

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего
образования
"САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ"

Кафедра № 33

УТВЕРЖДАЮ

Руководитель образовательной программы

зав.кафедрой, д.т.н.,проф.

(должность, уч. степень, звание)

С.В. Беззатеев

(инициалы, фамилия)

(подпись)

«20» февраля 2026 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Математические основы обработки информации»
(Наименование дисциплины)

Код направления подготовки/ специальности	10.05.03
Наименование направления подготовки/ специальности	Информационная безопасность автоматизированных систем
Наименование направленности/ специализации	Безопасность открытых информационных систем
Форма обучения	очная
Год приема	2026

Лист согласования рабочей программы дисциплины

Программу составил (а)

зав.кафедрой, д.т.н.,проф.
(должность, уч. степень, звание)

20.02.26

(подпись, дата)

С.В. Беззатеев

(инициалы, фамилия)

Программа одобрена на заседании кафедры № 33

«20» февраля 2026 г, протокол № 7

Заведующий кафедрой № 33

д.т.н.,проф.

(уч. степень, звание)

20.02.26

(подпись, дата)

С.В. Беззатеев

(инициалы, фамилия)

Заместитель директора института №3 по методической работе

доц.,к.т.н.

(должность, уч. степень, звание)

20.02.26

(подпись, дата)

Н.В. Решетникова

(инициалы, фамилия)

Аннотация

Дисциплина «Математические основы обработки информации» входит в образовательную программу высшего образования – программу специалитета по направлению подготовки/ специальности 10.05.03 «Информационная безопасность автоматизированных систем» направленности/специализации «Безопасность открытых информационных систем». Дисциплина реализуется кафедрой «№33».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

УК-1 «Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий»

ПК-9 «Способен осуществлять работы по оценке работоспособности и эффективности применяемых программно-аппаратных средств защиты информации»

ПК-13 «Способен проводить исследования в области оценки эффективности технологий автоматизации открытых информационных систем»

Содержание дисциплины охватывает круг вопросов, связанных с различными аспектами математической обработки информации. Некоторые из них: основные средства представления информации, математические модели как средство работы с информацией, использование элементов логики при работе с информацией, основы комбинаторики и статистической обработки исследовательских данных, числа, множества, операции, отношения, числовые последовательности и числовые функции, случайные события и случайные величины.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, практические занятия, самостоятельная работа обучающегося.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в форме зачета (5 семестр).

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа.

Язык обучения по дисциплине «русский»

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины - сформировать у студентов систему знаний, умений и навыков, связанных с особенностями математических способов представления и обработки информации, как базы для развития общих и профессиональных компетенций.

Задачи дисциплины:

- изучение способов представления информации с помощью математических средств;
- ознакомление с основными математическими моделями и типичными для предметной области задачами их использования;
- формирование системы знаний и умений, необходимых для понимания основ математического моделирования и статистической обработки информации;
- развитие умений переводить информацию с языка предметной области на математический язык, планировать процесс математической обработки экспериментальных данных, проводить практические расчёты с использованием статистических методов и компьютерной поддержки.

1.2. Дисциплина входит в состав части, формируемой участниками образовательных отношений, образовательной программы высшего образования (далее – ОП ВО).

1.3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОП ВО.

В результате изучения дисциплины обучающийся должен обладать следующими компетенциями или их частями. Компетенции и индикаторы их достижения приведены в таблице 1.

