МИНПРОСВЕЩЕНИЯ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования "Тульский государственный педагогический университет им. Л.Н. Толстого"

(ФГБОУ ВО "ТГПУ им. Л.Н. Толстого")

Теория чисел и элементы криптографии

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **кафедра алгебры, математического анализа и геометрии**

ОПОП **Направление 02.03.01 Математика и компьютерные науки**
направленность (профиль) Математические основы компьютерных наук

Квалификация **Бакалавр**

Год начала подготовки **2022**

Форма обучения **очная**

Общая трудоемкость **5 з.е.**

Виды контроля по семестрам:
экзамен 5

Семестр(Курс.Номер семестра на курсе)	**5(3.1)**		Итого	
	УП	РПД	УП	РПД
Лекции	24	24	24	24
Практические	34	34	34	34
Лабораторные	10	10	10	10
Итого ауд.	68	68	68	68
КСР	4	4	4	4
Контактная работа	72	72	72	72
Сам. работа	72	72	72	72
Часы на контроль	36	36	36	36
Практическая подготовка	0	0	0	0
Семинары	0	0	0	0
Консультации	0	0	0	0
Итого трудоемкость в часах	180	180	180	180

Программу составил(и):

к.ф.-м.н., доцент, Реброва Ирина Юрьевна

Рабочая программа дисциплины

Теория чисел и элементы криптографии

разработана в соответствии с ФГОС:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 02.03.01 Математика и компьютерные науки (приказ Минобрнауки России от 23.08.2017 г. № 807)

составлена на основании учебного плана:

Направление 02.03.01 Математика и компьютерные науки
направленность (профиль) Математические основы компьютерных наук
утвержденного Учёным советом вуза от 28.02.2022 протокол № 3.

РПД утверждена Учёным советом университета
протокол от 28.2.2022 г. № 3

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
1.	Дифференциальные и разностные уравнения
2.	Методы и технологии программирования
3.	технологическая (проектно-технологическая) практика
4.	Функциональный анализ
5.	Математический анализ
6.	Педагогика и психология
7.	Программирование
8.	Теория вероятностей и математическая статистика
9.	Архитектура вычислительных систем
10.	Дискретная математика и ее приложения в компьютерных науках
11.	Математическая логика и ее приложение в компьютерных науках
12.	Аналитическая геометрия
13.	Линейная алгебра
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
1.	Комплексный анализ
2.	Компьютерная геометрия и геометрическое моделирование
3.	Криптография и кодирование
4.	практика по получению профессиональных умений и опыта профессиональной деятельности (в том числе педагогическая практика)
5.	Теоретическая механика
6.	Теория и методика обучения математике
7.	Вариационное исчисление и методы оптимизации
8.	Математическое моделирование
9.	Моделирование бизнес-процессов
10.	научно-исследовательская работа
11.	Научные основы курса элементарной алгебры
12.	Параллельное программирование
13.	преддипломная практика

3. СООТНЕСЕНИЕ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ) С ИНДИКАТОРАМИ ДОСТИЖЕНИЯ КОМПЕТЕНЦИЙ

3.1 Компетенции обучающегося и индикаторы их достижения:

ОПК-1: Способен консультировать и использовать фундаментальные знания в области математического анализа, комплексного и функционального анализа алгебры, аналитической геометрии, дифференциальной геометрии и топологии, дифференциальных уравнений, дискретной математики и математической логики, теории вероятностей, математической статистики и случайных процессов, численных методов, теоретической механики в профессиональной деятельности	
ОПК-1.2	Умеет использовать базовые знания в области математических и естественных наук в профессиональной деятельности
	умеет использовать базовые знания теории чисел для оценки сложности арифметических операций; с помощью учебной и методической литературы решать задачи шифрования и дешифрования сообщений
ОПК-1.4	Имеет навыки выбора методов решения задач профессиональной деятельности на основе теоретических знаний в области математических и естественных наук
	владеет навыками научной аргументации выбора методов кодирования информации владеет навыками использования арифметических методов кодирования информации
ОПК-4: Способен находить, анализировать, реализовывать программно и использовать на практике математические алгоритмы, в том числе с применением современных вычислительных систем	
ОПК-4.1	Знает основные понятия, гипотезы, теоремы, методы, математические и алгоритмические модели, составляющие содержание фундаментальной и прикладной математики и связанные с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

	знает основные факты и положения теории делимости и теории сравнений; арифметические алгоритмы, связанные с криптографическими системами; основные этапы истории кодирования информации.

