Оглавление

Предисловие 3
1. Структура и компоненты информационных и компьютерных систем. Понятие об уязвимостях ИС, КС и их компонентах. Объекты защиты ИС и КС 4
1.1. Понятия информационной системы и компьютерной системы 4
1.2. Понятия о защите информации и информационной безопасности. Компоненты ИС и КС. 6
1.3. Понятия об угрозе безопасности информации, уязвимостях ИС и КС, а также атаках на ИС и КС. Модель угроз безопасности информации 9
1.4. Уязвимости прикладного ПО и основные уязвимости ОС 11
1.5. Аппаратные уязвимости 13
1.6. Объекты защиты ИС и КС. Классификация средств защиты информации 14
Вопросы к главе 1 17
2. Программные и аппаратные механизмы защиты. Понятие об ущербе. Понятие о политике безопасности 18
2.1. Программные механизмы защиты. 18
2.1.1. Средства защиты от НСД. 19
2.1.2. Системы мониторинга сетей. 20
2.1.3. Анализатор протоколов Wireshark. 23
2.1.4. Антивирусные средства защиты информации. 23
2.1.5. Криптографические средства защиты информации 27
2.1.6. Идентификация и аутентификация пользователя 29

2.1.7. Межсетевые экраны. 30
2.2. Аппаратные средства защиты информации. 31
2.3. Выбор программных или аппаратных средств защиты 34
2.4. Понятие об ущербе. 35
2.5. Понятие о политике безопасности. 35
Вопросы к главе 2. 36
3. Технические устройства идентификации и аутентификации. Устройства iButton. Бесконтактные радиочастотные карты Proximity. Пластиковые карты 38
3.1. Методы аутентификации. 38
3.2. Подтверждение подлинности субъекта. 39
3.3. Факторы аутентифицирующей информации. 40
3.4. Парольные подсистемы идентификации и аутентификации 41
3.5. Технические устройства идентификации и аутентификации 43
3.5.1. Устройство iButton. 43
3.5.2. Бесконтактные радиочастотные карты Proximity 45
3.5.3. Пластиковые карты пассивного типа. 46
3.5.4. Пластиковые карты активного типа. 47
3.5.5. SMART-карты 47
3.5.6. Структура и принцип работы системы RFID идентификации 48
3.5.7. Near Field Communication 49
3.5.8. Rutoken 50
Вопросы к главе 3. 51
4. Идентификация и аутентификация пользователей с помощью биометрических устройств. Архитектура системы биометрической идентификации. 52
4.1. Области применения биометрических систем идентификации и аутентификации. 52
4.2. Архитектура системы биометрической идентификации 52
4.3. Коэффициенты оценки эффективности работы биометрических систем 54

4.4. Идентификация и аутентификация по статическим параметрам 55
4.4.1. Идентификация по отпечатку пальца..... 56
4.4.2. Идентификация по радужной оболочке глаза... 57
4.4.3. Идентификация по геометрии лица..... 57
4.5. Идентификация и аутентификация по динамическим параметрам 59
4.5.1. Кардио-биометрический метод идентификации. 59
4.5.2. Клавиатурный почерк..... 60
4.5.3. Голосовая аутентификация..... 61
4.6. Статистика применения биометрических методов аутентификации 62
4.7. Примеры считывающих биометрических устройств.. 62
4.8. Развитие систем биометрического доступа 63
4.9. Крупные поставщики биометрических устройств идентификации 64
4.10. Системы контроля доступа 65
4.10.1. Процесс регистрации пользователя в биометрической СКД 65
4.10.2. Типы СКД..... 66
4.10.3. Пример топологии автономной СКД..... 67
4.10.4. Пример топологии сетевой СКД..... 68
4.10.5. Пример СКД..... 68
4.11. Преимущества и недостатки биометрических систем идентификации и аутентификации..... 72
Вопросы к главе 4..... 73
5. Защита программного обеспечения от несанкционированного использования. 74
5.1. Меры по обеспечению защиты ПО..... 74
5.2. Системы защиты ПО от несанкционированного использования 77
5.3. Встроенные механизмы защиты 78
5.4. Пристыковочные механизмы защиты..... 80
5.5. Протектор Software Passport Armadillo 80
5.6. Утилита Sentinel LDK Envelope..... 86
5.7. Направления противодействия механизмам защиты ПО 87

