

## HCIP-Security 4.0 (HCIP-SECURITY)

ID HU-HCIP-SECURITY Цена 320 900,- руб. Длительность 10 дней

### Кому следует посетить

- Инженеры в области ИБ

### Предварительные требования

Знания в объеме курса [Huawei Certified ICT Associate-Security \(HCIA-SECURITY\)](#) или аналогичный опыт.

### Цели курса

По окончании данной программы участники смогут:

- Описать принципы технологий высокой надежности брандмауэра
- Описать высоконадежный сетевой режим брандмауэра
- Описать сценарии применения высоконадежных технологий брандмауэра.
- Описать сценарии применения управления полосой пропускания
- Описывать основы управления пропускной способностью
- Описывать сценарии применения политик контроля квот
- Описывать основы политики контроля квот
- Освоить настройки управления трафиком брандмауэра
- Описать сценарии применения виртуальных систем
- Описывать основные понятия виртуальных систем
- Настраивать виртуальные системы
- Описывать основные концепции интеллектуального выбора восходящего канала
- Описать сценарии применения интеллектуального выбора восходящего канала
- Настроить интеллектуальный выбор восходящего канала
- Понимать основные принципы IPsec VPN
- Понимать типичные сценарии применения IPsec VPN.
- Освоить высоконадежный метод настройки IPsec VPN
- Изучить мастер-метод устранения неполадок IPsec VPN
- Понимать сценарии применения SSL VPN
- Освоить основные функции и принципы SSL VPN
- Понимать сети SSL VPN

- Освоить настройку SSL VPN
- Описать принципы распространенных однопакетных атак
- Описать принципы распространенных DDoS-атак
- Описать принципы защиты от однопакетных атак
- Описать принципы защиты от DDoS-атак
- Описать решение для защиты от DDoS и соответствующие принципы защиты
- Описать цепочку киберубийств
- Изучить меры защиты от уязвимостей
- Описать технические основы технологий фильтрации контента
- Описать основные принципы технологий фильтрации контента
- Работать с конфигурацией технологий фильтрации контента
- Описывать основные концепции реагирования на чрезвычайные ситуации в области кибербезопасности.
- Описать процесс реагирования на чрезвычайные ситуации в области кибербезопасности.
- Понимать технологии, связанные с реагированием на чрезвычайные ситуации в области кибербезопасности.
- Описать основные концепции NAC
- Описать принципы работы аутентификации пользователя.
- Описывать распространенные режимы аутентификации доступа и принципы их работы.
- Настроить аутентификацию доступа пользователей
- Применять различные технологии сетевой безопасности
- Разработать решения для сетевой безопасности
- Развернуть решения сетевой безопасности
- Быть знакомым с сетевой безопасностью O&M

### Программа курса

#### 1 Безопасная сеть

Обзор сертификации кибербезопасности

- Модели возможностей для инженеров по кибербезопасности
- Сертификация кибербезопасности

Технологии высокой надежности брандмауэра

- Обзор технологий высокой надежности брандмауэра
- Горячее резервирование брандмауэра
- Высокая надежность соединения брандмауэра
- Обновление версии с горячим резервированием и устранение неполадок

## Управление трафиком брандмауэра

- Управление пропускной способностью брандмауэра
- Политики управления квотами брандмауэра
- Пример настройки управления трафиком

## Виртуальная система брандмауэра

- Обзор виртуальной системы
- Основные концепции виртуальных систем
- Связь между виртуальными системами
- Конфигурация виртуальной системы

## Выбор интеллектуального восходящего канала брандмауэра

- Обзор интеллектуального выбора восходящего канала
- Принципы интеллектуального выбора восходящего канала
- Конфигурация интеллектуального выбора восходящего канала

## Технология и приложение IPsec VPN

- Основные принципы IPsec VPN
- Сценарии применения IPsec VPN
- Высокая надежность IPsec VPN
- Устранение неполадок IPsec VPN

## Технология и приложение SSL VPN

- Обзор SSL VPN
- Сервисные функции SSL VPN
- Примеры настройки SSL VPN
- Устранение неполадок SSL VPN

## 2 Граница зоны безопасности

### Кибератаки и защита

- Технологии защиты от атак с помощью брандмауэра
- Защита от однопакетных атак
- Защита от DDoS-атак

### Защита от уязвимостей и тестирование на проникновение

- Уязвимость
- Защита от уязвимостей
- Тестирование на проникновение

### Технологии фильтрации контента

- Обзор технологий фильтрации контента
- Принципы технологий фильтрации контента
- Примеры настройки технологий фильтрации контента

## 3 Центр управления безопасностью

### Аварийного реагирования

- Обзор экстренного реагирования
- Процесс реагирования на чрезвычайные ситуации
- Технологии и кейсы аварийного реагирования

### Контроль доступа к сети

- Обзор NAC
- Идентификация пользователя
- Аутентификация доступа
- Конфигурация NAC

### Комплексные кейсы корпоративной сетевой безопасности

- Обзор требований к безопасности корпоративной сети
- Разработка и развертывание решений корпоративной сетевой безопасности
- Устранение неполадок безопасности корпоративной сети