

**ОБРАЗОВАТЕЛЬНОЕ ЧАСТНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО
ОБРАЗОВАНИЯ "ЦЕНТР ОБУЧЕНИЯ "СПЕЦИАЛИСТ" УНЦ ПРИ
МГТУ ИМ. Н.Э. БАУМАНА
(ОЧУ ДПО «СПЕЦИАЛИСТ»)**

123242, город Москва, улица Зоологическая, дом 11, строение 2, этаж 2, помещение №1, комната №12,
ИНН 7701168244, ОГРН 1127799002990

Сверждаю:
Директор ОЧУ ДПО «Специалист»


/Д.Ю.Звездочкин/
17 января 2022 года
г. МОСКВА



**Дополнительная профессиональная программа
профессиональной переподготовки
«Linux. Уровень 7. Мониторинг оборудования и
интеграция с решениями Cisco»**

город Москва

Программа «Linux. Уровень 7. Мониторинг оборудования и интеграция с решениями Cisco» разработана в соответствии с требованиями Профессионального Стандарта

Повышение квалификации слушателей, осуществляемое в соответствии с программой, проводится с использованием модульного принципа построения учебного плана с применением различных образовательных технологий, в том числе дистанционных образовательных технологий и электронного обучения в соответствии с законодательством об образовании.

Дополнительная профессиональная программа повышения квалификации, разработана образовательной организацией в соответствии с законодательством Российской Федерации, включает все модули, указанные в учебном плане.

Содержание оценочных и методических материалов определяется образовательной организацией самостоятельно с учетом положений законодательства об образовании Российской Федерации.

Структура дополнительной профессиональной программы соответствует действующим нормативно-правовым актам:

- ФЗ №273 «Об образовании в Российской Федерации», приказу Минобрнауки России от 1 июля 2013 г.;

- Приказ Министерства образования и науки Российской Федерации от 1 июля 2013 г. N 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам».

Объем дополнительной профессиональной программы вне зависимости от применяемых образовательных технологий, должен быть не менее 16 академических часов. Сроки ее освоения определяются образовательной организацией самостоятельно.

Формы обучения слушателей (очная, очно-заочная, заочная) определяются образовательной организацией самостоятельно.

К освоению дополнительных профессиональных программ допускаются:

- лица, имеющие среднее профессиональное и (или) высшее образование;
- лица, получающие среднее профессиональное и (или) высшее образование.

Для определения структуры дополнительной профессиональной программы и трудоемкости ее освоения может применяться система зачетных единиц. Количество зачетных единиц по дополнительной профессиональной программе устанавливается организацией.

Образовательная деятельность слушателей предусматривает следующие виды учебных занятий и учебных работ: лекции, практические и семинарские занятия, лабораторные работы, круглые столы, мастер-классы, мастерские, деловые игры, ролевые игры, тренинги, семинары по обмену опытом, выездные занятия, консультации, выполнение аттестационной, дипломной, проектной работы и другие виды учебных занятий и учебных работ, определенные учебным планом.

Правила внутреннего распорядка обучающихся регулируются лицензией на осуществление образовательной деятельности № 039441 (бланк серия CP77Л01 № 0010312, регистрационный номер лицензии Л035-01298-77/00182700), от 20.06.2018 года "Центр обучения "Специалист" УНЦ при МГТУ им Н.Э. Баумана", а также другими локальными актами организации, регуливающими образовательную деятельность.

Аннотация. Авторы курса решили, что уж если обучать слушателей мониторингу сетевого оборудования, то на примере самого известного и передового. Кроме того, практический опыт совместной эксплуатации Cisco и *NIX систем доказал, что они прекрасно дополняют друг друга, и это не случайно – Cisco и Linux/FreeBSD имеют очень много общего.

