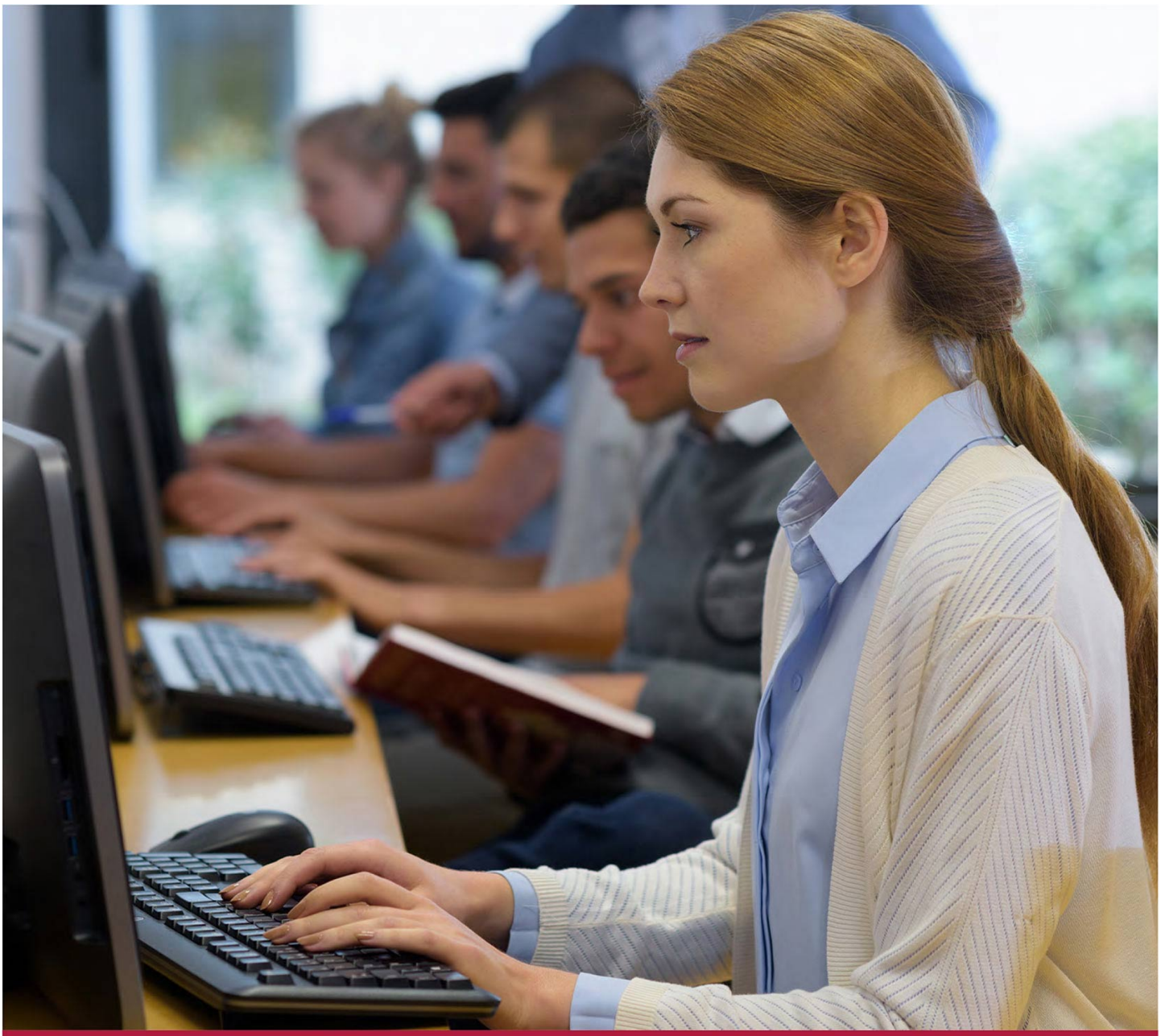
softline учебный центр



Администрирование АПКШ "Континент" версии 3.9

Код курса: АПКШ

8 (800) 505-05-07 | edusales@softline.com | edu.softline.com

Администрирование АПКШ "Континент" версии 3.9

Код курса: АПКШ

Длительность	32 ак. часа
Формат	Очно; Дистанционно
Разработчик курса	Код безопасности
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Авторизованный четырёхдневный курс Кода Безопасности «Администрирование АПКШ Континент версии 3.9» разработан для изучения работы сертифицированного изделия "Аппаратно-программный комплекс шифрования «Континент». Версия 3.9". В результате обучения слушатели получат теоретические знания и практические навыки, необходимые для инсталляции и управления компонентами комплекса, настройки защиты данных, передаваемых по сетям общего пользования, межсетевого экранирования и маршрутизации трафика.

Подробная информация

Профиль аудитории:

Курс предназначен для специалистов в сфере информационной безопасности, системных администраторов, руководителей ИТ-служб, архитекторов систем информационной безопасности, отвечающих за защиту каналов связи при передаче информации ограниченного доступа между сегментами сложных распределенных сетей по публичным или выделенным каналам связи.

Предварительные требования:

- Базовые знания по IP-сетям, основным протоколам и службам стека TCP/IP;
- Навыки работы с ОС Windows 7/2008 Server и желательно (но не обязательно) FreeBSD.

По окончании курса слушатели смогут:

- Ввести в эксплуатацию комплекс АПКШ «Континент версии 3.9»;
- Управлять криптографическими ключами комплекса АПКШ «Континент версии 3.9»;
- Управлять учетными записями администраторов АПКШ «Континент версии 3.9»;
- Выполнять локальное управлении сетевыми устройствами АПКШ «Континент версии 3.9»;
- Формировать правил фильтрации трафика;
- Настраивать Детектор Атак «Континент версии 3.9»;
- Организовать L3VPN-шлюз;
- Организовать совместную работу КШ с внешним маршрутизирующим устройством, поддерживающим трансляцию сетевых адресов (КШ за NAT);

- Организовать L2VPN-шлюз;
- Организовать VPN удаленного доступа с помощью комплекса АПКШ «Континент версии 3.9»;
- Выполнять резервное копирование и восстановление конфигурации ЦУС комплекса АПКШ «Континент версии 3.9»;
- Настраивать аппаратное резервировании ЦУС комплекса АПКШ «Континент версии 3.9»;
- Настраивать аппаратное резервировании и восстановлении КШ комплекса АПКШ «Континент версии 3.9»;
- Выполнять мониторинг состояния комплекса АПКШ «Континент версии 3.9» и настройку реакции на события;
- Выполнять обновление текущей версии ПО АПКШ «Континент версии 3.9»;
- Настраивать резервирование и отказоустойчивость каналов связи АПКШ «Континент версии 3.9»;
- Настраивать отказоустойчивость канала связи с помощью Multi-WAN Follower;
- Настраивать балансировку трафика между двумя внешними интерфейсами КШ с помощью Multi-WAN Load Balancing;
- Выполнять поиск и устранении неисправностей в АПКШ «Континент версии 3.9».

Программа курса

Модуль 1. Обзор технологий и развертывание системы защиты

- Назначение комплекса АПКШ «Континент»;
- Состав комплекса АПКШ «Континент версии 3.9»;
- Новые решения в АПКШ «Континент» 3.9 по сравнению с версией 3.7;
- Защитные механизмы комплекса АПКШ «Континент версии 3.9»;
- Принципы функционирования комплекса АПКШ «Континент версии 3.9»;
- Типовые аппаратные платформы АПКШ «Континент» и их производительность;
- Способы поставки ПО сетевых устройств АПКШ «Континент»;
- ПАК «Соболь»;
- Политика лицензирования комплекса АПКШ «Континент версии 3.9»;
- Порядок ввода в эксплуатацию комплекса АПКШ «Континент версии 3.9».
- Лабораторный модуль №1 «Инициализация компонентов системы»
- Лабораторная работа №1 «Инициализация ЦУС и СД»;
- Защитные механизмы комплекса АПКШ «Континент версии 3.9»;
- Лабораторная работа №2 «Установка подсистемы управления комплексом»;
- Лабораторная работа №3 «Конфигурирование БД журналов. Настройка агента ЦУС и СД»;
- Лабораторная работа №4 «Инициализация КШ»;

Модуль 2. Управление компонентами комплекса

- Управление криптографическими ключами комплекса
- Управление учетными записями администраторов
- Локальное управление сетевыми устройствами
- Лабораторный модуль №2 "Организация работы администраторов комплекса"
- Лабораторная работа №1 "Смена главного ключа КШ и ключа связи с ЦУС"
- Лабораторная работа №2 "Управление учетными записями администраторов"

Модуль 3. Правила фильтрации IP-пакетов и правила трансляции

- Межсетевой экран. Принцип действия
- Формирование правил фильтрации трафика;
- Трансляция сетевых адресов (правила NAT)
- Лабораторный модуль №3 "Правила фильтрации IP-пакетов и правила трансляции"
- Лабораторная работа №1 "Настройка правил фильтрации, разрешающих прохождение трафика между компьютерами из защищаемой сети и сети общего доступа"
- Лабораторная работа №2 "Настройка правила фильтрации, разрешающего прохождение трафика между компьютерами из внутренних сетей, защищаемых разными криптошлюзами"
- Лабораторная работа №3 "Настройка исходящего правила трансляции"
- Лабораторная работа №4 "Настройка входящего правила трансляции"

