Высшее образование

Учебник

В. В. Платонов

# ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

2-е издание

БАКАЛАВРИАТ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ACADEMIA

Высшее образование
БАКАЛАВРИАТ

В. В. ПЛАТОНОВ

# ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

## УЧЕБНИК

*Для студентов учреждений высшего профессионального образования, обучающихся по направлению подготовки «Информационная безопасность»*

2-е издание, стереотипное

ACADEMIA

Москва
Издательский центр «Академия»
2014

# ОГЛАВЛЕНИЕ

Предисловие ..... 3

**Глава 1. Обеспечение безопасности межсетевого взаимодействия** ..... 6

1.1. Основы сетевого и межсетевого взаимодействия ..... 7
1.2. Информационная безопасность ..... 13
1.3. Политика безопасности ..... 16
1.3.1. Шаблоны политик безопасности ..... 18
1.3.2. Сетевая политика безопасности ..... 19
1.3.3. Эшелонированная оборона ..... 22
1.4. Управление рисками ..... 24
1.4.1. Основные понятия ..... 24
1.4.2. Процесс оценки рисков ..... 26
1.4.3. Уменьшение рисков ..... 32
1.4.4. Пример содержания результирующего отчета ..... 38
1.5. Аудит информационной безопасности ..... 39
1.6. Механизмы и службы защиты ..... 41

**Глава 2. Вредоносные программы** ..... 43

2.1. Компьютерные вирусы ..... 45
2.1.1. Файловые вирусы ..... 48
2.1.2. Макровирусы ..... 50
2.1.3. Загрузочные вирусы ..... 51
2.1.4. Методы защиты от обнаружения ..... 52
2.2. Троянские кони ..... 54
2.3. Сетевые черви ..... 57
2.5. Потайные ходы ..... 60
2.6. Руткиты ..... 61
2.5.1. Руткиты уровня пользователя ..... 61
2.5.2. Руткиты уровня ядра ..... 62
2.6. Вредоносные программы для мобильных устройств ..... 63
2.7. Прочие вредоносные программы ..... 66
2.8. Наименование вирусов ..... 68
2.9. Элементы защиты от вредоносного программного обеспечения ..... 69
2.10. Технология Black и Whitelisting ..... 73

**Глава 3. Удаленные сетевые атаки** ..... 78

3.1. Сетевые атаки ..... 79
3.2. Обобщенный сценарий атаки ..... 82

3.2.1. Пассивная разведка ... 83
3.2.2. Активная разведка ... 85
3.2.3. Выбор эксплойта ... 85
3.2.4. Взлом целевой системы ... 86
3.2.5. Загрузка «полезного груза» ... 87
3.2.6. Сокрытие следов взлома ... 87
3.3. Атаки «отказ в обслуживании» ... 88
3.3.1. Распределенные атаки «отказ в обслуживании» ... 91
3.3.2. Распределенные рефлекторные атаки «отказ в обслуживании» ... 94
3.3.3. Таксономия атак «отказ в обслуживании» и защитных механизмов ... 96
3.4. Примеры атак ... 98
3.4.1. Атаки на протокол IP ... 100
3.4.2. Атаки на протокол ICMP ... 101
3.4.3. Атаки на протокол UDP ... 101
3.4.4 Атаки на протокол TCP ... 102
3.4.5. Генераторы атак ... 103
3.4.6. Атака К.Митника ... 104
3.5. Классификации удаленных атак ... 108
3.5.1. Списки терминов ... 108
3.5.2. Списки категорий ... 109
3.5.3. Матричные схемы ... 110
3.5.4. Процессы ... 110
3.5.5. Классификация Ховарда ... 112
2.4.6. Построение онтологии сетевых атак ... 116
3.6. Оценивание степени серьезности атак ... 119