3.2 Результаты обучения по дисциплине:
В результате освоения дисциплины обучающийся должен:

	Знать:
З.1	основные факты и положения теории делимости и теории сравнений;
З.2	арифметические алгоритмы, связанные с криптографическими системами;
З.3	основные этапы истории кодирования информации.
	Уметь:
У.1	использовать базовые знания теории чисел для оценки сложности арифметических операций;
У.2	с помощью учебной и методической литературы решать задачи шифрования и дешифрования сообщений
	Владеть:
В.1	владеет навыками научной аргументации выбора методов кодирования информации
В.2	владеет навыками использования арифметических методов кодирования информации

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература	Содержание
	Теория делимости				
1.1	Теория делимости /Лек/	5	2	Л1.1 Л1.2 Л1.3	Делимость и простые числа. Основная теорема арифметики. НОД и НОК. Теорема Чебышева о распределении простых чисел
1.2	Теория делимости /Пр/	5	4	Л1.1 Л1.2 Л1.3	Делимость и простые числа. Основная теорема арифметики. НОД и НОК. Теорема Чебышева о распределении простых чисел
1.3	/Ср/	5	6	Л1.1 Л1.2 Л1.3	
	Цепные дроби				
2.1	Цепные дроби /Лек/	5	2	Л1.1 Л1.2 Л1.3	Непрерывные дроби и их свойства. Представление рациональных чисел конечной чепной дробью. Квадратичные иррациональности и цепные дроби.
2.2	Цепные дроби /Пр/	5	4	Л1.1 Л1.2 Л1.3	Непрерывные дроби и их свойства. Представление рациональных чисел конечной чепной дробью. Квадратичные иррациональности и цепные дроби.
2.3	Самостоятельная работа /Ср/	5	6	Л1.1 Л1.2 Л1.3	
	Теория сравнений				
3.1	Числовые сравнения и их свойства. Полная и приведенная системы вычетов. /Лек/	5	2	Л1.1 Л1.2 Л1.3	Числовые сравнения и их свойства. Полная и приведенная системы вычетов.
3.2	Числовые сравнения и их свойства. Полная и приведенная системы вычетов. /Пр/	5	2	Л1.1 Л1.2 Л1.3	Числовые сравнения и их свойства. Полная и приведенная системы вычетов. Функция Эйлера. Теоремы Эйлера и Ферма.
3.3	Сравнения первой степени. Системы сравнений первой степени. /Лек/	5	2	Л1.1 Л1.2 Л1.3	Сравнения первой степени. Системы сравнений первой степени.
3.4	Сравнения первой степени. Системы сранений первой степени. /Пр/	5	2	Л1.1 Л1.2 Л1.3	Сравнения первой степени. Системы сравнений первой степени.
3.5	Сравнения высших степеней /Лек/	5	2	Л1.1 Л1.2 Л1.3	Сравнения n-ной степени по простому модулю. Сравнения n-ной степени по составному модулю.

