ЦЕНТРАЛЬНЫЙ УНИВЕРСИТЕТ

УТВЕРЖДЕНА

Решением Ученого совета
АНО ВО «Центральный университет»
«07» марта 2024 г.
Протокол №1

Рабочая программа дисциплины (модуля) «Алгоритмы Advanced»

Направление подготовки: *02.04.01 Математика и компьютерные науки*

Направленность (профиль) подготовки: *Backend-разработка*

Квалификация (степень) выпускника: *магистр*

Форма обучения: *очная*

Срок освоения программы: *2 года*

Год набора: *2024*

Москва
2024

Электронный документ

Содержание

1. Краткая характеристика дисциплины (модуля)

Рабочая программа дисциплины (модуля) «Алгоритмы Advanced» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования – магистратура по специальности 02.04.01 Математика и компьютерные науки, профиль Backend-разработка, утвержденный приказом Министерства науки и высшего образования Российской Федерации № 810 от 23.08.2017 года.

Изучение дисциплины (модуля) «Алгоритмы Advanced» расширяют у студентов знания о методах решения задач и оптимизации процессов, что является ключевым аспектом в программировании и разработке программного обеспечения. Эти навыки позволяют будущим специалистам эффективно анализировать, разрабатывать и внедрять алгоритмические решения, что существенно повышает их конкурентоспособность на рынке труда.

Место дисциплины (модуля) в структуре образовательной программы

Настоящая дисциплина (модуль) включена в учебный план по программе подготовки магистратуры по направлению 02.04.01 Математика и компьютерные науки, профиль Backend-разработка и входит в вариативную часть Блока 1, формируемую участниками образовательных отношений.

Дисциплина (модуль) изучается на 2 курсе в 3 семестре.

Цель изучения дисциплины (модуля): формирование умения разрабатывать, анализировать и эффективно применять алгоритмические методы для решения различных вычислительных задач.

Задачи изучения дисциплины (модуля):

— формирование знаний алгоритмов обхода графов и поиска кратчайших путей;

— формирование знаний динамического программирования как метод решения задач, мемоизация;

— формирование знаний синтаксиса регулярных выражений и их применение в решении алгоритмических задач;

— формирование знаний различных алгоритмов работы со строками;

— формирование знаний классических алгоритмов теории чисел и их применение в криптографии;

— формирование умения использовать регулярные выражения для решения практических задач разработки;

— формирование умения искать кратчайшие пути в графах, особенности и специфики различных вариантов решений;

— формирование умения эффективно решать задачи поиска подстрок и другие классические задачи, связанные с обработкой строк;

— формирование умения реализовывать простейшие алгоритмы обмена ключами для шифрования;

— формирование умения применять классические алгоритмы из области теории графов, теории обработки строк и теории чисел в прикладных задачах.

2. Перечень планируемых результатов обучения

Компетенции, формируемые в результате освоения дисциплины (модуля) при проведении учебных занятий в форме контактной работы обучающихся с педагогическими работниками Университета и в форме самостоятельной работы обучающихся:

Компетенция	Содержание компетенции	Индикатор компетенции	Перечень планируемых результатов обучения по дисциплине (модулю)
УК-6.	Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	УК-6.1.	Знает основные методы самооценки и анализа своей деятельности, а также принципы управления временем и целеполагания
		УК-6.2	Умеет ставить реалистичные и достижимые цели, определять приоритеты в своей деятельности, а также разрабатывать и внедрять планы по совершенствованию своих навыков и компетенций на основе полученной самооценки
		УК-6.3	Имеет практический опыт применения методов самооценки в своей профессиональной деятельности, включая участие в тренингах, семинарах и проектах, направленных на развитие личной эффективности и профессионального роста
ОПК-2.	Способен создавать и исследовать новые математические модели в естественных науках, совершенствовать и разрабатывать концепции, теории и методы	ОПК-2.1.	Знает основные математические модели и методы, используемые в естественных науках, включая статистическое моделирование, дифференциальные уравнения и численные методы, а также современные подходы к исследованию и анализу данных
		ОПК-2.2	Умеет разрабатывать и адаптировать математические модели для решения конкретных проблем в естественных науках, проводить их анализ и верификацию, а также интерпретировать полученные результаты в контексте научных исследований
		ОПК-2.3	Имеет практический опыт создания и исследования математических моделей в рамках научных проектов или

