

Учебный центр

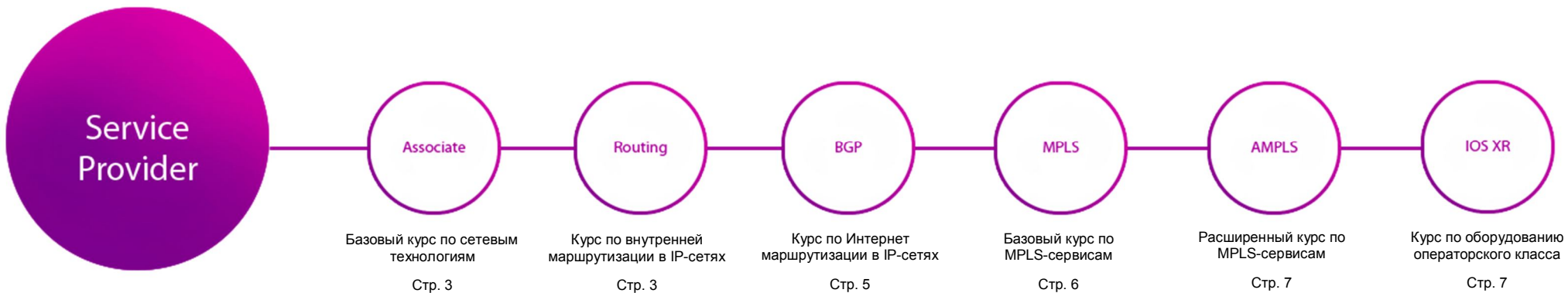
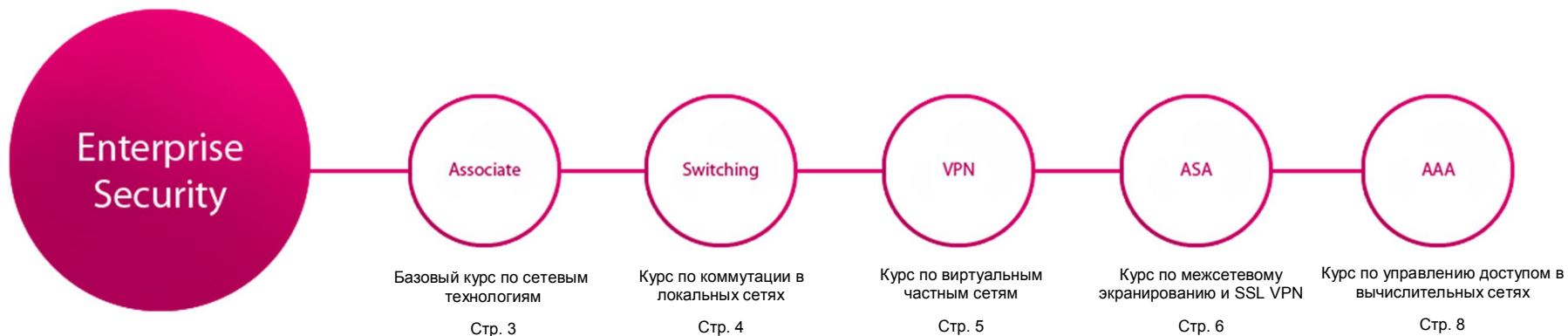
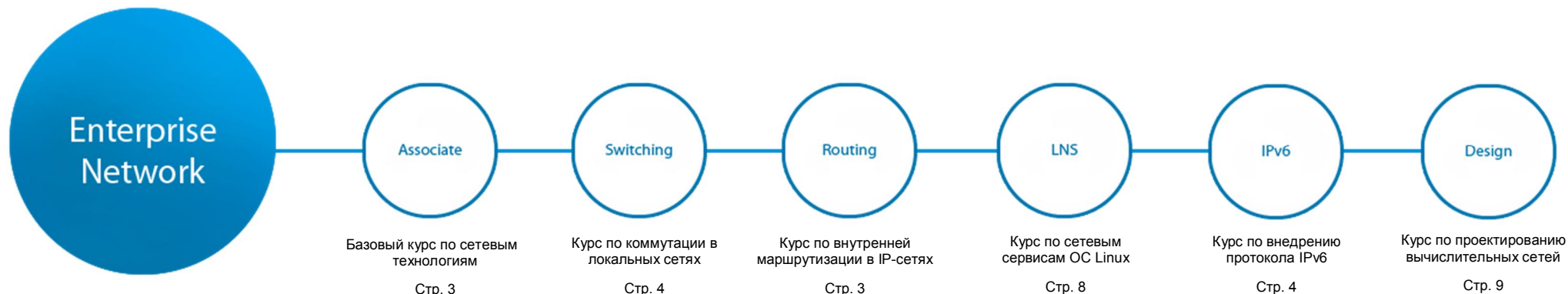
Программы обучения