В основу курса положена предложенная международной организацией по стандартизации FCAPS-модель, в которой отражены ключевые задачи мониторинга сетей:

- (F) Fault Management – Управление отказами
- (C) Configuration Management – Управление конфигурацией

- (A) Accounting Management – Учет работы сети
- (P) Performance Management – Управление производительностью
- (S) Security Management – Управление безопасностью

Курс построен на практическом опыте эксплуатации компьютерной сети Московского Государственного Технического Университета имени Н.Э. Баумана. В отличие от сертифицированных курсов компании Cisco, предназначенных для качественной подготовки к сертификации, наш курс ориентирован на решение практических жизненных задач, и демонстрирует уникальные возможности интеграции систем Linux/FreeBSD и Cisco.

Цель программы: программа повышения квалификации направлена на совершенствование и (или) получение новой компетенции, необходимой для профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся квалификации. Цель курса – предоставить слушателям комплекс знаний и практических навыков для работы системным администратором Linux, желающих развернуть систему мониторинга оборудования компании, в том числе устройств Cisco.

Совершенствуемые компетенции

№	Компетенция	Направление подготовки
		ФГОС ВО ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ 09.03.02 «ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ» (УРОВЕНЬ БАКАЛАВРИАТА)
		Код компетенции
1	Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности	ОПК-1
2	Способен использовать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности	ОПК-2
3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3
4	Способен участвовать в разработке технической документации, связанной с профессиональной деятельностью с использованием стандартов, норм и правил;	ОПК-4
5	Способен устанавливать программное и аппаратное обеспечение для информационных и автоматизированных систем	ОПК-5

6	Способен разрабатывать алгоритмы и программы, пригодные для практического применения в области информационных систем и технологий	ОПК-6
7	Способен осуществлять выбор платформ и инструментальных программно-аппаратных средств для реализации информационных систем	ОПК-7
8	Способен применять математические модели, методы и средства проектирования информационных и автоматизированных систем	ОПК-8

Совершенствуемые компетенции

Совершенствуемые компетенции в соответствии с трудовыми функциями профессионального стандарта 06.026 «Системный администратор информационно-коммуникационных систем» утвержден Приказом Министерства труда и социальной защиты Российской Федерации от 29.09.2020 № 680н

Совершенствуемые и/или формируемые компетенции	Направление подготовки
	ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ
	Трудовые функции (код)
	«Системный администратор информационно-коммуникационных систем»
A4 Технические работы по обслуживанию информационно-коммуникационной системы	<p>A/01.4 Выполнение работ по выявлению и устранению типичных инцидентов информационно-коммуникационных систем</p> <p>A/02.4 Выполнение работ по управлению стандартными изменениями в технических и программных средствах информационно-коммуникационных систем по инструкции</p> <p>A/03.4 Проведение инвентаризации и ведение учета технических и программных средств информационно-коммуникационных систем с использованием специализированных программ</p> <p>A/04.4 Выполнение контроля наличия запасов, своевременного проведения ремонта и наличия сервисных контрактов на обслуживание информационно-коммуникационных систем</p> <p>A/05.4 Подготовка отчетов о приобретаемых и расходуемых компонентах, подача заявок на приобретение комплектующих и проведение ремонта обслуживаемых компонентов информационно-коммуникационных систем</p>

<p>В5 Обслуживание информационно-коммуникационной системы</p>	<p>В/01.5 Выполнение работ по выявлению и устранению инцидентов в информационно-коммуникационных системах В/02.5 Обеспечение работы технических и программных средств информационно-коммуникационных систем В/03.5 Реализация схемы резервного копирования, архивирования и восстановления конфигураций технических и программных средств информационно-коммуникационных систем по утвержденным планам В/04.5 Внесение изменений в технические и программные средства информационно-коммуникационных систем по утвержденному плану работ В/05.5 Проведение обновления программного обеспечения технических средств информационно-коммуникационных систем по инструкциям производителей В/06.5 Диагностика исчерпания типовых ресурсов информационно-коммуникационных систем с использованием прикладных программных средств и средств контроля В/07.5 Проведение предварительных испытаний при проведении работ с возможными рисками перерывов в предоставлении сервисов информационно-коммуникационных систем</p>
<p>С6 Обслуживание сетевых устройств информационно-коммуникационной системы</p>	<p>С/01.6 Выполнение работ по выявлению и устранению сложных инцидентов, возникающих на сетевых устройствах информационно-коммуникационных систем С/02.6 Проведение анализа и выявление основных причин сложных проблем, возникающих на сетевых устройствах информационно-коммуникационных систем С/03.6 Разработка планов резервного копирования, архивирования и восстановления конфигураций сетевых устройств информационно-коммуникационных систем С/04.6 Планирование изменений сетевых устройств информационно-коммуникационных систем предметными специалистами из других областей</p>

