

УДК 004.056.5
ББК 32.973.202-018.2

Ш22

Ш22 Шаньгин В. Ф.

Защита информации в компьютерных системах и сетях. / В. Ф. Шаньгин, Москва: ДМК Пресс, 2012. – 592 с.: ил.

ISBN 978-5-94074-833-5

Книга посвящена методам и средствам многоуровневой защиты информации в компьютерных системах и сетях. Формулируются основные понятия защиты информации, анализируются угрозы информационной безопасности в компьютерных информационных системах. Обсуждаются базовые понятия и принципы политики информационной безопасности. Анализируются международные и отечественные стандарты информационной безопасности. Описываются криптографические методы и алгоритмы защиты информации. Обсуждаются методы и средства идентификации, аутентификации и управления доступом в корпоративных информационных системах. Обосновывается комплексный многоуровневый подход к обеспечению информационной безопасности корпоративных систем. Анализируются инфраструктура и безопасность «облачных» вычислений. Рассматриваются средства обеспечения безопасности операционных систем UNIX и Windows 7. Обсуждаются методы и средства формирования виртуальных защищенных каналов и сетей. Описываются функции межсетевых экранов. Рассматриваются технологии обнаружения и предотвращения вторжений в корпоративные информационные системы. Обсуждаются технологии защиты от вредоносных программ и спама. Рассматриваются методы управления средствами обеспечения информационной безопасности.

Данная книга представляет интерес для пользователей и администраторов компьютерных систем и сетей, менеджеров, руководителей предприятий, заинтересованных в безопасности своих корпоративных информационных систем и сетей. Книга может быть использована в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению «Информатика и вычислительная техника», а также для аспирантов и преподавателей вузов соответствующих специальностей.

Шаньгин Владимир Федорович
Защита информации
в компьютерных системах и сетях

Главный редактор Мовчан Д. А.
dm@dmk-press.ru
Корректор Синяева Г. И.
Верстка Паранская Н. В.
Дизайн обложки Мовчан А. Г.

Подписано в печать 26.03.2012. Формат 70×100 1/16 .
Гарнитура «Петербург». Печать офсетная.
Усл. печ. л. 48,1. Тираж 200 экз.
Заказ №

Web-сайт издательства: www.dmk-press.ru
Электронный адрес издательства: books@dmkpress.ru

ISBN 978-5-94074-833-5

© Шаньгин В. Ф., 2012

© Оформление, издание, ДМК Пресс, 2012



Оглавление

Предисловие	11
Введение	15
Список сокращений	18

ЧАСТЬ I

Проблемы информационной безопасности	23
--	----

Глава 1

Основные понятия и анализ угроз информационной безопасности	25
---	----

1.1. Основные понятия информационной безопасности и защиты информации	25
1.2. Анализ угроз информационной безопасности	30
1.3. Анализ угроз корпоративных сетей	40
1.3.1. Характерные особенности сетевых атак	40
1.3.2. Угрозы и уязвимости беспроводных сетей	52
1.4. Тенденции развития ИТ-угроз	55
1.5. Криминализация атак на компьютерные сети и системы	57
1.6. Появление кибероружия для ведения технологических кибервойн	60
1.7. Обеспечение информационной безопасности компьютерных систем	62
1.7.1. Меры и средства обеспечения информационной безопасности	62
1.7.2. Пути решения проблем информационной безопасности	65

Глава 2

Политика информационной безопасности	68
--	----

2.1. Основные понятия политики безопасности	69
---	----

4 ОГЛАВЛЕНИЕ

2.2. Структура политики безопасности организации	75
2.2.1. Базовая политика безопасности	76
2.2.2. Специализированные политики безопасности	76
2.2.3. Процедуры безопасности	79
2.3. Разработка политики безопасности организации	81
2.3.1. Компоненты архитектуры безопасности	85
2.3.2. Роли и ответственности в безопасности сети	87