Таблица 1 – Перечень компетенций и индикаторов их достижения

Категория (группа) компетенции	Код и наименование компетенции	Код и наименование индикатора достижения компетенции
Универсальные компетенции	УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.В.1 владеть навыками системного и критического мышления; методиками постановки цели, определения способов ее достижения
Профессиональные компетенции	ПК-9 Способен осуществлять работы по оценке работоспособности и эффективности применяемых программно-аппаратных средств защиты информации	ПК-9.3.1 знать методы и средства получения, обработки и передачи информации в операционных системах, системах управления базами данных и компьютерных сетях ПК-9.3.4 знать криптографические алгоритмы и особенности их программной реализации
Профессиональные компетенции	ПК-13 Способен проводить исследования в области оценки эффективности	ПК-13.3.2 знать методы построения и исследования математических моделей в области автоматизации информационно-аналитической деятельности ПК-13.У.1 уметь решать задачи исследования

	технологий автоматизации открытых информационных систем	информационно-аналитических систем методами моделирования
--	---	---

2. Место дисциплины в структуре ОП

Дисциплина базируется на знаниях, ранее приобретенных обучающимися при изучении следующих дисциплин:

- Алгебра и геометрия
- Математическая логика и теория алгоритмов
- Информатика
- Математический анализ
- Алгебра и геометрия
- Дискретная математика
- Теория вероятностей и математическая статистика
- Вычислительная математика

Знания, полученные при изучении материала данной дисциплины, имеют как самостоятельное значение, так и используются при изучении других дисциплин:

- Теория кодирования
- Моделирование систем
- Теория графов и ее приложения

3. Объем и трудоемкость дисциплины

Данные об общем объеме дисциплины, трудоемкости отдельных видов учебной работы по дисциплине (и распределение этой трудоемкости по семестрам) представлены в таблице 2.

Таблица 2 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам
		№5
1	2	3
Общая трудоемкость дисциплины, ЗЕ/ (час)	2/ 72	2/ 72
Из них часов практической подготовки	11	11
Аудиторные занятия, всего час.	51	51
в том числе:		
лекции (Л), (час)	34	34
практические/семинарские занятия (ПЗ), (час)	17	17
лабораторные работы (ЛР), (час)		
курсовой проект (работа) (КП, КР), (час)		
экзамен, (час)		
Самостоятельная работа, всего (час)	21	21
Вид промежуточной аттестации: зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.)	Зачет,	Зачет,

4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий. Разделы, темы дисциплины и их трудоемкость приведены в таблице 3.

Таблица 3 – Разделы, темы дисциплины, их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ) (час)	ЛР (час)	КП/КР (час)	СР (час)
Семестр 5					
Раздел 1. Элементы теории чисел Тема 1.1. Простые числа и "основная" теорема арифметики. Тема 1.2. Полная и приведенная системы вычетов. Тема 1.3. Теорема Эйлера и теорема Ферма. Тема 1.4. Алгоритм Евклида. Тема 1.5. Бинарный алгоритм возведения в степень. Тема 1.6. Китайская теорема об остатках. Тема 1.7. Квадратичные вычеты	10	5			4
Раздел 2. Тесты простоты Тема 2.1. Детерминистические тесты на простоту. Метод пробных делений. Критерий Вильсона. Тест Лукаса. Алгоритм Конягина-Померанса. Тема 2.2. Вероятностные тесты на простоту. Тест Соловея-Штрассена. Тест Рабина-Миллера. Тема 2.3. Построение больших простых чисел	6	6			4
Раздел 3. Задача факторизации составного числа. Тема 3.1. (P-1)-метод Полларда. Ро-метод Полларда. Тема 3.2. Факторизация целых чисел с субэкспоненциальной сложностью. Тема 3.3. Факторизация чисел с помощью квадратичного решета	6	6			5
Раздел 4. Решение квадратных уравнений в вычетной арифметике и дискретное логарифмирование. Тема 4.1. Извлечение корня по простому основанию. Тема 4.2. Извлечение корня по составному основанию. Тема 4.3. Алгоритм сопоставления для извлечения дискретного логарифма. Тема 4.3. Ро-метод Полларда для извлечения дискретного логарифма.	12	0			8
Итого в семестре:	34	17			21
Итого	34	17	0	0	21

4.2. Содержание разделов и тем лекционных занятий.

Содержание разделов и тем лекционных занятий приведено в таблице 4.