	<p>C/05.6 Выполнение обновления программного обеспечения сетевых устройств информационно-коммуникационных систем</p> <p>C/06.6 Прогнозирование влияния внешних и внутренних воздействий на поведение сетевых устройств информационно-коммуникационной системы</p> <p>C/07.6 Прогнозирование потребности в изменении объемов ресурсов, необходимых для обеспечения бесперебойной работы сетевых устройств информационно-коммуникационных систем</p> <p>C/08.6 Планирование и проведение работ по распределению нагрузки между имеющимися ресурсами, снятию нагрузки на сетевые устройства информационно-коммуникационных систем перед проведением регламентных работ, восстановлению штатной схемы работы в случае сбоев</p> <p>C/09.6 Определение потребностей в приобретении специализированных средств контроля и тестирования сетевых устройств информационно-коммуникационных систем</p>
<p>D6 Обслуживание серверных операционных систем информационно-коммуникационной системы</p>	<p>D/01.6 Выполнение работ по выявлению и устранению нетипичных инцидентов, возникающих в серверных операционных системах информационно-коммуникационной системы</p> <p>D/02.6 Проведение анализа и определение основных причин сложных проблем, возникающих на серверах и в серверных операционных системах</p> <p>D/03.6 Выполнение планирования резервного копирования, архивирования и восстановления конфигурации серверов и серверных операционных систем</p> <p>D/04.6 Планирование изменений параметров работы серверов и серверных операционных систем</p> <p>D/05.6 Выполнение обновления программного обеспечения серверных операционных систем</p> <p>D/06.6 Прогнозирование влияния внешних и внутренних воздействий на поведение серверных операционных систем</p>

	<p>D/07.6 Прогнозирование потребности в изменении объемов необходимых ресурсов для обеспечения бесперебойной работы серверов и серверных операционных систем</p> <p>D/08.6 Планирование и проведение работ по распределению нагрузки между имеющимися ресурсами, снятию нагрузки на серверы и серверные операционные системы перед проведением регламентных работ, восстановлению штатной схемы работы в случае сбоев</p> <p>D/09.6 Определение потребностей в приобретении специализированных средств контроля и тестирования серверов и серверных операционных систем</p>
--	---

По окончании курса слушатели будут уметь:

- настраивать коммутаторы и маршрутизаторы Cisco через командный интерфейс;
- использовать технологии DevOps, Infrastructure-as-Code (IaC) и Ansible в компьютерных сетях;
- использовать Linux Bond интерфейсы и систему конфигурации сети Netplan;
- использовать системы мониторинга Nagios и Prometheus;
- визуализировать процессы с использованием систем Cacti и Grafana;
- настраивать уведомления с использованием Prometheus Alertmanager и Grafana;
- использовать протокол SNMP в командной строке и системах мониторинга;
- настраивать автоматическое добавление новых устройств в систему мониторинга;
- использовать Logstash для разбора, обработки и копирования журналов в Elasticsearch;
- использовать модель безопасности Cisco AAA и протоколы RADIUS/TACACS+ для управления доступом к оборудованию и подключению пользователей к сети по протоколу EAP/802.1x;
- использовать Filebeat и Elasticsearch в качестве NetFlow Collector и Kibana в качестве NetFlow Analyzer;
- предотвращать попытки вторжения с использованием IDS Snort и протокола SPAN;
- настраивать взаимодействие маршрутизаторов Linux с коммутаторами Cisco по протоколу 802.1q;
- использовать протоколы динамической маршрутизации OSPF и BGP между системами Linux и Cisco.

