Образовательное частное учреждение
Дополнительного профессионального образования «Центр компьютерного обучения «Специалист» Учебно-научного центра при МГТУ им. Н.Э. Баумана»
(ОЧУ «Специалист»)

123242, город Москва, улица Зоологическая, дом 11, строение 2, помещение I, комната 11
ИНН 7701257303, ОГРН 1037739408189

Утверждаю:
Директор ОЧУ «Специалист»

/Т.С.Григорьева/
«01» июня 2018 года

Рабочая программа курса
«CCNA Безопасность в сетях Cisco»

Дополнительной программы профессиональной переподготовки
«Сертифицированный Сетевой Администратор (CCNA + Безопасность)»

город Москва

Программа разработана в соответствии с приказом 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".

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 требованиям Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам, утвержденного приказом Минобрнауки России от 1 июля 2013 г. N 499.

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.

Аннотация. Курс Cisco CCNA Security является следующим этапом для желающих улучшить свои навыки уровня CCNA**.** Учебная программа знакомит слушателя с основными теоретическими принципами безопасности и дает практические навыки, необходимые для установки, устранения неполадок и мониторинга сетевых устройств и позволяющие поддерживать целостность, конфиденциальность и доступность данных и устройств.

Цель программы: познакомить слушателей с основными теоретическими принципами безопасности и дать практические навыки, необходимые для установки, устранения неполадок и мониторинга сетевых устройств и позволяющие поддерживать целостность, конфиденциальность и доступность данных и устройств. Дать теоретические знания и практические навыки, необходимые для сдачи экзамена по международной сертификации CCNA.

Совершенствуемые компетенции

№	Компетенция	Направление подготовки
		ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО ОБРАЗОВАТЕЛЬНОГО СТАНДАРТА ВЫСШЕГО ОБРАЗОВАНИЯ ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ 09.03.02 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ (УРОВЕНЬ БАКАЛАВРИАТА)
		Код компетенции
1	способность обеспечивать безопасность и целостность данных информационных систем и технологий	ПК-31

Совершенствуемые компетенции в соответствии с трудовыми фикциями профессионального стандарта «Системный администратор информационно-коммуникационных систем" (Приказ Министерства труда и социальной защиты РФ от 5 октября 2015 г. N 684н "Об утверждении профессионального стандарта "Системный администратор информационно-коммуникационных систем").

№	Компетенция ОТФ	Направление подготовки
		ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ «Системный администратор информационно-коммуникационных систем»
		Трудовые функции (код)
1	D - Администрирование сетевой подсистемы инфокоммуникационной системы организации	D 03/6 Управление безопасностью сетевых устройств и программного обеспечения

Планируемый результат обучения:

После окончания обучения Слушатель будет знать:

- Как разработать политику безопасности сети, оценить возможные угрозы и эффективно бороться с ними, получите навыки по обеспечению безопасности сетевого периметра и сетевых устройств всех уровней.
- Как работать с современной сетью и пользоваться последними технологиями в сфере сетевой безопасности.
- Как работать с технологиями AAA, Firewall, VPN.

После окончания обучения Слушатель будет уметь:

- Разрабатывать политику безопасности сети, оценить возможные угрозы и эффективно бороться с ними, получите навыки по обеспечению безопасности сетевого периметра и сетевых устройств всех уровней.

- Работать с современной сетью и пользоваться последними технологиями в сфере сетевой безопасности.
- Научитесь работать с технологиями AAA, Firewall, VPN.

2. Учебный план:

Срок обучения: 72 академических часов, в том числе 16 аудиторных, 56 самостоятельно (СРС).
Форма обучения: очная, очно-заочная, заочная. По желанию слушателя форма обучения может быть изменена и/или дополнена.

Режим занятий: дневной, вечерний, группы выходного дня.

№ п/п	Наименование модулей по программе	Общая трудоемкость (акад. часов)	Всего ауд. ч	В том числе		СРС,ч	Форма ТА[1]
				Лекций	Практ занятий		
1	Модуль 1. Фундаментальные принципы безопасной сети	7	2	1	1	5	Лабораторная работа
2	Модуль 2. Безопасность Сетевых устройств OSI 2	7	2	1	1	5	Лабораторная работа
3	Модуль 3. Авторизация, аутентификация и учет доступа (AAA)	6	1	0	1	5	Лабораторная работа
4	Модуль 4. Реализация технологий брандмауэра	6	1	0	1	5	Лабораторная работа
5	Модуль 5. Реализация технологий предотвращения вторжения	7	2	1	1	6	Лабораторная работа
6	Модуль 6. Безопасность локальной сети	7	2	1	1	6	Лабораторная работа
7	Модуль 7. Криптографические системы	7	1	0	1	6	Лабораторная работа

[1] ПА – промежуточная аттестация.1

8	Модуль 8. Реализация технологий VPN	8	2	1	1	6	Лабораторная работа
9	Модуль 9. Управление безопасной сетью	7	1	0	1	6	Лабораторная работа
10	Модуль 10. Cisco ASA	8	2	1	1	6	Лабораторная работа
	Итого:	72	16	6	10	56	
	Промежуточная 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.

