Петров А. А.

Компьютерная безопасность

Криптографические методы защиты

Москва, 2008

ББК 32.973.26-018.2
П30

Петров А. А.
П30 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.

© Петров А. А.
© Компания АйТи
© ДМК Пресс, 2008

ISBN 5-89818-064-8

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 ... 93
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 ... 169
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

О книге

В настоящее время издано много руководств, справочников, пособий по проблемам защиты информации. Это и переводные книги, и оригинальные работы отечественных авторов, и вузовские учебники. У подавляющего большинства авторов книги либо чересчур «теоретичны», либо предельно популярны. И то, и другое отпугивает читателей-практиков, которым понимание теории необходимо для ее конкретного применения.

Монография А. Петрова «Компьютерная безопасность. Криптографические методы защиты» является в этом смысле приятным исключением. Наряду с описанием шифрующих преобразований и цифровой подписи в книге содержатся и актуальные сведения о современных криптографических протоколах, и практическая информация, посвященная принципам применения имеющихся на рынке сертифицированных криптографических средств («Криптон», «Верба», «Шип», «Игла» и др.).

Нельзя не отметить и те разделы книги, в которых излагаются теоретические основы компьютерной безопасности. Здесь впервые систематизированы и всесторонне рассмотрены атаки на современные компьютерные системы и различные способы защиты от них.

Монография, несомненно, представляет интерес для широкого круга читателей, в том числе обучающихся по типовым программам специальностей «Введение в криптографию», «Компьютерная безопасность», «Программно-аппаратные средства обеспечения информационной безопасности».

А. Ю. Щербаков,
доктор технических наук, научный консультант подразделения ФАПСИ,
руководитель группы систем защиты от информационного оружия,
почетный член Европейской ассоциации хакеров,
профессор кафедры «Информационная безопасность»
Московского государственного института электроники и математики

Разработчикам информационных систем повышенной сложности, таких как корпоративные информационные системы или информационные системы масштаба крупного предприятия, в последнее время приходится решать задачи, удачное решение которых полностью зависит от точного соблюдения основополагающих и общепринятых правил проектирования и эксплуатации виртуальных конструкций, как-то:

- поддержка стандартов, подразумевающая соответствие общепринятым технологическим стандартам, которыми руководствуются фирмы-производители программного обеспечения;
- масштабируемость, означающая, что программное обеспечение должно работать с приемлемой производительностью без внесения в него существенных изменений при увеличении мощности и количества используемого оборудования;
- многозвенность, где требуется, чтобы каждый уровень системы (клиент, Web-сервер, сервер приложений, сервер баз данных) отвечал и реализовывал только те функции, которые ему наиболее присущи;
- обеспечение (по возможности) аппаратно-платформенной независимости программного обеспечения, используемого при разработке системы;
- коммуникативность и интегрированность, что означает возможность различных уровней системы взаимодействовать между собой, как по данным, так и по приложениям;
- защищенность.

Безусловно, существуют и другие, менее важные задачи, но здесь хотелось бы отметить, что любая из перечисленных проблем внедрения корпоративных информационных систем на базе технологий Internet/intranet может быть успешно реализована только при наличии хорошо организованных средств защиты информации, централизованного управления информационными ресурсами и разграничения доступа к ним. Особенно это важно при обеспечении доступа пользователей из внешних сетей к ресурсам корпоративной ИС по так называемой extranet-технологии.

Как раз одному из этих направлений – защите информации в распределенных сетях – и посвящена книга А. Петрова «Компьютерная безопасность. Криптографические методы защиты», которую мне особенно приятно представить коллегам и читателям.

На сегодняшний день обеспечение безопасности потоков данных является одним из самых перспективных направлений науки и техники, имеющих большое теоретическое и практическое значение.

Автору удалось собрать в книге солидный фактический материал, систематизировать его, изложить свою точку зрения по конкретным вопросам, касающимся практического использования не только отечественных, но и зарубежных криптографических методов и средств защиты информации.

В приложениях, написанных сотрудниками ЦБ России, приведен список известных серверов по проблемам защиты информации. Эти сведения, безусловно, позволят читателям расширить свои знания в данной области.

Я надеюсь, что после знакомства с представляемой книгой моим коллегам станут ближе и понятнее проблемы защиты информации, в том смысле, что работа начинается с проектирования архитектуры информационной системы и заканчивается выбором средств на уровне шифрования.

Занимаясь вопросами создания реальных информационных систем, нам часто не хватает времени познакомиться и тем более сравнить различные варианты реализации средств защиты информации. Надеюсь, что данная книга и приложения к ней позволят уважаемым читателям и коллегам различить новые направления в такой широкой и в то же время такой специальной теме, как проблема построения защищенных информационных систем.

В. С. Лаптев,
кандидат технических наук,
президент Фонда развития программной инженерии

Предисловие

В настоящее время первостепенным фактором, влияющим на политическую и экономическую составляющие национальной безопасности, является степень защищенности информации и информационной среды. Вот почему важное значение приобретают вопросы обеспечения безопасности информационных и телекоммуникационных технологий и гарантированной защиты данных в компьютерных сетях экономически значимых структур. О необходимости надежной защиты свидетельствуют многочисленные компьютерные преступления, совершаемые как в кредитно-финансовой сфере, так и в государственных органах. При этом заметно увеличилось число противоправных деяний, совершенных путем удаленных атак с использованием территориально-распределенных сетей передачи данных. Подобные правонарушения опасны тем, что на сегодняшний день устоявшейся практики борьбы с ними не существует.

Вместе с тем необходимо отметить, что, несмотря на резкое возрастание интереса к проблемам защиты информации, в отечественной научно-технической литературе данная тема освещена слабо, и автор в меру своих сил попытался заполнить этот пробел. В предлагаемой книге рассматриваются вопросы применения криптографии для защиты информации в современных информационно-телекоммуникационных системах, отражающие только одну из областей компьютерной безопасности, однако, на взгляд автора, на сегодняшний день наиболее значимую. В книге освещаются как теоретические аспекты применения классической криптографии (глава 1) и современных криптографических протоколов (глава 2), так и практические вопросы (глава 3), которые возникают при осуществлении защиты информации криптографическими методами и средствами.

В данной книге также затрагиваются проблемы защиты платежных систем в Internet, безопасность современных операционных систем (Windows NT и Novell NetWare) и ряд других актуальных вопросов компьютерной безопасности.

Во введении обсуждается терминология, а также цели и задачи, возникающие при обеспечении информационной безопасности. Здесь определяется роль криптографических протоколов как наиболее перспективного