

Варлатая С. К., Шаханова М. В.

В18 Криптографические методы и средства обеспечения информационной безопасности: учебно-методический комплекс. — Москва : Проспект, 2015. — 152 с.

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 |