

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

Кафедра № 33

УТВЕРЖДАЮ  
 Руководитель направления  
 проф. д.т.н., доц.  
 (должность, уч. степень, звание)

С.В. Беззатеев  
 (подпись, фамилия)  
 (подпись)  
 «26» мая 2022 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	Безопасность открытых информационных систем
Форма обучения	очная

Лист согласования рабочей программы дисциплины

Программу составил (а)

д.т.н., доц.  
 (должность, уч. степень, звание)

  
 26.05.22  
 (подпись, дата)

С.В. Беззатеев  
 (подпись, фамилия)

Программа одобрена на заседании кафедры № 33

«27» мая 2021 г., протокол № 10

Заведующий кафедрой № 33

д.т.н., доц.  
 (уч. степень, звание)

  
 26.05.22  
 (подпись, дата)

С.В. Беззатеев  
 (подпись, фамилия)

Ответственный за ОП ВО 10.05.03(05)

доц. к.т.н., доц.  
 (должность, уч. степень, звание)

  
 26.05.22  
 (подпись, дата)

В.А. Мызынков  
 (подпись, фамилия)

Заместитель директора института №3 по методической работе

(должность, уч. степень, звание)

  
 26.05.22  
 (подпись, дата)

Н.В. Решетникова  
 (подпись, 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 «Безопасность открытых информационных систем». Дисциплина реализуется кафедрой «№33».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

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

ПК-12 «Способен проводить исследования в области оценки эффективности технологий автоматизации открытых информационных систем»

Содержание дисциплины охватывает круг вопросов, связанных с методами классической и современной алгебры и теории чисел, применяемых в криптографии, алгебраическими методами решения ряда основных задач, возникающих при синтезе криптографических алгоритмов.

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

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

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов.

Язык обучения по дисциплине «русский»

## 1. Перечень планируемых результатов обучения по дисциплине

### 1.1. Цели преподавания дисциплины

Целью преподавания дисциплины является: обеспечение фундаментальной математической подготовки в одной из наиболее важных областей современной прикладной математики – криптографии; ознакомление с рядом методов классической и современной алгебры и теории чисел, применяемых в криптографии, обучение алгебраическим методам решения ряда основных задач, возникающих при синтезе криптографических алгоритмов.

В процессе обучения студент должен получить фундаментальные теоретические знания и приобрести практические навыки в области построения и анализа вычислительно трудных теоретико-числовых функций, а также применения этих функций в задачах защиты информации.

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
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-12 Способен проводить исследования в области оценки эффективности технологий автоматизации открытых информационных систем	ПК-12.3.2 знать методы построения и исследования математических моделей в области автоматизации информационно-аналитической деятельности ПК-12.У.1 уметь решать задачи исследования 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
- Исследование операций и теории игр
- 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
<b>Общая трудоемкость дисциплины, ЗЕ/ (час)</b>	3/ 108	3/ 108
<b>Из них часов практической подготовки</b>	17	17
<b>Аудиторные занятия, всего час.</b>	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)		
<b>Самостоятельная работа, всего (час)</b>	57	57
<b>Вид промежуточной аттестации:</b> зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.**)	Зачет	Зачет

Примечание: \*\* кандидатский экзамен

### 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 (час)	СРС (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.	10	5			10

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 Соловья-Штрассена. Тест Рабина-Миллера. Тема 2.3. Построение больших простых чисел	6	6			10
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			10
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			27
Итого в семестре:	34	17			57
Итого	34	17	0	0	57

Практическая подготовка заключается в непосредственном выполнении обучающимися определенных трудовых функций, связанных с будущей профессиональной деятельностью.

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 Соловья-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 арифметике.	Решение задач	4	4	4
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. Курсовое проектирование/ выполнение 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)	30	30
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю успеваемости (ТКУ)	7	7
Домашнее задание (ДЗ)		
Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)	10	10
Всего:	57	57

#### 5. Перечень учебно-методического обеспечения

для самостоятельной работы обучающихся по дисциплине (модулю)

Учебно-методические материалы для самостоятельной работы обучающихся указаны в п.п. 7-11.

