ЧАСТЬ 1. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Глава 15. Архитектурная безопасность ОС

- Сетевая операционная система и сетевые службы
- Сетевые приложения
- Ядро и вспомогательные модули ОС
- Ядро в привилегированном режиме
- Микроядерная архитектура
  - Концепция
  - Преимущества и недостатки микроядерной архитектуры

Глава 16. Аутентификация и управление доступом в ОС

- аутентификация пользователей в ОС
- Управление доступом в ОС
- Аутентификация пользователей в ОС Windows
- Аутентификация пользователей ОС Unix
  - Обзор средств аутентификации в Unix
  - Хранение паролей
  - Аутентификация по протоколу SSH
- Контроль доступа в ОС Unix
  - Файловая модель доступа
  - Суперпользователь root
- Контроль доступа в ОС семейства Windows
  - Общая характеристика
  - Разрешения на доступ к каталогам и файлам
  - Встроенные группы пользователей и их права
- Система Kerberos
  - Первичная аутентификация
  - Получение разрешения на доступ к ресурсному серверу
  - Получение доступа к ресурсу
  - Достоинства и недостатки
- Справочная служба Active Directory компании Microsoft
  - Домены Active Directory
  - Объекты
  - Глобальный каталог
  - Иерархия организационных единиц Active Directory
  - Иерархия доменов. Доверительные отношения
  - Пространство имен
  - Аутентификация в многодоменной структуре Active Directory

Глава 17 Аудит событий безопасности

- Аудит событий в ОС Windows
  - Типы аудита
  - Утилита Event Viewer

Аудит событий безопасности в ОС Unix

Журналы событий

Сервис syslog

Аудит логических входов

Глава 18. Стандарты безопасности и сертификация

Оранжевая книга

Критерии сертификации вычислительных систем в области безопасности

Шесть базовых требований

Уровни и классы безопасности

Стандарт «общие критерии»

Общая структура и цели

Функциональные требования безопасности

Требования доверия безопасности

Задание по безопасности и профили защиты

Глава 19. Уязвимости программного кода и вредоносные программы

Использование уязвимостей программных кодов

Уязвимости, связанные с нарушением защиты оперативной памяти

Уязвимости контроля вводимых данных

Скрытые коммуникации и скрытые каналы

Внедрение в компьютеры вредоносных программ

Троянские программы

Сетевые черви

Вирусы

Программные закладки

Антивирусные программы

Ботнет

Глава 20 Безопасность веб-сервиса

Организация веб-сервиса

Веб- и HTML-страницы

Адрес URL

Веб-клиент и веб-сервер

Протокол HTTP

Формат HTTP-сообщений

Динамические веб-страницы

Безопасность веб-браузера

Приватность и куки

Безопасность коммуникаций браузера и протокол HTTPS

Безопасность средств создания динамических страниц

Глава 21 Безопасность электронной почты

- Организация почтового сервиса
  - Электронные сообщения
  - Протокол SMTP
  - Непосредственное взаимодействие клиента и сервера
  - Схема с выделенным почтовым сервером
  - Схема с двумя почтовыми серверами посредниками
  - Протоколы POP3 и IMAP
- Угрозы и механизмы защиты почты
  - Угрозы почтовому сервису
  - Аутентификация отправителя
  - Шифрование содержимого письма
  - Защита мета-данныех пользователя
- Атаки на компьютер с помощью почты
  - Спам
  - Атаки почтовых приложений

Глава 22. Системы защиты программного обеспечения

- Файерволы прикладного уровня
- Прокси-серверы
  - Функции прокси-сервера
  - Прокси-серверы прикладного уровня и уровня соединений
  - «Проксификация» приложений
- Программные файерволы хоста

ПРИЛОЖЕНИЕ 1. ОБЗОР НОРМАТИВНО-ПРАВОВЫХ АКТОВ РФ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Федеральный закон «Об информации, информационных технологиях и о защите информации» .

Уголовный кодекс РФ

Трудовой, гражданский, уголовный кодексы и кодекс об Административных Правонарушениях РФ

Федеральный закон «О национальной платежной системе»

Законы и нормативно-правовые акты о персональных данных

Правовые акты об электронной подписи

Правовые акты о лицензировании отдельных видов деятельности

ПРИЛОЖЕНИЕ 2. СТЕКИ КОММУНИКАЦИОННЫХ ПРОТОКОЛОВ

Многоуровневый подход

Модель OSI

Стек протоколов TCP/IP

- Типы адресов стека TCP/IP
- Формат IP-адреса
- Заголовок IP-пакета
- Порты
- Заголовки UDP- и TCP-сегментов
- Сокеты
- Протокол ICMP. Утилита ping