

**ОБРАЗОВАТЕЛЬНОЕ ЧАСТНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО
ОБРАЗОВАНИЯ "ЦЕНТР ОБУЧЕНИЯ "СПЕЦИАЛИСТ" УНЦ ПРИ
МГТУ ИМ. Н.Э. БАУМАНА
(ОЧУ ДПО «СПЕЦИАЛИСТ»)**

123317, г. Москва, Пресненская набережная, д 8, стр. 1, этаж 48, помещение 484с, комната 3,
ИНН 7701168244, ОГРН 1127799002990

Утверждаю:

Директор ОЧУ ДПО «Специалист»



/И.Д. Козьярский/

« 1 » августа 2016 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.

1. Цель программы:

В результате прохождения обучения слушатель должен приобрести теоретические знания и практические навыки, необходимые для защиты инфраструктуры сетей Microsoft, Linux.

Планируемый результат обучения:

Лица, успешно освоившие программу, должны овладеть следующими компетенциями:
Умение планировать, настраивать и обеспечивать требуемый уровень безопасности в сетях Microsoft Windows Server и UNIX.

После окончания обучения Слушатель будет знать:

- Как описать ключевые моменты криптографии
- Как настраивать безопасность компьютеров под управлением SuSe Linux Server
- Как настраивать безопасность компьютеров под управлением Windows Server

После окончания обучения Слушатель будет уметь:

- Использовать техники хакерских атак
- Исследовать защищенность Web-серверов
- Защищать серверы DNS и Web
- Выполнять анализ рисков
- Создавать политики безопасности
- Анализировать сигнатуры пакетов

2. Учебный план:

Категория слушателей: ИТ-специалисты крупных и средних предприятий, которые желают получить знания и опыт работы с современными средствами виртуализации серверов на базе технологий компании VMware и новейшего продукта VMware vSphere 6.

Требования к предварительной подготовке:

1. Успешное окончание курса «Тактическая периметровая защита предприятия», или эквивалентная подготовка.
2. Успешное окончание курса «Английский язык для IT специалистов (elementary)», или эквивалентная подготовка.

Срок обучения: 40 академических часов.

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)	В том числе	
			Лекций	Практических занятий
1	Криптография и защита данных	8	4	2
2	Укрепление компьютеров работающих под Linux	8	4	2
3	Укрепление Windows Server	8	4	2
4	Техники атаки	4	3	1
5	Защита в Интернете и WWW	5	4	1
6	Анализ рисков	2	1	1
7	Создание политики безопасности	2	1	1
8	Анализ подписей пакетов	3	2	1
	Итого	40	29	11

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

3. 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	8	8	8	8	8	-	-	40
Итого:								40

4. Рабочие программы учебных предметов

В курсе рассматриваются следующие вопросы:

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
- Соккрытие 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

5. 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.

6. 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.

Конкретные формы и процедуры текущего контроля успеваемости, промежуточной аттестации и итоговой аттестации слушателей устанавливаются образовательной организацией самостоятельно.

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.

Итоговая аттестация проводится по форме тестирования в соответствии с учебным планом.