			исследований, включая участие в публикациях, конференциях или коллаборациях, где были разработаны и апробированы новые концепции и методы
ПК-3.	Способен решать задачи профессиональной деятельности, формулировать результат, увидеть следствия полученного результата	ПК-3.1.	Знает основные принципы и методы решения задач профессиональной деятельности, а также способы формулирования и представления результатов, включая анализ последствий и их значимость в контексте проекта
		ПК-3.2.	Умеет применять математические и компьютерные методы для решения конкретных задач, формулировать четкие и обоснованные результаты, а также анализировать их последствия для дальнейших действий и решений
		ПК-3.3.	Имеет практический опыт в решении профессиональных задач, включая участие в проектах, где были получены результаты и проанализированы их следствия, что способствовало принятию обоснованных решений
ПК-4.	Способен публично представлять собственные и известные научные результаты	ПК-4.1.	Знает основные принципы эффективного публичного выступления, методы визуализации данных и основные требования к научным презентациям, включая структуру и содержание
		ПК-4.2.	Умеет четко и логично формулировать свои научные результаты, адаптируя их для различных аудиторий, а также использовать визуальные средства для улучшения восприятия информации
		ПК-4.3.	Имеет практический опыт участия в научных конференциях, семинарах или других мероприятиях, где успешно представлял свои и известные научные результаты, получая обратную связь и взаимодействуя с аудиторией

3. Тематический план

№ п/п	Наименование раздела дисциплины (модуля)	Трудоемкость, академические часы				ТКУ (текущий контроль успеваемости)
		Очная форма				
		Аудиторная работа		Контроль	Самостоятельная работа	
		Лекции	Семинары (практические занятия)			
1	Основы алгоритмов и сложности. Деревья. Алгоритмы обхода	5	5		26	Домашние задания
2	Алгоритмы оптимизации	5	5		28	Домашние задания
3	Вычислительная геометрия. Автоматы	5	5		26	Домашние задания Тест
	Зачет с оценкой			4		
	Итого:	***15***	***15***	***4***	***80***	
Объем дисциплины (модуля) (в ак. ч.)		***114***				
Объем дисциплины (модуля) (в зач. ед.)		***3***				

4. Содержание дисциплины (модуля)

№п/п	Наименование раздела дисциплины (модуля)	Содержание дисциплины (модуля) по темам
1	Основы алгоритмов и сложности. Деревья. Алгоритмы обхода	Понятие задачи динамического программирования. Линейное и квадратичное динамическое программирование: задачи поиска набольших общих/возрастающих подпоследовательностей, 0-1 рюкзак. Динамическое программирование на подотрезках: поиск наибольшей палиндромичной подпоследовательности, задача о минимальном числе умножений в перемножении матриц. Динамическое программирование по подмножествам: решение задачи о максимальной клике и задаче коммивояжера. Понятие графа. Деревья. Алгоритм обхода в глубину, поиск цикла и выделение компонент связности. Компоненты сильной связности, алгоритм Косарайю. Дерево обхода DFS. Поиск мостов и точек сочленения. Алгоритм обхода в ширину (BFS). Понятие взвешенного графа. Вариации BFS: 0-1 BFS, 1-k BFS, 0-k BFS.
2	Алгоритмы оптимизации	Задача поиска кратчайшего пути. Алгоритмы Дейкстры, Форда-Беллмана, Флойда-Уоршелла. Задача поиска наименьшего общего предка. Решение с помощью двоичных подъемов Модульная арфметика. Кольца Z_m. Быстрое возведение в степень. Факторизация. Нахождение обратного в Z_p. Функция Эйлера. Первообразные корни. Основы криптографических алгоритмов. Алгоритмы Диффи-Хеллмана и система RSA
3	Вычислительная геометрия. Автоматы	Вычислительная геометрия: работа с геометрическими примитивами, проверка многоугольника на выпуклость, подсчет площади многоугольника. Задача поиска подстроки. Полиномиальное хеширование. Обобщение на большие размерности. Задача поиска подстроки. Префикс-функция, Z-функция. Структура данных бор. Конечные автоматы: недетерминированные и детерминированные. Автомат Ахо-

		Корасик. Регулярные языки. Работа с регулярными выражениями. Эквивалентность классов регулярных и автоматных языков

5. Учебно-методическое обеспечение

Университет располагает полным набором лицензионного и свободно распространяемого программного обеспечения, включая продукты отечественного производства.

