

Администрирование Континент 4 (CONT4)

ID SD-CONT4 Цена 125 000,- руб. Длительность 5 дней

Кому следует посетить

Курс ориентирован на специалистов в сферах информационной и телекоммуникационной безопасности, системных администраторов, руководителей ИТ-служб, архитекторов систем информационной безопасности, которые отвечают за защиту сегментов корпоративной сети организации и ее филиалов, разделенных каналами связи общего доступа.

Предварительные требования

Предполагается наличие у слушателей опыта администрирования операционных систем семейств Windows и Linux, базовых знаний в области применения основных компонентов NGFW (DPI, COB, контентная фильтрация, потоковый антивирус, контроль протоколов и приложений), понимания принципов работы вспомогательных телекоммуникационных служб и сервисов (AD, GPO, Kerberos, DNS, DHCP, RADIUS, LDAP, syslog, SNMP), а также наличие опыта настройки оборудования локальной сети и базовых знаний в области применения технологий VPN.

Содержание курса

Учебный курс "Администрирование "Континент" 4" разработан для изучения работы сертифицированного изделия "Комплекс безопасности "Континент". Версия 4" (далее – комплекс Континент, Континент 4, Континент, комплекс). В результате обучения слушатели получат теоретические знания и практические навыки, необходимые для внедрения, настройки и обслуживания компонентов комплекса. В процессе обучения слушатели на практике будут изучать возможности Континент по настройке и администрированию определенных компонентов и сервисов.

Программа курса

День 1

Глава 1. Общие сведения по Континент 4

- Назначение и состав комплекса
- Принципы функционирования комплекса
- Управление комплексом
- ПАК "Соболь"
- Типовые аппаратные платформы и их производительность
- Политика лицензирования
- Порядок ввода комплекса в эксплуатацию
- Лабораторный модуль №1 "Развертывание ЦУС Континент, рабочего места главного администратора и подчиненных узлов безопасности"

Лабораторная работа №1 "Развертывание центра управления сетью Континент и регистрация главного администратора"

Лабораторная работа №2 "Подготовка рабочего места главного администратора"

Лабораторная работа №3 "Настройка подключения к подсистеме мониторинга"

Лабораторная работа №4 "Развертывание подчиненных узлов безопасности"

- Контрольные вопросы

День 2

Глава 2. Управление узлами Континент

- Роли администраторов. Назначение администраторов
- Дистанционный доступ по протоколу SSH
- Лабораторный модуль №2 "Управление узлами Континент"

Лабораторная работа №1 "Управление ролями и учетными записями администраторов"

Лабораторная работа №2 "Настройка дистанционного доступа по протоколу SSH"

- Контрольные вопросы

Администрирование Континент 4 (CONT4)

Глава 3. Настройка межсетевого экранирования

- Обработка трафика узлом безопасности
- Межсетевое экранирование
- Сетевые функции
- Виды объектов ЦУС
- Правила фильтрации
- Правила трансляции
- Установка политики
- Лабораторный модуль №3 "Настройка многофункционального межсетевого экрана на узлах безопасности в режиме UTM"

Некоторые особенности обработки сетевого трафика компонентами многофункционального межсетевого экрана в режиме UTM

Лабораторная работа №1 "Настройка правил фильтрации"

Лабораторная работа №2 "Настройка правил трансляции"

- Контрольные вопросы

Глава 4. Система обнаружения и предотвращения вторжений

- Концепция управления СОВ
- Управление детектором атак в режимах Monitor и Inline
- Установка БРП. Создание собственных сигнатур
- Формирование и установка политик СОВ
- Лабораторный модуль №4 "Инициализация, настройка и проверка функциональности детектора атак"

Лабораторная работа №1 "Инициализация детектора атак"

Лабораторная работа №2 "Настройка детектора атак: установка БРП, создание профиля и применение политик"

День 3

Глава 4. Система обнаружения и предотвращения вторжений

- Лабораторный модуль №4 "Инициализация, настройка и проверка функциональности детектора атак"

Лабораторная работа №3 "Проверка функциональности детектора атак"

Лабораторная работа №4 "Настройка СОВ в составе UTM-узла безопасности"

- Контрольные вопросы

Глава 5. Построение VPN

- VPN-туннель
- Шифрование
- Топология
- L3VPN IPSec
- VPN удаленного доступа
- Лабораторный модуль №5 "Построение VPN"

Лабораторная работа №1 "Организация проприетарного L3VPN между защищаемыми сетями"

Лабораторная работа №2 "Построение L3VPN IPSec между пересекающимися сетями"

Лабораторная работа №3 "Организация L3VPN между удаленным пользователем и защищаемой сетью"

День 4

Глава 5. Построение VPN

- L2VPN-туннель
- Лабораторный модуль №5 "Построение VPN"

Лабораторная работа №4 "Организация L3VPN между удаленным пользователем и защищаемой сетью за другим УБ Континент"

Лабораторная работа №5 "Организация L2VPN"

- Контрольные вопросы

Глава 6. Обеспечение отказоустойчивости комплекса

- Резервирование и восстановление конфигурации
- Аппаратное резервирование и восстановление узла безопасности
- Резервирование БД ЦУС
- Лабораторный модуль №6 "Резервирование и восстановление"

Лабораторная работа №1 "Резервирование узла безопасности"

Лабораторная работа №2 "Резервирование БД ЦУС"

Администрирование Континент 4 (CONT4)

Лабораторная работа №3 "Резервное копирование и восстановление данных узла безопасности или ЦУС"

- Контрольные вопросы

Глава 7. Мониторинг и аудит

- Общие сведения по системе мониторинга: инициализация, объекты мониторинга и типы информации, применение правил и шаблонов
- Просмотр сведений журналов
- Аудит
- Лабораторный модуль №7 "Мониторинг и аудит"

Лабораторная работа №1 "Настройка параметров аудита. Работа с подсистемой мониторинга"

Лабораторная работа №2 "Локальная работа с журналами аудита"

- Контрольные вопросы

День 5

Глава 8. Настройка Multi-WAN

- Лабораторный модуль №8 "Настройка Multi-WAN"

Лабораторная работа №1 "Обеспечение отказоустойчивости канала связи"

Лабораторная работа №2 "Настройка балансировки трафика между двумя внешними интерфейсами узла безопасности"

- Контрольные вопросы

Глава 9. Виртуальная маршрутизация

- Краткое описание механизма виртуальной маршрутизации
- Настройка VRF-зон
- Просмотр сведений о VRF-зонах в локальном меню узла безопасности
- Управление сетевыми интерфейсами в составе VRF-зоны
- Лабораторный модуль №9 "Настройка и применение виртуальной маршрутизации"

Лабораторная работа №1 "Настройка и применение виртуальной маршрутизации"

- Контрольные вопросы

Глава 10. Поддержка динамической маршрутизации

- Протоколы динамической маршрутизации
- Лабораторный модуль №10 "Поддержка динамической маршрутизации"

Лабораторная работа №1 "Настройка динамической маршрутизации по протоколу BGP"