По окончании курса слушатели будут знать:

- принципы подхода для управления и описания инфраструктуры сети через конфигурационные файлы Infrastructure-as-Code; IaC);
- принципы работы протокола SNMP;
- принципы работы протоколов CDP/LLDP;
- принципы работы протокола NetFlow;
- принципы работы протоколов RADIUS/TACACS+;
- принципы работы протокола EAP/802.1x;
- как использовать протокол SPAN для систем IDS/IPS;
- принципы работы протокола 802.1q;

- принципы работы протокола OSPF и BGP.

Учебный план

Категория слушателей: Курс предназначен для системных администраторов, работающих с системами Linux и использующих или планирующих использовать коммутаторы и маршрутизаторы Cisco в своих сетях.

Уровень образования: дополнительное профессиональное образование: повышение квалификации/ профессиональная переподготовка.

Требования к предварительной подготовке: Успешное окончание курса «Linux. Уровень 2. Администрирование сервисов и сетей.», или эквивалентная подготовка.

Срок обучения: 24 академических часа в группе с преподавателем, 12 академических часов самостоятельных занятий в аудитории (СРС).

Форма обучения: очная, очно-заочная, заочная. По желанию слушателя форма обучения может быть изменена и/или дополнена.

Режим занятий: утренний, дневной, вечерний, группы выходного дня, онлайн

Документ, выдаваемый после завершения обучения:
Удостоверение о повышении квалификации;
Свидетельство о прохождении курсов.

№	Наименование модулей	Кол-во часов	Виды учебных занятий			Форма контроля
			Лекции	Практические занятия	СРС	
1	Знакомство с командным интерфейсом оборудования Cisco	2	1	1	1	Лабораторная работа
2	Развертывание менеджмент станции	2	1	1	1	Лабораторная работа
3	Управление производительностью	4	1	3	2	Лабораторная работа
4	Управление конфигурацией	2	1	1	1	Лабораторная работа
5	Управление отказами	4	1	3	2	Лабораторная работа
6	Учет трафика в сетях Cisco	2	1	1	1	Лабораторная работа
7	Управление безопасностью	4	2	2	1	Лабораторная работа
8	Использование виртуальных сетей (VLAN)	2	1	1	1	Лабораторная работа

9	Управление маршрутизацией	2	1	1	1	Лабораторная работа
10	Дополнительные материалы				1	
	ИТОГО	24			12	
	Итоговая аттестация	Тестирование				

Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

Количество аудиторных занятий при очно-заочной форме обучения составляет 20-25% от общего количества часов.

Календарный учебный график

Календарный учебный график формируется при осуществлении обучения в течение всего календарного года. По мере набора групп слушателей по программе составляется календарный график, учитывающий объемы лекций, практики, самоподготовки.

Неделя обучения	1	2	3	4	5	6	7	Итого часов
	пн	вт	ср	чт	пт	сб	вс	
1 неделя	8	8	8ИА					24
СРС	2	2	2	2	2	2		12
Итого:								24/12
Примечание: ИА – Итоговая аттестация (тестирование)								

Учебная программа

Наименование	Виды учебных занятий	Содержание
Модуль 1. Знакомство с командным интерфейсом оборудования Cisco	Лекция	Сеть предприятия и схема стенда
	Лекция	Архитектура эмуляторов Dynamips/GNS3
	Лекция	Интерфейсы управления оборудованием Cisco
	Лекция	Командный интерфейс Cisco
	Лабораторная работа	Использование эмулятора GNS для работы с оборудованием Cisco
	Лабораторная работа	Интерфейсы управления оборудованием Cisco
Модуль 2. Развертывание менеджмент станции	Лабораторная работа	Командный интерфейс Cisco
	Лекция	Интеграция эмуляторов GNS и VirtualBox
	Лекция	Варианты конфигурации сети в Linux (Bond и Netplan)
	Лабораторная работа	Интеграция систем виртуализации VBox и GNS
Модуль 3. Управление производительностью	Лабораторная работа	Настройка ip параметров менеджмент станции с использованием Linux bonding и netplan
	Лекция	Производительность сети и её измерение
	Лекция	Протокол SNMP
	Лекция	Архитектура RRD баз данных