Глава 3

Стандарты информационной безопасности	91
3.1. Роль стандартов информационной безопасности	91
3.2. Международные стандарты информационной безопасности	93
3.2.1. Стандарты ISO/IEC 17799:2002 (BS 7799:2000)	93
3.2.2. Германский стандарт BSI	95
3.2.3. Международный стандарт ISO 15408	
«Общие критерии безопасности информационных технологий»	95
3.2.4. Стандарты для беспроводных сетей	98
3.2.5. Стандарты информационной безопасности для Интернета	101
3.3. Отечественные стандарты безопасности	
информационных технологий	105
3.3.1. Стандарт «Критерии оценки безопасности	
информационных технологий» ГОСТ Р ИСО/МЭК 15408	107

ЧАСТЬ II

Технологии защиты данных	109
---------------------------------------	------------

Глава 4

Криптографическая защита информации	111
4.1. Основные понятия криптографической защиты информации	111
4.2. Симметричные криптосистемы шифрования	115
4.2.1. Алгоритмы шифрования DES и 3-DES	119
4.2.2. Стандарт шифрования ГОСТ 28147-89	123
4.2.3. Стандарт шифрования AES	127
4.2.4. Другие симметричные криптоалгоритмы	130
4.2.5. Основные режимы работы блочного	
симметричного алгоритма	131
4.2.6. Особенности применения алгоритмов	
симметричного шифрования	135
4.3. Асимметричные криптосистемы шифрования	136

4.3.1. Алгоритм шифрования RSA	140
4.3.2. Асимметричные криптосистемы на базе эллиптических кривых	144
4.3.3. Алгоритм асимметричного шифрования ECES	146
4.4. Функции хэширования	147
4.4.1. Отечественный стандарт хэширования ГОСТ Р 34.11-94	149
4.5. Электронная цифровая подпись	15
4.5.1. Основные процедуры цифровой подписи	151
4.5.2. Алгоритм цифровой подписи DSA	154
4.5.3. Алгоритм цифровой подписи ECDSA	155
4.5.4. Алгоритм цифровой подписи ГОСТ Р 34.10-94.....	155
4.5.5. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-2001	157
4.5.6. Новый Федеральный закон РФ «Об электронной подписи»	161
4.6. Управление криптоключами	163
4.6.1. Использование комбинированной криптосистемы	165
4.6.2. Метод распределения ключей Диффи–Хеллмана	168
4.6.3. Протокол вычисления ключа парной связи ECKEP	170
4.7. Инфраструктура управления открытыми ключами PKI.....	171
4.7.1. Принципы функционирования PKI.....	172
4.7.2. Логическая структура и компоненты PKI	175

Глава 5

Идентификация, аутентификация и управление доступом	183
5.1. Аутентификация, авторизация и администрирование действий пользователей	183
5.2. Методы аутентификации, использующие пароли.....	187
5.2.1. Аутентификация на основе многоразовых паролей	188
5.2.2. Аутентификация на основе одноразовых паролей	190
5.3. Строгая аутентификация	191
5.3.1. Основные понятия	191
5.3.2. Применение смарт-карт и USB-токенов	192
5.3.3. Криптографические протоколы строгой аутентификации	203
5.4. Биометрическая аутентификация пользователя.....	210
5.5. Управление доступом по схеме однократного входа с авторизацией Single Sign-On	215
5.5.1. Простая система однократного входа Single Sign-On	217
5.5.2. Системы однократного входа Web SSO	219
5.5.3. SSO-продукты уровня предприятия	221
5.6. Управление идентификацией и доступом.....	223

