

ЧАСТЬ 1. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Глава 1. Основные понятия и принципы безопасности

Термины и определения

ИС как система контролируемого доступа к ресурсам

Концепция совместного использования ресурсов

Идентификация

Аутентификация

Авторизация

Модели информационной безопасности

Триада « Конфиденциальность, доступность, целостность»

Гексада Паркера и модель STRIDE

Уязвимость, угроза, атака, ущерб

Типы и примеры атак

Пассивные и активные атаки

Отказ в обслуживании

Внедрение вредоносных программ

Кража личности, фишинг

Сетевая разведка

Вопросы и упражнения

Глава 2. Управление рисками

Анализ уязвимостей и угроз

Ущерб как мера риска

Управление рисками

Стандартные методики оценки рисков

Рекомендации NIST

Методика оценки рисков RiskWatch

Методика CRAMM

Методика OCTAVE

Определение профилей угрозы для ключевых активов

Идентификация уязвимостей инфраструктуры

Разработка стратегии безопасности и планов снижения рисков

Вопросы и упражнения

Глава 3. Системный подход к управлению безопасностью

Иерархия средств защиты от информационных угроз

Законодательный уровень

Законы в области информационной безопасности

Стандарты в области информационной безопасности

Административный уровень. Политика безопасности

Определение политики безопасности
Верхний уровень политики безопасности
Средний уровень политики безопасности
Нижний уровень политики безопасности
Пример политики безопасности

Процедурный уровень
Процедуры управления персоналом
Процедуры реагирования на нарушения безопасности
Поддержка работоспособности предприятия
Физическая защита

Принципы защиты информационной системы
Подход сверху вниз
Защита как процесс
Эшелонированная защита
Сбалансированная защита
Компромиссы системы безопасности

Вопросы и упражнения

ЧАСТЬ 2. БАЗОВЫЕ ТЕХНОЛОГИИ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Глава 4. Криптография

Основные термины и понятия
Симметричные алгоритмы шифрования
Алгоритм DES
Проблема распределения ключей
Асимметричные алгоритмы шифрования
Исторические предпосылки
Концепция шифрования с открытым ключом

Алгоритм RSA
Атаки на криптосистемы
Сравнение симметричных и асимметричных методов шифрования
Односторонние функции шифрования. Обеспечение целостности

Глава 5. Технологии аутентификации

Факторы аутентификации человека
Многоразовые пароли
Электронные аутентификаторы
Биометрические аутентификаторы

Строгая аутентификация на основе многоразового пароля
Аутентификация пользователей сети средствами ОС
аутентификация по протоколу SHAP

Аутентификация на основе одноразового пароля

Схема с использованием синхронизации

Схема с использованием слова-вызова

Аутентификация на основе сертификатов

Схема использования сертификатов

Сертифицирующие центры

Инфраструктура с открытыми ключами

Технология единого логического входа

Аутентификация информации. Электронная подпись

Электронная подпись

Аутентификация программных кодов

Глава 6. Технологии авторизации и управления доступом

Формы представления ограничений доступа

Правила

Матрица прав доступа

Списки доступа

Группы

Способы назначения прав

Дискреционный метод управления доступом

Мандатный метод управления доступом

Ролевое управление доступом

Иерархия ролей

Разделение обязанностей

Формальные модели безопасности управления доступом

Модели на основе конечного автомата

Модель Белла-ЛаПадулы

Модель Биба

Аутентификация и авторизация на основе справочной службы

Назначение справочной службы

Архитектура справочной службы

Глава 7. Технологии защищенного канала

Способы образования защищенного канала

Иерархия технологий защищенного канала

Туннелирование

Протокол IPSec

Распределение функций между протоколами IPSec

Безопасная ассоциация

Транспортный и туннельный режимы

Протокол AH

Протокол ESP

Глава 8. Технологии анализа трафика и состояния сети

Аудит

Подотчетность

Задачи аудита

Файерволы

Сегментация сети

Фильтрация трафика

Определение файервола

Типы файерволов

Системы обнаружения вторжений

Типы систем обнаружения вторжений

Функциональная схема IDS

Правила обнаружения атак

ЧАСТЬ 3. ЗАЩИТА ТРАНСПОРТНОЙ ИНФРАСТРУКТУРЫ СЕТИ

Глава 9. Транспортная инфраструктура и ее уязвимости

Протоколы и их уязвимости

Атаки на транспортную инфраструктуру

TCP-атаки

Затопление SYN пакетами

Подделка TCP сегмента

Повторение TCP сегментов

Сброс TCP соединения

ICMP-атаки

Перенаправление трафика

ICMP Smurf-атака

Ping смерти и ping-затопление

UDP-атаки

UDP-затопление

Отраженное UDP-затопление

IP-атаки

Атака IP-опции

Атака IP-фрагментация

DNS-атаки

Организация DNS

Атаки на DNS

Методы защиты службы DNS

Сетевая разведка

Глава 10. Фильтрация и мониторинг трафика

Фильтрация трафика и фаерволы

Типы фильтрации трафика

Фаерволы на основе маршрутизаторов

NAT- фаерволы

Мониторинг сети

Сетевые снифферы

Система мониторинга NetFlow

Типовые архитектуры сетей, защищаемых фаерволами

Демилитаризованная зона

Обобщенная архитектура сети с защитой периметра и разделением внутренних зон

Глава 11. Безопасность маршрутизации на основе BGP

Принципы работы протокола маршрутизации BGP

Уязвимости и инциденты BGP

Защита BGP сессии между соседними маршрутизаторами

Защита маршрутизации BGP на основе данных региональных информационных центров

Интернет

Сертификаты ресурсов и их использование для защиты BGP

Защита полного маршрута BGP с помощью сертификатов RPKI

Глава 12. Виртуальные частные сети

Определение виртуальной частной сети

Свойства частной сети, имитируемые VPN

Типы VPN

MPLS VPN

VPN на основе шифрования

Глава 13. Безопасность локальных беспроводных сетей

Уязвимости локальных беспроводных сетей

Две схемы организации беспроводной сети

Методы защиты локальных беспроводных сетей

Протокол WEP

Стандарт WPA2

беспроводные системы обнаружения вторжений

Глава 14. Безопасность облачных сервисов

Что такое «облачные сервисы»

Определение облачных вычислений

Свойства облачных вычислений

Технологии облачных вычислений

Модели сервисов облачных вычислений

Преимущества облачных сервисов

Проблемы безопасности облачных сервисов

Значимость облачных сервисов

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-данных 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