Шаньгин В. Ф.

Защита компьютерной информации

Эффективные методы и средства

Допущено Учебно-методическим объединением вузов по университетскому политехническому образованию в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению 230100 «Информатика и вычислительная техника»

ДМК Пресс
издательство
Москва, 2010

УДК 004.056.5
ББК 32.973.202
Ш12

Шаньгин В. Ф.

Ш12 Защита компьютерной информации. Эффективные методы и средства / Шаньгин В. Ф. – М. : ДМК Пресс, 2010. – 544 с. : ил.

ISBN 978-5-94074-518-1

Формулируются основные понятия и определения защиты информации, анализируются угрозы информационной безопасности в компьютерных системах и сетях. Обсуждаются базовые понятия и принципы политики безопасности. Анализируются международные и отечественные стандарты информационной безопасности. Описываются основные криптографические методы и алгоритмы защиты компьютерной информации. Обосновываются многоуровневая защита и комплексный подход к обеспечению информационной безопасности корпоративных систем и сетей. Рассматривается защита информации в распространенных операционных системах. Описываются базовые технологии защиты межсетевого обмена данными. Обсуждаются методы и средства антивирусной защиты. Описывается организационно-правовое обеспечение информационной безопасности на основе государственных стандартов и руководящих документов Государственной технической комиссии России.

Книга рекомендуется в качестве учебного пособия для студентов вузов, обучающихся по специальностям направления «Информатика и вычислительная техника». Книга будет также полезна аспирантам и преподавателям вузов соответствующих специальностей.

Издание представляет практический интерес для пользователей и администраторов компьютерных сетей и систем, предпринимателей, бизнесменов, менеджеров, руководителей предприятий, стремящихся обеспечить безопасность своих корпоративных информационных систем и сетей.

Данное учебное пособие выполнено в соответствии с Инновационной Образовательной программой «Современное профессиональное образование для Российской Инновационной Системы в области электроники» в рамках Национального проекта «Образование».

УДК 004.056.5
ББК 32.973.202

ISBN 978-5-94074-518-1

© Шаньгин В. Ф., 2010
© ДМК Пресс, 2010

Оглавление

Предисловие 11
Введение 15
Список сокращений 19

ЧАСТЬ I
Проблемы информационной безопасности 23

Глава 1
Основные понятия и анализ угроз информационной безопасности 25

1.1. Основные понятия защиты информации и информационной безопасности 25
1.2. Анализ угроз информационной безопасности 30

Глава 2
Проблемы информационной безопасности сетей 40

2.1. Введение в сетевой информационный обмен 40
2.1.1. Использование сети Интернет 41
2.1.2. Модель ISO/OSI и стек протоколов TCP/IP 42
2.2. Анализ угроз сетевой безопасности 49
2.2.1. Проблемы безопасности IP-сетей 50
2.2.2. Угрозы и уязвимости проводных корпоративных сетей 60
2.2.3. Угрозы и уязвимости беспроводных сетей 62
2.3. Обеспечение информационной безопасности сетей 65
2.3.1. Способы обеспечения информационной безопасности 65
2.3.2. Пути решения проблем защиты информации в сетях 68

Глава 3
Политика безопасности 71

3.1. Основные понятия политики безопасности 72
3.2. Структура политики безопасности организации 78
3.2.1. Базовая политика безопасности 79
3.2.2. Специализированные политики безопасности 79
3.2.3. Процедуры безопасности 82
3.3. Разработка политики безопасности организации 84

Глава 4
Стандарты информационной безопасности 93

4.1. Роль стандартов информационной безопасности 93
4.2. Международные стандарты информационной безопасности 95
4.2.1. Стандарты ISO/IEC 17799:2002 (BS 7799:2000) 95
4.2.2. Германский стандарт BSI 97
4.2.3. Международный стандарт ISO 15408 «Общие критерии безопасности информационных технологий» 97
4.2.4. Стандарты для беспроводных сетей 99
4.2.5. Стандарты информационной безопасности в Интернете 103
4.3. Отечественные стандарты безопасности информационных технологий 106

ЧАСТЬ II
Технологии защиты данных 111

Глава 5
Криптографическая защита информации 113

5.1. Основные понятия криптографической защиты информации 113
5.2. Симметричные криптосистемы шифрования 117
5.2.1. Алгоритм шифрования DES 121
5.2.2. Стандарт шифрования ГОСТ 28147-89 124
5.2.3. Американский стандарт шифрования AES 128
5.2.4. Основные режимы работы блочного симметричного алгоритма 131
5.2.5. Особенности применения алгоритмов симметричного шифрования 135
5.3. Асимметричные криптосистемы шифрования 137
5.3.1. Алгоритм шифрования RSA 141
5.3.2. Асимметричные криптосистемы на базе эллиптических кривых 145
5.3.3. Алгоритм асимметричного шифрования ECES 147

