



ОГЛАВЛЕНИЕ

Предисловие	12
Введение	18
Часть I. Информационная безопасность	22
Глава 1. Анализ угроз информационной безопасности	23
1.1. Основные понятия информационной безопасности и защиты информации	23
1.1.1. Основные понятия информационной безопасности	24
1.1.2. Взаимодействие основных субъектов и объектов обеспечения информационной безопасности	25
1.1.3. Основные понятия защиты информации	29
1.2. Угрозы информационной безопасности	32
1.2.1. Анализ и классификация угроз информационной безопасности	32
1.2.2. Анализ угроз безопасности в компьютерных сетях	42
1.2.3. Криминализация атак на информационные системы	59
1.3. Появление кибероружия для ведения кибервойн	63
1.4. Прогноз киберугроз на 2013 год и далее	69
1.5. Меры и средства обеспечения информационной безопасности	73
Глава 2. Политика информационной безопасности	80
2.1. Основные понятия политики информационной безопасности	81

2.2. Структура политики информационной безопасности организации	88
2.2.1. Базовая политика безопасности	89
2.2.2. Специализированные политики безопасности	90
2.2.3. Процедуры безопасности	93
2.3. Разработка политики безопасности организации	96

Глава 3. Стандарты информационной безопасности

107

3.1. Роль стандартов информационной безопасности	107
3.2. Международные стандарты информационной безопасности	109
3.2.1. Стандарты ISO/IEC 17799:2002 (BS 7799:2000).....	110
3.2.2. Германский стандарт BSI	111
3.2.3. Международный стандарт ISO 15408 «Общие критерии безопасности информационных технологий»	112
3.2.4. Стандарты для беспроводных сетей	115
3.2.5. Стандарты информационной безопасности для Интернета.....	120
3.3. Отечественные стандарты безопасности информационных технологий	124

Часть II. Многоуровневая защита корпоративных информационных систем.....

129

Глава 4. Принципы многоуровневой защиты корпоративной информации

130

4.1. Корпоративная информационная система с традиционной структурой	130
4.2. Системы облачных вычислений.....	138
4.3. Многоуровневый подход к обеспечению информационной безопасности КИС.....	151
4.4. Подсистемы информационной безопасности традиционных КИС.....	154

Глава 5. Безопасность операционных систем	165
5.1. Проблемы обеспечения безопасности ОС	165
5.1.1. Угрозы безопасности операционной системы	165
5.1.2. Понятие защищенной операционной системы	168
5.2. Архитектура подсистемы защиты операционной системы	172
5.2.1. Основные функции подсистемы защиты операционной системы.....	172
5.2.2. Идентификация, аутентификация и авторизация субъектов доступа	173
5.2.3. Разграничение доступа к объектам операционной системы.....	175
5.2.4. Аудит	185
5.3. Обеспечение безопасности ОС Windows 7	188
5.3.1. Средства защиты общего характера.....	190
5.3.2. Защита данных от утечек и компрометации	194
5.3.3. Защита от вредоносного ПО	203
5.3.4. Безопасность Internet Explorer 8 и Internet Explorer 9	214
5.3.5. Совместимость приложений с Windows 7	224
5.3.6. Обеспечение безопасности работы в корпоративных сетях	228
Часть III. Технологии безопасности данных	230
Глава 6. Криптографическая защита информации	231
6.1. Основные понятия криптографической защиты информации	231
6.2. Симметричные криптосистемы шифрования.....	235
6.2.1. Алгоритмы шифрования DES и 3-DES	241
6.2.2. Стандарт шифрования ГОСТ 28147–89	245
6.2.3. Стандарт шифрования AES	250
6.2.4. Основные режимы работы блочного симметричного алгоритма	254
6.2.5. Особенности применения алгоритмов симметричного шифрования.....	259

