ГАОУ ВО «Дагестанский государственный университет народного хозяйства»

Утверждена решением
Ученого совета ДГУНХ,
протокол № 13
от 06 июля 2020 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

Форма обучения – очная

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 01D74C9001F08320000000072C4B0002
Владелец: Бучаев Ахмед Гамидович
Действителен: с 19.05.2021 до 19.05.2022

Махачкала – 2020

УДК 681.518(075.8)
ББК 32.81.73

Составитель – Галяев Владимир Сергеевич, кандидат физико-математических наук, доцент, заведующий кафедрой «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 1 декабря 2016 г., № 1515, 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

Галяев В.С. Рабочая программа дисциплины «Теория чисел» для направления подготовки 10.03.01 «Информационная безопасность», профиль «Безопасность автоматизированных систем». – Махачкала: ДГУНХ, 2020 г., 13 с.

Рекомендована к утверждению Учебно-методическим советом ДГУНХ 03 июля 2020 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» 30 июня 2020 г., протокол № 12

Содержание

Раздел 1. Перечень планируемых результатов обучения по дисциплине

Целью преподавания дисциплины является сформировать компетенции в области теории чисел и сформулировать математические основы криптографии.

Основными задачами дисциплины являются:

- Рассмотреть основные теоремы и закономерности теории чисел, необходимые для дальнейшего изучения криптографии;
- Освоить методики вычисления значений теоретико-числовых функций;
- Освоить методики применения конечных цепных дробей в прикладных задачах;
- Раскрыть принципы решения сравнений по произвольному модулю.

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

код компетенции	формулировка компетенции
ОПК	**ОБЩЕПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ**
ОПК-2	способность применять соответствующий математический аппарат для решения профессиональных задач

1.2 Планируемые результаты обучения по дисциплине

код и формулировка компетенции	компонентный состав компетенции		
	Знать:	Уметь:	Владеть:
ОПК-2: способность применять соответствующий математический аппарат для решения профессиональных задач	З1 - основные числовые закономерности; З2 - взаимосвязи между свойствами чисел; З3 - числовых последовательностей.	У1 - решать сравнения по произвольному модулю; У2 - применять конечные цепные дроби в прикладных задачах.	В1 - вычисления значений теоретико-числовых функций; В2 - нахождения канонического разложения числа; В3 - решения сравнений по простому модулю В4 - навыками решения системы сравнений

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

Код компетенции	Этапы формирования компетенций
	Тема 1. Делимость чисел. Наибольший общий делитель. Наименьшее общее кратное
	Тема 2. Простые числа
	Тема 3. Теоретико-числовые функции
	Тема 4. Конечные цепные дроби
	Тема 5. Приближение действительных чисел конечными цепными дробями. Теорема Дирихле
	Тема 6. Сравнения. Основные свойства сравнений
	Тема 7. Системы вычетов. Теоремы Эйлера и Ферма
	Тема 8. Системы сравнений
	Тема 9. Сравнения по простому и составному модулю
	Тема 10. Квадратные вычеты и невычеты. Критерий Эйлера
	Тема 11. Алгебраические и трансцендентные числа.
ОПК-2	+

Раздел 2. Место дисциплины в структуре образовательной программы

Дисциплина Б1.Б.34 «Теория чисел» относится к базовой части Блока 1 «Дисциплины (модули)» Учебного плана по направлению подготовки «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 «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.

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.

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.	Тема 1. Делимость чисел. Наибольший общий делитель. Наименьшее общее кратное.	8	2	-	2	-	-	-	4	Проведение опроса Тестирование Решение задач
2.	Тема 2. Простые числа.	8	2	-	2	-	-	-	4	Проведение опроса Тестирование Решение задач
3.	Тема 3. Теоретико-числовые функции.	12	4	-	4	-	-	-	4	Проведение опроса Тестирование Решение задач
4.	Тема 4. Конечные	8	2	-	2	-	-	-	4	Проведение опроса

	цепные дроби.									Тестирование Решение задач
5.	Тема 5. Приближение действительных чисел конечными цепными дробями. Теорема Дирихле.	12	4	-	4	-	-	-	4	Проведение опроса Тестирование Решение задач
6.	Тема 6. Сравнения. Основные свойства сравнений.	12	4	-	4	-	-	-	4	Проведение опроса Тестирование Решение задач
7.	Тема 7. Системы вычетов. Теоремы Эйлера и Ферма.	8	2	-	2	-	-	-	4	Проведение опроса Тестирование Решение задач
8.	Тема 8. Системы сравнений.	8	2	-	2	-	-	-	4	Проведение опроса Тестирование Решение задач
9.	Тема 9. Сравнения	8	2	-	2	-	-	-	4	Проведение опроса

	по простому и составному модулю.									Тестирование Решение задач
10.	Тема 10. Квадратные вычеты и невычеты. Критерий Эйлера.	12	4	-	4	-	-	-	4	Проведение опроса Тестирование Решение задач
11.	Тема 11. Алгебраические и трансцендентные числа.	12	4	-	4	-	-	-	4	Проведение опроса Тестирование Решение задач
12	**ИТОГО:**	**108**	**32**	**-**	**32**	**-**	**-**	**-**	**44**	
	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.	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
2.	Данилова Т.В.	Теория чисел: Задачи с примерами решений	Министерство образования и науки Российской Федерации, Северный (Арктический) федеральный университет имени М.В. Ломоносова. – Архангельск : САФУ, 2015. – 104 с.	https://biblioclub.ru/index.php?page=book_red&id=436368&sr=1
Дополнительная учебная литература				
а) Дополнительная учебная литература				
1.		Алгебра и теория чисел : учебное пособие / М.М. Михалева, Б.М. Веретенников	Министерство образования и науки Российской Федерации, Уральский федеральный университет им. первого Президента России Б. Н. Ельцина. - Екатеринбург : Издательство Уральского университета, 2014. - Ч. 1. - 51 с.	http://biblioclub.ru/index.php?page=book&id=276012
2.		Алгебраические числа=Algebraic numbers : монография / С. Ленг; ред.	Москва : Мир, 1966. - 224 с. : ил.	http://biblioclub.ru/index.php?page=book&id=4

		Л.Б. Штейнпресс, пер. с англ. Ю.И. Манина.		50339
3.	Вейль А.	Основы теории чисел	Москва : Мир, 1972. – 411 с.	http://biblioclub.ru/index.php?page=book&id=454858
4.	Виноградов И.М.	Основы теории чисел	Изд. 6-е, испр. - Москва ; Ленинград : Государственное издательство технико-теоретической литературы, 1952. - 181 с. : ил.	http://biblioclub.ru/index.php?page=book&id=449924
5.	Кнауб Л.В.	Теоретико-численные методы в криптографии	Министерство образования и науки Российской Федерации, Сибирский Федеральный университет. – Красноярск : Сибирский федеральный университет, 2011. – 160 с.	https://biblioclub.ru/index.php?page=book_red&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, обуча-

ющегося 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. Необходимый комплект лицензионного программного обеспечения:

- 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 занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации № 3.1 (*Россия, Республика Дагестан, 367008, г. Махачкала, ул. Джамалутдина Атаева, дом 5, учебный корпус № 2 литер «В»*)

Перечень основного оборудования:

Комплект специализированной мебели.

Доска меловая.

Набор демонстрационного оборудования: проектор, персональный компьютер (моноблок) 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).

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 «22» мая 2021 №10

Зав. кафедрой Галкин В.С.

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от «____»_____20___ №___

Зав. кафедрой_____

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от «____»_____20___ №___

Зав. кафедрой_____

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от «____»_____20___ №___

Зав. кафедрой_____