5.7.1. IDA Pro ... 87
5.7.2. SoftICE ... 92
Вопросы к главе 5 ... 93
6. Цели и задачи изучения работы ПО. Изучение ПО методом обратного проектирования. Защита от исследования программного кода ... 94
6.1. Цели изучения работы ПО ... 94
6.2. Задачи изучения работы ПО ... 95
6.3. Обратное проектирование ... 96
6.4. Отладчики ... 98
6.5. Дизассемблеры ... 102
6.6. Редакторы кода ... 104
6.7. Мониторы событий ... 105
6.8. Защита ПО от исследований ... 107
6.9. Способы защиты от отладки ... 109
Вопросы к главе 6 ... 110
7. Защита компонентов ПО от отладки и дизассемблирования. Динамическая модификация программы. Защита от трассировки по прерываниям. Обфускация программного кода ... 111
7.1. Защита компонентов ПО от отладки и дизассемблирования ... 111
7.1.1. Шифрование ... 111
7.1.2. Динамические преобразования ... 114
7.1.3. Использование отладочных механизмов ... 114
7.1.4. Контрольные точки останова ... 115
7.2. Методы противодействия режиму отладки ... 117
7.2.1. POP SS ... 117
7.2.2. Переопределение указателя стека ... 118
7.2.3. Перехват прерывания int 1 ... 119
7.2.4. Манипуляция регистрами отладки DR0–DR7 ... 120
7.2.5. Использование недокументированных возможностей процессора ... 121
7.2.6. Использование особенностей конвейеризации ... 122
7.2.7. Самомодифицирующийся код ... 123
7.2.8. Добавление «мусора» ... 123

7.2.9. Скрытие команд передачи управления 124
7.2.10. Косвенная передача управления 124
7.2.11. Нестандартные способы передачи управления. 124
7.3. Обфускация 125
7.3.1. Виды обфускации 126
7.3.2. Эффективные методы обфускации 129
7.3.3. Группы обфускаторов 129
7.3.4. Достоинства и недостатки обфускаторов 130
Вопросы к главе 7 131
8. Классификация вирусов и средств атаки на защиту программного обеспечения. Защита от разрушающих программных воздействий вирусов 132
8.1. Разрушающие программные воздействия 132
8.2. Классификация РПВ 133
8.3. Среда обитания компьютерных вирусов 134
8.4. Классификация РПВ 136
8.5. Жизненный цикл вирусов 139
8.6. Инфицирование 140
8.7. Управление РПВ 140
8.8. Основные модели работы РПВ 141
8.9. Классификация средств атаки на защиту программного обеспечения 142
8.10. Защита от РПВ вирусов 154
Вопросы к главе 8 155
9. Методы борьбы с разрушающими программными воздействиями 156
9.1. Основные методы борьбы с разрушающими программными воздействиями 156
9.2. Контроль целостности 157
9.3. Изолированная программная среда 161
9.4. Блокираторы 163
9.5. Путевое тестирование 167
9.6. Классификация технологий антивирусной защиты .. 168
9.7. Методы борьбы с РПВ с помощью антивирусных программ 169
9.7.1. Сканирование 170

9.7.2. Эвристический анализ ... 172
9.7.3. Вакцинирование программ ... 173
Вопросы к главе 9 ... 173
10. Сертификация программного обеспечения по уровню контроля отсутствия недекларированных возможностей. Статический анализ исходных текстов программ ... 175
10.1. Недекларированные возможности ... 175
10.2. Сертификация ПО ... 176
10.3. Уровни доверия ... 177
10.4. Выявление уязвимостей и недекларированных возможностей средств ... 179
10.5. Исследование по выявлению уязвимостей и НДВ объекта оценки ... 181
10.5.1. Подготовка к проведению исследования ... 182
10.5.2. Проведение исследования ... 183
Вопросы к главе 10 ... 189
11. Объекты защиты на уровне программного кода. Понятие о защищенном коде. Приемы защищенного программирования. Перечень типовых дефектов ПО ... 190
11.1. Анализ программного кода на уязвимости в процессах жизненного цикла ПО ... 190
11.2. Тестирование ПО (фаззинг) ... 193
11.3. Понятие о защищенном коде ... 196
11.4. Безопасное программирование ... 197
11.5. Наступательное программирование ... 198
11.6. Интеллектуальное повторное использование исходного кода ... 199
11.7. Приемы защищенного программирования ... 199
11.8. Перечень типовых уязвимостей и дефектов ПО ... 203
11.9. Примеры использования уязвимостей ПО ... 207
11.10. Формы проявления программных дефектов ... 207
11.11. Виды возникающих ошибок ... 208
11.12. Банки данных угроз и уязвимостей ... 209
Вопросы к главе 11 ... 213