6.3. Асимметричные криптосистемы шифрования	261
6.3.1. Алгоритм шифрования RSA	266
6.3.2. Асимметричные криптосистемы на базе эллиптических кривых	270
6.3.3. Алгоритм асимметричного шифрования ECES	273
6.4. Функции хэширования	274
6.5. Электронная цифровая подпись	278
6.5.1. Основные процедуры цифровой подписи	279
6.5.2. Алгоритм цифровой подписи DSA	282
6.5.3. Алгоритм цифровой подписи ECDSA	284
6.5.4. Алгоритм цифровой подписи ГОСТ Р 34.10–94.....	284
6.5.5. Отечественный стандарт цифровой подписи ГОСТ Р 34.10–2001	286
6.6. Управление криптоключами	291
6.6.1. Использование комбинированной криптосистемы	293
6.6.2. Метод распределения ключей Диффи–Хеллмана.....	297
6.6.3. Протокол вычисления ключа парной связи ECKEP	300
6.7. Инфраструктура управления открытыми ключами PKI.....	301
6.7.1. Принципы функционирования PKI	302
6.7.2. Логическая структура и компоненты PKI	306
Глава 7. Технологии аутентификации	315
7.1. Аутентификация, авторизация и администрирование действий пользователей.....	315
7.2. Методы аутентификации, использующие пароли	320
7.2.1. Аутентификация на основе многоразовых паролей	321
7.2.2. Аутентификация на основе одноразовых паролей.....	324
7.3. Строгая аутентификация	325
7.3.1. Основные понятия	325
7.3.2. Применение смарт-карт и USB-токенов	326
7.3.3. Криптографические протоколы строгой аутентификации	339
7.4. Биометрическая аутентификация пользователя	348

Часть IV. Базовые технологии сетевой безопасности	355
Глава 8. Протоколы защиты на канальном и сеансовом уровнях	356
8.1. Модель взаимодействия систем ISO/OSI и стек протоколов TCP/IP	356
8.1.1. Структура и функциональность стека протоколов TCP/IP	359
8.1.2. Особенности перехода на протокол IP v.6.....	365
8.2. Протоколы формирования защищенных каналов на канальном уровне	368
8.2.1. Протокол PPTP	369
8.2.2. Протоколы L2F и L2TP	372
8.3. Протоколы формирования защищенных каналов на сеансовом уровне.....	379
8.3.1. Протоколы SSL и TLS	379
8.3.2. Протокол SOCKS.....	384
8.4. Защита беспроводных сетей.....	388
Глава 9. Защита на сетевом уровне – протокол IPSec	394
9.1. Архитектура средств безопасности IPSec.....	395
9.2. Защита передаваемых данных с помощью протоколов АН и ESP	402
9.3. Протокол управления криптоключами IKE	414
9.4. Особенности реализации средств IPSec.....	419
Глава 10. Технологии межсетевого экранирования	424
10.1. Функции межсетевых экранов	424
10.1.1. Фильтрация трафика	426
10.1.2. Выполнение функций посредничества.....	427

10.1.3. Дополнительные возможности МЭ	430
10.2. Особенности функционирования межсетевых экранов на различных уровнях модели OSI	434
10.2.1. Экранирующий маршрутизатор	435
10.2.2. Шлюз сеансового уровня	437
10.2.3. Прикладной шлюз	440
10.2.4. Шлюз экспертного уровня	443
10.2.5. Варианты исполнения межсетевых экранов	444
10.3. Схемы сетевой защиты на базе межсетевых экранов	446
10.3.1. Формирование политики межсетевого взаимодействия	447
10.3.2. Основные схемы подключения межсетевых экранов	450
10.3.3. Персональные и распределенные сетевые экраны	456
10.3.4. Примеры современных межсетевых экранов	459
10.3.5. Тенденции развития межсетевых экранов	461

