

**Санкт-Петербургский государственный университет**

**РАБОЧАЯ ПРОГРАММА  
УЧЕБНОЙ ДИСЦИПЛИНЫ**

Теоретическая информатика  
Theoretical Informatics

**Язык(и) обучения**

русский

Трудоемкость в зачетных единицах: 19

Регистрационный номер рабочей программы: 043584

## **Раздел 1. Характеристики учебных занятий**

### **1.1. Цели и задачи учебных занятий**

Сообщение сведений о теоретической информатике в объеме, необходимом для общего развития и изучения смежных дисциплин физико-математического цикла. Усвоение основных идей, понятий и фактов теоретической информатики, умение применять их на практике при программировании ЭВМ.

### **1.2. Требования подготовленности обучающегося к освоению содержания учебных занятий (пререквизиты)**

Не предусмотрены.

### **1.3. Перечень результатов обучения (learning outcomes)**

Обучающийся должен овладеть теоретическим материалом в объеме, предусмотренном программой, уметь применять полученные знания при решении теоретических и прикладных задач, на основе анализа освоенных разделов: алгоритмы сортировки, алгоритмы на графах, жадные алгоритмы и динамическое программирование, структуры данных, производящие функции, матроиды, коды, исправляющие ошибки, алгебраические и вероятностные методы, теория формальных языков, вычислимость и выразимость, теория информации, классы задач и иерархии, интерактивные протоколы, схемная сложность, вероятно проверяемые доказательства; уметь применять полученные знания на практике при программировании ЭВМ.

### **1.4. Перечень и объём активных и интерактивных форм учебных занятий**

практические занятия 114 часов, из них практикум по программированию 16 часов, контрольные работы 6 часов, промежуточная аттестация (зачеты и экзамены) 16 часов

## Раздел 2. Организация, структура и содержание учебных занятий

### 2.1. Организация учебных занятий

#### 2.1.1 Основной курс

Трудоёмкость, объёмы учебной работы и наполняемость групп обучающихся																					
Код модуля в составе дисциплины, практики и т.п.	Контактная работа обучающихся с преподавателем											Самостоятельная работа				ср	к	вн	дое	МК	ст
	лекции	семинары	консультации	практические занятия	лабораторные работы	контрольные работы	коллоквиумы	текущий контроль	промежуточная аттестация	итоговая аттестация	под руководством преподавателя	в присутствии преподавателя	сам. раб. с использованием методических материалов	текущий контроль (сам. раб.)	промежуточная аттестация (сам. раб.)						
<b>ОСНОВНАЯ ТРАЕКТОРИЯ</b>																					
<b>очная форма обучения</b>																					
Семестр 1	48		2	44		2(1)		2				84		32		34	6				
	2-50		2-50	10-25		10-25		2-50				1-1		1-1							
Семестр 2	48		2	14				2				75		37		20	5				
	2-50		2-50	10-25				2-50				1-1		1-1							
Семестр 3	32		2	28		2(1)		2				45		31		34	4				
	2-50		2-50	10-25		10-25		2-50				1-1		1-1							
Семестр 4	32		2	28		2(1)		2				46		30		34	4				
	2-50		2-50	10-25		10-25		2-50				1-1		1-1							
ИТОГО	160		8	114		6		8				250		130					19		

Виды, формы и сроки текущего контроля успеваемости и промежуточной аттестации							
Код модуля в составе дисциплины, практики и т.п.	Формы текущего контроля успеваемости		Виды промежуточной аттестации		Виды итоговой аттестации (только для программ итоговой аттестации и дополнительных образовательных программ)		
	Формы	Сроки	Виды	Сроки	Виды	Сроки	
<b>ОСНОВНАЯ ТРАЕКТОРИЯ</b>							
<b>очная форма обучения</b>							
Семестр 1			зачёт, по результатам работы за период обучения, экзамен, устно, традиционная форма	по графику промежуточной аттестации, по графику промежуточной аттестации			
Семестр 2			зачёт, по результатам работы за	по графику промежуточной аттестации, по			

			<p>период оубчения, экзамен, устно, традиционная форма</p>	<p>графику промежуточной аттестации</p>		
Семестр 3			<p>зачёт, по результатам работы за период оубчения, экзамен, устно, традиционная форма</p>	<p>по графику промежуточной аттестации, по графику промежуточной аттестации</p>		
Семестр 4			<p>зачёт, по результатам работы за период оубчения, экзамен, устно, традиционная форма</p>	<p>по графику промежуточной аттестации, по графику промежуточной аттестации</p>		

## 2.2. Структура и содержание учебных занятий

Период обучения (модуль): Семестр 1

№ п/п	Наименование темы (раздела, части)	Вид учебных занятий	Количество часов
1	Дискретная математика-1	Лекции	24
		практические занятия	16
		практикум по программированию	16
		по методическим материалам	42
2	Контрольная работа	контрольная работа	4
3	Алгоритмы-1	Лекции	24
		практические занятия	16
		в присутствии преподавателя	
		по методическим материалам	42
4	Зачет	промежуточная аттестация (ауд)	2
5	Экзамен	промежуточная аттестация (ауд)	2
		промежуточная аттестация (с.р.)	32