Enterprise
Network

Enterprise
Security

Service
Provider



Associate

Базовый курс по сетевым технологиям

Описание курса

Курс предназначен для:

- инженеров, ответственных за построение и сопровождение небольших сетей;
- специалистов службы технической поддержки первой линии.

Цель курса

Получить знания и навыки, необходимые для настройки и эксплуатации небольших сетей (10-20 сетевых устройств), а также поиска и устранения неисправностей.

По окончании курса

Вы будет:

- знать принципы работы сетей передачи данных;
- иметь представление о сетевых протоколах и службах в соответствии с моделью OSI;
- обладать знаниями об архитектуре сетевых устройств Cisco;
- обладать навыками аппаратной диагностики работоспособности сетевых устройств Cisco;
- использовать командную строку для конфигурации коммутаторов и маршрутизаторов, а также средства для построения топологии сети;
- понимать принципы работы листов контроля доступа (ACL) и уметь их применять;
- уметь настраивать базовые сетевые службы на оборудовании Cisco (DNS, DHCP, NTP);
- уметь настраивать статическую и динамическую маршрутизацию;
- уметь настраивать технологии выхода в Интернет, такие как NAT, Reflexive-ACL, IP Inspect;
- иметь представление о WAN и VPN сетях;
- уметь находить неисправности в небольших сетях.

Содержание курса

Модуль	Тема	Время
1	Теория построения локальных сетей и архитектура сетевых устройств Cisco	8 а.ч.
2	Настройка технологий коммутации	8 а.ч.
3	Методы удалённого доступа и пакетная фильтрация	8 а.ч.
4	Маршрутизация в сетях передачи данных	8 а.ч.
5	Организация доступа в Интернет	8 а.ч.

Рекомендуемая предварительная подготовка

Базовая компьютерная грамотность, навыки работы с операционной системой Windows или Linux. Общее представление о методах построения сетей связи. Желательно наличие опыта работы с IP-сетями.

Routing

Курс по внутренней маршрутизации в IP-сетях

Описание курса

Курс предназначен для:

- инженеров, ответственных за построение и сопровождение сетей с использованием протоколов динамической маршрутизации.

Цель курса

Получить знания и навыки, необходимые для внедрения и эксплуатации протоколов динамической маршрутизации в сети предприятия.

По окончании курса

Вы будете:

- понимать принципы работы NMBA-сетей на примере технологии Frame-Relay;
- обладать знаниями об архитектуре сетевых устройств Cisco;
- внедрять протокол динамической маршрутизации Cisco EIGRP в сети предприятия;
- внедрять протокол динамической маршрутизации OSPF в нескольких областях;
- настраивать динамическую маршрутизацию для подключения к оператору по протоколу BGP;
- создавать политики обмена маршрутными записями между протоколами маршрутизации;
- осуществлять поиск неисправностей в работе протоколов динамической маршрутизации.

Содержание курса

Модуль	Тема	Часы
1	Обзор технологии Frame-Relay	4 а.ч.
2	Архитектура маршрутизаторов Cisco	4 а.ч.
3	Настройка протокола маршрутизации EIGRP	8 а.ч.
4	Использование протокола маршрутизации OSPF в предприятии	8 а.ч.
5	Базовая настройка протокола Интернет маршрутизации BGP и применение политик	16 а.ч.

Рекомендуемая предварительная подготовка

Прохождение обучения по курсу «Associate» или альтернативная подготовка.

Switching

Курс по коммутации в локальных сетях

Описание курса

Курс предназначен для:

- специалистов, ответственных за построение и сопровождение сетей с использованием коммутаторов Cisco Catalyst.

Цель курса

Получить знания и навыки, необходимые для настройки и эксплуатации технологий коммутации в локальных сетях, а также поиска и устранения неисправностей.