Глава 11. Технологии виртуальных защищенных сетей VPN

463

11.1. Концепция построения виртуальных защищенных сетей VPN	463
11.1.1. Основные понятия и функции сети VPN	464
11.1.2. Варианты построения виртуальных защищенных каналов	470
11.1.3. Обеспечение безопасности VPN	473
11.2. VPN-решения для построения защищенных сетей	475
11.2.1. Классификация VPN по рабочему уровню модели OSI	476
11.2.2. Классификация VPN по архитектуре технического решения	478
11.2.3. Основные виды технической реализации VPN	482
11.3. Современные VPN-продукты	485
11.3.1. Семейство VPN-продуктов компании «С-Терра СиЭсПи»	486
11.3.2. Устройства сетевой защиты Cisco ASA 5500 Series	494

Глава 12. Инфраструктура защиты на прикладном уровне	498
12.1. Управление идентификацией и доступом	499
12.1.1. Особенности управления доступом	501
12.1.2. Функционирование системы управления доступом.....	503
12.2. Организация защищенного удаленного доступа	507
12.2.1. Средства и протоколы аутентификации удаленных пользователей	509
12.2.2. Централизованный контроль удаленного доступа	526
12.3. Управление доступом по схеме однократного входа с авторизацией Single Sign On	532
12.3.1. Простая система однократного входа Single Sign-On	535
12.3.2. Системы однократного входа Web SSO	536
12.3.3. SSO-продукты уровня предприятия.....	539
12.4. Подсистема управления идентификацией и доступом IAM	542
Часть V. Технологии обнаружения и предотвращения вторжений	545
Глава 13. Обнаружение и предотвращение вторжений	546
13.1. Основные понятия.....	546
13.2. Обнаружение вторжений системой IPS	549
13.2.1. Обнаружение аномального поведения.....	549
13.2.2. Обнаружение злоупотреблений	550
13.3. Предотвращение вторжений в КИС.....	552
13.3.1. Предотвращение вторжений системного уровня	552
13.3.2. Предотвращение вторжений сетевого уровня.....	553
13.3.3. Защита от DDoS-атак	556
Глава 14. Защита от вредоносных программ и спама	564
14.1. Классификация вредоносных программ.....	564
14.2. Основы работы антивирусных программ	570

14.2.1. Сигнатурный анализ	570
14.2.2. Проактивные методы обнаружения.....	572
14.2.3. Дополнительные модули	576
14.2.4. Режимы работы антивирусов	578
14.2.5. Антивирусные комплексы	580
14.2.6. Дополнительные средства защиты	582
14.3. Облачная антивирусная технология	586
14.3.1. Предпосылки для создания «антивирусных облаков»	586
14.3.2. Как работают антивирусные облака.....	588
14.3.3. Преимущества облачной антивирусной защиты	591
14.3.4. Инновационная гибридная защита антивирусных продуктов Лаборатории Касперского	593
14.4. Защита персональных компьютеров и корпоративных систем от воздействия вредоносных программ и вирусов	595
14.4.1. Защита домашних персональных компьютеров от воздействия вредоносных программ и вирусов	595
14.4.2. Подсистема защиты корпоративной информации от вредоносных программ и вирусов	603
14.4.3. Серия продуктов Kaspersky Open Space Security для защиты корпоративных сетей от современных интернет-угроз.....	604

Часть VI. Управление информационной безопасностью

607

Глава 15. Управление средствами обеспечения информационной безопасности

608

15.1. Задачи управления информационной безопасностью	608
15.2. Архитектура управления информационной безопасностью КИС	616
15.2.1. Концепция глобального управления безопасностью GSM	616
15.2.2. Глобальная и локальные политики безопасности.....	618
15.3. Функционирование системы управления информационной безопасностью КИС	621
15.3.1. Назначение основных средств защиты	622

