АНО ДПО «Сетевая-Академия ЛАНИТ-ТИССА

(Наименование образовательного учреждения)

УТВЕРЖДАЮ
АНО ДПО «Сетевая Академия ЛАНИТ-ТИССА»
_____/К.К. Костылев/
«23» января 2017 «20 17» г.

Образовательная программа
дополнительного профессионального образования
(повышения квалификации)
«Проектирование и сопровождение сетевых решений и системная интеграция»

(Наименование программы)

Содержание

Пояснительная записка

Настоящая образовательная программа (далее – Программа) разработана в соответствии с:

1. Федеральным законом от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации»
2. Приказом Минобрнауки России от 1 июля 2013 г. N 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»
3. Уставом НОУ УЦ «Сетевая академия»

Содержание Программы представлено описанием программы, планируемыми результатами обучения, учебным планом, календарным учебным графиком, описанием организационно-педагогических условий реализации Программы, описанием оценочных материалов и форм аттестации, рабочими программами учебных курсов (дисциплин).

Планируемые результаты обучения представлены в виде общих для Программы компетенций, качественное изменение которых осуществляется в результате обучения по учебным курсам (дисциплинам), входящим в учебный план Программы. Также для каждого учебного курса (дисциплины) в рабочей программе представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине).

Учебный план Программы определяет перечень, трудоемкость, последовательность и распределение учебных курсов (дисциплин) и формы аттестации. Допускается формирование индивидуального учебного плана для каждого слушателя в пределах осваиваемой Программы. Содержание индивидуального учебного плана определяется НОУ УЦ «Сетевая академия» с учетом потребностей лица, организации, по инициативе которых осуществляется дополнительное профессиональное образование по настоящей Программе.

Календарный учебный график определяет основные параметры учебного процесса при организации занятий по освоению настоящей Программы, включая формы обучения, расписание занятий очных групп и т.п.

Описание организационно-педагогических условий реализации Программы определяет методические требования НОУ УЦ «Сетевая академия» к организации и проведению обучения по Программе и/или ее отдельным учебным курсам (дисциплинам).

Оценочные материалы и формы аттестации определяют структуру учебно-методических материалов, необходимых для проведения итоговой аттестации по Программе и контроля знаний по каждому учебному курсу (дисциплине) Программы, а также формы проведения итоговой аттестации и контроля знаний.

Рабочие программы учебных курсов (дисциплин) раскрывают рекомендуемую последовательность изучения разделов и тем каждого учебного курса (дисциплины).

Описание образовательной программы

Данная программа предназначена для повышения квалификации специалистов, деятельность которых связана с проектированием и сопровождением сетевых решений и системной интеграцией.

Данная программа предназначена для:

- сетевых администраторов;
- сотрудников компаний – системных интеграторов;
- специалистов служб технической поддержки.

Целью обучения является обеспечить слушателям уровень знаний и навыков, достаточный для эффективной работы по разработке, внедрению и сопровождению сетевых решений, подготовить слушателей к работе в крупных проектах системной интеграции.

Образовательная программа может использоваться для повышения квалификации специалистов, которым требуется качественно улучшить компетенции в областях, определяемых профессиональными стандартами в области информационных технологий «Специалист по системному администрированию» и «Специалист информационной безопасности».

Предварительная подготовка слушателей:

- Опыт работы с операционными системами Windows, Linux, Unix;
- Базовые знания сетевой инфраструктуры, стека протоколов TCP/IP и концепций сетевого взаимодействия;
- Опыт проектирования и внедрения сетевых решений.

Планируемые результаты обучения

Ниже представлен перечень компетенций, качественное изменение которых осуществляется в результате обучения по учебным курсам (дисциплинам), входящим в учебный план Программы. В силу практикоориентированности данной Программы компетенции сформулированы в терминологии умений и соответствующих им знаний.

После обучения слушатель сможет:

- Выполнять задачи сетевого администрирования;
- Понимать требования, предъявляемые к информационной сети;
- Определять основные этапы проектирования и реализации информационных систем;
- Выполнять задачи практического проектирования клиентских систем и серверных приложений, включая проектирование облачных решений;
- Проектировать и внедрять сложные гетерогенные сетевые решения, обеспечивающие сетевую защиту информации;
- Создавать инфраструктуру центров обработки данных.

Учебный план

Форма аттестации: итоговая аттестация в форме последовательности тестов по каждому учебному предмету Программы

№ п/п	Наименование учебных предметов (тем)	Всего, час	Форма контроля
1.	Тема 1: Сетевые технологии	40	Экзамен(ы) в форме теста
2.	Тема 2: Проектирование информационных сетей	40	Экзамен(ы) в форме теста
3.	Тема 3: Принципы системной интеграции	40	Экзамен(ы) в форме теста
	Итого	**120**	

Тема 1: Сетевые технологии

В рамках первой темы рассматриваются базовые вопросы построения компьютерных сетей такие, как: основные типы сетей, основные элементы сети, сетевые сервисы, одноранговые сети и сети с выделенными серверами, проводные и беспроводные сети, общие и частные сети, стандарты OSI и 802, виртуальные локальные сети, всемирная сеть Internet, сетевое оборудование, защита данных в сети, основы сетевого администрирования.

Для прохождения обучения по Теме 1 «Сетевые технологии» слушатель должен успешно завершить обучение на одном или нескольких учебных курсах(дисциплинах) из следующего списка общей продолжительностью не менее 40 академических часов:

ICND1 Использование сетевого оборудования Cisco (часть I) – 40 ак.часов
ICND2 Использование сетевого оборудования Cisco (часть II) – 40 ак.часов
EDU-JUN-IJOS Основы работы с операционной системой JUNOS – 8 ак.часов
EDU-JUN-JRE Основы работы с протоколами маршрутизации в JUNOS - 8 ак.часов
EDU-JUN-JIR Настройка протоколов маршрутизации в операционной системе JUNOS –16 ак.часов
EDU-JUN-JEX Коммутация в корпоративных сетях – 16 ак.часов

Тема 2: Проектирование информационных сетей

В рамках второй темы обсуждаются требования, предъявляемые к построению информационной сети, состав основных этапов проектирования и реализации, обнаружение сетевых проблем и их устранение, методологические основы проектирования сетей, вопросы практического проектирования с использованием сетевых устройств, проектирование клиентских систем и серверных приложений, масштабирование сетевых серверов, приложения и устройства для безопасного доступа.

Для прохождения обучения по Теме 2 «Проектирование информационных сетей» слушатель должен успешно завершить обучение на одном или нескольких учебных курсах (дисциплинах) из следующего списка общей продолжительностью не менее 40 академических часов:

ROUTE Маршрутизация в IP-сетях Cisco – 40 ак.часов
SWITCH Внедрение коммутируемых сетей Cisco – 40 ак.часов
TSHOOT Разрешение проблем и поддержка IP сетей, построенных на основе оборудования Cisco – 40 ак.часов
SPROUTE Развертывание протоколов маршрутизации в сетях сервис провайдеров построенных на оборудование компании Cisco – 40 ак.часов
IINS Обеспечение сетевой безопасности средствами Cisco IOS – 40 ак.часов
SENSS Внедрение решений Cisco по обеспечению безопасности периметра сети – 40 ак.часов
EDU-JUN-JSE Основы работы с системой Junos Space – 16 ак.часов
EDU-JUN-ERX Основы работы с маршрутизаторами E-серии – 8 ак.часов
EDU-JUN-BB Конфигурирование BRAS на маршрутизаторах E-серии – 32 ак.часа
EDU-JUN-JSPX Коммутация в сетях интернет-сервис провайдеров -16 ак.часов
EDU-JUN-JCOS Классы обслуживания в JunOS 16 ак.часов
EDU-JUN-JMV Технологии MPLS и VPN в JUNOS - 40 ак.часов
EDU-JUN-JMR Мультикастная маршрутизация в JUNOS – 16 ак.часов
EDU-JUN-AJSPR Продвинутая маршрутизация JUNOS в сети провайдера – 32 ак.часа
EDU-JUN-IPV6Работа с IPV6 в Junos – 16 ак.часов
EDU-JUN-JAUT Автоматизация Junos – 16 ак.часов
EDU-JUN-JSEC Операционная система JUNOS для устройств безопасности (SRX и J-Series) - 24 ак.часов
EDU-JUN-CJFV Основы конфигурирования межсетевых экранов / концентраторов IPSEC VPN Juniper -24 ак.часа
EDU-JUN-CJSA Конфигурирование безопасного удаленного доступа для платформ Juniper Secure Access – 16 ак.часов
ADVANCED-IPS Управление системами предотвращения вторжений CheckPointAdvanced IPS – 16 ак.часов
CCES-R80 Внедрение системы защиты безопасности информации при помощи CheckPointEndpointSecurity R80 - 24 ак.часа
CCSA-R77 Администрирование Check Point Certified Security Administrator R77 – 24 ак.часа
БТ01 Безопасность информационных технологий – 40 ак.часов
БТ02 Защита конфиденциальной информации от утечки по техническим каналам – 40 ак.часов
КП32 Защита персональных данных – 16 ак.часов
КП33 Техническая защита персональных данных - 24 ак.часа
КП35 Регулирование отношений при осуществлении проверок операторов персональных данных – 8 ак.часов
БТ03 Безопасность компьютерных сетей - 32 ак.часа
БТ05 Основы TCP/IP – 8 ак.часов
Т010 Использование электронной подписи и развертывание PKI на основе Удостоверяющего центра КриптоПро – 40 ак.часов
Т024 Инфраструктура открытых ключей на Windows Server 2008 R2 – 8 ак.часов

Тема 3: Принципы системной интеграции

В рамках третьей темы изучаются вопросы построения унифицированных сетей для передачи голосовых, цифровых и мультимедийных данных, создания интеграционных решений, построения инфраструктуры центров обработки данных, облачные и виртуализационные решения, принципы построения гетерогенных систем и сетей.

Для прохождения обучения по Теме 3 «Принципы системной интеграции» слушатель должен успешно завершить обучение на одном или нескольких учебных курсах (дисциплинах) из следующего списка общей продолжительностью не менее 40 академических часов:

ARCH Проектирование сервисной архитектуры сети Cisco) – 40 ак.часов
DESGN Дизайн распределённых сетей Cisco – 40 ак.часов
COMM Введение в Cisco Unified Communications – 40 ак.часов
CVOICE Голосовые коммуникации и качество обслуживания в сетях Cisco – 40 ак.часов
CIPT1 Реализация решений Cisco Unified Communications. Часть 1 – 40 ак.часов
CIPT2 Реализация решений Cisco Unified Communications. Часть 2 – 40 ак.часов
TVOICE Решение проблем в системах унифицированных взаимодействий Cisco – 40 ак.часов
EDU-JUN-DCD Центр обработки данных - оптимальный дизайн – 24 ак.часа
AV101Базовое администрирование АТС Avaya Aura Communication Manager – 40 ак.часов
AV102 Углубленное администрирование АТС Avaya Aura Communication Manager, поиск и устранение неисправностей – 40 ак.часов
AV201Установка и администрирование медиасерверов и шлюзов Avaya Aura Communication Manager – 40 ак.часов
AV401 Установка и администрирование системы Avaya IP-DECT – 16 ак.часов
AV601 Установка и администрирование Avaya IP Office – 24 ак.часа
AV801 Avaya Aura Session Manager И протокол SIP. Базовое администрирование – 32так.часа
CXD-203-3I Управление решениями на базе Citrix XenDesktop 7 – 40 академических часов
CBR-201-1 Администрирование Citrix Branch Repeater 6.0 – 16-академических часов
CXA-206I Администрирование Citrix XenApp 6.5 – 40 академических часов
CXA-301I Углубленное администрирование Citrix XenApp 6.5 – 40 академических часов
CMB-207I Citrix XenApp и XenDesktop - Ускоренный курс – 40 академических часов
CXD-300-4I Внедрение решений на базе Citrix XenDesktop 7 – 40 академических часов
CXD-202I Администрирование Citrix XenDesktop 5– 40 академических часов
CXD-400 Проектирование решений на базе Citrix XenDesktop – 40-академических часов
CXS-203 IАдминистрирование Citrix XenServer 6.0 – 40 академических часов
CNS-205I Основы и сетевая архитектура Citrix NetScaler 10 – 40 академических часов
CVA-500I Построение виртуальных решений на базе Citrix – 40-академических часов
VS5-DW Проектирование решений на основе VMware vSphere – 24 ак.часа
VS5.5-TR Решение проблем в среде VMware vSphere 5.5 – 40 ак.часов
VI5.5-SRM Установка, настройка и использование VMware vCenter Site Recovery Manager [V5.5] – 16 ак.часов
VICM5.2 VMware Horizon View: Установка, настройка и использование – 32 ак.часа
VV5.1-DBP Рекомендации по разработке решений на основе архитектуры VMware View V5.1 – 24 ак.часа

Календарный учебный график

Учебный год: круглогодичное обучение.
Продолжительность Программы: 120 академических часов.
Сменность занятий (при очной форме обучения): I смена.
Количество учебных дней в неделю при очном обучении: 5 дней.
Форма организации образовательного процесса: очное обучение по мере комплектования групп, заочное обучение, дистанционное обучение.
Начало учебных занятий: 9.00
Окончание учебных занятий: 17.00
Продолжительность урока: 1 час 30 минут (2 академических часа).
Продолжительность перемен: 30 минут, перерыв на обед – 60 минут.
Расписание занятий для очных групп:

	№ урока	**Время**
Конкретный день недели согласовывается во время учебного процесса	1	09:00 - 10:30
	2	11:00 - 12:30
	3	13:30 - 15:00
	4	15:60 - 17:00

Организационно-педагогические условия реализации Программы

При реализации Программы применяется форма организации образовательной деятельности, основанная на модульном принципе представления содержания образовательной программы и построения учебных планов, использовании различных образовательных технологий, в том числе дистанционных образовательных технологий и электронного обучения. Каждый модуль соответствует отдельному учебному курсу (дисциплине) Программы. При этом модули сгруппированы по учебным курсам (темам) с целью обеспечить комплексную подготовку слушателей в необходимом для достижения целей Программы объеме.

Учебные материалы по каждому курсу (дисциплине) Программы включают: рабочую программу, раздаточные материалы по курсу, методические материалы по курсу, данные примеров по курсу. Учебное пособие по каждому курсу выдается слушателям в бумажном или электронном виде в зависимости от специфики курса и формы обучения. Выдача учебных пособий регламентируется внутренними нормативными актами Учебного центра.

Занятия по каждому курсу (дисциплине), входящему в состав Программы, проводятся преподавателями, предварительно подтвердившими свою квалификацию в объеме, достаточном для рабочей программы соответствующего курса. В числе базовых требований ко всем преподавателям – требование обязательного прохождения программы «Train the Trainer» в форме учебного курса и пробной лекции, а также сдачи технических сертификационных тестов по продукту или технологии, рассматриваемым в курсе.

Обучение в очной форме проводится в учебных компьютерных классах, оборудованных персональными компьютерами на каждом рабочем месте слушателя, подключенными к локальной сети Учебного центра с доступом в интернет. Дополнительно учебный класс оборудуется персональным компьютером на рабочем месте преподавателя с подключенным к

нему проектором. В зависимости от специфики курса в учебном классе устанавливается необходимое программное обеспечение и/или оборудование.

Оценочные материалы и формы аттестации

Итоговая аттестация по Программе состоит из комплекса экзаменов по каждому учебному курсу (дисциплине) Программы. В случае обучения по индивидуальному учебному плану слушатель сдает только экзамены по учебным курсам (дисциплинам), которые включены в его индивидуальный учебный план.

Итоговая аттестация слушателей проводится в соответствии с “Положением о порядке проведения учебных занятий, текущей, промежуточной и итоговой аттестаций слушателей АНО ДПО "Сетевая Академия ЛАНИТ-ТИССА".

Экзамен по каждому учебному курсу (дисциплине) Программы проводится в форме тестирования. Тестирование может проводиться в электронном виде с использованием дистанционных образовательных технологий.

Для проведения экзамена по каждому учебному курсу (дисциплине) Программы разрабатываются оценочные материалы в форме теста. Оценочные материалы разрабатываются с учетом методических требований, установленных НОУ УЦ «Сетевая академия».

В случае успешной сдачи экзамена по отдельному учебному курсу (дисциплине) слушателю выдается сертификат о прохождении обучения по данному курсу по образцу, который установлен НОУ УЦ «Сетевая академия».

В случае успешного прохождения итоговой аттестации, т.е. успешной сдачи экзаменов по всем учебным курсам (дисциплинам) Программы, слушатель получает удостоверение о повышении квалификации. В случае неуспешного прохождения итоговой аттестации слушатель получает справку о прохождении обучения по данной Программе.

Рабочие программы учебных курсов (дисциплин)

Рабочая программа курса
ICND1 Использование сетевого оборудования Cisco (часть I)

Целью курса является обеспечение слушателей необходимыми знаниями и умениями для инсталляции, настройки и обслуживания сетей малого и среднего размера.

Предварительная подготовка слушателя:
Слушатель должен иметь:

- общее знакомство с компьютером;
- базовые навыки работы в Windows;
- базовые навыки навигации в сети Интернет;
- базовые навыки использования электронной почты.

Планируемые результаты обучения:
Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.
После изучения курса слушатель сможет:

- Описывать основы сетевых технологий и строить простые сети
- Соединять локальные сети с сетью Internet
- Управлять безопасностью сетевых устройств
- Расширять сети малого и среднего размера с помощью WAN-технологий
- Описывать основы работы протокола IPv6

Продолжительность курса: 40 академических часов (5 дней)

Содержание:

Тема 1. Построение простой сети
Описание функций сети
Модель взаимодействия устройств сети
Введение в локальные сети
Операционная система Cisco IOS
Базовая конфигурация коммутатора
Принципы работы технологии Ethernet
Устранение базовых проблем работы коммутатора
Практическое занятие: Загрузка и начальная конфигурация коммутатора
Практическое занятие: Устранение неисправностей работы коммутатора

Тема 2. Интернет-соединения
Понимание межсетевого уровня стека TCP/IP
IP-адресация и подсети
Понимание транспортного уровня стека TCP/IP
Описание функций маршрутизации
Базовая конфигурация маршрутизатора
Описание процесса доставки пакетов
Статическая маршрутизация
Управление трафиком с использованием ACL
Соединение локальной сети с сетью Internet
Практическое занятие: Загрузка и начальная конфигурация маршрутизатора
Практическое занятие: Соединение с Internet

Тема 3. Управление безопасностью сетевых устройств
Защита доступа к устройствам
Технологии безопасности устройств Cisco
Фильтрация трафика с использованием ACL
Практическое занятие: Настройка защищенного доступа к устройствам
Практическое занятие: Настройка технологии безопасности на устройствах Cisco
Практическое занятие: Фильтрация трафика с помощью ACL

Тема 4. Построение сети среднего размера
Технологии VLAN и Trunk Маршрутизация между VLAN
Настройка DHCP-сервера на устройствах Cisco
Введение в WAN-технологии
Протоколы динамической маршрутизации
Конфигурация протокола OSPF
Практическое занятие: Настройка коммутируемой сети среднего размера
*Практическое занят*ие: Настройка DCHP-сервера
Практическое занятие: Настройка протокола OSPF

Тема 5. Введение в IPv6
Введение в основы протокола IPv6
Понимание принципов работы IPv6

Конфигурация IPv6-маршрутизации
Практическое занятие: Базовая конфигурация IPv6 на маршрутизаторе Cisco
Практическое занятие: Настройка Stateless Autoconfiguration
Практическое занятие: Настройка IPv6-маршрутизации

Рабочая программа курса
ICND2 Использование сетевого оборудования Cisco (часть II)

Целью курса является обеспечение слушателей необходимыми знаниями и умениями для установки, настройки и обслуживания сетей среднего размера, включая технологии WAN и технологии сетевой безопасности.
По окончании данного курса слушатель сможет конфигурировать, анализировать и устранять неисправности работы различных устройств Cisco

Предварительная подготовка слушателя:
Обязательное требование: иметь знания в полном объеме курса ICND1 Использование сетевого оборудования Cisco (часть I)
Понимание основ работы сетевых технологий
Базовые умения настройки локальной сети с помощью оборудования Cisco
Базовые умения настройки Internet-соединений с помощью оборудования Cisco
Базовые умения настройки технологий безопасности на устройствах Cisco
Базовые умения настройки WAN-соединений
Базовые умения настройки протокола IPv6

Планируемые результаты обучения:
Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель сможет:
Настраивать маршрутизаторы и коммутаторы Cisco
Обнаруживать и устранять неисправности работы устройств Cisco

Продолжительность курса: 40 академических часов (5 дней)

Содержание:
Тема 1. Внедрение масштабируемых сетей среднего размера
Устранение неисправностей работы технологий VLAN и Trunk
Построение избыточных коммутируемых топологий
Улучшение характеристик работы избыточных коммутируемых топологий с помощью технологии EtherChannel
Понимание избыточности на третьем уровне модели OSI
Практическое занятие: Устранение неисправностей работы технологий VLAN и Trunk
Практическое занятие: Оптимизация протокола STP *Практическое занятие*: Конфигурация EtherChannel
Тема 2. Устранение базовых неисправностей работы сети
Устранение базовых неисправностей работы IPv4-соединений

Устранение базовых неисправностей работы IPv6-соединений
Практическое занятие: Устранение неисправностей IP-соединений

Тема 3. Внедрение решения на основе протокола EIGRP

Внедрение протокола EIGRP в IPv4-сети
Устранение неисправностей работы протокола EIGRP Внедрение протокола EIGRP в IPv6-сети
Практическое занятие: Конфигурация протокола EIGRP
Практическое занятие: Устранение неисправностей работы протокола EIGRP
Практическое занятие: Конфигурация протокола EIGRP для IPv6

Тема 4. Внедрение масштабируемого решения на основе протокола OSPF для нескольких областей

Обзор протокола OSPF
Внедрение протокола OSPF для нескольких областей в IPv4-сетях
Устранение неисправностей работы протокола OSPF Введение в OSPFv3
Практическое занятие: Конфигурация протокола OSPF для работы в нескольких областях
Практическое занятие: Устранение неисправностей работы протокола OSPF в нескольких областях
Практическое занятие: Конфигурация протокола OSPF для IPv6

Тема 5. Глобальные сети (WAN)

Понимание WAN-технологий
Конфигурация WAN-соединений «точка-точка»
Настройки WAN-соединений с использованием технологии Frame Relay
Введение в виртуальные частные сети (VPN) Конфигурация GRE-туннелей
Практическое занятие: Конфигурация и устранение неисправностей работы WAN-соединений «точка-точка»
Практическое занятие: Конфигурация Frame Relay WAN
Практическое занятие: Конфигурация GRE-туннелирования

Тема 6. Управление сетевыми устройствами

Конфигурация протоколов управления сетью на устройствах Cisco
Управление устройствами Cisco
Лицензирование
Практическое занятие: Базовая конфигурация протоколов SNMP и Syslog
Практическое занятие: Анализ данных протокола NetFlow
Практическое занятие: Управление устройствами Cisco и лицензиями
Финальное практическое занятие

Рабочая программа курса
ROUTE Маршрутизация в IP-сетях Cisco

Курс ROUTE предназначен для сетевых инженеров с опытом работы не менее одного года, готовых к улучшению своих навыков и к независимой работе со сложными сетевыми решениями. Слушатели научатся планировать, конфигурировать и проверять работу корпоративных LAN и WAN сетей с использованием различных протоколов маршрутизации. В материалы курса также входят темы, посвященные конфигурированию решений по поддержке удаленных офисов и мобильных пользователей.

Предварительная подготовка слушателя:

Приступая к изучению курса, слушатели должны иметь знания и навыки, позволяющие:
конфигурировать маршрутизаторы Cisco в объеме курса ICND;
настраивать стек протоколов TCP/IP;

разбивать сети на подсети с использованием масок переменной длины (VLSM);
конфигурировать протоколы маршрутизации RIP, EIGRP, OSPF в одной области;
создавать списки контроля доступа.

Планируемые результаты обучения:
Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель сможет:

понимать особенности функционирования Advanced Distance Vector и Link-state протоколов маршрутизации, сравнивать протоколы RIPv1, RIPv2, EIGRP, OSPF, BGP;
использовать подсети с переменной длиной маски (VLSM), иерархическую адресацию, суммаризацию, CIDR;
настраивать RIPv2 в больших сетях;
конфигурировать протокол маршрутизации OSPF для работы в нескольких областях в сетях множественного доступа, как поддерживающих, так и не поддерживающих широковещание (NBMA), а также на последовательных линиях точка-точка;
создавать Stub, Totally stubby и NSSA-области, использовать Virtual links, настраивать суммаризацию в протоколе OSPF;
конфигурировать протокол маршрутизации EIGRP, настраивать суммаризацию, балансировку трафика по параллельным маршрутам в EIGRP, ограничивать потребляемую EIGRP пропускную способность канала связи;
конфигурировать протокол маршрутизации BGP, понимать особенности конфигурации BGP в больших сетях, настраивать BGP в сетях с выходом на двух и более провайдеров (Multihoming);
обеспечивать редистрибуцию маршрутов между различными протоколами маршрутизации;
контролировать распространение сообщений протоколов маршрутизации;
настраивать Policy-based routing.

Продолжительность курса: 40 академических часов (5 дней)

Содержание:

Планирование сервисов маршрутизации (2 а.ч.) Применение решений на основе протокола EIGRP (12 а.ч.)
Применение масштабируемых решений на основе OSPF с использованием нескольких зон (14 а.ч.)
Применение решений, связанных с перераспределением IPv4 маршрутов (4 а.ч.)
Подключение корпоративных сетей к сетям провайдеров (8 а.ч.)

Рабочая программа курса¶
SPROUTE Развертывание протоколов маршрутизации в сетях сервис провайдеров построенных на оборудование компании Cisco

Курс SPROUTE разработан для предоставления информации по использованию расширенного функционала по маршрутизации и поддержки масштабируемости на маршрутизаторах Cisco, подключенных к локальным и глобальным сетям. Курс также включает лабораторные работы, позволяющие получить практический опыт настройки и закрепить полученный знания протоколов маршрутизации на устройствах с операционными системами Cisco IOS / IOS XE и Cisco IOS XR необходимых для поддержки расширенной маршрутизации в сетях сервис провайдеров

Предварительная подготовка слушателя:
Слушатели данного курса должны иметь опыт конфигурирования маршрутизаторов Cisco и выполнить следующие предварительные требования:

Обладать опытом и знаниями эквивалентными содержанию курсу ICND1;
Обладать опытом и знаниями эквивалентными содержанию курсу ICND2

Планируемые результаты обучения:
Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель сможет:

Планировать, внедрять и поддерживать маршрутизацию в сетях сервис провайдеров.