Таблица 4 – Содержание разделов и тем лекционного цикла

Номер раздела	Название и содержание разделов и тем лекционных занятий
1	Раздел 1. Элементы теории чисел Тема 1.1. Простые числа и "основная" теорема арифметики. Тема 1.2. Полная и приведенная системы вычетов. Тема 1.3. Теорема Эйлера и теорема Ферма. Тема 1.4. Алгоритм Евклида. Тема 1.5. Бинарный алгоритм возведения в степень. Тема 1.6. Китайская теорема об остатках. Тема 1.7. Квадратичные вычеты
2	Раздел 2. Тесты простоты Тема 2.1. Детерминистические тесты на простоту. Метод пробных делений. Критерий Вильсона. Тест Лукаса. Алгоритм Конягина-Померанса. Тема 2.2. Вероятностные тесты на простоту. Тест Соловея-Штрассена. Тест Рабина-Миллера. Тема 2.3. Построение больших простых чисел
3	Раздел 3. Задача факторизации составного числа. Тема 3.1. (P-1)-метод Полларда. Ро-метод Полларда. Тема 3.2. Факторизация целых чисел с субэкспоненциальной сложностью. Тема 3.3. Факторизация чисел с помощью квадратичного решета
4	Раздел 4. Решение квадратных уравнений в вычетной арифметике и дискретное логарифмирование. Тема 4.1. Извлечение корня по простому основанию. Тема 4.2. Извлечение корня по составному основанию. Тема 4.3. Алгоритм сопоставления для извлечения дискретного логарифма. Тема 4.3. Ро-метод Полларда для извлечения дискретного логарифма.

4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Практические занятия и их трудоемкость

№ п/п	Темы практических занятий	Формы практических занятий	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Семестр 5					
1	Элементы теории чисел	Решение задач	3	3	1
2	Тесты простоты	Решение задач	3	3	2
3	Задача факторизации составного числа	Решение задач	3	3	3
4	Решение квадратных уравнений в модульной	Решение задач	4	4	4

	арифметике.				
5	Задача поиска дискретного логарифма.	Решение задач	3	3	4
Всего			17	17	

4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 6.

Таблица 6 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Учебным планом не предусмотрено				
Всего				

4.5. Выполнение курсового проекта/ курсовой работы

Учебным планом не предусмотрено

4.6. Самостоятельная работа обучающихся

Виды самостоятельной работы и ее трудоемкость приведены в таблице 7.

Таблица 7 – Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 5, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	10	10
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю успеваемости (ТКУ)	5	5
Домашнее задание (ДЗ)		
Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)	6	6
Всего:	21	21

5. Перечень учебно-методического обеспечения

для самостоятельной работы обучающихся по дисциплине (модулю)

Учебно-методические материалы для самостоятельной работы обучающихся указаны в п.п. разделов 6-11.

6. Перечень печатных и электронных учебных изданий

Перечень печатных и электронных учебных изданий приведен в таблице 8.

Таблица 8– Перечень печатных и электронных учебных изданий

Шифр/ URL адрес	Библиографическая ссылка	Количество экземпляров в библиотеке (кроме электронных экземпляров)
	Коробейников, А.Г. Математические основы криптологии. [Электронный ресурс] / А.Г. Коробейников, Ю.А. Гатчин. — Электрон. дан. — СПб. : НИУ ИТМО, 2004. — 106 с. — Режим доступа: http://e.lanbook.com/book/43393 — Загл. с экрана.	
[519.6/.8 Л 17]	Лазарева С.В., Овчинников А.А. Лекции по математическим основам криптологии. ГУАП, 2006	79
512 К72	А.И. Кострикин. Введение в алгебру. М., Наука ФМ, 1977	12
51 В49	И.М. Виноградов. Основы теории чисел. М., Наука ФМ., 1980	5
519.6/.8 А 40	А. Акритас. Основы компьютерной алгебры с приложениями. М., Мир, 1994	1
519.6/.8 К53	Д. Кнут. Искусство программирования для ЭВМ. Т.2: Получисленные алгоритмы. М., Вильямс, 2005	22
004 К84	Крук Е.А., Линский Е.М. Криптография с открытым ключом. Кодовые системы. ГУАП, 2004.	20
519.6/.8 Ф 76	Дискретная математика и криптология [Текст] : курс лекций / В. М. Фомичев ; ред. Н. Д. Подуфалов. - М. : Диалог-МИФИ, 2010. - 400 с.	1

7. Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины приведен в таблице 9.

