

Шаханова М. В.

Ш 11 Современные технологии информационной безопасности: учебно-методический комплекс. — Москва: Проспект, 2015. — 216 с.

ОГЛАВЛЕНИЕ

Введение.....	3
1. Понятие информационной безопасности.....	5
2. Основные классификации угроз информационной безопасности.....	7
2.1. Классификация угроз, предложенная Стивом Кентом.....	8
2.2. Классификация угроз безопасности по средствам воздействия на систему.....	9
2.3. Угрозы безопасности в распределительных системах.....	15
2.4. Взаимосвязь различных видов угроз.....	16
3. Программы с потенциально опасными последствиями.....	17
3.1. Компьютерные вирусы.....	18
3.1.1. Основные виды вирусов и схемы их функционирования.....	20
3.1.2. Пути проникновения вирусов в компьютер и механизм распределения вирусных программ.....	23
3.1.3. Признаки появления вирусов.....	24
3.2. Люки.....	25
3.3. Троянские кони.....	26
3.4. Логическая бомба.....	27
3.5. Программные закладки.....	27
3.6. Атака "салями".....	32
4. Зарождение криптографии.....	33
5. Элементарные методы цифрового шифрования.....	38
5.1. Применение подстановок.....	39
5.1.1. Шифр Цезаря.....	39
5.2.Monoalfavitnye шифры.....	41
5.2.1. Шифрование инверсными символами (по дополнению до 255).....	44
5.3. Многоалфавитные методы.....	44
5.3.1. Шифр Плейфейера.....	45
5.3.2. Шифр Хилла.....	48
5.4. Полиалфавитные шифры.....	51
5.5. Шифр "двойной квадрат" Уитстона.....	56
5.6. Применение перестановок.....	58
5.6.1. Применение магических квадратов.....	59
5.7. Метод гаммирования.....	60
6. Симметричные системы защиты информации.....	62
6.1. Американский стандарт шифрования данных DES.....	62
6.2. Комбинирование блочных алгоритмов.....	77
6.3. Отечественный стандарт шифрования данных.....	79
6.4. Блочные и поточные шифры.....	90
7. Криптография с открытым ключом.....	97
7.1. Алгоритм RSA.....	98
7.2. Алгоритм Диффи-Хеллмана.....	105
7.3. Безопасность алгоритмов с открытыми ключами.....	106
7.4. Управление ключами.....	107
7.5. Электронная цифровая подпись.....	109
7.5.1. Алгоритм цифровой подписи RSA.....	111
7.5.2. Алгоритм цифровой подписи Эль Гамала (EGSA).....	113

7.5.3. Алгоритм цифровой подписи DSA.....	115
7.5.4. Отечественный стандарт цифровой подписи.....	117
7.6. Однонаправленные хеш-функции.....	118
8. Аутентификация.....	126
8.1. Пароли.....	127
8.2. Биометрические методы.....	137
8.3. Криптографические методы аутентификации.....	141
8.4. BAN-логика.....	142
8.5. Протокол Kerberos.....	144
9. Методы криптоанализа классических шифров.....	149
Заключение.....	162
Рабочая учебная программа.....	163
Организационно-методический раздел.....	163
Учебно-методическое обеспечение дисциплины.....	165
Методические указания к лабораторным работам.....	167
Лабораторная работа № 1.....	167
Лабораторная работа № 2.....	171
Лабораторная работа № 3.....	177
Лабораторная работа № 4.....	180
Лабораторная работа № 5.....	183
Контрольно-измерительные материалы.....	187
Методические рекомендации по разработке курсовых работ.....	202
Цели и задачи курсовой работы.....	202
Организация курсовой работы.....	203
Требования к содержанию пояснительной записки.....	206
Требования к оформлению пояснительной записки.....	209
Темы курсовых работ.....	209
Приложение А.....	211
Приложение Б.....	212
Приложение В.....	213
Список литературы.....	214