### Раздел 1: Дискретная математика-1

1. Ориентированные и неориентированные графы, пути, циклы, степень, связность, сильная связность. Компоненты сильной связности в неориентированных графах. Ориентированные графы без циклов. Топологическая сортировка. Гомоморфизмы и изоморфизмы графов.
2. Деревья, свойства деревьев, остовные деревья. Коды Прюффера. Теорема Келли о подсчете числа помеченных деревьев.
3. Разрезы и разделяющие множества. Теорема Менгера. Теорема Кенига. Структура двусвязных графов: граф блоков и точек сочленения.
4. Паросочетания в произвольных графах, теорема Татта, формула Бержа.
5. Правильные раскраски графов. Критерий двудольности. Вершинные раскраски графов, теорема Брукса, реберные раскраски, теорема Визинга. Хроматический многочлен. Списочные раскраски.
6. Числа Рамсея  $R(m,n)$ , верхняя оценка. Случай многих цветов. Бесконечный вариант теоремы Рамсея. Обобщение чисел Рамсея на гиперграфы. Теорема Рамсея. Примеры использования теоремы Рамсея: теорема Эрдеша-Секереша о выпуклом  $n$ -угольнике, теорема Шура об одноцветном решении уравнения  $x+y=z$ .
7. Планарные графы, формула Эйлера и следствия из нее. Непланарность  $K_{3,3}$  и  $K_5$ . Теорема о пяти красках, списочный вариант.

8. Перестановки, умножение перестановок, знак перестановки. Количество перестановок. Формула включений-исключений. Сочетания, сочетания с повторениями, размещения. Пути на решетке, обобщенные числа Каталана.
9. Производящие функции. Линейные рекурренты и рациональные производящие функции. Числа Фибоначчи. Производящая функция числа разбиений.
10. Экспонента, логарифм, биномиальный ряд. Экспоненциальные производящие функции. Производящая функция для чисел Каталана. Числа Стирлинга 1 и 2 рода.
11. Комбинаторная теорема о нулях. Вычисление коэффициентов многочленов. Приложение к списочным раскраскам графов.
12. Аддитивная комбинаторика: неравенство треугольника Русы, неравенство Плюнеке, теоремы Коши-Дэвенпорта и Эрдёша-Гайлбронна.

## Раздел 2: Алгоритмы-1

1. Тезис Чёрча. Равнодоступная адресная машина. Время и память. Скорость роста функций. Основные структуры данных: массив, очередь, очередь с приоритетами, стек, словарь, список.
2. st. Реализация рекурсии при помощи стека. Лемма о времени работы рекурсивных алгоритмов. Рекурсивное умножение чисел (алгоритм Карацубы). Алгоритм Штрассена для умножения матриц.
3. Быстрая сортировка. Оценка времени работы в среднем и в наихудшем случае. Сортировка на четырёх лентах. Нижняя оценка на число сравнений для сортировки массива абстрактных данных. Порядковые статистики (поиск k-го элемента в массиве за линейное время). Лексикографическая сортировка.
4. Куча. Сортировка при помощи кучи. Реализация очереди с приоритетами на основе кучи.
5. Динамическое программирование. Задача о рюкзаке. Задача о последовательности редактирования, алгоритм Хиршберга.
6. Деревья, представление в машине. Лес непересекающихся множеств. Поиск остовного дерева наименьшего веса. Изоморфизм деревьев.
7. Деревья поиска. AVL-деревья.
8. B, B+-деревья. Деревья промежутков.
9. Графы, ориентированные и неориентированные, представление в машине. Поиск в глубину и в ширину в неориентированном и ориентированном графе. Топологическая сортировка вершин. Поиск сильно связанных компонент.
10. Кратчайшие пути. Алгоритм Дейкстры, время его работы при различных реализациях. Алгоритм Беллмана-Форда (кратчайшие пути до всех вершин).

11. Задача о максимальном потоке. Теорема о максимальном потоке и минимальном разрезе. Метод Форда-Фалкерсона. Алгоритм Эдмондса-Карпа.

12. Алгоритм проталкивания предпотока. Алгоритм “поднять-и-в-начало”.

Период обучения (модуль): **Семестр 2**

№ п/п	Наименование темы (раздела, части)	Вид учебных занятий	Количество часов
1	Алгоритмы-2	Лекции	12
		практические занятия	16
		в присутствии преподавателя	
		по методическим материалам	38
2	Дискретная математика-2	Лекции	12
		практические занятия	16
		в присутствии преподавателя	
		по методическим материалам	37
3	Зачет	промежуточная аттестация (ауд)	2
4	Экзамен	промежуточная аттестация (ауд)	2
		промежуточная аттестация (с.р.)	37

### Раздел 1: Алгоритмы-2

1. Рекурсивно-перечислимые и рекурсивные множества. Существование рекурсивно-перечислимого, но не рекурсивного множества. Классы P и NP, NP-полные и NP-трудные задачи.

2. Задача о выполнимости булевой формулы. Теорема Шефера (без доказательства NP-полноты). Полиномиально разрешимые случаи.

3. Конечные автоматы. Поиск образца в строке: алгоритм Кнута-Морриса-Пратта. Поиск нескольких образцов в строке: алгоритм Ахо-Корасик.

4. Поиск в списке строк при помощи таблицы длин наибольших префиксов (с построением этой таблицы).

5. Суффиксные массивы. Сортировка суффиксов заданного текста. Построение таблицы длин наибольших префиксов для суффиксов заданного текста.

6. Жадный алгоритм для задачи о выборе заявок. Построение кода Хаффмена жадным алгоритмом. Жадный приближённый алгоритм для задачи о покрытии множествами (с весами).

7. Матроиды, алгоритм для нахождения независимого множества максимального веса. Задача о расписании, решение при помощи матроидов.

