МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Иркутский государственный университет»
(ФГБОУ ВО «ИГУ»)
Институт математики и информационных технологий

УТВЕРЖДАЮ
Директор ИМИТ
_____ М.В. Фалалеев
«21» 09 2022 г.

Рабочая программа дисциплины (модуля)

Наименование дисциплины (модуля): **Вычислительная сложность алгоритмов и программ**

Научная специальность: **1.2.2. Математическое моделирование, численные методы и комплексы программ**

Форма обучения: очная

Согласовано с УМК ИМИТ
протокол № 1 от «20» 09 2022 г.

Председатель УМК _____ /Антоник В.Г./

Программа рассмотрена на заседании кафедры вычислительной математики и оптимизации
«14» 09 2022 г. Протокол № 1

Зав. кафедрой _____ /Аргучинцев А.В./

Иркутск 2022 г.

Содержание

1. Цели и задачи дисциплины (модуля): введение в теорию алгоритмической сложности, формирование навыков оценивания вычислительной эффективности алгоритмов.

Задачи:

– изучить основные понятия алгоритмической сложности;
– изучить основные сложностные классы и взаимоотношения между ними;
– изучить основы теории приближенных алгоритмов;
– изучить основы вероятностных вычислений;
– изучить сложность задач, исследуемых в современной криптографии;
– изучить основные методы сложностной аргументации стойкости криптосистем.

2. Требования к результатам освоения дисциплины (модуля):

В результате изучения дисциплины аспирант должен:

Знать:
– основные концепции современной теории сложности алгоритмов
Уметь:
– строить оценки сложности реально используемых алгоритмов
– доказывать NP-полноту и NP-трудность комбинаторных задач
Владеть:
– навыками сложностной аргументации стойкости криптосистем

3. Объем дисциплины (модуля) и виды учебной работы

Вид учебной работы	**Всего академических часов**	**Курсы**			
			2		
Аудиторные занятия (всего)	**16**		**16**		
В том числе:					
Лекции	**8**		8		
Практические занятия (ПЗ)	**8**		8		
Самостоятельная работа (всего)	**18**		18		
В том числе:					
Реферат (при наличии)					
Контактная работа					
Подготовка к зачету	**18**		18		
Промежуточная аттестация (всего)	**2**		2		
В том числе:					
Контактная работа во время промежуточной аттестации	2		2		
Форма промежуточной аттестации (зачет, экзамен)	зачет		зачет		

Общая трудоемкость	часы	36		36		
	зачетные единицы	1		1		

4. Содержание дисциплины (модуля)

4.1. Содержание разделов и тем дисциплины (модуля).

№	Наименование раздела	Содержание раздела дисциплины
1.	Основные классы вычислительной (временной) сложности.	Задачи распознавания двоичных языков. Класс P. Полиномиальные недетерминированные вычисления и классы NP и co-NP. Основная гипотеза теории вычислительной сложности.
2.	Сводимость по Карпу и понятие NP-полноты. Теорема Кука.	Понятие сводимости по Карпу для двоичных языков и проблем распознавания. Свойства сводимости по Карпу, примеры. Преобразования Цейтина для булевых уравнений. Теорема Кука.
3.	Базовые NP-полные задачи.	NP-полнота ряда комбинаторных задач (3-ВЫПОЛНИМОСТЬ, совместность квадратичных систем над полем GF(2), 0-1-целочисленное линейное программирование, задачи на графах, задачи о сочетаниях и покрытиях, задачи 0-1-РЮКЗАК и РАЗБИЕНИЕ). Псевдополиномиальные алгоритмы и сильная NP-полнота.
4.	Понятие NP-трудности и некоторые NP-трудные задачи.	Оракульная машина Тьюринга и полиномиальная сводимость по Тьюрингу. Понятие NP-трудности и некоторые NP-трудные задачи. Примеры NP-трудных задач, не являющихся алгоритмически разрешимыми.
5.	Приближенные алгоритмы.	NP-трудная задача об упаковке контейнеров и приближенный алгоритм ее решения. Понятие погрешности приближенного алгоритма. Приближенные алгоритмы для задачи поиска минимального вершинного покрытия. Пример алгоритма, не являющегося дельта-приближенным ни для какого дельта.
6.	Вероятностное время и основные вероятностные классы.	Вероятностная машина Тьюринга и полиномиальное вероятностное время. Классы RP, co-RP, BPP и ZPP. Задача проверки простоты натуральных чисел и полиномиальный вероятностный алгоритм ее решения (тест Соловея-Штрассена).
7.	Теорема Рамсея и вероятностный метод в теории графов.	Формулировка и доказательство теоремы Рамсея. Проблема нижних оценок для чисел Рамсея. Вероятностный метод Эрдеша в теории графов и получение с его помощью нижних оценок для чисел Рамсея.
8.	Полиномиальная иерархия и схемная сложность.	Схемы из функциональных элементов над различными базисами. Возможность «распознавания» произвольного двоичного языка семейством схем экспоненциальной сложности. Класс P/poly. Полиномиальная иерархия. Теорема Стокмейера. Теорема Карпа-Липтона. Теорема

