

ОГЛАВЛЕНИЕ

Предисловие	3
Глава 1. Основные понятия и определения	5
1.1. Цели защиты информации.....	5
1.2. Технические угрозы.....	6
1.3. «Человеческий фактор»	8
1.4. Основные термины.....	9
Выводы	10
Глава 2. Шифрование	11
2.1. Основные определения.....	11
2.2. История симметричного шифрования, типы шифров.....	13
2.3. Типовая схема алгоритма симметричного шифрования	16
2.4. Современные алгоритмы симметричного шифрования	18
2.5. Асимметричное шифрование	44
2.6. Комбинированный метод шифрования.....	49
2.7. Ключевые схемы.....	51
2.8. Технологические возможности внедрения «черного хода».....	57
Выводы.....	59
Глава 3. Электронная цифровая подпись	61
3.1. Назначение и использование.....	61
3.2. Хэширование.....	63
3.3. Современные алгоритмы ЭЦП.....	66
3.4. Проблема подмены открытого ключа	75
3.5. Двухуровневая сертификация открытых ключей	76
3.6. Инфраструктура открытых ключей.....	83
3.7. Комплексный метод защиты информации	89
Выводы.....	93
Глава 4. Методы защиты межсетевого обмена данными	95
4.1. Виртуальные частные сети	95
4.2. Протокол IPSec	102
4.3. Протоколы SSL и TLS	106
4.4. Стандарт S/MIME	108
4.5. Стандарт SET	109
Выводы	111
Глава 5. Аппаратные шифраторы	113
5.1. Структура аппаратных шифраторов.....	113
5.2. Шифропроцессоры	115
5.3. Принципы разработки программного интерфейса ..	118
5.4. Ключевые схемы.....	120
5.5. Электронный замок.....	121
5.6. Варианты технической реализации	122
5.7. Технические характеристики	124
Выводы.....	124
Глава 6. Практика применения PGP	126
6.1. Инсталляция PGP	127

6.2. Основные функции	129
Выводы.....	143
Глава 7. Организация виртуальных сетей и создание логических дисков с криптозащитой	144
7.1. Инсталляция	144
7.2. Установка соединения	150
7.3. Создание зашифрованного логического диска.....	156
7.4. Конфигурирование встроенного межсетевое экрана.....	160
7.5. Активизация функции обнаружения атак.....	162
7.6. Стирание остатков файлов	163
7.7. Назначение горячих клавиш	163
Выводы	165
Библиография.....	166
Рекомендуемая литература	172

В пособии освещены актуальные вопросы защиты информации с помощью современных криптографических алгоритмов, подробно описаны методы защиты, основные атаки на криптоалгоритмы и способы противодействия этим атакам. Изложены основные принципы разработки и использования средств криптографической защиты, представлены типовые ключевые схемы.

Для студентов, обучающихся по специальностям 080801 «Прикладная информатика в экономике» и 230105 «Программное обеспечение вычислительной техники и автоматизированных систем», а также для преподавателей и аспирантов соответствующих специальностей.