8. Вероятностные алгоритмы. Вероятностный алгоритм для проверки умножения матриц. Алгоритм Соловья-Штрассена для проверки простоты числа. Вероятностный вариант быстрой сортировки.

9. Хеш-таблицы и хеш-функции. Универсальное семейство хеш-функций. Время доступа при использовании универсального семейства. Совершенное хеширование (модель с доступом к целым ячейкам памяти).

10. Параллельные алгоритмы, булевы схемы как вычислительная модель. Принцип Брента. Параллельные алгоритмы для умножения матриц и достижимости в графе. Параллельные алгоритмы для сложения и умножения чисел.

11. Дискретное преобразование Фурье. Теоремы о свёртке. Быстрое дискретное преобразование Фурье. Умножение полиномов.

12. Алгоритм Шёнхаге-Штрассена для умножения чисел (с анализом времени работы).

## Раздел 2: Дискретная математика-2

1. Матроиды. Базы, циклы, ранговая функция матроида. Двойственный матроид. Ранговая функция двойственного матроида. Прямая сумма матроидов. Образ матроида.

2. Объединение матроидов. Теорема Радо о независимой трансверсали. Обобщение. Ранговая функция образа матроида. Ранговая функция объединения матроидов. Теорема Нэша-Уильямса о покрытии графа лесами.

3. Вероятностный метод: нижняя оценка на числа Рамсея  $R(k,k)$ , оценка размера независимого множества, графы с большим обхватом и большим хроматическим числом.

4. Локальная лемма Ловаса.

5. Энтропия Шеннона и однозначно декодируемые коды, коды Хаффмена. Энтропия случайной величины. Полуаддитивность энтропии и ее использование в комбинаторике: Оценка суммы начального ряда биномиальных коэффициентов.

6. Угадывание числа по вопросам с одной ошибкой. Код Хемминга. Оценка Хемминга. Линейные коды, оценка Варшамова-Гилберта.

7. Код Адамара и его локальное декодирование, оценки Плоткина. Код Рида-Соломона и его декодирование.

8. Матрица смежности графа, собственные числа, лапласиан графа, матричная теорема о деревьях. Лемма Линдстрема-Гесселя-Вьенно.

9. Экспандеры. Существование алгебраических экспандеров: большинство  $d$ -регулярных графов являются экспандерами.

10. Конечные проективные плоскости и их свойства. Системы Штейнера и дизайны.

11. Тройное тождество Якоби, пентагональная теорема Эйлера. Оценка числа разбиений.

12. Теория перечисления Пойа. Формула обращения Лагранжа.



Период обучения (модуль): **Семестр 3**

№ п/п	Наименование темы (раздела, части)	Вид учебных занятий	Количество часов
1	Теория формальных языков	Лекции	10
		практические занятия	10
		в присутствии преподавателя	14
		по методическим материалам	
2	Контрольная работа	контрольная работа	4
3	Вычислимость и выразимость	Лекции	16
		практические занятия	14
		в присутствии преподавателя	22
		по методическим материалам	
4	Теория информации	Лекции	6
		практические занятия	4
		в присутствии преподавателя	7
		по методическим материалам	
5	Зачет	промежуточная аттестация (ауд)	2
6	Экзамен	промежуточная аттестация (ауд)	2
		промежуточная аттестация (с.р.)	31

**Раздел 1: Теория формальных языков**

1. Понятие о формальном языке. Способы задания языков (выражения, уравнения, грамматики, порождающие системы, принимающие устройства). Контекстно-зависимые языки, неразрешимость проблемы принадлежности.
2. Регулярные языки. Эквивалентные способы задания (детерминированные конечные автоматы, недетерминированные конечные автоматы, регулярные выражения, системы уравнений, право(лево)линейные грамматики).
3. Разрешимые проблемы для регулярных языков. Лемма о накачке.
4. Бесконтекстные языки. Задание грамматиками и магазинными автоматами. Распознавание принадлежности бесконтекстному языку.
5. Языки с предпросмотром. Синтаксический разбор.

**Раздел 2: Вычислимость и выразимость**

1. Вычислимые функции, разрешимые множества, определения перечислимого множества. Теорема Поста. Перечислимые множества как проекции разрешимых. Вычислимость функции и перечислимость ее графика. Универсальная функция. Вычислимая функция, которую нельзя доопределить до всюду определенной. Пример перечислимого, но неразрешимого множества.

2.  $m$ -сведения, другие примеры неразрешимых множеств. Последовательность Шпеккера. Теорема Успенского-Райса. Теорема Клини о неподвижной точке. Программа, печатающая свой текст. Доказательство теоремы Клини для искусственного языка программирования. Главные универсальные функции. Вывод теоремы Успенского-Райса из теоремы Клини.

3. Машины Тьюринга. Неразрешимость проблемы равенства слов в полугруппе (выводимости в одностороннем и двустороннем ассоциативном исчислении). Предикатные формулы (формулы I-го порядка). Интерпретации.

4. Предваренная нормальная форма. Выразимые предикаты. Доказательство невыразимости методом автоморфизмов.

5. Выразимость в арифметике. Арифметичность графика вычислимой функции.

6. Арифметическая иерархия. Универсальные множества в арифметической иерархии. Строгость арифметической иерархии. Теоремы Тарского и Геделя.

7. Элиминация кванторов как метод доказательства невыразимости. Пример задача о разбиении квадрата. Элиминация кванторов и аксиоматизация логических теорий.

8. Элиминация кванторов в элементарной теории вещественных чисел (алгоритм Тарского). Элиминация кванторов в алгебраически замкнутых полях.

