Оглавление

Введение ... 3
Часть I. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ... 7
Глава 1. Основные понятия и принципы безопасности ... 8
Термины и определения ... 8
ИС как система контролируемого доступа к ресурсам ... 10
Концепция совместного использования ресурсов ... 10
Идентификация ... 12
Аутентификация ... 13
Авторизация ... 14
Модели информационной безопасности ... 14
Триада «Конфиденциальность, доступность, целостность» ... 15
Гексада Паркера и модель STRIDE ... 17
Уязвимость, угроза, атака, ущерб ... 19
Типы и примеры атак ... 23
Пассивные и активные атаки ... 23
Отказ в обслуживании ... 24
Внедрение вредоносных программ ... 26
Кража личности, фишинг ... 27
Сетевая разведка ... 29
Вопросы к главе 1 ... 31
Глава 2. Управление рисками ... 34
Анализ уязвимостей и угроз ... 36
Ущерб как мера риска ... 39
Управление рисками ... 42
Стандартные методики оценки рисков ... 46
Рекомендации NIST ... 46
Методика оценки рисков RiskWatch ... 51
Методика CRAMM ... 53
Методика OCTAVE ... 56
Определение профилей угрозы для ключевых активов ... 57
Идентификация уязвимостей инфраструктуры ... 61
Разработка стратегии безопасности и планов снижения рисков ... 62
Вопросы к главе 2 ... 66

Глава 3. Системный подход к управлению безопасностью 68
Иерахия средств защиты от информационных угроз 68
Законодательный уровень 70
Законы в области информационной безопасности 70
Стандарты в области информационной безопасности 70
Административный уровень. Политика безопасности 77
Определение политики безопасности 77
Верхний уровень политики безопасности 79
Средний уровень политики безопасности 81
Нижний уровень политики безопасности 82
Пример политики безопасности 83
Процедурный уровень 91
Процедуры управления персоналом 92
Процедуры реагирования на нарушения безопасности 94
Поддержка работоспособности предприятия 95
Физическая защита 99
Принципы защиты информационной системы 101
Подход сверху вниз 101
Защита как процесс 102
Эшелонированная защита 103
Сбалансированная защита 105
Компромиссы системы безопасности 107
Вопросы к главе 3 110
Часть II. БАЗОВЫЕ ТЕХНОЛОГИИ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ 113
Глава 4. Криптография 114
Основные термины и понятия 114
Симметричные алгоритмы шифрования 117
Алгоритм DES 118
Проблема распределения ключей 122
Асимметричные алгоритмы шифрования 127
Исторические предпосылки 127
Концепция шифрования с открытым ключом 129
Алгоритм RSA 132
Атаки на криптосистемы 135
Сравнение симметричных и асимметричных методов шифрования 137
Односторонние функции шифрования. Обеспечение целостности 138
Вопросы к главе 4 141
Глава 5. Технологии аутентификации 144
Факторы аутентификации человека 144

Многоразовые пароли ... 145
Электронные аутентификаторы ... 149
Биометрические аутентификаторы ... 151
Строгая аутентификация на основе многоразового пароля .. 156
Аутентификация пользователей сети средствами ОС ... 156
Аутентификация по протоколу CHAP ... 158
Аутентификация на основе одноразового пароля ... 160
Схема с использованием синхронизации ... 161
Схема с использованием слова-вызова ... 162
Аутентификация на основе сертификатов ... 164
Схема использования сертификатов ... 164
Сертифицирующие центры ... 167
Инфраструктура с открытыми ключами ... 169
Технология единого логического входа ... 171
Аутентификация информации. Электронная подпись ... 176
Электронная подпись ... 177
Аутентификация программных кодов ... 180
Вопросы к главе 5 ... 181
Глава 6. Технологии авторизации и управления доступом ... 184
Формы представления ограничений доступа ... 184
Правила ... 185
Матрица прав доступа ... 186
Списки доступа ... 187
Группы ... 188
Способы назначения прав ... 190
Дискреционный метод управления доступом ... 190
Мандатный метод управления доступом ... 195
Ролевое управление доступом ... 199
Иерархия ролей ... 200
Разделение обязанностей ... 203
Формальные модели безопасности управления доступом ... 204
Модели на основе конечного автомата ... 205
Модель Белла–ЛаПадулы ... 206
Модель Биба ... 208
Аутентификация и авторизация на основе справочной службы 209
Назначение справочной службы ... 209
Архитектура справочной службы ... 211
Вопросы к главе 6 ... 217
Глава 7. Технологии защищенного канала ... 220
Способы образования защищенного канала ... 220
Иерархия технологий защищенного канала ... 222
Туннелирование ... 224

