

федеральное государственное бюджетное образовательное учреждение
высшего образования
РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ
УНИВЕРСИТЕТ

Кафедра Высшей математики и теоретического механики

Рабочая программа по дисциплине

ОСНОВЫ ТЕОРИИ ЧИСЕЛ

Основная профессиональная образовательная программа
высшего образования программы специалитета по специальности

10.05.02 «Информационная безопасность телекоммуникационных систем»

Специализация:

Разработка защищенных телекоммуникационных систем

Квалификация:

Специалист

Форма обучения

Очная

Согласовано
Руководитель ОПОП
«Информационная безопасность
телекоммуникационных систем»


Бурлов В.Г.

Утверждаю

Председатель УМС  И.И. Палкин

Рекомендована решением

Учебно-методического совета

 19 июня 2018 г., протокол № 4

Рассмотрена и утверждена на заседании кафедры

25 04 2018 г., протокол № 9

Зав. кафедрой  Матвеев Ю.Л.

Авторы-разработчики:

 Ржонсницкая Ю.Б.

1. Цели освоения дисциплины

Целью освоения дисциплины «Основы теории чисел» является: формирование способности разрабатывать алгоритмы преобразования информации и сигналов для защищенных телекоммуникационных систем на основе теоретико-числовых методов

2. Место дисциплины в структуре ОПОП

Дисциплина «Основы теории чисел» относится к базовой части для подготовки специалистов по направлению «Разработка защищенных телекоммуникационных систем». Изучение дисциплины базируется на дисциплине «Алгебра и геометрия».

Дисциплина «Основы теории чисел» обеспечивает изучение следующих дисциплин: «Криптографические методы защиты информации», «Цифровая обработка сигналов», «Теория информации и кодирования». Знания и практические навыки, полученные в результате изучения дисциплины «Основы теории чисел», используются в курсовом и дипломном проектировании.

Дисциплина изучается:

студентами набора 2017 года в 6 семестре, трудоемкость – 108 ак. часа, 3 з.е.

студентами набора 2016 года в 6 семестре, трудоемкость – 108 ак. часа, 3 з.е.

студентами набора 2015 года в 6 семестре, трудоемкость – 108 ак. часа, 3 з.е.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код компетенции	Компетенция
ОПК-2	способностью применять соответствующий математический аппарат для решения профессиональных задач
ОПК-6	способностью применять методы научных исследований в профессиональной деятельности

В результате освоения дисциплины обучающийся должен:

Код компетенции	Результаты обучения
ОПК-2	<p>Знать:</p> <ul style="list-style-type: none"> – основные понятия и теоремы теории чисел, основные свойства групп, колец, полей; <p>Уметь:</p> <ul style="list-style-type: none"> – решать прикладные задачи теории чисел. <p>Владеть:</p> <ul style="list-style-type: none"> – навыками решения прикладных задач с применением групп, колец и полей;
ОПК-6	<p>Знать:</p> <ul style="list-style-type: none"> – принципы построения ортонормированных конечномерных базисов. <p>Уметь:</p> <ul style="list-style-type: none"> – решать прикладные задачи модулярной арифметики. <p>Владеть:</p> <ul style="list-style-type: none"> – навыками выбора и оптимизации вида базисных функций, соответствующих обрабатываемым сигналам и элементной базе.

Основные признаки проявленности формируемых компетенций в результате освоения дисциплины «Основы теории чисел» сведены в таблице.

Соответствие уровней освоения компетенции планируемым результатам обучения и критериям их оценивания

Уровень освоения компетенции	Результат обучения	
	ОПК-2: Знать, уметь, владеть	ОПК-6: Знать, уметь, владеть
минимальный	не владеет	слабо ориентируется в терминологии и содержании
	не умеет	не выделяет основные идеи
	не знает	допускает грубые ошибки
базовый	Способен выделить основные идеи текста, работает с критической литературой	Способен выделить основные идеи текста, работает с критической литературой
	Способен показать основную идею в развитии	Способен показать основную идею в развитии
	Знает основные рабочие категории, однако не ориентируется в их специфике	Знает основные рабочие категории, однако не ориентируется в их специфике
продвинутый	Способен грамотно обосновать собственную позицию относительно решения современных проблем в заданной области	Видит источники современных проблем в заданной области анализа, владеет подходами к их решению
	Свободно ориентируется в заданной области анализа. Понимает ее основания и умеет выделить практическое значение заданной области	Выявляет основания заданной области анализа, понимает ее практическую ценность, однако испытывает затруднения описании сложных объектов анализа
	Может дать критический анализ современным проблемам в заданной области анализа	Знает основное содержание современных научных идей в рабочей области анализа,

		способен их сопоставить
--	--	-------------------------

Соответствие уровней освоения компетенции планируемым результатам обучения и критериям их оценивания

Этап (уровень) освоения компетенции	Основные признаки проявленности компетенции (дескрипторное описание уровня)				
	1.	2.	3.	4.	5.
минимальный	не владеет	слабо ориентируется в терминологии и содержании	Способен выделить основные идеи текста, работает с критической литературой	Владеет основными навыками работы с источниками и критической литературой	Способен дать собственную критическую оценку изучаемого материала
	не умеет	не выделяет основные идеи	Способен показать основную идею в развитии	Способен представить ключевую проблему в ее связи с другими процессами	Может соотнести основные идеи с современными проблемами
	не знает	допускает грубые ошибки	Знает основные рабочие категории, однако не ориентируется в их специфике	Понимает специфику основных рабочих категорий	Способен выделить характерный авторский подход
базовый	не владеет	плохо ориентируется в терминологии и содержании	Владеет приемами поиска и систематизации, но не способен свободно изложить материал	Свободно излагает материал, однако не демонстрирует навыков сравнения основных идей и концепций	Способен сравнивать концепции, аргументированно излагает материал
	не умеет	выделяет основные идеи, но не видит проблем	Выделяет конкретную проблему, однако излишне упрощает ее	Способен выделить и сравнить концепции, но испытывает сложности с их практической привязкой	Аргументированно проводит сравнение концепций по заданной проблематике
	не знает	допускает много ошибок	Может изложить основные рабочие категории	Знает основные отличия концепций в заданной проблемной области	Способен выделить специфику концепций в заданной проблемной области
продвинутый	не владеет	ориентируется в терминологии и содержании	В общих чертах понимает основную идею, однако плохо связывает ее с существующей проблематикой	Видит источники современных проблем в заданной области анализа, владеет подходами к их решению	Способен грамотно обосновать собственную позицию относительно решения современных проблем в заданной области
	не умеет	выделяет основные идеи, но не видит их в развитии	Может понять практическое назначение основной идеи, но затрудняется выявить ее основания	Выявляет основания заданной области анализа, понимает ее практическую ценность, однако испытывает затруднения в описании сложных объектов анализа	Свободно ориентируется в заданной области анализа. Понимает ее основания и умеет выделить практическое значение заданной области
	не знает	допускает ошибки при выделении рабочей области анализа	Способен изложить основное содержание современных научных идей в рабочей области анализа	Знает основное содержание современных научных идей в рабочей области анализа, способен их сопоставить	Может дать критический анализ современным проблемам в заданной области анализа

					раб ота			
1	Раздел 1. Основные понятия теории чисел	6	6	3	12		9	ОПК-2 ОПК-6
2	Раздел 2. Основные функции и теоремы теории чисел	6	6	3	12		9	ОПК-2 ОПК-6
3	Раздел 3. Решение сравнений по различным модулям	6	6	3	12		9	ОПК-2 ОПК-6
4	Раздел 4. Основы теории конечных групп, колец и полей	6	6	3	12		9	ОПК-2 ОПК-6
5	Раздел 5. Теоретико- числовые преобразования	6	8	4	12		12	ОПК-2 ОПК-6
	ИТОГО – 108 часа		32	16	60		48	

4.2. Содержание разделов дисциплины

Раздел 1. Основные понятия теории чисел

Множества и основные операции над ними. Основные правила комбинаторики. Размещения, перестановки, сочетания. Основные комбинаторные тождества. Треугольник Паскаля. Бином Ньютона.

