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

Кафедра №34

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

С.В. Беззатеев
(подпись)

«25» мая 2018 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Математические основы обработки информации»
(Название дисциплины)

Код специальности	10.05.03
Наименование специальности	Информационная безопасность автоматизированных систем
Наименование специализации	Обеспечение информационной безопасности распределенных информационных систем
Форма обучения	очная

Санкт-Петербург 2018 г.

Лист согласования рабочей программы дисциплины

Программу составил(а)

ст. преподаватель		Афанасьева. А.В.
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

Программа одобрена на заседании кафедры № 34

«24» мая 2018 г, протокол № 10

Заведующий кафедрой № 34

д.т.н.,доц.		С.В. Беззатеев
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

Ответственный за ОП 10.05.03(07)

доц.,к.т.н., доц.		В.А. Мыльников
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

Заместитель директора института (факультета) № 3 по методической работе

доц.,к.т.н.,доц.		М.В. Бураков
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

Аннотация

Дисциплина «Математические основы обработки информации» входит в базовую часть образовательной программы подготовки обучающихся по специальности «10.05.03 «Информационная безопасность автоматизированных систем» специализация «Обеспечение информационной безопасности распределенных информационных систем». Дисциплина реализуется кафедрой №34.

Дисциплина нацелена на формирование у выпускника

общекультурных компетенций:

ОК-8 «способность к самоорганизации и самообразованию»;

общепрофессиональных компетенций:

ОПК-1 «способность анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач»,

ОПК-2 «способность корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники».

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 2 зачетных единицы, 72 часа.

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

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:
ОК-8 «способность к самоорганизации и самообразованию»:

знать - основные результаты теории чисел;
уметь – осмысливать, систематизировать прогнозировать, осуществлять постановку исследовательских задач и выбору путей их решения;
владеть навыками – решения исследовательских задач и выбору путей их решенря;
иметь опыт деятельности - выявления естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности

ОПК-1 «способность анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач»:

знать – модели информационно-технологических ресурсов;
уметь - применять технологии получения, накопления, хранения, обработки, анализа, интерпретации и использования информации в ходе профессиональной деятельности;
владеть навыками - решению трудных проблем;
иметь опыт деятельности – использования информационных технологий для решения конкретных задач.

ОПК-2 «способность корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники»:
знать - математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации
уметь – использовать математический аппарат при решении профессиональных задач
владеть навыками – применения математический аппарат при решении профессиональных задач;
иметь опыт деятельности – проведения математических расчетов при решении профессиональных задач.

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
- Информационные технологии
- Теория вероятностей и математическая статистика
- Вычислительная математика
- Технологии и методы программирования

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
- Производственная (эксплуатационная) практика
- Моделирование систем
- Системное программное обеспечение
- Постквантовая криптография
- Теория графов и ее приложения
- Производственная (конструкторская) практика
- Научно-исследовательская работа
- Производственная преддипломная практика

3. Объем дисциплины в ЗЕ/академ. час

Данные об общем объеме дисциплины, трудоемкости отдельных видов учебной работы по дисциплине (и распределение этой трудоемкости по семестрам) представлены в таблице 1

Таблица 1 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам
		№5
1	2	3
Общая трудоемкость дисциплины, ЗЕ/(час)	2/ 72	2/ 72
Аудиторные занятия, всего час., ***В том числе***	34	34
лекции (Л), (час)	17	17
Практические/семинарские занятия (ПЗ), (час)	17	17
лабораторные работы (ЛР), (час)		
курсовой проект (работа) (КП, КР),		

(час)		
Экзамен, (час)		
Самостоятельная работа, всего	38	38
Вид промежуточного контроля: зачет, дифф. зачет, экзамен **(Зачет, Дифф. зач, Экз.)**	Зачет	Зачет

4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий

Разделы и темы дисциплины и их трудоемкость приведены в таблице 2.

Таблица 2. – Разделы, темы дисциплины и их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ)	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. 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	5	5			8
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	6			10
Раздел 3. Задача факторизации составного числа. Тема 3.1. (P-1)-метод Полларда. Ро-метод Полларда. Те ма 3.2. Факторизация целых чисел с субэкспоненциальной сложностью. Тема 3.3. Факторизация чисел с помощью квадратичного решета	3	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.	6	0			10
Итого в семестре:	17	17			38
Итого:	17	17	0	0	38

4.2. Содержание разделов и тем лекционных занятий

Содержание разделов и тем лекционных занятий приведено в таблице 3.

Таблица 3 - Содержание разделов и тем лекционных занятий

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.

	Те ма 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 4.

