ГАОУ ВО «Дагестанский государственный университет народного хозяйства»

Утверждена решением
Ученого совета ДГУНХ,
протокол № 13
от 29 мая 2021 г.

Кафедра «Информационные технологии и информационная безопасность

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«ТЕОРИЯ ЧИСЕЛ»

Направление подготовки

10.03.01 Информационная безопасность,

профиль «Безопасность автоматизированных систем»

Уровень высшего образования - бакалавриат

Формы обучения – очная, очно-заочная

Махачкала – 2021

УДК 681.518(075.8)
ББК 32.81.73

Составитель – Савина Елена Владимировна, кандидат физико-математических наук, доцент кафедры «Информационные технологии и информационная безопасность» ДГУНХ.

Внутренний рецензент - Гасанова Зарема Ахмедовна, кандидат педагогических наук, доцент кафедры «Информационные технологии и информационная безопасность» ДГУНХ.

Внешний рецензент – Абдурагимов Гусейн Эльдарханович, кандидат физико-математических наук, доцент кафедры прикладной математики Дагестанского государственного университета.

Представитель работодателя – Зайналов Джабраил Тажутдинович, директор регионального экспертно-аттестационного центра «Экспертиза», эксперт-представитель работодателя.

Рабочая программа дисциплины «Теория чисел» разработана в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации от 17 ноября 2020 г., № 1427, в соответствии с приказом Министерства образования и науки Российской Федерации от 5.04.2017 г. № 301 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры»

Рабочая программа дисциплины «Теория чисел» размещена на официальном сайте www.dgunh.ru

Савина Е.В. Рабочая программа дисциплины «Теория чисел» для направления подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем». – Махачкала: ДГУНХ, 2021 г., 17 с.

Рекомендована к утверждению Учебно-методическим советом ДГУНХ 28 мая 2021 г.

Рекомендована к утверждению руководителем основной профессиональной образовательной программы высшего образования – программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем», к.пед.н., Гасановой З.А.

Одобрена на заседании кафедры «Информационные технологии и информационная безопасность» 24 мая 2021 г., протокол № 10.

Содержание

Раздел 1. Перечень планируемых результатов обучения по дисциплине

Целью преподавания дисциплины является формирование компетенций в области теории чисел и освоение математических основ криптографии.

Основными задачами дисциплины являются:

- изучение базовых свойств целых чисел;
- изучение модульной арифметики и теории вычетов;
- освоение методов использования расширенного алгоритма Евклида, китайской теоремы об остатках, цепных дробей в прикладных задачах;
- освоение приемов использования теоретико-числовых методов в криптографии.

1.1. Компетенции выпускников, формируемые в результате освоения дисциплины «Теория чисел» как часть планируемых результатов освоения образовательной программы

Код компетенции	Формулировка компетенции
ОПК-3	Способен использовать необходимые математические методы для решения задач профессиональной деятельности

1.2 Планируемые результаты обучения по дисциплине

Код и наименование компетенции	*Код и наименование индикатора достижения компетенции*	*Планируемые результаты обучения по дисциплине*
ОПК-3. Способен использовать необходимые математические методы для решения задач профессиональной деятельности	**ИОПК-3.2**. Анализирует естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности	**Знать:** – базовые понятия теории чисел; – свойства простых и составных чисел; – расширенный алгоритм Евклида; – свойства сравнений по модулю. **Уметь:** – применять расширенный алгоритм Евклида; – использовать теоретико-числовые функции при решении задач; – применять конечные цепные дроби в прикладных задачах. **Владеть:** – навыками применения расширенного алгоритма Евклида и модульной арифметики к решению разных практических задач; – приемами использования канонического разложения в различных задачах; – навыками решения сравнений; – навыками использования цепных дробей.