15.3.2. Защита ресурсов	624
15.3.3. Управление средствами защиты	625
15.4. Аудит и мониторинг безопасности КИС	627
15.4.1. Аудит безопасности информационной системы.....	628
15.4.2. Мониторинг безопасности системы.....	632
15.5. Обзор современных систем управления безопасностью	634
15.5.1. Продукты компании Cisco для управления безопасностью сетей.....	634
15.5.2. Продукты компании Check Point Software Technologies для управления средствами безопасности.....	641

Глава 16. Обеспечение безопасности облачных технологий

651

16.1. Основные проблемы безопасности облачной инфраструктуры.....	651
16.2. Средства защиты в виртуальных средах	654
16.3. Обеспечение безопасности физических, виртуальных и облачных сред на базе платформы Trend Micro Deep Security 9	657
16.4. Выбор провайдера облачных услуг	661

Приложение. Универсальная электронная карта.....

666

П1. Смарт-карты	666
П2. Что такое универсальная электронная карта (УЭК).....	669
П3. Внешний вид УЭК.....	670
П4. Услуги по карте УЭК.....	670
П5. Безопасность универсальной электронной карты	673
П6. Об инфраструктуре УЭК	675



ПРЕДИСЛОВИЕ

Быстрый рост глобальной сети Интернет и стремительное развитие информационных технологий привели к формированию информационной среды, оказывающей влияние на все сферы человеческой деятельности. К числу наиболее перспективных направлений применения современных информационных технологий относится бизнес.

Эффективность бизнеса компании напрямую зависит от качества и оперативности управления бизнес-процессами. Одним из главных инструментов управления бизнесом являются корпоративные информационные системы. Предприятия нового типа – это разветвленная сеть распределенных подразделений, филиалов и групп, взаимодействующих друг с другом. Распределенные корпоративные информационные системы становятся сегодня важнейшим средством производства современной компании, они позволяют преобразовать традиционные формы бизнеса в электронный бизнес.

Электронный бизнес использует глобальную сеть Интернет и корпоративные информационные системы для повышения эффективности всех сторон деловых отношений, включая продажи, маркетинг, платежи, финансовый анализ, поиск сотрудников, поддержку клиентов и партнерских отношений.

Важнейшим условием существования электронного бизнеса является информационная безопасность, под которой понимается защищенность информации и поддерживающей инфраструктуры от случайных и преднамеренных воздействий, которые могут нанести ущерб владельцам или пользователям информации. Ущерб от нарушения информационной безопасности может привести не только к крупным финансовым потерям, но и к полному закрытию компании.

Несмотря на интенсивное развитие компьютерных средств и информационных технологий, уязвимость современных информационных систем и компьютерных сетей, к сожалению, не уменьшается. Средства взлома компьютерных систем и хищения информации развиваются так же быстро, как и все высокотехнологичные компью-

терные отрасли. Поэтому проблемы обеспечения информационной безопасности привлекают пристальное внимание как специалистов в области компьютерных систем и сетей, так и многочисленных пользователей, включая компании, работающие в сфере электронного бизнеса.

Обеспечение информационной безопасности КИС является приоритетной задачей, поскольку от сохранения конфиденциальности, целостности и доступности корпоративных информационных ресурсов во многом зависит эффективность работы КИС. Задачу обеспечения безопасности корпоративных информационных систем традиционно решают путем построения системы информационной безопасности (СИБ). Определяющим требованием к СИБ является сохранение вложенных в построение КИС инвестиций. Другими словами, СИБ должна функционировать абсолютно прозрачно для уже существующих в КИС приложений и быть полностью совместимой с используемыми в КИС информационными технологиями. По мере роста и развития КИС система информационной безопасности должна легко масштабироваться без потери целостности и управляемости.

Без знания и квалифицированного применения современных информационных технологий, стандартов, протоколов и средств защиты информации невозможно достигнуть требуемого уровня информационной безопасности компьютерных систем и сетей.

Предлагаемая вниманию читателя книга посвящена систематизированному изложению и анализу современных проблем и методов обеспечения информационной безопасности, технологий и средств защиты информации в корпоративных информационных системах и компьютерных сетях.

