ACADEMIA

учебное пособие



бакалавриат

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ

ОГЛАВЛЕНИЕ

Предисловие ... 3
Принятые сокращения ... 9
Глава 1. Безопасность информации в автоматизированных системах ... 10
1.1. Операционные системы и процессы обработки информации систем ... 10
1.2. Общие сведения об автоматизированных системах ... 13
1.3. Информация в автоматизированных системах и ее защищаемые свойства ... 15
1.4. Нарушитель в автоматизированных системах ... 17
1.5. Формальные виды политик безопасности и модели систем разграничения доступа ... 20
1.5.1. Дискреционная политика разграничения доступа ... 20
1.5.2. Мандатные политики разграничения доступа ... 24
1.5.3. Ролевая политика разграничения доступа ... 31
Глава 2. Защищенный режим процессоров общего назначения ... 34
2.1. Общие сведения ... 34
2.2. Страничный способ работы с памятью. Виртуальные и физические страницы ... 37
2.3. Жизненный цикл виртуальной страницы памяти ... 43
2.4. Работа с периферийными устройствами и режим DMA ... 46
2.5. Требования скорости передачи и безопасность информации. Случай FireWire ... 48
Глава 3. Доверенная загрузка операционной системы и организация замкнутой программной среды ... 52
3.1. Запуск компьютера и подготовка загрузки операционной системы ... 52
3.2. Эксперимент. Загрузка сторонней операционной системы как один из методов обхода механизмов защиты операционной системы ... 57
3.3. Особенности стартовой инициализации оборудования UEFI BIOS и Secure Boot ... 61
3.4. Стартовый и периодический контроль целостности ... 65
3.5. Организация замкнутой программной среды ... 67
3.5.1. Общие сведения ... 67
3.5.2. Методы организации замкнутой программной среды ... 68
3.5.3. Требования к программам, образующим замкнутую программную среду ... 69

Глава 4. Обеспечение безопасности в операционных системах семейства ОС Windows ... 74
4.1. Обзор архитектуры системы ... 74
4.2. Процессы, потоки и волокна ... 80
4.2.1. Общие сведения ... 80
4.2.2. Подсистема управления памятью ... 83
4.2.3. Подсистема ввода-вывода ... 83
4.2.4. Сетевая архитектура ... 87
4.3. Основные нововведения Windows 10 по сравнению с Windows 7 ... 89
4.4. Системные компоненты безопасности ... 93
4.5. Подсистема идентификации и аутентификации ... 96
4.6. Подсистема разграничения доступа ... 104
4.6.1. Общие сведения ... 104
4.6.2. Дискреционный контроль доступа ... 104
4.6.3. Заимствование прав ... 106
4.6.4. Аудит безопасности ... 107
4.6.5. Графический редактор списков управления доступом ... 108
4.6.6. Управление учетными записями пользователей ... 108
4.6.7. Изоляция привилегий пользовательского интерфейса ... 111
4.6.8. Уровни целостности ... 111
4.7. Средства обеспечения сетевой безопасности ... 113
4.7.1. Брандмауэр Защитника Windows ... 113
4.7.2. Защита сети ... 114
4.8. Подсистема организации ЗПС ... 115
4.8.1. Подсистемы Windows Defender ... 115
4.8.2. Средство удаления вредоносных программ ... 116
4.8.3. Технология AppLocker ... 116
4.8.4. Контроль целостности кода и блокировка неподписанных драйверов ... 117
4.8.5. Контроль модификации ядра ... 118
4.8.6. Приложение PowerShell ... 118
4.8.7. Рандомизация адресного пространства ... 119
4.9. Шифрование хранимой информации ... 122
4.10. Средства шифрования сетевого трафика ... 133
4.10.1. IPSec ... 133
4.10.2. Удаленный сетевой доступ ... 134
4.10.3. Подсистема регистрации и протоколирования ... 136
4.11. Защита ресурсов Windows ... 141
Глава 5. Обеспечение безопасности в операционных системах семейства Linux ... 144
5.1. Концепция защиты информации в Linux ... 144
5.1.1. Общая структура операционной системы на базе ядра Linux ... 144
5.1.2. Системные компоненты безопасности ... 147
5.1.3. О модульности решений по безопасности в Linux ... 147
5.2. Модули аутентификации ... 148
5.2.1. Общие сведения ... 148
5.2.2. Решения по хранению учетных данных ... 148
5.2.3. Модули PAM ... 150

5.3. Модули аудита ... 151
5.4. Модули контроля целостности ... 156
5.5. Модули прозрачного шифрования ... 156
5.6. Права доступа процессов ... 157
5.7. Контроль доступа в файловой системе ... 158
5.7.1. Общие принципы ... 158
5.7.2. Права на доступ к файлу и директории ... 158
5.7.3. Списки контроля доступа в Linux ... 159
5.7.4. Команды управления доступом к файлам ... 160
5.8. Расширенный контроль доступа ... 168
5.8.1. Механизм SELinux ... 168
5.8.2. Механизм Smack ... 170
5.8.3. Механизм AppArmor ... 170
5.8.4. Механизм TOMOYO ... 171
5.8.5. Механизм parsec ... 171
5.8.6. Механизм elmac ... 172

Глава 6. Защита информации с использованием технологий виртуализации ... 174
6.1. Применение механизмов виртуализации для защиты информации ... 174
6.2. Общие сведения об аппаратной поддержке виртуализации в процессорах семейства Intel x86 ... 177
6.3. Вопросы реализации виртуальных устройств в составе гипервизоров ... 188
6.4. Применение виртуализации для прозрачного шифрования хранимой и передаваемой информации. Пример BitVisor ... 194
6.5. Безопасность на основе виртуализации в Windows 10 ... 197
6.6. Реальные потоки информации и информационные потоки в моделях разграничения доступа, описывающих работу процессора для программиста ... 200

Глава 7. Внедрение дополнительных средств защиты в операционные системы ... 209
7.1. Общие сведения ... 209
7.2. Методы внедрения дополнительных механизмов защиты ... 211
7.2.1. Операционная система с открытым исходным кодом ... 211
7.2.2. Штатные интерфейсы для установки дополнительных средств защиты: Crypto API и CNG SDK в Windows ... 217
7.2.3. Послойная система организации обработки запросов в современных операционных системах ... 222
7.2.4. Установка детуров и патчей на бинарные модули ... 231
7.3. Антивирусные программы ... 236
7.4. Межсетевые экраны ... 243

Заключение ... 249
Список литературы ... 251