1.3. Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины

Код компетенции	Этапы формирования компетенций						
	Тема 1. Делимость чисел. НОК, НОД	Тема 2. Простые числа и составные числа. Каноническое разложение	Тема 3. Теоретико-числовые функции	Тема 4. Конечные цепные дроби	Тема 5. Приближение действительных чисел конечными цепными дробями.	Тема 6. Расширенный алгоритм Евклида	Тема 7. Сравнения. Основные свойства сравнений
ОПК-3	+	+	+	+	+	+	+

Код компетенции	Этапы формирования компетенций					
	Тема 8. Системы вычетов. Теоремы Эйлера и Ферма	Тема 9. Китайская теорема об остатках	Тема 10. Сравнения по простому и составному модулю	Тема 11. Квадратные вычеты и невычеты	Тема 12. Алгебраические и трансцендентные числа	Тема 13. Применение теории чисел в криптографии
ОПК-3	+	+	+	+	+	+

Раздел 2. Место дисциплины в структуре образовательной программы

Дисциплина Б1.О.34 «Теория чисел» относится к базовой части Блока 1 «Дисциплины (модули)» Учебного плана по направлению подготовки 10.03.01 Информационная безопасность, профилю «Безопасность автоматизированных систем».

Для успешного освоения курса необходимы знания, умения и навыки курсов «Алгебра» и «Геометрия».

Освоение данной дисциплины необходимо обучающемуся для изучения дисциплин «Теория информации», «Численные методы» и «Криптографические методы защиты информации».

Раздел 3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий), на самостоятельную работу обучающихся и форму промежуточной аттестации

Объем дисциплины в зачетных единицах составляет **4** зачетные единицы.

Очная форма обучения

Количество академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий), составляет **64** часа, в том числе:

на занятия лекционного типа – **32** ч.

на занятия семинарского типа – **32** ч.

Количество академических часов, выделенных на самостоятельную работу обучающихся – **44** ч.

Форма промежуточной аттестации: экзамен – **36** ч.

Очно-заочная форма обучения

Количество академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий), составляет **28** часов, в том числе:

на занятия лекционного типа – **16** ч.

на занятия семинарского типа – **16** ч.

Количество академических часов, выделенных на самостоятельную работу обучающихся – **76** ч.

Форма промежуточной аттестации: экзамен – **36** ч.

Раздел 4. Содержание дисциплины, структурированное по темам с указанием отведенного на них количества академических часов и видов учебных занятий.

Очная форма обучения

№ п/п	Тема дисциплины	Всего академических часов	В т.ч. занятия лекционного типа	В т.ч. занятия семинарского типа:					Самостоятельная работа	Форма текущего контроля успеваемости.
				семинары	Практические занятия	Лабораторные занятия (лабораторные работы, лабораторный практикум)	Коллоквиумы	Иные аналогичные занятия		
1.	Делимость чисел. НОК, НОД.	6	2	-	2	-	-	-	2	Проведение опроса Тестирование Решение задач
2.	Простые числа и составные числа. Каноническое разложение	12	4	-	4	-	-	-	4	Проведение опроса Тестирование Решение задач
3.	Теоретико-числовые функции.	6	2	-	2	-	-	-	2	Проведение опроса Тестирование Решение задач
4.	Конечные цепные дроби.	6	2	-	2	-	-	-	2	Проведение опроса Тестирование Решение задач
5.	Приближение дей-	8	2	-	2	-	-	-	4	Проведение опроса

	ствитель-ных чисел конечными цепными дробями.									Тестирование Решение задач
6.	Расширенный алгоритм Евклида.	12	4	-	4	-	-	-	4	Проведение опроса Тестирование Решение задач
7.	Сравнения. Основные свойства сравнений	6	2	-	2	-	-	-	2	Проведение опроса Тестирование Решение задач
8.	Системы вычетов. Теоремы Эйлера и Ферма.	8	2	-	2	-	-	-	4	Проведение опроса Тестирование Решение задач
9.	Китайская теорема об остатках	10	2	-	4	-	-	-	4	Проведение опроса Тестирование Решение задач
10.	Сравнения по простому и составному модулю	8	2	-	2	-	-	-	4	Проведение опроса Тестирование Решение задач
11.	Квадратные вычеты и невы-	8	2	-	2	-	-	-	4	Проведение опроса Тестирование

	четы									Решение задач
12.	Алгебраические и трансцендентные числа	8	2	-	2	-	-	-	4	Проведение опроса Тестирование Решение задач
13.	Применение теории чисел в криптографии	10	4	-	2	-	-	-	4	Проведение опроса Тестирование Решение задач
	ИТОГО:	**108**	**32**	**-**	**32**	**-**	**-**	**-**	**44**	
	Экзамен (групповая консультация в течение семестра, групповая консультация перед промежуточной аттестацией, экзамен)	**36**								
	ВСЕГО:	**144**								

Очно-заочная форма обучения

№ п/п	Тема дисциплины	Всего академических часов	В т.ч. занятия лекционного типа	В т.ч. занятия семинарского типа:					Самостоятельная работа	Форма текущего контроля успеваемости.
				семинары	Практические занятия	Лабораторные занятия (лабораторные работы, лабораторный практикум)	Коллоквиумы	Иные аналогичные занятия		
1	Делимость чисел. НОК, НОД.	6	-	-	1	-	-	-	5	Проведение опроса Тестирование Решение задач
2	Простые числа и составные числа. Каноническое разложение	12	2	-	1	-	-	-	9	Проведение опроса Тестирование Решение задач
3	Теоретико-числовые функции.	6	-	-	1	-	-	-	5	Проведение опроса Тестирование Решение задач
4	Конечные цепные дроби.	6	2	-	2	-	-	-	2	Проведение опроса Тестирование Решение задач
5	Приближение действитель-	8	1	-	-	-	-	-	7	Проведение опроса Тестирование

	ных чисел конечными цепными дробями.									Решение задач
6	Расширенный алгоритм Евклида.	12	2	-	2	-	-	-	8	Проведение опроса Тестирование Решение задач
7	Сравнения. Основные свойства сравнений	6	1	-	1	-	-	-	4	Проведение опроса Тестирование Решение задач
8	Системы вычетов. Теоремы Эйлера и Ферма.	9	2	-	1	-	-	-	6	Проведение опроса Тестирование Решение задач
9	Китайская теорема об остатках	9	1	-	2	-	-	-	6	Проведение опроса Тестирование Решение задач
10	Сравнения по простому и составному модулю	8	1	-	1	-	-	-	6	Проведение опроса Тестирование Решение задач
11	Квадратные вычеты и невычеты	8	1	-	1	-	-	-	6	Проведение опроса Тестирование Решение за-

										дач
12	Алгебраические и трансцендентные числа	8	1	-	1	-	-	-	6	Проведение опроса Тестирование Решение задач
13	Применение теории чисел в криптографии	10	2	-	2	-	-	-	6	Проведение опроса Тестирование Решение задач
	ИТОГО:	**108**	**16**	**-**	**16**	**-**	**-**	**-**	**80**	
	Экзамен (групповая консультация в течение семестра, групповая консультация перед промежуточной аттестацией, экзамен)	**36**								
	ВСЕГО:	**144**								

Раздел 5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

№ п/п	Автор	Название основной и дополнительной учебной литературы, необходимой для освоения дисциплины	Выходные данные	Количество экземпляров в библиотеке ДГУНХ/адрес доступа
Основная учебная литература				
1.	Данилова Т.В.	Теория чисел: Задачи с примерами решений	Минобрнауки РФ, Северный (Арктический) федеральный университет им. М.В. Ломоносова. – Архангельск: САФУ, 2015. – 104 с.	https://biblioclub.ru/index.php?page=book_red&id=436368&sr=1
2.	Галяев В.С., Гасанова З.А.	Учебное пособие по дисциплине «Теория чисел» для направления подготовки «Информационная безопасность», профиля «Безопасность информационных систем»	Махачкала: ДГУНХ, 2016. – 66 с.	http://www.dgunh.ru/content/glavnay/ucheb_deyatel/uposob/up-it_ib-fgos-50.pdf
Дополнительная литература				
А) Дополнительная учебная литература				
1.	Виноградов И.М.	Основы теории чисел	Изд. 6-е, испр. - Москва; Ленинград: Государственное издательство технико-теоретической литературы, 1952. - 181 с.	http://biblioclub.ru/index.php?page=book&id=449924
2.	Вейль А.	Основы теории чисел	Москва: Мир, 1972. – 411 с.	http://biblioclub.ru/index.php?page=book&id=454858
3.		Алгебраические числа=Algebraic numbers : монография / С. Ленг; ред. Л.Б. Штейнпресс, пер. с англ. Ю.И. Манина.	Москва: Мир, 1966. - 224 с.	http://biblioclub.ru/index.php?page=book&id=450339
4.	Кнауб Л.В.	Теоретико-численные методы в криптографии	Минобрнауки РФ, Сибирский Федеральный универ-	https://biblioclub.ru/index.php?page=book_red

			ситет. – Красноярск: Сибирский федеральный университет, 2011. – 160 с.	&id=229582&sr=1
Б) Официальные издания: сборники законодательных актов, нормативно-правовых документов и кодексов РФ				
1.	ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования www.standartgost.ru			
В) Периодические издания				
1.	Научный журнал «Прикладная дискретная математика».			
2.	Информатика и безопасность.			
3.	Рецензируемый научный журнал «Проблемы информационной безопасности».			