Основное содержание книги, состоящее из шестнадцати глав, разбито на шесть логически связанных частей:

- часть I «Информационная безопасность»;
- часть II «Комплексное обеспечение безопасности информационных систем»;
- часть III «Технологии безопасности данных»;
- часть IV «Базовые технологии сетевой безопасности»;
- часть V «Технологии обнаружения и предотвращения вторжений»;
- часть VI «Управление информационной безопасностью».

Каждая из этих частей объединяет несколько глав, связанных общей темой. Книга содержит также предисловие, введение, список сокращений и список литературы.

Часть I «Информационная безопасность» включает следующие главы:

- главу 1 «Анализ угроз информационной безопасности»;
- главу 2 «Политика информационной безопасности»;
- главу 3 «Стандарты информационной безопасности».

В главе 1 формулируются основные понятия и определения информационной безопасности и анализируются угрозы информационной безопасности в корпоративных системах и сетях, рассматриваются тенденции развития ИТ-угроз и криминализации атак, комментируется появление кибероружия для ведения кибервойн, формулируются меры и средства обеспечения информационной безопасности.

В главе 2 определяются базовые понятия политики информационной безопасности и описываются основные виды политик и процедур безопасности в корпоративных информационных системах.

Глава 3 посвящена описанию стандартов информационной безопасности. Рассматриваются основные международные стандарты информационной безопасности. Даны краткие описания популярных стандартов информационной безопасности для Интернета. Анализируются отечественные стандарты безопасности информационных технологий.

Часть II «Комплексное обеспечение безопасности информационных систем» включает следующие главы:

- главу 4 «Принципы многоуровневой защиты корпоративной информации»;
- главу 5 «Обеспечение безопасности операционных систем».

Глава 4 посвящена рассмотрению принципов многоуровневой защиты информации в корпоративных информационных системах. Анализируются традиционные структуры корпоративных информационных систем и инфраструктура «облачных» вычислений. Описывается стратегия многоуровневой защиты КИС.

В главе 5 анализируются угрозы безопасности в операционных системах (ОС), вводится понятие защищенной ОС, описываются архитектура и основные функции подсистемы защиты ОС. Рассматриваются средства обеспечения безопасности операционной системы Windows 7.

Часть III «Технологии безопасности данных» включает следующие главы:

- главу 6 «Криптографическая защита информации»;
- главу 7 «Технологии аутентификации».

В главе 6 описываются такие криптографические методы защиты корпоративной информации, как симметричные и асимметричные криптосистемы шифрования, комбинированные криптосистемы, электронная цифровая подпись, функции хэширования и управление криптоключами. Рассматривается инфраструктура управления открытыми ключами PKI (Public Key Infrastructure).

Глава 7 посвящена рассмотрению аутентификации, авторизации и администрированию действий пользователя. Описываются методы аутентификации, использующие многоцветные и одноразовые пароли, сертификаты, смарт-карты и USB-токены, протоколы строгой аутентификации, биометрическую аутентификацию пользователей.

Часть IV «Базовые технологии сетевой безопасности» объединяет следующие главы:

- главу 8 «Протоколы защиты на канальном и сеансовом уровнях»;
- главу 9 «Защита сетевого уровня – протокол IPSec»;
- главу 10 «Технологии межсетевого экранирования»;
- главу 11 «Технологии виртуальных защищенных сетей VPN»;
- главу 12 «Инфраструктура защиты на прикладном уровне».

В главе 8 рассматриваются модель взаимодействия систем ISO/OSI и стек протоколов TCP/IP, обсуждаются проблемы построения защищенных виртуальных каналов на канальном и сеансовом уровнях модели взаимодействия открытых систем OSI. Рассматриваются особенности применения протоколов на канальном уровне PPTP, L2F и L2TP. Описывается применение протоколов SSL и SOCKS для построения защищенных каналов на сеансовом уровне. Рассматривается защита беспроводных сетей.