		Адлмана о включении BPP в P/poly. Теорема Шеннона о схемной сложности почти всех булевых функций.
9.	Структурная теория сложности алгоритмов и современная криптография.	Понятие односторонней функции. Односторонние функции и основная гипотеза структурной теории сложности. Сложностной подход к определению псевдослучайного генератора (ПСГ). ПСГ и односторонние функции. Простейшие криптографические протоколы. Протокол подбрасывания монеты по телефону. Протокол забывающей передачи данных.

4.2. Разделы и темы дисциплины (модуля) и виды занятий

№ п/п	Наименование раздела	Наименование темы	Виды занятий в часах			
			Лекции	Практические занятия	Самостоятельная работа	Всего
1.	Основные классы вычислительной (временной) сложности.	Задачи распознавания двоичных языков. Класс P.	2		3	5
2.	Основные классы вычислительной	Полиномиальные недетерминированные вычисления и классы NP и co-NP. Основная гипотеза теории вычислительной сложности.			3	3
3.	Сводимость по Карпу и понятие NP-полноты. Теорема Кука.	Понятие сводимости по Карпу для двоичных языков и проблем распознавания. Свойства сводимости по Карпу, примеры.	2		2	4
4.	Сводимость по Карпу и понятие NP-полноты. Теорема Кука.	Преобразования Цейтина для булевых уравнений. Теорема Кука.		2	2	4
5.	Базовые NP-	NP-полнота	2		1	3

	полные задачи.	ряда комбинаторных задач (3-ВЫПОЛНИМОСТЬ, совместность квадратичных систем над полем GF(2), 0-1-целочисленное линейное программирование, задачи на графах, задачи о сочетаниях и покрытиях, задачи 0-1-РЮКЗАК и РАЗБИЕНИЕ). Псевдополиномиальные алгоритмы и сильная NP-полнота.				
6.	Понятие NP-трудности и некоторые NP-трудные задачи.	Оракульная машина Тьюринга и полиномиальная сводимость по Тьюрингу. Понятие NP-трудности и некоторые NP-трудные задачи. Примеры NP-трудных задач, не являющихся алгоритмически разрешимыми.		2	1	3
7.	Приближенные алгоритмы.	NP-трудная задача об упаковке контейнеров и приближенный алгоритм ее решения. Понятие погрешности приближенного			1	1

		алгоритма. Приближенные алгоритмы для задачи поиска минимального вершинного покрытия. Пример алгоритма, не являющегося дельта-приближенным ни для какого дельта.				
8.	Вероятностное время и основные вероятностные классы.	Вероятностная машина Тьюринга и полиномиальное вероятностное время. Классы RP, co-RP, BPP и ZPP. Задача проверки простоты натуральных чисел и полиномиальный вероятностный алгоритм ее решения (тест Соловея-Штрассена).			1	1
9.	Теорема Рамсея и вероятностный метод в теории графов.	Формулировка и доказательство теоремы Рамсея. Проблема нижних оценок для чисел Рамсея. Вероятностный метод Эрдеша в теории графов и получение с его помощью нижних оценок для чисел		2	1	3

