

УДК 614.2
ББК 32.973-018
В18

Электронные версии книг
на сайте www.prospekt.org

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 60×90^{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

© Дальневосточный государственный
технический университет, 2008
© ДВФУ, 2015
© ООО «Проспект», обложка, 2015

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ	4
1. БЕЗОПАСНОСТЬ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ	6
1.1. Пути несанкционированного доступа	6
1.2. Удаленные атаки на вычислительные системы	7
1.2.1. Классификация удаленных атак на распределенные вычислительные системы	8
1.2.2. Механизмы реализации типовых удаленных атак	12
1.3. Основные механизмы защиты информации в системах обработки данных	19
1.3.1. Идентификация и установление личности	22
1.3.2. Меры защиты против электронного и электромагнитного перехвата	22
1.4. Модель уязвимости информации	23
2. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ	28
2.1. Классификация методов криптографического преобразования информации	28
2.2. Криптографические алгоритмы	31
2.2.1. Симметричные алгоритмы	31
2.2.2. Ассиметричные алгоритмы	35
2.3. Цифровые подписи и цифровые сертификаты	39
2.4. Сравнительный анализ криптографических методов	42
2.5. Требования к криптографическим системам	47
2.6. Проблемы и перспективы криптографических систем	48
3. МНОГОУРОВНЕВЫЕ СИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ НА ОСНОВЕ КРИПТОГРАФИЧЕСКИХ МЕТОДОВ	53
3.1. Использование криптографических методов для контроля целостности информации	54
3.2. Криптографические протоколы	56
3.3. Анализ современного программного обеспечения криптозащиты	59
3.4. Синтез комплексов и систем криптозащиты	68
3.4.1. Анализ аппаратных комплексов криптографической защиты	68
3.4.2. Синтез многоуровневой системы обеспечения защиты конфиденциальной информации	75
4. АНАЛИЗ СОВРЕМЕННЫХ МЕТОДОВ ВСКРЫТИЯ АЛГОРИТМОВ ШИФРОВАНИЯ	77
4.1. Атаки на алгоритмы шифрования	77
4.2. Методы вскрытия криптографических алгоритмов	80
4.2.1. Метод вскрытия алгоритмов шифрования – дифференциальный криптоанализ	86
4.2.2. Метод вскрытия алгоритмов шифрования – линейный криптоанализ	90
ЗАКЛЮЧЕНИЕ	94
Организационно-методический раздел	98
Содержание дисциплины	99
Учебно-методическое обеспечение дисциплины	101
Лабораторная работа № 1	105
Лабораторная работа № 2	109
Лабораторная работа № 3	113
Лабораторная работа № 4	120
БИБЛИОГРАФИЧЕСКИЙ СПИСОК	149