Сергей Панасенко

АЛГОРИТМЫ ШИФРОВАНИЯ

специальный справочник

Санкт-Петербург

«БХВ-Петербург»

2009

УДК 681.3.06
ББК 32.973.26-018.2
П16

Панасенко С. П.

П16 Алгоритмы шифрования. Специальный справочник. — СПб.: БХВ-Петербург, 2009. — 576 с.: ил.

ISBN 978-5-9775-0319-8

Книга посвящена алгоритмам блочного симметричного шифрования. Дана общая классификация криптографических алгоритмов. Рассмотрено более 50 алгоритмов шифрования: история создания и использования, основные характеристики и структура, достоинства и недостатки. Описаны различные виды криптоаналитических атак на алгоритмы шифрования и на их реализации в виде программных или аппаратных шифраторов. Рассказано о конкурсах по выбору стандартов шифрования США и Евросоюза.

Для специалистов в области информационных технологий, преподавателей, студентов и аспирантов

УДК 681.3.06
ББК 32.973.26-018.2

Группа подготовки издания:

Главный редактор	*Екатерина Кондукова*
Зам. главного редактора	*Игорь Шишигин*
Зав. редакцией	*Григорий Добин*
Редактор	*Ирина Иноземцева*
Компьютерная верстка	*Натальи Караваевой*
Корректор	*Наталия Першакова*
Дизайн обложки	*Елены Беляевой*
Зав. производством	*Николай Тверских*

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 24.10.08.
Формат $70 \times 100^{1}/_{16}$. Печать офсетная. Усл. печ. л. 46,44.
Тираж 2000 экз. Заказ №
"БХВ-Петербург", 194354, Санкт-Петербург, ул. Есенина, 5Б.

Отпечатано с готовых диапозитивов
в ГУП "Типография "Наука"
199034, Санкт-Петербург, 9 линия, 12

ISBN 978-5-9775-0319-8

Оглавление