3.6	Сравнения высших степеней /Пр/	5	2	Л1.1 Л1.2 Л1.3	Сравнения n-ной степени по простому модулю. Сравнения n-ной степени по составному модулю.
3.7	Сравнения второй степени. Квадратичные вычеты и невычеты. /Лек/	5	2	Л1.1 Л1.2 Л1.3	Сравнения второй степени. Квадратичные вычеты и невычеты. Первообразные корни и индексы
3.8	Сравнения второй степени. Квадратичные вычеты и невычеты. Первообразные корни и индексы /Пр/	5	2	Л1.1 Л1.2 Л1.3	Сравнения второй степени. Квадратичные вычеты и невычеты. Первообразные корни и индексы
3.9	Самостоятельная работа /Ср/	5	20	Л1.1 Л1.2 Л1.3	
	Оценка сложности арифметических операций				
4.1	Свойства функций оценки сложности. Сложность арифметических операций с целыми числами /Лек/	5	4	Л1.1 Л1.2 Л1.3	Свойства функций оценки сложности. Сложность арифметических операций с целыми числами
4.2	Свойства функций оценки сложности. Сложность арифметических операций с целыми числами /Пр/	5	6	Л1.1 Л1.2 Л1.3	Свойства функций оценки сложности. Сложность арифметических операций с целыми числами
4.3	Самостоятельная работа /Ср/	5	10	Л1.1 Л1.2 Л1.3	
	Арифметические алгоритмы				
5.1	Арифметические алгоритмы /Лек/	5	6	Л1.1 Л1.2 Л1.3	Проверка простоты. Решето Эратосфена. Критерий Вильсона. Тест на основе малой теоремы Ферма. Построение больших простых чисел. Алгоритмы факторизации целых чисел
5.2	Арифметические алгоритмы /Пр/	5	8	Л1.1 Л1.2 Л1.3	Проверка простоты. Решето Эратосфена. Критерий Вильсона. Тест на основе малой теоремы Ферма. Построение больших простых чисел. Алгоритмы факторизации целых чисел.
5.3	Проверка простоты. /Лаб/	5	2	Л1.1 Л1.2 Л1.3	Тест на основе малой теоремы Ферма
5.4	Алгоритмы факторизации целых чисел /Лаб/	5	4	Л1.1 Л1.2 Л1.3	Алгоритмы факторизации целых чисел
5.5	Самостоятельная работа /Ср/	5	20	Л1.1 Л1.2 Л1.3	
	Криптографическая система RSA				
6.1	Криптографическая система RSA /Лек/	5	2	Л1.1 Л1.2 Л1.3	Выбор параметров системы RSA. Взаимосвязь между параметрами системы RSA
6.2	Криптографическая система RSA /Пр/	5	4	Л1.1 Л1.2 Л1.3	Выбор параметров системы RSA. Взаимосвязь между параметрами системы RSA
6.3	Криптоалгоритмы с открытыми ключами. Генерация простого большого числа. /Лаб/	5	4	Л1.1 Л1.2 Л1.3	Криптоалгоритмы с открытыми ключами. Генерация простого большого числа.
6.4	Самостоятельная работа /Ср/	5	10	Л1.1 Л1.2 Л1.3	
	Контрольная работа				
7.1	Контрольная работа /КСР/	5	4	Л1.1 Л1.2 Л1.3	

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

5.1. Типовые задания для проведения текущего контроля

Задания для практических занятий:

1. Разложить на простые множители.
2. Разложить в цепную дробь.
3. Решить в целых числах уравнения
4. Свернуть цепную дробь: [2; 1, 3, 2].
5. Вычислить функцию Эйлера □(124).
6. Решить сравнения первой степени
7. Решить в натуральных числах систему уравнений
8. Найти произведение наименьших натуральных решений сравнения
9. Решить систему сравнений первой степени
10. Установить, имеет ли решения сравнение.
11. Решить сравнение, предварительно приведя его к двучленному
12. Решить в целых числах уравнение
13. Найти сумму наименьших натуральных частных решений сравнения
14. Решить сравнения с помощью таблицы индексов

Вариант контрольной работы по разделам
«Теория делимости и числовые сравнения»

1. Вычислите функцию Эйлера
2. Сколько натуральных чисел в промежутке от 1 до 80, не взаимно простых с 25?
3. Решите уравнения.
4. Проверьте теорему Эйлера при заданных значениях.
5. Найдите остатки от деления числа
6. Методом подбора найдите решение сравнений
7. Решите сравнение методом преобразования коэффициентов.
8. Решите сравнение, используя теорему Эйлера.
9. Разложите простую дробь в правильную цепную дробь и найти ее подходящие дроби.

