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

Дополнительная профессиональная программа повышения квалификации

«SIMOS: Обеспечение безопасности мобильных решений на базе оборудования 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 обучения под руководством инструктора, являющийся частью учебной программы, направленной на получение сертификации **Cisco CCNP Security**.

Данный курс разработан с целью подготовить инженеров сетевой безопасности, предоставив им знания и опыт, необходимые для защиты данных, проходящих по разделяемой среде, такой как Internet, посредством внедрения и поддержки решений Cisco VPN. Слушатели курса получат практический опыт настройки и диагностики решений удаленного доступа на основе многофункциональных устройств Cisco ASA и маршрутизаторов, работающих под управлением Cisco IOS.

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 подготовить инженеров сетевой безопасности, предоставив им знания и опыт, необходимые для защиты данных, проходящих по разделяемой среде, такой как Internet, посредством внедрения и поддержки решений Cisco VPN.

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:

- Описать различные технологии VPN и варианты развертывания, а также криптографические алгоритмы и протоколы, которые обеспечивают безопасность VPN.
- Развертывание и поддержка решений Cisco site-to-site VPN.
- Развертывание и поддержка Cisco FlexVPN в point-to-point, hub-and-spoke, and spoke-to-spoke IPsec VPNs.
- Развертывание и поддержка бесклиентских Cisco SSL VPNs.
- Развертывание и поддержка Cisco AnyConnect SSL и IPsec VPN.
- Развертывание и поддержка безопасности оконечных устройств и динамических политик доступа (DAP)

После окончания обучения Слушатель будет уметь:

- Описать различные технологии VPN и варианты развертывания, а также криптографические алгоритмы и протоколы, которые обеспечивают безопасность VPN.
- Развертывание и поддержка решений Cisco site-to-site VPN.
- Развертывание и поддержка Cisco FlexVPN в point-to-point, hub-and-spoke, and spoke-to-spoke IPsec VPNs.
- Развертывание и поддержка бесклиентских Cisco SSL VPNs.
- Развертывание и поддержка Cisco AnyConnect SSL и IPsec VPN.
- Развертывание и поддержка безопасности оконечных устройств и динамических политик доступа (DAP)

2. Учебный план:

Категория слушателей: инженеров сетевой безопасности

Требования к предварительной подготовке:

Успешное окончание курса IINS 3.0: Внедрение безопасности в сетях CISCO. Версия 3.0 или эквивалентная подготовка.

Требуемая подготовка: «Английский язык. Уровень 2. Elementary, часть 2», 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. Основы технологий VPN и криптография	8	8	2	6	0	Лабораторная работа
2	Модуль 2. Внедрение защищенных решений для соединений Site-to-Site	8	8	2	6	0	Лабораторная работа
3	Модуль 3. Внедрение решений Site-to-Site FlexVPN на основе Cisco IOS	8	8	2	6	0	Лабораторная работа
4	Модуль 4. Внедрение AnyConnect VPN для удаленного доступа	8	8	2	6	0	Лабораторная работа
5	Модуль 5. Внедрение Cisco AnyConnect VPN	4	4	2	6	0	Лабораторная работа
6	Модуль 6. Обеспечение безопасности оконечных устройств и политик динамического доступа	4	4	2	6	0	Лабораторная работа
	Итого:	40	40	8	8	0	
	Итоговая аттестация	тестирование					

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

[1] ПА – промежуточная аттестация.

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. Основы технологий VPN и криптография

- Роль VPN в сетевой безопасности
- VPN и криптография

Модуль 2. Внедрение защищенных решений для соединений Site-to-Site

- Введение в решения Cisco для защищенных соединений Site-to-Site
- Внедрение Point-to-Point IPsec VPN на Cisco ASA
- Внедрение решений VTI Point-to-Point IPsec VPN на основе Cisco IOS
- Внедрение Cisco IOS DMVPNs
- Лабораторная работа: Осуществление безопасного соединения Site-to-Site на Cisco ASA
- Лабораторная работа: Развертывание Cisco IOS Static VTI Point-to-Point туннелей
- Лабораторная работа: Реализация DMVPN

Модуль 3. Внедрение решений Site-to-Site FlexVPN на основе Cisco IOS

- Введение в решение Cisco FlexVPN
- Внедрение Point-to-Point IPsec VPNs с использованием Cisco IOS FlexVPN
- Внедрение Hub-and-Spoke IPsec VPNs с использованием Cisco IOS FlexVPN
- Внедрение Spoke-and-Spoke IPsec VPNs с использованием Cisco IOS FlexVPN
- Лабораторная работа: Осуществление безопасного подключения к сети Site-to-Site
- с помощью Cisco IOS FlexVPN
- Лабораторная работа: Осуществление безопасного подключения к сети Hub-to-Spoke

- Лабораторная работа: Осуществление безопасного подключения к сети Spoke-to-Spoke
- с помощью Cisco IOS Flex VPN

Модуль 4. Внедрение AnyConnect VPN для удаленного доступа

- Обзор бесклиентских SSL VPN
- Внедрение базовых решений по бесклиентским SSL VPN
- Внедрение механизмов доступ к приложениям в бесклиентских SSL VPN
- Внедрение расширенной аутентификации в бесклиентских SSL VPN
- Лабораторная работа: Реализация базовой бесклиентской SSL VPN на ASA
- Лабораторная работа: Доступ к приложениям через бесклиентский SSL
- Лабораторная работа: Расширенное использование AAA для бесклиентского SSL

Модуль 5. Внедрение Cisco AnyConnect VPN

- Обзор Cisco AnyConnect VPN
- Внедрение базовых решений Cisco AnyConnect SSL VPN на Cisco ASA
- Внедрение расширенных решений Cisco AnyConnect SSL VPN на Cisco ASA
- Внедрение Cisco AnyConnect IPsec/IKEv2 VPN
- Внедрение расширенных методов аутентификации, авторизации и учета (AAA) в Cisco
- Лабораторная работа: Реализация базовой AnyConnect SSL VPN на ASA
- Лабораторная работа: Настройка расширенных решений Cisco AnyConnect SSL VPN на Cisco AS
- Лабораторная работа: Настройка Cisco AnyConnect IPsec/IKEv2 VPN на Cisco ASA
- Лабораторная работа: Настройка расширенной аутентификации для Cisco AnyConnect SSL VPN н

Модуль 6. Обеспечение безопасности оконечных устройств и политик динамического доступа

- Реализация сканирования узлов
- Реализация DAP для SSL VPN
- Лабораторная работа: Настройка Hostscan и DAP для AnyConect SSL VPN

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.

<u>Промежуточная аттестация:</u>

Практическая работа (выполнение заданий**):**

№п/п	***Тематика практического занятия***	***Форма ПА***
Модуль 2.	• Лабораторная работа: Осуществление безопасного соединения Site-to-Site на Cisco ASA • Лабораторная работа: Развертывание Cisco IOS Static VTI Point-to-Point туннелей • Лабораторная работа: Реализация DMVPN	Лабораторная работа
Модуль 3.	• Лабораторная работа: Осуществление безопасного подключения к сети Site-to-Site с помощью Cisco IOS FlexVPN • Лабораторная работа: Осуществление безопасного подключения к сети Hub-to-Spoke с помощью Cisco IOS Flex VPN	Лабораторная работа

	• Лабораторная работа: Осуществление безопасного подключения к сети Spoke-to-Spoke с помощью Cisco IOS Flex VPN	
Модуль 4.	• Лабораторная работа: Реализация базовой бесклиентской SSL VPN на ASA • Лабораторная работа: Доступ к приложениям через бесклиентский SSL • Лабораторная работа: Расширенное использование AAA для бесклиентского SSL	Лабораторная работа
Модуль 5.	• Лабораторная работа: Реализация базовой AnyConnect SSL VPN на ASA • Лабораторная работа: Настройка расширенных решений Cisco AnyConnect SSL VPN на Cisco ASA • Лабораторная работа: Настройка Cisco AnyConnect IPsec/IKEv2 VPN на Cisco ASA • Лабораторная работа: Настройка расширенной аутентификации для Cisco AnyConnect SSL VPN на Cisco ASA	Лабораторная работа
Модуль 6.	• Лабораторная работа: Настройка Hostscan и DAP для AnyConect SSL VPN	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