Продолжительность курса: 40 академических часов (5 дней)
Содержание:

Тема 1 - Маршрутизация в сетях сервис провайдеров
Изучения протоколов маршрутизации используемых в сетях сервис провайдеров
Тема 2 - Применение протокола OSPF в сетях сервис провайдеров
Введение в протокол OSPF Работа OSPF
Применение OSPF
Применение специализированных типов зон в протоколе OSPF
Тема 3 - Применение протокола IS-IS в сетях сервис провайдеров
Введение в протокол IS-IS
Применение IS-IS
Тема 4 - Применение протокола BGP в сетях сервис провайдеров
Введение в протокол BGP
Применение базовой BGP маршрутизации
Тема 5 - Инструменты управления протоколами маршрутизации и манипуляцией маршрутов
Обзор инструментов управления маршрутами Применение редистрибьюции маршрутов
Управление выбором BGP маршрутов

Рабочая программа курса¶
SWITCH Внедрение коммутируемых сетей Cisco

Данный курс специально разработан, чтобы научить инженеров планировать, конфигурировать и внедрять комплексные решения по коммутации, используя модель архитектуры кампуса предприятия Cisco (Cisco Enterprise Campus Architecture). Курс посвящен вопросам построения локальных сетей с использованием механизмов коммутации 2-го, 3-го и 4-го уровней, реализованных в коммутаторах Cisco Catalyst, и предназначен для сетевых администраторов, имеющих опыт работы с коммутаторами Catalyst. Для большей наглядности курс снабжен практическими лабораторными работами.

Предварительная подготовка слушателя:
Необходимо уметь конфигурировать маршрутизаторы и коммутаторы Cisco в объеме курсов ICND1 и ICND2.

Планируемые результаты обучения:
Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель сможет: Анализировать дизайн кампусной сети. Внедрять VLAN в сеть кампуса. Использовать протокол Spanning Tree. Использовать маршрутизацию между VLAN. Строить отказоустойчивые сети.
Использовать технику и технологии отказоустойчивости намаршрутизирующих коммутаторах кампусной сети.

Использовать механизмы безопасности в коммутируемых сетях. Интегрировать беспроводные сети в кампусную сеть.
Настраивать передачу голосового и видео трафика в кампусных сетях.

Продолжительность курса: 40 академических часов (5 дней)

Содержание:

Анализ дизайна кампусной сети Внедрение VLAN в кампусных сетях Внедрение Spanning Tree
Внедрение маршрутизации между VLAN Внедрение высокой доступности в сети Внедрение высокой доступности на 3 уровне
Минимизация потери услуг и кражи данных в кампусных сетях Внедрение голосового и видео трафика в кампусных сетях Интегрирование беспроводных сетей LAN в кампусную сеть

Рабочая программа курса¶
TSHOOT Разрешение проблем и поддержка IP сетей, построенных на основе оборудования Cisco

Курс знакомит слушателей с различными видами неисправностей в сетях передачи данных, построенных на оборудовании Cisco, а также методами их обнаружения и устранения.

Предварительная подготовка слушателя:
Рекомендуется иметь практический опыт инсталляции, конфигурирования и поддержания в рабочем состоянии маршрутизаторов и коммутаторов Cisco в сети масштаба предприятия
Необходимо прослушать курсы ICND1, ICND2, ROUTE, SWITCH или эквивалентный опыт практической работы;

Планируемые результаты обучения:
Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель сможет:

Планировать и документировать часто выполняемые функции по поддержанию в работоспособном состоянии сложной сети предприятия.

Разрабатывать план мероприятий по поиску и устранению проблем в сложной сети предприятия.

Выбирать инструменты лучше всего подходящие для выполнения процессов поддержания сети в рабочем состоянии, а также для поиска и устранения неисправностей в больших сетях предприятий.

Применять на практике процедуры поддержания сети в рабочем состоянии, а также устранения отказов в локальных коммутируемых сетях.

Применять на практике процедуры поддержания сети в рабочем состоянии, а также устранения отказов в маршутизируемых сетях.

Применять на практике процедуры поддержания сети в рабочем состоянии, а также устранения отказов в инфраструктуре, обеспечивающей безопасность.

Применять на практике процедуры поддержания сети в рабочем состоянии, а также устранения отказов в сложных сетях.

Продолжительность курса: 40 академических часов (5 дней)

Содержание:

Планирование поддержки для сложных сетей
Выбор приложений и инструментов для осуществления обслуживания сетей и разрешения проблем
Планирование процесса разрешения проблем для корпоративных сетей.
Разрешение проблем, связанных с коммутируемой инфраструктурой в кампусных сетях

Разрешение проблем, связанных с маршрутизируемой инфраструктурой в корпоративных сетях.
Разрешение проблем и обслуживание инфраструктуры сетевой безопасности.
Обслуживание и разрешение проблем в сложных сетевых инфраструктурах

Рабочая программа курса
ARCH Проектирование сервисной архитектуры сети Cisco (v2.1)

Данный курс позволяет слушателям научиться применять проверенные модели сетевых решений Cisco и рекомендуемые методы проектирования для создания жизнеспособных, стабильных решений для корпоративных вычислительных сетей.

В курсе представлены базовые концепции и примеры из практики, которые могут быть использованы при проектировании конвергированных мультисервисных сетей предприятия. Также рассматриваются продвинутые сетевые технологии, такие как VPN, и другие решения, направленные на обеспечение безопасности.

Занятия включают в себя лекционную и лабораторную части.

Предварительная подготовка слушателя:
Прохождение курса Interconnecting Cisco Network Devices 1 (ICND1); Прохождение курса Interconnecting Cisco Network Devices 2 (ICND2); Прохождение курса Implementing Cisco IP Switched Networks (SWITCH) Прохождение курса Implementing Cisco IP Routing (ROUTE)
Хорошее знание сетевых технологий, линейки изделий Cisco и функций Cisco IOS.

Планируемые результаты обучения:
Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель сможет:
представлять Корпоративную Сетевую Архитектуру Cisco и объяснять, как эта концепция удовлетворяет сетевые потребности компании в плане производительности, масштабируемости и доступности;
описывать то, как Корпоративная Сетевая Архитектура Cisco может быть использована в качестве "скелета" для проектируемой сети предприятия;
создавать концептуальные, промежуточные и детальные проекты сетевой инфраструктуры кампуса;
создавать концептуальные, промежуточные и детальные проекты сети центра обработки данных;
создавать концептуальные, промежуточные и детальные проекты сети границы предприятия и удаленного доступа;
создавать концептуальные, промежуточные и детальные проекты безопасности сетевых сервисов;
создавать концептуальные, промежуточные и детальные проекты виртуальных частных сетей (VPN).

Продолжительность курса: 40 академических часов (5 дней)

Содержание:

Корпоративная Сетевая Архитектура Cisco. Проектирование сетевой инфраструктуры кампуса. Проектирование расширенной схемы адресации и маршрутизации. Вопросы проектирования продвинутых сервисов WAN. Проектирование сети центра обработки данных.

Проектирование модуля электронной коммерции. Вопросы проектирования сети хранения данных (SAN). Проектирование безопасности сетевых сервисов. Проектирование IPsec и SSLVPN.

Проектирование IP Multicast.

Возможности сетевого администрирования Cisco IOS.

Рабочая программа курса¶
DESGN Дизайн распределённых сетей Cisco (v2.1)

Курс нацелен на получение сетевыми специалистами знаний и развитие базовых навыков, необходимых для того, чтобы начать работать над проектированием вычислительных сетей или оказывать помощь более опытному сетевому проектировщику.

Темы курса включают проектирование маршрутизируемой или коммутируемой сетевой инфраструктуры и сетевых сервисов с применением технологий локальных, глобальных вычислительных сетей и широкополосного удаленного доступа. Также рассматриваются вопросы виртуализации сервисов.

Композитная модель сети предприятия, на которой сфокусирован курс, определяет фазы жизненного цикла системы (PPDIOO) и позволяет создавать модульный дизайн мультисервисной сети, который обладает свойствами масштабируемости, отказоустойчивости, безопасности, простоты локализации и устранения проблем.

Занятия включают в себя лекционную и лабораторную части.

Предварительная подготовка слушателя:

Прохождение курса Interconnecting Cisco Network Devices 1 (ICND1);

Прохождение курса Interconnecting Cisco Network Devices 2 (ICND2);

Практический опыт работы с оборудованием Cisco и операционной системой Cisco IOS.

Прохождение курса Implementing Cisco IP Switched Networks (SWITCH)

Планируемые результаты обучения:

Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель сможет:

обсуждать методологию проектирования сетей;

описывать, как концепция Дизайна Корпоративной Архитектуры Cisco позволяет структурировать сети модулей кампуса предприятия и центра обработки данных;

проектировать модули Удаленного Подключения;

разрабатывать план сетевой адресации и выбирать подходящий протокол маршрутизации;

оценивать решения по безопасности сети;

обсуждать влияние принимаемых решений на передачу голоса по сети;
обсуждать влияние принимаемых решений на беспроводную связь.

Продолжительность курса: 40 академических часов (5 дней)

Содержание:
Применение методологии к проектированию сети. Структурирование и модуляризация сети.
Базовое проектирование сетей кампуса и центра обработки данных. Проектирование решений по удаленному подключению. Планирование IP-адресации и выбор протокола маршрутизации. Оценка принимаемых решений по безопасности в сети.
Учет специфики передачи голоса в сети.
Учет специфики беспроводных подключений в сети. Внедрение и сопровождение сетевого проекта.

Рабочая программа курса¶
IINS Обеспечение сетевой безопасности средствами Cisco IOS

Курс "Обеспечение сетевой безопасности средствами Cisco IOS (v2.0)" акцентирует внимание слушателей на важности глубокого понимания политик безопасности и их влияния на состояние сети. Курс дает базовые знания и навыки, необходимые для конфигурации защитных функций, эксплуатации и управления устройствами Cisco. Слушатели будут способны обеспечить безопасность сети небольшого филиала компании путём использования средств безопасности доступных через Веб-интерфейс (Cisco Security Device Manager) и интерфейс командной строки на маршрутизаторах и коммутаторах Cisco.

Предварительная подготовка слушателя:
Прохождение курса Interconnecting Cisco Networking Devices Part 1 (ICND1) или наличие эквивалентных знаний и навыков
Навыки работы с операционной системой Windows

Планируемые результаты обучения:
Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель сможет:
Разрабатывать комплексную политику сетевой безопасности для противодействия угрозам информационной безопасности
Настраивать маршрутизаторы периметра сети, используя средства безопасности операционной системы Cisco IOS
Настраивать как классический межсетевой экран, так и межсетевой экран, основанный на политиках зон для обеспечения базовой безопасности в сети
Настраивать статические (site-to-site) VPN соединения, используя средства Cisco IOS на маршрутизаторах Cisco конфигурировать систему предотвращения вторжений (IPS)
Конфигурировать устройства локальной сети для контроля доступа, сопротивления атакам, защиты других сетевых устройств и систем, а также поддержки целостности и

конфиденциальности сетевого трафика

Продолжительность курса: 40 академических часов (5 дней)

Содержание:
Тема 1 – Введение в принципы сетевой безопасности Рассмотрение основ сетевой безопасности Анализ методик сетевых атак
Рассмотрение основных процедур для обеспечения безопасности Разработка детальной политики сетевой безопасности Построение самозащищающихся сетей
Тема 2 - Защита периметра
Обеспечение безопасности административного доступа к маршрутизаторам Cisco
Введение в Cisco SDM
Настройка функций AAA на маршрутизаторах для работы с локальной базой
Настройка функций AAA на маршрутизаторах для использования Cisco Secure ACS
Внедрение безопасной системы управления и отчётов
Отключение ненужных сервисов на маршрутизаторе
Тема 3 - Обеспечение безопасности с помощью межсетевого экрана Cisco IOS
Введение в технологии межсетевых экранов
Создание статических пакетных фильтров с помощью списков управления доступом (ACL)
Настройка межсетевого экрана, основанного на политиках зон средствами Cisco IOS
Тема 4 - Статические VPN соединения Анализ криптографических сервисов
Рассмотрение симметричного шифрования
Изучение криптографических хэш-функций и цифровых подписей
Рассмотрение ассиметричного шифрования и инфраструктуры открытого ключа(PKI)
Изучение основ IPsec
Построение Site-to-Site IPsec VPN
Настройка Site-to-Site IPsec VPN с помощью Cisco SDM
Тема 5 - Защита сети с помощью программной системы предотвращения вторжений (IPS), встроенной в Cisco IOS
Введение в технологии IPS
Настройка Cisco IOS IPS с помощью Cisco SDM
Тема 6 - Обзор методов обеспечения безопасности в локальных сетях (LAN), сетях хранения данных (SAN), для голосового трафика и на конечных устройствах
Рассмотрение методов обеспечения безопасности на конечных устройствах
Обеспечение безопасности в сетях хранения данных Обеспечение безопасности передачи голосового трафика Противодействие атакам уровня 2

Рабочая программа курса¶
SENSS Внедрение решений Cisco по обеспечению безопасности периметра сети (Версия 1.0)

Данный курс поможет системным инженерам, специализирующихся на безопасности подготовиться к внедрению решения Cisco по защите периметра сети с использованием коммутаторов Cisco, маршрутизаторов Cisco и межсетевых экранов Cisco ASA. Основная цель курса - подготовить слушателей к внедрению решений, использующих Cisco ASA, маршрутизаторы с функциями межсетевого экранирования, а также коммутаторов Cisco. Слушатель получит практический опыт работы в настройке и конфигурировании различных

решений, обеспечивающих защиту периметра для предотвращения внешних угроз и контроля доменов безопасности. В конце курса слушатели смогут изучить, как снизить риск для своих IT-инфраструктур и приложений, с помощью коммутаторов Cisco, маршрутизаторов Cisco, Cisco ASA и оказывать оперативную техническую поддержку и управление этими продуктами.

Предварительная подготовка слушателя:
Слушатели данного расширенного курса должны иметь опыт конфигурирования устройств Cisco IOS и настоятельно рекомендуется иметь хорошее понимание тем курса IINS

Планируемые результаты обучения:
Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

По завершению данного курса, слушатели освоят:

Понимание и внедрение модульной архитектуры безопасности Cisco, таких как Secure и Trusses.
Развертывание управления и защиты Management plane
Настройка обеспечения безопасности на 2 и на 3 уровне модели OSI Внедрение и обслуживание технологии NAT на Cisco ASA
Внедрение и обслуживание технологии NAT на Cisco IOS устройствах
Разработка и разворачивание решений Cisco Threat Defense на Cisco ASA используя политики доступа и инспектирование на основе приложений и пользователей
Внедрение Botnet Traffic Filter
Разворачивание Cisco IOS Zone-Based Policy Firewall (ZBFW)
Настройка и проверка инспектирования на уровне приложений Cisco IOS ZBFW

Продолжительность курса: 40 академических часов (5 дней)

Содержание:

Тема 1 - Принципы дизайна безопасности Зоны сетевой безопасности Модульная архитектура сети Cisco Архитектура Cisco SecureX
Решение Cisco TrustSec
Тема 2 –Развертывание инфраструктуры сетевой безопасности
Введение в инфраструктуру сетевой безопасности
Развертывание защиты Control Plane устройств с операционной системой Cisco IOS
Развертывание защиты Management Plane устройств с операционной системой Cisco IOS
Развертывание защиты Management Plane устройств Cisco ASA Развертывание методов телеметрии Csico
Развертывание защиты Data Plane устройств канального Развертывание защиты Management Plane устройств сетевого уровня
Тема 3 - Внедрение технологии NAT на устройствах с Cisco IOS и ASA
Введение в трансляцию адресов

Развертывание трансляции адресов на Cisco ASA Развертывание трансляции адресов на Cisco IOS

Тема 4 - Развертывание средств защиты от угроз на Cisco ASA

Введение в межсетевое экранирование Cisco Внедрение основных политик доступа ASA Внедрение расширенных политик доступа ASA

Внедрение репутационных политик доступа ASA Внедрение политик идентификации ASA

Тема 5 - Развертывание средств защиты от угроз на Cisco IOS

Введение основных политик ZBF Cisco

Внедрение расширенных политик ZBF Cisco

Рабочая программа курса¶
CVOICE Голосовые коммуникации и качество обслуживания в сетях Cisco

Курс дает знания и навыки, необходимые для развертывания VoIP сетей и механизмов качества обслуживания в сетях Cisco.

Предварительная подготовка слушателя:

Практические знания основ и концепций компьютерных сетей (LAN, WAN), а также коммутации и маршрутизации IP

Базовые навыки организации структуры сетей, полученные на курсахICND (Interconnecting Cisco Network Devices) или эквивалентные знания

Умение настраивать маршрутизаторы и коммутаторы Cisco для реализации VLAN и DHCP

Понимание технологий и принципов работы коммутируемой телефонной сети общего пользования (PSTN)

Планируемые результаты обучения:

Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель сможет:

Понимать принципы, компоненты и механизмы работы голосовых шлюзов

Понимать и настраивать VoIP-плечи вызова

Внедрять Cisco Unified Communication Manager Express

Строить и адаптировать номерной план

Настраивать гейткиперы и Cisco Unified Border Element

Реализовывать механизмы качества обслуживания

Продолжительность курса: 40 академических часов (5 дней)

Содержание:

Тема 1 –Введение в голосовые шлюзы Cisco

Унифицированные коммуникации Cisco и роль шлюзов

Маршрутизация вызовов средствами шлюзов

Настройка голосовых портов

DSP-ресурсы, кодеки

Тема 2 – «Плечи» вызовов
Характеристики «плеча» вызова и передачи голосового трафика
Протокол сигнализации H.323
Протокол сигнализации SIP Протокол сигнализации MGCP Требования к «плечам» вызова
Настройка «плеча» вызова
Тема3 –Внедрение CUCME
Введение в CUCME
Требования CUCME к конечным устройствам
Настройка конечных устройств CUCME
Тема 4 –Построение номерного плана Введение в маршрутизацию вызовов Понимание номерного плана Манипуляции с цифрами
Выбор пути прохождения вызовов
Привилегии
Тема5 –Внедрение Гейткиперов и CUBE
Понимание Гейткипера
Работа CUBE
Тема 6 –Качество обслуживания
Введение в QOS
Понимание механизмов и моделей QOS
Классификация, маркировка и механизмы эффективного использования линков
Управление заторами
Понимание Cisco AutoQoS

Рабочая программа курса¶
CIPT1 Реализация решений Cisco Unified Communications.Часть 1

CIPT1 v8.0 - 5-дневный курс с лабораторными упражнениями. Курс дает знания и навыки, необходимые для развертывания сетей IP-телефонии на базе CUCM.

Предварительная подготовка слушателя:

Слушатели данного расширенного курса должны иметь опыт конфигурирования устройств
Cisco IOS и выполнить следующие предварительные требования
Знания основ компьютерных сетей
Опыт настройки коммутаторов Cisco (VLAN, DHCP)
Понимать основы работы цифровых интерфейсов, ТФОП, VOIP Базовые знания в области конвергированных сетей
Опыт настройки голосовых шлюзов Cisco

Планируемые результаты обучения:

Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель сможет:

Понимать функционал и архитектуры развертывания CUCM Выполнять начальную настройку CUCM
Настраивать обработку вызовов в рамках одной площадки Строить номерной план и подключаться к ТФОП Управлять медиа-ресурсами

Реализовывать дополнительные сервисы CUCM

Продолжительность курса: 40 академических часов (5 дней)

Содержание:
Тема1 –Введение в Cisco Unified Communications ManagerПонимание архитектуры CUCM Модели развертывания CUCM
Тема2 –Администрирование Unified Communications Manager Управление сервисами и начальная конфигурация CUCM Управление пользователями CUCM
Тема 3 –Звонки в рамках одной площадки
Типы конечных устройств
IP-телефоны
Тема4 –Подключение к ТФОП
Взаимодействие CUCM с голосовыми шлюзами
Планы маршрутизации вызовов
Настройка компонентов маршрутизации вызовов Понимание манипуляций с цифрами
Использование Partition и CSS
Настройка манипуляций с цифрами
Выбор маршрута прохождения вызова
Выбор голосового шлюза для подключения к ТФОП Call Coverage в CUCM
Тема5 –Медиа-ресурсы.
Использование медиа-ресурсов в CUCM
Тема 6 –Дополнительные сервисы и приложения CUCM
Сервисы IP-телефонов Сервис Presence Сервис Mobility

Рабочая программа курса¶
CIPT2 Реализация решений Cisco Unified Communications.Часть 2

Курс дает знания и навыки, необходимые для развертывания сложных сетей IP-телефонии на базе CUCM
Предварительная подготовка слушателя:
Прохождение курса CIPT1 или наличие эквивалентных знаний и навыков.
Планируемые результаты обучения:

Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель сможет:
Понимать особенности развертывания CUCM для нескольких площадок
Выполнять настройку SRST Управлять полосой пропускания Настраивать функционал Mobility Настраивать CCD
Продолжительность курса: 40 академических часов (5 дней)

Содержание:
Тема 1 –Особенности развертывания CUCM на нескольких площадках Проблемы развертывания CUCM на нескольких площадках Варианты развертывания CUCM на нескольких площадках Подключение площадок

Разработка номерного плана для нескольких площадок

Тема 2 –Централизованная модель обработки вызовов с обеспечением избыточности

Варианты избыточности для удалённых площадок

Технологии SRST и MGCP Fallback

Работа CUCME в режиме SRST

Тема 3 –Управление полосой пропускания и контроль за доступом для голосовых вызовов

Управление полосой пропускания

Внедрение CAC

Тема4 –Внедрение Device Mobility и Cisco Extension Mobility

Внедрение Device Mobility

Внедрение Cisco Extension Mobility

Тема 5 –Развертывание CCD

Развертывание SAF и CCD

Рабочая программа курса¶
TVOICE Решение проблем в системах унифицированных взаимодействий Cisco (v8.0)

Курс дает знания и навыки, необходимые для решения проблем, возникающих в системах унифицированных взаимодействий Cisco

Предварительная подготовка слушателя:

Слушатели данного расширенного курса должны иметь опыт конфигурирования устройств Cisco IOS и выполнить следующие предварительные требования:

Иметь эквивалентный опыт работы курсам ICND1 и ICND2

Прослушать курс CVOICE v.8.0 или иметь эквивалентный опыт работы (знание протоколов и стандартов H.323, MGCP, SIP и их конфигурирование на голосовых шлюзах Cisco)

Прослушать курсы CIPT1 v.8.0 и CIPT2 v8.0 или иметь эквивалентный опыт работы (конфигурирование Cisco Unified Communications Manager (CUCM), приложений и дополнительных сервисов, голосовых шлюзов в пределах одного сайта (single-site) и нескольких сайтов (multisite))

Планируемые результаты обучения:

Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель сможет:

Использовать системную методологию решения проблем систем унифицированных сообщений Cisco, пользоваться знаниями инструментария и генераторов отчетности о проблемах в сети

Выявлять и решать проблемы, связанные с работой CUCM

Диагностировать проблемы, связанные с установлением соединений, и решать их, как только они обнаруживаются

Решать проблемы сетей, поддерживающих межкластерное взаимодействие SAF (Service Advertisement Framework) и CCD (Call Control Discovery) и сервисом CCD (Call Control Discovery)
Диагностировать и решать проблемы, связанные с приложениями и дополнительными сервисами CUCM

Выявлять и решать проблемы, связанные с качеством (QoS) передачи голоса
Выявлять и решать проблемы, связанные с работой медиа-ресурсов

Продолжительность курса: 40 академических часов (5 дней)

Содержание:
Тема 1 – Введение в методы поиска и устранения неисправностей в решениях унифицированных взаимодействий Cisco
Варианты организации сетей на базе решений унифицированных взаимодействий Cisco
Использование методологии для поиска и устранения неисправностей
Использование инструментов для мониторинга и обнаружения проблем
Тема 2 – Решение проблем, связанных с CUCM
Решение общих проблем связанных с регистрацией шлюзов и абонентов
Решение проблем доступности сервисов CUCM Решение проблем репликации базы данных
Решение проблем интеграции по LDAP
Тема 3 – Решение проблем организации соединения
Изучение проблем установления соединения и их причин
Решение проблем, связанных с установлением соединения внутри сайта
Решение проблем, связанных с установлением соединения между абонентами разных сайтов через IP-сеть
Решение проблем, связанных с установлением соединения с абонентом через ТфОП
Тема 4 – Решение проблем сервиса меж кластерного взаимодействия SAF (Service Advertisement Framework) и CCD (Call Control Discovery)
Решение проблем, связанных с работой SAF Client и SAF Forwarder
Решение проблем меж кластерного взаимодействия по динамическому обновлению планов нумерации (CCD)
Тема 5 – Решение проблем приложений и дополнительных сервисов CUCM
Решение проблем сервиса мобильности устройства
Решение проблем сервиса мобильности профиля пользователя Решение проблем сервиса универсальной мобильности Решение проблем сервиса Presence
Тема 6 – Решение проблем качества и медиа-ресурсов
Решение проблем проигрывания музыки в режиме ожидания
Решение проблем MTP
Решение проблем, связанных с конференциями Решение проблем, связанных с транскодерами Решение проблем, связанных с RSVP-агентами Решение проблем качества передачи голоса устройствами проводной сети в беспроводных локальных сетях

Рабочая программа курса
EDU-JUN-IJOS Основы работы с операционной системой JUNOS

Целью курса является обеспечение слушателей базовыми знаниями и навыками, необходимыми для настройки сетевых устройств (коммутаторов, маршрутизаторов, сетевых экранов), работающих под управлением операционной системы JUNOS

Предварительная подготовка слушателя:

Слушатель должен:

иметь базовые знания в области сетевых технологий, понимать модель OSI и стек протоколов TCP/IP

Планируемые результаты обучения:

Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель сможет:

Понимать архитектуру операционной системы JUNOS Знать устройства, работающие под управлением JUNOS Осуществлять навигацию по командной строке Заниматься конфигурированием и отладкой

Обновлять операционную систему

Управлять файловой системой и восстанавливать пароль

Продолжительность курса: 8 академических часов (1 день)

Содержание:

Тема 1. Основы операционной системы JUNOS

Операционная система Обработка трафика Обзор платформ

Тема 2.Пользовательский интерфейс

Возможности Командная строка WEB-интерфейс Лабораторная работа 1

Тема 3. Начальное конфигурирование Заводская конфигурация Начальная конфигурация Конфигурирование интерфейсов Лабораторная работа 2

Тема 4. Конфигурирование дополнительных параметров

Пользователи и аутентификация Системные лог-файлы и отладка Протокол NTP Архивирование конфигураций

Протокол SNMP Лабораторная работа 3

Тема 5. Мониторинг и обслуживание Мониторинг системы и интерфейсов Сетевые утилиты

Обслуживание Восстановление пароля Лабораторная работа 4

Рабочая программа курса
EDU-JUN-JRE Основы работы с протоколами маршрутизации в JUNOS

Целью курса является обучение слушателей основным принципам маршрутизации. Курс содержит обзор протоколов маршрутизации, примеры конфигураций с использованием маршрутных политик, пакетных фильтров и классов обслуживания трафика.