### Раздел 3: Теория информации

1. Колмогоровская сложность, ее невычислимость. Доказательство Чайтина теоремы Геделя о неполноте. Бесконечность простых чисел. Нижняя оценка на сложность распознавания палиндромов на одноленточной машине Тьюринга.

2. Конструктивное доказательство Локальной леммы Ловаса. Условная колмогоровская сложность. Теорема Колмогорова-Левина. Неравенство  $2KS(x, y, z) \leq KS(x, y) + KS(y, z) + KS(x, z) + O(\log n)$ , неравенство о связи объема и площадей проекций трехмерного тела.

3. Коммуникационный протокол, коммуникационная сложность функции равенства. Вероятностный коммуникационный протокол для предиката равенства. Нижняя оценка на произведение времени и памяти для многоленточной машины Тьюринга, которая распознает язык палиндромов.

### Период обучения (модуль): Семестр 4

№ п/п	Наименование темы (раздела, части)	Вид учебных занятий	Количество часов
1	Классы задач и иерархии	Лекции	14
		практические занятия	10
		в присутствии преподавателя	
		по методическим материалам	17
2	Интерактивные протоколы	Лекции	8
		практические занятия	8
		в присутствии преподавателя	
		по методическим материалам	14

3	Контрольная работа	Контрольная работа	4
		Лекции	6
4	Схемная сложность	практические занятия	6
		в присутствии преподавателя	
		по методическим материалам	8
5	Вероятностно проверяемые доказательства	Лекции	4
		практические занятия	4
		в присутствии преподавателя	
		по методическим материалам	7
6	Зачет	промежуточная аттестация (ауд)	2
7	Экзамен	промежуточная аттестация (ауд)	2
		промежуточная аттестация (с.р.)	30

### Раздел 1: Классы задач и иерархии

1. Эффективная универсальная машина Тьюринга. Недетерминированные машины Тьюринга. Классы P, NP, сводимости. Полнота задачи об ограниченной остановке, полнота CircuitSAT, 3-SAT (теорема Кука-Левина). Универсальный алгоритм для задач поиска. Сведение задач поиска к задачам распознавания.
2. Не NP-полное множество в NP-P (теорема Ладнера). Оракулы. Оракул, разделяющий P и NP.
3. Вычисления с ограничениями по памяти: взаимоотношения между детерминированными, недетерминированными и конедетерминированными вычислениями. PSPACE-полнота QBF. Иерархия по памяти. Иерархия по времени для детерминированных и недетерминированных вычислений.
4. Полиномиальная иерархия Стокмеера. Определение через чередование кванторов, оракульное определение, эквивалентность. Полные задачи в уровнях полиномиальной иерархии. Булевы схемы, класс P/poly, связь с классом P. Теорема Карпа-Липтона.
5. Параллельные алгоритмы для сложения и умножения чисел и умножения матриц. NC1 содержится в DSpace[log n], NSpace[log n] содержится в NC2. P-полные задачи.
6. Вероятностные алгоритмы, классы BPP, RP, ZPP. Лемма Шварца-Циппеля. BPP содержится во втором уровне полиномиальной иерархии. Полиномиальные схемы для BPP.
7. Универсальное семейство хеш-функций. Лемма Вэлианта-Вазирани. Считающие классы, теорема Тода (с доказательством первой части).
8. Доказательство второй части теоремы Тода.

### Раздел 2: Интерактивные протоколы

1. Интерактивные протоколы с публичными и с секретными случайными битами. MA содержится в AM.  $AM(2)=AM(k)$ .  $IP(2)=IP(k)$ .  $IP=IP(poly)$ .

2. Теорема Шамира ( $IP=PSPACE$ ).
3. Интерактивный протокол для задачи о перманенте.
4. Протокол Гольдвассер-Сипсера оценки размера множества и его использование для замены секретных случайных битов публичными.

### **Раздел 3: Схемная сложность**

1. Нижние оценки схемной сложности фиксированным многочленом.
2. Монотонные булевы функции и монотонные схемы. Теорема Разборова о нижней оценке на размер монотонной функции, решающей задачу о клике.
3. Схемы ограниченной глубины. Лемма о переключении. Нижняя оценка на функцию четности для схем константной глубины.

### **Раздел 4: Вероятностно проверяемые доказательства**

1. Вероятностно проверяемые доказательства. PCP-теорема и сложность аппроксимации. Примеры приближенных алгоритмов.
2. Тестирование функции на линейность, доказательство включения NP в PCP(1, poly).

### **Раздел 3. Обеспечение учебных занятий**

#### **3.1. Методическое обеспечение**

##### **3.1.1 Методические указания по освоению дисциплины**

Посещение лекций и практических занятий

##### **3.1.2 Методическое обеспечение самостоятельной работы**

Основная и дополнительная литература

##### **3.1.3 Методика проведения текущего контроля успеваемости и промежуточной аттестации и критерии оценивания**

###### **Методика проведения зачета**

Зачет проводится в устной форме. Для получения зачета необходимо решить 60% задач, предлагаемых в течение семестра. В случае, если к моменту проведения зачета студент решил меньшее количество задач, на зачете ему предлагаются задачи аналогичные по тематике и сложности. Задачи даются в форме домашних заданий с устной сдачей («листочки»), практических заданий (написание программы для ЭВМ) и контрольных. Возможна выдача задач повышенной сложности, решение которых засчитывается в качестве индивидуальных достижений студента (при подаче заявок на именные стипендии, конкурсы и т.п.); сдача таких заданий проводится в устной форме.

