

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ЮЖНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

В. С. Пилиди

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

Рекомендовано экспертным советом по направлению
«Математика, механика, информатизация» ЮФУ
в качестве учебного пособия
для студентов, обучающихся по направлениям подготовки
«Фундаментальная информатика и информационные технологии»
и «Прикладная математика и информатика»

Ростов-на-Дону – Таганрог
Издательство Южного федерального университета
2019

УДК 511+512.5
ББК 22.13+22.144
ПЗ2

Печатается по решению экспертного совета «Математика, механика, информатизация» Южного федерального университета (протокол № 1 от 25 ноября 2019 г.)

Рецензенты:

кандидат технических наук, доцент, заведующий кафедрой
«Программное обеспечение вычислительной техники
и автоматизированных систем» ФГБОУ ВО ДГТУ

В. В. Долгов;

кандидат физико-математических наук,
доцент кафедры алгебры и дискретной математики
института математики, механики и компьютерных наук
Южного федерального университета

С. С. Михалкович

Пилиди, В. С.

ПЗ2 Математические основы защиты информации : учебное пособие / В. С. Пилиди ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2019. – 308 с.

ISBN 978-5-9275-3363-3

Настоящая книга представляет собой учебник по математическим основам защиты информации. Она посвящена изложению основ теории чисел и общей алгебры, в ней среди прочего рассматриваются такие вопросы как делимость чисел и мультипликативные функции, теория групп, элементы теории колец и полей, символы Лежандра и Якоби, тестирование чисел на простоту и дискретное логарифмирование. Во второе издание книги добавлены главы, посвященные введению в криптографию и теорию информации. Приведены решения всех имеющихся в тексте задач.

Пособие может быть использовано студентами, обучающимися по программам бакалавриата направлений подготовки «Фундаментальная информатика и информационные технологии» и «Прикладная математика и информатика».

Публикуется в авторской редакции.

УДК 511+512.5
ББК 22.13+22.144

ISBN 978-5-9275-3363-3

© Южный федеральный университет, 2019
© Пилиди В. С., 2019

Оглавление

Введение	3
1 Введение в теорию чисел	4
1.1 Предварительные сведения	4
1.2 Деление с остатком	5
1.3 Отношение делимости	8
1.4 Наибольший общий делитель	9
1.5 Алгоритм Евклида	13
1.6 Взаимно простые числа	17
1.7 Наименьшее общее кратное	20
1.8 Простые числа	22
1.9 Мультипликативные функции	27
1.10 Сравнения	37
1.11 Сравнения первой степени	41
1.12 Дополнения	44
2 Группы	48
2.1 Бинарная операция. Моноиды	48
2.2 Определение группы	53
2.3 Порядок элемента	61
2.4 Подгруппы	65
2.5 Циклические группы	68
2.6 Гомоморфизм и изоморфизм	72
2.7 Смежные классы	80
2.8 Нормальные подгруппы	90
2.9 Прямое произведение групп	95
2.10 Экспонента группы	95
3 Кольца и поля	99
3.1 Определение кольца	99
3.2 Кольцо многочленов	108

3.3	Идеалы	130
3.4	Характеристика поля, подполе	139
3.5	Конечные расширения	148
3.6	Дополнение 1. Поле частных	160
3.7	Дополнение 2. Отношение делимости в кольце	163
3.8	Дополнение 3. Евклидовы кольца	165
3.9	Дополнение 4. Формальные степенные ряды	167
3.10	Дополнение 5. Подполя конечных полей	171
4	Теория чисел. Продолжение	173
4.1	Дискретное логарифмирование	173
4.2	Двучленные сравнения	176
4.3	Символ Лежандра	178
4.4	Символ Якоби	186
4.5	Цикличность групп \mathbb{Z}_n^*	190
4.6	Структура группы $\mathbb{Z}_{2^n}^*$	196
4.7	Сравнения по составному модулю	199
4.8	Тестирование чисел на простоту	206
5	Криптосистемы	214
5.1	Основные определения	214
5.2	Примеры криптосистем	215
5.3	Криптоанализ	220
5.4	Стойкость криптосистем	238
6	Теория информации	244
6.1	Определение энтропии	244
6.2	Кодирование для канала без шума	254
6.3	Однозначно декодируемые коды	255
6.4	Ложные ключи и расстояние единственности	265
7	Решения задач	273
7.1	Задачи главы 1	273
7.2	Задачи главы 2	279
7.3	Задачи главы 3	287
7.4	Задачи главы 4	299