

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ 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)

«24» июня 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Математические основы обработки информации»
(Название дисциплины)

| | |
|---|---|
| Код направления | 10.05.05 |
| Наименование направления/ специальности | Безопасность информационных технологий в правоохранительной сфере |
| Наименование направленности | Технологии защиты информации в правоохранительной сфере |
| Форма обучения | очная |

Лист согласования рабочей программы дисциплины

Программу составил(а)

проф., д.т.н., доц.
должность, уч. степень, звание

«24» июня 2021 г.

подпись, дата

С.В. Беззатеев
инициалы, фамилия

Программа одобрена на заседании кафедры № 34

«24» июня 2021 г., протокол № 11

Заведующий кафедрой № 34

проф., д.т.н., доц.
должность, уч. степень, звание

«24» июня 2021 г.

подпись, дата

С.В. Беззатеев
инициалы, фамилия

Ответственный за ОП 10.05.05(01)

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

24.06.21

подпись, дата

В.А. Мыльников
инициалы, фамилия

Заместитель директора института (декана факультета) № 3 по методической работе

доц., к.э.н., доц.
должность, уч. степень, звание

24.06.21

подпись, дата

Г.С. Армашова-Тельник
инициалы, фамилия

Аннотация

Дисциплина «Математические основы обработки информации» входит в базовую часть образовательной программы подготовки обучающихся по специальности «10.05.05 «Безопасность информационных технологий в правоохранительной сфере» специализация «Технологии защиты информации в правоохранительной сфере». Дисциплина реализуется кафедрой №34.

Дисциплина нацелена на формирование у выпускника

общекультурных компетенций:

ОК-12 «способность работать с различными источниками информации, информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации»;

общепрофессиональных компетенций:

ОПК-1 «способность выявлять естественнонаучную

сущность проблем, возникающих в ходе

профессиональной деятельности и

использовать общенаучные методы, законы

физики, математический аппарат, методы

моделирования и прогнозирования развития

процессов и явлений при решении

профессиональных задач»;

профессиональных компетенций:

ПК-13 «способность осуществлять организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов»;

ПК-27 «способность готовить научные отчеты по результатам выполненных исследований»;

ПК-28 «способность выполнять предварительный технико-экономический анализ и обоснование проектных решений по созданию систем обеспечения безопасности информации и защиты государственной тайны».

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-12 «способность работать с различными источниками информации, информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации»:

знать - основные результаты теории чисел;

уметь - оценивать стойкость теоретико-числовых криптосистем с открытым ключом;

владеть навыками - построения и анализа вычислительно трудных теоретико-числовых функций;

иметь опыт деятельности - выявления естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности

ОПК-1 «способность выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности и использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач»:

знать - основные методы решения трудных теоретико-числовых проблем;

уметь - решать теоретико-числовые проблемы;

владеть навыками - применения этих функций в задачах защиты информации;

иметь опыт деятельности - работы с различными источниками информации, информационными ресурсами и технологиями;

ПК-13 «способность осуществлять организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов»:

знать – методы и средства организации организационно-правового обеспечения профессиональной деятельности;

уметь – реализовывать работы по получению, накоплению, обработке, анализу, использованию информации;

владеть навыками - защиты объектов информатизации, информационных технологий и ресурсов;

иметь опыт деятельности – в использовании математических моделей при обработке и анализе информации;

ПК-27 «способность готовить научные отчеты по результатам выполненных исследований»:

знать – нормативы по подготовке научных отчетов;
 уметь - готовить научные отчеты по результатам выполненных исследований;
 владеть навыками – формирования отчетности по созданным моделям;
 иметь опыт деятельности – подготовки научных отчетов;

ПК-28 «способность выполнять предварительный технико-экономический анализ и обоснование проектных решений по созданию систем обеспечения безопасности информации и защиты государственной тайны»:

знать - методику применения этой теории для разработки и оценки стойкости криптосистем;
 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.

2. Место дисциплины в структуре ОП

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

- Математика
- Дискретная математика
- Прикладная математика

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

- Технологии защиты от скрытой передачи данных
- Научно-технический семинар
- Теория кодирования
- Научно-исследовательская работа

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 |
| <i>Из них часов практической подготовки</i> | 10 | 10 |
| <i>Аудиторные занятия, всего час.,</i> | 34 | 34 |

| | | |
|--|-------|-------|
| <i>В том числе</i> | | |
| 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) (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. 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. Тема 3.2. Факторизация целых чисел с | 3 | 6 | | | 10 |

| | | | | | |
|--|----|----|---|---|----|
| 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. | 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 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 4.