ЧАСТЬ III

Многоуровневая защита корпоративных информационных систем227

Глава 6

Принципы многоуровневой защиты корпоративной информации ...229

- 6.1. Корпоративная информационная система с традиционной структурой229
- 6.2. Системы «облачных» вычислений235
 - 6.2.1. Модели «облачных» вычислений236
 - 6.2.2. Архитектура «облачных» сервисов238
 - 6.2.3. Основные характеристики «облачных» вычислений239
 - 6.2.4. Концепция архитектуры «облачной» системы240
- 6.3. Многоуровневый подход к обеспечению информационной безопасности КИС243
- 6.4. Подсистемы информационной безопасности традиционных КИС ...246
- 6.5. Безопасность «облачных» вычислений254
 - 6.5.1. Основные проблемы безопасности «облачной» инфраструктуры ...255
 - 6.5.2. Средства защиты в виртуальных средах257
 - 6.5.3. Выбор провайдера облачных услуг261

Глава 7

Обеспечение безопасности операционных систем.....266

- 7.1. Проблемы обеспечения безопасности ОС266
 - 7.1.1. Угрозы безопасности операционной системы266
 - 7.1.2. Понятие защищенной операционной системы268
- 7.2. Архитектура подсистемы защиты операционной системы272
 - 7.2.1. Основные функции подсистемы защиты операционной системы272
 - 7.2.2. Идентификация, аутентификация и авторизация субъектов доступа273
 - 7.2.3. Разграничение доступа к объектам операционной системы274
 - 7.2.4. Аудит283
- 7.3. Обеспечение безопасности ОС UNIX284
 - 7.3.1. Основные положения284
 - 7.3.2. Парольная защита287
 - 7.3.3. Защита файловой системы289
 - 7.3.4. Средства аудита294
 - 7.3.5. Безопасность системы UNIX при работе в сети298

7.4. Обеспечение безопасности ОС Windows 7	298
7.4.1. Средства защиты общего характера	300
7.4.2. Защита данных от утечек и компрометации	303
7.4.3. Защита от вредоносного ПО	310
7.4.4. Безопасность Internet Explorer 8 и 9	319
7.4.5. Совместимость приложений с Windows 7	326
7.4.6. Обеспечение безопасности работы в корпоративных сетях	329

Глава 8

Протоколы защищенных каналов	331
8.1. Модель взаимодействия систем ISO/OSI и стек протоколов TCP/IP.....	331
8.1.1. Структура и функциональность стека протоколов TCP/IP	333
8.2. Защита на канальном уровне – протоколы PPTP и L2TP	339
8.2.1. Протокол PPTP	339
8.2.2. Протокол L2TP	343
8.3. Защита на сетевом уровне – протокол IPSec	347
8.3.1. Архитектура средств безопасности IPSec	348
8.3.2. Защита передаваемых данных с помощью протоколов AH и ESP	353
8.3.3. Протокол управления криптоключами IKE	363
8.3.4. Особенности реализации средств IPSec	368
8.4. Защита на сеансовом уровне – протоколы SSL, TLS и SOCKS	371
8.4.1. Протоколы SSL и TLS	371
8.4.2. Протокол SOCKS	375
8.5. Защита беспроводных сетей	379
8.5.1. Общие сведения	379
8.5.2. Обеспечение безопасности беспроводных сетей	380

Глава 9

Технологии межсетевого экранирования	384
9.1. Функции межсетевых экранов	384
9.1.1. Фильтрация трафика	386
9.1.2. Выполнение функций посредничества	387
9.1.3. Дополнительные возможности МЭ	389
9.2. Особенности функционирования межсетевых экранов на различных уровнях модели OSI	392
9.2.1. Экранирующий маршрутизатор	394
9.2.2. Шлюз сеансового уровня	395

