

МИНОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ  
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ

Директор института прикладной  
математики и компьютерных наук

А.В. Замятин

« 02 »

2021 г.

## Теория чисел

### рабочая программа дисциплины

Закреплена за кафедрой	<i>компьютерной безопасности</i>
Учебный план	<i>10.05.01 Компьютерная безопасность, «Анализ безопасности компьютерных систем»</i>
Форма обучения	<i>Очная</i>
Общая трудоёмкость	<i>4 з.е.</i>
Часов по учебному плану	<i>144</i>
в том числе:	
аудиторная контактная работа	<i>71,5</i>
самостоятельная работа	<i>72,5</i>
Вид(ы) контроля в семестрах	
экзамен/зачет/зачет с оценкой	<i>Семестр 3 – экзамен</i>

Программу составил:  
канд. физ.-мат. наук, доцент  
кафедры компьютерной безопасности

М.А. Приходовский

Рецензент:  
канд. тех. наук, доцент  
заведующий кафедрой компьютерной безопасности

С.А. Останин

Рабочая программа дисциплины «Теория чисел» разработана в соответствии с образовательным стандартом высшего образования – специалитет, самостоятельно устанавливаемым федеральным государственным автономным образовательным учреждением высшего образования «Национальный исследовательский Томский государственный университет» по специальности 10.05.01 Компьютерная безопасность (Утвержден Ученым советом НИ ТГУ, протокол от 30.06.2021 г. № 06).

Рабочая программа одобрена на заседании кафедры компьютерной безопасности

Протокол от 02 июня 2021 г. № 06

Заведующий кафедрой компьютерной безопасности,  
канд. техн. наук, доцент

С.А. Останин

Рабочая программа одобрена на заседании учебно-методической комиссии института прикладной математики и компьютерных наук (УМК ИПМКН)

Протокол от 17 июня 2021 г. № 05

Председатель УМК ИПМКН,  
д-р техн. наук, профессор

С.П. Сущенко

### Цель освоения дисциплины

**Цель** – овладение студентами математическим аппаратом теории чисел, фундаментальными теоретическими и прикладными положениями этой науки.

### 1. Место дисциплины в структуре ОПОП

Дисциплина «Теория чисел» относится к обязательной части Блока 1 «Дисциплины», входит в модуль «Математика».

Для освоения дисциплины необходимо знать основы математического анализа, теории множеств и дискретной математики.

Пререквизиты дисциплины: «Математический анализ», «Дискретная математика», «Общая алгебра»

Постреквизиты дисциплины: «Математическая логика и теория алгоритмов», «Теория кодирования».

### 2. Компетенции и результаты обучения, формируемые в результате освоения дисциплины

Таблица 1.

Компетенция	Индикатор компетенции	Код и наименование результатов обучения (планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций)
ОПК-3. Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности	ИОПК-3.1 Демонстрирует навыки выполнения стандартных действий, решения типовых задач, формулируемых в рамках базовых математических дисциплин;	ОР-3.1.1 Имеет навыки работы с профессиональной литературой по теории чисел для успешной учебной деятельности.
	ИОПК-3.2 Осуществляет применение основных понятий, фактов, концепций, принципов математики и информатики для решения задач профессиональной деятельности;	ОР-3.2.1 Умеет решать задачи вычислительного и теоретического характера в области теории чисел, устанавливать взаимосвязи между вводимыми понятиями, доказывать, как известные утверждения, так и родственные им новые. ОР-3.2.2 Владеет разнообразными методами теории чисел, подбирая и сочетая их при анализе конкретных теоретических и прикладных задач. - выполнять операции в кольце вычетов; - анализировать функции целого переменного; - применять алгоритм Евклида и расширенный алгоритм Евклида, алгоритм нахождения НОДа, алгоритмы (бинарный и на основе теоремы Ферма) проверки простоты; - вычислять значения основных арифметических функций.
	ИОПК-3.3 Выявляет научную сущность проблем, возникающих в ходе профессиональной деятельности, и применяет соответствующий математический аппарат для их формализации, анализа и выработки решения.	ОР-3.3.1 Владеет знанием основных определений и основных свойств теории чисел, а также формулировки наиболее важных утверждений, некоторых стандартных методов их доказательств.