###### **Методика проведения экзамена**

Экзамен проводится в устной форме. Билет состоит из двух вопросов. Время подготовки ответа на вопросы билета составляет 60 минут.

Использование конспектов и учебников, а также электронных устройств хранения, обработки или передачи информации при подготовке и ответе на вопросы экзамена категорически запрещено. В случае обнаружения факта использования недопустимых материалов (устройств) составляется акт и студент удаляется с экзамена. После ответа на вопросы билета преподаватель задает несколько дополнительных вопросов, на основании оценки ответов на которые итоговая оценка по предмету может быть повышена или понижена.

###### **Критерии выставления оценок**

Оценка «отлично» ставится за полностью раскрытый теоретический материал и правильные ответы на дополнительные вопросы преподавателя. В болонской шкале оценка может быть скорректирована в ту или иную сторону с учетом малозначительных погрешностей изложения или, напротив, углубленного изложения материала.

Оценка «хорошо» ставится за изложенный теоретический материал билета (возможно с помощью наводящих подсказок преподавателя).

Оценка «удовлетворительно» ставится за знание основных вопросов по каждой теме.

Оценка «неудовлетворительно» выставляется, если не выполняются условия для получения оценок «отлично», «хорошо» и «удовлетворительно».

##### **3.1.4 Методические материалы для проведения текущего контроля успеваемости и промежуточной аттестации (контрольно-измерительные материалы, оценочные средства)**

Период обучения (модуль): **Семестр 1**

### Темы практических заданий:

1. Основные конструкции языка C и структуры данных.
2. Основные конструкции языка C++, использование стандартных библиотек, рекурсивные структуры данных.
3. Сортировки. Кучи. Порядковые статистики. Бинарный поиск.
4. Динамическое программирование.

### Темы теоретических задач:

1. Деревья. Связность графов. Паросочетания. Раскраски графов. Планарные графы.
2. Теория Рамсея. Перечислительная комбинаторика. Производящие функции. Полиномиальный метод. Аддитивная комбинаторика.
3. Асимптотика. Оценка времени работы программы.

### Список вопросов к экзамену:

1. Ориентированные и неориентированные графы, пути, циклы, степень, связность, сильная связность. Компоненты сильной связности в неориентированных графах. Ориентированные графы без циклов. Топологическая сортировка. Гомоморфизмы и изоморфизмы графов.
2. Деревья, свойства деревьев, остовные деревья. Коды Прюффера. Теорема Келли о подсчете числа помеченных деревьев.
3. Разрезы и разделяющие множества. Теорема Менгера. Теорема Кенига. Структура двусвязных графов: граф блоков и точек сочленения.
4. Паросочетания в произвольных графах, теорема Татта, формула Бержа.
5. Правильные раскраски графов. Критерий двудольности. Вершинные раскраски графов, теорема Брукса, реберные раскраски, теорема Визинга. Хроматический многочлен. Списочные раскраски.
6. Числа Рамсея  $R(m,n)$ , верхняя оценка. Случай многих цветов. Бесконечный вариант теоремы Рамсея. Обобщение чисел Рамсея на гиперграфы. Теорема Рамсея. Примеры использования теоремы Рамсея: теорема Эрдеша-Секереша о выпуклом  $n$ -угольнике, теорема Шура об одноцветном решении уравнения  $x+y=z$ .
7. Планарные графы, формула Эйлера и следствия из нее. Непланарность  $K_{3,3}$  и  $K_5$ . Теорема о пяти красках, списочный вариант.
8. Перестановки, умножение перестановок, знак перестановки. Количество перестановок. Формула включений-исключений. Сочетания, сочетания с повторениями, размещения. Пути на решетке, обобщенные числа Каталана.
9. Производящие функции. Линейные рекурренты и рациональные производящие функции. Числа Фибоначчи. Производящая функция числа разбиений.
10. Экспонента, логарифм, биномиальный ряд. Экспоненциальные производящие функции. Производящая функция для чисел Каталана. Числа Стирлинга 1 и 2 рода.

11. Комбинаторная теорема о нулях. Вычисление коэффициентов многочленов. Приложение к списочным раскраскам графов.
12. Аддитивная комбинаторика: неравенство треугольника Русы, неравенство Плюнеке, теоремы Коши-Дэвенпорта и Эрдёша-Гайлбронна.
13. Тезис Чёрча. Равнодоступная адресная машина. Время и память. Скорость роста функций. Основные структуры данных: массив, очередь, очередь с приоритетами, стек, словарь, список.
14. Рекурсия. Реализация рекурсии при помощи стека. Лемма о времени работы рекурсивных алгоритмов. Рекурсивное умножение чисел (алгоритм Карацубы). Алгоритм Штрассена для умножения матриц.
15. Быстрая сортировка. Оценка времени работы в среднем и в наихудшем случае. Сортировка на четырёх лентах. Нижняя оценка на число сравнений для сортировки массива абстрактных данных. Порядковые статистики (поиск k-го элемента в массиве за линейное время). Лексикографическая сортировка.
16. Куча. Сортировка при помощи кучи. Реализация очереди с приоритетами на основе кучи.
17. Динамическое программирование. Задача о рюкзаке. Задача о последовательности редактирования, алгоритм Хиршберга.
18. Деревья, представление в машине. Лес непересекающихся множеств. Поиск остовного дерева наименьшего веса. Изоморфизм деревьев.
19. Деревья поиска. AVL-деревья.
20. B, B+-деревья. Деревья промежутков.
21. Графы, ориентированные и неориентированные, представление в машине. Поиск в глубину и в ширину в неориентированном и ориентированном графе. Топологическая сортировка вершин. Поиск сильно связанных компонент.
22. Кратчайшие пути. Алгоритм Дейкстры, время его работы при различных реализациях. Алгоритм Беллмана-Форда (кратчайшие пути до всех вершин).
23. Задача о максимальном потоке. Теорема о максимальном потоке и минимальном разрезе. Метод Форда-Фалкерсона. Алгоритм Эдмондса-Карпа.
24. Алгоритм проталкивания предпотока. Алгоритм “поднять-и-в-начало”.