Таблица 9 – Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

URL адрес	Наименование
https://pro.guap.ru/	Материалы для выполнения практических работ, индивидуальные варианты для их выполнения, а также электронный лекционный материал по дисциплине размещаются внутри ЭИОС ГУАП «Интегрированная среда обучения» в течение учебного семестра

8. Перечень информационных технологий

8.1. Перечень программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине.

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10– Перечень программного обеспечения

№ п/п	Наименование
https://pro.guap.ru/	Материалы для выполнения практических работ, индивидуальные варианты для их выполнения, а также электронный лекционный

	материал по дисциплине размещаются внутри ЭИОС ГУАП «Интегрированная среда обучения» в течение учебного семестра
https://pro.guap.ru/	Материалы для выполнения практических работ, индивидуальные варианты для их выполнения, а также электронный лекционный материал по дисциплине размещаются внутри ЭИОС ГУАП «Интегрированная среда обучения» в течение учебного семестра
https://pro.guap.ru/	Материалы для выполнения практических работ, индивидуальные варианты для их выполнения, а также электронный лекционный материал по дисциплине размещаются внутри ЭИОС ГУАП «Интегрированная среда обучения» в течение учебного семестра

8.2. Перечень информационно-справочных систем,используемых при осуществлении образовательного процесса по дисциплине

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11– Перечень информационно-справочных систем

№ п/п	Наименование
1	ЭБС Znanium (https://znanium.ru/), доступ через личный кабинет читателя библиотеки ГУАП, а также по IP -адресам ГУАП
2	ЭБС «Лань» (https://e.lanbook.com/), доступ через личный кабинет читателя библиотеки ГУАП, а также по IP -адресам ГУАП
3	Электронный каталог библиотеки ГУАП с доступом к базе полнотекстовых изданий (https://lib.guap.ru/), доступ через личный кабинет читателя библиотеки ГУАП

9. Материально-техническая база

Состав материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине, представлен в таблице12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
1	Мультимедийная лекционная аудитория: Специализированная мебель; технические средства обучения, служащие для представления учебной информации большой аудитории; набор демонстрационного оборудования. Обеспечен доступ в электронную информационно-образовательную среду ГУАП по точке доступа Wi-Fi.	
2	Лаборатория компьютерного моделирования: – специализированная мебель; – технические средства обучения, служащие для представления учебной информации; панель интерактивная/телевизор; Лабораторное оборудование: ПЭВМ – «Место рабочее автоматизированное» – 13 шт. Обеспечен доступ в электронную информационно-образовательную среду	52-46, 52-44 (ул. Большая Морская, д.67, лит. А)

	ГУАП по локальной вычислительной сети.	
3	Помещение для самостоятельной работы, Интернет-класс. Специализированная мебель, возможность подключения к сети «Интернет» и доступ в электронную информационно-образовательную среду организации. 10 ПК, Принтер лазерный HPLJP4515n, Принтер HP LaserJetEnterprise 600 M602dn.	14-34 (ул. Большая Морская, д.67, лит. А)
4	Помещение для самостоятельной работы обучающихся - Читальный зал библиотеки ГУАП: специализированная мебель; персональные компьютеры – 10 шт., обеспечен доступ в электронную информационно-образовательную среду ГУАП по локальной вычислительной сети и точке доступа WiFi, а также к электронно-библиотечным системам, реферативной базе данных Scopus; копировальный аппарат Kyocera KM2035	22-19 (ул. Большая Морская, д.67, лит. А)

10. Оценочные средства для проведения промежуточной аттестации

10.1. Состав оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине приведен в таблице 13.