Модуль 4. Детектор атак

- Лабораторный модуль №4 "Детектор атак"
- Лабораторная работа №1 "Установка и инициализация ДА"
- Лабораторная работа №2 "Настройка и тестирование функциональности ДА"

Модуль 5. Организация и управление VPN-соединениями

- Организация L3VPN-шлюза
- Организация L2VPN-шлюза
- VPN удаленного доступа
- Лабораторный модуль №5 "Построение VPN"
- Лабораторная работа №1 "Организация L3VPN"
- Лабораторная работа №2 "Тестирование совместной работы КШ с внешним маршрутизирующим устройством, поддерживающим трансляцию сетевых адресов"
- Лабораторная работа №3 "Организация L3VPN между удаленным пользователем и защищаемой сетью"
- Лабораторная работа №4 "Организация L3VPN между удаленным пользователем и защищаемой сетью филиала"
- Лабораторная работа №5 "Организация L2VPN"

Модуль 6. Обеспечение отказоустойчивости комплекса

- Резервирование и восстановление конфигурации ЦУС;
- Аппаратное резервирование и восстановление КШ;
- Лабораторный модуль №6 "Архивирование и восстановление"
- Лабораторная работа №1 "Резервирование КШ"
- Лабораторная работа №2 "Резервирование ЦУС"

Модуль 7. Мониторинг и диагностика системы защиты

- Мониторинг состояния комплекса
- Лабораторный модуль №7 "Мониторинг и диагностика системы защиты"
- Лабораторная работа №1 "Мониторинг состояния компонентов системы и передаваемого трафика, настройка реакции на события"

Модуль 8. Обновление версии ПО

- Обновление текущей версии ПО

- Требования к эксплуатации комплекса
- Лабораторный модуль №8 "Обновление ПО"
- Лабораторная работа №1 "Обновление ПО ЦУС"
- Лабораторная работа №2 "Обновление ПО КШ"

Модуль 9. Резервирование и отказоустойчивость каналов связи (Multi-WAN)

- Отказоустойчивость каналов связи (Multi-WAN)
- Лабораторный модуль №9 "Настройка Multi-WAN"
- Лабораторная работа №1 "Обеспечение отказоустойчивости канала связи с помощью Multi-WAN"
- Лабораторная работа №2 "Настройка балансировки трафика между двумя внешними интерфейсами КШ"

Модуль 10. Поиск и устранение неисправностей

- Лабораторный модуль №10 «Поиск и устранение неисправностей»
- Лабораторная работа №1 "Отсутствует подключение КШ к ЦУС. Недоступен сетевой интерфейс на внешнем маршрутизирующем устройстве"
- Лабораторная работа №2 "Отсутствует подключение КШ к ЦУС. На внешнем маршрутизирующем устройстве заблокировано прохождение управляющего трафика между ЦУС и КШ"
- Лабораторная работа №3 "Отсутствует подключение КШ к ЦУС – несовместимость ключей связи"
- Лабораторная работа №4 "Отсутствует подключение КШ к ЦУС. Особенности настройки маршрутизации и Multi-WAN"
- Лабораторная работа №5 "Отсутствует шифрование между двумя КШ. Заблокирована возможность передачи данных на канале шифрования"
- Лабораторная работа №6 "Отсутствует шифрование между двумя КШ. Зашифрованный трафик передается только в одну сторону"
- Лабораторная работа №7 "Из защищаемой сети недоступен внешний ресурс при настроенных правилах фильтрации"
- Лабораторная работа №8 "Осуществляется передача трафика при настроенном запрещающем правиле фильтрации"
- Лабораторная работа №9 «Использование технологической информации при проведении диагностики КШ».

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Учебного центра Softline

8 (800) 505-05-07 | edusales@softline.com

Ждём вас на занятиях в Учебном центре Softline!

Почему Учебный центр Softline?

Лидер на рынке корпоративного обучения.

Более 300 тысяч подготовленных IT-специалистов.

Гибкий индивидуальный подход в обучении, скидки и акции.

Широкая сеть представительств в крупнейших городах РФ и СНГ; дистанционный формат обучение на вашей территории или в арендованном классе в любой точке мира.

Высокотехнологичное оборудование

Более **18 лет** опыта работы

Международные сертификаты для IT-специалистов и пользователей в Центрах тестирования

Сертифицированные тренеры с богатым практическим опытом работы

Авторизации от мировых производителей ПО (Microsoft, Cisco, VMware, Citrix, Лаборатория Касперского, Oracle, Autodesk, Код безопасности и других).

Разработка курсов и тестов под заказ, внедрение корпоративных систем обучения.

Подробнее об Учебном центре Softline
Вы можете узнать из профайла.