Основные утверждения теории делимости целых чисел. Наибольший общий делитель (НОД) целых чисел. Понятие целого числа большой длины (более 500 десятичных разрядов). Алгоритм Евклида. Вычислительная сложность алгоритма Евклида для целых чисел большой длины. Основные свойства НОД.

Наименьшее общее кратное целых чисел. Разложение чисел в непрерывные дроби. Каноническое разложение числа. Простые числа. Количество простых чисел большой длины на заданном интервале чисел. Вычислительная сложность проверки целых чисел большой длины на простоту. Вычислительная сложность задачи канонического разложения целых чисел большой длины.

Раздел 2. Основные функции и теоремы теории чисел

Основные функции теории чисел. Мультипликативные функции и их основные свойства. Функция Мёбиуса и ее свойства. Функция Эйлера и ее свойства. Сравнения по модулю m и их основные свойства. Полная система вычетов. Приведенная система вычетов. Теоремы Эйлера и Ферма. Количество решений сравнения первой степени. Вычислительная сложность задачи сравнения первой степени для чисел большой длины.

Раздел 3. Решение сравнений по различным модулям

Символ Лежандра. Критерий Эйлера. Основные свойства символа Лежандра. Символ Якоби и его основные свойства.

Решение сравнений первой степени с помощью непрерывных дробей. Решение сравнений первой степени с помощью функции Эйлера. Системы сравнений первой степени по попарно простым модулям. Системы сравнений первой степени по произвольным модулям. Сравнения любой степени по простому модулю. Число решений. Теорема Вильсона. Сравнения любой степени по составному модулю.

Решение сравнений вида $f(x) \equiv 0 \pmod{p^a}$. Сравнения второй степени по простому нечетному модулю. Число решений. Квадратичные вычеты.

Решение сравнений вида $x^2 \equiv a \pmod{2^a}$. Число решений. Решение сравнений вида $x^2 \equiv a \pmod{2^a p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}}$. Число решений.

Вычислительная сложность прямых и обратных арифметических операций над целыми числами большой длины при решении задач сравнения по простому и составному модулям.

Раздел 4. Основы теории конечных групп, колец и полей

Периодические группы, подгруппы. Изоморфизм групп. Абелевы группы. Геометрическое представление конечных абелевых групп. Кольца, основные определения и аксиомы. Кольцо классов вычетов по модулю m . Показатели и первообразные корни. Алгебраические структуры мультипликативных и аддитивных групп кольца Z_n . Конечные поля Галуа.

Раздел 5. Теоретико-числовые преобразования

Понятия континуального, счетного и конечномерного функциональных пространств. Системы координат и размерность функционального пространства. Связь координатных осей и базисных функций. Проекция многомерного вектора-сигнала на координатные оси (базисные функции). Представление спектра вектора-сигнала как результат прямого дискретного ортогонального преобразования. Представление вектора-сигнала во временной области как результат обратного дискретного ортогонального преобразования спектра. Понятие обобщенной цифровой фильтрации сигналов в спектральной области. Определения характеров и их основные свойства. Ортонормированные базисы: полиномиальный, Уолша, базис отсчетных функций. Обобщенные функции Радемахера и Хаара. Полнота и замкнутость. Преобразования Фурье-Галуа. Теоретико-числовые преобразования над конечным полем комплексных чисел.