Предварительная подготовка:

Слушатель должен:

иметь базовые знания в области сетевых технологий, понимать модель OSI, стек протоколов TCP/IP,

знать принципы работы и конфигурирования операционной системы Junos в рамках курса Основы работы с Junos Software

Планируемые результаты обучения:
Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель сможет: Узнать базовые принципы маршрутизации
Ознакомиться с таблицами маршрутизации и форвардинга
Изучить статическую маршрутизацию Ознакомиться с протоколом OSPF Ознакомиться с политиками и фильтрами Понять RPF
Уметь настраивать и применять классы обслуживания трафика (CoS)

Продолжительность курса: 8 академических часов (1 день)

Содержание:
Тема 1. Основные принципы маршрутизации
Тема 2.Маршрутные политики и пакетные фильтры
Тема 3.Классы обслуживания (CoS)

Рабочая программа курса
EDU-JUN-JIR Настройка протоколов маршрутизации в операционной системе JUNOS

Целью курса является обеспечение слушателей знаниями и навыками по настройке протоколов маршрутизации в операционной системе JUNOS. Курс включает в себя обзор протокольно-независимых настроек, балансировку, маршрутизация на основе фильтров, OSPF, BGP, IP туннелирование и настройку параметров высокой доступности (high availability -HA)

Предварительная подготовка:
Слушатель должен:
иметь базовые знания в области передачи данных, а также знания по операционной системе JUNOS в рамках курсов Introduction to the Junos Operating System (IJOS) и Junos Routing Essentials (JRE)

Планируемые результаты обучения:
Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель сможет:
Настраивать статические, агрегированные и генерированные маршруты
Настраивать и использовать routing instances Конфигурировать балансировку маршрутов .
Конфигурировать маршрутизацию на основе фильтров Понимать логику работы OSPF.
Конфигурировать и отлаживать OSPF Понимать логику работы BGP Конфигурировать и настраивать BGP Понимать концепцию IP tunneling
Конфигурировать и отлаживать GRE и туннели IP-IP

Понимать и настраивать различные возможности высокой доступности (high availability)

Продолжительность курса: 16 академических часов (2 дня)

Содержание:

Тема 1. Протокольно-независимые настройки
•Статические маршруты
•Агрегированные и генерированные маршруты
•Routing Instances
•Лабораторная работа 1
Тема 2. Балансировка и маршрутизация на основе фильтров
•Обзор балансировки
•Конфигурирование и мониторинг балансировки
•Конфигурирование и мониторинг маршрутизации на основе фильтров
•Лабораторная работа 2
Тема3. Open Shortest Path First
•Обзор OSPF
•Формирование отношение и выборы DR
•Масштабируемость OSPF
•Конфигурирование и мониторинг OSPF
•Базовая отладка OSPF
•Лабораторная работа 3
Тема 4. Border Gateway Protocol
•Обзор BGP
•Атрибуты BGP
•IBGP против EBGP
•Конфигурирование и мониторинг BGP
•Лабораторная работа 4
Тема 5. IP Tunneling
•Обзор технологий туннелирования
•GRE и IP-IP Tunnels
•Внедрение GRE и IP-IP Tunnels
•Лабораторная работа 5
Тема 6. Высокая доступность
•Обзор сетей с высокой доступностью (High Availability Networks)
•Graseful Restart
•Graceful RE Switchover
•Безостановочная маршрутизация (Nonstop Active Routing)
•BFD
•VRRP
•Лабораторная работа 6

Рабочая программа курса
EDU-JUN-ERX Основы работы с маршрутизаторами E-серии

Целью курса является обеспечение слушателей начальными знаниями, необходимыми для работы с маршрутизаторами E-серии (ERX). В курсе рассматриваются возможности, применение и архитектура ERX-платформ. Кроме того, в курсе дается краткий обзор командной строки операционной системы JUNOSe. Курс знакомит слушателей с базовыми операциями и начальным конфигурированием маршрутизаторов E-серии. Также в курсе

рассматривается концепция виртуальных маршрутизаторов и базовые операции по их конфигурированию.

Предварительная подготовка:
Слушатель должен:
обладать общими знаниями о стеке протоколов TCP/IP, адресации и принципах маршрутизации в Интернете.

Продолжительность курса: 8 академических часов (1 день)
Содержание:

- **Тема 1. Обзор маршрутизаторов E-серии**
  - Линейка маршрутизаторов Juniper Networks
  - Применение E-серии (BRAS)
  - Система SDX-300 (Policy and Network Management System)
  - Система SRC (Session and Resource Control)
- **Тема2. Внутренняя архитектура маршрутизаторов E-серии**
  - Линейка и типы шасси
  - Архитектура ERX-14xx/7xx/310
  - Архитектура E320
  - Движение пакетов
  - Аппаратное резервирование
  - Инсталляция
- **Тема3. Введение в интерфейс командной строки и базовое конфигурирование**
  - Режимы командной строки
  - Базовые операции
  - Скрипты и макросы
  - Загрузка и перезагрузка
- **Тема4. Виртуализация, виртуальные маршрутизаторы**
  - Концепция виртуализации
  - Конфигурирование и управление виртуальными маршрутизаторами
  - Лабораторная работа 1. Знакомство с режимом командной строки
  - Лабораторная работа 2. Базовые настройки маршрутизаторов Juniper ERX

Рабочая программа курса
EDU-JUN-BB Конфигурирование BRAS на маршрутизаторах E-серии

Курс разработан для того, чтобы предоставить сетевым инженерам навыки, необходимые для успешной инсталляции, конфигурирования и обслуживания маршрутизаторов E-серии, работающих как серверы широкополосного доступа (broadband remote access server - B-RAS).

Предварительная подготовка:
Слушатель должен иметь:
знания по маршрутизации и адресации TCP/IP,
базовые знания по маршрутизаторам E-серии, представленные в курсе Основы работы с маршрутизаторами E-серии

Планируемые результаты обучения:
Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель сможет:

Выполнять задачи по системному администрированию маршрутизаторов E-серии Конфигурировать IP-over-ATM; Конфигурировать bridged Ethernet; Конфигурировать PPP-over-ATM; Конфигурировать PPP-over-Ethernet; Конфигурировать динамические интерфейсы; Конфигурировать L2TP;
Производить отладку; Настраивать базовые политики.

Продолжительность курса: 32академических часа (4 дня)

Содержание:

Тема 1. Обзор маршрутизаторов E-серии
Линейка маршрутизаторов Juniper Networks
Применение E-серии (BRAS)
Система SDX-300 (Policy and Network Management System)
Система SRC (Session and Resource Control)
Тема 2. Внутренняя архитектура маршрутизаторов E-серии
Линейка и типы шасси
Архитектура ERX-14xx/7xx/310
Архитектура E320
Движение пакетов Аппаратное резервирование Инсталляция
Тема 3. Введение в интерфейс командной строки и базовое конфигурирование
Режимы командной строки
Базовые операции Скрипты и макросы Загрузка и перезагрузка
Тема 4. Виртуализация, виртуальные маршрутизаторы
Концепция виртуализации
Конфигурирование и управление виртуальными маршрутизаторами Лабораторная работа 1. Знакомство с режимом командной строки Лабораторная работа 2. Базовые настройки маршрутизаторов Juniper ERX

Рабочая программа курса
EDU-JUN-JSPX Коммутация в сетях интернет-сервис провайдеров

Целью курса является обеспечение слушателей необходимыми базовыми знаниями поосновным понятиям коммутации, такими как локальные сети, бриджинг, процесс MAC learning, виртуальные локальные сети, трансляция VLAN, протокол Spanning Tree и Ethernet OAM (Operation, Administration and Maintenance). Курс также покрывает такие темы, как настройка в JUNOS параметров интегрированной маршрутизации и бриджинга (IRB), виртуальных свитчей, балансировки и зеркалирования трафика.

Предварительная подготовка:
Слушатель должен иметь:

базовые знания в области передачи данных,

знания по операционной системе JUNOS в рамках курсов Основы работы с операционной системой JUNOS и Основы работы с протоколами маршрутизации в JUNOS

Планируемые результаты обучения:
Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель сможет:
Понимать особенности применения технологии Ethernet в провайдерских сетях
Понимать возможности сервисных маршрутизаторов MX Series 3D Внедрять виртуальные локальные сети и IRB
Конфигурировать фильтрацию на втором уровне
Понимать сущность виртуальных маршрутизаторов и свитчей
Настраивать виртуальные свитчи
Конфигурировать и отлаживать провайдерский бриджинг Понимать и настраивать протокол Spanning Tree Настраивать RSTP, MSTP и VSTP
Настраивать Ethernet OAM
Конфигурировать и отлаживать ERP (Ethernet Ring Protection)

Продолжительность курса: 16 академических часов (2 дня)

Содержание:
Тема 1. Провайдерский Ethernet Ethernet в глобальных сетях Стандарты Ethernet Маршрутизаторы серии MX и их возможности

Тема2. Ethernet коммутация и виртуальные локальные сети
Локальные сети Ethernet
Бриджинг
Конфигурирование и мониторинг VLANs Конфигурирование и мониторинг IRB Процесс изучения адресов на коммутаторах Фильтрация на уровне 2
Лабораторная работа 1
Тема3. Виртуальные коммутаторы
Обзор разных типов routing instance
Конфигурирование и мониторинг виртуальных коммутаторов
Соединение Routing Instances
Лабораторная работа 2
Тема4. Бриджинг в сетях интернет-сервис провайдеров Бриджинг в провайдерских сетях Конфигурирование и мониторинг
Бриджинг в магистральной сети
Лабораторная работа 3
Тема5. Протокол Spanning Tree
Обзор STP, RSTP, MSTP, VSTP
Конфигурирование и мониторинг разных типов STP Понимание BPDU
Лабораторная работа 4
Тема6. Ethernet OAM Обзор OAM LFM

CFM
Конфигурирование и мониторинг OAM Лабораторная работа 5
Тема7. Ethernet Ring Protection
Обзор ERP
Конфигурирование и мониторинг ERP Лабораторная работа 6

Рабочая программа курса
EDU-JUN-JCOS Классы обслуживания в JunOS

Целью курса является обеспечение слушателей знаниями и навыками настройки и понимания работы классов обслуживания трафика в ОС JunOS. Обсуждаются классификация трафика, ограничение скорости, работа планировщика, маркировка пакетов. Также рассматривается функционал Class-based forwarding, и даются примеры настройки.

Предварительная подготовка:
Слушатель должен иметь:
базовые знания в области передачи данных,
знания по операционной системе JUNOS в рамках курсов Основы работы с операционной системой JUNOS, Основы работы с протоколами маршрутизации в JUNOS и Настройка протоколов маршрутизации в операционной системе JUNOS
понимание базовых концепций CoS

Планируемые результаты обучения:
Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель сможет: Понимать историю и эволюцию CoS
Уметь идентифицировать поля в пакетах, играющих роль для CoS Понимать этапы работы CoS
Знать настройки CoS по умолчанию
Знать классификацию behavior aggregate (BA) и multifield (MF)
Знать двух- и трехцветную маркировку Знать планировщик и его настройку Знать о многоуровневых планировщиках Знать о перемаркировке пакета
Уметь создавать конфигурации CoS на основе требуемых параметров

Продолжительность курса: 16 академических часов (2 дня)

Содержание:
Тема 1. Обзор CoS
История и эволюции CoS CoS и DiffServ
Поля в пакетах, играющие роль для CoS Работа CoS
Тема2.Классификация пакетов
Обзор
Forwarding Class, Packet Loss Priority Фиксированная классификация Multifield-классификация
Behavior Aggregate классификация
Лабораторная работа 1

Тема3.Ограничение скорости
Обзор
Односкоростной двухцветный полисер
Трехцветная маркировка
Применение на интерфейсе и в фильтре
Лабораторная работа 2
Тема4.Планировщик
Обзор
Скорость передачи
Приоритет очереди
Буферы задержки
Drop Profiles, Drop Profile Maps Настройка Scheduling Лабораторная работа 3
Тема5.Многоуровневые планировщики
Обзор
Режимы работы
Уровни иерархии
Пример с полосой пропускания
Оставшийся трафик Свойства очередей Общая схема работы Лабораторная работа 4
Тема6.Правила перемаркировки
Обзор перемаркировки в заголовке пакета Правила и таблицы перемаркировки Варианты Лабораторная работа 5
Тема7.CoS-based forwarding
Обзор Настройка Лабораторная работа 6
Тема8.Дополнительные примеры
Случай с VoIP
Узел на входе
Транзитный и конечный узел

Рабочая программа курса
EDU-JUN-JMV Технологии MPLS и VPN в JUNOS

Целью курса является обеспечение слушателей необходимыми знаниями и навыками по настройке виртуальных частных сетей (VPN), основанных на технологии MPLS. Курс включает в себя обзор концепций MPLS, контроль и передачу данных в сети, RSVP Traffic Engineering, LDP, Layer 3 VPN, мультикастные VPN следующего поколения (MVPNs), BGP Layer 2 VPNs, LDP Layer 2 Circuits, сервис виртуальной локальной сети (VPLS).

Предварительная подготовка:
Слушатель должен иметь:

- иметь базовые знания в области сетей передачи данных,
- понимать модель Open Systems Interconnection (OSI) и стек протоколов TCP/IP,
- иметь знания по операционной системе JUNOS в рамках курсов Introduction to the Junos Operating System (IJOS), Junos Routing Essentials (JRE), Junos Service Provider Switching (JSPX).

Для понимания концепции MVPN необходимо знание работы Protocol Independent Multicast-Sparse Mode (PIM-SM)

Планируемые результаты обучения:

Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель будет иметь следующие знания и навыки:

Знание общих терминов, используемых в технологии MPLS Процесс передачи MPLS-трафика
Понимание работы label-switched path (LSP)
Конфигурирование и проверка работы форвардинга MPLS-трафика
Понимание Label Information Base
Разница двух используемых протоколов распределения меток Конфигурирование и отладка для LSP, сигнализированных по RSVP и LDP Ограничения RSVP и LDP
Работа RSVP без Constrained Shortest Path First (CSPF) Расширения IGP для работы Traffic Engineering Database (TED) Алгоритм CSPF
Административные группы Защита трафика RSVP LSP Основная и резервные LSP
Приоритет LSP и преемственность Функция fast reroute
Защита линка и узла
Оптимизация LSP и другие функции
Определение понятия VPN (Virtual Private Network) Определение разницы провайдерского и клиентского VPN Определение разницы L2 и L3 VPN
Функции провайдерских VPN в JunOS Роли маршрутизаторов в сети (P, PE, CE) VPN-IPv4 адреса / Route distinguisher Понимание работы RFC 4364
Создание и настройка VPN routing instance Функции BGP extended communities
Динамическая маршрутизация в VPN, настройка Routing-instance switch
Проблемы, возникающие с трафиком на VPN-интерфейсах
Использование операционных команд для проверки работы L3 VPN
Мониторинг и поиск проблем в маршрутизации между клиентом и провайдером
Четыре способа улучшения масштабирования L3 VPN
Три способа предоставить услугу доступа в интернет с L3 VPN Команда auto-export и routing table groups
Прохождение трафика в топологии hub-and-spoke
CoS в L3 VPN
GRE и IPSec для L3 VPN Контрольный и дата-трафик в MVPN Конфигурирование и мониторинг в MVPN Работа BGP Layer 2 VPN
Роли маршрутизаторов в сети L2 VPN (P, PE, CE)
Контрольный и дата-трафик в BGP L2 VPN
Настройка, мониторинг и поиск неисправностей BGP L2 VPN Масштабирование BGP Layer 2 VPN и route reflection Поддержка BGP L2 VPN CoS в JunOS
Контрольный и дата-трафик при работе LDP Layer 2 circuit Конфигурирование, мониторинг и поиск неисправностей LDP Layer 2 circuit Circuit cross-connect (CCC) в MPLS
Разница между Layer 2 MPLS VPN и VPLS
Сигналинг и роли устройств в VPLS
Процесс заучивания адресов и передачи трафика в VPLS Возможность образования петель в сети VPLS Конфигурирование BGP и LDP VPLS
Поиск неполадок в VPLS

Продолжительность курса: 40 академических часов **(**5 дней)

Содержание:

Тема 1. Основы MPLS Базовые концепции Терминология Конфигурирование Форвардинг трафика Лабораторная работа 1

Тема 2. Протоколы распределения меток
RSVP LDP Лабораторнаяработа2

Тема 3. Constrained Shortest Path First
RSVP без CSPF Алгоритм CSPF
Выбор в случае равных возможностей Административные группы Лабораторная работа 3

Тема 4. Оптимизация и защита трафика
Работа по умолчанию Основная и резервные LSP FastReroute
BypassLSPs Оптимизация LSP Лабораторная работа 4

Тема 5. Другие функции MPLS Интеграция таблиц маршрутизации Forwarding Adjacencies
Контроль политиками Метрика LSP Automatic Bandwidth Обработка TTL
Конфигурирование Explicit Null
MPLS ping
Лабораторная работа 5

Тема 6. Обзор VPN Обзор Провайдерские VPN
VPN, организованный клиентом

Тема 7. VPN уровня 3
Терминология L3 VPN Адреса VPN-IPv4
Характеристики работы
Лабораторная работа 6

Тема 8. Базовая настройка L3 VPN Предварительные шаги Конфигурирование PE маршрутизатора Лабораторная работа 7

Тема 9. Поиск неисправностей для L3 VPN

Уровневой подход Routing-instance switch Traceroute (PE, CE) Таблицы VRF и сигналинг Мониторинг протоколов PE-CE

Рабочая программа курса
EDU-JUN-JMR Мультикастная маршрутизация в JUNOS

Целью курса является обеспечение слушателей знаниями и навыками о работе основных сетевых мультикастных протоколов, включая Internet Group Management Protocol (IGMP), Protocol Independent Multicast-Dense Mode (PIM-DM), Protocol Independent Multicast-Sparse Mode (PIM-SM), и Multicast Source Discovery Protocol (MSDP). Благодаря подробному изложению теоретического материала и большому количеству лабораторных работ, слушатели получат опыт настройки ОС JUNOS и мониторинга состояния устройств и протоколов, необходимый для настройки и поддержки работы сети, использующей возможности ip multicast.

Предварительная подготовка:
Слушатель должен иметь:
базовые знания в области передачи данных,

знания по операционной системе JUNOS в рамках курсов Основы работы с операционной системой JUNOS, Основы работы с протоколами маршрутизации в JUNOS и Настройка протоколов маршрутизации в операционной системе JUNOS

Планируемые результаты обучения:
Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель сможет:
Понимать схемы передачи трафика в ip multicast
Знать компоненты ip multicast
Знать мультикастную адресацию
Понимать необходимость reverse path forwarding (RPF) для работы мультикастинга
Понимать предназначения протокола IGMP, отличия версий протокола
Уметь настраивать и выполнять мониторинг IGMP Знать протоколы маршрутизации multicast
Понимать разницу режимов работы dense-mode и sparse-mode
Понимать работу rendezvous point (RP)
Конфигурировать и выполнять мониторинг PIM dense и sparse modes
Понимать методы обнаружения RP Понимать работы MSDP
Знать работу MSDP в одном PIM-домене с Anycast RP Знать работу MSDP в случае многих доменов PIM Настраивать и выполнять мониторинг MSDP
Сравнить модели any-source multicast (ASM) и source-specific multicast (SSM)
Знать требования, преимущества и проблемы SSM
Знать адреса, используемые в случае SSM vРоль IGMPv3 и PIM-SM в работе SSM
Настраивать и выполнять мониторинг SSM
Описывать работу PIM sparse mode по умолчанию
Понимать влияние политик маршрутизации на PIM
Описывать, как MSDP делает message advertisement, и роль политик в этом
Использовать политики для установления границ мультикастинга

Продолжительность курса: 40 академических часов **(**5 дней)

Содержание:
Тема 1. Начальные сведения Обзор мультикастинга Адресация
Форвардинг по обратному пути - Reverse Path Forwarding Протокол Internet Group Management Protocol Лабораторная работа 1
Тема 2. Мультикастные протоколы маршрутизации
Обзор PIM-DM
Лабораторная работа 2
PIM-SM
Лабораторная работа 3
Тема 3. Протокол MSDP
MSDP Anycast RP Лабораторная работа 4
Тема 4. Source-Specific Multicast
Обзор Адресация IGMPv3 и SSM PIM-SM и SSM
Примеры работы SSM Лабораторная работа 5

Тема 5. Политики и мультикаст Фильтрация PIM Join сообщений Использование ограничительной политики Фильтрация сообщений BSR
Фильтрация сообщений SA Лабораторная работа 6

Рабочая программа курса
EDU-JUN-AJSPR Продвинутая маршрутизация JUNOS в сети провайдера

Целью курса является обеспечение слушателей знаниями и навыками настройки протоколов OSPF, IS-IS, BGP и политик маршрутизации в JUNOS. Благодаря подробному изложению теоретического материала и большому количеству лабораторных работ, слушатели получат опыт настройки протоколов маршрутизации в ОС JUNOS и мониторинга состояния устройств и этих протоколов.

Предварительная подготовка:
Слушатель должен:
- иметь базовые знания в области сетей передачи данных,
- понимать модель Open Systems Interconnection (OSI) и стек протоколов TCP/IP,
- иметь знания по операционной системе JUNOS в рамках курсов Introduction to the Junos Operating System (IJOS), Junos Routing Essentials (JRE) и Junos Intermediate Routing (JIR)

Планируемые результаты обучения:
Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель будет иметь следующие знания и навыки: Описание разных типов OSPF LSA
Распространение LSA в сети OSPF Алгоритм поиска кратчайшего маршрута Ключевые отличия OSPF версий 2 и 3
Типы областей (area) OSPF
Конфигурирование областей OSPF разных типов
Суммаризация и ограничение маршрутов
Практика использования разных опций и политик OSPF Понимание работы протокола IS-IS
Пакеты IS-IS PDU
Соседство IS-IS и типичные проблемы
Настройка и мониторинг IS-IS База данных о состоянии каналов Дополнительные опции IS-IS
Использование политик маршрутизации для IS-IS Работа IS-IS в нескольких сетевых областях Методы суммаризации в IS-IS
Настройка и мониторинг сети IS-IS с несколькими областями
Основы работы BGP Атрибуты BGP
Процесс выбора наилучшего маршрута BGP Возможности влияния на выбор маршрута
Дополнительные опции в пиринге BGP Подробности BGP атрибутов
Манипуляции с атрибутами при помощи маршрутных политик

Возможные причины нестабильности маршрутов
BGP damping
Работа демпфирования по умолчанию и при наличии маршрутных политик
Просмотр маршрутов, подвергшихся демпфированию
Рефлектинг BGP-маршрутов Настройка Route Reflector BGP-конфедерации
Отношения пиров в BGP конфедерации

Продолжительность курса: 32 академических часа (4 дня)

Содержание:

Тема 1. Протокол OSPF
Обзор OSPFv2
Link State Advertisements (LSA) Работа протокола Аутентификация OSPF
Обзор OSPFv3
Лабораторная работа 1

Тема 2. Области OSPF
Обзор
Области типа Stub и их настройка Области типа NSSA и их настройка Суммаризация маршрутов Лабораторная работа 2

Тема 3. Разбор примеров настройки OSPF
Виртуальные линки
Соседство с разными областями Внешняя доступность
Лабораторная работа 3

Тема 4. Протокол IS-IS
Обзор Пакеты IS-IS Установление соседства
Конфигурирование и мониторинг
Лабораторная работа 4

Тема 5. Дополнительные темы IS-IS
Работа IS-IS Дополнительные опции Политики маршрутизации Лабораторная работа 5

Тема 6. Многоуровневые сети IS-IS
Работа L1 и L2
Настройка сети
Лабораторная работа 6

Тема 7. Протокол BGP
Обзор
Работа протокола
Выбор маршрута и опции конфигурации
Лабораторная работа 7

Тема 8. Атрибуты и политики BGP
Политика для BGP
Next Hop
Лабораторная работа 8
Атрибуты Origin, MED Атрибут AS Path
Лабораторная работа 9
Атрибут Local Preference
Communities маршрута
Лабораторная работа 10

Тема 9. Демпинг маршрутов BGP
Обзор
Параметры дэмпинга Настройка и мониторинг

Лабораторная работа 11
Тема 10. Route Reflection и конфедерации Работа рефлектора маршрутов Настройка
Прохождение маршрутной информации
Конфедерации BGP Лабораторная работа 12

Рабочая программа курса
EDU-JUN-IPV6 Работа с IPV6 в Junos

Целью курса является обеспечение слушателей знаниями и навыками по работе с протоколом IPv6 в ОС Junos, в том числе: адресация IPv6, ICMPv6 Neighbor Discovery, маршрутизация (включая статическую и протоколы RIPng, OSPFv3, IS-IS, BGP). Обсуждается поддержка IPv6 при работе с MPLS и VPLS, и разные методы миграции с IPv4 на IPv6. Благодаря подробному изложению теоретического материала и большому количеству демонстраций и лабораторных работ, слушатели получат достаточный для практической работы опыт настройки IPv6 в ОС Junos.