В главе 9 описываются архитектура стека протоколов IPSec, протокол аутентификации AH, протокол формирования защищенного пакета ESP, протокол управления криптоключами IKE. Приводятся сведения об алгоритмах аутентификации и шифрования, применяемых в стеке протоколов IPSec. Рассматриваются особенности реализации средств IPSec.

В главе 10 рассматриваются функции межсетевых экранов. Описываются схемы сетевой защиты на базе межсетевых экранов. Рассматривается применение персональных и распределенных сетевых экранов.

Глава 11 посвящена рассмотрению защищенных виртуальных сетей VPN (Virtual Private Network). Поясняется важное свойство сети VPN – туннелирование. Анализируются варианты построения

виртуальных защищенных каналов. Рассматриваются варианты архитектуры сетей VPN, приводятся основные виды технической реализации VPN.

В главе 12 рассматриваются управление идентификацией и доступом, организация защищенного удаленного доступа; анализируются протоколы аутентификации удаленных пользователей и системы централизованного контроля удаленного доступа. Описывается управление доступом по схеме однократного входа с авторизацией Single Sign-On. Рассматривается функционирование подсистемы управления идентификацией и доступом IAM.

Часть V «Технологии предотвращения вторжений и защиты от вредоносных программ» включает две главы:

- главу 13 «Обнаружение и предотвращение вторжений»;
- главу 14 «Защита от вредоносных программ и спама».

Глава 13 посвящена проблемам обнаружения и предотвращения вторжений. Рассматриваются методы обнаружения и предотвращения вторжений в корпоративные информационные системы, а также защита от распределенных атак. Описываются современные средства предотвращения вторжений, разработанные компанией Cisco Systems.

В главе 14 описываются технологии защиты от вредоносных программ и спама. Приводится классификация вредоносных программ. Рассматриваются сигнатурный анализ и проактивные методы обнаружения вирусов и других вредоносных программ. Описываются облачная антивирусная технология и инновационная гибридная защита от интернет-угроз, разработанные в Лаборатории Касперского. Приводятся сведения о современных антивирусных продуктах Лаборатории Касперского.

Часть VI «Управление информационной безопасностью» объединяет следующие главы:

- главу 15 «Управление средствами обеспечения информационной безопасности»;
- главу 16 «Обеспечение безопасности облачных вычислений».

В главе 15 рассматриваются методы управления средствами защиты корпоративной информации. Сформулированы задачи управления системой информационной безопасности масштаба предприятия. Анализируются варианты архитектуры управления средствами безопасности. Приводится обзор современных систем управления информационной безопасностью. Рассматриваются продукты ком-

паний Cisco Systems и Check Point для управления средствами безопасности.

В главе 16 анализируются основные проблемы безопасности облачной инфраструктуры. Рассматриваются средства защиты в виртуальных средах. Описывается процедура обеспечения безопасности облачных сред на базе платформы Trend Micro Deep Security 9. Приводятся рекомендации по выбору провайдера облачных услуг.

В конце книги дано приложение П1, посвященное универсальным электронным картам (УЭК). Такие карты планируется выдавать гражданам России с 2013 года для обеспечения им доступа к государственным, муниципальным и иным услугам, а также возможности оплаты оказанных услуг. УЭК создаются на базе смарт-карт (интеллектуальных электронных карт). В приложении рассмотрены принципы работы и возможности применения смарт-карт. Описываются преимущества и безопасность УЭК, приводятся сведения об инфраструктуре УЭК.

Материал книги базируется только на открытых публикациях в Интернете, отечественной и зарубежной печати. В основу книги положены материалы лекций, читаемых автором в Национальном исследовательском университете «МИЭТ». Автор заранее благодарен читателям, которые пришлют ему свои замечания и пожелания по адресу shanico@mail.ru.