5.4. Функция хэширования 148
5.5. Электронная цифровая подпись 151
5.5.1. Основные процедуры цифровой подписи 151
5.5.2. Алгоритм цифровой подписи DSA 154
5.5.3. Стандарт цифровой подписи ГОСТ Р 34.10-94 156
5.5.4. Алгоритм цифровой подписи ECDSA 157
5.5.5. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-2001 157
5.6. Управление криптоключами 162
5.6.1. Использование комбинированной криптосистемы 164
5.6.2. Метод распределения ключей Диффи–Хеллмана 167
5.6.3. Протокол вычисления ключа парной связи ECKEP 170

Глава 6
Технологии аутентификации 172

6.1. Аутентификация, авторизация и администрирование действий пользователей 172
6.2. Методы аутентификации, использующие пароли и PIN-коды 176
6.2.1. Аутентификация на основе многоразовых паролей 177
6.2.2. Аутентификация на основе одноразовых паролей 182
6.2.3. Аутентификация на основе PIN-кода 184
6.3. Строгая аутентификация 188
6.3.1. Основные понятия 188
6.3.2. Строгая аутентификация, основанная на симметричных алгоритмах ... 190
6.3.3. Строгая аутентификация, основанная на асимметричных алгоритмах . 194
6.4. Биометрическая аутентификация пользователя 196
6.5. Аппаратно-программные системы идентификации и аутентификации 201

ЧАСТЬ III
Многоуровневая защита корпоративных сетей 221

Глава 7
Модели безопасности операционных систем 223

7.1. Проблемы обеспечения безопасности ОС 223
7.1.1. Угрозы безопасности операционной системы 223
7.1.2. Понятие защищенной операционной системы 225
7.2. Архитектура подсистемы защиты операционной системы 229
7.2.1. Основные функции подсистемы защиты операционной системы 229
7.2.2. Идентификация, аутентификация и авторизация субъектов доступа 230

7.2.3. Разграничение доступа к объектам операционной системы 231
7.2.4. Аудит 239
7.3. Защита в операционной системе UNIX 241
7.4. Средства безопасности ОС Windows XP Professional 254

Глава 8
Технологии межсетевых экранов 262

8.1. Функции межсетевых экранов 262
8.1.1. Фильтрация трафика 264
8.1.2. Выполнение функций посредничества 265
8.1.3. Дополнительные возможности МЭ 267
8.2. Особенности функционирования межсетевых экранов на различных уровнях модели OSI 271
8.2.1. Экранирующий маршрутизатор 272
8.2.2. Шлюз сеансового уровня 273
8.2.3. Прикладной шлюз 276
8.2.4. Шлюз экспертного уровня 279
8.2.5. Варианты исполнения межсетевых экранов 280
8.3. Схемы сетевой защиты на базе межсетевых экранов 282
8.3.1. Формирование политики межсетевого взаимодействия 282
8.3.2. Основные схемы подключения межсетевых экранов 285
8.3.3. Персональные и распределенные сетевые экраны 290
8.3.4. Проблемы безопасности межсетевых экранов 291

Глава 9
Основы технологии виртуальных защищенных сетей VPN 293

9.1. Концепция построения виртуальных защищенных сетей VPN 293
9.1.1. Основные понятия и функции сети VPN 294
9.1.2. Варианты построения виртуальных защищенных каналов 299
9.1.3. Средства обеспечения безопасности VPN 301
9.2. VPN-решения для построения защищенных сетей 307
9.2.1. Классификация сетей VPN 308
9.2.2. Основные варианты архитектуры VPN 312
9.2.3. Основные виды технической реализации VPN 316
9.3. Технические и экономические преимущества технологий VPN 320

Глава 10
Защита на канальном и сеансовом уровнях 323

10.1. Протоколы формирования защищенных каналов на канальном уровне 323
10.1.1. Протокол PPTP 324
10.1.2. Протоколы L2F и L2TP 327
10.2. Протоколы формирования защищенных каналов на сеансовом уровне 333
10.2.1. Протоколы SSL и TLS 334
10.2.2. Протокол SOCKS 337
10.3. Защита беспроводных сетей 341