12. Базы данных как объект защиты. Серверы и системы управления базами данных. Объекты защиты БД 214
12.1. Виды SQL-серверов 214
12.2. Основные функции и классификация СУБД 215
12.3. Защита СУБД от НСД, объекты защиты СУБД 218
12.4. Угрозы базам данных, классификация причин нарушения работы БД 220
12.5. Категории пользователей БД 220
12.6. Принципы построения системы защиты СУБД, основные методы защиты баз данных 221
12.7. Дополнительные средства защиты баз данных 223
12.8. Оценка уязвимостей MSSQL server 224
12.9. Привилегии в СУБД 225
12.10. Разграничение прав доступа MSSQL server 228
12.11. Шифрование в СУБД MSSQL Server 230
12.12. Резервное копирование системных баз данных 233
12.13. Средство контроля значений данных в соответствии с типами 233
12.14. Хранимые процедуры (MSSQL) 234
12.15. Уровни блокировок в СУБД 235
12.16. Создание сертификата в MSSQL Server 237
12.17. SQL-инъекция: пример реализации и методы защиты 237
Вопросы к главе 12 238
13. Классификация угроз безопасности операционной системы. Типовые атаки на ОС 240
13.1. Доверенная вычислительная база 240
13.2. Понятие защищенной операционной системы 240
13.3. Угрозы безопасности ОС и их классификация 242
13.4. Типовые атаки на операционные системы 249
13.4.1. Сканирование файловой системы 250
13.4.2. Хищение ключевой информации 251
13.4.3. Сборка мусора 252
13.4.4. Программные закладки 254
13.4.5. Жадные программы 255
Вопросы к главе 13 256

14. Понятие защищенной операционной системы. Подходы к построению защищенных ОС. Аудит безопасности 257
14.1. Понятие защищенной операционной системы 257
14.2. Подходы к построению защищенных ОС 257
14.3. Разграничение доступа к домашнему каталогу Linux 259
14.4. Изолированная среда выполнения Linux 260
14.5. Административные меры защиты 260
14.6. Адекватная политика безопасности 261
14.7. Этапы определения и поддержания адекватной политики 262
14.8. Аудит безопасности 263
14.8.1. Политика аудита в ОС Windows 264
14.8.2. Настройка системных списков управления доступом SACL 266
14.8.3. Регистрация событий в Linux 267
14.9. IRP-система штатными средствами ОС Windows 270
Вопросы к главе 14 272
15. Аппаратное обеспечение средств защиты ОС. Защищаемые объекты КС. Методы и средства контроля и ограничения доступа к объектам КС 273
15.1. Аппаратное обеспечение средств защиты ОС 273
15.1.1. Управление оперативной памятью 273
15.1.2. Управление планированием задач 274
15.1.3. Обеспечение корректности совместного доступа к объектам 276
15.1.4. Предотвращение тупиковых ситуаций 276
15.2. Защищаемые объекты КС 277
15.3. Методы и средства контроля и ограничения доступа к объектам КС 279
15.4. Расширение функционала ОС по работе с привилегиями 281
Вопросы к главе 15 281
16. Достоинства и недостатки программных и аппаратных средств защиты. Особенности использования программно-аппаратных средств для защиты информационных ресурсов организации 282

16.1. Защитные меры 282
16.2. Использование программно-аппаратных средств для защиты информационных ресурсов организации 284
16.2.1. Системы управления доступом 284
16.2.2. Системы управления правами на информацию 285
16.2.3. Система управления событиями информационной безопасности 287
16.2.4. Системы обнаружения и предотвращения вторжений 295
16.2.5. Система предотвращения потери данных 299
16.2.6. Поведенческий анализ пользователей и сущностей 303
16.2.7. Центр оперативного управления информационной безопасностью 309
16.2.8. Платформа для управления разведывательными данными об угрозах 309
16.2.9. Платформа реагирования на инциденты 311
16.2.10. Оркестрация, автоматизация и реагирование в области информационной безопасности 311
Вопросы к главе 16 313
Литература 314