Таблица 4 – Практические занятия и их трудоемкость

| № п/п | Темы практических занятий | Формы практических занятий | Трудоемкость, (час) | Из них часов практической подготовки | № раздела дисциплины |
|-----------|--|----------------------------|---------------------|--------------------------------------|----------------------|
| Семестр 5 | | | | | |
| 1 | Элементы теории чисел | Решение задач | 3 | 2 | 1 |
| 2 | Тесты простоты | Решение задач | 3 | 2 | 2 |
| 3 | Задача факторизации составного числа | Решение задач | 3 | 2 | 3 |
| 4 | Решение квадратных уравнений в модульной арифметике. | Решение задач | 4 | 2 | 4 |
| 5 | Задача поиска дискретного логарифма. | Решение задач | 3 | 2 | 4 |
| | | | | | |
| Всего: | | | 17 | 10 | |

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 студентов 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) |
|----------------|--|---|
| | Б. А. Фороузан Криптография и безопасность сетей. Бином. Лаборатория знаний, 2010 г. | |
| [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 |
| | С. Н. Владимиров, И. В. Измайлов, Б. Н. Пойзнер. Нелинейно-динамическая криптология. Радиофизические и оптические системы. | |

| | | |
|-----------------|--|----|
| | ФИЗМАТЛИТ, 2009 | |
| [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 |
| | Нечаев В.И. Элементы криптографии: Основы теории защиты информации. М., 1999. - 120 с. | |
| [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 |
| | Н. Смарт. Криптография. Серия: Мир программирования, Техносфера, 2006 г., 528 стр. | |
| | Венбо Мао. Современная криптография. Теория и практика. Вильямс, 2005 г., 768 стр. | |

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-12 «способность работать с различными источниками информации, информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации» | |
| 1 | Математика. Аналитическая геометрия и линейная алгебра |
| 1 | Математика. Математический анализ |
| 1 | Иностранный язык |
| 1 | Общая теория государства и права |
| 1 | Актуальные проблемы государственного права |
| 1 | Промышленная экология |
| 1 | Конституционное право |
| 1 | Экология |
| 2 | Дискретная математика |
| 2 | Физика |
| 2 | Иностранный язык |
| 2 | Математика. Математический анализ |
| 2 | Математика. Аналитическая геометрия и линейная алгебра |
| 2 | Культурология |
| 3 | Иностранный язык |
| 3 | Средства вычислительной техники |
| 3 | Математика. Теория вероятностей и математическая статистика |
| 3 | Физика |
| 4 | Административное право |
| 4 | Криминалистика |
| 4 | Правоведение |
| 4 | Иностранный язык |
| 4 | Прикладная математика |
| 4 | Административный процесс |
| 5 | Основы электро-, радиоизмерений |
| 5 | Математические основы обработки информации |
| 5 | Микропроцессорные системы |
| 5 | Профессиональная этика и служебный этикет |
| 5 | Организация ЭВМ и вычислительных систем |
| 5 | Теория информации |
| 7 | Техническая защита информации |
| 8 | Технологии защиты от скрытой передачи данных |

| | |
|---|---|
| 8 | Психология профессиональной деятельности |
| 8 | Защита и обработка документов ограниченного доступа |
| 9 | Научно-технический семинар |
| 9 | Технологии защищенного документооборота |
| 10 | Научно-технический семинар |
| ОПК-1 «способность выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности и использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач» | |
| 1 | Математика. Математический анализ |
| 1 | Математика. Аналитическая геометрия и линейная алгебра |
| 2 | Математика. Математический анализ |
| 2 | Математика. Аналитическая геометрия и линейная алгебра |
| 2 | Физика |
| 3 | Математика. Теория вероятностей и математическая статистика |
| 3 | Основы электротехники и радиоэлектроники |
| 3 | Физика |
| 4 | Основы электротехники и радиоэлектроники |
| 4 | Прикладная математика |
| 5 | Математические основы обработки информации |
| 5 | Мультимедиа технологии |
| 5 | Технологии обработки аудио- и видеоданных |
| 6 | Программно-аппаратная защита информации |
| 6 | Теория кодирования |
| 6 | Системы и сети передачи данных |
| 7 | Специальные информационные технологии в правоохранительной деятельности |
| 8 | Организационная защита информации |
| ПК-13 «способность осуществлять организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов» | |
| 4 | Программирование. Методы и технологии программирования |
| 5 | Математические основы обработки информации |
| 6 | Гражданский процесс |
| 7 | Информационное право |
| 8 | Программирование. Языки программирования |
| 8 | Правовая защита информации |
| 9 | Управление информационной безопасностью |
| ПК-27 «способность готовить научные отчеты по результатам выполненных исследований» | |