		Рамсея.				
10.	Полиномиальная иерархия и схемная сложность.	Схемы из функциональных элементов над различными базисами. Возможность «распознавания» произвольного двоичного языка семейством схем экспоненциальной сложности. Класс P/poly. Полиномиальная иерархия.			1	1
11.	Полиномиальная иерархия и схемная сложность.	Теорема Стокмейера. Теорема Карпа-Липтона. Теорема Адлмана о включении BPP в P/poly. Теорема Шеннона о схемной сложности почти всех булевых функций.		2	1	3
12.	Структурная теория сложности алгоритмов и современная криптография.	Понятие односторонней функции. Односторонние функции и основная гипотеза структурной теории сложности. Сложностной подход к определению псевдослучайного генератора (ПСГ). ПСГ и	2		1	3

		односторонние функции. Простейшие криптографические протоколы. Протокол подбрасывания монеты по телефону. Протокол забывающей передачи данных.				
	ВСЕГО:		8	8	18	34

4.3. Перечень семинарских, практических занятий и лабораторных работ

№ п/п	№ раздела и темы дисциплины (модуля)	Наименование семинаров, практических и лабораторных работ	Трудоемкость (часы)	Оценочные средства
1	**2**	**3**	**4**	**5**
2	Тема 2	Решение систем булевых уравнений с использование различных методов (SAT, BDD, линеаризационные множества).	2	Устный опрос, сам.работа
4	Тема 4	Доказательство разрешимости ряда задач на полиномиальной памяти.	2	Устный опрос, сам.работа
5	Тема 7	Вероятностный метод Эрдеша в теории графов и получение с его помощью нижних оценок для чисел Рамсея.	2	Устный опрос, сам.работа
6.	Тема 8	Теорема Стокмейера. Теорема Карпа-Липтона.	2	Устный опрос, сам.работа

5. Примерная тематика рефератов, докладов, проектов (при наличии): не предусмотрены

6. Учебно-методическое и информационное обеспечение дисциплины (модуля):

а) основная литература

1. Алгоритмы: построение и анализ [Текст] : научное издание / Т. Кормен [и др.]. - 2-е изд. - М. ; СПб. ; Киев : Вильямс, 2007. - 1290 с. : ил. ; 24 см. - Библиогр.: с.1257-1276. - Предм. указ.: с. 1277-1290. - Пер. изд. : Introduction to Algorithms / T. Cormen, C. Leiserson, R. Riverst. - 2 ed. - ISBN 5-8459-0857-4 : 939.43 р. Экз-ры: физмат 25828 (8 экз.)

2. Глухов, М. М. Математическая логика. Дискретные функции. Теория алгоритмов : учебное пособие / М. М. Глухов, А. Б. Шишков. — Санкт-Петербург : Лань, 2022. — 416 с. — ISBN 978-5-8114-1344-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/210980 — Режим доступа: для авториз.

пользователей.

3. Введение в теоретико-числовые методы криптографии : учебное пособие / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. — Санкт-Петербург : Лань, 2022. — 400 с. — ISBN 978-5-8114-1116-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/210746 — Режим доступа: для авториз. пользователей.

б) дополнительная литература

1. Герман, Олег Николаевич Теоретико-числовые методы в криптографии [Электронный ресурс] : учеб. для студ. учрежд. высш. проф. образования, обуч. по направл. подгот. "Информ. безопасность" и "Математика" / О. Н. Герман. - ЭВК. - М. : Академия, 2012. - Режим доступа: ЭЧЗ "Библиотех". - 20 доступов. - ISBN 978-5-8695-6786-5 (20 экз.)

2. Асанов, М. О. Дискретная математика: графы, матроиды, алгоритмы [Текст] / М. О. Асанов, В. А. Баранский, В. В. Расин. - Электрон. текстовые дан. - Москва : Лань, 2010. - 368 с. - ЭБС "Лань". - неогранич. доступ. - ISBN 978-5-8114-1068-2

в) программное обеспечение

Windows 7 + Microsoft Office

г) интернет-ресурсы, базы данных, информационно-справочные и поисковые системы (при наличии)

1. https://isu.bibliotech.ru — электронно-библиотечная система ИГУ
2. http://e.lanbook.com — электронно-библиотечная система ЛАНЬ
3. http://rucont.ru — электронная библиотека РУКОНТ
4. http://ibooks.ru — электронно-библиотечная система ibooks
5. http://e-library.ru — научная электронная библиотека eLIBRARY
6. http://educa.isu.ru — образовательный портал ИГУ

7. Материально-техническое обеспечение дисциплины (модуля):

Учебная аудитория для проведения занятий лекционного и семинарского типа на 25 посадочных мест, оборудованная специализированной (учебной) мебелью; доска для маркеров, техническими средствами обучения, служащими для представления учебной информации большой аудитории по дисциплине: Моноблок Hewlett-Packard DualCore Intel Core i3-3240, 3.40 GHz; мобильный проектор Epson EB-X12, XGA1024*768.

