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/
«03» июня 2018 года

Дополнительная профессиональная программа повышения квалификации

«KL 031.30 Kaspersky Security для виртуальных сред. Легкий агент»

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. На курсе Слушатели изучат, как оптимально провести внедрение, настроить и обслуживать защиту, оптимизировать параметры виртуальных систем.

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.

Предоставить слушателям знания и навыки, необходимые для настройки безопасности ИТ-инфраструктуры. В курсе рассказывается о значимости настроек безопасности и демонстрируются средства защиты. Вы изучите продукт, который способен защитить виртуальные машины на базе трех самых популярных гипервизоров: VMware vSphere, Microsoft Hyper-V, Citrix XenServer.

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:

- структуру и принципы работы Kaspersky Security для виртуальных сред 3.0. Легкий агент
- процесс развертывания серверов защиты и управления
- основные настройки и инструменты по мониторингу защиты

После окончания обучения Слушатель будет уметь:

- описывать возможности Kaspersky Security для виртуальных сред. Легкий агент и излагать его преимущества по сравнению с классической защитой и безагентским решением;
- проектировать и внедрять оптимальную защиту виртуальной среды;
- поддерживать внедренную систему защиты.

Учебный план:

Категория слушателей: для IT-специалистов и компаний, которые занимаются безопасностью и используют виртуальные среды. Также курс позволяет подготовиться к сдаче экзамена KLE 031.30: Kaspersky Security для виртуальных сред. Легкий агент.

Требования к предварительной подготовке:
KL - 002.10 Kaspersky Endpoint Security and Management. Базовый курс или эквивалентная подготовка.

Срок обучения: 16 академических часов, в том числе 8 аудиторных, 8 самостоятельно (СРС).

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.

№	Наименование модулей	Обща	Всег	В том числе	СРС	Форм

п/п	по программе	я трудоемкость (акад. часов)	о ауд. ч	Лекций	Практ занятий	,ч	а ПА[1]
1	**Модуль 1. Введение**	3	1	1		2	
2	**Модуль 2. Внедрение**	5	3	2	1	2	Лабораторная работа
3	**Модуль 3. Управление**	5	3	2	1	2	Лабораторная работа
4	**Модуль 4. Масштабирование и сопровождение**	3	1	1		2	Лабораторная работа
		16	8	6	2	8	
	Итоговая аттестация	Лабораторная 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	4	0	4ИА	0	-	-	-	8
СРС	4	0	4	0	-	-	-	8
Итого:	8	0	8	0	-	-	-	16
Примечание: ИА – Итоговая аттестация								

[1] ПА – промежуточная аттестация.

2. Рабочие программы учебных предметов

Модуль 1. Введение
В этом модуле объясняется принцип виртуализации и защиты виртуальных машин. Рассматривается архитектура и принцип работы Kaspersky Security для виртуальных сред 3.0. Легкий агент

Темы:

- **Виртуализация**
  - Гипервизоры
  - Полная виртуализация и паравиртуализация
  - Платформы виртуализации
- **Защита виртуальных машин**
- **Структура и принципы работы Kaspersky Security для виртуальных сред 3.0. Легкий агент**
  - Сервер защиты
  - Легкий агент
  - Распространение обновлений
  - Обнаружение Легкими агентами Серверов защиты

Модуль 2. Внедрение
В этом модуле изучаются вопросы планирования системы. Рассматривается и на практике выполняется процесс развертывания серверов защиты и управления. Реализуется внедрение легких агентов на виртуальные машины.