5.2. Типовые задания для проведения промежуточной аттестации

Вопросы к экзамену

1. Делимость и простые числа. Основная теорема арифметики. НОД и НОК.
2. Теорема Чебышева о распределении простых чисел.
3. Непрерывные дроби и их свойства.
4. Представление рациональных чисел цепными дробями.
5. Числовые сравнения и их свойства. Полная и приведенная системы вычетов.
6. Функция Эйлера. Теоремы Эйлера и Ферма.
7. Сравнения первой степени. Системы сравнений первой степени.
8. Сравнения n-ной степени по простому модулю.
9. Сравнения n-ной степени по составному модулю.
10. Сравнения второй степени. Квадратичные вычеты и невычеты.
11. Первообразные корни и индексы.
12. Свойства функций оценки сложности.
13. Сложность арифметических операций с целыми числами.
14. Сложность алгоритма Евклида.
15. Сложность операций в кольце вычетов.
16. Проверка простоты. Решето Эратосфена. Критерий Вильсона. Тест на основе малой теоремы Ферма.
17. Построение больших простых чисел.
18. Алгоритмы факторизации целых чисел.
19. Выбор параметров системы RSA. Взаимосвязь между параметрами системы RSA.

5.3. Перечень видов оценочных средств

Задания для практических занятий
Контрольная работа
Экзамен

5.4. Процедура применения оценочных материалов

Составляющие итоговой оценки за дисциплину:
1) Текущий контроль (общий вес 60 баллов):
до 15 баллов – посещение занятий;
до 30 баллов – выполнение заданий в ходе практических занятий и заданий для самостоятельной работы

до 15 баллов – выполнение заданий в ходе лабораторных работ
2) Итоговый контроль заключается в проведении экзамена (общий вес - 40 баллов). Экзамен проводится по вопросам билетов с обязательным решением задач. Как правило, студент получает два вопроса из приведенного выше списка и две задачи, готовится в присутствии преподавателя и дает подробные комментарии. Студент, пропускавший занятия в ходе семестра, получает дополнительные вопросы и задачи по каждой пропущенной им теме (на усмотрение преподавателя).

Шкала перевода баллов в оценку:
«отлично»: 81-100
«хорошо»: 61 - 80
«удовлетворительно» 41 - 60
«неудовлетворительно» 0 - 40

Промежуточная аттестация может проводиться с применением электронного обучения и (или) дистанционных образовательных технологий в соответствии с «Порядком проведения промежуточной аттестации с применением электронного обучения и /или дистанционных образовательных технологий».
Проведение экзамена с применением дистанционных образовательных технологий может проходить по следующим процедурам:
в форме устного собеседования преподавателя со студентом по предложенным вопросам к экзамену (без предварительной подготовки к конкретному вопросу в период проведения экзамена),
в виде решения обучающимся уникального кейс-задания,
в виде защиты индивидуального учебного проекта;
в виде решения обучающимися экзаменационных тестовых заданий (с ограничением по времени выполнения);
в виде электронного портфолио обучающегося.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год (кол-во экземпляров для печатных изданий)	Ссылка на электронное издание
Л1.1	Виноградов И. М., Рывкин А. Э.	Основы теории чисел	м- л.: Государственное издательство технико-теоретической литературы, 1952	http://biblioclub.ru/index.php?page=book&id=449924
Л1.2	Васильева И. Н.	Криптографические методы защиты информации: Учебник и практикум	М.: Издательство Юрайт, 2019	https://www.biblio-online.ru/book/kriptograficheskie-metody-zaschity-informacii-433610
Л1.3	А.Е. Устян	Алгебра и теория чисел: В 2 частях	ТГПУ им. Л. Н. Толстого, 2002 (71 шт.)	