8. Образовательные технологии:

- Научная электронная библиотека eLIBRARY.RU, более 20 полнотекстовых версий журналов по тематике курса. Доступ с любого компьютера, подключенного через прокси-сервер Иркутского государственного университета.
- Электронная библиотека "Труды ученых ИГУ" (http://ellib.library.isu.ru). Доступ к полным текстам учебных пособий, монографий и статей сотрудников университета, осуществляемый с любого компьютера сети Иркутского государственного университета.

- Общероссийский математический портал **-** информационная система Math-Net.Ru – доступ к российским математическим журналам и обзорам ВИНИТИ РАН
- Журнал "Известия Иркутского университета. Серия Математика". Свободный доступ к электронным полнотекстовым версиям с 2007 г. осуществляется с сайта университета http://www.isu.ru/izvestia
- Архив научных журналов JSTOR (http://www.jstor.org). Доступ с любого компьютера, подключенного через прокси-сервер Иркутского государственного университета.

9. Фонды оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации

9.1 Оценочные средства текущего контроля:

Устный опрос по темам занятий

Показатели	Критерии
Содержание реплик и выступлений	Четкое, научное аргументирование своей позиции. Правильное и уместное использование терминологии.
Корректность поведения	Доброжелательность по отношению к оппонентам. Конструктивная критика мнения собеседника. Способность к компромиссному разрешению спорных моментов. Корректно использует заимствованную аргументацию (делает ссылки на авторов).
Культура общения, организация речевого высказывания	Четкая организация высказывания: связность, логичность, целостность. Естественность речи, отсутствие штампов. Легкость восприятия речи на слух.

Шкала оценивания: 0 баллов – полное отсутствие критерия; 1 балл – частичное выполнение критерия; 2 балла – полное выполнение критерия

60-75% от максимально возможного количества баллов - удовлетворительно,
76-85% от максимально возможного количества баллов - хорошо,
86-100% от максимально возможного количества баллов – отлично.

Сам.работа - решение задач (примеры задач)

1) Покажите, что задача К-РАСРАШИВАЕМОСТЬ ГРАФА лежит в NP. Задача формулируется следующим образом: дан произвольный граф $G = (V, E)$ и натуральное число K. Определить верно ли, что граф можно раскрасить в K цветов (напомним, что К-раскраской графа G называется функция $f : V \to \{1,2,...,K\}$ при этом для $\forall \{u, v\} \in E \Rightarrow f(u) \neq f(v)$, то есть вершины графа, соединенные общим ребром должны быть покрашены в разные цвета). Приведите примеры семейств К- раскрашиваемых графов и графов не являющихся таковыми.

2) Пусть $G = (V, E)$ – произвольный граф (неориентированный, без петель). Докажите, что если $\deg G \leq n - 1$, то граф G – n-раскрашиваем.

3) Покажите, что задача ИЗОМОРФИЗМ ГРАФОВ лежит в NP. Задача формулируется следующим образом: Даны два графа $G_1 = (V_1, E_1), G_2 = (V_2, E_2)$, при этом $|V_1| = |V_2| = n \in \mathbf{N}$ и можно считать, что множества вершин данных графов представлены набором натуральных чисел $\{1,2,...,n\}$. Вопрос: верно ли, что графы G_1 и G_2 изоморфны, то есть существует ли такая перестановка σ на множестве $\{1,2,...,n\}$ в результате которой граф G_1 переходит в граф G_2 (более точно $\sigma \circ G_1 \to G_2$ является изоморфизмом тогда и только тогда (по определению), когда $\{\sigma(u), \sigma(v)\} \in E_2 \Leftrightarrow \{u, v\} \in E_1$). Привести примеры изоморфных графов и указать соответствующие перестановки.