Период обучения (модуль): **Семестр 2**

Темы **практических заданий**:

1. Поиск в ширину и глубину. Динамическое программирование на дереве. Кратчайшие пути.
2. Жадные алгоритмы. Минимальный остов.
3. Деревья поиска. Статистики на отрезке. Неявный ключ.

#### 4. Персистентность.

#### Темы теоретических задач:

1. Матроиды.
2. Вероятностный метод в комбинаторике и в теории графов.
3. Коды.
4. Алгебраическая теория графов.
5. Теория перечисления Пойа. Мастер-теорема Макмагона.

#### Список вопросов к экзамену:

1. Рекурсивно-перечислимые и рекурсивные множества. Существование рекурсивно-перечислимого, но не рекурсивного множества. Классы P и NP, NP-полные и NP-трудные задачи.
2. Задача о выполнимости булевой формулы. Теорема Шефера (без доказательства NP-полноты). Полиномиально разрешимые случаи.
3. Конечные автоматы. Поиск образца в строке: алгоритм Кнута-Морриса-Пратта. Поиск нескольких образцов в строке: алгоритм Ахо-Корасик.
4. Поиск в списке строк при помощи таблицы длин наибольших префиксов (с построением этой таблицы).
5. Суффиксные массивы. Сортировка суффиксов заданного текста. Построение таблицы длин наибольших префиксов для суффиксов заданного текста.
6. Жадный алгоритм для задачи о выборе заявок. Построение кода Хаффмена жадным алгоритмом. Жадный приближённый алгоритм для задачи о покрытии множествами (с весами).
7. Матроиды, алгоритм для нахождения независимого множества максимального веса. Задача о расписании, решение при помощи матроидов.
8. Вероятностные алгоритмы. Вероятностный алгоритм для проверки умножения матриц. Алгоритм Соловья-Штрассена для проверки простоты числа. Вероятностный вариант быстрой сортировки.
9. Хеш-таблицы и хеш-функции. Универсальное семейство хеш-функций. Время доступа при использовании универсального семейства. Совершенное хеширование (модель с доступом к целым ячейкам памяти).
10. Параллельные алгоритмы, булевы схемы как вычислительная модель. Принцип Брента. Параллельные алгоритмы для умножения матриц и достижимости в графе. Параллельные алгоритмы для сложения и умножения чисел.
11. Дискретное преобразование Фурье. Теоремы о свёртке. Быстрое дискретное преобразование Фурье. Умножение полиномов.
12. Алгоритм Шёнхаге-Штрассена для умножения чисел (с анализом времени работы).



13. Матроиды. Базы, циклы, ранговая функция матроида. Двойственный матроид. Ранговая функция двойственного матроида. Прямая сумма матроидов. Образ матроида.
14. Объединение матроидов. Теорема Радо о независимой трансверсали. Обобщение. Ранговая функция образа матроида. Ранговая функция объединения матроидов. Теорема Нэша-Уильямса о покрытии графа лесами.
15. Вероятностный метод: нижняя оценка на числа Рамсея  $R(k,k)$ , оценка размера независимого множества, графы с большим обхватом и большим хроматическим числом.
16. Локальная лемма Ловаса.
17. Энтропия Шенона и однозначно декодируемые коды, коды Хаффмена. Энтропия случайной величины. Полуаддитивность энтропии и ее использование в комбинаторике: Оценка суммы начального ряда биномиальных коэффициентов.
18. Угадывание числа по вопросам с одной ошибкой. Код Хемминга. Оценка Хемминга. Линейные коды, оценка Варшамова-Гилберта.
19. Код Адамара и его локальное декодирование, оценки Плоткина. Код Рида-Соломона и его декодирование.
20. Матрица смежности графа, собственные числа, лапласиан графа, матричная теорема о деревьях. Лемма Линдстрема-Гесселя-Вьенно.
21. Экспандеры. Существование алгебраических экспандеров: большинство  $d$ -регулярных графов являются экспандерами.
22. Конечные проективные плоскости и их свойства. Системы Штейнера и дизайны.
23. Тройное тождество Якоби, пентагональная теорема Эйлера. Оценка числа разбиений.
24. Теория перечисления Пойа. Формула обращения Лагранжа.

Период обучения (модуль): **Семестр 3**

Темы **теоретических задач**:

1. Конечные автоматы. Доказательства нерегулярности. Формальные грамматики.
2. Разрешимость, перечислимость. Доказательства неразрешимости. Теорема Клини о неподвижной точке.
3. Доказательства невыразимости методом автоморфизмов. Арифметическая иерархия. Элиминация кванторов.
4. Колмогоровская сложность. Коммуникационная сложность.

**Список вопросов к экзамену:**

1. Понятие о формальном языке. Способы задания языков (выражения, уравнения, грамматики, порождающие системы, принимающие устройства). Контекстно-зависимые языки, неразрешимость проблемы принадлежности.

