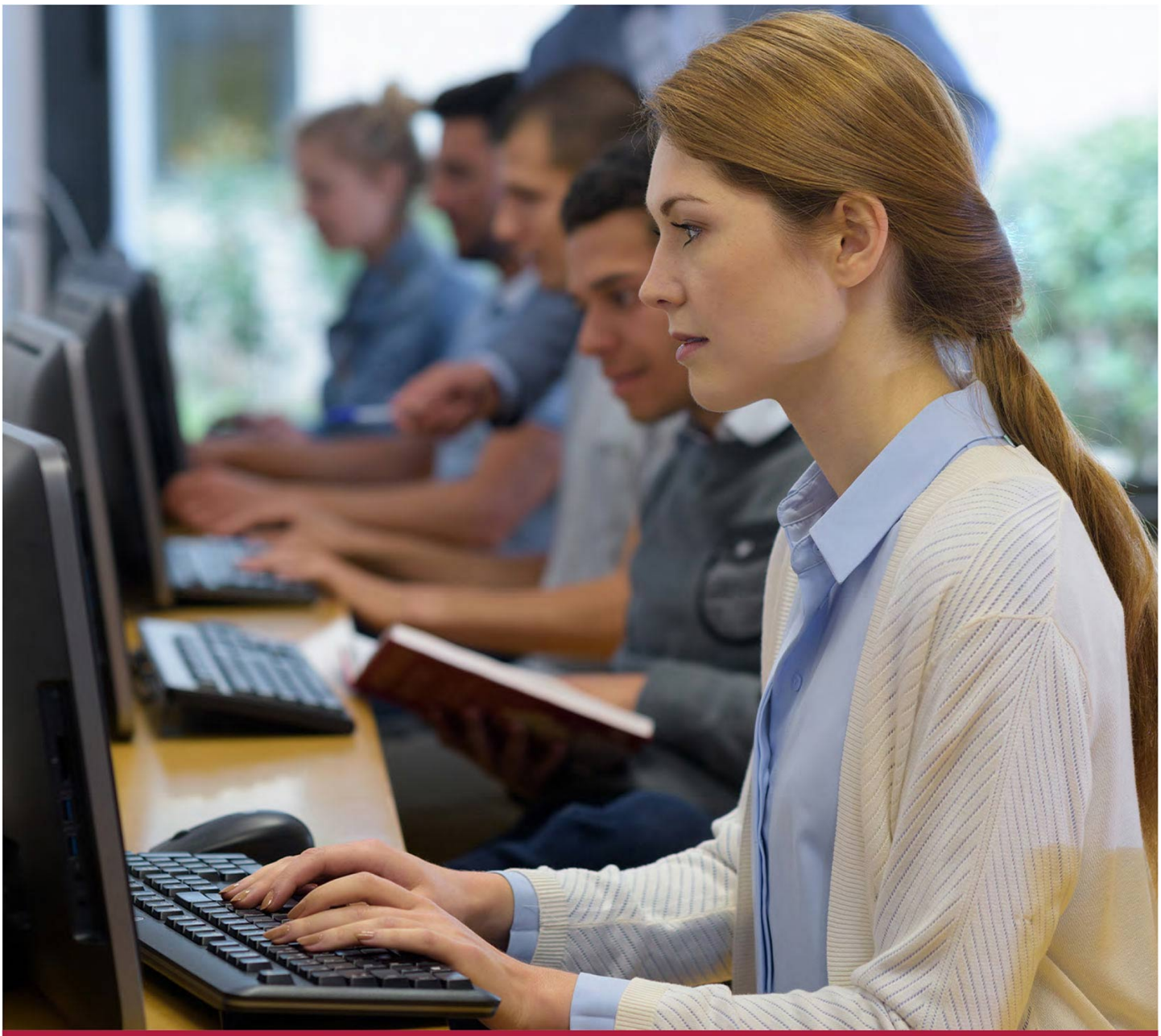
Академия АйТи
a Softline Company



Специалист по безопасности сетей

Код курса: cybernet

+7 (495) 150 96 00 | academy@academyit.ru | academyit.ru

© Академия АйТи, 2024

Специалист по безопасности сетей

Код курса: cybernet

Длительность	80 ак. часов
Формат	Очно
Разработчик курса	Академия АйТи
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Этот курс будет полезен тем, кто начинает путь в сфере информационной безопасности и хочет специализироваться в области защиты сетей. Программа также ориентирована на сетевых и системных администраторов, которые хотят структурировать, обновить свои знания и навыки в области построения защищенных компьютерных сетей.