4) Перестановка вершин произвольного графа $G = (V, E)$, переводящая этот граф в себя, называется автоморфизмом данного графа (перестановка σ на множестве вершин переводит граф в себя если и только если (по определению) она инвариантна по отношению к множеству ребер этого графа). Вопрос: сколько автоморфизмов имеет полный граф (клика)?

5) Покажите, что задача ИЗОМОРФИЗМ ПОДГРАФУ является NP-полной (указание: сведите к данной задаче по Карпу распознавательный вариант задачи КЛИКА).

6) Покажите, что задача НЕЗАВИСИМОЕ ПОДМНОЖЕСТВО (НП) NP-полна (указание: используйте результат о связи задачи НП и задачи КЛИКА).

7) Покажите, что задача ВЕРШИННОЕ ПОКРЫТИЕ (ВП) NP-полна (указание: используйте результат о связи задачи ВП и задачи КЛИКА).

8) Дан граф $G = (V, E)$ и натуральное число K. Про граф G известно, что в дополнительном к нему графе $\overline{G} = (V, \overline{E})$ максимальная степень вершины ограничена сверху числом D (не зависящим от $n = |V|$). Постройте полиномиальный (по n) алгоритм решения задачи ВЕРШИННОЕ ПОКРЫТИЕ на исходном графе G.

9) Дана КНФ

$$(x_1 \vee \overline{x}_2 \vee x_3) \cdot (\overline{x}_1 \vee \overline{x}_2 \vee x_4) \cdot (x_2 \vee x_4 \vee \overline{x}_5) \cdot (x_2 \vee x_3 \vee \overline{x}_5 \vee \overline{x}_7) \cdot (x_1 \vee \overline{x}_6 \vee x_7 \vee \overline{x}_8)$$

Сведите проблему SAT для нее к распознавательному варианту задачи 0-1-целочесленное линейное программирование

10)** Постройте полиномиальный алгоритм решения задачи 2-ВЫПОЛНИМОСТЬ.

11) Используя алгоритм динамического программирования, решите следующие задачи о 0-1- рюкзаке:

$$S = \{1,8,3,5,10,12\}, R = 13; \; S = \{9,1,10,7,4\}, R = 14$$

12) Решите задачу РАЗБИЕНИЕ для следующих множеств:

$$S = \{1,9,5,3,8\}; \; S = \{2,10,4,5,7\}.$$

13) Используя ROBDD, решите следующие системы булевых уравнений:

$$\begin{cases} (x_1 \vee x_2) \to x_3 = 1 \\ x_1 \cdot x_2 \oplus x_3 = 0 \end{cases}; \begin{cases} (x_1 \oplus x_2) \vee x_3 = 1 \\ (x_1 \to x_2) \oplus x_3 = 0 \end{cases}$$

14) Найдите ключевые пары для RSA при следующих значениях (p, q):

$$(p, q) = (3,11); (5,7); (3,13).$$

15) Докажите, что из $NP \neq co-NP$ следует $P \neq NP$.

16) Докажите включение: $P \subseteq NP \bigcap co-NP$. С Вашей точки зрения, является ли это включение строгим ?

17) Дана КНФ

$$(x_1 \vee \bar{x}_2 \vee \bar{x}_3) \cdot (\bar{x}_1 \vee x_2) \cdot (x_1 \vee x_3 \vee x_4 \vee \bar{x}_5) \cdot (\bar{x}_2 \vee x_3 \vee \bar{x}_4 \vee x_5) \cdot (\bar{x}_1 \vee \bar{x}_4 \vee \bar{x}_5)$$

Сведите проблему SAT для нее к проблеме поиска корней диофантова уравнения.

18) Дана КНФ

$$(x_1 \vee \bar{x}_2 \vee x_3) \cdot (\bar{x}_1 \vee x_2 \vee \bar{x}_4) \cdot (x_1 \vee \bar{x}_5) \cdot (\bar{x}_2 \vee x_3 \vee \bar{x}_5 \vee \bar{x}_7) \cdot (\bar{x}_1 \vee \bar{x}_6 \vee x_7)$$

Сведите проблему SAT для нее к задаче поиска глобального минимума полинома в $\mathbf{R}^n$.