### 3. Структура и содержание дисциплины

#### 3.1. Структура и трудоемкость видов учебной работы по дисциплине

Общая трудоемкость дисциплины составляет 4 зачетные единицы, 144 часа.

Таблица 2.

Вид учебной работы	Трудоемкость в академических часах	
	3 семестр	всего
<b>Общая трудоемкость</b>	144	144
<b>Контактная работа:</b>	71,5	71,5
Лекции (Л):	32	32
Практики (ПЗ)	32	32
Лабораторные работы (ЛР)		
Семинары (СЗ)		
Групповые консультации	2	2
Индивидуальные консультации	3,2	3,2
Промежуточная аттестация	2,3	2,3
<b>Самостоятельная работа обучающегося:</b>	40,8	40,8
- изучение учебного материала, публикаций по теме дисциплины	20	20
- подготовка к практическим занятиям	12	12
- подготовка к текущему контролю	6	6
- другие формы самостоятельной работы (индивидуализация образовательной траектории)	2,8	2,8
<b>Подготовка к экзамену</b>	31,7	31,7
<b>Вид промежуточной аттестации (зачет, зачет с оценкой, экзамен)</b>	<b>Экзамен</b>	<b>Экзамен</b>

### 3.2. Содержание и трудоемкость разделов дисциплины

Таблица 3.

Код занятия	Наименование разделов и тем и их содержание	Вид учебной работы, занятий, контроля	С е м е с т р	Часы в электронной форме	Всего (час.)	Литература	Код (ы) результата(ов) обучения
	<b>Раздел 1. Теория чисел</b>		<b>7</b>		<b>64</b>	<b>1,2,3,4,5,6,7,8,9</b>	ОР-1.4.1, ОР-1.4.2, ОР-2.4.1
1.1.	<i>Делимость и простые числа. Теорема о делении с остатком. НОД чисел. Алгоритм Евклида. Простые числа. Основная теорема арифметики.</i>	Лекции Практики	7		8	<b>1,2,3,4,5,6,7,8,9</b>	
1.2.	<i>Арифметические функции. Мультипликативные функции и их примеры.</i>	Лекции Практики	7		10	<b>1,2,3,4,5,6,7,8,9</b>	
1.3	<i>Цепные дроби.</i>	Лекции Практики	7		8	<b>1,2,3,4,5,6,7,8,9</b>	ОР-1.4.3, ОР-1.4.4, ОР-2.4.1, ОР-2.4.2, ОР-2.4.3
1.4.	<i>Сравнения 1-й степени</i>	Лекции Практики	7		8	<b>1,2,3,4,5,6,7,8,9</b>	
1.5.	<i>Сравнения n-степени.</i>	Лекции Практики	7		10	<b>1,2,3,4,5,6,7,8,9</b>	
1.6.	<i>Сравнения 2-степени</i>	Лекции Практики	7		8	<b>1,2,3,4,5,6,7,8,9</b>	
1.7.	<i>Первообразные корни и индексы.</i>	Лекции Практики	7		12	<b>1,2,3,4,5,6,7,8,9</b>	
	<b>Подготовка к промежуточной аттестации в форме экзамена</b>	СРС	<b>3</b>		<b>31,7</b>	<b>1, 2, 3, 4, 5, 6, 7, 8</b>	
	<b>Прохождение промежуточной аттестации в форме экзамена</b>	Э	<b>3</b>		<b>4,3</b>		

#### 4. Образовательные технологии, учебно-методическое и информационное обеспечение для освоения дисциплины

В ходе реализации дисциплины используются классические образовательные технологии – лекции, практические занятия, самостоятельное изучение материалов студентами, проверка знаний путем проведения контрольных работ и экзамена.