Предварительная подготовка:
Слушатель должен иметь:
базовые знания в области сетей передачи данных,
знания по операционной системе Junos в рамках курсов Introduction to the Junos Operating System (IJOS), Junos Routing Essentials (JRE) и Junos Intermediate Routing (JIR)

Планируемые результаты обучения:
Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.
После изучения курса слушатель будет:
Знать IPv4 и IPv6 - сходства и различия
Знать Extension headers IPv6
Знать разные типы адресов IPv6
Обнаруживать соседей IPv6
Работать с MTU
Знать VRRP и IPv6
Понимать таблицы маршрутизации IPv6
Знать статические и агрегированные маршруты
Настраивать фильтров IPv6 в JunOS
Настраивать OSPFv3
Настраивать IS-IS для IPv6
Настраивать BGP с соседями IPv4 и IPv6 для передачи трафика IPv6
Понимать варианты перехода с IPv4 на IPv6
Настраивать устройства Juniper в режиме двойного стека протоколов
Описывать разные методы туннелирования
Заниматься отладкой для IPv6
Знать и использовать основные команды операционного режима
Описывать и настраивать RIPng

Продолжительность курса: 16 академических часов **(**2 дня)

Содержание:

Тема1.Настройка адресации IPv6
Сравнение адресации IPv4 и IPv6
Extension headers
Подсети
Настройка интерфейсов
Лабораторная работа
Тема2.Протокол IPv6 и сервисы
ICMPv6
Neighbor Discovery MTU Discovery VRRP
DHCPv6
DNS
Лабораторная работа
Тема3.Протокольно-независимые функции
Таблицы маршрутизации Протокольно-независимые функции Фильтры
Лабораторная работа
Тема4.OSPFv3
Обзор и настройка
Лабораторная работа
Тема5. Поддержка IPv6 в IS-IS Обзор и настройка Лабораторная работа
Тема6.BGP и IPv6
Обзор и теория
Лабораторная работа
Тема7.Варианты перехода с IPv4 на IPv6
Варианты Двойной стек Туннелирование Лабораторная работа
Тема8.Поиск неисправностей
Основные методы
Команды операционного режима
Лабораторная работа

Рабочая программа курса
EDU-JUN-JAUT Автоматизация Junos

Целью курса является обеспечение слушателей знаниями и навыками, необходимыми для разработки сценариев (скриптов) при работе с ОС Junos. Курс содержит обзор языков Extensible Markup Language (XML) и Stylesheet Language Alternative Syntax (SLAX), шаблонов и библиотек Junos, и скриптов трех видов: commit, operation и event. Благодаря подробному изложению теоретического материала и большому количеству лабораторных работ, слушатели получат достаточный для практической работы опыт создания скриптов и автоматизации JunOS.

Предварительная подготовка:
Слушатель должен иметь:
базовые знания в области сетей передачи данных,
знания по операционной системе JUNOS в рамках курсов Основы работы с операционной системой JUNOS и Основы работы с протоколами маршрутизации в JUNOS
знакомство с каким-либо из языков программирования, таким как C, C++, Perl, Java.

Планируемые результаты обучения:
Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель сможет: Знать преимущества автоматизации Junos
Понимать разницу между commit, op, и event скриптами
Знать формат документа XML
Использовать XML в Junos в операционном и конфигурационном режимах
Знать взаимодействие скриптов с XML Знать структуру скрипта SLAX
Знать переменные SLAX и контроль выполнения
Уметь создавать и тестировать SLAX-скрипты
Знать функции расширения Junos
Использовать commit скрипты для изменения конфигурации
Использовать commit скрипты для вывода сообщений и проверки конфигурации
Настраивать и подключать commit скрипты
Использовать op скрипты
Определять аргументы и вызывать команды операционного режима
Использовать op скрипты для изменения конфигурации
Настраивать op скрипты
Знать политики и скрипты, выполняемые по событию (event) Настраивать event скрипты

Продолжительность курса: 16 академических часов (2 дня)

Содержание:
Тема1.Основы автоматизации
Обзор
Введение в commit, op, и event скрипты
Решения по автоматизации
Тема2.XML
Обзор XML XML в Junos XML в скриптах
Лабораторная работа 1
Тема3.SLAX
Введение в SLAX Шаблоны
XML-тэги
Переменные
Контроль выполнения в SLAX Структура скрипта Дополнительные ссылки Лабораторная работа 2
Тема4.Библиотека функций Junos Функции расширения Junos Логические функции
Манипулирование данными Ввод-вывод
Утилиты Аргументы Лабораторная работа 3
Тема5.Commit-скрипты
Введение
Внесение изменений в конфигурацию Вывод сообщений об ошибках Собственные настройки в конфигурации
Настройка и подключение commit скриптов
Лабораторная работа 4
Тема6.Op-скрипты Введение Простой пример

Аргументы
Вызов команд операционного режима
Вывод
Использование op скриптов для изменения конфигурации
Настройка скриптов
Лабораторная работа 5
Тема7.Event-скрипты
Введение
Обработка событий
Event policy
Написание event-скриптов
Лабораторная работа 6

Рабочая программа курса
EDU-JUN-JEX Коммутация в корпоративных сетях

Целью этого двухдневного курса является предоставление общих сведений о технологиях коммутации в локальных сетях и примеры конфигурации. Курс включает в себя обзор технологий коммутации, виртуальные локальные сети, протокол Spanning Tree, настройка различных функций безопасности на коммутаторах и реализацию резервирования.

Предварительная подготовка:
Слушатель должен:
понимать протоколы TCP/IP
иметь общее представление о работе современных сетей.
владеть командной строкой Junos в рамках курсов Основы работы с операционной системой JUNOS и Основы работы с протоколами маршрутизации в JUNOS.

Планируемые результаты обучения:
Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель сможет: Понимать концепции бриджинга
Понимать особенности оборудование Juniper для локальных сетей
Конфигурировать интерфейсов на коммутаторах Понимать концепции виртуальных локальных сетей Знать порты доступа и транковые порты Конфигурировать и выполнять мониторинг VLAN Понимать голосовой VLAN и Native VLAN Понимать маршрутизацию между VLAN
Знать протокол Spanning Tree и Rapid Spanning Tree
Понимать безопасность в локальных сетях
Знать пакетные фильтры
Понимать вопросы обеспечения высокой надежности
Знать виртуальное шасси на платформе 4200

Продолжительность курса: 16 академических часов **(**2 дня)

Содержание:

Тема 1. Коммутация второго уровня
Основы Ethernet Bridging
Терминология и особенности дизайна локальных сетей
Обзор платформ серии EX Конфигурирование и мониторинг
Лаб 1. Внедрение коммутации на втором уровне
Тема2. Виртуальные локальные сети (VLANs)
Обзор VLANs
Конфигурирование и мониторинг VLANs
Голосовой VLAN
Native VLAN
Маршрутизируемые интерфейсы VLAN (RVIs) Лаб 2. Конфигурирование и мониторинг VLANs
Тема3. Протоколы Spanning Tree
Протокол Spanning Tree (STP) Rapid Spanning Tree (RSTP)
Конфигурирование и мониторинг STP и RSTP Резервирование портов (защита)
Лаб 3. RSTP и резервирование портов

Тема4. Безопасность
Ограничение по MAC-адресам (MAC Limiting) Инспектирование ARP (Dynamic ARP Inspection (DAI) Перехват DHCP (Snooping)
Защита на основе IP адреса (IP Source Guard) Лаб 4. Внедрение функций безопасности
Тема5. Безопасность коммутатора и пакетные фильтры Защита от броадкастного шторма (Storm Control) Пакетные фильтры
Лаб 5. Настройка защиты коммутатора
Тема6. Обеспечение высокой надежности Агрегирование линков (LAGs) Резервирование транковых групп (RTG) Лаб 6. Конфигурирование LAGs и RTG Виртуальное шасси
Лаб 7. Конфигурирование виртуального шасси

Рабочая программа курса
EDU-JUN-JSEC Операционная система JUNOS для устройств безопасности (SRX и J-Series)

Этот трехдневный курс дает слушателям навыки для конфигурирования, эксплуатации и внедрения устройств сетевой безопасности.

Предварительная подготовка:

Слушатель должен:

иметь базовые знания в области сетевых технологий, понимать модель OSI, стек протоколов TCP/IP,

знания по операционной системе JUNOS в рамках курсов Основы работы с операционной системой JUNOS, Основы работы с протоколами маршрутизации в JUNOS и Настройка протоколов маршрутизации в операционной системе JUNOS

Планируемые результаты обучения:

Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель сможет:

Дать описание традиционного понимания маршрутизации и сетевой безопасности, а также последние наработки в этой области

Знать обзор устройств безопасности Juniper Networks и архитектуры JUNOS Понимать обработку пакетов и сессий внутри устройств безопасности Конфигурировать зоны и политик и

Знать обзор и предотвращение различных типов сетевых атак

Понимать конфигурирование и мониторинг NAT, IPSec VPN, IDP

Понимать конфигурирование и мониторинг кластеров для обеспечения высокой надежности

Продолжительность курса: 24 академических часа **(**3 дня)

Содержание:

Тема1.Введение в устройства безопасности JUNOS Маршрутизация в традиционном понимании Безопасность в традиционном понимании Порвать с традицией

Архитектура JUNOS

Тема2.Зоны безопасности Определение зон Конфигурирование зон Мониторинг зон безопасности Лабораторная работа 1

Тема3.Политики безопасности Обзор политик безопасности Компоненты политик Проверка работы политик Планирование политик

Пример внедрения политик безопасности

Лабораторная работа 2

Тема4.Аутентификация пользователей

Обзор

Аутентификация в режиме pass-through

Аутентификация через Web Клиентские группы Использование внешних серверов

Проверка функционирования механизмов аутентификации

Лабораторная работа 3

Тема 6. Возможности SCREEN Многоуровневая защита сети Типы и стадии атак

Использование режима SCREEN

Внедрение и мониторинг SCREEN Лабораторная работа 4

Тема5.Трансляция адресов (NAT)

Обзор NAT

Трансляция по адресу назначения Трансляция по адресу источника Proxy ARP

Мониторинг NAT Лабораторная работа 5

Тема6.IPSec VPN

Типы виртуальных частных сетей

Требования безопасности для VPN

Описание, конфигурирование и мониторинг IPSec VPN Лабораторная работа 6

Тема7.Введение в IDP

Компоненты политик IDP и их конфигурирование

Атаки и база данных сигнатур Пример политик IDP Мониторинг IDP

Лабораторная работа 7

Тема8.Кластеры и высокая надежность

Обзор

Компоненты, работа, конфигурирование и мониторинг кластеров

Лабораторная работа 8

Рабочая программа курса
EDU-JUN-CJFV Основы конфигурирования межсетевых экранов /концентраторов IPSEC VPN Juniper

Это первый курс в линейке курсов Juniper по продуктам сетевой безопасности, работающим под управлением ОС ScreenOS, то есть всех устройств семейств SSG, ISG и Netscreen Firewall/IPSEC VPN. В течение трех дней в теории и на практике изучается работа с данными устройствами. Основными темами являются: начальное конфигурирование и администрирование, маршрутизация, настройка политик безопасности, основы защиты от атак, трансляция сетевых адресов, конфигурирование виртуальных частных сетей (ВЧС).

Значительное время в течение курса уделяется лабораторным работам, что позволяет закрепить на опыте полученные знания. Специалисты, прослушавшие и усвоившие материал курса, будут обладать достаточным набором знаний и навыков для настройки продуктов Juniper Firewall/IPSec VPN для большинства практических применений.

Предварительная подготовка:
Слушатель должен иметь базовые знания по следующим темам: Компьютерные сети и Интернет
Технология Ethernet Маршрутизация и коммутация Основы TCP/IP
Продолжительность курса: 24 академических часа **(**3 дня)

Содержание:
Тема 1. Основы ScreenOS, терминология, поддерживаемое оборудование
Требования к устройствам сетевой безопасности
Архитектура ОС ScreenOS Аппаратура
Тема 2. Начальная настройка Компоненты системы Установление соединения
Поиск неисправностей
Тема 3. Управление устройствами
Управление Восстановление пароля Лабораторная работа
Тема 4. Работа на сетевом уровне (Layer 3) Необходимость маршрутизации
Конфигурирование и отладка L3-функционала Интерфейс loopback
Интерфейсная трансляция сетевых адресов
Лабораторная работа
Тема 5. Основы конфигурирования политик безопасности
Функции
Конфигурация
Часто возникающие проблемы Глобальные политики Проверка работы политик
Лабораторная работа
Тема 6. Опции политик безопасности
Обзор Журналирование Счетчики
Выполнение по расписанию Авторизация пользователей Лабораторная работа
Тема 7. Трансляция сетевых адресов Обзор возможных вариантов Трансляция адреса источника (NAT-src)
Трансляция адреса назначения (NAT-dst) Функциональность и конфигурирование Virtual IP
Функциональность и конфигурирование Mapped IP Лабораторная работа
Тема 8. Прозрачный режим (опционально)
Обзор

Функциональность и конфигурирование работы в прозрачном (Layer 2) режиме
Отладка
Лабораторная работа
Тема 9. Концепции ВЧС
Обзор концепций и терминология
Протокол IPSEC
Тема 10. ВЧС на основе политик безопасности
Конфигурирование Отладка Лабораторная работа
Тема 11. ВЧС на основе маршрутизации Концепция и термины Конфигурирование
Отладка
Лабораторная работа

Рабочая программа курса
EDU-JUN-CJSA Конфигурирование безопасного удаленного доступа для платформ Juniper Secure Access

Этот курс посвящен настройке продуктов Juniper Secure Access (SA) в типичных сетевых конфигурациях. В курсе обсуждаются технология доступа по SSL, основные принципы и возможности конфигурирования и управления. Большое количество лабораторных работ позволяет слушателям самим научиться настраивать, тестировать и устранять проблемы при работе с устройствами Juniper Secure Access.

Предварительная подготовка:
Слушатель должен иметь базовые знания по следующим темам:
компьютерные сети и Интернет, основы TCP/IP.

Планируемые результаты обучения:
Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель будет:
Иметь представление о платформах Juniper Secure Access и знать соответствующую терминологию
Знать технологии SSL и PKI
Понимать типичные варианты установки устройств SA в сети
Знать роли пользователей, области авторизации
Знать ресурсные политики, политики входа
Знать серверы аутентификации (локальный, RADIUS, LDAP, NT, NIS) Понимать политики аутентификации
Понимать возможности приложений Host Checker и Cache Cleaner
Знать о поддержке приложений клиент/сервер: Secure Application Manager (SAM) Знать о поддержке приложений клиент/сервер: Network Connect (NC)

Продолжительность курса: 16 академических часов **(**2 дня)

Содержание:

Тема1.Обзор продуктов и функционала SA
Обзор Secure Access
Варианты развертывания системы Аппаратные платформы и набор функций Методы доступа
Тема2.Технология и терминология
Методы доступа Instant Virtual Extranet (IVE)
Архитектура IVE Терминология IVE
Тема3.Начальная настройка Конфигурирование с консоли Интерфейс администратора
Лабораторная работа 1
Тема4.Роли пользователей
Конфигурирование ролей пользователей

Соответствие ролей
Настройка интерфейса пользователя
Лабораторная работа 2
Тема 6.Журналы и отладка Журналы
Инструменты отладки
Лабораторная работа 3
Тема 7.Ресурсные политики
Определение ресурса
Конфигурирование ресурсных политик
Опции ресурсных политик
Конфигурирование профилей ресурсов
Лабораторная работа 4
Тема 8.Серверы аутентификации
Настройка серверов аутентификации Лабораторная работа 5
Тема 9.Поддержка приложений клиент/сервер
Необходимость поддержки приложений клиент/сервер Secure Application Manager (SAM) Network Connect (NC) Telnet и SSH Терминальные сервисы Лабораторная работа 6
Тема 10.Безопасность конечного пользовательского оборудования
Инициатива защиты пользователя Juniper (JEDI) Конфигурирование приложения Host Checker
Настройка безопасного виртуального рабочего пространства
Конфигурирование Cache Cleaner Политики аутентификации Настройка ограничений ролей Лабораторная работа 7

Рабочая программа курса
EDU-JUN-JSE Основы работы с системой Junos Space

Этот двухдневный курс дает слушателям необходимые знания и навыки для работы с системой управления Junos Space. В курсе разбирается инсталляция Junos Space (в том числе в виде кластера из нескольких узлов), ее администрирование и мониторинг. Изучаются такие аспекты централизованного управления устройствами, как сохранение конфигураций, синхронизация, апгрейды, шаблоны, и др. Разбирается работа с конкретными приложениями, такими как Service Now и Service Insight.

Предварительная подготовка:
Слушатель должен иметь базовые знания по следующим темам: Основы TCP/IP
Junos в объеме курса IJOS
Продолжительность курса: 16 академических часов **(**2 дня)

Содержание:
Тема 1.Junos Space - введение Роль Junos Space Архитектура Приложения
Тема 2. Развертывание Junos Space
Два варианта реализации
Начальная настройка (демонстрация) Фабрика из нескольких узлов Безопасность
Веб-интерфейс
Лабораторная работа
Тема 3. Администрирование
Управление заданиями
Роли и администраторы
Управление платформой
Тема 4. Управление устройствами Обнаружение и управление устройствами
Конфигурация устройств
Мониторинг сети
Лабораторная работа
Тема 5. Шаблоны
Введение
Определения шаблонов
Шаблоны
Лабораторная работа
Тема 6. Автоматизация сервисов
Обзор Service Now Service Insight; Лабораторная работа

Рабочая программа курса
AV101 Базовое администрирование АТС Avaya Aura Communication Manager

В данном курсе изучается администрирование телефонных станций Avaya: MultiVantage S8300/S8400/8500/8700, Definity, начиная от момента установки. Рассмотрены все базовые понятия и основные возможности станций. Детально рассмотрены вопросы подключения к ТфОП, особенности настройки российских протоколов сигнализации, настройки маршрутизации исходящих и распределения входящих вызовов, управления привилегиями пользователей. Курс в значительной степени ориентирован на практическую работу, поэтому в нем разбираются стандартные ошибки администратора, особенности применения отдельных функций, содержатся рекомендации на часто встречающиеся случаи. Важную часть курса составляют практические занятия - каждый слушатель в процессе курса настраивает «с нуля» реальную станцию. Курс рассчитан на администраторов и инсталляторов телефонных станций Avaya.

Предварительная подготовка слушателя:
Умение работать с PC, иметь представление о работе сетей телефонной связи. Наличие хотя бы небольшого опыта администрирования станции приветствуется.
Планируемые результаты обучения:
Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по

данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.
После изучения курса слушатель сможет:
администрировать (создавать первичную конфигурацию) станции:
поддерживать станцию в работоспособном состоянии.

Продолжительность курса: 40 академических часов (5 дней)

Содержание:

Тема 1.Введение
Общие вопросы телефонии
Тема 2.Архитектура системы
Архитектура классических станций Definity
Архитектура медиа-систем (медиа-сервера S8xx0, медиа-гейтвеи)
Абонентские и транковые платы
Телефоны
Тема 3.Введение в администрирование
Программы для администрирования ATE, ASA Адресация плат и портов
Структура команд Первоначальные настройки Номерной план
Тема 4.Подключение и настройка абонентов Настройка аналоговых и цифровых телефонов Пользовательские функции
Тема 5.Группы пользователей
Группа ответа на вызов отсутствующего абонента
Группа перехвата вызова Группа поиска Оповещение (пейджинг)
Тема 6.Системные ограничения
Настройка COR
Анализ платных вызовов "toll analysis" Настройка COS
Тема 7.Автоматическая обработка вызовов
Доступ к ресурсам извне Голосовые сообщения Векторы
Тема 8.Автоматическая маршрутизация
Единый номерной план UDP
Типы маршрутизации (ARS и AAR) Схема маршрутизации
Таблицы маршрутизации
Пример настройки маршрутизации
Тема 9.Настройка транков Аналоговые транки Цифровые транки ISDN
Российские протоколы (R1.5, R2)
CO-транки на абонентских линиях
Тема 10.Обслуживание
Общие вопросы - введение Детализированная запись звонков (CDR) Тесты телефонов и транков
Ошибки и стратегия их устранения
Настройка и просмотр статистики (measurements) Сохранение конфигурации
Вопросы безопасности

Рабочая программа курса

AV102 Углубленное администрирование АТС Avaya Aura Communication Manager, поиск и устранение неисправностей

Курс предназначен для инженеров, занимающихся установкой и сопровождением АТС Definity. Курс является продолжением базового курса Администрирование АТС Definity и имеет направленность на построение сложных конфигураций и рассмотрение различных способов разрешения проблем.

Материал курса посвящен следующим основным темам:
Сигнализации сетей связи, применяемые на Definity в России и странах СНГ, описание способов их отладки при помощи встроенных средств и внешних протокольных анализаторов. В лабораторных работах моделируются наиболее типичные проблемы, встречаемые при подключении Definity в ТфОП и построении корпоративных телефонных сетей.
Также рассматриваются вопросы настройки каналообразующего оборудования.
Вопросы технического обслуживания, поиска и устранения неисправностей в сложных конфигурациях Definity: выносы, системы с резервированием и т.п.
Подробно рассматривается архитектура новой линейки продуктов семейства MultiVantage (Медиа-серверы S8700, S8300, Медиа-шлюзы G700, G600). Также рассматриваются методы модернизации программного обеспечения, установки лицензий и связанные с этим вопросы.
Настройки АТС Definity, не рассматриваемые, или рассмотренные не полностью в базовом курсе Администрирование Definity.
Всем слушателям будет предложено на практике под руководством преподавателя найти решение различных проблемных ситуаций, используя изученные методы.

Предварительная подготовка слушателя:
Обязательно знание основ администрирования АТС Definity в рамках базового курса: заведение телефонов, транков, настройка маршрутизации, настройка плана нумерации, основы тестирования и устранения неисправностей.
Слушатель должен иметь общее представление об устройстве телефонных сетей, цифровых синхронных магистралей в объеме базового курса.
Крайне желателен практический опыт по администрированию станции - не менее года.

Планируемые результаты обучения:

Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель сможет:

настраивать сложные конфигурации АТС Definity

осуществлять подключение к публичным сетям строить корпоративные сети

устранять и диагностировать неисправности различной природы

Продолжительность курса: 40 академических часов (5 дней)

Содержание:

Тема 1.Протокол ISDN

Идеология протокола, связь с ОКС7

Структура сообщений LAPD Структура сообщений Q.931

Форматы нумерации

Порядок обмена сообщениями, таймеры Европейский стандарт: EuroISDN Расширения Q.931 (Q.SIG, DPNSS,…)

Тема 2.Система сигнализации R2

Линейная сигнализация и контроль над линией Идеология регистровой сигнализации

Распространенные виды регистровых сигнализаций Проблемы при использовании R2 на ВСС

Тема 3.Семейство протоколов 2ВСК

Структура сети

Линейная сигнализация

Виды регистровых сигнализаций Руководящие документы Реализация в Definity

Типичные проблемы при стыке с ТфОП

Тема 4.Сигнализация для подключения удаленных абонентов через цифровые каналы

Обзор V5.2, ОКС7

Настройка протоколов сигнализации и их отладка при помощи протокольных анализаторов

Проблемы, возникающие при организации транзитов между разными системами сигнализаций

Тема 5. Особенности подключения оборудования третьих производителей

Конфигурирование кабельных и оптических модемов, разрешение проблем Выносы

Системы с резервированием

Тема 6.Архитектура новых конструктивов

Media Servers: S8700, S8500, S8300

Возможные способы построения архитектуры сети с новыми Media Servers

Лицензии и работа с ними

Upgrade и Update программного обеспечения. Часто встречающиеся проблемы

Новые возможности в 11 версии (особенности версий 11.1, 11.2, 11.3)

Тема 7.Внутренняя архитектура: пакетная и TDM-шины

Методы и инструменты тестирования пакетной шины

Методы тестирования и локализации неисправностей TDM-шины

Тема 8.Способы тестирования внешних и внутренних каналов

Аналоговые линии

Цифровые линии

Типичные неисправности абонентских и транковых плат

Тема 9.Инструменты отладки и тестирования

Трассировка

Журнал событий (events) Журнал MST

Дополнительные инструменты

Средства уведомления администратора о внештатных ситуациях

Рабочая программа курса

AV201 Установка и администрирование медиасерверов и шлюзов Avaya Aura Communication Manager

Курс предназначен для инсталляторов, администраторов и инженеров по обслуживанию телекоммуникационных систем компании Avaya на основе линейки серверов S8300, S8500, S8700. Курс в значительной степени ориентирован на приобретение практического опыта работы с новым оборудованием.

Предметом данного курса является новая архитектура построения корпоративной телефонной сети связи Avaya MultiVantage Applications, которая является развитием давно известной и хорошо зарекомендовавшей себя платформы Definity. Рассматриваются возможности и особенности построения новых систем, пути модернизации старых систем; вопросы лицензирования, инсталляции и администрирования, технической поддержки. Содержится обзор методов обеспечения отказоустойчивости, возможностей резервирования различных элементов.

В лабораторных работах моделируется весь процесс установки систем разного масштаба, изменения конфигурации сети, рассматриваются типовые ошибки.

Предварительная подготовка слушателя:

Обязательно знание основ построения и использования сетей передачи данных на основе протокола TCP/IP (понятия IP-адреса, маршрутизатора, коммутатора и т.п.).

Слушатели должны разбираться в основах администрирования станции Definity в рамках базового курса: заведение телефонов, транков, настройка маршрутизации, настройка плана нумерации, основы тестирования и устранения неисправностей.

Желательно иметь представление о способах передачи голоса поверх сетей передачи данных (IP-телефония), а также умение администрировать функции IP-телефонии на станции Avaya Definity (заведением IP-телефонов, создание IP-транков).

Приветствуется практический опыт по администрированию станции Definity.

Планируемые результаты обучения:

Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель сможет:

Устанавливать, настраивать и администрировать новые системы на основе Avaya Media Server S8300/8500/8700

Создавать надежные, отказоустойчивые конфигурации и модернизации традиционных систем Avaya Definity

Продолжительность курса: 40 академических часов (5 дней)

Содержание:

Тема 1. Технологии построения корпоративных сетей связи

Обзор технологий

IP — универсальный транспорт
Архитектура Avaya Aura Communication Manager
Тема 2. Компоненты Avaya MultiVantage
Media Servers Media Gateways Абонентские терминалы Communication Manager
Дополнительное программное обеспечение

Тема 3. Системы связи на основе Avaya Communication Manager
Традиционная платформа Definity Definity с поддержкой IP Дублированные системы
Степени надёжности на дублированных системах
IP сети, подключаемые к серверу Требования к подключаемым IP сетям S8500
S8300 и малые шлюзы G450/G430
Резервные серверы — LSP и ESS Емкость систем S8x00

Тема 4. Подключение компонентов системы
Интерфейсы медиа-серверов
Сборка стека из G650
Переходники для подключения ethernet
Установка CM Duplex
Тема 5. Конфигурирование медиа-серверов
Необходимый софт
Лицензионный и аутентификационный файлы
Пароли по умолчанию
Установка ПО
Конфигурирование серверов S8x00
Работа дублированной системы серверов S8800/Common Servers
Особенности настройки LSP и ESS
Тема 6. Конфигурирование Media Gateway Настройка параметров платы IPSI Создание кабинета в трансляции CM
Проверка и диагностика регистрации кабинета
Настройка плат C-LAN, MedPro
Настройка шлюзов G450/G430
Создание шлюза в трансляции CM
Проверка и диагностика регистрации шлюза
Синхронизация в IP системах
Тема 7. IP-абоненты и IP-транки
Общие принципы IP-телефонии

Параметры IP-сети, влияющие на качество речи
Протоколы H.323, H.225 RAS, H.225 CS, H.245
Реализация H.323 в системах Communication Manager
IP-телефоны Avaya
Настройка DHCP и TFTP серверов
Апгрейд и русификация IP-телефонов
Сетевые регионы распределенной системы Communication Manager
Настройка H.323 IP-транка
Работа факсов и модемов по IP
Тема 8. Обслуживание новых систем
Процедуры сохранения и восстановления конфигурации системы
Апгрейд прошивок на платах, модулях, шлюзах

Апгрейд Communication Manager Обновления софта (Service Pack) Диагностика и устранение аварий Работа с VAL announcement Мониторинг загрузки IP-ресурсов Вопросы безопасности

Рабочая программа курса
AV401 Установка и администрирование системы Avaya IP-DECT

Курс посвящен описанию системы микросотовой связи Avaya DECT - расширению АТС Definity. Курс будет полезен администраторам и инсталляторам телефонных решений фирмы Avaya.
В ходе курса рассматривается весь процесс установки и сопровождения решения Avaya DECT, начиная от планирования системы и инсталляции оборудования и заканчивая программной настройкой и сопровождением системы.

Предварительная подготовка слушателя:

Не требуется глубоких знаний в области настройки АТС Definity.

Желательно (но не обязательно) иметь представление об администрировании АТС Definity в объёме: план нумерации, заведение и настройка абонентов, настройка протокола ISDN-PRI.

Планируемые результаты обучения:

Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель сможет:

устанавливать и сопровождать систему микросотовой связи Avaya DECT.

Продолжительность курса: 16 академических часов (2 дня)

Содержание:

Тема 1.Введение. Описание стандарта DECT Физические принципы работы DECT
Частотно-временное расписание FTDMA
Технические характеристики и возможности DECT Обеспечение безопасности в беспроводной сети DECT
Аутентификация, авторизация, криптозащита. Передача факсов и данных
Ссылки на стандарты, регламентирующие работу DECT

Тема 2.Архитектура Avaya IP-DECT Описание архитектуры IP-DECT Описание ADMM :
Системные ограничения
Описание базовых станций, сравнение, особенности
DECT-терминалы - телефонные трубки Avaya 3711, 3701, GAP-совместимые трубки
Синхронизация внутри IP-DECT-системы, кластеры
IP-транк между системой IP-DECT и станцией Avaya Communication Manager: поддерживаемые кодеки; особенности работы
Функциональность ADMM
Лицензирование IP-DECT: схемы лицензирования IP-DECT; необходимые лицензии на Avaya CM; лицензирование ADMM для работы с IPO и с CM; тонкости и особенности лицензирования системы Avaya IP-DECT

Тема 3.Первичная инсталляция и настройка IP-DECT

Задание базовых настроек для базовых станций RFP через DHCP и в статическом режиме
Настройка базовых станций чере java-апплет
Инсталляция ADMM на выделенный сервер S8510
Настройка ADMM: установка лицензий; просмотр статуса баз, построение кластеров; создание регионов; настройка используемых кодеков; настройка транка в сторону Avaya Communication Manager
Настройка Avaya Communcation Manager: просмотр установленных лицензий; настройка транка до IP-DECT; настройка сигнальной группы
Добавление абонентов: добавление абонентов в CM; прописывание абонента в ADMM; регистрация абонента на ADMM; пакетная регистрация абонентов на ADMM; просмотр статуса абонента

Тема 4.Обслуживание системы IP-DECT

Использование syslog, SNMP

Трассировки с использованием станции (li tra tac) и Wireshark
Использование IP DECT NetMonitor: задание необходимых настроек на ADMM, запуск NetMonitor, установка соединения основные возможности Dect Monitor, основные экраны; проверка синхронизации между базами в кластере; проверка работы хендовера между базами; роуминга между кластерами

Рабочая программа курса
AV601 Установка и администрирование Avaya IP Office

Курс содержит обзор архитектуры Avaya IP Office, обзор решений в области телефонии, передачи данных, на базе оборудования IP Office, подробно рассматривается система речевой почты Voice Mail Pro. Теоретическая часть курса сопровождается практическими упражнениями по настройке IP Office, соединению нескольких IP Office между собой по различным каналам связи (ISDN, IP over LAN, IP over WAN) и использованию Voice Mail Pro.

Предварительная подготовка слушателя:
Необходимы знания основ телефонии, передачи данных. Специальных знаний по предмету курса не требуется.

Планируемые результаты обучения:
Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель сможет:

- разбираться в линейке продуктов Avaya под общим наименованием IP Office
- конфигурировать IP Office, включая настройку системы, пользователей, групп, соединительных линий (ISDN, LAN, WAN), маршрутизации вызовов, средств передачи данных
- разбираться в построении алгоритмов интерактивного речевого взаимодействия (IVR) на примере построения алгоритма автоответчика

Продолжительность курса: 24 академических часа (3 дня)

Содержание:

Тема 1.Введение:

Назначение и позиционирование Основные возможности Архитектура системы
Функциональные компоненты системы
Вопросы лицензирования

Тема 2.Аппаратные средства IP Office

Общая концепция управления системой
Средства мониторинга системы

Тема 3.Приложения пользователя: PhoneManagerLite&Pro SoftConsole

Тема 4.Конфигурирование IP Office: Общие настройки системы Объекты традиционной телефонии
Система голосовой почты Voice Mail Lite
Средства передачи данных: система удаленного доступа RAS; IP маршрутизация; передача данных через ISDN; передача VoIP через LAN, WAN; FireWall
Система сбора статистики SMDR

Тема 5.Система речевой почты Voice Mail Pro:

Основные принципы, компоненты и требования к оборудованию
Построение простейшего голосового меню (Short Code Auto Attendant)
Описание функциональных элементов, применяемых в Voice Mail Pro: применение default start point; применение modules

Рабочая программа курса
AV801 Avaya Aura Session Manager и протокол SIP. Базовое администрирование

Данный курс предназначен для инженеров, которым предстоит устанавливать и эксплуатировать Avaya Aura Session Manager и протокол SIP. Курс также может быть полезен всем, кто занимается эксплуатацией телефонных станций Avaya.

Предварительная подготовка слушателя:

Обязательно знание основ построения и использования сетей передачи данных на основе протокола TCP/IP (понятия IP-адреса, маршрутизатора, коммутатора, DNS, DHCP, HTTP и т.п.).

Знание основ администрирования Avaya Aura Communication Manager в рамках базового курса: заведение телефонов, транков, настройка маршрутизации, настройка плана нумерации, основы тестирования и устранения неисправностей.

Желательно иметь представление о способах передачи голоса поверх сетей передачи данных (IP-телефония, кодеки, QoS), а также умение администрировать функции IP-телефонии на Avaya Aura Communication Manager (заведением IP-телефонов, создание IP-транков).

Продолжительность курса:24 академических часа(3 дня)

Содержание:

Тема 1.Введение в протокол SIP.

Назначение и задачи протокола SIP, стандарты SIP

Основные компоненты протокола SIP: User Agent, Registrar, Location, Proxy и др.
Адресация в SIP, SIP URI

Клиент-серверная архитектура протокола SIP: Диалог SIP, Транзакция SIP, SIP запрос и SIP ответ, основные методы и типы ответов Средства диагностики прокола SIP - Wireshark Регистрация и поиск SIP абонентов
Установление сеанса связи
Протокол описания сессий – SDP
Основные функции: перевод вызова, постановка на удержание, переадресация

Тема 2.Архитектура Avaya Aura.

Задачи и функции архитектуры Avaya Aura
Компоненты Avaya Aura: Communication manager, System Manager, Session Manager

Тема 3.Аппаратное обеспечение Avaya Common Media Servers и System Platform

Обзор серверов Avaya
S8800, S8300
DELL PowerEdge R610
HP ProLiant DL360 G7
Avaya Aura System Platform
MidSize Enterprise Platform

Тема 4.Программная архитектура Session Manager.

Security Module SM100
Service Director Service Host Management Server

Тема 5.Установка System и Session Manager.

Установка и подключение оборудования
Установка System Platform Установка System Manager Установка Session Manager
Регистрация Session Manager в System manager и Data Replication Service
Лицензирование, WebLM
Общие вопросы конфигурирования посредством System Manager. Структура и назначение элементов конфигурирования

Тема 6.Администрирование SIP абонентов.

Создание учетных записей абонентов в System Manager
Конфигурирование профилей абонентов
Подключение SIP телефонов

Тема 7.Администрирование SIP шлюзов.

Создание SIP Entity Регистрация шлюзов Маршрутизация SIP.

Тема 8.Интеграция Session Manager и Communication Manager.

Два режима работы Communication Manager: Feature Server, Software Evolution Server
Администрирование абонентов Communication Manager
Маршрутизация вызовов

Тема 9.Техническое обслуживание.

Резервное копирование
Установка патчей
Сбор диагностической информации (логи) и аварийных сообщений

Рабочая программа курса
CBR-201-1 Администрирование Citrix Branch Repeater 6.0

В этом курсе слушатели познакомятся с Citrix Branch Repeater 6.0 и получат знания, необходимые для использования данного решения по оптимизации и контролю трафика для филиалов и мобильных пользователей.

Предварительная подготовка слушателя:
Для эффективного обучения Citrix рекомендует слушателям обладать базовыми знаниями в следующих областях:

- Цели и задачи технологии виртуализации
- Вычислительная архитектура, включая вычислительные сети, устройства хранения данных, драйверы устройств и операционные системы
- Принципы установки и администрирования Windows Server 2008 R2
- Принципы виртуализации серверов, рабочих станций и приложений

Планируемые результаты обучения:
Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель сможет:

- Описывать преимущества технологии Branch Repeater
- Описывать режимы развертывания Branch Repeater, а также интеграцию с другими продуктами Citrix
- Устанавливать и настраивать Branch Repeater, Repeater VPX Branch Repeateru Repeater Plug-in, а также устранять неисправности в них
- Выполнять задачи базового администрирования, такие как настройка ускорения CIFS и MAPI, а также настройку пропускной способности канала
- Настраивать Quality of Service (QoS)
- Настраивать SSL
- Выполнять мониторинг, создавать отчеты, а также выявлять и устранять основные неисправности

Продолжительность курса: 16 академических часов (2 дня)

Содержание:

- **Тема 1: Введение в Branch Repeater**
- **Тема 2: Планирование развертывания**
- **Тема 3: Установка компонентов Branch Repeater**
- **Тема 4: Настройка основных параметров**
- **Тема 5: Настройка сервисных классов и Quality of Service**
- **Тема 6: Настройка параметров безопасности**
- **Тема 7: Мониторинг, отчеты и устранение неисправностей**

Рабочая программа курса
CXA-206I Администрирование Citrix XenApp 6.5

Курс CXA-206I предназначен для администраторов серверов и сетей, знакомых со средой Microsoft Windows, а также для системных инженеров, аналитиков, консультантов, архитекторов и администраторов предыдущих версий XenApp, желающих обновить свои навыки.
Курс научит находить и устранять неисправности в среде XenApp, оптимизировать и масштабировать среду XenApp, а также осуществлять управление XenApp при помощи EdgeSight или стандартных утилит.

Предварительная подготовка слушателя:

Знакомство с Microsoft Windows Server 2008 R2.

Опыт работы с Microsoft SQL Server или другими СУБД. Опыт работы с Active Directory и групповыми политиками.

Базовые знания о службах удаленных рабочих столов (службах терминалов) Windows Server.

Знакомство с технологиями виртуализации приложений, таких как Citrix application treaming или Microsoft App-V.

Понимание основ сетевых сервисов Windows Server, таких как DNS, IIS, балансировка нагрузки, службы общего доступа к файлам и принтерам.

Знакомство с инструментами мониторинга серверов.

Базовое понимание концепций VPN, включая SSL шифрование и сертификаты.

Продолжительность курса: 40 академических часов (5 дней)

Содержание:

Тема 1. Введение в XenApp.

Тема 2. Лицензирование XenApp. Тема 3. Установка XenApp.

Тема 4. Администрирование конфигурирования XenApp. Тема 5. Администрирование конфигурирования XenApp.

Тема 6. Передача приложений и контента.

Тема 7. Потоковое распространение приложений. Тема 8. Конфигурирование политик.

Тема 9. Управление конфигурированием нагрузки. Тема 10. Оптимизация HDX.

Тема 11. Конфигурирование приложений самообслуживания. Тема 12. Конфигурация печати.

Тема 13. Защита XenApp.

Тема 14. Мониторинг XenApp.

Тема 15. Дополнительные компоненты.

Рабочая программа курса
CXA-301I Углубленное администрирование Citrix XenApp 6.5

Курс "Углубленное администрирование Citrix XenApp 6.5" предназначен для IT-профессионалов, таких как: администраторы серверов и сетей и системные администраторы, которые знакомы со средой Microsoft Windows Server 2008 R2. Обучение также полезно для системных инженеров, аналитиков, консультантов, архитекторов и партнеров Citrix. Действующие администраторы XenApp, особенно с некоторым опытом по XenApp 6.5, а также все желающие получить сертификацию CCAA или CCEE являются идеальными кандидатами. В этом курсе обучение основано на практических занятиях и включает многочисленные упражнения, которые подкрепляют и расширяют содержание курса.

Планируемые результаты обучения:

Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель будет иметь:

Опыт работы с фермами XenApp, включая администрирование пользователей, публикацию приложений и настройку политик

Знакомство с компонентами окружения XenApp и ролями сервера

Основные знания о целях и задачах технологий виртуализации

Базовый опыт установки и администрирования Windows Server 2008 R2 со службами удаленных рабочих столов

Понимание вычислительной архитектуры, включая сети и устройства хранения, драйверы устройств и операционные системы

Базовое понимание концепций сетевой безопасности

Продолжительность курса: 40 академических часов (5 дней)

Содержание:

Тема 1: Поиск и устранение неисправностей в среде XenApp
Тема 2: Масштабирование среды XenApp Тема 3: Создание избыточности ферм Тема 4: Поддержка среды XenApp
Тема 5: Оптимизация среды XenApp
Тема 6: Оптимизация рабочей среды пользователя
Тема 7: Оптимизация печати
Тема 8: Безопасность XenApp
Тема 9: Мониторинг XenApp с помощью стандартных утилит
Тема 10: Мониторинг XenApp с помощью EdgeSight

Рабочая программа курса
CMB-207I Citrix XenApp и XenDesktop - Ускоренный курс

Ускоренный курс CMB-207I охватывает выборочное содержимое курсов CXA-206 и CXD-207 и предоставляет основные знания для эффективного управления десктопами и приложениями в дата-центрах и предоставления их в качестве сервиса пользователям, находящимся в любом месте.

Курс предназначен для IT-профессионалов, таких как системные, серверные и сетевые администраторы, обладающие опытом работы с системами MS Windows, включая Windows Server 2008 R2. Курс будет интересен администраторам XenApp, желающим улучшить свои знания и навыки в виртуализации десктопов с использованием Citrix XenDesktop. Системные инженеры, менеджеры по продажам, аналитики, консультанты и системные архитекторы также могут быть заинтересованы в прослушивании данного курса.

Предварительная подготовка слушателя:

MS Windows Server 2008 R2 и службы удаленных рабочих столов
Сетевые устройства, устройства хранения, драйвера устройств, операционные системы
Сетевые технологии: DNS, DHCP, IIS, балансировка нагрузки, службы печати, файловые службы
Active Directory и групповые политики
Принципы виртуализации серверов, десктопов и приложений

Планируемые результаты обучения:
Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель будет уметь:

Устанавливать и настраивать сервер лицензирования, импортировать лицензии, настраивать мониторинг лицензий, просматривать тенденции использования лицензий
Устанавливать и настраивать серверы XenApp для создания новой фермы или подключения к существующей;
Создавать учетные записи администраторов и назначать им соответствующие разрешения
Настраивать журналирование административных изменений в базу данных
Создавать и применять рабочие группы серверов (worker groups) для упрощения администрирования опубликованных ресурсов и политик
Устанавливать роль Web Interface
Создавать и настраивать сайты XenApp, Web Services, XenApp Services
Настраивать внешний вид, контент и макет веб-сайта XenApp
Публиковать приложения и десктопы для пользователей и контролировать поведение функции Workspace Control
Просматривать и управлять пользовательскими сессиями из административной консоли

Устанавливать ПО, необходимое для создания профилей приложений, создавать профили приложений для потоковой доставки, связывать зависимые профили для взаимодействия потоковых приложений
Публиковать потоковые приложения и проверять корректность их работы
Создавать политики для улучшения производительности, ограничения пользовательского доступа, контроля пользовательских сессий посредством Shadowing.
Тестировать политики для проверки правильности их применения
Настраивать собственные анализаторы нагрузки (Load evaluators) и применять их к серверам и приложениям
Настраивать и тестировать отказоустойчивость с использованием политик балансировки нагрузки
Устанавливать Citrix Receiver, настраивать и доставлять подключаемые пакеты, проверять возможность самостоятельного добавления приложений (self-service applications) на клиентских устройствах
Настраивать печать, включая автоматическое создание принтеров, списки совместимости драйверов, сессионные принтеры, политики печати
Настраивать веб-сайт XenApp на использование режима ICA Proxy
Определять утилиты, необходимые для мониторинга серверов и сессий XenApp
Определять дополнительные компоненты, включенные в редакцию XenApp Platinum
Настраивать серверы XenServer для предоставления десктопов
Изменять параметры виртуальных машин
Выполнять резервное копирование метаданных виртуальных машин на общий ресурс
Импортировать виртуальные машины
Устанавливать XenDesktop
Добавлять контроллер в существующий сайт
Устанавливать, настраивать и обеспечивать безопасность сервера Web Interface
Делегировать администрирование XenDesktop

Подготавливать эталонную виртуальную машину
Назначать пользователям пулы или выделенные виртуальные десктопы Изменять каталоги десктопов, их группы и эталонную виртуальную машину Выполнять мониторинг сессий XenDesktop
Контролировать пользовательские сессии XenDesktop посредством Shadowing
Устанавливать и настраивать службы Provisioning Services
Подготавливать общий vDisk
Создавать потоковые виртуальные десктопы с использованием служб Provisioning Services
Обновлять vDisk
Определять ключевые функции XenDesktop 5.5

Продолжительность курса: 40 академических часов (5 дней)

Содержание:

Часть 1. XenApp

Тема 1. Введение и обзор курса
Тема 2. Введение в базовое администрирование XenApp 6
Тема 3. Лицензирование XenApp
Тема 4. Установка XenApp
Тема 5. Настройка администрирования XenApp
Тема 6. Установка и настройка Web Interface Тема 7. Доставка приложений и контента Тема 8. Потоковые приложения
Тема 9. Настройка политик
Тема 10. Управление нагрузкой
Тема 11. Оптимизация работы пользователей
Тема 12. Настройка самообслуживающихся приложений
Тема 13. Настройка печати
Тема 14. Обеспечение безопасности XenApp
Тема 15. Мониторинг XenApp
Тема 16. Дополнительные компоненты

Часть 2. XenDesktop 5

Тема 1. Введение и обзор курса
Тема 2. Введение в XenDesktop
Тема 3. Настройка гипервизора для доставки десктопов
Тема 4. Установка и настройка XenDesktop
Тема 5. Управление каталогами и группами десктопов
Тема 6. Настройка работы пользователей
Тема 7. Мониторинг сайтов XenDesktop
Тема 8. Потоковая передача десктопов в виртуальные и физические машины
Тема 9. Создание общего vDisk’a
Тема 10. Администрирование компонентов Provisioning Services
Тема 11. Доставка локальных виртуальных десктопов
Тема 12. Новые возможности XenDesktop 5.5

Рабочая программа курса
CXD-300-4I Внедрение решений на базе Citrix XenDesktop 7 (Deploying Citrix XenDesktop 7 Solutions)

Курс предоставляет слушателям знания и навыки, необходимые для успешного внедрения законченных решений Citrix по виртуализации приложений и десктопов в среде Windows Server 2012. Курс основан на финальной версии продукта и доступен в авторизованных учебных центрах Citrix.
В процессе курса слушатели научатся, как настраивать инфраструктуру, состоящую из перечисленных компонентов Citrix: XenServer, XenDesktop, Citrix License Server, MCS, PVS, Personal vDisk, Storefront, NetScaler (ICA Proxy, Load Balancing, Endpoint Analysis), and Citrix Receiver.
По окончании курса слушатели научатся построению с нуля инфраструктуру, включающую все компоненты Citrix XenDesktop 7.

Предварительная подготовка слушателя:

Понимание концепций виртуализации серверов, десктопов и приложений; Опыт работы с Windows Server 2012, включающий:

- Active Directory
- Службы удаленных рабочих столов
- Протокол DHCP
- DNS
- Мониторинг производительности
- Объекты групповых политик

Опыт работы с MS SQL Server

Планируемые результаты обучения:
Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель сможет: Выполнять настройку гипервизора Настраивать инфраструктурные компоненты Настраивать компоненты XenDesktop 7
Настраивать ресурсы XenDesktop 7 (серверные и десктопные ОС, серверные приложения)
Настраивать профили и политики
Настраивать Provisioning Services
Выполнять тестирование для подготовки к развертыванию

Продолжительность курса: 40 академических часов (5 дней)

Содержание:

Тема 1 Понимание Citrix XenDesktop 7
Тема 2 Настройка гипервизора
Тема 3 Настройка инфраструктурных компонентов
Тема 4 Настройка инфраструктуры Citrix
Тема 5 Настройка ресурсов XenDesktop 7
Тема 6 Настройка политик

Тема 7 Настройка Provisioning Services
Тема 8 Подготовка среды к развертыванию

Рабочая программа курса
CXD-203-3I Управление решениями на базе Citrix XenDesktop

Данный курс предоставляет слушателям знания и навыки, необходимые для эффективной поддержки решений Citrix по виртуализации рабочих столов и приложений в среде Windows Server 2012. В курсе рассматриваются вопросы масштабирования решений, связанные с добавлением новых приложений, рабочих столов, ростом количества пользователей.

Предварительная подготовка слушателя:

Для успешного прослушивания курса Citrix рекомендует обладать перечисленными знаниями и навыками:

Понимание концепций виртуализации серверов, десктопов и приложений; Опыт работы с Windows Server 2012, включающий:

- Active Directory
- Домены
- Учетные записи пользователей и групп
- Подразделения
- Объекты групповых политик

Опыт работы с пользовательским интерфейсом Windows 7 и Windows 8; Опыт работы с SQL Server 2012, включающий:

- Понимание бах данных, разрешений, безопасности, кластеров и зеркалирования, обеспечения высокой доступности

Базовые знания сетевых технологий, включающие:

- Протоколы (TCP/IP, UDP, HTTP и др.)

Знание систем хранения данных (управление типами хранилищ, добавление нового хранилища);

Базовые знания о лицензировании Citrix;

Опыт работы с одним из гипервизоров (XenServer, Hyper-V, vSphere);

Базовое понимание различных типов профилей (локальные, постоянные, перемещаемые);

Базовое понимание сертификатов, их типов, удостоверяющих центров.

Планируемые результаты обучения:

Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель будет:

Понимать архитектуру, компоненты и коммуникации XenDesktop 7

Делегировать административные полномочия и управлять лицензиями

Управлять и выполнять мониторинг гипервизора Управлять приложениями и десктопами

Управлять StoreFront и внешними лицензиями Управлять политиками

Управлять профилями пользователей

Управлять сессиями, сайтами и пользователями
Управлять печатью
Управлять Provisioning Services и персональными vDisks **Продолжительность курса:** 40 академических часов (5 дней)

Содержание:

Тема 1.Понимание архитектуры Citrix XenDesktop 7
Тема 2.Делегирование административных полномочий и управление лицензиями
Тема 3.Управление и мониторинг гипервизора Тема 4.Управление приложениями и десктопами Тема 5.Управление StoreFront и внешним доступом
Тема 6.Управление политиками
Тема 7.Управление профилями пользователей
Тема 8.Управление сессиями, сайтами и пользователями
Тема 9.Управление печатью
Тема 10.Управление Provisioning Services и персональными vDisks
Тема 11.Итоги курса

Рабочая программа курса
CXD-400 Проектирование решений на базе Citrix XenDesktop

Курс рекомендован специалистам в области проектирования решений по виртуализации десктопов.

Предварительная подготовка слушателя:

Для успешного прохождения курса Citrix рекомендует обладать перечисленными знаниями и навыками:

Углубленные знания концепций и компонентов виртуализации десктопов Citrix
Базовое понимание дисциплины управления проектами и ведения соответствующей документации
Опыт проведения презентаций
Знания Windows Server (Windows Server 2012), включающие:
- AD
- DHCP

Базовые знания сетевых технологий
SQL Server – общее понимание баз данных, разрешений, безопасности, высокой доступности
Общее понимание физических и виртуальных систем хранения данных:
- NAS, SAN, SSD
- CIFS

Знание технологий гипервизоров (XenServer, Hyper-V, vSphere)

Планируемые результаты обучения:

Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель сможет:

Определять компоненты и протоколы коммуникаций для архитектуры Excalibur

Применять архитектурные принципы при проектировании решений виртуализации

Руководствоваться при проектировании требованиями и возможностями организации, существующими приложениями, количеством пользователей

Проектировать решения по виртуализации десктопов

Проверять и презентовать проектные рекомендации

Решать возможные проблемы, связанные с проектированием решений по виртуализации

Продолжительность курса: 40 академических часов (5 дней)

Содержание:

Тема 1. Архитектура

Тема 2. Определение ресурсов, процессов, условий, необходимых для развития бизнеса (business drivers)

Тема 3. Сбор данных

Тема 4. Сегментация пользователей Тема 5. Инвентаризация риложений Тема 6. Управление проектами

Тема 7. Проектирование пользователей

Тема 8. Получатели

Тема 9. Рекомендации по ресурсным требованиям

Тема 10. Доступ

Тема 11. Десктопы

Тема 12. Доставка приложений Тема 13. Доставка десктопов Тема 14. Сетевой уровень

Тема 15. Уровень платформы

Тема 16. Обслуживание

Тема 17. Верификация

Тема 18. Финальная лабораторная работа

Рабочая программа курса
CXS-203I Администрирование Citrix XenServer 6.0

Курс даст слушателям все необходимые навыки для работы с XenServer 6.0. В процессе обучения слушатель сможет проработать вопросы администрирования XenServer 6.0, управления целевыми устройствами, миграции и резервного копирования

Предварительная подготовка слушателя:

Базовые знания о технологии виртуализации.

Понимание компьютерной архитектуры, включая сети, системы хранения, драйверы устройств и операционные системы.

Базовый опыт в установке и администрировании Windows Server 2003 or Windows Server 2008.

Базовый опыт в установке и администрировании Linux.

Знание активных сетевых устройств, архитектуры корпоративных сетей, включая настройку vLAN.

Базовые знания терминологии и технологий систем хранения, включая партиции, SAN, LUNs, iSCSI, общие папки NFS и CIFS.

Продолжительность курса: 40 академических часов (5 дней)

Содержание:

Тема 1. Знакомство с XenServer.

Тема 2. Установка XenServer и XenCenter. Тема 3. Виртуальные машины с ОС Windows. Тема 4. Виртуальные машины с ОС Linux. Тема 5. Шаблоны и операции обслуживания. Тема 6. XenConvert.

Тема 7. Управление ресурсами. Тема 8. Сетевые параметры. Тема 9. Управление XenServer. Тема 10. Хранилища.

Тема 11. Ресурсные пулы. Тема 12. Наборы ресурсов.

Тема 13. Обеспечение отказоустойчивости. Тема 14. Балансировка нагрузки.

Тема 15. Поиск и устранение неполадок.

Тема 16. Установка и настройка Provisioning Services. Тема 17. Администрирование Виртуальных машин.

Рабочая программа курса
CNS-205I Основы и сетевая архитектура Citrix NetScaler 10

Целью данного курса является предоставление информации об основных концепциях Citrix NetScaler 10, а также научить слушателей навыкам, необходимым для внедрения Citrix NetScaler, его конфигурирования, мониторинга, оптимизации, обеспечения безопасности и решения возможных проблем. Курс специально разработан для слушателей, у которых нет или небольшой опыт работы с NetScaler.

Планируемые результаты обучения:

Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель сможет:

- Определять возможности и функционал NetScaler
- Описывать основные параметры сетевой архитектуры NetScaler
- Получать, устанавливать и управлять лицензиями NetScaler
- Описывать, каким образом SSL используется для обеспечения безопасности NetScaler
- Внедрять технологию NetScaler TriScale, включая кластеризацию
- Настраивать расширенные параметры балансировки сетевой загрузки и GSLB в системах NetScaler
- Оптимизировать систему NetScaler для обработки и управления сетевым трафиком
- Настраивать систему NetScaler с учетом требований к трафику и контенту
- Использовать встроенные инструменты журналирования для формирования отчетов и мониторинга
- Использовать рекомендованные методы и утилиты для решения типичных проблем, связанных с сетью NetScaler и подключениями

Продолжительность курса: 40 академических часов (5 дней)

Содержание:

Тема 1: Введение.

Тема 2: Основы сетевой архитектуры.

Тема 3: Основы балансировки загрузки.

Тема 4: Обеспечение высокой доступности.
Тема 5: Политики и выражения.
Тема 6: Переключение контента. Тема 7: Настройка соединений.
Тема 8: Global Server Load Balancing (GSLB).
Тема 9: Кластеризация.
Тема 10: Безопасность и аутентификация.
Тема 11: Rewrite, Responder и трансформация URL. Тема 12: Оптимизация трафика.
Тема 13: Расширенный мониторинг. Тема 14: Устранение неисправностей.

Рабочая программа курса
CVA-500I Построение виртуальных решений на базе Citrix

Курс CVA-500I обучает архитекторов Citrix технике анализа и разработки комплексных решений виртуализации Citrix. Курс ориентирован на IT-специалистов (к которым можно отнести администраторов серверов, сетей). Курс также рекомендован системным инженерам, аналитикам, консультантам и архитекторам.

Предварительная подготовка слушателя:

Требуется опыт работы со следующими продуктами: Citrix XenApp 4.5 или выше
Citrix XenServer 5.0 или выше
Citrix XenDesktop 3.0 или выше
Citrix Provisioning Services 5.0 или выше
Citrix EdgeSight for Load Testing 3.0
Citrix EdgeSight for Endpoints 5.0
Citrix EdgeSight for XenApp 5.0
Citrix Access Gateway Enterprise Edition 9.0 или выше
Citrix Branch Repeater 5.0 или выше
Также требуется опыт работы с Windows Server, включая:
Active Directory Terminal Services DHCP
DNS
Мониторинг производительности
Групповые политики

Слушатель должен понимать следующие технологии:

Виртуализация сервера, включая конфигурацию гипервизора и инструменты управления виртуальными машинами

Серверное оборудование, в том числе настройка NIC, питание, охлаждение
Виртуальные сети, VLAN, адресация
Системы хранения
Виртуализация приложений Citrix XenApp Citrix XenDesktop и Provisioning Services SSL VPN

Продолжительность курса: 40 академических часов (5 дней)

Содержание:

Тема 1. Управление проектами. Тема 2. Бизнес-цели.
Тема 3. Доставка операционных систем. Тема 4. Доставка приложений.
Тема 5. Виртуализация серверов. Тема 6. Инфраструктура.

Тема 7. Безопасность.
Тема 8. Управление и поддержка.
Тема 9. Разработка инфраструктуры виртуализации.
Тема 10. Планирование инфраструктуры доставки операционных систем. Тема 11. Планирование инфраструктуры доставки приложений.
Тема 12. Доставка рабочих станций. Тема 13. Планирование доступа. Тема 14. Оптимизация нагрузки.
Тема 15. Планирование непрерывности бизнеса.

Рабочая программа курса

VS5.5-TR Решение проблем в среде VMware vSphere 5.5

Курс ориентирован на системных администраторов и системных инженеров, кому необходимы знания, навыки и пути решения проблем в инфраструктурах vSphere 5.x.

Предварительная подготовка:
Слушатель должен:

Иметь практический опыт работ по настройке виртуальной инфраструктуры на основе VMware vSphere (ESX/ESXi и vCenter Server)

Планируемые результаты обучения:
Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса слушатель сможет:

Использовать Web-клиента vSphere, командную строку и файлы журналов для определения и решения проблем в vSphere.

Определять и решать проблемы SSL-сертификатов.

Определять и решать проблемы сетей и виртуальных коммутаторов. Определять и решать проблемы систем хранения данных. Определять и решать проблемы vCenter сервера.

Определять и решать проблемы гипервизора ESXi. Определять и решать проблемы кластеров vSphere. Определять и решать проблемы Vmware VMotion. Определять и решать проблемы виртуальных машин.

Продолжительность курса: 40 академических часов (5 дней)

Содержание:

Тема 1. Основы поиска и устранения проблем.

Определение системной проблемы.

Сбор информации о проблеме.

Просмотр и интерпретация диагностической информации. Определение возможных причин проблемы.

Определение первопричины проблемы. Устранение проблемы.

Тема 2. Инструменты поиска и устранения проблем.

Основы работы с командной строкой.

- Способы доступа к командной строке

- Оболочка ESXi.
- Использование vMA.
- Добавление vMA в домен AD.
- Просмотр в командной строке информации о системах хранения данных.
- Просмотр в командной строке информации о настройках сетевых интерфейсов.
- Просмотр в командной строке информации о стандартных виртуальных коммутаторах.
- Просмотр в командной строке информации о распределенных виртуальных коммутаторах.
- Просмотр в командной строке информации об аппаратном оборудовании сервера.
- Команда vmware-cmd.
- Просмотр в командной строке информации о виртуальных машинах.
- Просмотр в командной строке информации о слепках состояния (Snapshot) виртуальных машин.

Использование журналов для поиска и устранения проблем.

- Расположение журналов Vcenter.
- Расположение журналов хоста ESXi.
- Полезные для поиска проблем журналы Vcenter.
- Полезные для поиска проблем журналы ESXi.
- Просмотр журналов с помощью Web-клиента.
- Просмотр журналов с помощью DCUI.
- Использование vSphere Syslog Collector.
- Сбор диагностической информации для VMware Technical Support.
- Экспорт файлов журналов с помощью Web-клиента.
- Экспорт данных с помощью команды vm-support.

Лабораторные работы 1-3.

Тема 3. SSL-сертификаты.

Как работает SSL.

Использование SSL-сертификатов в vSphere. Процесс установки новых сертификатов. Создание CSR с помощью OpenSSL. Изменение конфигурационного файла CSR. Генерация CSR.

Генерация сертификата из CSR.

Установка и настройка сертификата для Vcenter. Установка и настройка сертификата для Web-клиента. Установка и настройка сертификата для ESXi. Распространенные проблемы установки сертификатов. Лабораторная работа 4.

Тема 4. Поиск и устранение сетевых проблем.

Обзор использования стандартных виртуальных коммутаторов. Сетевая проблема 1.

- Возможная причина: Неправильная настройка сети на ESXi.
- Возможная причина: Неправильная настройка NIC Teaming.
- Возможная причина: Не поддерживаемое или сбойное оборудование.
- Возможная причина: Медленная работа сети.

Сетевая проблема 2.

- Возможная причина: Настройки IP и проблемы межсетевого экрана.
- Возможная причина: Ошибка Windows IPSec.
- Возможная причина: Неправильные настройки портовых груп.

- Возможная причина: Проблемы передачи данных на ESXi.
- Возможная причина: Нет свободных портов на виртуальном коммутаторе.

Лабораторные работы 5-7.

Сетевая проблема 3.

- Передача пакетов между vCenter и ESXi.
- Определение возможных причин проблемы.
- Возможная причина: Порт заблокирован межсетевых экраном Windows.
- Возможная причина: vCenter сервер не использует порт 902.
- Возможная причина: Высокая загрузка сетевого канала.

Сетевая проблема 4.

- Предотвращение потери сетевого управления.

Использование технологии Host Networking Rollback.

Обзор использования технологии Distributed Switch Rollback.

- Восстановление потери управляющей сети: стандартный виртуальный коммутатор.
- Восстановление потери управляющей сети: распределенный виртуальный коммутатор.
- Использование распределенных виртуальных коммутаторов.
- Восстановление после неправильной настройки распределенного виртуального коммутатора.
- Создание резервной копии конфигурации распределенного виртуального коммутатора.
- Восстановление и импортирование сохраненной конфигурации распределенного виртуального коммутатора.

Лабораторные работы 8-13.

Тема 5. Поиск и устранение проблем систем хранения данных.

Обзор vSphere Storage.

Обзор вариантов подключения iSCSI систем хранения.

Проблема системы хранения 1.

- Возможная причина: проблемы оборудования.
- Возможная причина: Плохая производительность iSCSI систем хранения.
- Возможная причина: Неправильная настройка интерфейса VMkernel.
- Возможная причина: Неправильная настройка iSCSI HBA.
- Возможная причина: Нет обмена данных с iSCSI-портом.
- Возможная причина: Неправильная настройка NFS.
- Возможная причина: Несоответствие метаданных VMFS.
- Лабораторные работы 14-18.

Проблема системы хранения 2.

- Ситуация Permanent Data Loss.
- Ситуация All Path Down.
- Возможная причина: Неправильная настройка NIC Teaming.
- Возможная причина: Неправильно настроенная политика выбора пути.
- Лабораторные работы 19-22.

Тема 6. Поиск и устранение проблем кластеров vSphere.

Обзор vSphere HA.

Проблема кластера vSphere HA 1.

- Возможная причина: Неправильная настройка кластера vSphere HA.
- Возможная причина: Отсутствует доступ к Heartbeat Datastore.
- Возможная причина: FDM-агент не устанавливается на хосте ESXi.
- Возможная причина: Потеря связи с хостом.

Проблема кластера vSphere HA 2.

- Возможная причина: Завышенные значения резервирования виртуальных машин.
- Возможная причина: Неправильная настройка Admission Control.
- Возможная причина: Недостаточное количество ресурсов в ресурсном пуле.

Обзор vMotion. Проблема vMotion 1.

- Возможная причина: Неправильная настройка фейса VMkernel.
- Возможная причина: Ошибки настройки виртуальной инфраструктуры.
- Возможная причина: Отсутствует необходимое дисковое пространство.
- Возможная причина: Не выполняются требования резервации ресурсов.
- Возможная причина: Параметр log.rotateSize установлен в значение “Low”.

Проблема vMotion 2.

- Возможная причина: Неправильная настройка DRS.

Лабораторные работы 23-33.

Тема 7.Поиск и устранение проблем сервера vCenter и ESXi.

ОбзорVMwareSingleSignOn.

Проблема SSO 1.

- Возможная причина: Отсутствует доступ к базе данных SSO.
- Возможная причина: Просрочен пароль доступа к базе данных SSO.

Проблема vCenter 1.

- Возможная причина: Неправильная настройка ODBC.
- Возможная причина: Заняты порты 902, 80 и 443.
- Возможная причина: Сервис VMware VCMSDS не запущен.

Проблема vCenter 2.

- Рост базы данных vCenter.
- Контролирование заданий с помощью заданий Rollup.
- Реинициализация базы данных vCenter.

Проблема ESXi 1.

- Проверка краха хоста ESXi.
- Восстановление хоста после PSOD.

Проблема ESXi 2.

- Проверка подвисания хоста ESXi.
- Восстановление хоста после подвисания.

Лабораторные работы 34-42.

Тема 8.Поиск и устранение проблем виртуальных машин.

Обзор используемых файлов виртуальных машин. Идентификаторы Content ID в файлах-слепках. Проблема виртуальных машин 1.

- Несоответствие значений Content ID в файлах-слепках виртуальной машины.

Проблема виртуальных машин 2.

- Решение проблемы выполнения Quiesce при создании слепка виртуальной машины

Проблема виртуальных машин 3.

- Решение проблемы отсутствия слепков в Snapshot Manager.

Проблема виртуальных машин 4.

- Возможная причина: Нет полномочий для создания слепков.
- Возможная причина: Отсутствует Delta Discriptor файл.
- Возможная причина: Достигнут максимальный размер файла.
- Возможная причина: Недостаточно места на хранилище данных.

Проблема виртуальных машин 5.

- Отсутствуют файлы виртуальной машины.
- Файл виртуальной машины заблокирован.
- Недостаточно ресурсов на хосте ESXi.
- Обзор состояний виртуальной машины.

Лабораторные работы 43-45.

Проблема виртуальных машин 6.

- Возможная причина: Выполняются операции vMotion или DRS Migration.
- Возможная причина: Виртуальная машина удалена вне vCenter сервера.
- Возможная причина: Наличие недопустимых символов в файле vmx.
- Возможная причина: Заполнение на хосте ESXi Root Filesystem.

Проблема виртуальных машин 7.

- Возможная причина: Неправильно указана операционная система.
- Не подключается образ ISO.
- Не найден образ ISO.
- Поврежден образ ISO с VMware Tools.

Лабораторные работы 46-50.

в ОС Windows

Рабочая программа курса ADVANCED-IPS Управление системами предотвращения вторжений CheckPointAdvanced IPS

Цель этого курса обучить слушателей расширенным знаниям по настройке и использованию CheckPoint IPS SoftwareBlade. Курс обеспечивает необходимые навыки для создания клиентского профиля, анализа статистики, обеспечения безопасности данных и решения проблем различного уровня сложности.

Предварительная подготовка:

Слушатели должны иметь:

- Хорошие знания операционных систем Windows и UNIX
- Общие знания принципов работы сетей передачи данных.
- Хорошие знания стека протоколов TCP/IP
- Знание основных принципов работы сети Интернет
- Опыт работы с продуктами CheckPoint не менее шести месяцев

Планируемые результаты обучения:

Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по

данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса вы:

- Узнаете стратегии развертывания IPS
- Научитесь использовать сервис GeoProtection для контроля траффика
- Научитесь обнаружению атак, вирусов, червей
- Обсудите основные компоненты архитектуры IPS EventAnalysis
- Получите обзор преимуществ SecureXL и CoreXL
- Узнаете функции PSL
- Научитесь настраивать DNS сервера, веб-сервера и почтовые сервера для реализации IPS защиты.

Продолжительность курса: 16 академических часов (2 дня)

Содержание курса.

- **Лабораторные работы:**
  - Конфигурация IPS SoftwareBlade
  - Тестирование политик безопасности и демонстрация инструментов
  - Развертывание GeoProtection в IPS
  - Тестирование IPS GeoProtection
  - Создание новых профилей
  - Загрузка. Установка, использование и обновление IPS Protections
  - Предотвращение различного рода атак
  - Настройка параметров
  - Траблшутинг

Рабочая программа курса
CCES-R80 Внедрение системы защиты безопасности информации при помощи CheckPointEndpointSecurity R80

Цель этого курса – обучить слушателей навыкам развертывания, настройки, администрирования и обеспечения безопасности сети предприятия с помощью новой версии CheckPointEndpointSecurity**.**

Предварительная подготовка:

Слушатели должны иметь:

- Общие знания сетевых технологий
- Опыт администрирования ОС Windows
- Понимание задач по обеспечению безопасности рабочих станций.

Планируемые результаты обучения:

Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса вы сможете:

- Планировать решения по обеспечению безопасности сети с помощью

CheckPointEndpointSecurity

- Развертывать спроектированные вами решения
- Управлять и администрировать CheckPointEndpointSecurity, в том числе удаленно
- ИнтегрироватьCheck Point Endpoint Security с Microsoft Active Directory
- Вести мониторинг и строить отчеты о работе CheckPointEndpointSecurity
- Обеспечивать комплексную защиту сети предприятия с помощью CheckPointEndpointSecurity

Продолжительность курса:24 академических часа (3 дня)

Содержание курса:

- Обзор EndpointSecurity.
- EndpointSecuritySoftwareBlades
- Архитектура EndpointSecurity.
- Развертывание EndpointSecurity.
- Управление EndpointSecurity.
- Интеграция с Active Directory
- Мониторинг и Отчеты.
- Политика безопасности.
- Удаленный доступ
- Firewall and SecurityComplianceVerification
- FullDiskEncryption
- MediaEncryption and Port Protection
- AntiMalware and Program Control
- WebCheckSecureBrowsing
- TotalEndpointSecurity

Рабочая программа курса
CCSA-R77 Администрирование Check Point Certified Security Administrator R77

Цель этого курса обучить слушателей базовым знаниям и навыкам, необходимым для конфигурирования и эксплуатации файрволаCheckPoint. Вы научитесь конфигурировать параметры работы сервера управления и шлюзов CheckPoint, создавать политики безопасности, проводить мониторинг работы всех частей файрвола, строить VPN туннели между шлюзами CheckPoint.

Предварительная подготовка:

Слушатели должны иметь:

- Хорошее знание операционных систем Windows и UNIX
- Общие знания принципов работы сетей передачи данных.
- Хорошие знания стека протоколов TCP/IP
- Знание основных принципов работы сети Интернет

Планируемые результаты обучения:
Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по

данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса вы:

- Научитесь проводить распределенную инсталляцию файрвола **CheckPoint**.
- Изучите механизмы резервного копирования и восстановления системы
- Научитесь создавать сетевые объекты
- Научитесь развертывать сетевые шлюзы, используя веб интерфейс **Gaia**
- Оценивать существующие политики и оптимизировать требования системы
- Научитесь управлять локальными учетными записями пользователей и работать с удаленными серверами аутентификации
- Научитесь использовать возможности **SmartUpdate** для управления лицензиями и обновления ПО шлюзов.
- Научитесь устанавливать, настраивать и использовать возможности IdentityAwareness
- Познакомитесь с настройкой VPN туннелей.

Продолжительность курса: 24 академических часа (3 дня)

Содержание курса:

- **Основные темы курса:**
  - Обзор технологий **CheckPoint**
  - Знакомство с оборудованием
  - Создание политики файрвола.
  - Мониторинг трафика и соединений
  - Использование сервиса NAT
  - Аутентификация пользователей
  - Использование **SmartUpdate**
  - Использование программного блейда **IdentityAwareness**
  - Построение **VPN**
- **Лабораторные работы:**
  - Установка сетевых шлюзов
  - Использование инструментов системы
  - Создание политики безопасности
  - Настройка **DMZ**
  - Настройка **NAT**
  - Мониторинг траффика
  - Аутентификация пользователей
  - Использование **IdentityAwareness**
  - Site-to-site VPN.

Рабочая программа курса
БТ01 Безопасность информационных технологий

Целью этого курса является обучение слушателей технологиям обеспечения информационной безопасности, рациональному распределению функций и организации эффективного взаимодействия по вопросам защиты информации всех подразделений и сотрудников, использующих и обеспечивающих функционирование автоматизированных систем. В курсе подробно рассматриваются вопросы разработки нормативно-методических и организационно-распорядительных документов с учетом требований российского

законодательства, национальных и международных стандартов (BS 7799, ISO/IEC 27002, ISO/IEC 27001, ISO/IEC 15408, ISO/IEC TR 13335, NIST и др.), необходимых для реализации рассмотренной технологии обеспечения информационной безопасности. Среди прочего в курсе анализируются возможности различных видов программных и программно-аппаратных средств защиты информации, даются рекомендации по выбору рациональных вариантов и решений по их эффективному применению для противодействия угрозам безопасности автоматизированных систем.

Программа данного учебного курса согласована с Федеральной службой по техническому и экспортному контролю в качестве программы курса повышения квалификации и профессиональной подготовки руководителей и специалистов подразделений технической защиты информации.

Обучение на данном курсе является обязательным условием для получения в Учебном центре «Информзащита» государственного документа о повышении квалификации по направлению «Безопасность информационных технологий», необходимого для получения организацией лицензии на деятельность по технической защите конфиденциальной информации.

Предварительная подготовка:

Слушатели должны иметь:

- Общие представления об информационных системах
- Представления о правовых, организационных и технических аспектах обеспечения информационной безопасности автоматизированных систем.

Планируемые результаты обучения:

Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса вы сможете:

- разрабатывать основные положения концепции построения и эффективного применения комплексных систем защиты информации в автоматизированных системах;
- планировать защиту и рационально распределять соответствующие функции между подразделениями и сотрудниками предприятия, организовывать их взаимодействие на различных этапах жизненного цикла автоматизированных систем;
- организовывать деятельность служб технической защиты информации в действующих и проектируемых системах защиты информации;
- проводить информационные обследования и анализ рисков автоматизированных систем;
- разрабатывать организационно-распорядительные документы по вопросам защиты информации;
- ориентироваться в проблемах информационной безопасности в сетях Интернет/Интранет, уязвимостях сетевых протоколов и служб, атаках в IP-сетях;
- ориентироваться в средствах защиты информации от несанкционированного доступа, межсетевых экранах, средствах контроля контента, средствах анализа защищенности и средствах обнаружения атак для обеспечения информационной безопасности в IP-сетях;

- обоснованно выбирать необходимые программные и программно-аппаратные средства защиты информации в автоматизированных системах;
- организовывать поиск и использование оперативной информации о новых уязвимостях в системном и прикладном программном обеспечении, а также других актуальных для обеспечения информационной безопасности данных.

Продолжительность курса: 40 академических часов (5 дней)

Содержание курса:

- **Тема 1. Основы безопасности информационных технологий**
  - Актуальность проблемы обеспечения безопасности информационных технологий. Место и роль автоматизированных систем в управлении бизнес-процессами. Основные причины обострения проблемы обеспечения безопасности информационных технологий.
  - Основные понятия в области безопасности информационных технологий. Что такое безопасность информационных технологий. Информация и информационные отношения. Субъекты информационных отношений, их интересы и безопасность, пути нанесения им ущерба. Основные термины и определения. Конфиденциальность, целостность, доступность. Объекты, цели и задачи защиты автоматизированных систем и циркулирующей в них информации.
  - Угрозы безопасности информационных технологий. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем. Угрозы безопасности информации, автоматизированных систем и субъектов информационных отношений. Основные источники и пути реализации угроз. Классификация угроз безопасности и каналов проникновения в автоматизированную систему и утечки информации. Основные непреднамеренные и преднамеренные искусственные угрозы. Неформальная модель нарушителя.
  - Виды мер и основные принципы обеспечения безопасности информационных технологий. Виды мер противодействия угрозам безопасности. Достоинства и недостатки различных видов мер защиты. Основные принципы построения системы обеспечения безопасности информации в автоматизированной системе.
  - Правовые основы обеспечения безопасности информационных технологий. Законы Российской Федерации и другие нормативные правовые акты, руководящие и нормативно-методические документы, регламентирующие отношения субъектов в информационной сфере и деятельность организаций по защите информации. Защита информации ограниченного доступа, права и обязанности субъектов информационных отношений. Лицензирование деятельности, сертификация средств защиты информации и аттестация объектов информатизации. Требования руководящих документов ФСТЭК России и ФСБ России. Вопросы законности применения средств криптографической защиты информации. Ответственность за нарушения в сфере защиты информации.
  - Государственная система защиты информации. Состав государственной системы защиты информации. Организация защиты информации в системах и средствах информатизации и связи. Контроль состояния защиты информации. Финансирование мероприятий по защите информации.
  - Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты. Идентификация и аутентификация пользователей.

Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированных систем. Регистрация и оперативное оповещение о событиях безопасности. Криптографические методы защиты информации. Контроль целостности программных и информационных ресурсов. Обнаружение атак. Защита периметра компьютерных сетей. Управление механизмами защиты.

- **Тема 2. Обеспечение безопасности информационных технологий**
  - Организационная структура системы обеспечения безопасности информационных технологий. Понятие технологии обеспечения безопасности информации и ресурсов в автоматизированной системе. Цели создания системы обеспечения безопасности информационных технологий. Регламентация действий пользователей и обслуживающего персонала автоматизированной системы. Политика безопасности предприятия. Основные организационные и организационно-технические мероприятия по созданию и обеспечению функционирования комплексной системы защиты информации. Распределение функций по обеспечению безопасности информационных технологий. Система организационно-распорядительных документов по обеспечению безопасности информационных технологий.
  - Обязанности конечных пользователей и ответственных за обеспечение безопасности информационных технологий в подразделениях. Общие правила обеспечения безопасности информационных технологий при работе сотрудников с ресурсами автоматизированной системы. Обязанности ответственного за обеспечение безопасности информации в подразделении. Ответственность за нарушения. Порядок работы с носителями ключевой информации.
  - Документы, регламентирующие правила парольной и антивирусной защиты. Инструкции по организации парольной и антивирусной защиты.
  - Документы, регламентирующие порядок допуска к работе и изменения полномочий пользователей автоматизированной системы. Инструкция по внесению изменений в списки пользователей. Правила именования пользователей. Процедура авторизации сотрудников. Обязанности администраторов штатных и дополнительных средств защиты.
  - Документы, регламентирующие порядок изменения конфигурации аппаратно-программных средств автоматизированной системы. Обеспечение и контроль физической целостности и неизменности конфигурации аппаратно-программных средств автоматизированных систем. Регламентация процессов обслуживания и осуществления модификации аппаратных и программных средств. Процедура внесения изменений в конфигурацию аппаратных и программных средств защищенных серверов и рабочих станций. Экстренная модификация (обстоятельства форс-мажор).
  - Регламентация процессов разработки, испытания, опытной эксплуатации, внедрения и сопровождения задач. Взаимодействие подразделений на этапах проектирования, разработки, испытания и внедрения новых автоматизированных подсистем.
  - Определение требований к защите и категорирование ресурсов. Положение о категорировании ресурсов. Проведение информационных обследований и анализ подсистем автоматизированной системы как объекта защиты. Определение градаций важности и соответствующих уровней обеспечения защиты ресурсов. Проведение обследований подсистем, инвентаризация, категорирование и документирование защищаемых ресурсов автоматизированных систем.

- Планы защиты и планы обеспечения непрерывной работы и восстановления подсистем автоматизированной системы. Регламентация действий при возникновении кризисных ситуаций.
- Основные задачи подразделения обеспечения безопасности информационных технологий. Организация работ по обеспечению безопасности информационных технологий. Организационная структура, основные функции подразделения безопасности.
- Концепция безопасности информационных технологий предприятия. Документальное оформление вопросов, отражающих официально принятую систему взглядов на проблему обеспечения безопасности информационных технологий, в качестве методологической основы для формирования и проведения в организации единой политики в области обеспечения информационной безопасности для принятия управленческих решений и разработки практических мер по воплощению данной политики в жизнь.

- **Тема 3. Средства защиты информации от несанкционированного доступа**
  - Назначение и возможности средств защиты информации от несанкционированного доступа. Задачи, решаемые средствами защиты информации от несанкционированного доступа.
  - Рекомендации по выбору средств защиты информации от несанкционированного доступа. Распределение показателей защищенности по классам для автоматизированных систем. Требования руководящих документов ФСТЭК России к средствам защиты информации от несанкционированного доступа. Рекомендации по выбору средств защиты информации от несанкционированного доступа.
  - Аппаратно-программные средства защиты информации от несанкционированного доступа. Краткий обзор существующих на рынке средств защиты информации от несанкционированного доступа. Существующие средства аппаратной поддержки. Задача защиты от вмешательства посторонних лиц и аппаратные средства аутентификации.
  - Возможности применения штатных и дополнительных средств защиты информации от несанкционированного доступа. Стратегия безопасности и сертифицированные решения Microsoft. Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированной системы. Защита от несанкционированной модификации программ и данных. Защита данных от несанкционированного копирования и перехвата средствами шифрования. Регистрация событий, имеющих отношение к безопасности. Оперативное оповещение о зарегистрированных попытках несанкционированного доступа. Управление средствами защиты.

- **Тема 4. Обеспечение безопасности компьютерных систем и сетей**
  - Проблемы обеспечения безопасности в компьютерных системах и сетях. Типовая корпоративная сеть. Уровни информационной инфраструктуры корпоративной сети. Сетевые угрозы, уязвимости и атаки. Средства защиты сетей.
  - Назначение, возможности, и основные защитные механизмы межсетевых экранов (МЭ). Назначение и виды МЭ. Основные защитные механизмы, реализуемые МЭ. Основные возможности и варианты размещения МЭ. Достоинства и недостатки МЭ. Основные защитные механизмы: фильтрация пакетов, трансляция сетевых адресов, промежуточная аутентификация, script rejection, проверка почты, виртуальные частные сети, противодействие атакам,

нацеленным на нарушение работоспособности сетевых служб, дополнительные функции. Общие рекомендации по применению. Политика безопасности при доступе к сети общего пользования. Демилитаризованная зона. Назначение, особенности и типовая схема «HoneyNet».

- Анализ содержимого почтового и Web трафика (Content Security). Системы анализа содержимого. Компоненты и функционирование систем контроля контента (электронная почта и HTTP трафик). Политики безопасности, сценарии и варианты применения и реагирования.
- Виртуальные частные сети (VPN). Назначение, основные возможности, принципы функционирования и варианты реализации VPN. Структура защищенной корпоративной сети. Варианты, достоинства и недостатки VPN-решений. Общие рекомендации по их применению. Решение на базе ОС Windows 2003. VPN на основе аппаратно-программного комплекса шифрования «Континент». Угрозы, связанные с использованием VPN.
- Антивирусные средства защиты. Общие правила применение антивирусных средств в автоматизированных системах. Технологии обнаружения вирусов. Возможные варианты размещение антивирусных средств. Антивирусная защита, как средство нейтрализации угроз.
- Обнаружение и устранение уязвимостей. Назначение, возможности, принципы работы и классификация средств анализа защищенности. Место и роль в общей системе обеспечения безопасности. Сравнение возможностей с межсетевыми экранами. Средства обеспечения адаптивной сетевой безопасности. Варианты решений по обеспечению безопасности сети организации. Обзор средств анализа защищенности сетевого уровня и уровня узла. Специализированный анализ защищенности.
- Мониторинг событий безопасности. Категории журналов событий. Способы построения, дополнительные компоненты и реализация инфраструктуры управления журналами событий. Технология обнаружения атак. Классификация систем обнаружения атак. Специализированные системы обнаружения атак.

Рабочая программа курса
БТ02 Защита конфиденциальной информации от утечки по техническим каналам

Цель этого курса обучить слушателей теоретическим знаниям по вопросу обеспечения безопасности информации и защиты от ее утечки по техническим каналам и провести практическую подготовку к использованию методов и средств выявления и блокирования технических каналов утечки информации.

В процессе обучения подробно рассматриваются организационно-правовые вопросы создания (усовершенствования) и эффективного функционирования службы защиты информации на предприятиях различных форм собственности и видов деятельности, концептуальные вопросы информационной безопасности предприятия. Программа включает изучение технических каналов утечки информации, их классификацию и механизмы возникновения, методики оценки возможностей технических средств разведки, используемой для экономического шпионажа. Особое внимание уделяется методам и средствам выявления и блокирования технических каналов утечки информации, новейшим технологиям и средствам защиты информации, а также контролю эффективности принятых мер защиты.

Для проведения практических работ используется широкий спектр современного оборудования ведущих российских производителей средств защиты конфиденциальной информации от утечки по техническим каналам. Занятия проходят в лаборатории, оснащенной современным поисковым оборудованием и средствами активной защиты. В рамках практических занятий и в ходе учебных поисковых мероприятий специалисты в индивидуальном порядке обучаются работе с техническими средствами поиска подслушивающих устройств (индикаторами поля, сканирующими приемниками, программно-аппаратными комплексами, универсальными приборами, нелинейными локаторами и т.п.), осуществляют поиск, обнаружение демаскирующих признаков и локализацию закладочных устройств.

Обучение на данном курсе является обязательным условием для получения в Учебном центре "Информзащита" государственного документа о повышении квалификации по направлению "Комплексная защита конфиденциальной информации в организации", необходимого для получения организацией лицензии на деятельность по технической защите конфиденциальной информации.

Предварительная подготовка:
Слушатели должны иметь:

- Общие представления о правовых, организационных и технических аспектах обеспечения безопасности информации
- Базовые знания по физике и радиотехнике.

Планируемые результаты обучения:
Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса вы сможете:

- изучить характеристики и особенности применения основных приборов и оборудования, используемых для
- выявления технических каналов утечки конфиденциальной информации;
- применять средства оценки защищенности информации от утечки по техническим каналам;
- приобрести практические навыки по выбору и применению необходимых средств защиты конфиденциальной информации;
- осуществлять контроль эффективности принятых мер.

Продолжительность курса: 40 академических часов (5 дней)

Содержание курса:

Тема 1. Правовые основы обеспечения защиты конфиденциальной информации

- Государственная система защиты информации в Российской Федерации.
- Законы Российской Федерации и другие нормативно-правовые документы, регламентирующие отношения субъектов в информационной сфере идеятельность организаций по технической защите конфиденциальной информации. Техническая защита конфиденциальной информации, обязанности и права субъектов информационных отношений. Лицензирование деятельности по технической защите конфиденциальной информации, сертификация средств защиты

информации и аттестация объектов информатизации. Требования руководящих документов ФСТЭК России и ФСБ России.

Тема 2. Технические каналы утечки информации

- Вводная часть. Особенности утечки информации. Возможные каналы утечки информации. Их краткая характеристика.
- Каналы утечки речевой информации. Акустический и виброакустический каналы. Краткая характеристика речевой информации. Особенности распространения звуковых колебаний в различных средах. Примеры, механизмы реализации.
- Утечка речевой информации по проводным коммуникациям. Акустоэлектрические преобразования и высокочастотное «навязывание» (облучение).
- Каналы утечки информации, возникающие при эксплуатации средств вычислительной техники. Побочные электромагнитные излучения и наводки (ПЭМИН). Физические основы возникновения каналов утечки информации за счет ПЭМИН. Структура каналов, особенности реализации. Примеры, механизмы реализации.
- Физические основы функционирования канала утечки акустической информации, возникающего за счет прямого и модуляционного акустоэлектрических преобразований. Механизмы реализации. Электромагнитный, электродинамический, и др. эффекты. Примеры реализации.
- Физические основы функционирования канала утечки акустической информации, возникающего за счет параметрических преобразований. Механизмы модуляции, в том числе параметрической.
- Физические основы функционирования канала утечки акустической информации, возникающего за счет оптико-электронного (лазерного) излучения. Особенности выявления и защиты от съема информации по данному каналу.
- Особенности утечки информации по техническим каналам с использованием закладочных устройств. Краткая характеристика возможных каналов утечки информации используемых закладочными устройствами. Структура и демаскирующие признаки закладочных устройств. Особенности их выявления и нейтрализации.
- Основные критерии оценки защиты информации от утечки по техническим каналам.

Тема 3. Основы организации и обеспечения работ по технической защите конфиденциальной информации

- Цели и задачи технической защиты конфиденциальной информации. Способы и средства их реализации. Классификация способов и средств технической защиты конфиденциальной информации. Основные механизмы защиты.
- Подходы к созданию комплексной системы защиты конфиденциальной информации в организации. Определение перечня сведений конфиденциального характера, составляющих коммерческую тайну в организации. Общая последовательность и методика принятия управленческого решения на организацию защиты информации. Оценка обстановки. Выявление проблем. Постановка задачи на организацию технической защиты конфиденциальной информации. Определение путей и очередности решения вопросов технической защиты конфиденциальной информации. Разработка

вариантов дальнейших действий. Моделирование, оценка эффективности и выбор оптимального варианта организационно-технических мер защиты. Формулирование управленческого решения. Разработка директивных указаний подчиненным.

- Структура подразделений технической защиты информации. Основные принципы построения системы защиты конфиденциальной информации в организации. Функции и задачи подразделений технической защиты информации. Разработка концепции и политики информационной безопасности организации.
- Аттестация объектов информатизации, как комплекс организационно-технических мероприятий, подтверждающий соответствие защищаемого объекта требованиям стандартов или иных нормативно-технических документов по безопасности информации. Планирование работ по технической защите конфиденциальной информации. Обоснование требований к системе защиты конфиденциальной информации. Требования к применяемым техническим средствам защиты информации.

- **Тема 4. Средства оценки защищенности конфиденциальной информации от утечки по техническим каналам**
  - Методы оценки защищенности информации от утечки по техническим каналам. Модель канала утечки. Принципы оценки. Соотношение сигнал-шум. Методы достижения условий защищённости. Принципы проведения замеров и расчётов.
  - Обзор средств контроля защищенности. Состав контрольно-измерительной аппаратуры для проведения измерений уровней акустических (вибрационных) сигналов. Состав контрольно-измерительной аппаратуры для проведения измерений напряженности электромагнитного поля ПЭМИ от технических средств, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации. Состав контрольно-измерительной аппаратуры для проведения измерений напряжения, наведенного в токопроводящих коммуникациях информативного сигнала.
- **Тема 5. Типовые средства защиты конфиденциальной информации и особенности их эксплуатации**
  - Общая характеристика средств защиты информации от утечки по техническим каналам. Их назначение, реализуемые функции, состав. Фильтры частотные. Ограничители малых сигналов. Генераторы шума. Принципы их работы. Конструктивные решения. Обзор моделей. Технические характеристики. Особенности применения. Рекомендации по выбору средств защиты информации по видам объектов обрабатывающих конфиденциальную информацию: каналы связи, помещения для ведения конфиденциальных переговоров, автоматизированные системы и т.д. Рекомендации по установке, настройке и эксплуатации.
  - Обзор средств активной защиты: акустика, виброакустика, системы виброакустического зашумления, средства защиты слаботочных линий, постановщики помех сотовым телефонам, диктофонам.
  - Обзор средств выявления демаскирующих признаков закладочных устройств. Средства радиоконтроля, поисковая техника, средства неразрушающего контроля, досмотровая техника, средства дозиметрии. Изучение универсальных поисковых приборов, средств контроля проводных коммуникаций, средств активной защиты, подавителей диктофонов, сотовых телефонов, постановщиков помех.

- Средства защиты от утечки по каналам ПЭМИН. Назначение. Обзор моделей. Технические характеристики, особенности применения. Рекомендации по выбору, установке, настройке и эксплуатации. Генераторы шума. Диапазон. Размещение и выбор в зависимости от уровня опасного сигнала. Доработанные по специальным требованиям основные технические средства и системы. Назначение. Обзор моделей. Технические характеристики. Особенности применения. Рекомендации по выбору, установке, настройке и эксплуатации.
- Средства защиты сети питания. Назначение. Обзор моделей. Технические характеристики. Особенности применения. Частотные фильтры. Особенности и принципы работы. Задерживающие и поглощающие. Построение системы электропитания и заземления. Линейное зашумление. Ограничители малых сигналов. Оценка эффективности. Линейные генераторы шума. Особенности применения. Оценка эффективности. Разнос, экранирование линий.
- Устройства защиты телефонных линий. Назначение. Обзор моделей. Технические характеристики. Особенности применения. Рекомендации по выбору, установке, настройке и эксплуатации.
- Рекомендации по проектированию, созданию и эксплуатации комплексных систем защиты конфиденциальной информации.
- Организация и осуществление работ по выявлению технических каналов утечки информации, образованных при помощи закладочных устройств. Выявление демаскирующих признаков закладочных устройств при поиске.

Рабочая программа курса

КП32 Защита персональных данных

В июле 2011 года были внесены значительные изменения в Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных». За последнее время особенности обработки персональных данных определены также другими законами, принят целый ряд постановлений Правительства РФ, нормативно-правовых актов и методических документов уполномоченных органов власти.

Цель этого учебного курса заключается в том, чтобы помочь специалистам различных категорий, от руководителей предприятий и их структурных подразделений до лиц, ответственных за организацию обработки персональных данных, обеспечить работу с персональными данными в соответствии с требованиями российских законов, тщательно проанализировать изменения в законодательстве и их последствия для деятельности предприятий и организаций.

В течение двух дней будет рассмотрен весь комплекс мероприятий по обеспечению правомерности и конфиденциальности обработки персональных данных с использованием правовых, организационных и технических мер, способы снижения рисков утечки персональных данных и наложения штрафных санкций со стороны государственных надзорных органов. На практических примерах будут разобраны действия операторов персональных данных в рамках трудовых отношений с собственным персоналом, гражданско-правовых отношений, связанных с передачей и предоставлением персональных данных третьим лицам, в том числе органам государственной власти, их распространением и раскрытием.

Особое внимание в курсе уделяется практическим вопросам защиты персональных данных: разработке внутренних нормативных документов, классификации информационных систем,

созданию модели угроз, реализации мер защиты, подготовке уведомлений в уполномоченный орган по защите прав субъектов персональных данных и др.

В курсе рассматриваются проблемы минимизации рисков, связанных с обработкой персональных данных, и затрат на их защиту, в том числе – при передаче обработки персональных данных на аутсорсинг внешним организациям.

Предварительная подготовка:

Слушатели должны иметь:

- Общее представление о правовых, организационных и технических аспектах защиты сведений ограниченного доступа, основах законодательства в области защиты прав граждан и обеспечения безопасности.

Планируемые результаты обучения:

Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса вы сможете:

- готовить внутренние нормативные документы, обеспечивающие защиту персональных данных;
- формировать модель угроз персональным данным;
- строить систему технической защиты персональных данных в соответствии с требованиями государственных регуляторов;
- готовить уведомления в уполномоченный орган по защите прав субъектов персональных данных.

Продолжительность курса: 16 академических часов (2 дня)

Содержание курса:

- **Тема 1. Введение. Персональные данные в организации (на предприятии)**
  - Защита персональных данных как реализация конституционных прав граждан на неприкосновенность частной жизни.
  - Международное законодательство и национальное законодательство зарубежных стран о защите персональных данных.
  - Персональные данные в системе документооборота предприятия. Персональные данные в автоматизированных системах и приложениях.
  - Значимые утечки персональных данных в России.
- **Тема 2. Основные понятия Федерального закона «О персональных данных»**
  - Основные понятия. Персональные данные в Федеральном законе и Трудовом кодексе РФ. Содержание категории «персональные данные».
  - Область применения закона. Ограничения.
  - Обработка персональных данных: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.
  - Принципы обработки персональных данных.
  - Условия обработки персональных данных. Согласие субъекта. Обработка

биометрических данных. Трансграничная передача персональных данных. Особенности обработки персональных данных в государственных или муниципальных информационных системах персональных данных (ИСПДн).
  - Специальные категории персональных данных и особенности их обработки.
  - Права субъектов персональных данных и их соблюдение при обработке.
  - Обязанности оператора персональных данных в ходе сбора и обработки персональных данных, ответы на запросы субъектов. Прекращение обработки.
  - Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных законом и принятыми в соответствии с ним нормативно-правовыми актами.
  - Уведомления об обработке персональных данных в уполномоченный орган по защите прав субъектов персональных данных.
  - Ответственность за нарушение требований по обращению с персональными данными: гражданско-правовая, уголовная, административная, дисциплинарная, материальная. Практика правоприменения.
- **Тема 3. Работа с персональными данными на предприятии (в организации)**
  - Мероприятия по защите сведений ограниченного доступа. Практические шаги по приведению порядка обработки в соответствие с требованиями законодательства. Правовые основания обработки персональных данных. Получение согласия субъектов на обработку. Содержание договоров с субъектами в части обработки персональных данных.
  - Ограничение доступа к персональным данным. Учет лиц, допущенных к персональным данным. Определение порядка обращения с такими сведениями, контроля за его соблюдением. Организация доступа пользователей к ИСПДн.
  - Внутренние нормативные документы по обработке персональных данных и обеспечению их безопасности, их содержание, порядок разработки и ввода в действие.
  - Особенности обработки персональных данных, осуществляемой без использования средств автоматизации.
  - Лица, ответственные за организацию обработки персональных данных в организациях, порядок их назначения и их обязанности.
  - Подготовка уведомлений об обработке персональных данных в уполномоченный орган.
- **Тема 4. Техническая защита персональных данных в информационных системах**
  - Требования Федерального закона и Постановления Правительства РФ 2007 г. № 781 к обеспечению безопасности персональных данных. Обязательные механизмы защиты.
  - Уровни защищенности персональных данных при их обработке в ИСПДн в зависимости от угроз безопасности этим данным и классификация ИСПДн.
  - Модель угроз персональным данным. Базовая модель угроз. Перечень источников угроз. Уровень исходной защищенности. Методика актуализации угроз.
  - Каналы утечки информации при обработке персональных данных в информационных системах.
  - Построение системы защиты персональных данных в ИСПДн.
- **Тема 5. Лицензирование деятельности по технической защите конфиденциальной информации**
  - Понятие технической защиты как лицензируемого вида деятельности.
  - Лицензионные требования.

- Ответственность за незаконную деятельность в области защиты информации.
- Незаконное предпринимательство.
- Оценка и управление риском, связанным с отсутствием лицензии на техническую защиту конфиденциальной информации.

- **Тема 6. Аутсорсинг обработки персональных данных и их технической защиты**
  - Требования, выдвигаемые законом к порядку обработки персональных данных внешней организацией, содержание договора на обработку персональных данных.
  - Передача внешней организации функций технической защиты персональных данных.
  - Передача внешней организации функций лица, ответственного за организацию обработки персональных данных
  - Достоинства и недостатки аутсорсинга обработки персональных данных и их защиты.
- **Тема 7. Контроль и надзор за соблюдением законодательства о персональных данных**
  - Система государственного контроля и надзора за обеспечением безопасности персональных данных.
  - Область применения Федерального закона «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении госконтроля (надзора) и муниципального контроля» и регулируемые им вопросы.
  - Принципы защиты прав юридических лиц, индивидуальных предпринимателей при осуществлении государственного контроля (надзора).
  - Порядок планирования, организации и проведения проверок.
  - Права и обязанности проверяемых и проверяющих.
  - Меры, принимаемые должностными лицами органа госконтроля (надзора) при выявлении фактов нарушений.

Рабочая программа курса
КПЗ3 Техническая защита персональных данных

Цель этого учебного курса заключается в том, чтобы помочь специалистам различных категорий, от руководителей предприятий и их структурных подразделений до непосредственно отвечающих за защиту информации организовать обработку персональных данных в соответствии с требованиями российского законодательства.

Создание курса продиктовано необходимостью решения задач, поставленных перед всеми российскими предприятиями и организациями в связи с принятием Федерального закона«О персональных данных». Курс является логическим продолжением курса КП32 «Защита персональных данных» и полностью посвящён вопросам технической реализации требований законодательства по защите персональных данных.

Особое внимание в курсе уделяется практическим вопросам выполнения требований государственных регулирующих органов по технической защите этой категории сведений ограниченного доступа – анализу и классификации информационных систем, построению модели угроз, созданию подсистемы информационной безопасности, разработке внутренних организационно-распорядительных документов, описанию системы защиты персональных данных.

В течение трёх дней подробно рассматривается весь комплекс организационных мероприятий и технических мер по обеспечению безопасности обработки персональных данных. На примерах разбираются основные необходимые действия операторов персональных данных (ПДн) по приведению информационных систем персональных данных (ИСПДн) в соответствие требованиям российского законодательства по защите ПДн.

Предварительная подготовка:
Слушатели должны иметь:

- Общее представление об организационных и технических аспектах проблемы защиты конфиденциальных сведений, основах законодательства в области безопасности.

Планируемые результаты обучения:
Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса вы сможете:

- осуществлять анализ и классификацию ИСПДн;
- формировать модель угроз персональным данным и модель нарушителей в ИСПДн в соответствии с требованиями государственных регуляторов;
- готовить внутренние нормативные (организационно-распорядительные) документы, обеспечивающие техническую защиту ПДн;
- строить систему технической защиты ПДн в соответствии с требованиями государственных регуляторов;
- готовить ИСПДн к проверке соответствия требованиям по безопасности.

Продолжительность курса: 24 академических часа (3 дня)

Содержание курса:

- **Введение**
  - Нормативная база организации технической защиты персональных данных. Государственные органы, осуществляющие контроль и надзор в данной сфере деятельности (Роскомнадзор, ФСБ России, ФСТЭК России, Минкомсвязи России). Ответственность операторов ПДн за невыполнение требований по обеспечению безопасности ПДн при их обработке в ИСПДн.
- **Тема 1. Основные этапы работ по обеспечению безопасности ПДн в ИСПДн**
  - Перечень основных этапов работ и краткий обзор мероприятий, необходимых для приведения ИСПДн в соответствие требованиям российского законодательства по защите ПДн.
- **Тема 2. Сбор и анализ исходных данных по ИСПДн**
  - Обследование информационных систем с целью выявления фактов обработки ПДн, форм представления ПДн, целей и законности обработки, способов, сроков и объёмов их обработки, источников получения и др. Формирование перечня ПДн и выделение сегментов ИСПДн.
  - Сбор, анализ и документирование исходных данных по ИСПДн, необходимых для: выявления ИСПДн; классификации ИСПДн; определения исходной защищённости ИСПДн; построения модели угроз и определения актуальности угроз; проектирования СЗПДн и организации физической защиты.
  - Описание технологии обработки и защиты ПДн.