Таблица 13 – Состав оценочных средств для проведения промежуточной аттестации

Вид промежуточной аттестации	Перечень оценочных средств
Зачет	Список вопросов; Тесты; Задачи.

10.2. В качестве критериев оценки уровня сформированности (освоения) компетенций обучающимися применяется 5-балльная шкала оценки сформированности компетенций, которая приведена в таблице 14. В течение семестра может использоваться 100-балльная шкала модульно-рейтинговой системы Университета, правила использования которой, установлены соответствующим локальным нормативным актом ГУАП.

Таблица 14 – Критерии оценки уровня сформированности компетенций

Оценка компетенции	Характеристика сформированных компетенций
5-балльная шкала	
«отлично» «зачтено»	Обучающийся: – глубоко и всесторонне усвоил программный материал; – уверенно, логично, последовательно и грамотно его излагает; – опираясь на знания основной и дополнительной литературы, тесно связывает усвоенные научные положения с практической деятельностью направления; – умело обосновывает и аргументирует выдвигаемые им идеи; – делает выводы и обобщения; – свободно владеет системой специализированных понятий. – правильно выполнил от 90% до 100% тестовых заданий ^{**} .
«хорошо» «зачтено»	Обучающийся: – твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; – не допускает существенных неточностей; – увязывает усвоенные знания с практической деятельностью направления; – аргументирует научные положения; – делает выводы и обобщения; – владеет системой специализированных понятий.

Оценка компетенции	Характеристика сформированных компетенций
5-балльная шкала	
	– правильно выполнил от 70% до 89% тестовых заданий ^{**} .
«удовлетворительно» «зачтено»	– обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; – допускает несущественные ошибки и неточности; – испытывает затруднения в практическом применении знаний направления; – слабо аргументирует научные положения; – затрудняется в формулировании выводов и обобщений; – частично владеет системой специализированных понятий. – правильно выполнил от 51% до 69% тестовых заданий ^{**} .
«неудовлетворительно» «не зачтено»	– обучающийся не усвоил значительной части программного материала; – допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; – испытывает трудности в практическом применении знаний; – не может аргументировать научные положения; – не формулирует выводов и обобщений. – правильно выполнил менее 51% тестовых заданий ^{**} .

10.3. Типовые контрольные задания или иные материалы.

Вопросы (задачи) для экзамена представлены в таблице 15.

Таблица 15 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена	Код индикатора
	Учебным планом не предусмотрено	

Вопросы (задачи) для зачета / дифф. зачета представлены в таблице 16.

Таблица 16 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифф. зачета	Код индикатора
1	Простые числа и "основная" теорема арифметики. Полная и приведенная системы вычетов. Теорема Эйлера и теорема Ферма. Алгоритм Евклида. Бинарный алгоритм возведения в степень. Китайская теорема об остатках.	УК-1.В.1
2	Тест Лукаса. Алгоритм Конягина-Померанса. Детерминистические и вероятностные тесты на простоту. Тест Соловея-Штрассена. Тест Рабина-Миллера. Построение больших простых чисел Задача факторизации составного числа. (P-1)-метод Полларда. Ро-метод Полларда. Факторизация чисел с помощью квадратичного решета.	ПК-9.3.1
3	Извлечения корня по модулю простого числа.	ПК-9.3.4

	Извлечение корня по составному основанию.	
4	Определение дискретного логарифма. Алгоритм сопоставления. Ро-алгоритм Полларда для поиска дискретного логарифма.	ПК-13.3.2
5	Квадратичные вычеты Метод пробных делений. Критерий Вильсона.	ПК-13.У.1

Перечень тем для выполнения курсового проекта/ курсовой работы представлены в таблице 17.

Таблица 17 – Перечень тем для выполнения курсового проекта / курсовой работы

№ п/п	Примерный перечень тем для выполнения курсового проекта/ курсовой работы
	Учебным планом не предусмотрено

Вопросы для проведения промежуточной аттестации в виде тестирования представлены в таблице 18.