| | |
|--|---|
| 5 | Математические основы обработки информации |
| 6 | Производственная (эксплуатационная) практика |
| 7 | Безопасность систем баз данных |
| 8 | Производственная практика |
| 9 | Научно-технический семинар |
| 9 | Научно-исследовательская работа |
| 9 | Информационно-аналитическое обеспечение правоохранительной деятельности |
| 9 | Научно-исследовательская работа |
| 9 | Компьютерная экспертиза |
| 10 | Научно-исследовательская работа |
| 10 | Научно-исследовательская работа |
| 10 | Научно-технический семинар |
| 10 | Производственная преддипломная практика |
| ПК-28 «способность выполнять предварительный технико-экономический анализ и обоснование проектных решений по созданию систем обеспечения безопасности информации и защиты государственной тайны» | |
| 4 | Производственная (технологическая) практика |
| 5 | Математические основы обработки информации |
| 7 | Распределенные информационные системы |
| 8 | Защита информации в распределенных информационных системах |
| 9 | Экономика проектов в информационных технологиях |
| 9 | Прикладная экономика |

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 | |
| $85 \leq K \leq 100$ | «отлично» «зачтено» | <ul style="list-style-type: none"> - 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. |
| $70 \leq K \leq 84$ | «хорошо» «зачтено» | <ul style="list-style-type: none"> - 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; |

| | | |
|---------------------|---------------------------------------|---|
| | | <ul style="list-style-type: none"> - делает выводы и обобщения; - владеет системой специализированных понятий. |
| $55 \leq K \leq 69$ | «удовлетворительно» «зачтено» | <ul style="list-style-type: none"> - 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. |
| $K \leq 54$ | «неудовлетворительно» «не зачтено» | <ul style="list-style-type: none"> - 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 |
|-------|--|
| | <ol style="list-style-type: none"> 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 |
|-------|---|
| | <p>Примеры заданий по теме: Элементы теории чисел</p> <p>Задание 1. Вычислить: $(5 \cdot 7 - 83) \bmod 27$ $(5 : 29 + 7) \bmod 25$ $(8 : 6 - 9) \bmod 33$</p> <p>Задание 2. Нахождение мультипликативных обратных с помощью расширенного алгоритма Евклида. Пример задания: Вычислить: $11^{-1} \bmod 47$</p> <p>Задание 3. Бинарный алгоритм возведения в степень. Пример задания: Вычислить: $26^{67} \bmod 97$.</p> <p>Задание 4. Китайская теорема об остатках. Пример задания: $X \bmod 5 = 2$ $X \bmod 7 = 6$ $X \bmod 12 = 8$ Найти X.</p> <p>Задание 5. Квадратичные вычеты. Примеры заданий: 1. Вычислить символ Лежандра для 3 по модулю 17.</p> |

| | |
|--|--|
| | <p>2. Вычислить символ Якоби для числа 8 по модулю 15.</p> <p>3. Выяснить является ли число 6 квадратичным вычетом по модулю 11.</p> <p>Примеры заданий по теме: Тесты простоты:</p> <p>Проверить на простоту число 71</p> <ol style="list-style-type: none"> a) методом пробного деления b) тестом Миллера-Рабина c) По теореме Ферма d) методом Соловья-Штрассена <p>Примеры заданий по теме: Факторизация чисел:</p> <p>Разложить на множители число 63</p> <ol style="list-style-type: none"> 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. 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, приходиться 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 Косягина-Померанса.

Тема 2.2. Вероятностные тесты на простоту. Тест Соловья-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:

– экзамен – форма оценки знаний, полученных обучающимся в процессе изучения всей дисциплины или ее части, навыков самостоятельной работы, способности применять их для решения практических задач. Экзамен, как правило, проводится в период экзаменационной сессии и завершается аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

– 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».

– дифференцированный зачет – это форма оценки знаний, полученных обучающимся при изучении дисциплины, при выполнении курсовых проектов, курсовых работ, научно-исследовательских работ и прохождении практик с аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

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 |
|---|-----------------------------------|--------------------------------------|-----------------------|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |