



## Администрирование АПКШ "Континент" версии 3.9

Код курса: АК3.9

## Администрирование АПКШ "Континент" версии 3.9

Код курса: АК3.9

|                          |                          |
|--------------------------|--------------------------|
| <b>Длительность</b>      | 40 ак. часов             |
| <b>Формат</b>            |                          |
| <b>Разработчик курса</b> | Код безопасности         |
| <b>Тип</b>               | Учебный курс             |
| <b>Способ обучения</b>   | Под руководством тренера |

### О курсе

Учебный курс "Администрирование АПКШ "Континент" версии 3.9" разработан для изучения работы сертифицированного изделия "Аппаратно-программный комплекс шифрования "Континент". Версия 3.9" (далее – комплекс, АПКШ "Континент", "Континент"). В результате обучения слушатели получат теоретические знания и практические навыки, необходимые для внедрения, настройки и обслуживания сетевых компонентов комплекса. Во время прохождения обучения слушатели на практике будут изучать возможности АПКШ "Континент" по настройке межсетевого экранирования и маршрутизации трафика, по применению технологии NAT, по организации виртуальных частных сетей на основе общих сетей передачи данных, по мониторингу и аудиту компонентов системы, а также познакомятся с возможностями более тонкой настройки виртуальных частных сетей, со способами обеспечения отказоустойчивости работы узлов "Континент" при сбоях в каналах связи. Кроме того, в лабораторных работах показаны способы расширенной диагностики сетевых узлов комплекса и примеры диагностирования и устранения нештатных ситуаций.

### Подробная информация

#### Профиль аудитории:

- Специалисты в сфере информационной безопасности
- Системные администраторы
- Руководители ИТ-служб
- Архитекторы систем информационной безопасности,
- Все, кто занимается внедрением, обслуживанием и администрированием систем безопасности, основанных на АПКШ "Континент".

#### Предварительные требования:

- Наличие у слушателей опыта администрирования операционных систем семейств Windows и Linux
- Понимание принципов работы сетей передачи данных, знания стека протоколов TCP/IP
- Наличие опыта настройки оборудования локальной сети.

#### По окончании курса слушатели смогут:

- Получить теоретические знания и практические навыки, необходимые для внедрения, настройки и обслуживания сетевых компонентов комплекса.
- Изучить возможности АПКШ "Континент" по настройке межсетевого экранирования и маршрутизации трафика, по применению технологии NAT, по организации виртуальных частных сетей на основе общих сетей передачи данных, по мониторингу и аудиту компонентов системы
- Познакомится с возможностями более тонкой настройки виртуальных частных сетей, со способами обеспечения отказоустойчивости работы узлов "Континент" при сбоях в каналах связи
- Рассмотреть способы расширенной диагностики сетевых узлов комплекса и примеры диагностирования и устранения нештатных ситуаций.

## Программа курса

### **Модуль 1. Обзор технологий и развертывание системы защиты**

- Назначение и состав комплекса
- Защитные механизмы
- Принципы функционирования комплекса
- Типовые аппаратные платформы "Континент" и их производительность
- Способы поставки ПО сетевых устройств АПКШ "Континент"
- ПАК "Соболь"
- Политика лицензирования
- Порядок ввода комплекса в эксплуатацию

Лабораторная работа №1 "Инициализация ЦУС и СД"

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

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)

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**

- Общее описание работы ДА

Лабораторная работа №1 "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

Лабораторная работа №1 "Организация L3VPN"

Лабораторная работа №2 "Тестирование совместной работы КШ с внешним маршрутизирующим устройством, поддерживающим трансляцию сетевых адресов"

Лабораторная работа №3 "Построение L3VPN между пересекающимися подсетями, защищенными разными КШ"

Лабораторная работа №4 "Организация L3VPN между удаленным пользователем и защищаемой сетью"

Лабораторная работа №5 "Организация L3VPN между удаленным пользователем и защищаемой сетью филиала"

Лабораторная работа №6 "Организация L2VPN"

#### **Модуль 6. Обеспечение отказоустойчивости комплекса**

- Резервирование и восстановление конфигурации ЦУС
- Аппаратное резервирование и восстановление КШ

Лабораторная работа №1 "Резервирование КШ"

Лабораторная работа №2 "Резервирование ЦУС"

#### **Модуль 7. Мониторинг и диагностика системы защиты**

- Мониторинг состояния комплекса

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

Лабораторная работа №1 "Обновление ПО ЦУС"

Лабораторная работа №2 "Обновление ПО КШ"

Лабораторная работа №3 "Подключение к ЦУС сетевого узла "Континент" младшей версии с последующим обновлением ОС"

### **Модуль 9. Резервирование и отказоустойчивость каналов связи**

- Отказоустойчивость каналов связи (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**

- Основы устранения 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 шифрование между двумя КШ. Заблокирована возможность передачи данных на канале шифрования"

Лабораторная работа №5 "Отсутствует шифрование между двумя КШ. Зашифрованный трафик передается только в одну сторону"

Лабораторная работа №6 "Из защищаемой сети недоступен внешний ресурс при настроенных правилах фильтрации"

Лабораторная работа №7 "Осуществляется передача трафика при настроенном запрещающем правиле фильтрации"

Лабораторная работа №8 "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](mailto: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](#).