Каждый студент в течение всего периода обучения получает индивидуальный неограниченный доступ к электронно-библиотечной системе и электронной информационно-образовательной среде университета. Эти системы предоставляют возможность доступа к ресурсам из любой точки, где есть подключение к сети Интернет, как на территории университета, так и за его пределами.

Студентам обеспечен удаленный доступ к современным профессиональным базам данных и информационным справочным системам.

Основная литература:

1. Методы оптимизации: теория и алгоритмы : учебник для вузов / А. А. Черняк, Ж. А. Черняк, Ю. М. Метельский, С. А. Богданович. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2025. — 354 с. — (Высшее образование). — ISBN 978-5-534-04103-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/559380.

2. Сухарев, А. Г. Численные методы оптимизации : учебник и практикум для вузов / А. Г. Сухарев, А. В. Тимохов, В. В. Федоров. — 3-е изд., испр. и доп. — Москва : Издательство Юрайт, 2025. — 367 с. — (Высшее образование). — ISBN 978-5-534-17381-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/562179.

Дополнительная литература:

1. Палий, И. А. Линейное программирование : учебник для вузов / И. А. Палий. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2025. — 175 с. — (Высшее образование). — ISBN 978-5-534-04716-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/563472.

6. Материально-техническое обеспечение

Университет располагает материально-технической базой, соответствующей действующим противопожарным правилам и нормам и обеспечивающей проведение всех видов дисциплинарной и междисциплинарной подготовки, практической и научно-исследовательской работ обучающихся, предусмотренных учебным планом.

Помещения, которые представляют собой учебные аудитории для проведения занятий лекционного типа, занятий семинарского (практического) типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования. Помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Изучение дисциплины (модуля) обеспечивается в учебных аудиториях, оснащенных:

— столами и стульями;

— компьютерной техникой;

— специализированным оборудованием, включая демонстрационное оборудование.

Помещения для самостоятельной работы обучающихся, в том числе приспособленные для использования инвалидами и лицами с ограниченными возможностями здоровья, оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к в электронную информационно-образовательную среду Университета.

Обучающимся предоставляется доступ (в том числе удаленный) к ресурсам информационно-телекоммуникационной сети «Интернет», электронным ресурсам (в том числе электронным библиотечным системам, современным профессиональным базам данных и информационным справочным системам):

№	Наименование портала (издания, курса, документа)	Ссылка
1.	Научная электронная библиотека elibrary.ru библиотека	https://elibrary.ru/defaultx.asp
2.	База данных для IT-специалистов	https://habr.com
3.	База данных ScienceDirect	https://www.sciencedirect.com
4.	Официальный сайт Министерства науки и высшего образования Российской Федерации	https://minobrnauki.gov.ru/
5.	Федеральный портал «Российское образование"	https://www.edu.ru/
6.	Информационная система "Единое окно доступа к образовательным ресурсам"	http://window.edu.ru/
7.	Единая коллекция цифровых образовательных ресурсов	http://school-collection.edu.ru/
8.	Федеральный центр информационно - образовательных ресурсов	http://fcior.edu.ru/

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), в том числе комплект лицензионного программного обеспечения, современные профессиональные базы данных и информационные справочные системы:

Наименование ПО	Производство	Лицензионное / свободно распространяемое
Операционные системы:		
Microsoft Imagine (Windows Client, Server)	зарубежное	лицензионное
Браузеры:		
Яндекс.Браузер	отечественное	свободно распространяемое
Google Chrome	зарубежное	свободно распространяемое
Офисные приложения:		
Microsoft Imagine (Visio, OneNote)	зарубежное	лицензионное
TeXstudio	зарубежное	свободно распространяемое
Adobe Acrobat Reader	зарубежное	свободно распространяемое
Программное обеспечение для планирования и учета времени:		
Toggle app	зарубежное	свободно распространяемое
Системы управления проектами:		
Microsoft Imagine (Project)	зарубежное	лицензионное
Системы управления базами данных:		
Microsoft Imagine (SQL Server)	зарубежное	лицензионное
Системы резервного копирования (backup):		
Acronis Backup Advanced for HyperV	зарубежное	лицензионное
Справочно-правовые системы:		
КонсультантПлюс: справочно-правовая система	отечественное	лицензионное
Средства антивирусной защиты:		
Kaspersky Endpoint Security для бизнеса Стандартный Russian Edition	отечественное	лицензионное