6.3.Информационные технологии

6.3.1 Перечень лицензионного и свободно распространяемого программного обеспечения

1.	Операционная система Microsoft Windows XP Professional Russian. Лицензия № 16698685 от 08.08.2003 г.
2.	Операционная система Microsoft Windows Professional 7 Russian. Лицензия №48497058 от 13.05.2011 г., договор № Пр/16/6 от 05 апреля 2016 г.
3.	Операционная система Microsoft Windows 10 Professional Russian. Контракт № ПР/ФЕН/15/18 от 23.10.2015 г., договор № Пр/16/6 от 05 апреля 2016 г.
4.	Программное обеспечение Microsoft Office Enterprise 2007 Russian. Лицензия №46138962 от 16.11.2009
5.	Программное обеспечение Microsoft Office 2013 Professional. Контракт № 405535 от 2 ноября 2015 года, контракт № ПР/ФЕН/15/18 от 23.10.2015 г.
6.	Программа для распознавания текста ABBYY FineReader 9.0 Corporate Edition. Лицензионный сертификат - код позиции AF90-3U1V25-102, ABBYY FineReader 9.0 Corporate Edition Volume License Concurrent от 28 июля 2009 г.
7.	Электронный словарь ABBYY Lingvo X3 Европейская версия - Код позиции AL14-2U1V05-102, ABBYY Lingvo x3 Европейская версия. Именная лицензия Concurrent от 28 июля 2009 г.
8.	Комплексная система антивирусной защиты Kaspersky Endpoint Security для бизнеса – стандартный Russian Edition. 500-999 Node 2 year Educational Renewal License. Лицензия № 13C8-190514-084943-783-1256 от 15.05.2019
9.	Браузеры Google Chrome, Mozilla, Opera. Свободно распространяемое ПО
10.	Программа просмотра файлов формата RPD Adobe Acrobat Reader DC. Свободно распространяемое ПО
11.	Система облачного хранилища Dropbox. Свободно распространяемое ПО

6.3.2 Перечень информационных справочных систем и профессиональных баз данных

1.	Компьютерная информационно-правовая система «Гарант»
2.	Официальный интернет-портал базы данных правовой информации (http://pravo.gov.ru)
3.	Полнотекстовый архив ведущих западных научных журналов на российской платформе Национального электронно-информационного консорциума (НЭИКОН)(http://neicon.ru)

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Ауд.	Назначение	Оборудование и технические средства обучения	Вид
4-304	Лекционная с мультимедийным комплексом	доска учебная, проектор, стол преподавателя, столы учебные, стул преподавателя, экран	Лек
4-305	Компьютерный класс	аудиоколонки для проектора и интерактивной доски, аудиоколонки учебные, интерактивная доска, компьютеры, кондиционер, маркерная доска, проектор, столы компьютерные, столы учебные	Пр
4-306	Компьютерный класс	аудиоколонки для проектора и интерактивной доски, интерактивная доска, компьютеры, кондиционер, маркерная доска, проектор, столы компьютерные, столы учебные	Лаб
4-303	Помещение для самостоятельной работы	аудиоколонки, кондиционер, маркерная доска, столы компьютерные, столы учебные, компьютерная техника с возможностью подключения сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду университета	Ср

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина «Теория чисел и элементы криптографии» направлена на формирование систематизированных теоретических знаний в области теории чисел и некоторых ее приложений к криптографии. Самостоятельная работа студентов по дисциплине составляет 50% от всего объема часов, отводимого учебным планом на изучение дисциплины. В связи с этим успешное изучение материала данного курса в значительной степени зависит от качества самостоятельной подготовки студентов. С целью активизации самостоятельной работы студентов на каждом практическом занятии повторяется соответствующий теоретический материал и закрепляются основные навыки и умения владением математическим аппаратом.

В начале изучения курса студенты получают темы и вопросы практических занятий. По второму разделу предусмотрено выполнение четырех лабораторных работ.