2. Регулярные языки. Эквивалентные способы задания (детерминированные конечные автоматы, недетерминированные конечные автоматы, регулярные выражения, системы уравнений, право(лево)линейные грамматики).
3. Разрешимые проблемы для регулярных языков. Лемма о накачке.
4. Бесконтекстные языки. Задание грамматиками и магазинными автоматами. Распознавание принадлежности бесконтекстному языку.
5. Языки с предпросмотром. Синтаксический разбор.
6. Вычислимые функции, разрешимые множества, определения перечислимого множества. Теорема Поста. Перечислимые множества как проекции разрешимых. Вычислимость функции и перечислимость ее графика. Универсальная функция. Вычислимая функция, которую нельзя доопределить до всюду определенной. Пример перечислимого, но неразрешимого множества.
7.  $m$ -сведения, другие примеры неразрешимых множеств. Последовательность Шпеккера. Теорема Успенского-Райса. Теорема Клини о неподвижной точке. Программа, печатающая свой текст. Доказательство теоремы Клини для искусственного языка программирования. Главные универсальные функции. Вывод теоремы Успенского-Райса из теоремы Клини.
8. Машины Тьюринга. Неразрешимость проблемы равенства слов в полугруппе (выводимости в одностороннем и двустороннем ассоциативном исчислении). Предикатные формулы (формулы  $I$ -го порядка). Интерпретации.
9. Предваренная нормальная форма. Выразимые предикаты. Доказательство невыразимости методом автоморфизмов.
10. Выразимость в арифметике. Арифметичность графика вычислимой функции.
11. Арифметическая иерархия. Универсальные множества в арифметической иерархии. Строгость арифметической иерархии. Теоремы Тарского и Геделя.
12. Элиминация кванторов как метод доказательства невыразимости. Пример задача о разбиении квадрата. Элиминация кванторов и аксиоматизация логических теорий.
13. Элиминация кванторов в элементарной теории вещественных чисел (алгоритм Тарского). Элиминация кванторов в алгебраически замкнутых полях.
14. Колмогоровская сложность, ее невычислимость. Доказательство Чайтина теоремы Геделя о неполноте. Бесконечность простых чисел. Нижняя оценка на сложность распознавания палиндромов на одноленточной машине Тьюринга.
15. Конструктивное доказательство Локальной леммы Ловаса. Условная колмогоровская сложность. Теорема Колмогорова-Левина. Неравенство  $2KS(x, y, z) \leq KS(x, y) + KS(y, z) + KS(x, z) + O(\log n)$ , неравенство о связи объема и площадей проекций трехмерного тела.
16. Коммуникационный протокол, коммуникационная сложность функции равенства. Вероятностный коммуникационный протокол для предиката равенства. Нижняя оценка на

произведение времени и памяти для многоленточной машины Тьюринга, которая распознает язык палиндромов.

Период обучения (модуль): **Семестр 4**

Темы **теоретических задач**:

1. Недетерминированные машины Тьюринга. Доказательства NP-полноты. Построение полных задач в различных классах сложности.
2. Диагонализация. Совместные оценки по памяти и времени. Вычисления с ограниченной памятью.
3. Вероятностные классы сложности. Интерактивные протоколы. Иерархия по времени и памяти.
4. Нижние оценки на размер формул и схем. Хэш-функции. Коды, исправляющие ошибки.

**Список вопросов к экзамену:**

1. Эффективная универсальная машина Тьюринга. Недетерминированные машины Тьюринга. Классы P, NP, сводимости. Полнота задачи об ограниченной остановке, полнота CircuitSAT, 3-SAT (теорема Кука-Левина). Универсальный алгоритм для задач поиска. Сведение задач поиска к задачам распознавания.
2. Не NP-полное множество в NP-P (теорема Ладнера). Оракулы. Оракул, разделяющий P и NP.
3. Вычисления с ограничениями по памяти: взаимоотношения между детерминированными, недетерминированными и конедетерминированными вычислениями. PSPACE-полнота QBF. Иерархия по памяти. Иерархия по времени для детерминированных и недетерминированных вычислений.
4. Полиномиальная иерархия Стокмеера. Определение через чередование кванторов, оракульное определение, эквивалентность. Полные задачи в уровнях полиномиальной иерархии. Булевы схемы, класс P/poly, связь с классом P. Теорема Карпа-Липтона.
5. Параллельные алгоритмы для сложения и умножения чисел и умножения матриц. NC1 содержится в DSpace[log n], NSpace[log n] содержится в NC2. P-полные задачи.
6. Вероятностные алгоритмы, классы BPP, RP, ZPP. Лемма Шварца-Циппеля. BPP содержится во втором уровне полиномиальной иерархии. Полиномиальные схемы для BPP.
7. Универсальное семейство хэш-функций. Лемма Вэлианта-Вазирани. Считающие классы, теорема Тода (с доказательством первой части).
8. Доказательство второй части теоремы Тода.
9. Интерактивные протоколы с публичными и с секретными случайными битами. MA содержится в AM.  $AM(2)=AM(k)$ .  $IP(2)=IP(k)$ .  $IP=IP(poly)$ .
10. Теорема Шамира ( $IP=PSPACE$ ).
11. Интерактивный протокол для задачи о перманенте.