Протокол IPSec ... 226
Распределение функций между протоколами IPSec ... 226
Безопасная ассоциация ... 227
Транспортный и туннельный режимы ... 229
Протокол AH ... 230
Протокол ESP ... 232
Базы данных SAD И SPD ... 234
Вопросы к главе 7 ... 236
Глава 8. Технологии анализа трафика и состояния сети ... 238
Аудит ... 238
Подотчетность ... 238
Задачи аудита ... 239
Файерволы ... 242
Сегментация сети ... 242
Фильтрация трафика ... 243
Определение файервола ... 247
Типы файерволов ... 251
Системы обнаружения вторжений ... 254
Типы систем обнаружения вторжений ... 254
Функциональная схема IDS ... 256
Правила обнаружения атак ... 257
Вопросы к главе 8 ... 258
Часть III. ЗАЩИТА ТРАНСПОРТНОЙ ИНФРАСТРУКТУРЫ СЕТИ ... 260
Глава 9. Транспортная инфраструктура и ее уязвимости ... 261
Протоколы и их уязвимости ... 261
Атаки на траспортную инфраструктуру ... 267
TCP-атаки ... 268
Затопление SYN-пакетами ... 268
Подделка TCP-сегмента ... 272
Повторение TCP-сегментов ... 273
Сброс TCP-соединения ... 273
ICMP-атаки ... 275
Перенаправление трафика ... 275
ICMP Smurf-атака ... 277
Ping смерти и ping-затопление ... 278
UDP-атаки ... 279
UDP-затопление ... 279
ICMP/UDP-затопление ... 280
UDP/echo/chargen-затопление ... 280
IP-атаки ... 281
Атака IP-опции ... 281

Атака IP-фрагментация ... 282
DNS-атаки ... 286
Организация DNS ... 286
Атаки на DNS ... 291
Методы защиты службы DNS ... 300
Сетевая разведка ... 301
Вопросы к главе 9 ... 306
Глава 10. Фильтрация и мониторинг трафика ... 309
Фильтрация трафика и файерволы ... 309
Типы фильтрации трафика ... 309
Файерволы на основе маршрутизаторов ... 310
Файерволы с функцией NAT ... 317
Мониторинг сети ... 323
Сетевые снифферы ... 323
Система мониторинга NetFlow ... 328
Типовые архитектуры сетей, защищаемых файерволами ... 333
Демилитаризованная зона ... 333
Обобщенная архитектура сети с защитой периметра и разделением внутренних зон ... 336
Вопросы к главе 10 ... 339
Глава 11. Безопасность маршрутизации на основе BGP ... 343
Принципы работы протокола маршрутизации BGP ... 343
Уязвимости и инциденты BGP ... 346
Защита BGP сессии между соседними маршрутизаторами ... 350
Защита маршрутизации BGP на основе данных региональных информационных центров Интернет ... 350
Сертификаты ресурсов и их использование для защиты BGP 353
Защита полного маршрута BGP с помощью сертификатов RPKI ... 356
Вопросы к главе 11 ... 356
Глава 12. Виртуальные частные сети ... 359
Определение виртуальной частной сети ... 359
Свойства частной сети, имитируемые VPN ... 359
Типы VPN ... 361
MPLS VPN ... 363
VPN на основе шифрования ... 365
Вопросы к главе 12 ... 368
Глава 13. Безопасность локальных беспроводных сетей ... 370
Уязвимости локальных беспроводных сетей ... 370
Две схемы организации беспроводной сети ... 371
Методы защиты локальных беспроводных сетей ... 372

Протокол WEP ... 373
Стандарт WPA2 ... 374
Беспроводные системы обнаружения вторжений ... 375
Вопросы к главе 13 ... 376
Глава 14. Безопасность облачных сервисов ... 377
Что такое «облачные сервисы» ... 377
Определение облачных вычислений ... 378
Свойства облачных вычислений ... 378
Технологии облачных вычислений ... 379
Модели сервисов облачных вычислений ... 380
Преимущества облачных сервисов ... 383
Проблемы безопасности облачных сервисов ... 386
Значимость облачных сервисов ... 390
Вопросы к главе 2 ... 390
Часть IV. БЕЗОПАСНОСТЬ СИСТЕМНОГО И ПРИКЛАДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ... 392
Глава 15. Архитектурная безопасность ОС ... 394
Сетевая операционная система и сетевые службы ... 394
Сетевые приложения ... 399
Ядро и вспомогательные модули ОС ... 401
Ядро в привилегированном режиме ... 402
Микроядерная архитектура ... 405
Концепция ... 405
Преимущества и недостатки микроядерной архитектуры ... 408
Вопросы к главе 15 ... 411
Глава 16. Аутентификация и управление доступом в ОС ... 413
Аутентификация пользователей в ОС ... 413
Управление доступом в ОС ... 415
Аутентификация пользователей в ОС Windows ... 416
Структура и протоколы системы аутентификации ОС Windows ... 416
Политика управления паролями ... 419
Аутентификация пользователей в ОС Unix ... 419
Обзор средств аутентификации Unix ... 419
Хранение паролей ... 421
Аутентификация по протоколу SSH ... 423
Контроль доступа в ОС Unix ... 426
Файловая модель доступа ... 426
Суперпользователь root ... 428
Контроль доступа в ОС семейства Windows ... 431
Разрешения на доступ к каталогам и файлам ... 434
Встроенные группы пользователей и их права ... 437