По окончании курса

Вы будете:

- знать принципы построения коммутируемых сетей;
- понимать и уметь внедрять технологии VLAN, Q-in-Q, Etherchannel, UDLD, DTP и VTP;
- настраивать протоколы избегания петель RPVST+ и MST с расширенными функциями STP Toolkit;
- внедрять протоколы отказоустойчивого шлюза HSRP, VRRP и GLBP;
- понимать и применять методы управления порядком обработки трафика CBWFQ, WRED, Policing и Shaping, L2 QoS;
- понимать и уметь настраивать технологии безопасности коммутируемой среды: Port-Security, Storm-Control, VACL, Private VLAN, DHCP Snooping, 802.1x.

Содержание курса

Модуль	Название	Время
1	Принципы построение коммутируемой сети	8 а.ч.
2	Протоколы избегания петель	6 а.ч.
3	Протоколы отказоустойчивости шлюза	4 а.ч.
4	Настройка технологий L2 и L3 QoS	12 а.ч.
5	Безопасность коммутируемых сетей	10 а.ч.

Рекомендуемая предварительная подготовка

Прохождение обучения по курсу «Associate» или альтернативная подготовка.

IPv6

Курс по внедрению протокола IPv6

Описание курса

Курс предназначен для:

- администраторов информационных систем;
- инженеров, ответственных за построение и сопровождение IPv6 сетей с использованием сетевого оборудования.

Цель курса

Получить знания и навыки, необходимые для внедрения и эксплуатации сетей на основе протокола IPv6.

По окончании курса

Вы будете:

- знать принципы работы протокола IPv6;
- разбираться в классификации адресов в IPv6;
- использовать IPv6 в листах контроля доступа;
- понимать работу DHCPv6;
- иметь представление о принципах многоадресной рассылки в IPv6;
- уметь внедрять протоколы динамической маршрутизации для IPv6: RIPng, EIGRPv6, OSPFv3, MP-BGP, IS-IS;
- осуществлять управление маршрутными записями между протоколами динамической маршрутизации;
- применять туннели IPv4 <-> IPv6;
- использовать механизмы трансляции адресов.

Содержание курса

Модуль	Название	Время
1	Основы IPv6	2 а.ч.
2	Протоколы динамической маршрутизации IPv6	8 а.ч.
3	Туннелирование между IPv4 и IPv6	2 а.ч.
4	Принципы работы многоадресной рассылки протокола IPv6	2 а.ч.
5	Преобразование адресов между IPv4 и IPv6	2 а.ч.

Рекомендуемая предварительная подготовка

Прохождение обучения по курсам «Associate», «Routing» или альтернативная подготовка.

VPN

Курс по виртуальным частным сетям

Описание курса

Курс предназначен для технических специалистов, проектирующих, внедряющих и сопровождающих виртуальные частные сети, построенные на основе технологии IPsec.

Virtual Private Network (VPN) – важнейший инструмент построения корпоративных сетей передачи данных с возможностью шифрования передаваемого трафика.

Инструментарий Cisco IOS предоставляет целый набор технологий, подходящих под различные сценарии.

Цель курса

Получить знания и навыки, необходимые для настройки и эксплуатации технологий виртуальных частных сетей в сети предприятия.

По окончании курса

Вы будете:

- знать принципы работы технологии IPsec;
- иметь представление об инфраструктуре открытых ключей (PKI);
- настраивать туннели сеть-сеть: IPsec, IPsec VTI, GRE, GRE over IPsec, DMVPN, GET VPN;
- внедрять технологии удаленного доступа по протоколам PPTP, L2TP, Easy VPN, DVTI, SSL;
- осуществлять поиск неисправностей в сетях VPN.

Содержание курса

Модуль	Название	Время
1	Архитектура IPsec	8 а.ч.
2	Инфраструктура открытых ключей	6 а.ч.
3	Настройка VPN сеть-сеть	14 а.ч.
4	Настройка VPN для удаленного доступа	8 а.ч.
5	Поиск неисправностей в сетях VPN	4 а.ч.

Рекомендуемая предварительная подготовка

Прохождение обучения по курсам «Associate», «Routing», «Switching» или альтернативная подготовка.

BGP

Курс по Интернет маршрутизации в IP-сетях

Описание курса

Курс предназначен для:

- администраторов информационных систем;
- инженеров операторов услуг и крупных предприятий, ответственных за построение и сопровождение сетей с использованием протокола динамической маршрутизации BGP.