Таблица 18 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
1	1. Что является базовым объектом алгебры высказываний? 1. Множество 2. Высказывание 3. Граф 4. Функция Правильный ответ: 2 2. Какая логическая операция соответствует союзу «И»? 1. Дизъюнкция 2. Импликация 3. Конъюнкция 4. Отрицание Правильный ответ: 3 3. Чему равен результат логического сложения (дизъюнкции) высказываний 1 И 0? 1. 0 2. 1 3. Неопределенно 4. 2 Правильный ответ: 2	УК-1.В.1
2	1. Что является базовым объектом алгебры высказываний? 1. Множество 2. Высказывание 3. Граф 4. Функция Правильный ответ: 2 2. Какая логическая операция соответствует союзу «И»? 1. Дизъюнкция 2. Импликация 3. Конъюнкция 4. Отрицание Правильный ответ: 3	ПК-9.3.1

	3. Чему равен результат логического сложения (дизъюнкции) высказываний 1 И 0? 0 1 - Неопределенно 2 Правильный ответ: 2	
3	8. Совокупность объектов, обладающих общим свойством, в математике называется: - Графом - Множеством - Алгоритмом - Сигналом Правильный ответ: 2 9. Какая операция над множествами объединяет элементы, принадлежащие хотя бы одному из множеств? - Пересечение - Объединение - Разность - Дополнение Правильный ответ: 2 10. Как называется множество, не содержащее ни одного элемента? - Универсальное - Пустое - Бесконечное - Булево Правильный ответ: 2	ПК-9.3.4
4	12. Какое отношение называется отношением эквивалентности? - Рефлексивное, симметричное и транзитивное - Только рефлексивное - Антисимметричное - Асимметричное Правильный ответ: 1 13. Граф состоит из: - Вершин и ребер - Столбцов и строк - Чисел и знаков - Точек и плоскостей Правильный ответ: 1 14. Если ребра графа имеют направление, то граф называется: - Неориентированным - Ориентированным (орграфом) - Связным - Полным Правильный ответ: 2	ПК-13.3.2
5	15. Что показывает степень вершины графа? - Длину пути - Количество инцидентных ей ребер - Вес вершины - Удаленность от начала Правильный ответ: 2	ПК-13.У.1

16. Какой путь в графе называется эйлеровым? 1. Проходящий через все вершины по одному разу 2. Проходящий через все ребра ровно по одному разу 3. Самый короткий путь 4. Замкнутый цикл минимальной длины Правильный ответ: 2 17. Какая мера количества информации по К. Шеннону используется для дискретных случайных величин? 1. Энтропия 2. Дисперсия 3. Ковариация 4. Медиана Правильный ответ: 1 18. При каком условии энтропия источника сообщений максимальна? 1. Когда все сообщения равновероятны 2. Когда одно сообщение достоверно, а остальные невозможны 3. Когда вероятности равны нулю 4. Энтропия не зависит от вероятностей Правильный ответ: 1 19. Какое кодирование позволяет восстановить исходный текст без потерь? 1. Кодирование с потерями 2. Однозначно декодируемое (без потерь) 3. Случайное 4. Аналоговое Правильный ответ: 2 20. Что такое избыточность информации? 1. Полезный объем данных 2. Дополнительная доля информации, используемая для защиты от ошибок или сжатия 3. Полная потеря данных 4. Шум в канале связи Правильный ответ: 2 21. Какая теорема К. Шеннона описывает пропускную способность канала связи при наличии шума? 1. Первая теорема Шеннона 2. Вторая теорема Шеннона (теорема кодирования для канала с шумом) 3. Теорема Байеса 4. Теорема о среднем значении Правильный ответ: 2 22. Какое кодовое расстояние по Хеммингу необходимо для обнаружения до $\lfloor s \rfloor$ ошибок? 1. $\lfloor s + 1 \rfloor$ 2. $\lfloor s \rfloor$ 3. $\lfloor 2s \rfloor$ 4. $\lfloor 1 \rfloor$ Правильный ответ: 1 23. Какой метод сжатия данных использует частые коды для частых символов и длинные для редких (построение дерева)? 1. Метод Хаффмана	
---	--