- **Тема 3. Классификация информационных систем персональных данных**
  - Нормативная база классификации ИСПДн.
  - Критерии классификации ИСПДн. Классы ИСПДн. Порядок проведения классификации ИСПДн и её документального оформления. Подклассы ИСПДн.
  - Вопросы оптимизации состава ПДн и процессов их обработки (реинжениринг ИСПДн).
- **Тема 4. Формирование модели угроз ПДн и модели нарушителей**
  - Нормативная база для формирования модели угроз безопасности ПДн в ИСПДн. Нормативно-методические документы ФСТЭК России и ФСБ России.
  - Традиционный подход к построению моделей угроз и нарушителей.
  - Формирование модели угроз безопасности ПДн на основании документов ФСТЭК России.
  - Определение перечня актуальных угроз.
  - Методология формирования модели угроз безопасности персональным данным на основании документов ФСБ России.
  - Методология формирования модели нарушителей на основании документов ФСБ России.
- **Тема 5. Разработка (проектирование) системы защиты персональных данных (СЗПДн)**
  - Меры по обеспечению безопасности персональных данных при их обработке. Требования Федерального закона от 27.07.2006 г. №152-ФЗ и Постановления Правительства РФ от 17.11.2007 г. №781 к обеспечению безопасности персональных данных. Обязательные механизмы защиты.
  - Общий порядок организации обеспечения безопасности ПДн в ИСПДн.
  - Мероприятия по защите ПДн (требования к мерам и средствам защиты) в зависимости от классов (и подклассов) ИСПДн.
  - Определение структуры, состава и основных функций СЗПДн.
  - Определение перечня предполагаемых к использованию сертифицированных средств защиты информации и их настроек.
- **Тема 6. Разработка и внедрение организационных мер и организационно-распорядительных документов по обеспечению защиты персональных данных**
  - Планирование организационных мероприятий по защите ПДн.
  - Разработка организационно-распорядительной документации, регламентирующей вопросы организации обеспечения безопасности ПДн и эксплуатации СЗПДн в ИСПДн.
- **Тема 7. Развертывание, настройка и опытная эксплуатация СЗПДн в ИСПДн**
  - Обеспечение охраны и физической защиты компонентов ИСПДн.
  - Организация и проведение работ по развёртыванию СЗПДн и настройке ее элементов в ИСПДн.
  - Испытания СЗПДн в процессе развертывания и опытной эксплуатации ИСПДн.
- **Тема 8. Закрытие технических каналов утечки ПДн в ИСПДн**
  - Технические каналы утечки ПДн при их обработке в ИСПДн. Условия и причины возникновения, особенности проявления, способы и методы защиты.
  - Мероприятия по защите ПДн от утечки по техническим каналам для различных классов ИСПДн.
- **Тема 9. Лицензирование деятельности по защите ПДн в ИСПДн**
  - Техническая защита конфиденциальной информации и техническое обслуживание СКЗИ как лицензируемые виды деятельности.

- Получение оператором лицензий ФСТЭК и ФСБ России. Лицензионные требования.

Рабочая программа курса
КП35 Регулирование отношений при осуществлении проверок операторов персональных данных

Цель этого учебного курса - дать знания руководителям и специалистам организаций-операторов персональных данных (ПДн), необходимые им для подготовки к прохождению проверок порядка обработки и защиты ПДн в соответствии с требованиями российского законодательства, осуществляемых органами государственного контроля и надзора.

Создание курса продиктовано необходимостью решения задач, поставленных перед российскими предприятиями и организациями в связи с принятием Федерального закона № 152-ФЗ "О персональных данных".

Основное внимание уделяется рассмотрению действующего законодательства, регламентирующего организацию и проведение проверок выполнения требований по обработке и защите персональных данных, определяющего права и обязанности, как контролируемых юридических лиц, так и контролирующих органов, а также основаниям и порядку проведения контрольных мероприятий. Особое внимание уделяется рассмотрению положений Федерального закона N 294-ФЗ от 26 декабря 2008 года "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля". На примерах разбираются результаты проведенных проверок.

Обязательные требования к обработке и защите ПДн, предусмотренные законодательством РФ, рассматриваются в курсе кратко, детально эти требования обсуждаются в рамках других курсов Учебного центра "Информзащита" - КП32 "Защита персональных данных" и КП33 "Техническая защита персональных данных".

Предварительная подготовка:
Слушатели должны иметь:

- Общие сведения о правовых, организационных и технических аспектах обработки персональных данных в соответствии с законодательством РФ.

Планируемые результаты обучения:
Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса вы сможете:

- подготовиться к проверкам и представлять интересы организации при прохождении проверок в строгом соответствии с российским законодательством
- разбираться в вопросах регулирования отношений операторов ПДн и контролирующих органов при организации и осуществлении государственного контроля и надзора за соблюдением законодательства в области обработки персональных данных
- обладать знаниями по вопросам прав и обязанностей юридических лиц (организаций-

операторов ПДн) при осуществлении проверок

- иметь подготовку по вопросам прав и обязанностей органов государственного контроля (надзора) при осуществлении проверок за соблюдением законодательства в области обработки ПДн.

Продолжительность курса: 8 академических часов (1 день)

Содержание курса:

- **Тема 1. Регулирование отношений в области организации и осуществления государственного контроля и надзора**
  - Система государственного контроля и надзора за соблюдением законодательства в области обработки персональных данных.
  - Нормативная база организации контроля и надзора за выполнением обязательных требований законодательства в области обработки и обеспечения безопасности ПДн.
  - Законодательная защита прав юридических лиц при осуществлении государственного контроля (надзора).
  - Полномочия государственных контролирующих органов по вопросам защиты ПДн. Область компетенции ведомств. Порядок взаимодействия ведомств при проведении проверки.
  - Административные регламенты проведения проверок и отдельных мероприятий при осуществлении федерального государственного контроля (надзора). Статус и содержание административных регламентов.
- **Тема 2. Организация проверки**
  - Основания для проведения проверок. Порядок и сроки уведомления оператора о проведении проверки.
  - Требования к документам, оформляемым до проведения проверки и предоставляемым контролирующими органами при проведении проверок. Типовая форма распоряжения или приказа о проведении проверки юридического лица.
- **Тема 3. Проведение проверки**
  - Виды проверок. Плановые и внеплановые проверки. Выездные и документарные проверки.
  - Периодичность проведения проверок. Сроки (продолжительность) проведения проверок.
  - Ограничение круга участников выездной проверки.
  - Обязательные требования, выполнение которых проверяется (может проверяться) при проверках. Перечень запрашиваемых у операторов документов.
  - Пределы компетенции должностных лиц, участвующих в проверке.
  - Анализ требований, выдвигаемых контролирующими органами, их обоснование. Порядок обжалования действий (бездействия) должностных лиц, осуществляющих проверку.
  - Варианты завершения проверок.
- **Тема 4. Оформление акта проверки**
  - Форма акта проверки.
  - Требования к составлению акта проверки.
  - Документирование разногласий. Изложение особого мнения.

- Возможные виды нарушений, допускаемых при проведении проверки и их юридические последствия. Перечень грубых нарушений.

- **Тема 5. Ответственность**
  - Виды ответственности за невыполнение обязательных требований, воспрепятствование контрольным и надзорным мероприятиям, неисполнение полученных предписаний и неустранение нарушений.
  - Меры, принимаемые должностными лицами в отношении фактов нарушений, выявленных при проведении проверки.
  - Порядок направления материалов в правоохранительные органы, прокуратуру, суд.
  - Примеры из правоприменительной практики.

Рабочая программа курса

БТ03 Безопасность компьютерных сетей

Цель этого учебного курса преподать слушателям систематизированные теоретические сведения и сопроводить их более чем 20-ю практическими работами. В курсе подробно рассматриваются источники угроз и причины появления уязвимостей систем, возможности и недостатки основных защитных механизмов, демонстрируются типичные приемы и инструменты, используемые нарушителями, моделируются хакерские атаки на сетевые протоколы и службы, предлагаются решения по обеспечению безопасности корпоративной сети и рациональному выбору средств защиты информации в компьютерных сетях. Значительная часть курса посвящена практической работе со средствами поиска уязвимостей систем и обнаружения атак (как свободно распространяемых, так и коммерческих) на специальных реконфигурируемых стендах, позволяющих моделировать реальные корпоративные сети предприятий.

Обучение на данном курсе является обязательным условием для получения специалистом государственного документа о повышении квалификации по направлению "Безопасность компьютерных систем и сетей", необходимого для получения организацией лицензии на деятельность по технической защите конфиденциальной информации в соответствии с постановлением Правительства РФ №504 от 15.08.2006.

Предварительная подготовка:
Слушатели должны иметь:

- Базовые знания по IP-сетям, основным протоколам и службам стека TCP/IP
- Навыки работы с ОС Windows 2000/2003/XP и Linux.

Планируемые результаты обучения:

Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса вы сможете:

- использовать сетевые анализаторы для мониторинга трафика;
- использовать хакерские инструменты: Cain, Nmap, Netcat и другие;
- работать со средствами выявления уязвимостей и обнаружения атак;
- управлять пакетным фильтром на базе Linux;
- квалифицированно использовать протоколы защиты трафика: IPsec, SSL;

- строить «сети-приманки» для изучения поведения нарушителей.

Продолжительность курса: 32 академических часа (4 дня)

Содержание курса.

- **Краткое введение в безопасность компьютерных сетей.**
  - Типовая IP-сеть организации. Уровни информационной инфраструктуры корпоративной сети. Концепция глубокоэшелонированной защиты. Угрозы, уязвимости и атаки. Варианты классификации уязвимостей и атак. Обзор механизмов защиты компьютерных систем. Базовые принципы сетевого взаимодействия Архитектура TCP/IP. Краткая характеристика протоколов.
- **Безопасность физического и канального уровней.**
  - Сетевые анализаторы и «снифферы». Методы обнаружения «снифферов». Проблемы аутентификации на основе MAC-адресов. Уязвимости сетевого оборудования.
- **Проблемы безопасности протокола разрешения адресов ARP.**
  - Варианты атак с использованием уязвимостей протокола ARP. ARP Spoofing. Особенности работы механизма разрешения MAC-адресов в различных операционных системах. Меры защиты от атак на протокол ARP, утилита arpwatch. Обнаружение сетевых анализаторов с помощью протокола ARP, утилита Cain.
- **Стандарт 802.1x. Безопасность на уровне порта.**
  - Протокол EAP. Этапы построения сетевой инфраструктуры, удовлетворяющей требованиям стандарта 802.1x.
- **Безопасность сетевого уровня модели OSI.**
  - Протоколы IP и ICMP. AddressSpoofing и его использование. Атаки с использованием протокола ICMP. Уязвимости механизма фрагментации.
- **Защита периметра сети.**
  - Межсетевые экраны и их разновидности. Пакетные фильтры, технология StatefulInspection. Пакетный фильтр iptables на базе ОС Linux. Посредники и системы анализа содержимого. Изучение базовых возможностей межсетевого экрана CheckPoint NGX. Защита от атаки AddressSpoofing.
- **Введение в прикладную криптографию.**
  - Криптографические методы защиты информации. Стеганография. Симметричные алгоритмы шифрования. Асимметричные алгоритмы шифрования. Алгоритмы хеширования.
- **Виртуальные частные сети.**
  - Определение VPN. Разновидности VPN-технологий. Реализации VPN-технологий. Топологии VPN. Схемы использования технологий VPN. Краткие сведения об IPsec. Протокол L2TP. Протокол PPTP. Сертифицированные решения для построения VPN.
- **Проблемы безопасности протокола IP версии 6.**
  - Краткое описание протокола. Проблемы безопасности. Итоговые рекомендации.
- **Безопасность транспортного уровня модели OSI.**
  - Протоколы TCP и UDP. Распределённые DoS-атаки и меры защиты от них. DoS-умножение. Сканирование портов, утилита nmap. Атаки SYNFlood и LAND. Подмена участника TCP-соединения. Разрыв TCP-соединения с помощью протокола ICMP.

- **Анализ защищённости корпоративной сети как превентивный механизм защиты.**
    - Классификация сканеров безопасности. Принципы анализа защищённости на сетевом уровне. Возможности и варианты использования сетевых сканеров безопасности. Работа с программой InternetScanner.
- **Защита трафика на прикладном уровне.**
    - Протоколы SSL/TLS, SSH. Теория и практика атак «человек посередине».
- **Обнаружение сетевых атак.**
    - Архитектура систем обнаружения атак. Классификация систем обнаружения атак. Анализ сигнатур. Виды сигнатур. Примеры систем обнаружения атак. Система обнаружения атак Snort.
- **Общие проблемы безопасности служб прикладного уровня.**
    - Уязвимости протокола DHCP. Обнаружение ложного DHCP-сервера. Изучение механизма DNSSpoofing.
- **Honeynet или сеть-приманка для изучения поведения нарушителей.**
    - Принципы организации Honeynet. Классификация сетей-приманок, практические реализации. Утилита honeyd, проект HoneyNet. Сценарии использования сетей-приманок (обнаружение сетевых червей, контроль распространении спама и т. д.). Риски, связанные с использованием сетей-приманок.

Рабочая программа курса

БТ05 Основы TCP/IP

Целью этого учебного курса является интенсивное изучение основ сетевого взаимодействия, современных сетевых технологий и протоколов семейства TCP/IP. В курсе чередуются систематизированные теоретические сведения и практические работы каждого слушателя под руководством опытного инструктора. Занятия курса направлены на понимание содержимого сетевых пакетов и механизмов взаимодействия узлов сети.

Предварительная подготовка:

Слушатели должны иметь:

- Навыки работы с ОС Windows и/или Linux на уровне пользователя.

Планируемые результаты обучения:

Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса вы сможете:

- Использовать свои знания по современным сетевым технологиям и протоколам, их уязвимостям и особенностям, существенным для обеспечения безопасности;
- обладать принципами работы и настройки стека TCP/IP;
- применять сетевые анализаторы для контроля обмена данными и понимания происходящих в сети процессов.

Продолжительность курса: 8 академических часов (1 день)

Содержание курса:

- Базовые принципы сетевого взаимодействия. Приём, передача данных по сети. Сетевые пакеты. Протоколы, интерфейсы. Уровни сетевого взаимодействия. Модель OSI.
- Обзор современных сетевых технологий. Примеры сетей. Физический уровень. Основные сетевые устройства. Технология Ethernet. Сетевые анализаторы.
- Обзор современных сетевых протоколов. Архитектура TCP/IP. Документы RFC.
- Организация взаимодействия со средой передачи в стеке TCP/IP. Протокол разрешения адресов ARP.
- Сетевой уровень в стеке TCP/IP. Протокол IP как основа межсетевого взаимодействия. Маршрутизация. Протокол передачи управляющих сообщений ICMP.
- Транспортный уровень в стеке TCP/IP. Протоколы TCP и UDP.
- Службы прикладного уровня. Архитектура и принципы работы. Протоколы TELNET, FTP и др.
- Электронная почта. Протоколы SMTP и POP3.

Рабочая программа курса
T010 Использование электронной подписи и развертывание PKI на основе Удостоверяющего центра КриптоПро

Целью этого учебного курса является знакомство слушателей с программой, которая охватывает общие вопросы использования электронной цифровой подписи (ЭЦП), различных видов электронных подписей (ЭП), инфраструктуры открытых ключей (PublicKeyInfrastructure, PKI) и практические аспекты их использования.

В программе 1-го модуля рассматриваются теоретические и практические основы использования ЭЦП, различных видов электронных подписей и инфраструктуры открытых ключей в корпоративных информационных системах (электронный документооборот, электронная почта, электронный бизнес, банковские платежные системы и т.д.). Более 50% учебного времени уделяется практическим работам, в рамках которых слушатели решают прикладные задачи с использованием программно-аппаратных средств защиты различных производителей - уникальная возможность почувствовать разницу между различными средствами защиты.

Слушатели курса могут самостоятельно выбрать и выполнить лабораторные работы на тех аппаратных решениях, которые используются или планируются к использованию в их организациях. Кроме того, слушатели имеют возможность познакомиться с целым спектром современных средств защиты от наиболее опасных атак на счета клиентов систем дистанционного банковского обслуживания.

На практических занятиях слушатели имеют возможность познакомиться с различными технологиями по защите решений с применением электронной подписи в облачных сервисах. Обучение по программе Модуля 1 можно пройти отдельно, её содержание соответствует программе курса КП06 "Использование ЭЦП и PKI".

В рамках 2-го модуля рассматриваются структура, основные функции и принципы построения PKI на базе Удостоверяющего центра "КриптоПро УЦ" для создания юридически значимой электронной цифровой подписи в системах электронного документооборота. В программу Модуля 2 вошли вопросы установки и настройки компонент "КриптоПро УЦ".

Большое внимание уделяется практическим вопросам использования возможностей комплекса "КриптоПро УЦ" для выпуска сертификатов с применением различных программно-аппаратных средств смарт-карт и токенов (eToken, Рутокен) от ведущих компаний-производителей, таких как "Аладдин Р.Д.", "Актив", "Цифровые Технологии", а также для создания и проверки юридически значимости электронной цифровой подписи.

В проведении обучения по данному модулю принимает участие представитель компании "КРИПТО-ПРО", который дает комментарии по наиболее сложным вопросам, связанным с эксплуатацией комплекса.

Предварительная подготовка:

Слушатели должны иметь:

- Базовые знания и навыки по работе с Windows.

Планируемые результаты обучения:

Ниже представлен перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения по данному учебному курсу (дисциплине). В силу практикоориентированности данного курса компетенции сформулированы в терминологии умений и соответствующих им знаний.

После изучения курса вы сможете:

- осуществлять настройку и использовать средства ЭЦП и компоненты PKI в корпоративных информационных системах;
- использовать ЭЦП в прикладных программах, интегрированных с PKI;
- применять различные программные и аппаратные средства ЭЦП;
- оценивать риски, связанные с применением ЭЦП и предлагать варианты их снижения.

Продолжительность курса: 40 академических часов (5 дней)

Содержание курса:

- **Модуль 1.**
  - **Электронные документы.** Угрозы безопасности субъектам электронного документооборота. Модель нарушителя.
  - **Электронная подпись.** Виды электронной подписи. Правовые вопросы применения ЭП и СКЗИ в России. Особенности юридического определения ЭП. Федеральный закон "Об электронной подписи".
  - **Электронная цифровая подпись.** Правовые вопросы применения ЭЦП и СКЗИ в России. Особенности юридического определения ЭЦП. Федеральный закон "Об электронной цифровой подписи".
  - **Криптографические методы защиты информации.** Криптография с симметричными ключами. Криптография с открытыми ключами. Доверие к открытому ключу и цифровые сертификаты.
  - **Электронный сертификат.** Структура сертификата. Сертификаты стандарта X.509. Основной контекст сертификата. Расширения сертификатов. Классы сертификатов. Хранилища сертификатов. Закрытые ключи, риски использования по умолчанию. КриптоАРМ. Создание самоподписанного сертификата. Анализ сертификата. Импорт и экспорт сертификатов.
  - **Криптопровайдеры.** Набор CSP (Cryptographic Service Provider) по умолчанию. Microsoft CSP.
  - **Создание электронной подписи.** Установка и эксплуатация "КриптоАРМ", "КриптоТри", "eTokenКриптоАРМ".

- **Электронные ключи eToken.** Модели eToken. JaCarta. Российская криптография в eToken ГОСТ. Установка и настройка различных моделей eToken. Настройка параметров. Режимы работы. Получение сертификата с использованием электронных ключей eToken.
- **Электронная подпись для AppleiOS.** Решения и технологии применения российской криптографии для электронной подписи на iPad и iPhone.
- **Электронные идентификаторы Рутокен.** Модели Рутокен. Российская криптография в Рутокен ЭЦП. Рутокен Web. Установка и настройка различных моделей Рутокен. Настройка параметров. Режимы работы. Получение сертификата с использованием электронных ключей Рутокен.
- **КриптоПро CSP.** Основные характеристики. Реализуемые алгоритмы. Установка. Настройка параметров. Получение сертификатов с использованием средства криптографической защиты "СКЗИ КриптоПро". Функциональный ключевой носитель. КриптоПро УЭК CSP. Практика применения КриптоПро eToken CSP и КриптоПро Рутокен CSP.
- **Проблемы безопасности при применении электронных подписей.** Интернет-банкинг. Примеры атак на системы дистанционного банковского обслуживания. Обзор типовых методов атак на счета клиентов систем ДБО. Визуальный контроль содержания передаваемых в смарт-карту данных. Применение устройств доверенного ввода информации для защиты платежей. Просмотр содержания подписываемых документов в доверенной среде.
- **Web-порталы и облачные сервисы.** Особенности применения электронной подписи в решениях с облачной архитектурой. Квалифицированная электронная подпись. Неквалифицированная электронная подпись. Применение технологии OTP для защиты решений с использованием электронных подписей.
- **Компоненты PKI.** Орган сертификации. Орган регистрации. Хранилище. Архив. Пользователи инфраструктуры.
- **Принципы доверия PKI.** Иерархическая модель доверительных отношений. Сетевая модель доверительных отношений. Регулируемые доверительные отношения. Базовые ограничения. Ограничения по именам. Ограничения по политике выдачи сертификатов. Ограничения по политике приложений. Получение и регистрация частного номера организации. Формирование объектных идентификаторов областей применения сертификатов открытых ключей. Регулируемые доверительные отношения.
- **Эксплуатация PKI.** Создание файла конфигурации для корневого центра сертификации (ЦС). Установка и настройка корневого ЦС. Публикация списков отозванных сертификатов корневого ЦС. Установка подчиненного ЦС. Настройка WEB-интерфейса, подчиненного ЦС.
- **Проверка подлинности цифровых сертификатов в инфраструктуре Windows PKI.** Процедуры сличения. Стандартная процедура обработки цепочки сертификатов. Обработка цепочки списков CTL. Обработка цепочки кросс-сертификатов. Получение сертификата пользователя. Организация защищенной электронной почты.
- **Процедуры аннулирования сертификатов в Windows PKI.** Списки аннулированных сертификатов (CertificateRevocationList, CRL). Риски, связанные с технологией CRL.
- **КриптоПро OCSP Server.** Краткое описание протокола Online Certificate Status Protocol (OCSP). Установка КриптоПро OCSP Server. Создание экземпляра

Службы. Управление операторами Службы. Запуск Службы. Установка модуля поддержки OCSP.

- **КриптоПро RevocationProvider.** Ключевые особенности. Установка RevocationProvider. Как работает RevocationProvider.
- **КриптоПро TSP Server.** Для чего нужны штампы времени. Краткое описание протокола TimeStampingProtocol (TSP). Установка КриптоПро TSP Server. Запуск Службы. Установка модуля поддержки TSP КриптоАРМ.
- **Усовершенствованная подпись КриптоПро.** Доказательство момента подписи документа и действительности сертификата ключа подписи на этот момент. Проверка подлинности ЭЦП без сетевых обращений. Архивное хранение электронных документов. Формат усовершенствованной электронной цифровой подписи. Технологические процедуры создания усовершенствованной ЭП. Проверка усовершенствованной ЭП.

- **Модуль 2.**
  - **Назначение и основные возможности комплекса Удостоверяющий центр "КриптоПро УЦ".** Режимы работы Удостоверяющего центра: регистрация и управление ключами и сертификатами пользователей. Объекты управления Удостоверяющего центра: пользователи, сертификаты и запросы на сертификаты пользователей, запросы на отзыв сертификатов, список отозванных сертификатов. Обеспечение юридической значимости электронного документооборота с использованием ЭП и комплекса "КриптоПро УЦ".
  - **Структура, состав, размещение и взаимодействие компонентов Удостоверяющего центра.** Программные компоненты Удостоверяющего центра: Центр сертификации (ЦС), Центр регистрации (ЦР), автоматизированное рабочее место (АРМ) администратора ЦР, СКЗИ КриптоПро CSP, средство сетевой аутентификации КриптоПро TLS. Требования к оборудованию и базовому программному обеспечению ЦС, ЦР, АРМ администратора ЦР и пользовательских рабочих станций. Типовая схема размещения и взаимодействия компонентов Удостоверяющего центра. Подготовка компьютеров и базовых операционных систем к установке. Последовательность установки.
  - **ЦС Удостоверяющего центра.** Компоненты и режимы его работы. Схема взаимодействия компонентов ЦС. Требования к аппаратно-программным средствам. Последовательность установки и настройки компонентов ЦС. Установка службы сертификации. Обработка запроса на сертификат ЦР. Подключение ЦР в составе Удостоверяющего центра. Управление ключами ЦС.
  - **ЦР Удостоверяющего центра.** Компоненты и режимы его работы. Схема взаимодействия компонентов ЦР. Требования к аппаратно-программным средствам. Последовательность установки и настройки компонентов ЦР. Установка службы очереди сообщений. Выпуск и инсталляция сертификата Web-сервера ЦР. Выпуск и установка сертификата ЦР, создание базы данных. Отправка почтовых сообщений. Подключение привилегированных пользователей. Применение и управление списком отозванных сертификатов на ЦР. Смена ключей ЦР и Web-сервера ЦР.
  - **Управление ЦР.** Настройка и изменение параметров программного обеспечения ЦР. Смена размещения базы данных ЦР. Пользователи ЦР: зарегистрированные, активные, проходящие процедуру удаленной регистрации.

Ролевая модель взаимодействия пользователей с ЦР. Основные предустановленные роли. Настройка разрешений к допустимым действиям ЦР, регламентных заданий и политик имен пользователей.

- **АРМ администратора ЦР.** Основные объекты управления: пользователи, запросы на регистрацию, отзыв и сертификат. Требования для установки и работы с приложением. Запуск и настройка АРМ. Конфигурация программного обеспечения АРМ в процессе эксплуатации. Интерфейс приложения АРМ. Смена ключа и сертификата администратора. Регистрация пользователей ЦР. Управление ключами и сертификатами пользователей. Обработка запросов пользователей ЦР. Управление объектами ЦС. Аудит ЦР.
- **АРМ пользователя.** Объекты управления: запрос на регистрацию, запрос на сертификат, запрос на отзыв, служебные ключи и сертификаты, рабочие ключи и сертификаты. Настройка и запуск АРМ пользователя. Работа с АРМ пользователя. Удаленная (сетевая) регистрация.
- **Типовые варианты применения.** Политика удаленной регистрации. Политика централизованной регистрации с созданием служебного, личного и открытого ключа пользователя.
- **АРМ Разбора конфликтных ситуаций.** Применение АРМ РКС для проверки подлинности ЭП/ЭЦП в электронном документе.