической неразрешимости и методы	Знать: определение детерминиров анной и недетерминир ованной k- ленточной машины Тьюринга: внешний и внутренний алфавиты,	Знать: определение детерминированной и недетерминированной k-ленточной машины Тьюринга: внешний и внутренний алфавиты, команды и программа, конфигурация, описание выполнения команд в терминах преобразования конфигураций, языки,	Знать: определение детерминированной и недетерминированной k-ленточной машины Тьюринга: внешний и внутренний алфавиты, команды и программа, конфигурация, описание выполнения команд в терминах преобразования конфигураций, языки, принимаемые (допускаемые, распознаваемые) k-ленточными детерминированными и недетерминированными машинами Тьюринга, подходы к оценкам сложности алгоритмов и вычислений, временная и емкостная меры сложности (детерминированный и недетерминированный случаи), полиномиально
--	-------	-------	--	---	---	---

<p>м обесп ечени я инфор мацио нной безопа сност и, матем атичес ки доказ ывать их соотве тствие выбра нным полит икам безопа сност и</p>			<p>построения эффективных алгоритмов И-ПК-1.11 умеет оценивать сложность алгоритмов и вычислений</p>	<p>команды и программа, конфигурация, описание выполнения команд в терминах преобразовани я конфигураций , языки, принимаемые (допускаемые, распознаваем ые) k- ленточными детерминиров анными и недетерминир ованными машинами Тьюринга, подходы к оценкам сложности алгоритмов и вычислений, временная и емкостная меры сложности (детерминиров анный и</p>	<p>принимаемые (допускаемые, распознаваемые) k- ленточными детерминированными и недетерминированными машинами Тьюринга, подходы к оценкам сложности алгоритмов и вычислений, временная и емкостная меры сложности (детерминированный и недетерминированный случай), полиномиально ограниченные машины Тьюринга, классы языков P-TIME и P-SPACE, NP-TIME, пример языка, не входящего в класс P-TIME, проблема NP = P? Полиномиальная сводимость, NP-полнота проблемы распознавания выполнимости для булевых функций (The satisfiability problem for boolean functions, SAT- problem, SAT), сложность проблемы</p>	<p>ограниченные машины Тьюринга, классы языков P-TIME и P-SPACE, NP-TIME, пример языка, не входящего в класс P-TIME, проблема NP = P? Полиномиальная сводимость, NP-полнота проблемы распознавания выполнимости для булевых функций (The satisfiability problem for boolean functions, SAT-problem, SAT), сложность проблемы распознавания функциональной полноты системы булевых функций, сложность проблем вхождения в классы самодвойственных, монотонных и линейных функций, проблемы распознавания и проблемы вхождения в языки, NP-трудные и NP-полные языки (задачи, проблемы), NP-полные проблемы из различных разделов математики, сложностная классификация языков: классы TIME(f(n)) и SPACE(f(n)), классы TIME(n^k), P-TIME и TIME(2ⁿ), сложностные иерархии, элементарные и неэлементарные задачи (языки), сложность разрешимости элементарной теории поля действительных чисел и арифметики Пресбургера, теорема Рабина-Фишера, алгоритмически неразрешимые проблемы в области защиты информации, дискреционная политика управления доступом, модель HRU - неразрешимый и разрешимые варианты, нормальные алгоритмы А.А.Маркова, сложность его описания как мера сложности алгоритма, RAM-машины (МПД).</p> <p>Уметь: разрабатывать алгоритмы и оценивать сложность его реализации и сложной решаемой задачи, решать стандартные задачи по оценке сложности алгоритмов.</p>
---	--	--	--	---	--	---

			<p>недетерминированный случай), полиномиально ограниченные машины Тьюринга, классы языков P-TIME и P-SPACE, NP-TIME, пример языка, не входящего в класс P-TIME, проблема NP = P? Полиномиальная сводимость, NP-полнота проблемы распознавания выполнимости для булевых функций (The satisfiability problem for boolean functions, SAT-problem, SAT), сложность</p>	<p>распознавания функциональной полноты системы булевых функций, сложность проблем вхождения в классы самодвойственных, монотонных и линейных функций, проблемы распознавания и проблемы вхождения в языки, NP-трудные и NP-полные языки (задачи, проблемы), NP-полные проблемы из различных разделов математики, сложностная классификация языков: классы TIME(f(n)) и SPACE(f(n)), классы TIME(n^k), P-TIME и TIME(2ⁿ), сложностные иерархии, элементарные и неэлементарные задачи (языки), сложность разрешимости элементарной теории поля действительных чисел и арифметики Пресбургера, теорема</p>	
--	--	--	--	---	--