Форма Промежуточной аттестации – см. в ЛНА «Положение о проведении промежуточной аттестации слушателей и осуществлении текущего контроля их успеваемости» п.3.3.

1. 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, выезды на объекты.

Неделя обучения	1	2	3	4	5	6	7	Итого часов
	пн	вт	ср	чт	пт	сб	вс	
1 неделя	1	-	1	-	1	-	-	3
СРС	3	-	3	-	4	-	-	10
2 неделя	1	-	1	-	1	-	-	3
СРС	3	-	3	-	3	-	-	9
3 неделя	1	-	1	-	1	-	-	3
СРС	3	-	3	-	3	-	-	9
4 неделя	1	-	1	-	1	-	-	3
СРС	3	-	3	-	3	-	-	9
5 неделя	1	-	0	-	0	-	-	1
СРС	3	-	3	-	3	-	-	9
6 неделя	1	-	0	-	2ПА	-	-	3
СРС	3	-	3	-	4	-	-	10
Итого:	24	-	22	-	26	-	-	72
Примечание: ПА – Промежуточная аттестация (тестирование)								

2. Рабочие программы учебных предметов

Модуль 1. Фундаментальные принципы безопасной сети
Современные угрозы сетевой безопасности
Вирусы, черви и троянские кони
Методы атак

Модуль 2. Безопасность Сетевых устройств OSI 2
Безопасный доступ к устройствам
Назначение административных ролей
Мониторинг и управление устройствами
Использование функция автоматизированной настройки безопасности

Модуль 3. Авторизация, аутентификация и учет доступа (AAA)
Свойства AAA
Локальная AAA аутентификация
Server-based AAA

Модуль 4. Реализация технологий брандмауэра
ACL
Технология брандмауэра
Контекстный контроль доступа (CBAC)
Политики брандмауэра основанные на зонах

Модуль 5. Реализация технологий предотвращения вторжения
IPS технологии
IPS сигнатуры
Реализация IPS
Проверка и мониторинг IPS

Модуль 6. Безопасность локальной сети
Обеспечение безопасности пользовательских компьютеров
Соображения по безопасности второго уровня (Layer-2)
Конфигурация безопасности второго уровня
Безопасность беспроводных сетей, VoIP и SAN

Модуль 7. Криптографические системы
Криптографические сервисы
Базовая целостность и аутентичность
Конфиденциальность
Криптография открытых ключей

Модуль 8. Реализация технологий VPN
VPN
GRE VPN
Компоненты и функционирование IPSec VPN
Реализация Site-to-site IPSec VPN с использованием CLI
Реализация Site-to-site IPSec VPN с использованием CCP
Реализация Remote-access VPN

Модуль 9. Управление безопасной сетью

Принципы безопасности сетевого дизайна.
Безопасная архитектура.
Управление процессами и безопасность
Тестирование сети на уязвимости
Непрерывность бизнеса, планирование восстановления аварийных ситуаций.
Жизненный цикл сети и планирование.
Разработка регламентов компании и политик безопасности.

Модуль 10. Cisco ASA
Введение в Адаптивное устройство безопасности ASA
Конфигурация фаирвола на базе ASA с использованием графического интерфейса ASDM
Конфигурация VPN на базе ASA с использованием графического интерфейса ASDM

3. 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.

4. 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.

Текущая аттестация проводится в форме, предусмотренной ЛНА «Положение о проведении промежуточной аттестации слушателей и осуществлении текущего контроля их успеваемости» п.3.3. и определяется преподавателем курса. К промежуточной аттестации допускаются слушатели, выполнившие все виды текущей аттестации, предусмотренные в настоящей программе.

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) отчисленные 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).