	2. Метод перебора 3. Метод Гаусса 4. Метод наименьших квадратов Правильный ответ: 1 24. Что из перечисленного является дискретным каналом передачи информации? 1. Обычный проводной телефонный разговор без оцифровки 2. Линия оптической связи, передающая битовый поток 3. Непрерывный радиоэфир 4. Звуковая волна в воздухе Правильный ответ: 2	
--	---	--

Перечень тем контрольных работ по дисциплине обучающихся заочной формы обучения, представлены в таблице 19.

Таблица 19 – Перечень контрольных работ

№ п/п	Перечень контрольных работ
	Не предусмотрено

10.4. Методические материалы, определяющие процедуры оценивания индикаторов, характеризующих этапы формирования компетенций, содержатся в локальных нормативных актах ГУАП, регламентирующих порядок и процедуру проведения текущего контроля успеваемости и промежуточной аттестации обучающихся ГУАП.

11. Методические указания для обучающихся по освоению дисциплины

Методические указания для обучающихся по освоению лекционного материала

Основное назначение лекционного материала – логически стройное, системное, глубокое и ясное изложение учебного материала. Назначение современной лекции в рамках дисциплины не в том, чтобы получить всю информацию по теме, а в освоении фундаментальных проблем дисциплины, методов научного познания, новейших достижений научной мысли. В учебном процессе лекция выполняет методологическую, организационную и информационную функции. Лекция раскрывает понятийный аппарат конкретной области знания, её проблемы, дает цельное представление о дисциплине, показывает взаимосвязь с другими дисциплинами.

Планируемые результаты при освоении обучающимися лекционного материала:

- получение современных, целостных, взаимосвязанных знаний, уровень которых определяется целевой установкой к каждой конкретной теме;
- получение опыта творческой работы совместно с преподавателем;
- развитие профессионально–деловых качеств, любви к предмету и самостоятельного творческого мышления.
- появление необходимого интереса, необходимого для самостоятельной работы;
- получение знаний о современном уровне развития науки и техники и о прогнозе их развития на ближайшие годы;
- научиться методически обрабатывать материал (выделять главные мысли и положения, приходить к конкретным выводам, повторять их в различных формулировках);
- получение точного понимания всех необходимых терминов и понятий.

Лекционный материал может сопровождаться демонстрацией слайдов и использованием раздаточного материала при проведении коротких дискуссий об особенностях применения отдельных тематик по дисциплине.

Структура предоставления лекционного материала:

Раздел 1. Элементы теории чисел

Тема 1.1. Простые числа и "основная" теорема арифметики.

Тема 1.2. Полная и приведенная системы вычетов.

Тема 1.3. Теорема Эйлера и теорема Ферма.

Тема 1.4. Алгоритм Евклида.

Тема 1.5. Бинарный алгоритм возведения в степень.

Тема 1.6. Китайская теорема об остатках.

Тема 1.7. Квадратичные вычеты

Раздел 2. Тесты простоты

Тема 2.1. Детерминистические тесты на простоту. Метод пробных делений. Критерий Вильсона. Тест Лукаса. Алгоритм Конягина-Померанса.

Тема 2.2. Вероятностные тесты на простоту. Тест Соловея-Штрассена. Тест Рабина-Миллера.

Тема 2.3. Построение больших простых чисел

Раздел 3. Задача факторизации составного числа.

Тема 3.1. (P-1)-метод Полларда. Ро-метод Полларда.

Тема 3.2. Факторизация целых чисел с субэкспоненциальной сложностью.

Тема 3.3. Факторизация чисел с помощью квадратичного решета

Раздел 4. Решение квадратных уравнений в вычетной арифметике и дискретное логарифмирование.

Тема 4.1. Извлечение корня по простому основанию.

Тема 4.2. Извлечение корня по составному основанию.

