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/
«02» июня 2018 года

Дополнительная профессиональная программа повышения квалификации

«Тактическая периметровая защита предприятия»

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. Отключение интернета в офисе практически наверняка означает сбой в работе всей компании. Несмотря на все плюсы, доступ к возможностям Всемирной паутины имеет и обратную сторону – необходимость защиты корпоративной сети предприятия от различных угроз: вирусных атак, утечек информации и т.д. Обеспечить сетевую безопасность компании вам поможет построение системы тактической периметровой защиты.

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.

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 проводить выбор исходных данных для проектирования	ПК-4
2	Способность 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 планировать, настраивать и обеспечивать требуемый уровень безопасности в сетях Microsoft Windows Server, Cisco и Unix
- Как настраивать защиту сети на маршрутизаторах с помощью списков контроля доступа и техник укрепления маршрутизаторов, проектировать и настраивать файерволлы, внедрять безопасность IP (IPSec) и VPN, проектировать и настраивать систему обнаружения вторжения (IDS)

После окончания обучения Слушатель будет уметь:

- Описать ключевые вопросы построения периметровой системы защиты
- Описать расширенные концепции стека протоколов TCP/IP
- Настраивать защиту сети на маршрутизаторах, с помощью списков контроля доступа и техник укрепления маршрутизаторов
- Проектировать и настраивать фаерволлы
- Внедрять безопасность IP (IPSec) и VPN
- Проектировать и настраивать систему обнаружения вторжения (IDS)
- Защищать беспроводные сети посредством использования систем шифрования

Учебный план:

Категория слушателей: для системных администраторов и инженеров, которые имеют опыт установки и использования решений на базе Microsoft Windows Server и хотят повысить свою квалификацию в области настройки системы безопасности.

Требования к предварительной подготовке:
M20411 Администрирование Windows Server 2012, или курса Межсетевое взаимодействие в сетях на базе TCP/IP, или эквивалентная подготовка.
Курс 10967A: Основы инфраструктуры Windows Server 2012 или эквивалентная подготовка

Срок обучения: 40 академических часов, в том числе 40 аудиторных

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.

№ 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 защиты сети**	2	2	1	1		Практическая работа
2	**Модуль 2. Изучение TCP/IP**	6	6	3	3		Практическая работа
3	**Модуль 3. Маршрутизаторы и списки контроля доступа**	6	6	3	3		Практическая работа
4	**Модуль 4. Проектирование фаерволлов**	2	2	1	1		Практическая работа
5	**Модуль 5. Настройка фаерволлов**	4	4	2	2		Практическая работа
6	**Модуль 6. Применение IPSec и VPN**	4	4	2	2		Практическая работа
7	**Модуль 7. Проектирование системы обнаружения вторжения (IDS)**	2	2	1	1		Практическая работа
8	**Модуль 8. Настройка IDS**	6	6	3	3		Практическая работа
9	**Модуль 9. Защита беспроводных сетей**	8	8	4	4		Практическая работа
		40	40	20	20		
	Итоговая аттестация	Практическая работа					

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.

[1] ПА – промежуточная аттестация.

Неделя обучения /день недели	1	2	3	4	5	6	7	Итого часов
	пн	вт	ср	чт	пт	сб	вс	
1 неделя	2	-	4	-	4	-	-	10
СРС	0	-	0	-	0	-	-	0
2 неделя	2	-	4	-	4	-	-	10
СРС	0	-	0	-	0	-	-	0
3 неделя	2	-	4	-	4	-	-	10
СРС	0	-	0	-	0	-	-	0
4 неделя	2	-	4	-	4ИА	-	-	10
СРС	0	-	0	-	0	-	-	0
Итого:	8	-	16	-	16			40
Примечание: ИА – Итоговая аттестация								

2. Рабочие программы учебных предметов

Модуль 1. Основы защиты сети

- Обзор защиты сети
- Технологии защиты сети
- Цели управления доступом
- Влияние уровневой защиты на работу сети
- Концепции сетевого аудита
- **Практическая работа:** Изучение основ защиты сети

Модуль 2. Изучение TCP/IP

- Ключевые концепции TCP/IP
- Анализ сеансов TCP
- Анализ IP пакета
- Анализ сообщений ICMP
- Анализ заголовков TCP
- Анализ заголовков UDP
- Анализ фрагментации пакетов
- Анализ целого сеанса
- **Практическая работа:** Исследование структуры TCP/IP пакетов с помощью Wireshark

Модуль 3. Маршрутизаторы и списки контроля доступа

- Настройка основной безопасности маршрутизаторов
- Принципы маршрутизации
- Удаление неиспользуемых протоколов и служб
- Создание списков контроля доступа
- Применение списков контроля доступа
- Концепции ведения журналов
- **Практическая работа:** Администрирование и настройка мер безопасности на маршрутизаторах Cisco

Модуль 4. Проектирование фаерволлов

- Основные принципы проектирования и реализации фаерволлов
- Создание политики фаерволлов
- Создание набора правил для фильтрации пакетов
- Функции прокси-сервера
- Бастионные хосты
- Функции honeypot в сетевом окружении
- **Практическая работа:** Изучение вариантов применения фаерволлов

Модуль 5. Настройка фаерволлов

- Основные функции и общие методы применения фаерволлов
- Настройка и мониторинг фаерволлов Microsoft
- Концепции IP таблиц
- Настройка iptables в Linux
- Применение технологий фаерволлов
- **Практическая работа:** Конфигурирование правил ISA и iptables

Модуль 6. Применение IPSec и VPN

- Функции IPSec
- Управление политиками IPSec
- Настройка IPSec в режиме AH
- Комбинирование AH и ESP в IPSec
- Основы VPN
- Туннельные протоколы
- Проектирование и архитектура VPN
- Безопасность VPN
- Настройка VPN на Windows Server
- **Практическая работа:** Реализация шифрования и подписывания трафика с помощью IPSec

Модуль 7. Проектирование системы обнаружения вторжения (IDS)

- Цели IDS
- Технологии и техники обнаружения вторжений
- Обнаружение вторжения на уровне хостов
- Обнаружение вторжения на уровне сети
- Принципы анализа данных для обнаружения вторжения
- Использование IDS
- Чего не может IDS
- **Практическая работа:** Изучение вариантов применения систем обнаружения вторжений

Модуль 8. Настройка IDS

- Принципы работы Snort
- Установка Snort
- Правила Snort
- Настройка Snort на использование базы данных
- Настройка IDS под Linux

- **Практическая работа:** Настройка и тестирование системы обнаружения вторжений Snort

Модуль 9. Защита беспроводных сетей

- Основы беспроводной связи
- Основы беспроводных сетей (WLAN)
- Безопасность беспроводных сетей
- Аудит беспроводных сетей
- Доверенные беспроводные сети
- **Практическая работа:** Захват, анализ и защита трафика беспроводной сети

4. 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.

5. 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 1	**Практическая работа:** Изучение основ защиты сети	Практическая работа
Модуль 2	**Практическая работа:** Исследование структуры TCP/IP пакетов с помощью Wireshark	Практическая работа
Модуль 3	**Практическая работа:** Администрирование и настройка мер безопасности на маршрутизаторах Cisco	Практическая работа
Модуль 4	**Практическая работа:** Изучение вариантов применения фаерволлов	Практическая работа
Модуль 5	**Практическая работа:** Конфигурирование правил ISA и iptables	Практическая работа
Модуль 6	**Практическая работа:** Реализация шифрования и подписывания трафика с помощью IPSec	Практическая работа
Модуль 7	**Практическая работа:** Изучение вариантов применения систем обнаружения вторжений	Практическая работа
Модуль 8	**Практическая работа:** Настройка и тестирование системы обнаружения вторжений Snort	Практическая работа
Модуль 9	**Практическая работа:** Захват, анализ и защита трафика беспроводной сети	Практическая работа

Итоговая аттестация по курсу:

Практическая работа «Захват, анализ и защита трафика беспроводной сети»