

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ В КРИПТОГРАФИИ

ПРАКТИКУМ

Специальность
10.05.01 Компьютерная безопасность

Ставрополь
2017

УДК 004.056.55 (075.8)
ББК 32.973-018 я73
Т 33

Печатается по решению
редакционно-издательского совета
Северо-Кавказского федерального
университета

Рецензенты:

канд. техн. наук, доцент *В. А. Гимбицкий*,
канд. техн. наук, доцент *А. В. Росенко*

Т 33 Теоретико-числовые методы в криптографии: учебное пособие / авт.-сост.: Ф. Б. Тебуева, В. О. Антонов. – Ставрополь: Изд-во СКФУ, 2017. – 107 с.

Практикум составлен в соответствии с требованиями ФГОС ВО, призван способствовать формированию и закреплению общепрофессиональных компетенций, и освоению базовых принципов построения и математического обоснования криптографических систем. Содержит теоретический материал, образцы решения задач, задания, литературу.

Предназначен для студентов, обучающихся по специальности 10.05.01 Компьютерная безопасность.

УДК 004.056.55 (075.8)
ББК 32.973-018 я73

Авторы-составители:

д-р физ.-мат. наук, профессор *Ф. Б. Тебуева*,
аспирант *В. О. Антонов*

© ФГАОУ ВО «Северо-Кавказский
федеральный университет», 2017

СОДЕРЖАНИЕ

Предисловие	4
1. Нахождение наибольшего общего делителя	5
2. Арифметические операции над целыми числами	21
3. Решение сравнений второй степени	36
4. Умножение методом Карацубы – Офмана	44
5. Алгоритм быстрого преобразования Фурье	50
6. Алгоритм Шенхаге – Штрассена для умножения целых чисел	64
7. Вероятностные алгоритмы проверки чисел на простоту ..	72
8. Детерминированные алгоритмы проверки чисел на простоту	81
9. Разложение чисел на множители	90

ПРЕДИСЛОВИЕ

Целью проведения практических занятий по дисциплине «Теоретико-числовые методы в криптографии» изложение базовых принципов построения и математического обоснования криптографических систем является формирование и закрепление общепрофессиональных компетенций будущего специалиста специальности 10.05.01 Компьютерная безопасность.

Задачи изучения дисциплины:

- получение навыков применения теоретико-числовых методов в криптографии;
- освоение основных алгебраических, аналитических и вероятностных методов анализа криптосистем;
- формирование навыков разработки эффективных алгоритмов для решения прикладных задач;
- воспитание коммуникационной готовности к применению в работе математических средств защиты информации;
- формирование общепрофессиональных компетенций, таких как ОПК-2 – способность при решении профессиональных задач корректно применять аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов.