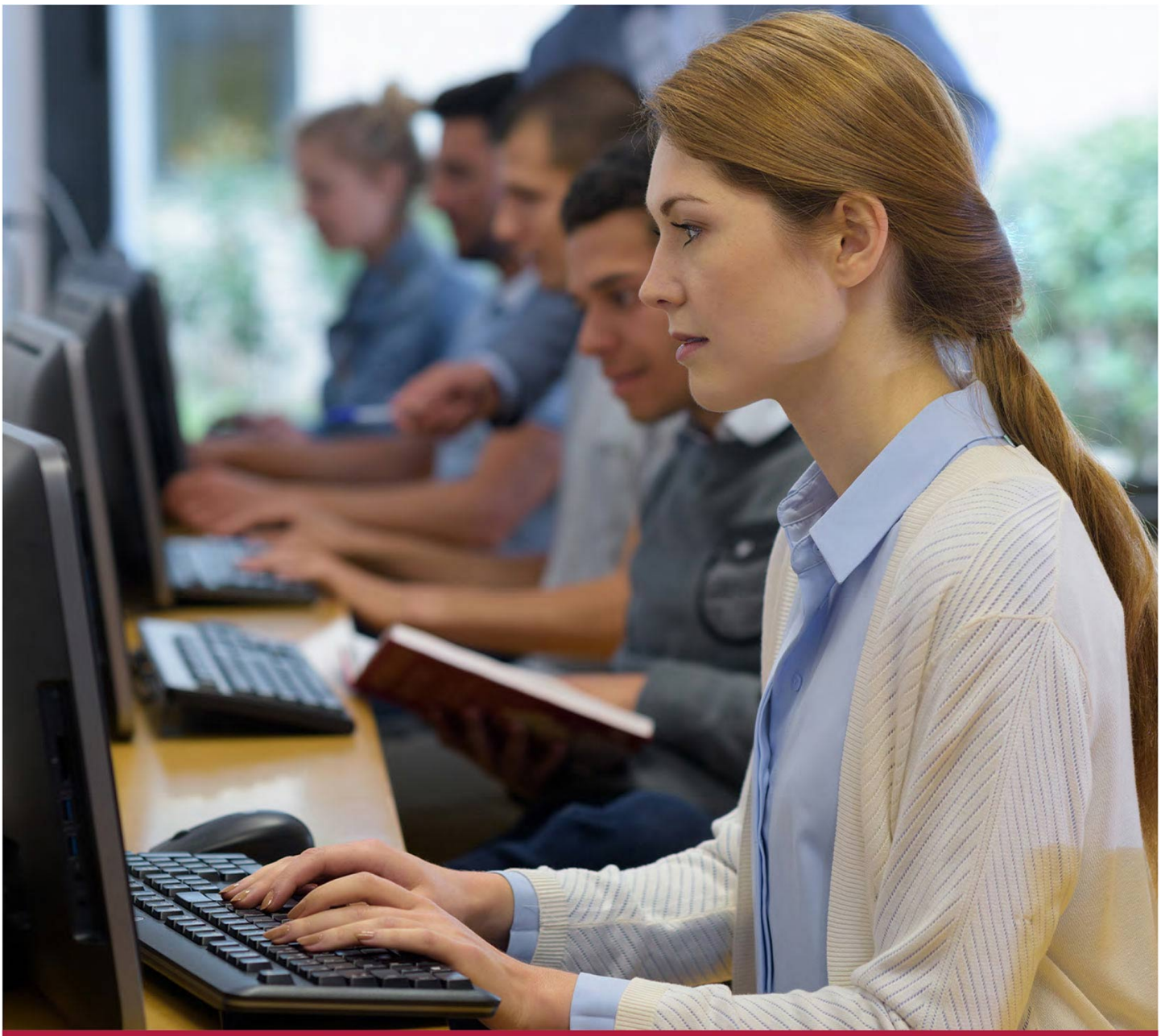
Академия АйТи
a Softline Company



Специалист по безопасности сетей

Код курса: cybernet

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

Специалист по безопасности сетей

Код курса: cybernet

Длительность	80 ак. часов
Формат	
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

- 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

Модуль 1. Технологии трансляции IP-адресов

- Технология NAT (SNAT, DNAT)».
- Настройка SNAT на межсетевом экране
- Настройка проброса портов для сервисов

Модуль 2. Технологии межсетевых экранов

- Обзор технологий межсетевых экранов и их возможностей
- Настройка локального межсетевого экрана для защиты Linux-сервера
- Настройка межсетевого экрана для защиты локальной сети

Модуль 3. Системы обнаружения вторжений (СОВ/IDS)

- Принцип работы IDS/IPS систем
- Анализ протоколов
- UTM и NGFW
- Настройка IDS/IPS систем

Модуль 4. Прокси-серверы

- Типы прокси-серверов: socks-прокси и прикладной прокси (HTTP/HTTPS и FTP)
- Виды прокси-серверов: обычный прокси и обратный (reverse) прокси
- Преимущества прокси-сервера перед межсетевым экраном
- Настройка прикладного прокси

Модуль 5. Сегментация локальной сети

- Сегментация на третьем уровне модели OSI
- Обзор технологии VLAN
- Использование VLAN для сегментации локальной сети
- Простая настройка сегментации на маршрутизаторе
- Настройка VLAN на сетевом оборудовании
- Изоляция сегментов с помощью правил межсетевого экрана

Модуль 6. Безопасная конфигурация и управление VPN

- Основы технологии VPN
- Протоколы, используемые при развертывании VPN: IPSec VPN и TLS/SSL VPN
- Безопасная настройка VPN

Модуль 7. Защита беспроводных сетей

- Компоненты беспроводной сети.
- Шифрование WEP, WPA, WPA2 и WPA3
- Описание протокола RADIUS.
- Аутентификация через RADIUS-сервер при беспроводном подключении к сегменту локальной сети
- Настройка безопасности беспроводной сети

Модуль 8. Использование UTM-решений для защиты сети

- Популярные UTM-решения с открытым исходным кодом
- Знакомство с Zentyal Server
- Знакомство с OPNSense
- Установка и настройка Zentyal Server
- Установка и настройка OPNSense.

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Академии АйТи

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