Темы:

- **Планирование**
- **Установка Серверов защиты**
  - Системные требования
  - Что должно быть перед установкой
  - Установка на Hyper-V и XenServer
  - Установка на VMware ESXi
  - Первоначальная настройка
- **Развертывание Легких агентов**
  - Этапы внедрения
  - Подготовка
  - Установка на постоянные машины
  - Установка на непостоянные машины
- **Лабораторная работа №1:** Подготовка к установке Сервера защиты
- **Лабораторная работа №2.** Установка Сервера защиты
- **Лабораторная работа №3**. Установка лицензии
- **Лабораторная работа №4.** Обновление
- **Лабораторная работа №5.** Обнаружение Сервера защиты в нескольких подсетях
- **Лабораторная работа №6.** Подготовка к установке Легкого агента
- **Лабораторная работа №7.** Установка Легкого агента на защищаемые узлы
- **Лабораторная работа №8.** Подготовка шаблона
- **Лабораторная работа №9.** Пересоздание виртуальных машин в VDI
- **Лабораторная работа №10.** Динамический режим для VDI

Модуль 3. Управление

В этом модуле объясняются механизмы и принципы управления средствами защиты. Изучаются основные настройки и инструменты по мониторингу защиты.

Темы:

- **Принципы управления Kaspersky Security для виртуальных сред 3.0. Легкий агент**
  - Создание структуры управляемых компьютеров
- **Настройка параметров защиты (в сравнении с Kaspersky Endpoint Security)**
  - Алгоритм проверки файлов
  - Технологии оптимизации проверки
  - Технологии проверки
  - Сравнение настроек Kaspersky Endpoint Security и Kaspersky Security для виртуальных сред
- **Мониторинг защиты**
- **Лабораторная работа №11:** Отказоустойчивость
- **Лабораторная работа №12:** Обнаружение неполадок с подключением к Серверу защиты

Модуль 4. Масштабирование и сопровождение
В этом модуле изучаются вопросы поддержки и обслуживание системы и рассматриваются возможные сценарии масштабирования системы.

Темы:

- **Масштабирование ресурсов Сервера защиты**
- **Особенности обнаружения Серверов защиты Легкими агентами**
  - Привязка к Серверу защиты
- **Особенности взаимодействия Серверов защиты с автоматической балансировкой нагрузки в кластере гипервизоров**
  - VMware vSphere
  - Microsoft Hyper-V
  - Citrix XenServer
- **Контроль устройств на виртуальных машинах**
  - Доступ к устройствам в виртуальной среде
  - Политика для RDP-клиента
  - Политика для Citrix Receiver
  - Политика VMware View Client
- **Изменение настроек подключения к Серверу защиты и удаление Сервера защиты**
  - Изменение настроек Сервера защиты
  - Удаление Сервера защиты
- **Лабораторная работа №13** (дополнительная): Контроль устройств

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.

<u>Промежуточная аттестация:</u>
Практическая работа (выполнение заданий**):**

№п/п	***Тематика практического занятия***	***Форма ПА***
Модуль 2	**Лабораторная работа №1: Подготовка к установке Сервера защиты**	Лабораторная работа
Модуль 2	**Лабораторная работа №2. Установка Сервера**	Лабораторная

	защиты	работа
Модуль 2	**Лабораторная работа №3. Установка лицензии**	Лабораторная работа
Модуль 2	**Лабораторная работа №4. Обновление**	Лабораторная работа
Модуль 2	**Лабораторная работа №5. Обнаружение Сервера защиты в нескольких подсетях**	Лабораторная работа
Модуль 2	**Лабораторная работа №6. Подготовка к установке Легкого агента**	Лабораторная работа
Модуль 2	**Лабораторная работа №7. Установка Легкого агента на защищаемые узлы**	Лабораторная работа
Модуль 2	**Лабораторная работа №8. Подготовка шаблона**	Лабораторная работа
Модуль 2	**Лабораторная работа №9. Пересоздание виртуальных машин в VDI**	Лабораторная работа
Модуль 2	**Лабораторная работа №10. Динамический режим для VDI**	Лабораторная работа
Модуль 3	**Лабораторная работа №11: Отказоустойчивость**	Лабораторная работа
Модуль 3	**Лабораторная работа №12: Обнаружение неполадок с подключением к Серверу защиты**	Лабораторная работа
Модуль 4	**Лабораторная работа №13 (дополнительная): Контроль устройств**	Лабораторная работа

Итоговая аттестация по курсу:
Лабораторная работа «**Контроль устройств»**