Тема 4.3. Алгоритм сопоставления для извлечения дискретного логарифма.

Тема 4.3. Ро-метод Полларда для извлечения дискретного логарифма..

Методические указания для обучающихся по прохождению практических занятий

Практическое занятие является одной из основных форм организации учебного процесса, заключающейся в выполнении обучающимися под руководством преподавателя комплекса учебных заданий с целью усвоения научно-теоретических основ учебной дисциплины, приобретения умений и навыков, опыта творческой деятельности.

Целью практического занятия для обучающегося является привитие обучающемуся умений и навыков практической деятельности по изучаемой дисциплине.

Планируемые результаты при освоении обучающимся практических занятий:

- закрепление, углубление, расширение и детализация знаний при решении конкретных задач;
- развитие познавательных способностей, самостоятельности мышления, творческой активности;
- овладение новыми методами и методиками изучения конкретной учебной дисциплины;
- выработка способности логического осмысления полученных знаний для выполнения заданий;
- обеспечение рационального сочетания коллективной и индивидуальной форм обучения.

Функции практических занятий:

- познавательная;
- развивающая;
- воспитательная.

По характеру выполняемых обучающимся заданий по практическим занятиям подразделяются на:

- ознакомительные, проводимые с целью закрепления и конкретизации изученного теоретического материала;
- аналитические, ставящие своей целью получение новой информации на основе формализованных методов;
- творческие, связанные с получением новой информации путем самостоятельно выбранных подходов к решению задач.

Формы организации практических занятий определяются в соответствии со специфическими особенностями учебной дисциплины и целями обучения. Они могут проводиться:

- в интерактивной форме (решение ситуационных задач, занятия по моделированию реальных условий, деловые игры, игровое проектирование, имитационные занятия, выездные занятия в организации (предприятия), деловая учебная игра, ролевая игра, психологический тренинг, кейс, мозговой штурм, групповые дискуссии);
- в не интерактивной форме (выполнение упражнений, решение типовых задач, решение ситуационных задач и другое).

Методика проведения практического занятия может быть различной, при этом важно достижение общей цели дисциплины.

Требования к проведению практических занятий

Практические занятия проводятся в виде разбора и решения задач. По каждой теме предусмотрено выполнение ряда задач. Контроль и закрепление знаний по каждой теме осуществляется в виде опроса у доски, аудиторных контрольных работ и домашних заданий.

Методические указания для обучающихся по прохождению самостоятельной работы

В ходе выполнения самостоятельной работы, обучающийся выполняет работу по заданию и при методическом руководстве преподавателя, но без его непосредственного участия. Для обучающихся по заочной форме обучения, самостоятельная работа может включать в себя контрольную работу.

В процессе выполнения самостоятельной работы, у обучающегося формируется целесообразное планирование рабочего времени, которое позволяет им развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивает высокий уровень успеваемости в период обучения, помогает получить навыки повышения профессионального уровня.

Методическими материалами, направляющими самостоятельную работу обучающихся являются:

- учебно-методический материал по дисциплине;
- методические указания по выполнению контрольных работ (для обучающихся по заочной форме обучения).

Методические указания для обучающихся по прохождению промежуточной аттестации

Промежуточная аттестация обучающихся предусматривает оценивание промежуточных и окончательных результатов обучения по дисциплине. Она включает в себя:

- зачет – это форма оценки знаний, полученных обучающимся в ходе изучения учебной дисциплины в целом или промежуточная (по окончании семестра) оценка знаний обучающимся по отдельным разделам дисциплины с аттестационной оценкой «зачтено» или «не зачтено».

Система оценок при проведении промежуточной аттестации осуществляется в соответствии с требованиями Положений «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программам высшего образования» и «О модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП»

Лист внесения изменений в рабочую программу дисциплины

Дата внесения изменений и дополнений. Подпись внесшего изменения	Содержание изменений и дополнений	Дата и № протокола заседания кафедры	Подпись зав. кафедрой