8 ОГЛАВЛЕНИЕ

9.2.3. Прикладной шлюз	397
9.2.4. Шлюз экспертного уровня	400
9.2.5. Варианты исполнения межсетевых экранов	401
9.3. Схемы сетевой защиты на базе межсетевых экранов	402
9.3.1. Формирование политики межсетевого взаимодействия	403
9.3.2. Основные схемы подключения межсетевых экранов	405
9.3.3. Персональные и распределенные сетевые экраны	410
9.3.4. Примеры современных межсетевых экранов	412
9.3.5. Тенденции развития межсетевых экранов	414
Глава 10	
Технологии виртуальных защищенных сетей VPN	417
10.1. Концепция построения виртуальных защищенных сетей VPN.....	417
10.1.1. Основные понятия и функции сети VPN	418
10.1.2. Варианты построения виртуальных защищенных каналов	423
10.1.3. Средства обеспечения безопасности VPN	425
10.2. VPN-решения для построения защищенных сетей	430
10.2.1. Классификация сетей VPN	431
10.2.2. Основные варианты архитектуры VPN	435
10.2.3. Основные виды технической реализации VPN	439
10.3. Современные VPN-продукты	443
10.3.1. Семейство VPN-продуктов компании «С-Терра СиЭсПи	443
10.3.2. Устройства сетевой защиты Cisco ASA 5500 Series	449
Глава 11	
Защита удаленного доступа	453
11.1. Особенности удаленного доступа	454
11.1.1. Методы управления удаленным доступом	455
11.1.2. Функционирование системы управления доступом	457
11.2. Организация защищенного удаленного доступа	460
11.2.1. Средства и протоколы аутентификации удаленных пользователей	462
11.2.2. Централизованный контроль удаленного доступа	475
11.3. Протокол Kerberos	480
Глава 12	
Технологии обнаружения и предотвращения вторжений	489
12.1. Основные понятия	489
12.2. Обнаружение вторжений системой IPS	492

12.3. Предотвращение вторжений в КИС	494
12.3.1. Предотвращение вторжений системного уровня	494
12.3.2. Предотвращение вторжений сетевого уровня	495
12.3.3. Защита от DDoS-атак	498
Глава 13	
Технологии защиты от вредоносных программ и спама	502
13.1. Классификация вредоносных программ	502
13.2. Основы работы антивирусных программ	507
13.2.1. Сигнатурный анализ	507
13.2.2. Особенности «облачной» антивирусной технологии	509
13.2.3. Проактивные методы обнаружения	510
13.2.4. Дополнительные модули	513
13.2.5. Режимы работы антивирусов	515
13.2.6. Антивирусные комплексы	516
13.2.7. Дополнительные средства защиты	518
13.3. Защита персональных компьютеров и корпоративных систем от воздействия вредоносных программ и вирусов	521
13.3.1. Защита домашних персональных компьютеров от воздействия вредоносных программ и вирусов	521
13.3.2. Подсистема защиты корпоративной информации от вредоносных программ и вирусов	523
13.3.3. Серия продуктов «Kaspersky Open Space Security» для защиты корпоративных сетей от современных интернет-угроз	525
ЧАСТЬ IV	
Управление информационной безопасностью	529
Глава 14	
Управление средствами обеспечения информационной безопасности	531
14.1. Задачи управления информационной безопасностью	531
14.2. Архитектура управления информационной безопасностью КИС	537
14.2.1. Концепция глобального управления безопасностью GSM	537
14.2.2. Глобальная и локальные политики безопасности	539
14.3. Функционирование системы управления информационной безопасностью КИС	542
14.3.1. Назначение основных средств защиты	543

10 ОГЛАВЛЕНИЕ

14.3.2. Защита ресурсов	544
14.3.3. Управление средствами защиты	545
14.4. Аудит и мониторинг безопасности КИС	547
14.4.1. Аудит безопасности информационной системы	547
14.4.2. Мониторинг безопасности системы	551
Глава 15	
Обзор современных систем управления безопасностью	554
15.1. Продукты компании ЭЛВИС+ для управления средствами безопасности	554
15.2. Продукты компании Cisco для управления безопасностью сетей	556
15.3. Продукты компании IBM для управления средствами безопасности	562
15.4. Продукты компании Check Point Software Technologies для управления средствами безопасности	567
Список литературы	576
Предметный указатель	581