

Н. Г. Бутакова
Н. В. Федоров

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Учебное пособие

Санкт-Петербург, 2020



ОГЛАВЛЕНИЕ

ЧАСТЬ 1. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ.....	14
Тема 1. История развития криптографии.....	14
1.1. Криптография в Античные времена.....	17
1.2. Криптография в Средневековье.....	20
1.3. Криптография в Эпоху Возрождения.....	22
1.4. Криптография в Новое и Новейшее время.....	28
Тема 2. Основные задачи современной криптографии.....	35
2.1. Конфиденциальность.....	36
2.2. Целостность.....	39
2.3. Аутентификация.....	40
2.4. Неотслеживаемость.....	42
2.5. Цифровая подпись.....	43
2.6. Управление ключами.....	45
2.7. Общие требования к криптосистемам.....	47
Тема 3. Математические основы криптографии. Элементы теории чисел, абстрактной алгебры и алгебраической геометрии.....	49
3.1. Простые числа и непрерывные дроби.....	50
3.2. Мультипликативные функции.....	62
3.3. Сравнение целых чисел по модулю.....	67
3.4. Решение сравнений первой степени.....	72
3.5. Группы и их свойства.....	75
3.6. Кольца и тела в абстрактной алгебре.....	76
3.7. Конечные поля.....	77
3.8. Эллиптически кривые над конечными полями.....	81
Тема 4. Классификация шифров.....	90
4.1. Классификация шифров.....	90
4.2. Математические модели шифров.....	94
4.3. Математические модели открытого текста.....	96
4.4. Критерии распознавания открытого текста.....	98

Тема 5. Шифры перестановки	100
5.1. Шифр Сцитала	100
5.2. Маршрутные перестановки	100
5.3. Шифры вертикальной перестановки	102
5.4. Поворотные решетки.....	103
5.5. Задача Эйлера.....	104
5.6. Элементы криптоанализа шифров перестановки.....	105
 Тема 6. Шифры замены.....	 109
6.1. Поточные шифры простой замены	109
6.2. Шифры многоалфавитной замены.....	112
6.3. Биграммные и n-граммные шифры замены	116
6.4. Матричные шифры	118
6.5. Модель шифров замены.....	120
6.6. Классификация шифров замены	121
6.7. Криптоанализ поточного шифра простой замены	123
 Тема 7. Шифры гаммирования.....	 126
7.1. Основные требования к гамме	126
7.2. Шифр Виженера	128
7.3. Одноразовый блокнот К.Шеннона	130
7.4. Аддитивные методы шифрования	130
7.5. Режим гаммирования ГОСТ 28147-89 и Магма.....	131
 Тема 8. Поточные системы шифрования	 136
8.1. Регистры сдвига с обратной связью	136
8.2. Скремблеры.....	138
8.3. Методы рандомизации сообщений.....	144
8.4. Поточные шифрсистемы.....	146
 Тема 9. Блочные системы шифрования	 149
9.1. Блочные системы шифрования	149
9.2. Конструкции Фейстеля	150
9.3. Режимы шифрования блочных шифров.....	152

9.4.Алгоритмы блочного шифрования	156
Тема 10. Системы шифрования с открытыми ключами.....	165
10.1.Асимметричные системы	165
10.2.Открытое распределение ключей. Схема Диффи-Хеллмана.....	168
10.3.Криптосистема RSA	170
10.4.Схема шифрования Эль-Гамала.....	172
10.5.Криптография на эллиптических кривых	174
10.6.Криптоанализ шифра RSA.....	176
Тема 11. электронные Цифровые подписи	178
11.1. Механизм действия электронной цифровой подписи	178
11.2.Функции хэширования.....	181
11.3. Алгоритмы цифровой подписи	183
11.4. Криптоанализ односторонних хэш-функций	199
Тема 12. Квантовая криптография.....	201
12.1.Природа секретности квантового канала связи.....	201
12.2. Основные направления развития квантовой криптографии	202
12.3.Протоколы квантового обмена информацией	203
12.4. Квантовый криптоанализ.....	210
12.5. Проблемы практической реализации систем квантовой криптографии	211
ЧАСТЬ 2.СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ	
ИНФОРМАЦИИ.....	213
Тема 1. Нормативно-правовые основы криптографической защиты информации.....	213
1.1.Действующие стандарты криптографической защиты информации.....	213
1.2.Федеральный закон об электронной подписи.....	228
1.3.Нормативно-правовые акты ФСБ по обеспечению безопасности персональных данных с использованием СКЗИ	228
1.4.Нормативно-правовые акты ФСБ по обеспечению функционирования и эксплуатации СКЗИ	233

1.5.Виды работ и услуг, составляющих лицензируемую деятельность с использованием СКЗИ	233
1.6. Порядок лицензирования деятельности с использованием СКЗИ.....	234
1.7.Правила сертификации СКЗИ по требованиям ФСБ.....	237
1.8.Таможенные ограничения на ввоз и вывоз СКЗИ.....	238
Тема 2. Классификация средств криптографической защиты информации.....	241
2.1.Классификация средств криптографической защиты информации по различным признакам	242
2.2.Требования к средствам криптографической защиты информации.....	245
2.3.Программные СКЗИ. Особенности и примеры.....	246
2.4.Аппаратные и программно-аппаратные СКЗИ.	250
2.5.Критерии выбора СКЗИ.....	253
2.6.Основные принципы построения СКЗИ	254
2.7.Принципы построения аппаратных СКЗИ.....	256
2.8.Принципы построения программных и программно-аппаратных СКЗИ	257
2.9.Основные подходы к обеспечению надежности СКЗИ.....	259
Тема 3. Средства криптографической защиты информации на персональном компьютере	264
3.1.Задачи обеспечения информационной безопасности на персональном компьютере с использованием СКЗИ	264
3.2.Криптографическая защита жестких дисков и съемных носителей ..	265
3.3.Средства шифрования, встроенные в операционную систему Windows	274
3.4.Шифрование архиваторов	287
3.5.СКЗИ свободного доступа.....	289
3.6. СКЗИ от несанкционированного доступа.....	292
Тема 4. Средства криптографической защиты сетевого взаимодействия.....	309
4.1.Криптографические средства создания защищенных виртуальных сетей (VPN).....	309

4.2. Технология построения криптозащищенных туннелей	310
4.3. Криптографическая защита удаленного доступа к локальной сети	310
4.4. СКЗИ для передачи данных в локальных сетях	315
4.5. Сетевые протоколы криптографической защиты	318
4.6. Персональные криптографические средства аутентификации	327
ПРИЛОЖЕНИЯ	332
ЛИТЕРАТУРА	371