Система Kerberos ... 437
Первичная аутентификация ... 442
Получение разрешения на доступ к ресурсному серверу ... 444
Получение доступа к ресурсу ... 445
Достоинства и недостатки ... 446
Справочная служба Active Directory компании Microsoft ... 448
Домены Active Directory ... 448
Объекты ... 449
Глобальный каталог ... 450
Иерархия организационных единиц Active Directory ... 452
Иерархия доменов. Доверительные отношения ... 454
Пространство имен ... 457
Аутентификация в многодоменной структуре Active Directory ... 460
Вопросы к главе 16 ... 464
Глава 17. Аудит событий безопасности ... 467
Аудит событий в ОС Windows ... 467
Аудит событий безопасности в ОС Unix ... 471
Вопросы к главе 17 ... 475
Глава 18. Стандарты безопасности и сертификация ... 477
Оранжевая книга ... 477
Критерии сертификации вычислительных систем в области безопасности ... 478
Шесть базовых требований ... 480
Уровни и классы безопасности ... 482
Стандарт «Общие критерии» ... 490
Общая структура и цели ... 490
Функциональные требования безопасности ... 492
Требования доверия безопасности ... 493
Задание по безопасности и профили защиты ... 495
Вопросы к главе 18 ... 498
Глава 19. Уязвимости программного кода и вредоносные программы ... 500
Использование уязвимостей программных кодов ... 500
Уязвимости, связанные с нарушением защиты оперативной памяти ... 500
Уязвимости контроля вводимых данных ... 506
Скрытые коммуникации и скрытые каналы ... 509
Внедрение в компьютеры вредоносных программ ... 517
Троянские программы ... 517
Сетевые черви ... 518
Вирусы ... 522
Программные закладки ... 523

Антивирусные программы ... 525
Ботнет ... 527
Вопросы к главе 19 ... 528
Глава 20. Безопасность веб-сервиса ... 531
Организация веб-сервиса ... 532
Веб- и HTML-страницы ... 532
Адрес URL ... 533
Веб-клиент и веб-сервер ... 533
Протокол HTTP ... 536
Формат HTTP-сообщений ... 537
Динамические веб-страницы ... 539
Безопасность веб-браузера ... 541
Приватность и куки ... 541
Безопасность коммуникаций браузера и протокол HTTPS ... 546
Безопасность средств создания динамических страниц ... 551
Вопросы к главе 20 ... 552
Глава 21. Безопасность электронной почты ... 555
Организация почтового сервиса ... 555
Электронные сообщения ... 555
Протокол SMTP ... 558
Непосредственное взаимодействие клиента и сервера ... 559
Схема с выделенным почтовым сервером ... 560
Схема с двумя почтовыми серверами посредниками ... 562
Протоколы POP3 и IMAP ... 564
Угрозы и механизмы защиты почты ... 565
Угрозы почтовому сервису ... 565
Аутентификация отправителя ... 567
Шифрование содержимого письма ... 572
Защита метаданных пользователя ... 572
Атаки на компьютер с помощью почты ... 574
Спам ... 574
Атаки почтовых приложений ... 576
Вопросы к главе 21 ... 577
Глава 22. Системы защиты программного обеспечения ... 579
Файерволы прикладного уровня ... 579
Прокси-серверы ... 581
Функции прокси-сервера ... 584
Прокси-серверы прикладного уровня и уровня соединений ... 584
«Проксификация» приложений ... 585
Программные файерволы хоста ... 587
Вопросы к главе 22 ... 591

Приложение 1. Обзор нормативно-правовых актов РФ в области информационной безопасности ... 593
Федеральный закон «Об информации, информационных технологиях и о защите информации» ... 593
Уголовный кодекс РФ ... 597
Трудовой, гражданский кодексы и кодекс об Административных правонарушениях РФ ... 598
Федеральный закон «О национальной платежной системе» . 598
Законы и нормативно-правовые акты о персональных данных ... 599
Правовые акты об электронной подписи ... 602
Правовые акты о лицензировании отдельных видов деятельности ... 603
Приложение 2. Стеки коммуникационных протоколов ... 604
Многоуровневый подход ... 604
Модель OSI ... 606
Распределение функций между различными элементами сети 608
Стек протоколов TCP/IP ... 610
Типы адресов стека TCP/IP ... 612
Формат IP-адреса ... 613
Заголовок IP-пакета ... 614
Порты ... 615
Заголовки UDP- и TCP-сегментов ... 617
Сокеты ... 618
Протокол ICMP. Утилита ping ... 621
Ответы на контрольные вопросы ... 623
Предметный указатель ... 627
Литература ... 631