	Лекция	Системы Prometheus SNMP exporter и Grafana
	Лабораторная работа	Использование средств тестирования производительности сети iperf и speedtest
	Лабораторная работа	Работа с пакетом NetSNMP
	Лабораторная работа	Использование Sacti для отображения профиля загрузки сети
	Лабораторная работа	Установка Grafana из Docker образа
	Лабораторная работа	Использование Prometheus SNMP exporter и Grafana для отображения профиля загрузки сети
Модуль 4. Управление конфигурацией	Лекция	Система описания диалогов Exect
	Лекция	Протоколы TFTP/SCP
	Лекция	Протоколы CDP/LLDP
	Лекция	Система управления конфигурациями Ansible
	Лекция	Система управления версиями Git
	Лабораторная работа	Управление конфигурацией с использованием диалогов Exect
	Лабораторная работа	Управление конфигурацией с использованием протоколов TFTP/SCP
	Лабораторная работа	Управление конфигурацией инфраструктуры с использованием Ansible
	Лабораторная работа	Использование Ansible и протокола CDP для построения топологии сети
	Лабораторная работа	Управление конфигурацией с использованием SNMP
	Лабораторная работа	Использование SNMP Trap для регистрации событий изменения конфигурации
	Лабораторная работа	Хранения истории изменения конфигураций с использованием Git
Модуль 5. Управление отказами	Лекция	Сервис Nagios
	Лекция	Сервис Prometheus blackbox exporter, Alertmanager и Pushgateway
	Лекция	Протокол Syslog
	Лекция	Расширение протокола SNMP Trap
	Лекция	Протокол RMON
	Лабораторная работа	Использование Nagios для уведомления о сбоях в сети
	Лабораторная работа	Использование Prometheus blackbox exporter и Alertmanager для уведомления о сбоях в сети
	Лабораторная работа	Использование Prometheus Pushgateway для мониторинга произвольных элементов сети
	Лабораторная работа	Использование Syslog в качестве коллектора журналов устройств Cisco
	Лабораторная работа	Использование Logstash для разбора, обработки и копирования журналов в Elasticsearch
	Лабораторная работа	Использование SNMP Trap для уведомления о сбоях и критических нагрузках в сети
	Лекция	Протокол NetFlow, пакеты nfdump и стек ELK

Модуль 6. Учет трафика в сетях Cisco	Лабораторная работа	Использование пакета nfdump в качестве NetFlow Collector и Analyzer
	Лабораторная работа	Использование Filebeat и Elasticsearch в качестве NetFlow Collector и Kibana в качестве NetFlow Analyzer
Модуль 7. Управление безопасностью	Лекция	Архитектура модели безопасности AAA оборудования Cisco
	Лекция	Протоколы RADIUS/TACACS+
	Лекция	Протокол 802.1x
	Лекция	Протокол SPAN
	Лекция	Системы IDS/IPS
	Лекция	Сервис Fail2Ban
	Лабораторная работа	Использование протоколов RADIUS/TACACS+ для управления учетными записями и доступом в оборудовании Cisco
	Лабораторная работа	Управление доступом пользователей к сети по протоколу 802.1x
	Лабораторная работа	Использование протокола SPAN для IDS Snort
Модуль 8. Использование виртуальных сетей (VLAN)	Лекция	Протокол 802.1q
	Лабораторная работа	Настройка маршрутизатора Linux в качестве Router-on-a-Stick
Модуль 9. Управление маршрутизацией	Лекция	Проверка отказоустойчивости ядра сети в случае частичного отказа оборудования
	Лекция	Статическая и динамическая маршрутизация
	Лекция	Протоколы OSPF и BGP
	Лабораторная работа	Настройка протоколов OSPF и BGP между маршрутизаторами Cisco и Linux
Модуль 10. Дополнительные материалы		https://www.specialist.ru/center/video/1221/elastic-stack-dlya-setevogo-inzhenera