Цель курса

Получить знания и навыки, необходимые для установки и эксплуатации протокола динамической маршрутизации BGP в сетях поставщиков услуг и предприятий, а также поиска и устранения неисправностей.

По окончании курса

Вы будете:

- знать принципы работы протокола BGP;
- понимать сценарии применения атрибутов путей: AS-PATH, Local Preference, MED, WEIGHT и др.;
- настраивать фильтры для маршрутных записей;
- применять методы обновления политик маршрутизации: soft-reconfig, route-refresh и ORF;
- использовать атрибут COMMUNITY для логического отделения маршрутных записей;
- внедрять масштабируемые сценарии протокола BGP с помощью peer-group, peer-template, route-reflector, confederation;
- понимать роль протокола BGP для работы технологий MPLS VPN и IPv6;
- осуществлять поиск неисправностей в сетях BGP.

Содержание курса

Модуль	Название	Время
1	Базовая настройка протокола BGP	2 а.ч.
2	Настройка фильтров маршрутных записей	8 а.ч.
3	Методы применения и обновления политик маршрутизации	4 а.ч.
4	Масштабируемые сценарии протокола BGP	8 а.ч.
5	Сценарии применения MP-BGP	2 а.ч.

Рекомендуемая предварительная подготовка

Прохождение обучения по курсам «Associate», «Routing» или альтернативная подготовка.

ASA

Курс по межсетевому экранированию и SSL VPN

Описание курса

Курс предназначен для специалистов по информационной безопасности, ответственных за сегментирование, экранирование сетей и построение гибкого VPN доступа к ресурсам предприятия.

Цель курса

Получить знания и навыки, необходимые для построения безопасных сетей с помощью оборудования Cisco ASA.

По окончании курса

Вы будете:

- понимать принципы работы межсетевых экранов Cisco ASA;
- сегментировать сети с помощью сетевых экранов;
- внедрять протоколы маршрутизации и коммутации на межсетевых экранах Cisco ASA;
- понимать сценарии применения сетевых экранов;
- настраивать технологии VPN сеть-сеть;
- настраивать гибкий и управляемый VPN удаленный доступ с помощью SSL VPN;
- внедрять сетевые экраны в отказоустойчивом режиме;
- применять технологию виртуализации с помощью контекстов безопасности;
- осуществлять поиск неисправностей.

Содержание курса

Модуль	Название	Время
1	Основы работы в ASA OS	4 а.ч.
2	Настройка технологий фильтрации и трансляции	8 а.ч.
3	Маршрутизация и коммутация средствами сетевых экранов	4 а.ч.
4	Внедрение технологий VPN	8 а.ч.
5	Применение средств повышения доступности и масштабируемости	8 а.ч.

Рекомендуемая предварительная подготовка

Прохождение обучения по курсам «Associate», «Routing», «Switching», «VPN» или альтернативная подготовка.

MPLS

Базовый курс по MPLS-сервисам

Описание курса

Курс предназначен для инженеров, ответственных за внедрение сетевых сервисов с использованием технологии многопротокольной коммутации MPLS в сетях предприятий и поставщиков услуг.

Цель курса

Получить знания и навыки, необходимые для установки и эксплуатации сетевых сервисов в сетях предприятий и поставщиков услуг.

По окончании курса

Вы будете:

- понимать принципы работы технологии MPLS и архитектуру маршрутизаторов Cisco;
- подбирать сервисы MPLS для реализации поставленных задач;
- внедрять технологию MPLS и сервис MPLS L3 VPN;
- внедрять протоколы внутренней и внешней маршрутизации на стыке PE-CE;
- настраивать оборудование для поддержки PIM Multicast: Dense Mode, Sparse Mode, SSM, MSDP;
- внедрять сервис MPLS Multicast VPN;
- осуществлять поиск неисправностей в сетях MPLS.

Содержание курса

Модуль	Название	Время
1	Архитектура сервисов MPLS	4 а.ч.
2	Настройка MPLS как сервисной платформы	8 а.ч.
3	Внедрение технологии L3 MPLS VPN	4 а.ч.
4	Настройка оборудования для поддержки многоадресной рассылки	6 а.ч.
5	Внедрение технологии MPLS Multicast VPN	2 а.ч.