Раздел 6. Перечень ресурсов информационно-телекоммуникационной сети Интернет, необходимых для освоения дисциплины

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к одной или нескольким электронно-библиотечным системам и к электронной информационно-образовательной среде университета (http://e-dgunh.ru). Электронно-библиотечная система и электронная информационно-образовательная среда обеспечивает возможность доступа, обучающегося из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети Интернет, как на территории университета, так и вне ее.

Для самостоятельного изучения материала и ознакомления с регламентирующими документами и текущей практикой в области информационной безопасности, рекомендуется использовать следующие Интернет-ресурсы:

1. http://www.math.ru/lib/ - Электронная библиотека
2. http://allsummary.ru – Конспекты лекций по техническим, экономическим и юридическим предметам.
3. http://dvoika.net - Высшая математика, физика, теоретические основы электротехники, информатика - лекции, курсовые, примеры решения задач, интегралы и производные, ТФКП
4. http://www.fxyz.ru/ -Интерактивный справочник формул и сведения по алгебре, тригонометрии, геометрии, физике.
5. http://ilib.mccme.ru/plm/ Лекции по математике.
6. http://xplusy.isnet.ru/ Решения типовых студенческих задач из различных разделов высшей Математики.

Раздел 7. Перечень лицензионного программного обеспечения, информационных справочных систем и профессиональных баз данных

7.1. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства:

- Windows 10
- Microsoft Office Professional
- Adobe Acrobat Reader DC
- VLC Media player
- 7-zip

7.2. Перечень информационных справочных систем:

- не предусмотрены

7.3. Перечень профессиональных баз данных:

- научная электронная библиотека https://elibrary.ru/ и др.

Раздел 8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для преподавания дисциплины «Теория чисел» используются следующие специальные помещения – **учебные аудитории**:

Учебная аудитория для проведения учебных занятий № 3.3 (Россия, Республика Дагестан, 367008, г. Махачкала, ул. ДжамалутдинаАтаева, дом 5, учебный корпус № 2 литер «В»)

Перечень основного оборудования:

Комплект специализированной мебели.

Доска меловая.

Набор демонстрационного оборудования: проектор, персональный компьютер с доступом к сети Интернет и корпоративной сети университета, ЭБС «Университетская библиотека ONLINE» (www.biblioclub.ru), ЭБС «ЭБС Юрайт» (www.urait.ru), акустическая система.

***Перечень учебно-наглядных пособий*:**

Комплект наглядных материалов (баннеры, плакаты);

Комплект электронных иллюстративных материалов (презентации, видеоролики).

Помещение для самостоятельной работы № 4.5 (*Россия, Республика Дагестан, 367008, г. Махачкала, ул. Джамалутдина Атаева, дом 5, учебный корпус № 2 литер «В»*)

Перечень основного оборудования:

Персональные компьютеры с доступом к сети «Интернет» и в электронную информационно-образовательную среду – 19 ед.

Помещение для самостоятельной работы № 1-1 (*Россия, Республика Дагестан, 367008, г. Махачкала, ул. Джамалутдина Атаева, дом 5, учебный корпус № 1*)

Перечень основного оборудования:

Персональные компьютеры с доступом к сети «Интернет» и в электронную информационно-образовательную среду – 60 ед.

Раздел 9. Образовательные технологии

Образовательные технологии, используемые при проведении учебных занятий по дисциплине «Теория чисел», обеспечивают развитие у обучающихся необходимых знаний и навыков.

На занятиях лекционного типа применяются такие методы обучения как Управляемая дискуссия, Проблемная лекции.

На практических занятиях, целью которых является приобретение учащимися определенных практических умений, научить их аналитически мыслить, эффективными будут такие методы как решение задач, дискуссии.

Лист актуализации рабочей программы дисциплины

«Теория чисел»

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от «_____»_____ 20___ г. №_____

Зав. кафедрой _____

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от «_____»_____ 20___ г. №_____

Зав. кафедрой _____

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от «_____»_____ 20___ г. №_____

Зав. кафедрой _____

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от «_____»_____ 20___ г. №_____

Зав. кафедрой _____