19) Опишите псевдополиномиальные алгоритмы для задачи вычисления дискретного логарифма в мультипликативной группе по простому модулю и для задачи факторизации произвольного натурального числа.

20) Опишите детерминированный конечный автомат, распознающий все двоичные слова, оканчивающиеся двумя нулями, и постройте схему, представляющую результат работы данного автомата на произвольных словах длины 3.

21)* Дан произвольный детерминированный конечный автомат A_L, распознающий некоторый двоичный язык L, и натуральное число n. Вопрос: верно ли, что в $\{0,1\}^n$ существует слово x, принадлежащее языку L? Покажите, что данная задача принадлежит классу NP. С Вашей точки зрения, принадлежит ли она классу P? Обоснуйте ответ.

22) Докажите, что среди любых шести людей всегда найдутся либо трое попарно знакомых, либо трое попарно незнакомых.

23)* Язык USAT определяется как множество двоичных кодировок всевозможных КНФ, выполнимых на единственном наборе. Покажите, что USAT находится во втором уровне полиномиальной иерархии.

24) Опишите счетное семейство схем, представляющее функцию $f : \{0,1\}^* \to \{1\}$, являющуются тождественной единицей. Является ли данное семейство схем униформным?

25)**Язык PRIMES определяется как язык, образованный двоичными кодировками всевозможных простых чисел. Докажите, что PRIMES находится в $NP \bigcap co-NP$. Дополнение: принадлежность PRIMES co-RP установлена в 70-х года XX века (тесты Соловея-Штрассена и Миллера-Рабина). В 2002 году группой индийских математиков было установлено, что PRIMES лежит в P (соответствующий алгоритм не используется на практике из-за высокой степени полинома, оценивающего его сложность).

26)** Дано натуральное число n. Вопрос: верно ли, что существует простое число $p \in \{1,...,\lfloor \frac{n}{2} \rfloor\}$, являющееся делителем n? Покажите, что данная задача находится в $NP \bigcap co-NP$ (указание: воспользуйтесь тем фактом, что PRIMES лежит в P).

27) Емкостной сложностью (сложностью по памяти) алгоритма A на входе x называется количество ячеек ленты (регистров памяти), задействованных для решения некоторой задачи, закодированной словом x (с момента старта A до момента остановки).

По аналогии с временной сложностью определить емкостную сложность алгоритма A в общем случае. Дать определение задач, разрешимых детерминированным образом на полиномиальной памяти.

28) Показать, что любая задача из NP разрешима детерминированным образом на полиномиальной памяти.

29) Предположим, что входное слово x записывается на рабочую ленту ДМТ (или МНР) в ячейки $h_1,...,h_{|x|}$. Затем запускается программа, которая обязательно останавливается и выдает некоторый ответ. Под промежуточными вычислениями понимаются такие вычисления, оперирующие с содержимым ячеек $h_1,...,h_{|x|}$, в результате которых могут возникать данные, требующие хранения в памяти до определенного момента, для чего используются ячейки, отличные от $h_1,...,h_{|x|}$. Такие ячейки назовем промежуточной памятью. Постройте алгоритм умножения матрицы на вектор, промежуточная память в котором выражается константой, не зависящей от объема входа.

Оценка «отлично» выставляется если, обучающийся знает основную терминологию по теме дисциплины, основные понятия и определения, владеет изученными методами решения задач, умеет решать задачи по дисциплине и приводить анализ полученного решения.

Оценка «хорошо» выставляется, если обучающийся знает основную терминологию по теме дисциплины, основные понятия и определения, и умеет решать задачи по дисциплине изученными методами.

Оценка «удовлетворительно» выставляется, если обучающийся умеет решать базовые задачи по дисциплине изученными методами.

Оценка «неудовлетворительно» выставляется, если обучающийся не знает основную терминологию по теме дисциплины, основные понятия и определения, не владеет изученными методами решения задач и не умеет решать задачи по дисциплине изученными методами и приводить анализ полученного решения.

9.2. Оценочные средства для промежуточной аттестации:

Промежуточная аттестация по дисциплине проходит в форме зачета.