**Глава 4. Технологии межсетевых экранов** ... 123

4.1. Развитие технологий межсетевого экранирования ... 123
4.1.1. Фильтрация пакетов ... 125
4.1.2. Межсетевые экраны уровня соединения ... 130
4.1.3. Межсетевые экраны прикладного уровня ... 133
3.1.4. Межсетевые экраны с динамической фильтрацией пакетов ... 136
4.1.5. Межсетевые экраны инспекции состояний ... 139
4.1.6. Межсетевые экраны уровня ядра ... 147
4.1.7. Персональные межсетевые экраны ... 151
4.1.8. Распределенные межсетевые экраны ... 154
4.1.9. Межсетевые экраны Web-приложений ... 154
4.1.10. Новое поколение межсетевых экранов ... 158
4.2. Обход межсетевых экранов ... 161
4.2.1. Постепенный подход ... 161
4.2.2. Туннелирование ... 162
4.3. Требования и показатели защищенности межсетевых экранов ... 165

4.4. Тестирование межсетевых экранов ... 167
4.5. Отечественный межсетевой экран СППТ-2 ... 171

**Глава 5. Системы обнаружения атак и вторжений** ... 176
5.1. Модели систем обнаружения вторжений ... 178
5.1.1. Модель Д. Деннинг ... 179
5.1.2. Модель CIDF ... 185
5.2. Классификация систем обнаружения вторжений ... 186
5.3. Обнаружение сигнатур ... 189
5.4. Система обнаружения вторжений Snort ... 195
5.4.1. Декодер пакетов ... 197
5.4.2. Препроцессоры ... 197
5.4.3. Препроцессоры сборки пакетов ... 198
5.4.4. Препроцессоры нормализации протоколов ... 202
5.4.5. Препроцессоры обнаружения аномалий ... 204
5.4.6. Процессор обнаружения ... 204
5.4.7. Модули вывода ... 205
5.4.8. Правила Snort ... 206
5.4.9. Примеры правил ... 210
5.5. Обнаружение аномалий ... 211
5.5.1. Методы Data Mining ... 212
5.5.2. Методы технологии мобильных агентов ... 214
5.5.3. Методы построения иммунных систем ... 218
5.5.4. Применение генетических алгоритмов ... 219
5.5.5. Применение нейронных сетей ... 226
5.5.6. Языки описания атак ... 232
5.6. Другие методы обнаружения вторжений ... 234
5.6.1. Системы анализа защищенности ... 235
5.6.2. Системы анализа целостности ... 236
5.6.3. Вспомогательные средства обнаружения ... 239
5.7. Методы обхода систем обнаружения вторжений ... 243
5.7.1. Методы обхода сетевых систем обнаружения вторжений ... 245
5.7.2. Методы обхода хостовых систем обнаружения вторжений ... 246
5.7.3. Динамические методы обхода ... 250
5.8. Тестирование систем обнаружения вторжений ... 252
5.8.1. Тестирование коммерческих систем ... 253
5.8.2. Тестирование исследовательских прототипов ... 257
5.8.3. Методы формирования тестовых наборов ... 258
5.8.4. Матрица несоответствий ... 259
5.9. Системы предупреждения вторжений ... 261

**Глава 6. Виртуальные частные сети** ... 267
5.1. Туннелирование ... 268
6.2. Протоколы VPN канального уровня ... 271
6.3. Протокол IPSec ... 272

6.3.1. Ассоциация обеспечения безопасности ..... 273
6.3.2. Туннельный и транспортный режимы протокола IPSec ... 275
6.3.3. Протокол обмена интернет-ключами ..... 275
6.3.4. Протокол аутентификации заголовка ..... 286
6.3.5. Протокол безопасной инкапсуляции содержимого пакета ..... 288
6.3.6. Пример применения протокола IKE ..... 290
6.3.7. Совместное использование протоколов ESP и AH ..... 292
6.3.8. Основные типы защищенных связей ..... 293
6.4. Протоколы VPN транспортного уровня ..... 296
6.5. Цифровые сертификаты ..... 298
6.6. Примеры отечественного построения VPN ..... 300
6.7. Инфраструктура PKI ..... 302

Приложения ..... 310
Список литературы ..... 326