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

ŋqdqɐɐʎ bɇ dɘdɇbʎɜɘ d ɕɔɑbɔɐ Ɉqdqʎqɐè

УДК 511+512.5
ББК 22.13+22.144
П32

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

Р е ц е н з е н т ы :
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.
П32 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

Оглавление