4.3. Семинарские, практические, лабораторные занятия, их содержание

№ п/п	№ раздела дисциплины	Тематика практических занятий	Форма проведения	Формируемые компетенции
-------	----------------------	-------------------------------	------------------	-------------------------

1	Раздел 1.	Основные понятия теории чисел	Активная и интерактивная	ОПК-2 ОПК-6
2	Раздел 2.	Основные функции и теоремы теории чисел	Активная и интерактивная	ОПК-2 ОПК-6
3	Раздел 3.	Решение сравнений по различным модулям	Активная и интерактивная	ОПК-2 ОПК-6
4	Раздел 4.	Основы теории конечных групп, колец и полей	Активная и интерактивная	ОПК-2 ОПК-6
5	Раздел 5.	Теоретико-числовые преобразования	Активная и интерактивная	ОПК-2 ОПК-6

5. Учебно-методическое обеспечение самостоятельной работы студентов и оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

5.1. Текущий контроль

Текущий контроль проводится в виде коллоквиума и выполнения контрольной работы

а). Образцы тестовых и контрольных заданий текущего контроля

Вопросы:

1.

Тестовые вопросы и задания:

Примерные вопросы

1) Решить линейное сравнение

$$151x \equiv 105 \pmod{89}$$

2) Зашифровать и расшифровать сообщение M с помощью системы RSA

$$M = 11; p = 3; q = 7$$

3) Представить $\frac{a}{b}$ в виде непрерывной дроби, выписать подходящие дроби

$$a = 1490; b = 1040$$

4) Найти линейное представление НОД чисел 478 и 46.

4) Найти показатель, скоторым число 11 содержится в числе

5) Найти количество натуральных чисел, не превышающих числа 1800 и имеющих с ним наибольшим общим делителем число 36.

б) Определить погрешность, полученную при замене числа 17 подходящей дробью пятого порядка.

5.2. Методические указания по организации самостоятельной работы

1. Выполнить домашнее задание.
2. Перед следующим практическим занятием внимательно прочитайте конспект последней лекции.
3. Прочитать дополнительную литературу.

5.3. Промежуточный контроль: экзамен.

Перечень вопросов к экзамену:

1. Множества и основные операции над ними.
2. Основные правила комбинаторики.
3. Размещения, перестановки, сочетания.
4. Основные комбинаторные тождества.
5. Треугольник Паскаля. Бином Ньютона.
6. Основные утверждения теории делимости целых чисел.
7. Наибольший общий делитель (НОД) целых чисел.
8. Понятие целого числа большой длины (более 500 десятичных разрядов).
9. Алгоритм Евклида.
10. Вычислительная сложность алгоритма Евклида для целых чисел большой длины.
11. Основные свойства НОД.
12. Наименьшее общее кратное целых чисел.
13. Разложение чисел в непрерывные дроби.
14. Каноническое разложение числа.
15. Простые числа.
16. Количество простых чисел большой длины на заданном интервале чисел.
17. Вычислительная сложность проверки целых чисел большой длины на простоту.
18. Вычислительная сложность задачи канонического разложения целых чисел большой длины.
19. Основные функции теории чисел.
20. Мультипликативные функции и их основные свойства.
21. Функция Мёбиуса и ее свойства.
22. Функция Эйлера и ее свойства.
23. Сравнения по модулю m и их основные свойства.
24. Полная система вычетов.
25. Приведенная система вычетов.
26. Теоремы Эйлера и Ферма.
27. Количество решений сравнения первой степени.
28. Вычислительная сложность задачи сравнения первой степени для чисел большой длины.
29. Символ Лежандра.
30. Критерий Эйлера.
31. Основные свойства символа Лежандра.
32. Символ Якоби и его основные свойства.
33. Решение сравнений первой степени с помощью непрерывных дробей.

34. Решение сравнений первой степени с помощью функции Эйлера.
35. Системы сравнений первой степени по попарно простым модулям.
36. Системы сравнений первой степени по произвольным модулям.
37. Сравнения любой степени по простому модулю.
38. Число решений. Теорема Вильсона.
39. Сравнения любой степени по составному модулю.
40. Решение сравнений вида $f(x) \equiv 0 \pmod{p^a}$.
41. Сравнения второй степени по простому нечетному модулю.
42. Число решений. Квадратичные вычеты.
43. Решение сравнений вида $x^2 \equiv a \pmod{2^a}$.
44. Число решений.
45. Решение сравнений вида $x^2 \equiv a \pmod{2^a p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}}$.
46. Число решений.
47. Вычислительная сложность прямых и обратных арифметических операций над целыми числами большой длины при решении задач сравнения по простому и составному модулям.
48. Периодические группы, подгруппы.
49. Изоморфизм групп.
50. Абелевы группы.
51. Геометрическое представление конечных абелевых групп.
52. Кольца, основные определения и аксиомы.
53. Кольцо классов вычетов по модулю m .
54. Показатели и первообразные корни.
55. Алгебраические структуры мультипликативных и аддитивных групп кольца Z_n .
56. Конечные поля Галуа.
57. Понятия континуального, счетномерного и конечномерного функциональных пространств.
58. Системы координат и размерность функционального пространства.
59. Связь координатных осей и базисных функций.
60. Проекция многомерного вектора-сигнала на координатные оси (базисные функции).
61. Представление спектра вектора-сигнала как результат прямого дискретного ортогонального преобразования.
62. Представление вектора-сигнала во временной области как результат обратного дискретного ортогонального преобразования спектра.
63. Понятие обобщенной цифровой фильтрации сигналов в спектральной области.
64. Определения характеров и их основные свойства.
65. Ортонормированные базисы: полиномиальный, Уолша, базис отсчетных функций.
66. Обобщенные функции Радемахера и Хаара.
67. Полнота и замкнутость.
68. Преобразования Фурье-Галуа.
69. Теоретико-числовые преобразования над конечным полем комплексных чисел.

6. Учебно-методическое и информационное обеспечение дисциплины

а) Основная литература:

1. Гмурман, В. Е. Руководство к решению задач по теории вероятностей и математической статистике [Текст] : учеб. пособие / В. Е. Гмурман. - 8-е изд., стереотип. - Москва : Высшая школа, 2003. - 403 с.- Режим доступа:<https://bibli-online.ru/viewer/5CB717D8-C75A-4D84-A587-7FAF134B32E9/ruk> (вставлена ссылка)

2. Виноградов, И. М. Основы теории чисел / И. М. Виноградов. — М. : Издательство Юрайт, 2018. — 102 с. - Режим доступа: <https://biblio-online.ru/book/11AEFEED-CA8B-4B8A-A7BD-33BE0B021F74/osnovy-teorii-chisel>
3. Письменный, Д. Т. Конспект лекций по теории вероятностей, математической статистике и случайным процессам [Текст] / Письменный Д.Т. - 6-е изд. - Москва : Айрис Пресс, 2013. - 287 с.

б) дополнительная литература:

1. Горелова, Г. В. Теория вероятностей и математическая статистика в примерах и задачах с применением EXCEL [Текст] : учеб.пособие / Г. В. Горелова, И. А. Кацко. - 3-е изд., перераб. и доп. - Ростов-на-Дону : Феникс, 2005. - 475(1) с
2. Кремер, Н. Ш. Теория вероятностей и математическая статистика [Текст] : учебник / Кремер Н.Ш. - 2-е изд., перераб. и доп. - Москва : ЮНИТИ, 2004. - 573 с.

в) программное обеспечение и Интернет-ресурсы:

<https://biblio-online.ru> – ЭБС Юрайт;

<http://elib.rshu.ru/> - ЭБС [ГидроМетеоОнлайн](http://biblio-online.ru) структурная часть фонда библиотеки РГГМУ

<http://www.prospektnauki.ru> - ЭБС издательства «Прспект науки»

<http://znanium.com> – ЭБС znanium.com

www.intuit.ru – Национальный открытый университет

www.inf1.info/ - Планета Информатики

7. Методические указания для обучающихся по освоению дисциплины

Вид учебных занятий	Организация деятельности студента
Лекции	<p>Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины.</p> <p>Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь.</p> <p>Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе.</p> <p>Если самостоятельно не удастся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом (семинарском) занятии.</p>
Практические занятия	<p>Проработка рабочей программы, уделяя особое внимание целям и задачам структуре и содержанию дисциплины.</p> <p>Конспектирование источников.</p> <p>Работа с конспектом лекций, -подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы и работа с текстом. Решение тестовых заданий, решение задач и другие виды работ.</p>

Индивидуальные задания (подготовка докладов, рефератов)	<p>Знакомство с основной и дополнительной литературой, включая справочные издания, зарубежные источники, конспект основных положений, терминов, сведений, требующих запоминания и являющихся основополагающими в этой теме.</p> <p>Составление аннотаций к прочитанным литературным источникам и другое. Изложение основных аспектов проблемы, анализ мнений авторов и формирование собственного суждения по исследуемой теме.</p>
Подготовка к зачету и экзамену	<p>При подготовке необходимо ориентироваться на конспекты лекций, рекомендуемую литературу, вопросы для подготовки к экзамену и т.д.</p>

8. Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Освоение дисциплины "Избранные вопросы теории чисел" предполагает использование следующего программного обеспечения и информационно-справочных систем:

Операционная система Microsoft Windows Professional 7 Russian

Браузер Mozilla Firefox

Браузер Google Chrome

AdobeReader XI

Тема (раздел) дисциплины	Образовательные и информационные технологии	Перечень программного обеспечения и информационных справочных систем
Раздел 1. Основные понятия теории чисел	лекции-визуализации (с использованием слайд-презентаций)	
Раздел 2. Основные функции и теоремы теории чисел	лекции-визуализации (с использованием слайд-презентаций)	
Раздел 3. Решение сравнений по различным модулям	лекции-визуализации (с использованием слайд-презентаций)	
Раздел 4. Основы теории конечных групп, колец и полей	лекции-визуализации (с использованием слайд-презентаций)	
Раздел 5. Теоретико-числовые преобразования	лекции-визуализации (с использованием слайд-презентаций)	

9. Особенности освоения дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

обучение обучающихся с ограниченными возможностями здоровья при необходимости осуществляется на основе адаптированной рабочей программы с использованием специальных методов обучения и дидактических материалов, составленных с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (обучающегося).

При определении формы проведения занятий с обучающимся-инвалидом учитываются рекомендации, содержащиеся в индивидуальной программе реабилитации инвалида, относительно рекомендованных условий и видов труда.

При необходимости для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья создаются специальные рабочие места с учетом нарушенных функций и ограничений жизнедеятельности.

10. Материально-техническое обеспечение дисциплины

Материально-техническое обеспечение программы соответствует действующим санитарно-техническим и противопожарным правилам и нормам и обеспечивает проведение всех видов лекционных, практических занятий и самостоятельной работы бакалавров.

Учебный процесс обеспечен аудиториями, комплектом лицензионного программного обеспечения, библиотекой РГГМУ.

Учебная аудитория для проведения занятий лекционного типа – укомплектована специализированной (учебной) мебелью, презентационной переносной техникой (проектор, экран, ноутбук).

Учебная аудитория для проведения занятий практического типа - укомплектована специализированной (учебной) мебелью, презентационной переносной техникой (проектор, экран, ноутбук).

Учебная аудитория для групповых и индивидуальных консультаций - укомплектована специализированной (учебной) мебелью, презентационной переносной техникой (проектор, экран, ноутбук).

Учебная аудитория для текущего контроля и промежуточной аттестации - укомплектована специализированной (учебной) мебелью, презентационной переносной техникой (проектор, экран, ноутбук), служащей для представления учебной информации.

Помещение для самостоятельной работы – укомплектовано специализированной (учебной) мебелью, оснащено компьютерной техникой с возможностью подключения к сети "Интернет".