

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Алтайский государственный технический университет им. И.И. Ползунова»

СОГЛАСОВАНО

Декан ФИТ

А.С. Авдеев

Рабочая программа дисциплины

Код и наименование дисциплины: **Б1.Б.36 «Основы теории чисел»**

Код и наименование направления подготовки (специальности): **10.03.01**

Информационная безопасность

Направленность (профиль, специализация): **Организация и технология защиты информации**

Статус дисциплины: **обязательная часть (базовая)**

Форма обучения: **очная**

Статус	Должность	И.О. Фамилия
Разработал	доцент	Р.В. Дегтерева
Согласовал	Зав. кафедрой «ИВТиИБ»	А.Г. Якунин
	руководитель направленности (профиля) программы	Е.В. Шарлаев

г. Барнаул

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции из УП и этап её формирования	Содержание компетенции	В результате изучения дисциплины обучающиеся должны:		
		знать	уметь	владеть
ОПК-2	способностью применять соответствующий математический аппарат для решения профессиональных задач	<p>понятия, методы, модели разделов математики, необходимые для решения профессиональных задач, в том числе основные теоретико-числовые понятия; основные результаты о делимости целых чисел и теории сравнений; основные алгоритмы решения стандартных задач.</p>	<p>- использовать математические методы для решения профессиональных задач; - строить математические модели задач профессиональной области, в том числе применять теорему о делении с остатком и свойства делимости к решению различных арифметических задач; применять алгоритм Евклида для нахождения наибольшего общего делителя целых чисел, его линейного разложения и наименьшего общего кратного; используя "решето" Эратосфена, составлять таблицы простых чисел и решать задачи на применение основной теоремы арифметики и свойств простых чисел. находить разложение заданного рационального числа в конечную цепную дробь, вычислять подходящие дроби и применять свойства подходящих дробей при решении задач; применять</p>	<p>навыками применения математических расчетов для решения профессиональных задач</p>

Код компетенции из УП и этап её формирования	Содержание компетенции	В результате изучения дисциплины обучающиеся должны:		
		знать	уметь	владеть
			<p>определение и свойства сравнений по заданному модулю при составлении полной и приведённой систем вычетов; вычислять значения функции Эйлера и остатки арифметических выражений от деления на заданное число, используя свойства сравнений и теоремы Эйлера и Ферма.</p> <p>решать различными способами линейные сравнения первой степени с одним неизвестным.</p> <p>применять обобщённый признак делимости Паскаля для конструирования конкретных признаков делимости.</p> <p>проверять правильность выполнения простейших арифметических действий с помощью сравнений.</p>	

2. Место дисциплины в структуре образовательной программы

Дисциплины (практики), предшествующие изучению дисциплины, результаты освоения которых необходимы для освоения данной дисциплины.	Дискретная математика, Математика
Дисциплины (практики), для которых результаты освоения данной дисциплины будут необходимы, как входные знания, умения и владения для	Криптографические методы защиты информации, Математическая логика и теория алгоритмов

их изучения.

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

Общий объем дисциплины в з.е. /час: 3 / 108

Форма промежуточной аттестации: Зачет

Форма обучения	Виды занятий, их трудоемкость (час.)				Объем контактной работы обучающегося с преподавателем (час)
	Лекции	Лабораторные работы	Практические занятия	Самостоятельная работа	
очная	17	0	17	74	45

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

Форма обучения: очная

Семестр: 3

Лекционные занятия (17ч.)

1. Теория делимости в кольце целых чисел(2ч.)[2,3] Теорема о делении с остатком. Делимость нацело и её свойства. Наибольший общий делитель. Алгоритм Евклида. Линейное разложение НОД. Наименьшее общее кратное. Взаимно простые числа и их свойства

2. Основная теорема арифметики. Решето Эратосфена. {лекция с разбором конкретных ситуаций} (2ч.)[2,3] Простые числа и их свойства. Основная теорема арифметики. Описание делителей натурального числа. Количество и сумма делителей натурального числа. Нахождение НОД и НОК с помощью канонических разложений. Бесконечность количества простых чисел в арифметических прогрессиях. Решето Эратосфена.

3. Подходящие дроби и их основные свойства.(2ч.)[2,3] Конечные цепные дроби. Подходящие дроби и их основные свойства. Теорема о представлении рациональных чисел конечными цепными дробями. Применение конечных цепных дробей к нахождению линейного разложения НОД.

4. Теория сравнений {дискуссия} (2ч.)[2] Отношение сравнимости по модулю и его основные свойства. Мультипликативные функции. Функция Эйлера и её основные свойства. Теоремы Эйлера и Ферма.

5. Сравнения и системы сравнений(2ч.)[2,3] Китайская теорема об остатках. Структура решений линейного сравнения первой степени.

6. Арифметические приложения теории сравнений.(2ч.)[1,2] Неопределенные уравнения.

Системы сравнений. Решение систем сравнений.

7. Системы счисления {беседа} (2ч.)[1,2] Переход от одной системы счисления в другую. Решение задач в разных системах счисления.

8. Обзорная лекция(3ч.)[4] Повторение пройденного материала. Разбор сложных задач. Подготовка к зачету

Практические занятия (17ч.)

1. Простые числа(2ч.)[1,2] Простые числа и их свойства. Основная теорема арифметики. Бесконечность количества простых чисел в арифметических прогрессиях. Решето Эратосфена.

2. Делимость в кольце целых чисел {образовательная игра} (2ч.)[1,2] Делимость нацело и её свойства. Наибольший общий делитель. Алгоритм Евклида. Линейное разложение НОД. Наименьшее общее кратное. Взаимно простые числа и их свойства

3. Конечные цепные дроби.(2ч.)[1,3] Подходящие дроби и их основные свойства. Теорема о представлении рациональных чисел конечными цепными дробями. Применение конечных цепных дробей к нахождению линейного разложения НОД.

4. Контрольная работа по теме 1.(2ч.)[4]

5. Теория сравнений(2ч.)[1,3] Отношение сравнимости по модулю и его основные свойства. Мультипликативные функции. Функция Эйлера и её основные свойства. Теоремы Эйлера и Ферма.

6. Китайская теорема об остатках. Структура решений линейного сравнения первой степени. {творческое задание} (2ч.)[1,3] Сравнения первой степени и их решение. Неопределенные уравнения.

Системы сравнений. Решение систем сравнений.

7. Системы счисления(3ч.)[1,4] Арифметические приложения теории сравнений. Системы счисления и их применение при решении задач.

8. Контрольная работа по теме 2.(2ч.)[1]

Самостоятельная работа (74ч.)

1. Подготовка к практическим занятиям(17ч.)[2,3]

2. Подготовка к контрольным работам(21ч.)[1,4]

3. Выполнение домашнего задания {разработка проекта} (24ч.)[2,3]

4. Подготовка к зачету(12ч.)[2,2]

5. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

Для каждого обучающегося обеспечен индивидуальный неограниченный доступ к электронно-библиотечным системам: Лань, Университетская библиотека он-лайн, электронной библиотеке АлтГТУ и к электронной информационно-образовательной среде:

1. Данилова Т.В. Теория чисел: Задачи с примерами решений: Учебное пособие. Архангельск: САФУ, 2015. Доступ из ЭБС «Университетская библиотека Online» Режим доступа: <http://biblioclub.ru/index.php?page=book&id=436368>

6. Перечень учебной литературы

6.1. Основная литература

2. Виноградов, И.М. Основы теории чисел [Электронный ресурс] : учебное пособие / И.М. Виноградов. — Электрон. дан. — Санкт-Петербург : Лань, 2009. — 176 с. — Режим доступа: <https://e.lanbook.com/book/46>. — Загл. с экрана.

3. Веселова Л. В., Тихонов О. Е. Алгебра и теория чисел: учебное пособие. Казань: Издательство КНИТУ, 2014. Доступ из ЭБС «Университетская библиотека Online» Режим доступа: <http://biblioclub.ru/index.php?page=book&id=428287>

6.2. Дополнительная литература

4. Ермолаева, Н.Н. Практические занятия по алгебре. Элементы теории множеств, теории чисел, комбинаторики. Алгебраические структуры [Электронный ресурс] : учебное пособие / Н.Н. Ермолаева, В.А. Козынченко, Г.И. Курбатова ; под ред. Курбатовой Г.И.. — Электрон. дан. — Санкт-Петербург : Лань, 2014. — 112 с. — Режим доступа: <https://e.lanbook.com/book/49469>. — Загл. с экрана.

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

5. <http://window.edu.ru> Единое окно доступа к образовательным ресурсам

8. Фонд оценочных материалов для проведения текущего контроля успеваемости и промежуточной аттестации

Содержание промежуточной аттестации раскрывается в комплекте контролирующих материалов, предназначенных для проверки соответствия уровня подготовки по дисциплине требованиям ФГОС, которые хранятся на кафедре-разработчике РПД в печатном виде и в ЭИОС.

Фонд оценочных материалов (ФОМ) по дисциплине представлен в приложении А.

9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

Для успешного освоения дисциплины используются ресурсы электронной информационно-образовательной среды, образовательные интернет-порталы, глобальная компьютерная сеть Интернет. В процессе изучения дисциплины происходит интерактивное взаимодействие обучающегося с преподавателем через личный кабинет студента.

№пп	Используемое программное обеспечение
1	LibreOffice
2	Windows
3	Антивирус Kaspersky

№пп	Используемые профессиональные базы данных и информационные справочные системы
1	Бесплатная электронная библиотека онлайн "Единое окно к образовательным ресурсам" для студентов и преподавателей; каталог ссылок на образовательные интернет-ресурсы (http://Window.edu.ru)
2	Национальная электронная библиотека (НЭБ) — свободный доступ читателей к фондам российских библиотек. Содержит коллекции оцифрованных документов (как открытого доступа, так и ограниченных авторским правом), а также каталог изданий, хранящихся в библиотеках России. (http://нэб.рф/)

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

Наименование специальных помещений и помещений для самостоятельной работы
учебные аудитории для проведения занятий лекционного типа
учебные аудитории для проведения занятий семинарского типа
учебные аудитории для проведения групповых и индивидуальных консультаций
учебные аудитории для проведения текущего контроля и промежуточной аттестации
помещения для самостоятельной работы

Материально-техническое обеспечение и организация образовательного процесса по дисциплине для инвалидов и лиц с ограниченными возможностями здоровья осуществляется в соответствии с «Положением об обучении инвалидов и лиц с ограниченными возможностями здоровья».