Для проведения текущего контроля СРС преподаватель может проводить небольшие тесты в начале каждого занятия.

Вопросы экзамена позволяют оценить уровень сформированности компетенций и понимания сформированности физической картины в рамках данных разделов.

Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения, характеризующих этапы формирования компетенций, и методические материалы, определяющие процедуры оценивания результатов обучения, приведены в Приложении 1 к рабочей программе «Фонд оценочных средств».

Типовые контрольные задания или иные материалы, необходимые для текущей аттестации, и методические материалы, определяющие процедуры оценивания результатов текущей аттестации, приведены в Приложении 2 к рабочей программе «Примерные оценочные средства текущей аттестации».

##### 4.1. Рекомендуемая литература и учебно-методическое обеспечение

№ п/п	Авторы / составители	Заглавие	Издательство	Год издания, количество страниц
Основная литература				
1.	Кузьмина А. С., Мальцев Ю. Н.	Теория чисел	Барнаул	2011 г., 240 с.
2.	Бухштаб А. А.	Теория чисел	СПб.: Лань	2015 г., 384 с.
3.	Виноградов И.М.	Основы теории чисел	СПб.: Лань	2006 г., 176 с.
Дополнительная литература				
4.	Деза Е. И., Котова Л. В.	Сборник задач по теории чисел.	М.: Либроком/URSS	2012 г., 224 с.
5.	Манин Ю. И., Панчишкин А.А.	Введение в современную теорию чисел.	М.: МЦНМО	2013 г., 552 с.
6.	Сушкевич А.К.	Теория чисел.	М.: Вузовская книга	2016 г., 240 с.
7.	Арнольд И.В.	Теория чисел.	М.: Ленанд	2019 г., 288 с.
8.	Боревич З.И., Шафаревич И.Р.	Теория чисел.	М.: Ленанд	2019 г., 504 с.
9.	Куликов Л. Я., Москаленко А. И., Фомин А. А.	Сборник задач по алгебре и теории чисел.	М.: Просвещение	1993 г., 288 с.

##### 4.2. Базы данных и информационно-справочные системы, в том числе зарубежные

- 1) <http://alexhvorost.narod2.ru/>
  - 2) <https://www.youtube.com/playlist?list=PL2ar10WmyGU5A6qkfwbujIMJYXR6S5PiP>
  - 3) [https://ru.wikipedia.org/wiki/Теория\\_чисел](https://ru.wikipedia.org/wiki/Теория_чисел)
- Курс в MOODLE ТГУ: <https://moodle.tsu.ru/course/view.php?id=12937>

### **4.3. Перечень лицензионного и программного обеспечения**

ОС Windows, пакет Microsoft Office

### **4.4. Оборудование и технические средства обучения**

Для проведения лекционных занятий используются классические аудитории с доской и, возможно, проектором и компьютером.

### **5. Методические указания обучающимся по освоению дисциплины**

Для выработки необходимых компетенций рекомендуется индивидуальные задания для студентов, такие как решение задач по теме дисциплины, подготовка докладов. Самостоятельная работа направлена на выработку навыка самостоятельного поиска информации, закрепление лекционного материала, развитие необходимых практических навыков, установление связей с различными разделами дисциплины. Для выработки необходимых компетенций и осуществления обратной связи рекомендуется обсуждение проблем, возникающих при выполнении индивидуальных заданий, выступления и научные дискуссии студентов по отдельным проблемам. Формой промежуточного контроля являются принятие индивидуальных заданий и докладов. Итоговый контроль проводится в форме экзамена.

### **6. Преподавательский состав, реализующий дисциплину**

Приходовский Михаил Анатольевич, к.ф.-м.н., доцент кафедры компьютерной безопасности.

### **7. Язык преподавания – русский язык.**