Список вопросов к зачету:

1. Основные классы вычислительной сложности (P, NP, co-NP). Примеры и отличия.
2. Понятие сводимости по Карпу. Основные свойства (рефлексивность и транзитивность). Определение NP-полной задачи.
3. Пример сводимости по Карпу (ГЦ к КОММИВОЯЖЕР).
4. Теорема о консервативных преобразованиях логических уравнений (преобразования Цейтина).
5. Теорема Кука.
6. NP-полнота задачи 3-ВЫП.
7. NP-полнота задачи о совместности системы билинейных уравнений над полем GF(2).
8. NP-полнота задачи «0-1-ЦЛП».
9. NP-полнота задачи КЛИКА.
10. Теорема о связи задач КЛИКА, НЕЗАВИСИМОЕ ПОДМНОЖЕСТВО и ВЕРШИННОЕ ПОКРЫТИЕ (NP-полнота НП и ВП).
11. Задачи 2-С, 3-С, ТП-3 (формулировки, утверждения о сложностной классификации).

12. Задача 0-1-РЮКЗАК и её NP-полнота.
13. Задача РАЗБИЕНИЕ и её NP-полнота.
14. Алгоритм типа «динамическое программирование» для задачи 0-1-РЮКЗАК.
15. Псевдополиномиальные алгоритмы и сильная NP-полнота. Сильная NP-полнота задачи о коммивояжере.
16. Задачи поиска. Оракульная машина Тьюринга и полиномиальная сводимость по Тьюрингу. Определение NP-трудности. Примеры NP-трудных задач.
17. NP-трудность и алгоритмическая неразрешимость. Пример алгоритмически неразрешимой задачи, которая является NP-трудной.
18. Задача об упаковке контейнеров и приближенный алгоритм ее решения.
19. Понятие погрешности приближенных алгоритмов. Примеры. 1-приближенный алгоритм решения задачи построения минимального вершинного покрытия в простом графе.
20. Алгоритм построения вершинного покрытия, не являющийся ε-приближенным.
21. Вероятностные пространства в вычислительных экспериментах. Примеры. Аксиоматика А.Н. Колмогорова.
22. Вероятностные вычислительные модели. Полиномиально ограниченные вероятностные вычисления. Классы RP, co-RP и BPP.
23. Задача проверки натуральных чисел на простоту. Тест Соловея-Штрассена. Задача поиска больших простых чисел.
24. ZPP-алгоритмы (Лас-Вегас -алгоритмы). Соотношения между вероятностными классами.
25. Вероятностный метод в теории графов. Понятие случайного графа. Вероятностное пространство случайных графов.
26. Теорема Рамсея. Числа Рамсея. Вероятностные метод П. Эрдеша получения нижних оценок для чисел Рамсея.
27. Схемы из функциональных элементов. Примеры. Сложность различных реализаций булевых функций.
28. Распознавание языков схемами из функциональных элементов. Классы схемной сложности. Теорема о том, что любой двоичный язык распознается семейством схем экспоненциальной сложности.
29. Класс языков, распознаваемых семействами схем полиномиальной сложности (класс P/poly). Теорема о том, что P/poly содержит алгоритмически нераспознаваемые языки.
30. Теорема Адлмана о включении BPP в P/poly.
31. Теорема Шеннона о сложности почти всех булевых функций.
32. Полиномиальная иерархия, основные определения, примеры.
33. Теорема Стокмейера.
34. Теорема Карпа-Липтона.
35. Односторонние функции и их связь с основной проблемой структурной теории сложности.
36. Сложностной подход к определению псевдослучайного генератора (ПСГ). ПСГ и односторонние функции.
37. Понятие криптографического протокола; примеры. Протокол RSA передачи секретных данных и построение цифровых подписей.
38. Протокол подбрасывания монеты по телефону.
39. Протокол забывающей передачи данных.
40. Проблема аргументации высокой сложности задач обращения некоторых криптографических функций.

Критерии оценки:

- оценка «зачтено» выставляется обучающемуся, если он ответил на вопросы и полностью выполнил предусмотренное в программе курса практическое задание;
- оценка «не зачтено» выставляется обучающемуся, если он не ответил на два вопроса, и не выполнил предусмотренное в программе курса практическое задание.

В случае спорных вопросов, учитываются результаты текущего контроля.

Разработчики:

(подпись)	доцент (занимаемая должность)	Антонова В.С. (инициалы, фамилия)