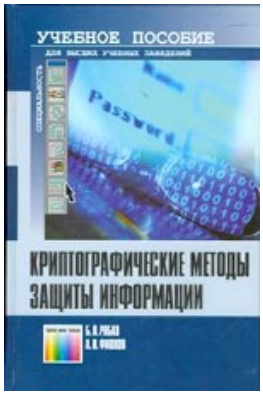
Новые книги



Рябко Б. Я., Фионов А. Н.
Криптографические методы защиты информации : учеб. пособие для вузов по специальностям. – М. : Горячая линия-Телеком, 2005. – 229 с. : ил.

ISBN 5-93517-265-8

Изложены основные подходы и методы современной криптографии для решения задач, возникающих при обработке, хранении и передаче информации. Основное внимание уделено новым направлениям криптографии, связанным с обеспечением конфиденциальности взаимодействий пользователей компьютеров и компьютерных сетей. Рассмотрены основные шифры с открытыми ключами, методы цифровой подписи, основные криптографические протоколы, блоковые и потоковые шифры, криптографические хеш-функции, а также редко встречающиеся в литературе вопросы о конструкции доказуемо невскрываемых криптосистем и криптографии на эллиптических кривых. Изложение теоретического материала ведется достаточно строго, но с использованием элементарного математического аппарата. Подробно описаны алгоритмы, лежащие в основе криптографических отечественных и международных стандартов. Приведены задачи и упражнения, необходимые при проведении практических занятий и лабораторных работ.

Для студентов, обучающихся по направлению «Телекоммуникации», может быть полезна специалистам.