УДК 614.2
ББК 32.973-018
В18

Рецензенты:
Корнюшин П. Н. — д-р физ.-мат. наук, зав. кафедрой информационной безопасности ДВГУ;
Глушков С. В. — канд. техн. наук, профессор, зав. кафедрой АИС МГУ.

Варлатая С. К., Шаханова М. В.

В18 Криптографические методы и средства обеспечения информационной безопасности: учебно-методический комплекс. — Москва : Проспект, 2017. — 152 с.

ISBN 978-5-392-23168-3

Учебно-методический комплекс по дисциплине «Криптографические методы и средства обеспечения информационной безопасности» включает в себя учебное пособие, рабочую учебную программу по дисциплине, методические рекомендации к выполнению лабораторных работ и контрольно-измерительные материалы.

В пособии собраны основные криптографические методы и средства обеспечения информационной безопасности. В работе изложены математические основы криптографической защиты информации в компьютерных сетях и системах связи. Представлен синтез и анализ криптографических алгоритмов, приведены основные принципы построения криптоалгоритмов и практических приложений в области защиты информации. В данном пособии рассмотрены актуальные вопросы защиты информации при создании и использовании распределенных корпоративных информационных систем. Особое внимание уделено однонаправленным функциям и методам их построения, протоколам цифрового шифрования, аутентификации и методам криптоанализа различных шифров.

Учебное пособие предназначено как для академической, так и для профессиональной аудитории и может выступать в качестве основы курса «Криптографические методы и средства обеспечения информационной безопасности» для студентов, также материалы пособия могут быть использованы для современных профессиональных образовательных программ повышения квалификации и переподготовки специалистов по защите информации.

УДК 614.2
ББК 32.973-018

Учебное издание

Варлатая Светлана Климентьевна,
Шаханова Марина Владимировна

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебно-методический комплекс

Оригинал-макет подготовлен компанией ООО «Оригинал-макет»
www.o-maket.ru; тел.: (495) 726-18-84
Санитарно-эпидемиологическое заключение
№ 77.99.60.953.Д.004173.04.09 от 17.04.2009 г.
Подписано в печать 20.12.2016. Формат $60\times90^{1}/_{16}$.
Печать цифровая. Печ. л. 9,5. Тираж 20 экз. Заказ № 15501.

ООО «Проспект»
111020, г. Москва, ул. Боровая, д. 7, стр. 4.

Отпечатано в типографии ООО «Паблит»
127282, Москва, ул. Полярная, д. 31В, стр. 1 Тел.: (495) 230-20-52

ISBN 978-5-392-23168-3

ОГЛАВЛЕНИЕ