#### 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: <a href="http://e.lanbook.com/book/43393">http://e.lanbook.com/book/43393</a> — 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
<a href="http://e.lanbook.com/view/book/46/">http://e.lanbook.com/view/book/46/</a>	Виноградов И.М. Основы теории чисел. Лань, 2009.
<a href="http://e.lanbook.com/view/book/1540/">http://e.lanbook.com/view/book/1540/</a>	Глухов М. М., Круглов И. А., Пичкур А. Б., Черемушкин А. В. Введение в теоретико-числовые методы криптографии. Лань, 2011.
<a href="http://e.lanbook.com/view/book/3506/">http://e.lanbook.com/view/book/3506/</a>	Федунец Н.И., Куприянов В.В. Теория принятия решений. Горная книга, 2004.

#### 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
	Не предусмотрено

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
-------	--------------



Не предусмотрено
------------------

### 9. Материально-техническая база

Состав материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине, представлен в таблице 12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
1	Лекционная аудитория	
2	Класс для практических занятий	

### 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 5-балльная шкала	Характеристика сформированных компетенций
«отлично» «зачтено»	– обучающийся глубоко и всесторонне усвоил программный материал; – уверенно, логично, последовательно и грамотно его излагает; – опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления; – умело обосновывает и аргументирует выдвигаемые им идеи; – делает выводы и обобщения; – свободно владеет системой специализированных понятий.
«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	
«удовлетворительно» «зачтено»	<ul style="list-style-type: none"> <li>– обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы;</li> <li>– допускает несущественные ошибки и неточности;</li> <li>– испытывает затруднения в практическом применении знаний направления;</li> <li>– слабо аргументирует научные положения;</li> <li>– затрудняется в формулировании выводов и обобщений;</li> <li>– частично владеет системой специализированных понятий.</li> </ul>
«неудовлетворительно» «не зачтено»	<ul style="list-style-type: none"> <li>– обучающийся не усвоил значительной части программного материала;</li> <li>– допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении;</li> <li>– испытывает трудности в практическом применении знаний;</li> <li>– не может аргументировать научные положения;</li> <li>– не формулирует выводов и обобщений.</li> </ul>

### 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. Квадратичные вычеты Метод пробных делений. Критерий Вильсона.	ПК-9.3.1
2	Тест Лукаса. Алгоритм Конягина-Померанса. Детерминистические и вероятностные тесты на простоту. Тест Соловья-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-9.3.4
3	Извлечения корня по модулю простого числа. Извлечение корня по составному основанию.	ПК-12.3.2
4	Определение дискретного логарифма. Алгоритм сопоставления.	ПК-12.У.1

	Ро-алгоритм Полларда для поиска дискретного логарифма.	
--	--	--

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

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

№ п/п	Примерный перечень тем для курсового проектирования/выполнения 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
	<p>Примеры заданий по теме: Элементы теории чисел</p> <p>Задание 1. Вычислить:  <math>(5 \cdot 7 - 83) \bmod 27</math>  <math>(5 : 29 + 7) \bmod 25</math>  <math>(8 : 6 - 9) \bmod 33</math></p> <p>Задание 2. Нахождение мультипликативных обратных с помощью расширенного алгоритма Евклида. Пример задания: Вычислить: <math>11^{-1} \bmod 47</math></p> <p>Задание 3. Бинарный алгоритм возведения в степень. Пример задания: Вычислить: <math>26^{67} \bmod 97</math>.</p> <p>Задание 4. Китайская теорема об остатках. Пример задания:  <math>X \bmod 5 = 2</math>  <math>X \bmod 7 = 6</math>  <math>X \bmod 12 = 8</math>  Найти X.</p> <p>Задание 5. Квадратичные вычеты. Примеры заданий:  1. Вычислить символ Лежандра для 3 по модулю 17.  2. Вычислить символ Якоби для числа 8 по модулю 15.  3. Выяснить является ли число 6 квадратичным вычетом по модулю 11.</p> <p>Примеры заданий по теме: Тесты простоты: Проверить на простоту число 71  a) методом пробного деления  b) тестом Миллера-Рабина  c) По теореме Ферма  d) методом Соловья-Штрассена</p> <p>Примеры заданий по теме: Факторизация чисел: Разложить на множители число 63  a) методом деления</p>	

b)	(p-1)-методом Полларда	
c)	Po-методом Полларда	
d)	методом Ферма	

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

Целью дисциплины является – получение студентами необходимых знаний, умений и навыков в области алгебраических методов криптографии, создание поддерживающей образовательной среды преподавания криптографических методов и средств защиты информации, предоставление возможности студентам развить и продемонстрировать навыки в области дискретной математики, компьютерной алгебры и алгебраической алгоритмики.

#### **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 обучающимся 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