Чипига, А. **Ф.**
Информационная безопасность автоматизированных систем: учеб. пособие для студентов вузов, обучающихся по специальностям в обл. информ. безопасности / А. Ф. Чипига. — М.: Гелиос АРВ, 2010. — 336 с, ил.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Глава 1. Комплексная защита сетевой файловой системы

1.1.Комплексная защита сетевой файловой системы

1.1.1.Модель комплексной защиты сетевой файловой системы

1.1.2.Характер связей и взаимодействий в модели комплексной защиты сетевой файловой системы

1.2.Средства защиты сетевой файловой системы

1.2.1.Устройства предотвращения несанкционированного доступа к ресурсам

1.2.2.Возможности шифрующей файловой системы EFS

Контрольные вопросы

Глава 2. Комплексная защита электронной почты и документооборота

2.1.Защита электронной почты

2.1.1.Общие сведения о процедурах защиты электронной почты
2.1.2.Реализация контуров защиты электронной почты
2.2.Применение криптографии с открытыми ключами. Борьба со спамом.
2.2.1.Применение криптографии с открытыми ключами для обеспечения информационной безопасности
2.2.2.Борьба со спамом
Контрольные вопросы

Глава 3. Комплексная защита сетевых приложений и баз данных

3.1.Защита сетевых приложений и баз данных
3.1.1.Типовые архитектуры сетевых приложений
3.1.2.Комплексная защита сетевых приложений и баз данных
3.1.3.Защита процедур взаимодействия средств представления информации со средствами ее обработки
3.1.4.Защита информации в базах данных
3.2.Безопасность J2EE
3.2.1.Общие сведения о языке Java и J2EE
3.2.2.Архитектура J2EE
3.3.Защита информации в современных базах данных
3.3.1. Безопасность .NET в среде Windows

3.3.2. **Б**езопасность ASP.NET
Контрольные вопросы

Глава 4. Комплексная защита телекоммуникационных систем

4 1. Комплексная защита телекоммуникационной инфраструктуры
4.1.1.Взаимосвязь состояния систем телекоммуникаций и уровня информационной безопасности общества
4.1.2.Концептуальные основы обеспечения информационной безопасности в телекоммуникационных системах и сетях
4.2.Протоколы защиты на канальном и сеансовом уровнях
4.2.1.Протоколы формирования защищенных каналов на канальном уровне
4.2.2.Протоколы формирования защищенных каналов на сеансовом уровне
4.3.Защита сетевого уровня — протокол IPSec
4.3.1.Архитектура средств безопасности IPSec
4.3.2.Защита передаваемых данных с помощью протоколов AH и ESP
4.3.3.Протокол управления криптоключами IKE
4.3.4.Особенности реализации средств IPSec
4.4.Инфраструктура защиты на прикладном уровне
4.4.1.Управление идентификацией и доступом
4.4.2.Организация защищенного удаленного доступа
4.4.3.Инфраструктура управления открытыми ключами PKI
4.5.Виды и характеристика сетевых атак
4.5.1.Классификация удаленных атак

4.5.2.Характеристика атак на поток данных в сетях
4.6.Технологии обнаружения атак
4.6.1.Концепция адаптивного управления безопасностью
4.6.2.Технологии обнаружения атак
4.7.Комплексная защита видеоконференций и IP-телефонии
4.7.1.Безопасность протоколов VoIP и потоковой трансляции медиаданных
4.7.2.Решения по защите VoIP-сетей
Контрольные вопросы
Глава 5. Управление информационной безопасностью
5.1.Методы управления средствами сетевой безопасности
5.1.1.Архитектура управления средствами сетевой безопасности
5.1.2.Назначение основных средств безопасности
5.1.3.Аудит и мониторинг безопасности
5.2.Комплексная система управления информационной безопасностью
5.2.1.Принципы построения многоуровневых иерархических систем обеспечения безопасности информации
5.2.2.Проблемы управления средствами ITSEC в больших компаниях
Контрольные вопросы
ЛИТЕРАТУРА
ГЛОССАРИЙ