Среды разработки:		
Visual Studio Code	зарубежное	свободно распространяемое
Bash (Unix shell)	зарубежное	свободно распространяемое
Anaconda	зарубежное	свободно распространяемое
Robotic Operating System	зарубежное	свободно распространяемое
CopelliaSim	зарубежное	свободно распространяемое
Google Colaboratory	зарубежное	свободно распространяемое
Пакеты программных средств и библиотек:		
AutoPsy	зарубежное	свободно распространяемое
Interactive Disassembler (IDA)	зарубежное	свободно распространяемое
Системы управления библиографической информацией:		
Zotero	зарубежное	свободно распространяемое
Сервисы и службы:		
Bind	зарубежное	свободно распространяемое
Docker	зарубежное	свободно распространяемое

7. Методические и оценочные материалы

Методические указания для обучающихся по освоению дисциплины (модуля)

В процессе изучения дисциплины (модуля) «Алгоритмы Advanced» в рамках текущего контроля успеваемости используются такие виды учебной работы, как лекции, практические занятия, домашние задания, тесты, а также различные виды самостоятельной работы обучающихся по заданию преподавателя, направленные на развитие навыков профессиональной лексики, закрепление практических профессиональных компетенций, поощрение инициатив.

Лекция – систематическое, последовательное, монологическое изложение преподавателем учебного материала, как правило, теоретического характера.

В процессе лекций рекомендуется вести конспект лекций: кратко и схематично фиксировать основные идеи, выводы и обобщения лекции; выделять важные мысли, ключевые слова и термины. Необходимо отметить вопросы или материалы, которые вызывают затруднения, и попытаться найти ответы в рекомендованной литературе. Если разобраться в материале не удается, следует сформулировать вопрос и задать его преподавателю на консультации или во время семинарского (практического) занятия.

Участие в семинаре (практическом занятии) – активная работа студента на семинаре, его ответы на вопросы преподавателя и участие в дискуссии.

Для успешного участия в семинаре студентам рекомендуется заранее ознакомиться с темой обсуждения, прочитать необходимые материалы и подготовить вопросы. Важно активно слушать и вовлекаться в дискуссию, высказывая свои мнения и аргументируя их. При ответах на вопросы преподавателя стоит быть уверенным, четким и логичным, опираясь на изученный материал. Также полезно поддерживать диалог с однокурсниками, чтобы обогатить обсуждение и расширить свои знания.

Домашнее задание – набор задач по темам недели.

При работе над домашними заданиями важно внимательно ознакомиться с требованиями и сроками выполнения. Рекомендуется разбивать задания на этапы, чтобы избежать перегрузки и лучше усвоить материал. Использовать различные источники информации, включая учебники и онлайн-ресурсы, для более глубокого понимания темы.

Тест – особая форма проверки знаний. Проводится после освоения одной или нескольких тем и свидетельствует о качестве понимания основных понятий изучаемого материала. Тестовые задания составлены к ключевым понятиям, основным разделам,

важным терминологическим категориям изучаемой дисциплины (модуля).

Для подготовки к тесту необходимо знать терминологический аппарат дисциплины (модуля), понимать смысл научных категорий и уметь их использовать в профессиональной лексике. Владение понятийным аппаратом, включённым в тестовые задания, позволяет преподавателю быстро проверить уровень понимания студентами важных методологических категорий.

Самостоятельная работа – работа студентов, направленная на углубленное изучение отдельных тем и вопросов учебной дисциплины (модуля).

В процессе самостоятельной работы студенты взаимодействуют с рекомендованными материалами при минимальном участии преподавателя. Задачи студента включают работу с конспектами лекций (обработка текста), повторное изучение учебных материалов планов и тезисов ответов, изучение дополнительных тем, выполнение учебно-исследовательских заданий и другое.

Система оценивания результатов обучения по дисциплине (модулю)

Критерии получения уровня и оценивания сформированности компетенций по дисциплине (модулю) «Алгоритмы Advanced»

Оценивание уровня учебных достижений обучающихся по дисциплине (модулю) осуществляется в виде текущего контроля успеваемости и промежуточной аттестации.

Промежуточная аттестация по дисциплине (модулю) осуществляется в форме ***зачета с оценкой***, при этом проводится оценка компетенций, сформированных по дисциплине.

Для оценивания текущего контроля успеваемости и промежуточной аттестации используется десятибалльная шкала оценивания, которая соотносится с традиционной пятибалльной шкалой следующим образом:

Десятибалльная оценка	**Пятибалльная оценка**	**Оценка за зачет**	**Общая характеристика результата обучения по дисциплине (модулю)**
10	Отлично	Зачтено	Студент полностью владеет знаниями, изложенными в рабочей программе, и глубоко осмысляет дисциплину (модуль). Он самостоятельно и логически последовательно отвечает на все вопросы, акцентируя внимание на наиболее важном. Умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать изученный материал, выделяя ключевые моменты и устанавливая причинно-следственные связи. Четко формулирует ответы, уверенно интерпретирует результаты анализов и других исследований, а также решает сложные задачи. Студент хорошо знаком с методами исследования, необходимыми для практической деятельности, и умеет связывать теоретические аспекты дисциплины (модуля) с практическими
9	Отлично	Зачтено	
8	Отлично	Зачтено	

Десятибалльная оценка	Пятибалльная оценка	Оценка за зачет	Общая характеристика результата обучения по дисциплине (модулю)
			задачами.
7	Хорошо	Зачтено	Студент обладает знаниями предмета почти в полном объеме рабочей программы и самостоятельно, логически последовательно и всесторонне отвечает на все вопросы, акцентируя внимание на наиболее значимых моментах. Он умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать изученный материал, выделяя его ключевые аспекты и устанавливая причинно-следственные связи. Формулирует свои ответы, уверенно интерпретирует результаты анализов и других исследований, а также решает сложные ситуационные задачи. Студент хорошо знаком с методами исследования, необходимыми для практической деятельности, и умеет связывать теоретические аспекты предмета с практическими задачами.
6	Хорошо	Зачтено	
5	Удовлетворительно	Зачтено	Студент обладает базовыми знаниями по дисциплине (модулю), но испытывает трудности при самостоятельных ответах и использует неточные формулировки. В ходе ответов он допускает ошибки, касающиеся сути вопросов. Студент способен решать только самые простые задачи и владеет лишь минимальным набором методов исследования.
4	Удовлетворительно	Зачтено	
3	Не сдан	Не зачтено	Студент не овладел обязательным минимумом знаний по предмету и не может ответить на вопросы, даже если преподаватель задает дополнительные наводящие вопросы.
2	Не сдан	Не зачтено	
1	Не сдан	Не зачтено	

Дисциплина (модуль) «Алгоритмы Advanced» оценивается следующим образом:

Активность	Вес	Описание
Домашние задания	50%	За каждое из заданий можно набрать 10 баллов
Тесты	20%	Ответы на вопросы по изученным темам
Зачет с оценкой	30%	Письменная или устная работа над заданием, направленным на проверку полученных знаний и навыков по дисциплине (модулю)

Формула расчёта итоговой оценки по дисциплине (модулю) «Алгоритмы Advanced»: «0,5 × среднее за домашние задания + 0,2 × среднее за тесты+ 0,3 × зачет с оценкой».

Текущий контроль успеваемости обучающихся по дисциплине (модулю)

Примерные домашние задания

Домашнее задание: **Динамическое программирование на подотрезках**

1. Объясните, что такое палиндромичная подпоследовательность.
2. Напишите рекуррентное соотношение для задачи поиска длины наибольшей палиндромичной подпоследовательности в строке.
3. Для строки "character" найдите длину наибольшей палиндромичной подпоследовательности.
4. Опишите задачу минимального числа умножений при перемножении цепочки матриц.
5. Для последовательности матриц с размерами 10×30, 30×5, 5×60 найдите минимальное число скалярных умножений.

Домашнее задание: **Динамическое программирование по подмножествам**

1. Дайте определение максимальной клики в графе.
2. Опишите, как динамическое программирование по подмножествам используется для решения задачи максимальной клики.
3. Приведите пример графа из 4 вершин и найдите максимальную клику.
4. Опишите задачу коммивояжера и её формулировку для динамического программирования по подмножествам.
5. Для графа из 4 вершин с заданными весами ребер решите задачу коммивояжера методом динамического программирования по подмножествам.

Домашнее задание: **Графы и алгоритмы обхода**

1. Дайте определение графа и дерева. Чем дерево отличается от графа?
2. Опишите алгоритм обхода графа в глубину (DFS).
3. Как с помощью DFS найти циклы в графе?
4. Объясните, что такое компоненты связности в неориентированном графе и как их найти.
5. Опишите алгоритм Косарайю для поиска компонент сильной связности в ориентированном графе.

Примерные задания для тестов

Тест 1.