Подробная информация

Для кого:

Для специалистов, желающих начать карьеру в области безопасности сетей

Для системных администраторов/системных инженеров

Для сетевых администраторов/сетевых инженеров

Что вы будете изучать:

- источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению
- сущность и содержание понятия информационной безопасности, характеристик, ее составляющих
- принципы построения компьютерных систем и сетей
- стек протоколов TCP/IP
- типовые методы и протоколы идентификации, аутентификации и авторизации в компьютерных сетях
- топологию и протоколы сетевого взаимодействия, применяемые в эксплуатируемых компьютерных сетях
- состав и основные характеристики оборудования, применяемого при построении компьютерных сетей
- уязвимости компьютерных систем и сетей
- типичные сетевые атаки и способы защиты от них
- программно-аппаратные средства и методы защиты информации в компьютерных сетях

© Академия АйТи, 2024

- порядок реализации методов и средств межсетевого экранирования
- общие принципы функционирования средств криптографической защиты информации в компьютерных сетях
- порядок обеспечения безопасности информации при эксплуатации компьютерных сетей

После обучения вы будете уметь:

- обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях
- устанавливать межсетевые экраны в компьютерных сетях
- конфигурировать межсетевые экраны в соответствии с заданными правилами
- настраивать правила фильтрации пакетов в компьютерных сетях
- применять программно-аппаратные средства защиты информации в компьютерных сетях
- работать в компьютерных сетях с соблюдением действующих требований по защите информации
- конфигурировать и контролировать корректность работы программно-аппаратных средств защиты информации в компьютерных сетях
- проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в компьютерных сетях
- проводить мониторинг функционирования программно-аппаратных средств защиты информации в компьютерных сетях

Сможете владеть навыками:

- формирования предложений по устранению выявленных уязвимостей компьютерных сетей
- установки программно-аппаратных средств защиты информации в компьютерных сетях
- установки средств межсетевого экранирования в соответствии с действующими требованиями по защите информации
- настройки программных и аппаратных средств построения компьютерных сетей, использующих криптографическую защиту
- ввода в эксплуатацию программно-аппаратных средств защиты информации в компьютерных сетях
- управления функционированием программно-аппаратных средств защиты информации в компьютерных сетях
- управления средствами межсетевого экранирования в компьютерных сетях в соответствии с действующими требованиями
- выполнения работ по обнаружению вредоносного программного обеспечения

Темы, изучаемые на курсе:

- Технологии трансляции IP-адресов
- Межсетевые экраны и системы обнаружения вторжений
- Прокси-серверы и VPN
- Технологии сегментации сетей
- Защита беспроводных сетей

Программа курса

© Академия АйТи, 2024

Модуль 1. Технологии трансляции IP-адресов

- Публичные («белые») и частные («серые») IP-адреса
- Замена IP-адреса и порта источника (SNAT)
- Сокрытие сетей средствами SNAT
- **Практика: Настройка SNAT на межсетевом экране**
- Замена IP-адреса и порта назначения (DNAT)
- Проброс портов и связанные с ним риски безопасности
- **Практика: Настройка проброса портов для сервисов**

Модуль 2. Технологии межсетевых экранов

- Логика работы брандмауэра
- Три поколения брандмауэров
- Логика Statefull Inspection Firewall
- Ограничения брандмауэров
- Типы брандмауэров (аппаратные, программно-аппаратные, программные)
- **Практика: Настройка локального брандмауэра для защиты Linux-сервера**
- Топологии брандмауэров: Bastion host, Screened subnet и Multi homed firewall
- **Практика: Настройка межсетевого экрана для защиты локальной сети**

Модуль 3. Системы обнаружения вторжений (СОВ/IDS)

- Назначение IDS
- Роль IDS в защите сети
- Функции IDS
- События, обрабатываемые IDS
- Чем не являются IDS
- Логика работы IDS
- Обнаружение статистических аномалий
- Полный анализ протоколов
- Компоненты IDS: Сетевые датчики, Системы оповещения, Командная консоль, Система реагирования, База данных сигнатур атак
- Особенности систем предотвращения вторжений
- **Практика: Настройка системы обнаружения вторжений**

Модуль 4. Прокси-серверы

- Next Generation Firewall (NGFW)
- Отличия NGFW от Unified threat management (UTM) и Unified Security Gateway (USG)
- Application Level Firewall (Прокси-сервер)
- Типы прокси-серверов: socks-прокси и прикладной прокси (HTTP/HTTPS и FTP)
- Виды прокси-серверов: обыный прокси и обратный (reverse) прокси
- Преимущества прокси-сервера перед брандмауэром
- **Практика: Настройка прикладного прокси**

Модуль 5. Сегментация локальной сети

- Сегментация на третьем уровне модели OSI
- **Практика: Простая настройка сегментации на маршрутизаторе**

© Академия АйТи, 2024

- Обзор технологии VLAN
- Использование VLAN для сегментации локальной сети
- **Практика: Настройка VLAN на сетевом оборудовании**
- **Практика: Изоляция сегментов с помощью правил брандмауэра**

Модуль 6. Безопасная конфигурация и управление VPN

- Основы технологии VPN
- Архитектура VPN: Client-to-Site VPN (удаленный доступ) и Site-to-Site VPN (сеть в сеть)
- Протоколы, используемые при развертывании VPN: IPSec VPN и TLS/SSL VPN
- Двухфакторная аутентификакция пользователей VPN
- **Практика: Безопасная настройка VPN**

Модуль 7. Защита беспроводных сетей

- Терминология беспроводных сетей
- Виды беспроводных технологий: 4G,WiMax,Wifi,Bluetooth
- Беспроводные стандарты IEEE
- Топологии беспроводных сетей: Ad-Hoc и Infrastructure mode
- Типичное использование беспроводных сетей
- Компоненты беспроводной сети
- Шифрование WEP, WPA, WPA2 и WPA3
- **Практика: Настройка безопасности беспроводной сети**

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Академии АйТи

+7 (495) 150 96 00 | academy@academyit.ru

© Академия АйТи, 2024