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 №I, комната №12,
ИНН 7701168244, ОГРН 1127799002990

Утверждаю:
Директор ОЧУ ДПО «Специалист»

/Е.В.Добрыднева/
«01» июня 2018 года

Дополнительная профессиональная программа повышения квалификации
«CCNA Безопасность в сетях Cisco»

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. Обучение построено с упором на практику и дает необходимые навыки для получения международной сертификации CCNA Security. На данный момент учебные материалы по курсу представлены на английском языке. Курс готовит к сдаче экзамена для получения престижной международной сертификации CCNA Security. После обучения слушатель получает сертификат об успешном прохождении курса от компании Cisco Systems. Данный курс готовит к успешной сдаче международных сертификационных экзаменов: IINS Implementing Cisco IOS Network Security.

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 практические знания и навыки, необходимые для установки, устранения неполадок и мониторинга сетевых устройств.

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	способностью проводить выбор исходных данных для проектирования	ПК-4
2	способностью использовать математические методы обработки, анализа и синтеза результатов профессиональных исследований	ПК-25

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	B5 Администрирование прикладного программного Обеспечения инфокоммуникационной системы организации	B/01.5 Установка прикладного программного обеспечения B/02.5 Оценка критичности возникновения инцидентов при работе прикладного программного обеспечения. B/03.5 Оптимизация функционирования прикладного программного обеспечения B/04.5 Интеграция прикладного программного обеспечения в единую

		структуру инфокоммуникационной системы. B/05.5 Реализация регламентов обеспечения информационной безопасности прикладного программного обеспечения. B/06.5 Разработка нормативно-технической документации на процедуры управления прикладным программным обеспечением. B/07.5 Разработка требований к аппаратному обеспечению и поддерживающей инфраструктуре для эффективного функционирования прикладного 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.
- работать с технологиями AAA, Firewall, VPN.

2. Учебный план:

Категория слушателей: курс рекомендован всем, кто хочет научиться маршрутизировать в сетях Cisco. Программа курса предоставляет всесторонние теоретические знания на языке, который оптимально подходит для изложения инженерных принципов. На курсе будут также и интерактивные занятия, дополняющие подробные теоретические материалы.

Требования к предварительной подготовке: Успешное окончание курса CCNA 3.0 Маршрутизация и коммутация в сетях Cisco или эквивалентная подготовка.

Срок обучения: 60 академических часов, в том числе 48 аудиторных, 12 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 ПА[1]
				Лекций	Практ занятий		
1	Модуль 1. Фундаментальные принципы безопасной сети	2	1	1	0	1	-
2	Модуль 2. Безопасность Сетевых устройств OSI	2	1	1	0	1	Лабораторная работа
3	Модуль 3. Авторизация, аутентификация и учет доступа (AAA)	3	2	1	1	1	Лабораторная работа
4	Модуль 4. Реализация технологий брандмауэра	3	2	1	1	1	Лабораторная работа
5	Модуль 5. Реализация технологий предотвращения вторжения	4	2	1	1	2	Лабораторная работа
6	Модуль 6. Безопасность локальной сети	4	2	1	1	2	Лабораторная работа
7	Модуль 7. Криптографические системы	4	2	1	1	2	Лабораторная работа
8	Модуль 8. Реализация технологий VPN	4	2	1	1	2	Лабораторная работа
9	Модуль 9. Управление безопасной сетью	3	1	0	1	2	Лабораторная работа
10	Модуль 10. Cisco ASA	3	1	0	1	2	Лабораторная работа

[1] ПА – промежуточная аттестация.

	Итого:	32	16	8	8	16	
	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.

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	4	-	4	-	-	-	-	8
СРС	4	-	4	-	-	-	-	8
2 неделя	4	-	4	-	-	-	-	8
СРС	4	-	4	-	-	-	-	8
Итого:	16	-	16	-	-	-	-	32
Примечание: ИА – Итоговая 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

- 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

- 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.

- 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 дополнительной профессиональной программы слушателей включает текущий контроль успеваемости и итоговую аттестацию.

Промежуточная аттестация по данному курсу проводится в форме выполнения практических работ, к итоговой аттестации допускаются слушатели, выполнившие все практические работы.

Результаты итоговой аттестации слушателей ДПП в соответствии с формой итоговой аттестации, установленной учебным планом, выставляются по двух бальной шкале («зачтено\незачтено»).

Слушателям, успешно освоившим дополнительную профессиональную программу и прошедшим итоговую аттестацию, выдается удостоверение о повышении квалификации.

Слушателям, не прошедшим итоговой аттестации или получившим на итоговой аттестации неудовлетворительные результаты, а также лицам, освоившим часть дополнительной профессиональной программы и (или) отчисленным из образовательной организации, выдается справка об обучении или о периоде обучения по образцу, самостоятельно устанавливаемому образовательной организацией. Результаты итоговой аттестации заносятся в соответствующие документы.

Итоговая аттестация проводится по форме представления учебных проектов и подготовки личного портфолио.

Промежуточная аттестация:

Практическая работа (выполнение заданий**):**

№п/п	***Тематика практического занятия***	***Форма ПА***
Модуль 2.	Использование функция автоматизированной настройки безопасности	Лабораторная работа
Модуль 3.	Server-based AAA	Лабораторная работа
Модуль 4.	Политики брандмауэра основанные на зонах	Лабораторная работа
Модуль 5.	Проверка и мониторинг IPS	Лабораторная работа
Модуль 6.	Безопасность беспроводных сетей, VoIP и SAN	Лабораторная работа
Модуль 7.	Криптография открытых ключей	Лабораторная работа
Модуль 8.	Реализация Remote-access VPN	Лабораторная работа
Модуль 9.	Разработка регламентов компании и политик безопасности.	Лабораторная работа
Модуль 10.	Конфигурация VPN на базе ASA с использованием графического интерфейса A	Лабораторная работа

Итоговая аттестация по курсу (тестирование):

Вопросы теста/ответ:

Как называются дополнительные 32 бита в директиве access-list?
• Биты шаблона

Каким образом маршрутизатор различает стандартные списки управления доступом и расширенные?
• Стандартные списки управления доступом имеют номера от 1 до 99. Расширенные списки управления доступом имеют номера от 100 до 199

Какому из приведенных ниже высказываний эквивалентно выполнение
команды Router(config)# access-list 1 156.1.0.0 0.0.255.255?
• "Разрешить доступ только к моей сети."

Какую из приведенных ниже команд следует использовать для того, чтобы выяснить, установлены ли на данном интерфейсе списки управления доступом?

• show ip interface

Команда show access-list используется для того, чтобы:
• просмотреть директивы списка управления доступом

Утверждение: "При задании разрешения на доступ в списке управления, сопровождаемом неявным "отказать всем", всем потокам данных, кроме указанного в директиве permit, будет отказано в доступе".
• Истинно