1. **Что такое наименьший общий предок (НОП)?**
   a) Наименьший элемент в дереве
   b) Наименьший узел, который является предком двух узлов
   c) Наибольший узел в дереве
   d) Узел, который не имеет потомков

2. **Какой алгоритм используется для поиска НОП с помощью двоичных подъемов?**
   a) Алгоритм Дейкстры

b) Алгоритм Флойда-Уоршелла
c) Алгоритм двоичных подъемов
d) Алгоритм Краскала

3. **Что такое модульная арифметика?**
   a) Арифметика с использованием отрицательных чисел
   b) Арифметика с остатками от деления
   c) Арифметика с дробями
   d) Арифметика с комплексными числами

4. **Как обозначается кольцо Z_m?**
   a) Кольцо всех целых чисел
   b) Кольцо целых чисел по модулю m
   c) Кольцо дробных чисел
   d) Кольцо вещественных чисел

5. **Что такое быстрое возведение в степень?**
   a) Метод для нахождения квадратного корня
   b) Метод для быстрого вычисления степеней с использованием двоичного разложения
   c) Метод для нахождения логарифмов
   d) Метод для факторизации чисел

6. **Какова основная цель факторизации?**
   a) Нахождение делителей числа
   b) Нахождение квадратного корня
   c) Нахождение наибольшего общего делителя
   d) Нахождение обратного элемента

7. **Как найти обратный элемент в Z_p?**
   a) Умножить на 0
   b) Использовать алгоритм Евклида
   c) Использовать расширенный алгоритм Евклида
   d) Умножить на 1

8. **Что такое функция Эйлера?**
   a) Функция, подсчитывающая количество делителей числа
   b) Функция, подсчитывающая количество чисел, взаимно простых с n
   c) Функция, вычисляющая факториал числа
   d) Функция, вычисляющая сумму цифр числа

9. **Что такое первообразный корень по модулю p?**
   a) Число, которое делится на p
   b) Число, которое является квадратом по модулю p
   c) Число, которое генерирует все элементы группы Z_p*
   d) Число, которое является делителем p

10. **Какой из следующих алгоритмов используется в криптографии?**
    a) Алгоритм сортировки
    b) Алгоритм Дейкстры
    c) Алгоритм RSA
    d) Алгоритм Краскала

11. **Какова основная идея алгоритма Диффи-Хеллмана?**
    a) Обмен ключами через открытый канал
    b) Шифрование данных
    c) Декодирование сообщений
    d) Создание цифровой подписи

12. **Что такое система RSA?**
    a) Симметричная система шифрования
    b) Ассиметричная система шифрования
    c) Система для генерации случайных чисел
    d) Система для компрессии данных

13. **Какой ключ используется для шифрования в системе RSA?**
    a) Приватный ключ
    b) Открытый ключ
    c) Секретный ключ
    d) Симметричный ключ

14. **Какой из следующих методов используется для генерации ключей в RSA?**
    a) Сложение
    b) Умножение
    c) Факторизация больших чисел
    d) Модульная арифметика

15. **Какой из следующих шагов является первым в алгоритме Диффи-Хеллмана?**
    a) Выбор общего простого числа
    b) Обмен открытыми ключами
    c) Генерация приватного ключа
    d) Шифрование сообщения

Задания для промежуточной аттестации по дисциплине (модулю)

№ п/п	Задание	Ответ	Компетенция
1.	Что такое максимальная клика в графе? A) Подмножество вершин, где каждая пара вершин соединена ребром B) Подмножество вершин, где не все пары соединены ребром C) Подмножество рёбер, соединяющее все вершины графа D) Вершина, которая соединена с максимальным количеством рёбер	A	ОПК-2
2.	Какой алгоритм используется для нахождения компонент сильной связности в ориентированном графе? A) Алгоритм Дейкстры B) Алгоритм Краскала C) Алгоритм Косарайю D) Алгоритм Флойда-Уоршелла	C	ПК-3

3.	Какой метод позволяет быстро находить обратный элемент в кольце Z_p?	Алгоритм Евклида / алгоритм для нахождения НОД / алгоритм нахождения наибольшего общего делителя / Евклидова алгоритм / метод Евклида / алгоритм Евклида для делителей	ПК-4
4.	К чему подходит описание: множество вершин и рёбер	Граф	УК-6
5.	Как вычисляется функция Эйлера для числа n?	Количество натуральных чисел, меньших n и взаимно простых с n	ОПК-2