

ГАОУ ВО «Дагестанский государственный университет народного хозяйства»

*Утверждена решением
Ученого совета ДГУНХ,
протокол № 11
от 06 июня 2023 г*

**Кафедра «Информационные технологии и информационная
безопасность»**

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«ТЕОРИЯ ЧИСЕЛ»**

**Специальность 10.02.05 Обеспечение информацион-
ной безопасности автоматизированных систем**

Квалификация – техник по защите информации

Форма обучения – очная

Махачкала – 2023

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 среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утверждённого приказом Министерства образования и науки Российской Федерации от 9 декабря 2016 г., № 1553, в соответствии с приказом Минпросвещения России от 24.08.2022 г., № 762 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам среднего профессионального образования».

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

Савина Е.В. Рабочая программа дисциплины «Теория чисел» для специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем. – Махачкала: ДГУНХ, 2021 г., 12 с.

Рекомендована к утверждению Учебно-методическим советом ДГУНХ 06 апреля 2021 г.

Рекомендована к утверждению руководителем образовательной программы СПО – программы подготовки специалистов среднего звена по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, к.пед.н., Гасановой З.А.

Одобрена на заседании кафедры «Информационные технологии и информационная безопасность» 03 апреля 2021 г, протокол № 10.

Содержание

Раздел 1.	Перечень планируемых результатов обучения по дисциплине	4
Раздел 2.	Место дисциплины в структуре образовательной программы	5
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	6
Раздел 4.	Содержание дисциплины, структурированное по темам с указанием отведенного на них количества академических часов и видов учебных занятий	7
Раздел 5.	Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	10
Раздел 6.	Перечень ресурсов информационно-телекоммуникационной сети Интернет, необходимых для освоения дисциплины	11
Раздел 7.	Перечень лицензионного программного обеспечения, информационных справочных систем и профессиональных баз данных	11
Раздел 8.	Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине	12
Раздел 9.	Образовательные технологии	12

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
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам

1.2 Планируемые результаты обучения по дисциплине

Код компетенции	Формулировка компетенции	Знания, умения
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	<p>Умения: распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы;</p> <p>владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника).</p> <p>Знания: актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте.</p> <p>алгоритмы выполнения работ в профессио-</p>

		нальной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности.
--	--	---

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.
ОК 01.	+	+	+	+	+

Код компетенции	Этапы формирования компетенций				
	Тема 6. Расширенный алгоритм Евклида	Тема 7. Сравнения. Основные свойства сравнений	Тема 8. Системы вычетов. Теоремы Эйлера и Ферма	Тема 9. Китайская теорема об остатках	Тема 10. Сравнения по простому и составному модулю
ОК 01.	+	+	+	+	+

Код компетенции	Этапы формирования компетенций		
	Тема 11. Квадратные вычеты и невычеты	Тема 12. Алгебраические и трансцендентные числа	Тема 13. Применение теории чисел в криптографии
ОК 01.	+	+	+

Раздел 2. Место дисциплины в структуре образовательной программы

Дисциплина «ОП.09 Теория чисел» относится к общепрофессиональному циклу учебного плана по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Для успешного освоения курса необходимы знания, умения и навыки курса «Математика».

Освоение данной дисциплины необходимо обучающемуся для изучения дисциплин «Основы теории информации», «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

Количество академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий), составляет **76** часов, в том числе:

на занятия лекционного типа – **38** ч.

на занятия семинарского типа – **38** ч.

Количество академических часов, выделенных на самостоятельную работу обучающихся – **0** ч.

Форма промежуточной аттестации: зачет.

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

№ 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.	4	2	-	2	-	-	-		Проведение опроса Тестирование Решение задач
2.	Простые числа и составные числа. Каноническое разложение	8	4	-	4	-	-	-		Проведение опроса Тестирование Решение задач
3.	Теоретико-числовые функции.	4	2	-	2	-	-	-		Проведение опроса Тестирование Решение задач
4.	Конечные цепные дроби.	4	2	-	2	-	-	-		Проведение опроса Тестирование Решение задач

5.	Приближе- ние дей- ствитель- ных чисел конечными цепными дробями.	4	2	-	2	-	-	-	Проведение опроса Тестирование Решение за- дач
6.	Расширен- ный алго- ритм Ев- клида.	8	4	-	4	-	-	-	Проведение опроса Тестирование Решение за- дач
7.	Сравнения. Основные свойства сравнений	4	2	-	2	-	-	-	Проведение опроса Тестирование Решение за- дач
8.	Системы вычетов. Теоремы Эйлера и Ферма.	4	2	-	2	-	-	-	Проведение опроса Тестирование Решение за- дач
9.	Китайская теорема об остатках	6	2	-	4	-	-	-	Проведение опроса Тестирование Решение за- дач
10.	Сравнения по про- стому и составно- му модулю	8	4	-	4	-	-	-	Проведение опроса Тестирование Решение за- дач
11.	Квадрат-	8	4	-	4	-	-	-	Проведение

	ные вычеты и невычеты									опроса Тестирование Решение задач
12.	Алгебраические и трансцендентные числа	6	4	-	2	-	-	-		Проведение опроса Тестирование Решение задач
13.	Применение теории чисел в криптографии	6	4	-	2	-	-	-		Проведение опроса Тестирование Решение задач
14.	Зачет	2			2					
	ИТОГО:	76	38	-	38	-	-	-		

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.	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
Дополнительная литература				
А) Дополнительная учебная литература				
1.	Вейль А.	Основы теории чисел	Москва: Мир, 1972. – 411 с.	http://biblioclub.ru/index.php?page=book&id=454858
2.		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
3.	Кнауб Л.В.	Теоретико-численные методы в криптографии	Минобрнауки РФ, Сибирский Федеральный университет. – Красноярск: Сибирский федеральный университет, 2011. – 160 с.	https://biblioclub.ru/index.php?page=book_red&id=229582&sr=1

4.			
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.fxuz.ru/> -Интерактивный справочник формул и сведения по алгебре, тригонометрии, геометрии, физике.
5. <http://ilib.mcsme.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**:

Кабинет математических дисциплин, учебная аудитория для проведения занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации (367008, Республика Дагестан, г. Махачкала, пр-кт Али-Гаджи Акушинского, д 20, учебный корпус № 1, литер А, этаж 1, помещение № 5.)

Перечень основного оборудования:

Комплект учебной мебели,

Доска меловая,

Набор технических средств: персональный компьютер с доступом к сети Интернет и корпоративной сети университета, ЭБС «Университетская библиотека ONLINE» (www.biblioclub.ru), ЭБС «ЭБС Юрайт» (www.urait.ru).

Перечень учебно-наглядных пособий:

Комплект наглядных материалов (баннеры, плакаты);

Комплект электронных иллюстративных материалов (презентации, видеоролики)..

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 лекция.

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