Рекомендуемая предварительная подготовка

Прохождение обучения по курсам «Associate», «Routing», «BGP» или альтернативная подготовка.

AMPLS

Расширенный курс по MPLS-сервисам

Описание курса

Курс предназначен для инженеров, ответственных за внедрение сетевых сервисов с использованием технологии многопротокольной коммутации MPLS в сетях поставщиков услуг.

Цель курса

Получить знания и навыки, необходимые для установки и эксплуатации сетевых сервисов в сетях поставщиков услуг.

По окончании курса

Вы будете:

- применять технологию поддержки провайдеров Carrier Supporting Carrier;
- внедрять MPLS L3 VPN в сценарии Inter-AS по опциям A/B/C;
- внедрять Inter-AS Multicast MPLS VPN;
- внедрять технологии L2 VPN: AToM, L2TPv3, VPLS;
- управлять трафиком в сетях с помощью технологии MPLS Traffic Engineering;
- иметь представление о сервисе защиты от распределенных DOS-атак;
- осуществлять поиск неисправностей в сетях MPLS.

Содержание курса

Модуль	Название	Время
1	Применение технологии CSC	4 а.ч.
2	Построение Inter-AS MPLS L3 VPN	8 а.ч.
3	Построение Inter-AS MPLS Multicast VPN	4 а.ч.
4	Внедрение технологий L2 VPN	8 а.ч.
5	Применение технологии MPLS Traffic Engineering	8 а.ч.

Рекомендуемая предварительная подготовка

Прохождение обучения по курсам «Associate», «Routing», «BGP», «MPLS» или альтернативная подготовка.

IOS XR

Курс по оборудованию операторского класса

Описание курса

Курс предназначен для сетевых инженеров, ответственных за построение и сопровождение сетей с использованием высокопроизводительного оборудования серий Cisco ASR/XR/GSR/CRS, работающего на операционной системе Cisco IOS-XR.

Цель курса

Получить знания и навыки, необходимые для установки и эксплуатации оборудования на основе Cisco IOS-XR в сетях поставщиков услуг, а также поиска и устранения неисправностей.

По окончании курса

Вы будете:

- описывать архитектуру сетевых устройств на базе Cisco IOS-XR;
- внедрять протоколы маршрутизации RIP, EIGRP, OSPF, IS-IS, BGP;
- настраивать технологию MPLS и Traffic Engineering;
- внедрять MPLS L2VPN и MPLS L3VPN в сценариях Intra-AS и Inter-AS;
- настраивать оборудование для поддержки многоадресной рассылки;
- осуществлять поиск неисправностей в работе Cisco IOS-XR.

Содержание курса

Модуль	Название	Время
1	Основы работы в Cisco IOS-XR	8 а.ч.
2	Настройка протоколов маршрутизации	8 а.ч.
3	Внедрение технологий MPLS, MPLS TE и MPLS VPN	8 а.ч.
4	Настройка оборудования для поддержки многоадресной рассылки	4 а.ч.
5	Миграция сервисов с Cisco IOS на Cisco IOS-XR	4 а.ч.

Рекомендуемая предварительная подготовка

Прохождение обучения по курсам «Associate», «Routing», «BGP», «MPLS», «AMPLS» или альтернативная подготовка.

LNS

Курс по сетевым сервисам ОС Linux

Описание курса

Курс предназначен для инженеров, ответственных за внедрение сетевых сервисов с использованием Linux.

Цель курса

Получить знания и навыки, необходимые для установки и эксплуатации сетевых сервисов в сетях предприятий на основе Linux.

По окончании курса

Вы будете:

- уметь настраивать сетевые сервисы NTPD, DNSD, DHCPD, FTPD, SCPD, NFS, RSYNC, SQUID, WCCP, VMPS;
- настраивать маршрутизатор Linux в качестве router-on-a-stick с поддержкой тэгов 802.1Q;
- внедрять протоколы динамической маршрутизации RIP, OSPF, BGP;
- внедрять технологии NAT, CARP, VRRP;
- выполнять мониторинг сетей с помощью SYSLOG, SNMP, TFTP, NetFlow, SPAN, RMON;
- иметь представление взаимодействию сетей Linux с сетями Microsoft Windows (LDAP-интеграция);
- выполнять базовую настройку серверов приложений Apache, NGINX, SENDMAIL/POSTFIX, MySQL, Postgress.

