Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук

УТВЕРЖДЕНО:
Директор
А. В. Замятин

Рабочая программа дисциплины

Теория чисел

по направлению подготовки / специальности

10.05.01 Компьютерная безопасность

Направленность (профиль) подготовки/ специализация:
Анализ безопасности компьютерных систем

Форма обучения
Очная

Квалификация
Специалист по защите информации

Год приема
2024

СОГЛАСОВАНО:
Руководитель ОП
В.Н. Тренькаев

Председатель УМК
С.П. Сущенко

Томск – 2024

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-3 Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-3.1 Демонстрирует навыки выполнения стандартных действий, решения типовых задач, формулируемых в рамках базовых математических дисциплин

ИОПК-3.2 Осуществляет применение основных понятий, фактов, концепций, принципов математики и информатики для решения задач профессиональной деятельности

ИОПК-3.3 Выявляет научную сущность проблем, возникающих в ходе профессиональной деятельности, и применяет соответствующий математический аппарат для их формализации, анализа и выработки решения

2. Задачи освоения дисциплины

– Освоить аппарат теории чисел, методы решения сравнений и систем сравнений.

– Научиться применять понятийный аппарат теории чисел для решения практических задач профессиональной деятельности.

3. Место дисциплины в структуре образовательной программы

Дисциплина относится к Блоку 1 «Дисциплины (модули)».

Дисциплина относится к обязательной части образовательной программы. Дисциплина входит в «Модуль «Математика».

4. Семестр(ы) освоения и форма(ы) промежуточной аттестации по дисциплине

Третий семестр, экзамен

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются результаты обучения по следующим дисциплинам: введение в математику, общая алгебра.

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 4 з.е., 144 часов, из которых:
-лекции: 32 ч.
-практические занятия: 32 ч.
Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

Тема 1. Делимость и простые числа.
Делимость и простые числа. Теорема о делении с остатком. НОД чисел.
Алгоритм Евклида. Простые числа. Основная теорема арифметики.
Арифметические функции. Мультипликативные функции и их примеры.
Цепные дроби.

Тема 2. Сравнения

Сравнения 1-й степени
Сравнения n-степени.
Сравнения 2-степени
Первообразные корни и индексы.

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем контроля посещаемости, проведения контрольных работ, тестов по лекционному материалу и фиксируется в форме контрольной точки не менее одного раза в семестр.

Оценочные материалы текущего контроля размещены на сайте ТГУ в разделе «Информация об образовательной программе» - https://www.tsu.ru/sveden/education/eduop/.

10. Порядок проведения и критерии оценивания промежуточной аттестации

Экзамен в третьем семестре проводится в письменной форме по билетам. Экзаменационный билет состоит из двух частей. Продолжительность экзамена 1,5 часа.

Первая часть содержит один вопрос, проверяющий ИОПК-2.2. Ответ на вопрос второй части дается в развернутой форме.

Третья часть содержит 2 вопроса, проверяющих ИПК-3.3 и ИУК-1.1 и оформленные в виде практических задач. Ответы на вопросы третьей части предполагают решение задач и краткую интерпретацию полученных результатов.

Примеры теоретических вопросов

1) Мультипликативность функции $\tau(n)$. Доказать, что если $n = p^{\alpha}\ldots q^{\gamma}$ – каноническое разложение числа n, то $\tau(n) = (\alpha + 1)\ldots(\gamma + 1)$.

2) Мультипликативность функции $\sigma(n)$. Доказать, что если $n = p^{\alpha}\ldots q^{\gamma}$ – каноническое разложение числа n, то $\sigma(n) = [(p^{\alpha} - 1)\ldots(q^{\gamma} - 1)]/[(p - 1)\ldots(q - 1)]$.

3) Примеры совершенных чисел. Доказать, что четное число n является совершенным тогда и только тогда, когда $n = 2^{a-1}(2^a - 1)$, где $a \geq 2$ и $2^a - 1$ – простое число.

4) Доказать, что если $2^a - 1$ – простое число, то число a также простое.

5) Докажите мультипликативность функции Мебиуса $\mu(n)$.

Примеры задач:

Вариант 1

1. Методом решета все простые числа между 118 и 131.
2. При каких натуральных n числа n, $n + 13$, $n + 17$ являются простыми?
3. Пусть $a = 248$, $b = 182$. При помощи расширенного алгоритма Евклида найти их НОД.
4. Найдите сумму и число всех натуральных делителей следующих чисел:
1) 165; 2) 270; 3) 363.

Вариант 2

1. Методом решета все простые числа между 870 и 900.
2. Сколько натуральных чисел ≤ 210, не делящихся ни на 3, ни на 5?
3. Пусть $a = 138$, $b = 162$. При помощи расширенного алгоритма Евклида найти их НОД.
4. Найдите каноническое разложение числа 30!

Вариант 3

1. Методом решета все простые числа между 110 и 130.
2. При каких натуральных n числа n, $n + 5$, $n + 9$, $n + 19$ являются простыми?
3. Разложите в непрерывную дробь: –15/57 и $-\sqrt{15}$.
4. Вычислить символы Лежандра: (18/29) и (13/41).

Результаты экзамена определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

1) Полный ответ, изложенный кратко и ясно – «отлично».

2) Ответ неполный (но > 80%), пояснения логически непротиворечивы – «хорошо».

3) Ответ неполный (но > 50%), есть проблемы в логике и пояснениях – «удовлетворительно».

4) Ответ неполный (< 50%), отсутствие логики в пояснениях – «неудовлетворительно».

Оценочные материалы для проведения промежуточной аттестации размещены на сайте ТГУ в разделе «Информация об образовательной программе» - https://www.tsu.ru/sveden/education/eduop/.

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в LMS IDO
- https://lms.tsu.ru/course/view.php?id=33412

б) Оценочные материалы текущего контроля и промежуточной аттестации по дисциплине.

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

Бухштаб А. А.	Теория чисел	СПб.: Лань	2015 г., 384 с.
Виноградов И.М.	Основы теории чисел	СПб.: Лань	2006 г., 176 с.

б) дополнительная литература:

Деза Е. И., Котова Л. В.	Сборник задач по теории чисел.	М.: Либроком/URSS	2012 г., 224 с.
Манин Ю. И., Панчишкин А.А.	Введение в современную теорию чисел.	М.: МЦНМО	2013 г., 552 с.
Сушкевич А.К.	Теория чисел.	М.: Вузовская книга	2016 г., 240 с.

в) ресурсы сети Интернет:

1) http://alexhvorost.narod2.ru/

2) https://ru.wikipedia.org/wiki/Теория_чисел

3) Электронный учебный курс по дисциплине в электронном университете «Moodle» - https://moodle.tsu.ru/course/view.php?id=33412

13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:
ОС Windows, пакет Microsoft Office

б) информационные справочные системы:

– Электронный каталог Научной библиотеки ТГУ – http://chamo.lib.tsu.ru/search/query?locale=ru&theme=system

– Электронная библиотека (репозиторий) ТГУ – http://vital.lib.tsu.ru/vital/access/manager/Index

– ЭБС Лань – http://e.lanbook.com/

14. Материально-техническое обеспечение

Аудитории для проведения занятий лекционного типа.

Аудитории для проведения занятий семинарского типа, индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации.

15. Информация о разработчиках

Приходовский Михаил Анатольевич, канд. физ.-мат. наук, доцент, доцент кафедры компьютерной безопасности ТГУ.