			<p>проблемы распознавания функциональной полноты системы булевых функций, сложность проблем вхождения в классы самодвойственных, монотонных и линейных функций, проблемы распознавания и проблемы вхождения в языки, NP-трудные и NP-полные языки (задачи, проблемы), NP-полные проблемы из различных разделов математики, сложностная классификация языков:</p>	<p>Рабина-Фишера, алгоритмически неразрешимые проблемы в области защиты информации, дискреционная политика управления доступом, модель HRU - неразрешимый и разрешимые варианты, нормальные алгоритмы А.А.Маркова, сложность его описания как мера сложности алгоритма, RAM-машины (МПД).</p> <p>Уметь: разрабатывать алгоритмы и оценивать сложность его реализации и сложной решаемой задачи, решать стандартные задачи по оценке сложности алгоритмов.</p>	
--	--	--	---	--	--

				<p> классы $\text{TIME}(f(n))$ и $\text{SPACE}(f(n))$, классы $\text{TIME}(n^k)$, P- TIME и $\text{TIME}(2^n)$, сложностные иерархии, элементарные и неэлементарн ые задачи (языки), сложность разрешимости элементарной теории поля действительн ых чисел и арифметики Пресбургера, теорема Рабина- Фишера, алгоритмическ и неразрешимые проблемы в области защиты информации, дискреционна </p>		
--	--	--	--	---	--	--

				я политика управления доступом, модель HRU - неразрешимы й и разрешимые варианты, нормальные алгорифмы А.А.Маркова, сложность его описания как мера сложности алгоритма, RAM-машины (МПД).		
ПК-2. Способ анализировать математические модели и системы обесп	Зачет	7-12	И_ПК-2.12 владеет навыками применения методов и фактов теории алгоритмов для разработки алгоритмов И-ПК-2.13 умеет оценивать сложность алгоритмов и	Уметь: разрабатывать алгоритмы и оценивать сложность его реализации и сложной решаемой задачи.	Уметь: разрабатывать алгоритмы и оценивать сложность его реализации и сложной решаемой задачи. Владеть навыками: оценки временной и емкостной сложности алгоритмов, получения верхних оценок	Уметь: разрабатывать алгоритмы и оценивать сложность его реализации и сложной решаемой задачи. Владеть навыками: оценки временной и емкостной сложности алгоритмов, получения верхних оценок

ечени я инфор мацио нной безопа сност и, а также прово дить тестир овани е средст в защит ы инфор мации на соотве тствие этим модел ям			вычислений			

Целью процедуры оценивания является определение степени овладения студентом ожидаемыми результатами обучения (знаниями, умениями, навыками и (или) опытом деятельности).

Процедура оценивания степени овладения студентом ожидаемыми результатами обучения осуществляется с помощью методических материалов, представленных в разделе «Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций»

3.3 Критерии оценивания степени овладения знаниями, умениями, навыками и (или) опытом деятельности, определяющие уровни сформированности компетенций

Пороговый уровень (общие характеристики):

- владение основным объемом знаний по программе дисциплины;
- знание основной терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы без существенных ошибок;
- владение инструментарием дисциплины, умение его использовать в решении стандартных (типовых) задач;
- способность самостоятельно применять типовые решения в рамках рабочей программы дисциплины;
- усвоение основной литературы, рекомендованной рабочей программой дисциплины;
- знание базовых теорий, концепций и направлений по изучаемой дисциплине;
- самостоятельная работа на практических и лабораторных занятиях, периодическое участие в групповых обсуждениях, достаточный уровень культуры исполнения заданий.

Продвинутый уровень (общие характеристики):

- достаточно полные и систематизированные знания в объеме программы дисциплины;
- использование основной терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать выводы;
- владение инструментарием дисциплины, умение его использовать в решении учебных и профессиональных задач;
- способность самостоятельно решать сложные задачи (проблемы) в рамках рабочей программы дисциплины;
- усвоение основной и дополнительной литературы, рекомендованной рабочей программой дисциплины;
- умение ориентироваться в базовых теориях, концепциях и направлениях по изучаемой дисциплине и давать им сравнительную оценку;
- самостоятельная работа на практических и лабораторных занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

Высокий уровень (общие характеристики):

- систематизированные, глубокие и полные знания по всем разделам дисциплины;
- точное использование терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы;
- безупречное владение инструментарием дисциплины, умение его использовать в постановке и решении научных и профессиональных задач;

- способность самостоятельно и творчески решать сложные задачи (проблемы) в рамках рабочей программы дисциплины;
- полное и глубокое усвоение основной и дополнительной литературы, рекомендованной рабочей программой дисциплины;
- умение ориентироваться в основных теориях, концепциях и направлениях по изучаемой дисциплине и давать им критическую оценку;
- активная самостоятельная работа на практических и лабораторных занятиях, творческое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

3.4 Описание процедуры выставления оценки

В зависимости от уровня сформированности каждой компетенции по окончании освоения дисциплины студенту выставляется оценка. Для дисциплин, изучаемых в течение нескольких семестров, оценка может выставляться не только по окончании ее освоения, но и в промежуточных семестрах. Вид оценки («отлично», «хорошо», «удовлетворительно», «неудовлетворительно», «зачтено», «незачтено») определяется рабочей программой дисциплины в соответствии с учебным планом.

Оценка «отлично» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована на высоком уровне.