Организационно-педагогические условия

Соблюдение требований к кадровым условиям реализации дополнительной профессиональной программы:

а) преподавательский состав образовательной организации, обеспечивающий образовательный процесс, обладает высшим образованием и стажем преподавания по изучаемой тематике не менее 1 года и (или) практической работы в областях знаний, предусмотренных модулями программы, не менее 3 (трех) лет;

б) образовательной организацией наряду с традиционными лекционно-семинарскими занятиями применяются современные эффективные методики преподавания с применением интерактивных форм обучения, аудиовизуальных средств, информационно-телекоммуникационных ресурсов и наглядных учебных пособий.

Соблюдение требований к материально-техническому и учебно-методическому обеспечению дополнительной профессиональной программы:

а) образовательная организация располагает необходимой материально-технической базой, включая современные аудитории, библиотеку, аудиовизуальные средства обучения, мультимедийную аппаратуру, оргтехнику, копировальные аппараты. Материальная база соответствует санитарным и техническим нормам и правилам и обеспечивает проведение

всех видов практической и дисциплинарной подготовки слушателей, предусмотренных учебным планом реализуемой дополнительной профессиональной программы.

б) в случае применения электронного обучения, дистанционных образовательных технологий каждый обучающийся в течение всего периода обучения обеспечивается индивидуальным неограниченным доступом к электронной информационно образовательной среде, содержащей все электронные образовательные ресурсы, перечисленные в модулях дополнительной профессиональной программы.

Формы аттестации и оценочные материалы

Образовательная организация несет ответственность за качество подготовки слушателей и реализацию дополнительной профессиональной программы в полном объеме в соответствии с учебным планом.

Оценка качества освоения слушателями программы курса включает текущий контроль успеваемости и промежуточную аттестацию.

Слушатели, успешно освоившие программу курса и прошедшие промежуточную аттестацию, получают удостоверение о повышении квалификации, а также допускаются к освоению следующего курса, входящего в состав дипломной программы (ДПП подготовки).

Слушателям, не прошедшим промежуточной аттестации или получившим на промежуточной аттестации неудовлетворительные результаты, а также лицам, освоившим часть курса и (или) отчисленным из образовательной организации, выдается справка об обучении или о периоде обучения по образцу, самостоятельно устанавливаемому образовательной организацией.

К итоговой аттестации по ДПП переподготовки допускаются только те слушатели, которые сдали промежуточную аттестацию по всем курсам (включая данный), входящим в дипломную программу (ДПП переподготовки).

Промежуточная аттестация проводится по форме выполнения задания в соответствии с учебным планом. Результаты промежуточной аттестации заносятся в соответствующие документы. Результаты промежуточной аттестации слушателей ДПП выставляются по двух бальной шкале («зачтено»/ «не зачтено»). «Зачтено» выставляется, если слушатель набирает не менее 70% баллов (правильных ответов и/или выполненных заданий).

Учебно-методическое обеспечение и информационное обеспечение программы (литература)

Нормативно-правовые документы, дополнительная литература: авторские наработки преподавателя.

Материально-технические условия реализации программы: чехол одноразовый на наушник, файл-вкладыш А4, тетрадь, ручка

Текущая аттестация (выполнение практических/лабораторных работ по модулям)

Лабораторные работы по первому модулю:

Использование эмулятора GNS для работы с оборудованием Cisco

Интерфейсы управления оборудованием Cisco

Командный интерфейс Cisco

Лабораторные работы по второму модулю:

Интеграция систем виртуализации VBox и GNS

Настройка ip параметров менеджмент станции с использованием Linux bonding и netplan

Лабораторные работы по третьему модулю:

Использование средств тестирования производительности сети iperf и speedtest

Работа с пакетом NetSNMP

Использование Cacti для отображения профиля загрузки сети

Установка Grafana из Docker образа

Использование Prometheus SNMP exporter и Grafana для отображения профиля загрузки сети

Лабораторные работы по четвертому модулю:

Управление конфигурацией с использованием диалогов Exрrest

Управление конфигурацией с использованием протоколов TFTP/SCP

Управление конфигурацией инфраструктуры с использованием Ansible

Использование Ansible и протокола CDP для построения топологии сети

Управление конфигурацией с использованием SNMP

Использование SNMP Trap для регистрации событий изменения конфигурации

Хранения истории изменения конфигураций с использованием Git

Лабораторные работы по пятому модулю:

Использование Nagios для уведомления о сбоях в сети

Использование Prometheus blackbox exporter и Alertmanager для уведомления о сбоях в сети

Использование Prometheus Pushgateway для мониторинга произвольных элементов сети

Использование Syslog в качестве коллектора журналов устройств Cisco

Использование Logstash для разбора, обработки и копирования журналов в Elasticsearch

Использование SNMP Trap для уведомления о сбоях и критических нагрузках в сети

Лабораторные работы по шестому модулю:

Использование Filebeat и Elasticsearch в качестве NetFlow Collector и Kibana в качестве NetFlow Analyzer

Лабораторные работы по седьмому модулю:

Использование протоколов RADIUS/TACACS+ для управления учетными записями и доступом в оборудовании Cisco

Управление доступом пользователей к сети по протоколу 802.1x

Использование протокола SPAN для IDS Snort

Использование связки Snort/Fail2Ban для построения системы IPS

Лабораторные работы по восьмому модулю:

Настройка маршрутизатора Linux в качестве Router-on-a-Stick

Лабораторные работы по девятому модулю:

Настройка протоколов OSPF и BGP между маршрутизаторами Cisco и Linux

Итоговая аттестация по курсу (тестирование):

Аттестация проводится в виде теста на последнем занятии или на основании оценок практических работ, выполняемых во время обучения на курсе. Для успешной сдачи теста Вам нужно правильно ответить на 25 вопросов из 30.

Вопрос 1

Что обозначает аббревиатура SMNP?

Выберите один ответ:

Simple Network Management Protocol

Security Not My Problem

Вопрос 2

База RRD имеет объем данных, который со временем

Выберите один ответ:

не меняется

уменьшается

увеличивается

Вопрос 3

Какая из перечисленных характеристик сети НЕ относится к производительности?

Выберите один ответ:

Скорость передачи данных

Задержка передачи данных

Стоимость передачи данных

Надежность передачи данных

Вопрос 4

Технология Transparent Proxy перестала быть актуальной по причине

Выберите один ответ:

массового перехода сайтов на протокол HTTPS

необходимости настройки браузеров пользователей

отсутствия поддержки в Linux

Вопрос 5

В модели AAA, ехес это список

Выберите один ответ:

аутентификации

авторизации

учета

Вопрос 6

Какое утверждение верно?

Выберите один ответ:

Протокол RADIUS включает все возможности протокола TACACS+

Протокол TACACS+ включает все возможности протокола RADIUS

Протокол TACACS+ и протокол RADIUS не имеют отношения друг к другу

Вопрос 7

Какие технологии можно использовать в маршрутизаторе Cisco для мониторинга возможности использования нескольких ISP?

Выберите один ответ:

SLA

EIGRP

CDP

Вопрос 8

Какое утверждение, в отношении протокола маршрутизации OSPF, верно?

Выберите один ответ:

OSPF - проприетарный протокол

OSPF - дистанционно векторный протокол

OSPF – протокол внутримоментной маршрутизации

Вопрос 9

Какая технология может использоваться для балансировки нагрузки между несколькими ISP?

Выберите один ответ:

PBR

OSPF

CDP

Вопрос 10

В архитектуре протокола Netflow размещением данных в хранилище занимается
Выберите один ответ:

- сенсор
- коллектор
- анализатор

Вопрос 11

В архитектуре протокола Netflow формированием отчетов занимается
Выберите один ответ:

- сенсор
- коллектор
- анализатор

Вопрос 12

В архитектуре протокола Netflow сбором статистики занимается
Выберите один ответ:

- сенсор
- коллектор
- анализатор

Вопрос 13

Какая клавиша дописывает ключевые слова команды в Cisco?

Выберите один ответ:

- «tab»
- «пробел»
- «?»

Вопрос 14

Какая команда в Cisco используется для поиска строк, содержащих заданный образец?

Выберите один ответ:

- grep
- inc
- find

Вопрос 15

Какая клавиша выводит варианты набора команды в Cisco?

Выберите один ответ:

- «tab»
- «пробел»
- «?»

Вопрос 16

Какое утверждение НЕ верно?

Выберите один ответ:

- Трафик, передающийся в Native VLAN, не тегируется
- При настройке Router-on-a-stick адрес Native VLAN настраивается на физическом интерфейсе Linux
- Native VLAN всегда совпадает с Vlan 1

Вопрос 17

Как увеличивается размер фрейма в протоколе 802.1q?

Выберите один ответ:
На 4 байта
На 8 байт
Остается неизменным

Вопрос 18

Какой командой Cisco IOS можно посмотреть содержимое файла конфигурации, расположенного на TFTP сервере?

Выберите один ответ:
more
less
cat

Вопрос 19

Чем значение OID ifAdminStatus отличается от ifOperStatus?

Выберите один ответ:
Ничем, это синонимы
ifAdminStatus имеет приоритет над ifOperStatus
ifAdminStatus определяет, разрешено ли использовать интерфейс, ifOperStatus – реальное состояние

Вопрос 20

Существует ли Open source реализация Cisco Discovery Protocol?

Выберите один ответ:
Да
Нет
Да, но требует лицензирования

Вопрос 21

Для получения trap сообщений менеджер SNMP по умолчанию использует

Выберите один ответ:
транспортный протокол TCP и порт 161
транспортный протокол UDP и порт 161
транспортный протокол UDP и порт 162

Вопрос 22

Для протокола Syslog по умолчанию используется

Выберите один ответ:
транспортный протокол TCP и порт 110
транспортный протокол UDP и порт 514
транспортный протокол UDP и порт 69

Вопрос 23

Тип сообщений, передаваемых Cisco устройством Syslog серверу, определяется в конфигурации

Выберите один ответ:
Cisco устройства
Syslog сервера

Вопрос 24

Когда нужно настраивать IP адрес на layer 2 коммутаторе?

Выберите один ответ:

Всегда, иначе устройство работать не будет.

Никогда, поскольку IP адреса используются на layer 3.

Если планируется управление/мониторинг коммутатора.

Вопрос 25

На каком интерфейсе коммутаторов Cisco настраивается IP адрес?

Выберите один ответ:

На Vlan интерфейсе

На Ethernet интерфейсе

На layer 3 интерфейсе

Вопрос 26

Какое утверждение про протокол RMON HE верно?

Выберите один ответ:

Протокол RMON позволяет производить обработку данных на стороне устройства

Использование протокола RMON позволяет уменьшить SNMP трафик

Протокол RMON периодически уведомляет станцию управления о результатах мониторинга

Вопрос 27

Для чего HE используется общий секрет между RADIUS сервером и сервером доступа?

Выберите один ответ:

Для шифрования всего трафика

Для шифрования паролей пользователей

Для подтверждения подлинности транзакций

Вопрос 28

Пригодна ли технология Cisco SPAN как источник данных для систем IDS/IPS?

Выберите один ответ:

Да

Нет

Вопрос 29

Какая команда SMNP используется для перебора значений внутри заданного OID'ом диапазона?

Выберите один ответ:

WALK

GET

GETNEXT

Вопрос 30

Можно ли использовать порт коммутатора Cisco одновременно и для SPAN и для передачи трафика, адресованного подключенной к этому порту рабочей станции?

Выберите один ответ:

Да

Нет

Если позволяет загрузка порта