Содержание курса

Модуль	Название	Время
1	Настройка сетевых сервисов	8 а.ч.
2	Использование Linux в качестве маршрутизатора	8 а.ч.
3	Мониторинг сетей	8 а.ч.
4	Настройка серверов приложений	4 а.ч.
5	Взаимодействие с сетями Microsoft Windows	4 а.ч.

Рекомендуемая предварительная подготовка

Прохождение обучения по курсам «Associate», «Routing», «Switching» или альтернативная подготовка.

AAA

Курс по управлению доступом в вычислительных сетях

Описание курса

Курс предназначен для сетевых инженеров и специалистов по информационной безопасности, ответственных за построение сетей с централизованным управлением. В курсе рассматривается работа AAA на Linux и Cisco в связке с сервером BE ACS.

Цель курса

Получить знания и навыки, необходимые для установки и эксплуатации оборудования на основе Cisco IOS-XR в сетях поставщиков услуг, а также поиска и устранения неисправностей.

По окончании курса

Вы будете:

- описывать архитектуру протокола RADIUS;
- описывать архитектуру протокола TACACS+;
- настраивать AAA на Linux и Cisco клиентах;
- внедрять сервер AAA BE-ACS;
- осуществлять поиск неисправностей в работе AAA.

Содержание курса

Модуль	Название	Время
1	Архитектура RADIUS	4 а.ч.
2	Архитектура TACACS+	3 а.ч.
3	Настройка AAA на клиентах Cisco и Linux	3 а.ч.
4	Настройка AAA сервера	4 а.ч.
5	Поиск неисправностей	2 а.ч.

Рекомендуемая предварительная подготовка

Прохождение обучения по курсам «Associate», «Switching», «VPN», «ASA», «LNS» или альтернативная подготовка.

LSS

Курс по сервисам безопасности ОС Linux

Описание курса

Курс предназначен для специалистов по информационной безопасности, ответственных за внедрение сервисов безопасности с использованием Linux.

Цель курса

Получить знания и навыки, необходимые для установки и эксплуатации сетевых сервисов в сетях поставщиков услуг.

По окончании курса

Вы будете:

- применять пакетный фильтр и межсетевой экран (iptables);
- внедрять VPN технологии на базе OpenVPN, Remote Access (SSH, SSL, PPTP, GRE и т.д.);
- использовать Proxy сервер Squid для организации WebVPN;
- оценивать безопасность систем и сервисов с помощью сканеров Nmap и Nessus;
- оценивать безопасность передаваемой по сети конфиденциальной информации с помощью сканера Etherscap;
- настраивать клиента протоколов RADIUS/TACACS;
- настраивать клиентов протокола 802.1x.

Содержание курса

Модуль	Название	Время
1	Настройка iptables	4 а.ч.
2	Построение VPN сетей	8 а.ч.
3	Настройка WebVPN	4 а.ч.
4	Оценка безопасности систем и сервисов	8 а.ч.
5	Применение протоколов RADIUS/TACACS/802.1x	8 а.ч.

Рекомендуемая предварительная подготовка

Прохождение обучения по курсам «Associate», «VPN», «LNS», «AAA», или альтернативная подготовка.

Design

Курс по проектированию вычислительных сетей

Описание курса

Курс предназначен для инженеров-проектировщиков, персонал служб развития корпоративных систем, ответственных за проектирование мультисервисных сетей с использованием оборудования Cisco.

Цель курса

Получить знания и навыки, необходимые для проектирования мультисервисных сетей.

По окончании курса

Вы будете:

- описывать основные принципы проектирования проводных и беспроводных сетей;
- описывать основные принципы дизайна протоколов маршрутизации;
- описывать основные принципы проектирования сервисов безопасности;
- описывать основные принципы дизайна сетей центров обработки данных;
- описывать основные принципы проектирования сетей поставщиков услуг.

Содержание курса

Модуль	Название	Время
1	Проектирование проводных и беспроводных сетей	8 а.ч.
2	Дизайн протоколов маршрутизации	8 а.ч.
3	Проектирование сервисов безопасности	8 а.ч.
4	Дизайн сетей центров обработки данных	8 а.ч.
5	Проектирование сетей поставщиков услуг	8 а.ч.

Рекомендуемая предварительная подготовка

Прохождение обучения по курсам программ Enterprise Network, Enterprise Security, Service Provider или альтернативная подготовка.