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/
«02» июня 2018 года

Дополнительная профессиональная программа повышения квалификации

«Стратегическая защита инфраструктуры 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. Корпоративная сеть любой современной компании тесно интегрирована с интернетом. Почтовый и файловые серверы, интернет-шлюзы, виртуальные среды – благодаря возможностям Сети передача данных друг другу, совместная и удаленная работа стали намного удобней и быстрей. Однако конфиденциальную информацию вашей организации могут перехватить и злоумышленники, а значит, что каждое из звеньев локальной сети предприятия нуждается в грамотной защите.

Каждый модуль программы включает практическую работу по изученным темам: это позволит слушателям закрепить пройденный материал. После окончания учебы вы сможете компетентно оценить уровень сетевой безопасности вашей компании и исправить существующие недочеты, вооружившись знаниями, полученными от преподавателя-профессионала.

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:

- Что и как нужно сделать, чтобы обеспечить нормальную работу организации и предотвратить ущерб от атак на корпоративную сеть
- Как шифровать ценные сведения с помощью CrypTool, и изучите способы укрепления защиты компьютеров с операционными системами Windows и Linux
- Как защищать серверы DNS и Web, выполнять анализ рисков, создавать политики безопасности и анализировать сигнатуры пакетов.
- Основные инструменты взломщиков – от вирусов до социальной инженерии

После окончания обучения Слушатель будет уметь:

- Описать ключевые моменты криптографии
- Настраивать безопасность компьютеров под управлением SuSe Linux Server
- Настраивать безопасность компьютеров под управлением Windows Server
- Использовать техники хакерских атак
- Исследовать защищенность Web-серверов
- Защищать серверы DNS и Web
- Выполнять анализ рисков
- Создавать политики безопасности
- Анализировать сигнатуры пакетов

Учебный план:

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

Требования к предварительной подготовке:
Тактическая периметровая защита предприятия или эквивалентная подготовка.
Английский язык для IT специалистов (elementary) 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. Криптография и защита данных**	8	8	4	4		Практическая работа
2	**Модуль 2. Укрепление компьютеров работающих под Linux**	8	8	4	4		Практическая работа
3	**Модуль 3. Укрепление Windows Server**	8	8	4	4		Практическая работа
4	**Модуль 4. Техники атаки**	4	4	2	2		Практическая работа
5	**Модуль 5. Защита в Интернете и WWW**	5	5	3	2		Практическая работа
6	**Модуль 6. Анализ рисков**	2	2	1	1		Практическая работа
7	**Модуль 7. Создание политики безопасности**	2	2	1	1		Практическая работа
8	**Модуль 8. Анализ подписей пакетов**	3	3	2	1		Практическая работа
		40	40	21	19		
	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.

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

[1] ПА – промежуточная аттестация.

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. Криптография и защита данных

- История криптографии
- Математические функции в криптографии
- Обмен закрытыми ключами
- Обмен открытыми ключами
- Аутентификация
- **Практическая работа:** Изучение алгоритмов шифрования с помощью CrypTool

Модуль 2. Укрепление компьютеров работающих под Linux

- Основы администрирования Linux
- Процесс администрирования в Linux
- Управление пользователями и защитой файловой системы
- Настройка безопасности сетевых интерфейсов
- Создание и защита скриптов для Linux
- Средства безопасности Linux
- **Практическая работа:** Применение мер безопасности в Suse Linux Enterprise Server

Модуль 3. Укрепление Windows Server

- Концепции защиты инфраструктуры Windows Server
- Основы аутентификации в Windows
- Средства настройки безопасности Windows
- Защита ресурсов Windows
- Настройка аудита и ведение журналов в Windows
- Настройка шифрующей файловой системы (EFS)
- Методы защиты сетей Windows
- **Практическая работа:** Применение мер безопасности Windows Server

Модуль 4. Техники атаки

- Рекогносцировка сети
- Создание карты сети
- Определение рабочих станций сети
- Сканирование сети
- Сканирование уязвимостей
- Вирусы, черви и троянские кони
- Получение контроля над системой

- Запись нажатий клавиш
- Взлом зашифрованных паролей
- Раскрытие скрытых паролей
- Социальная инженерия
- Получение несанкционированного доступа
- Сокрытие атаки
- Проведение DoS атаки
- **Практическая работа:** Применение атакующих техник в лабораторном окружении

Модуль 5. Защита в Интернете и WWW

- Основные компоненты Интернета
- Защита DNS серверов
- Идентификация техник Web-атак
- Методы атак на пользователей Интернет
- **Практическая работа:** Настройка безопасности серверов DNS, IIS, Apache

Модуль 6. Анализ рисков

- Концепции анализа рисков
- Методы анализа рисков
- Процесс анализа рисков
- Техники сведения рисков к минимуму
- Непрерывная оценка рисков
- **Практическая работа:** Анализ рисков компании ABC

Модуль 7. Создание политики безопасности

- Концепции политик безопасности
- Стандарты проектирования политики безопасности
- Содержание политики
- Пример политики
- Реагирование на инциденты и эскалация
- Политики коммуникаций со стратегическими партнерами
- **Практическая работа:** Создание политики безопасности компании ABC

Модуль 8. Анализ подписей пакетов

- Концепции анализа сигнатур пакетов TCP/IP
- Общие уязвимости и раскрытия (CVE)
- Концепции основных сигнатур злонамеренного трафика
- Сигнатуры нормального трафика
- Сигнатуры не нормального трафика
- **Практическая работа:** Исследование сигнатур пакетов Snort

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 алгоритмов шифрования с помощью CrypTool	Практическая работа
Модуль 2	**Практическая работа:** Применение мер безопасности в Suse Linux Enterprise Server	Практическая работа

Модуль 3	**Практическая работа:** Применение мер безопасности Windows Server	Практическая работа
Модуль 4	**Практическая работа:** Применение атакующих техник в лабораторном окружении	Практическая работа
Модуль 5	**Практическая работа:** Настройка безопасности серверов DNS, IIS, Apache	Практическая работа
Модуль 6	**Практическая работа:** Анализ рисков компании ABC	Практическая работа
Модуль 7	**Практическая работа:** Создание политики безопасности компании ABC	Практическая работа
Модуль 8	**Практическая работа:** Исследование сигнатур пакетов Snort	Практическая работа

Итоговая аттестация по курсу:

Практическая работа «Исследование сигнатур пакетов Snort»