А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

УЧЕБНИК ДЛЯ АКАДЕМИЧЕСКОГО БАКАЛАВРИАТА

2-е издание, исправленное

Рекомендовано Учебно-методическим отделом высшего образования в качестве учебника для студентов высших учебных заведений, обучающихся по инженерно-техническим направлениям и специальностям

Книга доступна в электронной библиотеке biblio-online.ru, а также в мобильном приложении «Юрайт.Библиотека»

Москва ▪ Юрайт ▪ 2019

УДК 004.056(075.8)
ББК 32.811.4я73
Л79

Авторы:

Лось Алексей Борисович — кандидат технических наук, доцент, заведующий кафедрой компьютерной безопасности Департамента прикладной математики Московского института электроники и математики Национального исследовательского университета «Высшая школа экономики»;

Нестеренко Алексей Юрьевич — кандидат физико-математических наук, доцент кафедры компьютерной безопасности Департамента прикладной математики Московского института электроники и математики Национального исследовательского университета «Высшая школа экономики»;

Рожков Михаил Иванович — доктор технических наук, старший научный сотрудник, профессор кафедры компьютерной безопасности Департамента прикладной математики Московского института электроники и математики Национального исследовательского университета «Высшая школа экономики».

Рецензенты:

Хаметов В. М. — доктор юридических наук, профессор, почетный работник высшего профессионального образования РФ, заведующий кафедрой уголовно-процессуального права Московского государственного юридического университета имени О. Е. Кутафина (МГЮА);

Попов. В. Л. — доктор физико-математических наук, професор Математичекого института имени В. А. Стеклова.

Лось, А. Б.

Л79 Криптографические методы защиты информации : учебник для академического бакалавриата / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — М. : Издательство Юрайт, 2019. — 473 с. — (Серия : Бакалавр. Академический курс).

ISBN 978-5-534-10673-2

В учебнике «Криптографические методы защиты информации» изложен курс алгоритмической теории чисел и ее приложений к вопросам защиты информации. Основное внимание уделено строгому математическому обоснованию, эффективной реализации и анализу трудоемкости алгоритмов, используемых в криптографических приложениях. Приведено описание современных криптографических схем и протоколов, использующих изложенные теоретические сведения.

В отличие от существующих пособий по данной тематике учебник содержит в себе изложение, построенное по принципу «от простого к сложному», что позволит освоить рассматриваемый материал без существенного использования дополнительной литературы.

Соответствует актуальным требованиям Федерального государственного образовательного стандарта высшего образования.

Для студентов, учащихся по специальности «Компьютерная безопасность», магистрантов, обучающихся по специальности «Математические методы защиты информации», а также аспирантов и научных работников.

УДК 004.056(075.8)
ББК 32.811.4я73

ISBN 978-5-534-10673-2

Оглавление