12. Протокол Гольдвассер-Сипсера оценки размера множества и его использование для замены секретных случайных битов публичными.
13. Нижние оценки схемной сложности фиксированным многочленом.
14. Монотонные булевы функции и монотонные схемы. Теорема Разборова о нижней оценке на размер монотонной функции, решающей задачу о клике.
15. Схемы ограниченной глубины. Лемма о переключении. Нижняя оценка на функцию четности для схем константной глубины.
16. Вероятностно проверяемые доказательства. PCP-теорема и сложность аппроксимации. Примеры приближенных алгоритмов.
17. Тестирование функции на линейность, доказательство включения NP в PCP(1, poly).

### **3.1.5 Методические материалы для оценки обучающимися содержания и качества учебного процесса**

#### **3.2. Кадровое обеспечение**

##### **3.2.1 Образование и (или) квалификация штатных преподавателей и иных лиц, допущенных к проведению учебных занятий**

К чтению лекций должны привлекаться преподаватели, имеющие ученую степень доктора или кандидата наук (в том числе степень PhD, прошедшую установленную процедуру признания и установления эквивалентности) и/или ученое звание профессора или доцента.

##### **3.2.2 Обеспечение учебно-вспомогательным и (или) иным персоналом**

не требуется

#### **3.3. Материально-техническое обеспечение**

##### **3.3.1 Характеристики аудиторий (помещений, мест) для проведения занятий**

Стандартно оборудованные лекционные аудитории, должны вмещать поток в соответствии со списком студентов. Для практикума по программированию требуется компьютерный класс.

##### **3.3.2 Характеристики аудиторного оборудования, в том числе неспециализированного компьютерного оборудования и программного обеспечения общего пользования**

Доска для письма мелом или фломастером. Для практикума по программированию компьютерный класс должен быть оборудован компьютерами из расчета один компьютер на одного студента с возможностью выхода в сеть Интернет.

##### **3.3.3 Характеристики специализированного оборудования**

не требуется

##### **3.3.4 Характеристики специализированного программного обеспечения**

не требуется

### **3.3.5 Перечень и объёмы требуемых расходных материалов**

Мел — не менее 1 куска на час лекционных занятий, фломастеры для доски, губка

## **3.4. Информационное обеспечение**

### **3.4.1 Список обязательной литературы**

1. Н. Вирт. Алгоритмы и структуры данных. Новая версия для Оберона. – М.: ДМК Пресс, 2014.

2. В.А. Емеличев и др. Лекции по теории графов. – М.: Наука, 1990.

3. Б.К.Мартыненко. Языки и трансляции. – СПб: Издательство СПбГУ, 2013.

4. А. М. Райгородский. Вероятность и алгебра в комбинаторике. М.: МЦНМО, 2008, 48 с.

<http://www.mccme.ru/free-books/dubna/raigor-1.pdf>

5. А. Китаев, А. Шень, М. Вялый. Классические и квантовые вычисления. М.: МЦНМО, 1999, 192 с.

<http://www.mccme.ru/free-books/qcomp/qbook.ps.gz>

6. А. Шень. Программирование: теоремы и задачи, 2-е изд., М.: МЦНМО, 2004, 296 с.

<http://www.mccme.ru/free-books/shen/shen-progbook.pdf>

7. Н. К. Верещагин, В. А. Успенский, А. Шень. Колмогоровская сложность и алгоритмическая случайность. М.: МЦНМО, 2013, 576 с.

<http://www.mccme.ru/free-books/shen/kolmbook.pdf>

8. Н. К. Верещагин, А. Шень. Лекции по математической логике и теории алгоритмов. В 3 частях. 4-е изд., испр., М.: МЦНМО, 2012.

<http://www.mccme.ru/free-books/shen/shen-logic-part1-2.pdf>

<http://www.mccme.ru/free-books/shen/shen-logic-part2-2.pdf>

<http://www.mccme.ru/free-books/shen/shen-logic-part3-2.pdf>

9. А. М. Райгородский. Гипотеза Кнезера и топологический метод в комбинаторике. М.: МЦНМО, 2011, 32 с.

<http://www.mccme.ru/free-books/dubna/raigor-3.pdf>

10. А. М. Райгородский. Модели случайных графов. М.: МЦНМО, 2011, 136 с.

<http://www.mccme.ru/free-books/dubna/raigor-4.pdf>

### **3.4.2 Список дополнительной литературы**

1. А. Х. Шень. Программирование: теоремы и задачи. – М.: МЦНМО, 2007.

2. М. А. Бабенко, М. В. Левин. Введение в теорию алгоритмов и структур данных. – М.: МЦНМО, 2012.

3. Т. Кормен, Ч. Лейзерсон, И. Ривест, К. Штайн. Алгоритмы: построение и анализ. – М., СПб, Киев: Издательский дом “Вильямс”, 2012.
4. Р. Грэхем, Д. Кнут, О. Паташник. Конкретная математика: основание информатики. – М.: Мир, 2006.
5. С.К. Ландо, Лекции о производящих функциях. – М.: МЦНМО, 2004.
6. Н. Алон, Дж. Спенсер. Вероятностный метод. – М.: БИНОМ, Лаборатория знаний, 2007.
7. Н.К. Верещагин, В.А. Успенский, А. Шень. Колмогоровская сложность и алгоритмическая случайность. – М.: МЦНМО, 2013.

### **3.4.3 Перечень иных информационных источников**

#### **Раздел 4. Разработчики программы**

Гирш Эдуард Алексеевич, доктор физ.-мат. наук, ведущий научный сотрудник ПОМИ РАН, [hirsch@pdmi.ras.ru](mailto:hirsch@pdmi.ras.ru)