Текущая аттестация:

Практическая работа (выполнение заданий**):**

№п/п	***Тематика практического занятия***	***Форма ПА***
Модуль 1.	Фундаментальные принципы безопасной сети	Лабораторная работа
Модуль 2.	Безопасность Сетевых устройств OSI 2	Лабораторная работа
Модуль 3.	Авторизация, аутентификация и учет доступа (AAA)	Лабораторная работа
Модуль 4.	Реализация технологий брандмауэра	Лабораторная работа
Модуль 5.	Реализация технологий предотвращения вторжения	Лабораторная работа
Модуль 6.	Безопасность локальной сети	Лабораторная работа
Модуль 7.	Криптографические системы	Лабораторная работа
Модуль 8.	Реализация технологий VPN	Лабораторная работа
Модуль 9.	Управление безопасной сетью	Лабораторная работа
Модуль 10.	Cisco ASA	Лабораторная работа

Промежуточная аттестация по курсу (тестирование):

Вопросы теста/ответ:

Вопрос 1

Отметить

Какой тип трафика, вероятнее всего, создаст проблемы при прохождении через устройство NAT?

Выберите один ответ:

- Telnet
- IPsec
- HTTP
- ICMP
- DNS

Вопрос 2

Отметить

Сетевой инженер настраивает интерфейс, вводя следующую команду: SanJose(config)# ip address 192.168.2.1 255.255.255.0 Команда отклоняется устройством. В чем причина?

Выберите один ответ:

- команда вводится в неправильным режиме работы
- используется неправильный синтаксис команды
- неправильная маска подсети
- интерфейс выключен и должен быть включен до того, как коммутатор утвердит IP-адрес

Вопрос 3

Отметить

В местном учебном заведении студентам разрешено подключаться к беспроводной сети без пароля. В каком режиме работает точка доступа?

Выберите один ответ:

- сетевой
- открытый
- пассивный
- режим общего ключа

Вопрос 4

Отметить

Какое утверждение о маршрутизации IPv6 является правильным?

Выберите один ответ:

- Маршрутизация IPv6 включена на маршрутизаторах Cisco по умолчанию
- IPv6 поддерживает только протоколы маршрутизации OSPF и EIGRP.

- Маршруты IPv6 отображаются в той же таблице маршрутизации, что и маршруты IPv4.
- IPv6 использует локальный канальный адрес соседей в качестве адреса следующего перехода для динамических маршрутов.

Вопрос 5

Отметить

Взгляните на рисунок. Сетевой администратор настраивает управление доступом к коммутатору SW1. Если администратор использует консольное подключение для подключения к коммутатору, какой пароль требуется ввести для доступа к пользовательскому режиму EXEC?

```
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)# enable password letmein
SW1(config)# enable secret secretin
SW1(config)# line console 0
SW1(config-line)# password lineconin
SW1(config-line)# login
SW1(config-line)# exit
SW1(config)# line vty 0 15
SW1(config-line)# password linevtyin
SW1(config-line)# login
SW1(config-line)# end
SW1#
```

Выберите один ответ:

- letmein
- secretin
- lineconin
- linevtyin

Вопрос 6

Отметить

Сетевой администратор решает проблему низкой производительности в коммутируемой сети 2-го уровня. Проанализировав IP-заголовок, администратор замечает, что значение TTL не уменьшается. Почему значение TTL не становится меньше?

Выберите один ответ:

- Это нормальное поведение для сети 2-го уровня.
- Таблица MAC-адресов заполнена
- База данных VLAN повреждена
- Входящий интерфейс настроен на полудуплексную передачу

Вопрос 7

Отметить

Сеть содержит несколько сетей VLAN, охватывающих несколько коммутаторов. Что происходит, когда устройство в VLAN 20 передаёт широковещательный Ethernet-кадр?

Выберите один ответ:

- Все устройства во всех сетях VLAN видят этот кадр.
- Только устройства в VLAN 20 видят этот кадр
- Устройства в VLAN 20 и VLAN управления (management VLAN) видят этот кадр.
- Только устройства, подключённые к локальному коммутатору, видят этот кадр.

Вопрос 8

Отметить

Сколько голосовых каналов 64 кбит/с содержит линия T1?

Выберите один ответ:

- 8
- 16
- 24
- 32

Вопрос 9

Отметить

Сообщения SNMP какого типа немедленно информируют систему управления сетями (NMS) об отдельных важных событиях?

Выберите один ответ:

- Запрос GET
- Запрос SET
- Ответ GET
- Ловушка (TRAP)

Вопрос 10

Отметить

Что показывает стоимость канала OSPF?

Выберите один ответ:

- Более высокая стоимость канала OSPF означает более быстрый путь к месту назначения

- Стоимость канала указывает пропорцию суммарного значения маршрута до места назначения.
- Стоимость соответствует пропускной способности.
- Более низкая стоимость указывает лучший путь к месту назначения, чем при более высокой стоимости.