Глава 11
Защита на сетевом уровне – протокол IPSec 346

11.1. Архитектура средств безопасности IPSec 347
11.2. Защита передаваемых данных с помощью протоколов AH и ESP 352
11.2.1. Протокол аутентифицирующего заголовка AH 352
11.2.2. Протокол инкапсулирующей защиты ESP 355
11.2.3. Алгоритмы аутентификации и шифрования в IPSec 359
11.3. Протокол управления криптоключами IKE 362
11.3.1. Установление безопасной ассоциации 362
11.3.2. Базы данных SAD и SPD 364
11.3.3. Согласование параметров защищенных каналов и распределение криптографических ключей 368
11.4. Особенности реализации средств IPSec 375
11.4.1. Основные схемы применения IPSec 376
11.4.2. Преимущества средств безопасности IPSec 378

Глава 12
Инфраструктура защиты на прикладном уровне 380

12.1. Управление идентификацией и доступом 381
12.1.1. Особенности управления доступом 382
12.1.2. Функционирование системы управления доступом 384
12.2. Организация защищенного удаленного доступа 387
12.2.1. Протоколы аутентификации удаленных пользователей 389
12.2.2. Централизованный контроль удаленного доступа 396

12.3. Управление доступом по схеме однократного входа с авторизацией Single Sign-On ... 401
12.3.1. Простая система однократного входа Single Sign-On ... 404
12.3.2. Системы однократного входа Web SSO ... 405
12.3.3. SSO-продукты уровня предприятия ... 407
12.4. Протокол Kerberos ... 409
12.5. Инфраструктура управления открытыми ключами PKI ... 416
12.5.1. Принципы функционирования PKI ... 417
12.5.2. Логическая структура и компоненты PKI ... 422

ЧАСТЬ IV
Технологии обнаружения вторжений ... 427

Глава 13
Технологии обнаружения атак ... 429
13.1. Концепция адаптивного управления безопасностью ... 429
13.2. Технология анализа защищенности ... 433
13.2.1. Средства анализа защищенности сетевых протоколов и сервисов ... 435
13.2.2. Средства анализа защищенности операционной системы ... 436
13.2.3. Общие требования к выбираемым средствам анализа защищенности ... 437
13.3. Средства обнаружения сетевых атак ... 439
13.3.1. Методы анализа сетевой информации ... 439
13.3.2. Классификация систем обнаружения атак ... 441
13.3.3. Компоненты и архитектура системы обнаружения атак ... 444
13.3.4. Особенности систем обнаружения атак на сетевом и операционном уровнях ... 446
13.3.5. Методы реагирования ... 448
13.4. Обзор современных средств обнаружения атак ... 449

Глава 14
Технологии защиты от вирусов ... 453
14.1. Компьютерные вирусы и проблемы антивирусной защиты ... 454
14.1.1. Классификация компьютерных вирусов ... 454
14.1.2. Жизненный цикл вирусов ... 456
14.1.3. Основные каналы распространения вирусов и других вредоносных программ ... 462

14.2. Антивирусные программы и комплексы 464
14.2.1. Антивирусные программы 465
14.2.2. Антивирусные программные комплексы 471
14.3. Построение системы антивирусной защиты сети 473
14.3.1. Актуальность централизованного управления антивирусной защитой корпоративной сети предприятия 474
14.3.2. Этапы построения системы антивирусной защиты корпоративной сети 476
14.3.3. Возможные решения антивирусной защиты корпоративной сети 478

ЧАСТЬ V
Управление средствами защиты информации 481

Глава 15
Методы управления средствами сетевой защиты 483

15.1. Задачи управления системой сетевой защиты 483
15.2. Архитектура управления средствами сетевой защиты 485
15.2.1. Основные понятия 486
15.2.2. Концепция глобального управления безопасностью 487
15.2.3. Глобальная и локальная политики безопасности 488
15.2.4. Функционирование системы управления средствами защиты 491
15.3. Аудит и мониторинг безопасности 496
15.3.1. Аудит безопасности информационной системы 496
15.3.2. Мониторинг безопасности системы 499
15.4. Обзор современных систем управления сетевой защитой 501
15.4.1. Централизованное управление безопасностью, реализованное в продуктах «ЗАСТАВА 3.3» 501
15.4.2. Продукты компании IBM Tivoli для управления средствами безопасности 503

Глава 16
Требования к системам защиты информации 507

16.1. Общие требования и рекомендации 507
16.2. Основные требования и рекомендации по защите информации, составляющей служебную или коммерческую тайну, а также персональных данных 511
16.3. Порядок обеспечения защиты конфиденциальной информации в АС 512

16.4. Защита конфиденциальной информации на рабочих местах пользователей ПК 513
16.5. Защита информации при использовании съемных накопителей информации большой емкости 514
16.6. Защита информации в локальных вычислительных сетях 515
16.7. Защита информации при межсетевом взаимодействии 516
16.8. Защита информации при работе с системами управления базами данных 516
16.9. Защита информации при взаимодействии абонентов с сетями общего пользования 517

Список литературы 524

Предметный указатель 530