

ББК 32.973.26-018.2

ПЗ0

Петров А. А.

ПЗ0 Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК Пресс, 2008. – 448 с.: ил.

ISBN 5-89818-064-8

В книге рассматриваются актуальные вопросы защиты данных при создании распределенных информационных систем масштаба предприятия, приводятся подробные описания принципов применения современных криптографических средств, имеющихся на рынке («Криптон», «Верба», «Шип», «Игла» и др.). Значительное место уделяется проблемам сохранения тайны при финансовых обменах через Internet, а также электронной коммерции.

Завершают книгу приложения, посвященные практическим рекомендациям по самым острым вопросам обеспечения защиты информации.

ББК 32.973.26-018.2

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.

Материал, изложенный в данной книге, многократно проверен. Но поскольку вероятность технических ошибок все равно существует, издательство не может гарантировать абсолютную точность и правильность приводимых сведений. В связи с этим издательство не несет ответственности за возможные ошибки, связанные с использованием книги.

ISBN 5-89818-064-8

© Петров А. А.

© Компания АйТи

© ДМК Пресс, 2008

Содержание

О книге	7
Предисловие	10
Введение	14
Глава I	
Общие сведения по классической криптографии	21
1.1. Общие сведения	21
1.1.1. Стойкость алгоритмов шифрования	23
1.1.2. Типы алгоритмов шифрования	28
1.1.3. Аппаратная и программная реализация алгоритмов шифрования	31
1.2. Алгоритмы блочного шифрования	34
1.2.1. Общие сведения	34
1.2.2. Алгоритм DES	40
1.2.3. Алгоритм блочного шифрования	46
1.2.4. Применение алгоритмов блочного шифрования	51
1.3. Асимметричные алгоритмы шифрования	53
1.3.1. Общие сведения	53
1.3.2. Стандарт асимметричного шифрования RSA	55
1.3.3. Стойкость алгоритма RSA	57
1.3.4. Методы ускорения вычислений, применяемых в асимметричных алгоритмах	59
1.3.5. Практическое применение	62
1.4. Электронно-цифровая подпись	65
1.4.1. Общие положения	65
1.4.2. Атаки на ЭЦП	68
1.4.3. Алгоритм DSA	70
1.4.4. Стандарт на процедуры выработки и проверки ЭЦП	72
1.4.5. Практическое применение ЭЦП	74
1.4.6. Арбитраж ЭЦП	76
1.5. Хэш-функции	78
1.5.1. Общие сведения	78
1.5.2. Типы хэш-функций	79
1.5.3. Требования к хэш-функциям	83
1.5.4. Стойкость хэш-функций	84

1.6. Ключевая информация	85
1.6.1. Общие сведения	85
1.6.2. Генерация ключевой информации	86
1.6.3. Хранение ключей	88
1.6.4. Распределение ключей	89
1.6.5. Минимальная длина ключа	90

Глава II

Теоретические аспекты создания

и применения криптографических протоколов

2.1. Общие сведения	93
2.1.1. Область применения	93
2.1.2. Вопросы безопасности криптопротоколов	95
2.1.3. Формальные методы анализа криптопротоколов	99
2.2. Протоколы аутентификации	104
2.2.1. Общие сведения	104
2.2.2. Простая аутентификация	109
2.2.3. Строгая аутентификация	113
2.2.4. Протоколы аутентификации, обладающие свойством доказательства с нулевым знанием	121
2.3. Протоколы распределения и управления ключевой информацией ...	124
2.3.1. Протоколы распределения ключевой информации	124
2.3.2. Управление ключевой информацией	139
2.4. Специфические криптографические протоколы	157
2.4.1. Безопасные выборы	157
2.4.2. Совместная подпись контракта	159
2.4.3. Групповая подпись	160
2.4.4. Доверенная подпись	161
2.4.5. Неоспариваемая подпись	162
2.4.6. Слепая подпись	163
2.4.7. Забывающая передача	165
2.4.8. Подбрасывание монеты по телефону	166
2.4.9. Разделение знания секрета	167

Глава III

Компьютерная безопасность

и практическое применение криптографии

3.1. Общие сведения	169
3.1.1. Физический и канальный уровни	176
3.1.2. Сетевой уровень	177
3.1.3. Транспортный уровень	179

3.1.4. Прикладной уровень	179
3.1.5. Обзор стандартов в области защиты информации	180
3.1.6. Подсистема информационной безопасности	185
3.2. Защита локальной рабочей станции	189
3.2.1. Угрозы и задачи информационной безопасности для локальных рабочих станций	190
3.2.2. Методы и средства обеспечения информационной безопасности локальных рабочих станций	196
3.2.3. Организационно-технические меры защиты локальной рабочей станции	216
3.2.4. Штатные средства защиты современных операционных систем на примере Windows NT	221
3.2.5. Аудит	229
3.3. Защита в локальных сетях	231
3.3.1. Общие вопросы безопасности в ЛВС	232
3.3.2. Безопасность в сетях Novell NetWare	237
3.3.3. Безопасность в сетях Windows NT	241
3.3.4. Система Secret Net NT	257
3.4. Защита информации при межсетевом взаимодействии	260
3.4.1. Общие сведения	260
3.4.2. Обеспечение защиты информации при построении VPN	270
3.5. Защита технологии «клиент-сервер»	292
3.5.1. Типовые угрозы и обеспечение информационной безопасности при использовании технологии «клиент-сервер»	294
3.5.2. Подходы, применяемые к обеспечению информационной безопасности в клиент-серверных ИВС	300
3.5.3. Криптографические протоколы, используемые для защиты технологии «клиент-сервер»	302
3.5.4. Решения по защите информации в Web-технологиях	312
3.6. Применение межсетевых экранов	317
3.6.1. Пакетные фильтры	318
3.6.2. Шлюзы сеансового уровня	320
3.6.3. Шлюзы уровня приложений	321
3.6.4. Использование межсетевых экранов для создания VPN	323
3.6.5. Proxy-серверы	324
3.6.6. Виды подключения межсетевых экранов	326
3.6.7. Использование межсетевых экранов	328
3.6.8. Применение криптографии в межсетевых экранах на примере CheckPoint Firewall-1	329

3.7. Защита электронной почты	336
3.7.1. Принципы защиты электронной почты	337
3.7.2. Средства защиты электронной почты	340
3.7.3. Защита в архитектуре X.400	351
3.8. Корпоративные системы и опыт обеспечения информационной безопасности в них	361
3.8.1. Система S.W.I.F.T.	361
3.8.2. Технология SmartCity	372
3.8.3. Система UEPS	380
3.9. Электронные платежные системы и Internet	382
3.9.1. Классификация платежных систем	383
3.9.2. Теоретические основы электронных денег	393
3.9.3. Смарт-карты	397
3.9.4. Средства обеспечения безопасности электронных платежных систем	401
Приложение 1. Сравнительные характеристики отечественных средств построения VPN	407
Приложение 2. Система санкционированного доступа к ресурсам корпоративной информационной системы	418
Приложение 3. Ресурсы в Internet, посвященные вопросам компьютерной безопасности	433
Список рекомендуемой литературы	437