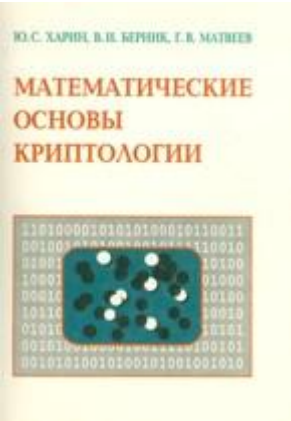
МАТЕМАТИЧЕСКИЕ ОСНОВЫ КРИПТОЛОГИИ

Харин Ю. С. и др. Математические основы криптологии: Учеб. пособие / Ю. С.Харин, В. И. Берник, Г. В. Матвеев. — Мн.: БГУ, 1999. -319 с: ил.

ISBN 985-445-217-4

Данное пособие является первым отечественным учебным пособием по новому актуальному направлению прикладной математики — математические методы защиты информации.



Изложены математические основы криптографической зашиты ин формации в компьютерных сетях и системах связи. Исследованы математические модели симметричных и несимметричных криптосистем, а также методы их анализа. Описаны методы генерации и тестирования случайных и псевдослучайных последовательностей. Представлены математические подходы к решению проблем аутентификации. Изложены протоколы функционирования сетевых криптосистем.

Для студентов (бакалаврского и магистерского уровней), аспирантов, обучающихся по математическим и инженерно-техническим специальностям, слушателей факультетов переподготовки и повышения квалификации, а также для специалистов в области прикладной математики, информатики и электроники, желающих познакомиться с математическими методами защиты информации.

Оглавление