Таблица 4 – Практические занятия и их трудоемкость

№ п/п	Темы практических занятий	Формы практических занятий	Трудоемкость, (час)	№ раздела дисциплины
Семестр 5				
1	Элементы теории чисел	Решение задач	3	1
2	Тесты простоты	Решение задач	3	2
3	Задача факторизации составного числа	Решение задач	3	3
4	Решение квадратных уравнений в модульной арифметике.	Решение задач	4	4
5	Задача поиска дискретного логарифма.	Решение задач	3	4
		Всего:	17	

4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	№ раздела дисциплины
Учебным планом не предусмотрено			
Всего:			

4.5. Курсовое проектирование (работа)

Учебным планом не предусмотрено

4.6. Самостоятельная работа студентов

Виды самостоятельной работы и ее трудоемкость приведены в таблице 6.

Таблица 6 Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 5, час
1	2	3
Самостоятельная работа, всего	38	38
изучение теоретического материала дисциплины (ТО)	30	30
курсовое проектирование (КП, КР)		
расчетно-графические задания (РГЗ)		
выполнение реферата (Р)		
Подготовка к текущему контролю (ТК)	8	8
домашнее задание (ДЗ)		
контрольные работы заочников (КРЗ)		

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Учебно-методические материалы для самостоятельной работы обучающихся указаны в п.п. 8-10.

6. Перечень основной и дополнительной литературы

6.1. Основная литература

Перечень основной литературы приведен в таблице 7.

Таблица 7 – Перечень основной литературы

Шифр	Библиографическая ссылка / URL адрес	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

6.2. Дополнительная литература

Перечень дополнительной литературы приведен в таблице 8.

Таблица 8 – Перечень дополнительной литературы

Шифр	Библиографическая ссылка/ URL адрес	Количество экземпляров в библиотеке (кроме электронных экземпляров)
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 ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины

Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины приведен в таблице 9.

Таблица 9 – Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины

URL адрес	Наименование

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

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

8.1. Перечень программного обеспечения

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10 – Перечень программного обеспечения

№ п/п	Наименование
	Не предусмотрено

8.2. Перечень информационно-справочных систем

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11 – Перечень информационно-справочных систем

№ п/п	Наименование
	Не предусмотрено

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Состав материально-технической базы 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. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

10.1. Состав фонда оценочных средств приведен в таблице 13

Таблица 13 - Состав фонда оценочных средств для промежуточной аттестации

Вид промежуточной аттестации	Примерный перечень оценочных средств
Зачет	Список вопросов; Тесты.

10.2. Перечень компетенций, относящихся к дисциплине, и этапы их формирования в процессе освоения образовательной программы приведены в таблице 14.

Таблица 14 – Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Номер семестра	Этапы формирования компетенций по дисциплинам/практикам в процессе освоения ОП
ОК-8 «способность к самоорганизации и самообразованию»	
1	История
1	Алгебра и геометрия
1	Математическая логика и теория алгоритмов
1	Информатика
1	Математический анализ
1	Иностранный язык
1	Экономика
2	Алгебра и геометрия
2	Математический анализ
2	Дискретная математика
2	Физика
2	Культурология
2	Философия
2	Иностранный язык
3	Информационные технологии
3	Теория вероятностей и математическая статистика
3	Физика
3	Социология и политология
3	Электротехника
3	Иностранный язык
4	Основы радиотехники
4	Вычислительная математика
4	Иностранный язык
5	Математические основы обработки информации
5	Теория информации
6	Международный бизнес
6	Мировая экономика
6	Теория кодирования
8	Исследование операций и теории игр
9	Прикладная экономика
9	Экономика проектов в информационных технологиях
ОПК-1 «способность анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач»	

1	Математический анализ
1	Математическая логика и теория алгоритмов
2	Физика
2	Математический анализ
2	Учебная (ознакомительная) практика
3	Теория вероятностей и математическая статистика
3	Электротехника
3	Физика
3	Инженерная графика
4	Основы радиотехники
4	Вычислительная математика
4	Технологии и методы программирования
4	Учебная практика
4	Электроника и схемотехника
5	Мультимедиа технологии
5	Технологии обработки аудио- и видеоданных
5	Устройства и системы беспроводной связи
5	Организация ЭВМ и вычислительных систем
5	Метрология
5	Микропроцессорная техника
5	Математические основы обработки информации
6	Производственная (эксплуатационная) практика
6	Моделирование систем
6	Системное программное обеспечение
6	Операционные системы
7	Распределенные информационные системы
7	Постквантовая криптография
7	Безопасность сетей ЭВМ
7	Распределенные сети хранения данных
7	Безопасность операционных систем
8	Языки программирования
8	Теория графов и ее приложения
8	Производственная (конструкторская) практика
8	Исследование операций и теории игр
9	Научно-исследовательская работа
9	Научно-исследовательская работа
9	Защита информации в сенсорных сетях
10	Научно-исследовательская работа
10	Научно-исследовательская работа
10	Производственная преддипломная практика
ОПК-2 «способность корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники»	

1	Математическая логика и теория алгоритмов
1	Алгебра и геометрия
1	Математический анализ
2	Алгебра и геометрия
2	Математический анализ
2	Дискретная математика
2	Физика
3	Инженерная графика
3	Физика
3	Теория вероятностей и математическая статистика
4	Вычислительная математика
5	Математические основы обработки информации
6	Теория кодирования
7	Постквантовая криптография
8	Исследование операций и теории игр
8	Теория графов и ее приложения

10.3. В качестве критериев оценки уровня сформированности (освоения) у обучающихся компетенций применяется шкала модульно–рейтинговой системы университета. В таблице 15 представлена 100–балльная и 4-балльная шкалы для оценки сформированности компетенций.

Таблица 15 –Критерии оценки уровня сформированности компетенций

Оценка компетенции		Характеристика сформированных компетенций
100-балльная шкала	4-балльная шкала	
$85 \le К \le 100$	«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.
$70 \le К \le 84$	«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.
$55 \le К \le 69$	«удовлетво-рительно» «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.

$К \leq 54$	«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.

10.4. Типовые контрольные задания или иные материалы:

1. Вопросы (задачи) для экзамена (таблица 16)

Таблица 16 – Вопросы (задачи) для экзамена

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

2. Вопросы (задачи) для зачета / дифференцированного зачета (таблица 17)

Таблица 17 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифференцированного зачета
	1. Простые числа и "основная" теорема арифметики. 2. Полная и приведенная системы вычетов. 3. Теорема Эйлера и теорема Ферма. 4. Алгоритм Евклида. 5. Бинарный алгоритм возведения в степень. 5. Китайская теорема об остатках. 6. Квадратичные вычеты 7. Метод пробных делений. 8. Критерий Вильсона. 9. Тест Лукаса. 9. Алгоритм Конягина-Померанса. 10. Детерминистические и вероятностные тесты на простоту. 11. Тест Соловея-Штрассена. 12. Тест Рабина-Миллера. 13. Построение больших простых чисел 14. Задача факторизации составного числа. 15. (P-1)-метод Полларда. 16. Ро-метод Полларда. 17.Факторизация чисел с помощью квадратичного решета. 18.Извлечения корня по модулю простого числа. 19. Извлечение корня по составному основанию. 20. Определение дискретного логарифма. 21. Алгоритм сопоставления. 22. Ро-алгоритм Полларда для поиска дискретного логарифма.

3. Темы и задание для выполнения курсовой работы / выполнения курсового проекта (таблица 18)

Таблица 18 – Примерный перечень тем для выполнения курсовой работы / выполнения курсового проекта

№ п/п	Примерный перечень тем для выполнения курсовой работы / выполнения

	курсового проекта
	Учебным планом не предусмотрено

4. Вопросы для проведения промежуточной аттестации при тестировании (таблица 19)

Таблица 19 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов
	Учебным планом не предусмотрено

5. Контрольные и практические задачи / задания по дисциплине (таблица 20)

Таблица 20 – Примерный перечень контрольных и практических задач / заданий

№ п/п	Примерный перечень контрольных и практических задач / заданий
	Примеры заданий по теме: Элементы теории чисел Задание 1. Вычислить: (5*7-83) mod 27 (5:29+7)mod 25 (8:6-9) mod 33 Задание 2. Нахождение мультипликативных обратных с помощью расширенного алгоритма Евклида. Пример задания: Вычислить: 11^{-1} mod 47 Задание 3. Бинарный алгоритм возведения в степень. Пример задания: Вычислить: 26^{67} mod 97. Задание 4. Китайская теорема об остатках. Пример задания: X mod 5 = 2 X mod 7 = 6 X mod 12 =8 Найти X. Задание 5. Квадратичные вычеты. Примеры заданий: 1. Вычислить символ Лежанра 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. 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 Соловэя-Штрассена Примеры заданий по теме: Факторизация чисел: Разложить на множители число 63

	a)	методом деления
	b)	(p-1)-методом Полларда
	c)	Ро-методом Полларда
	d)	методом Ферма

10.5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и / или опыта деятельности, характеризующих этапы формирования компетенций, содержатся в Положениях «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».

11.

12. 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;

– научится 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 обучающемся умений и навыков практической деятельности по изучаемой дисциплине.

Планируемые результаты при освоении обучающемся 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 тема 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