Оценка «хорошо» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована не ниже, чем на продвинутом уровне.

Оценка «удовлетворительно» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована не ниже, чем на пороговом уровне.

Оценка «неудовлетворительно» выставляется студенту, у которого хотя бы одна компетенция (полностью или частично формируемая данной дисциплиной) сформирована ниже, чем на пороговом уровне.

Оценка «зачет» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована не ниже, чем на пороговом уровне.

Оценка «незачтено» выставляется студенту, у которого хотя бы одна компетенция (полностью или частично формируемая данной дисциплиной) сформирована ниже, чем на пороговом уровне.

Оценка ответа на экзамене

Экзаменационный ответ оценивается по 4-х бальной системе, в соответствие с которой выставляются оценки **«отлично»**, **«хорошо»**, **«удовлетворительно»**, **«неудовлетворительно»**.

Правила выставления оценки:

оценка **«отлично»** выставляется студенту, если он владеет материалом дисциплины; четко и определенно отвечает на вопросы, легко сравнивает различные части, сближает самые отдаленные точки учения, разбирает новые и сложные предлагаемые ему случаи, знает слабые стороны учения, места, где сомневается, и что можно возразить против теории.

оценка **«хорошо»** выставляется студенту, если он твердо знает и понимает материал, грамотно и по существу излагает его, не допускает существенных неточностей в ответе на поставленные вопросы, правильно

применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.

оценка **«удовлетворительно»** выставляется студенту, если он имеет знания основного материала, но не усвоил его деталей, знает дисциплину только в том виде, как она была ему преподана, но приходит в замешательство от соприкосновенных вопросов, предлагаемых на тот конец, чтобы он сблизил между собой отдаленнейшие точки; испытывает затруднения при выполнении практических работ.

оценка **«неудовлетворительно»** выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями и ошибками выполняет практические задания.

Оценка устного ответа на зачете

Устный ответ на зачете оценивается по 2 балльной системе: **«зачтено»**, **«незачтено»**.

Оценка **«зачтено»** ставится, если:

- демонстрируемые студентом знания отличаются достаточной глубиной и содержательностью,
- дается достаточно полный ответ, как на основные вопросы, так и на дополнительные;
- студент достаточно свободно владеет терминологией;
- ответ студента не содержит принципиальных ошибок.

Оценка **«незачтено»** ставится, если:

- обнаружено незнание или непонимание студентом основных разделов дисциплины;
- студент допускает существенные фактические ошибки, которые он не может исправить самостоятельно;
- на значительную часть дополнительных вопросов студент затрудняется дать правильный ответ.

Оценивание контрольных работ:

Каждая из четырёх задач оценивается следующими баллами:

0 (задача не сделана), 1 (сделано кое-что), 2 (сделана приблизительно наполовину), 3 (сделана с некоторыми недочетами), 4 (сделана полностью). Общее число баллов за все 4 задания составляет 16. Оценка за работу студента ставится в зависимости от набранного им числа баллов:

- 0 – 4 балла – неудовлетворительно,
- 5 – 8 баллов – удовлетворительно,
- 9 – 12 баллов – хорошо
- 13 – 16 баллов – отлично.

Приложение №2 к рабочей программе дисциплины «Сложность вычислений»

Методические указания для студентов по освоению дисциплины

Основной формой изложения учебного материала по дисциплине "Сложность вычислений" являются лекции, что связано, прежде всего, с достаточно высоким уровнем абстрактности изучаемых в теории алгоритмов и сложности вычислений, ее глубокими и прочными связями с основаниями математики и информатики. По большинству тем предусмотрены практические занятия, целью которых является закрепление лекционного материала путем решения специальным образом подобранных задач и упражнений.

Для успешного освоения дисциплины важно самостоятельное решение достаточно большого набора хорошо подобранных задач, как в аудитории, так и самостоятельно в качестве домашних заданий. Примеры решения задач разбираются на лекциях и практических занятиях, при необходимости по наиболее трудным темам проводятся дополнительные консультации. Основная цель решения задач – помочь усвоить фундаментальные понятия и основы математической логики. Для решения задач необходимо не только знать, но и понимать лекционный материал. Поэтому в процессе изучения дисциплины рекомендуется регулярная работа с конспектами лекций и рекомендованной литературой.

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

Для проверки и контроля усвоения теоретического материала, приобретенных практических навыков работы с основными понятиями математической логики в течение обучения проводятся мероприятия текущей аттестации в виде устного опроса на практических занятиях и контрольной работы в 5-ом семестре. Также проводятся консультации (при необходимости) по лекционному материалу и разбору некоторых заданий для самостоятельной работы.

В конце изучения дисциплины студенты сдают экзамен. Экзамен принимается по экзаменационным билетам, каждый из которых включает в себя два теоретических вопроса. Билеты формируются на основании списка вопросов к экзамену, который охватывает полностью всю программу дисциплины. На самостоятельную подготовку к экзамену выделяется 3 дня, во время подготовки к экзамену предусмотрена групповая консультация.