Бауманский учебный центр «Специалист»

Программа курса KL 005.11: Защита серверов Windows и встраиваемых систем

Код курса: **КЛ00510**

Тема	Ак. часов
Модуль 1. Введение • Основные функции Kaspersky Security для Windows Server • Системные требования Kaspersky Security для Windows Server • Компоненты защиты Kaspersky Security для Windows Server • Компоненты управления и мониторинга Kaspersky Security для Windows Server • Лицензирование • Основные функции Kaspersky Embedded Systems Security • Системные требования Kaspersky Embedded Systems Security • Компоненты защиты Kaspersky Embedded Systems Security • Компоненты управления и мониторинга Kaspersky Embedded Systems Security • Лицензирование Kaspersky Embedded Systems Security • Варианты установки Kaspersky Embedded Systems Security	**1**
Модуль 2. Внедрение • Порядок внедрения • Мастер первоначальной настройки • Список установочных пакетов • Изменение настроек инсталляционного пакета (опционально) • Создание отдельной группы для Kaspersky Security для Windows Server (опционально) • **Лабораторная работа 1.** Подготовьте сервер администрирования • Способы установки Kaspersky Security для Windows Server • Результат установки • Активация Kaspersky Security для Windows Server • **Лабораторная работа 2.** Установите Kaspersky Security для Windows Server и Kaspersky Embedded Systems Security • Установка консоли Kaspersky Security для Windows Server • **Лабораторная работа 3.** Установите консоль управления Kaspersky Security для Windows Server	**2**
Модуль 3. Настройка групповых задач • Что делать после установки Kaspersky Security для Windows Server • Задача обновления баз • Задача обновления модулей программы • Задача проверки по требованию • **Лабораторная работа 4.** Настройте обновления и проверку по требованию	**1**
Модуль 4. Защита файловой системы • **Лабораторная работа 5.** Настройте постоянную защиту • **Лабораторная работа 6.** Проверьте защиту Windows Subsystem for Linux • Защита от эксплойтов • **Лабораторная работа 7.** Проверьте защиту от эксплойтов • Защита от шифрования • Как настроить защиту от шифрования • Как настроить период блокировки недоверенного устройства • **Лабораторная работа 8.** Настройте защиту папок общего доступа • **Лабораторная работа 9.** Настройте компонент Защита от шифрования	**2**

Модуль 5. Защита от сетевых угроз • Как Kaspersky Security для Windows Server защищает от сетевых атак • Как настроить защиту от сетевых угроз • **Лабораторная работа 10.** Настройте защиту от сетевых угроз	**2**
Модуль 6. Защита служб Удаленного рабочего стола • Модель угроз для служб удаленного рабочего стола • Защита сетевого трафика: Драйверный перехват • Компоненты защиты сеансов удаленного рабочего стола • Защита сетевого трафика: Перенаправление трафика • Защита сетевого трафика: Внешний прокси • **Лабораторная работа 11.** Настройте компонент Защита трафика в режиме Драйверный перехват • **Лабораторная работа 12.** Настройте компонент Защита трафика для проверки почтового трафика • **Лабораторная работа 13.** Настройте компонент Защита трафика в режиме Внешний прокси-сервер	**2**
Модуль 7. Компоненты контроля сервера • Контроль запуска программ • **Лабораторная работа 14.** Включите Контроль запуска программ в режиме тестирования • **Лабораторная работа 15.** Переключите Контроль запуска программ в активный режим • **Лабораторная работа 16.** Создайте разрешающие правила для установочных пакетов и обновлений	**2**
Модуль 8. Контроль устройств • Для чего нужен Контроль устройств • Как настроить контроль устройств в Kaspersky Embedded Systems Security	**1**
Модуль 9. Диагностика системы • Мониторинг файловых операций • Анализ Журналов • **Лабораторная работа 17.** Настройте компоненты Диагностики системы	**1**
Модуль 10. Защита систем хранения данных • Возможности защиты систем хранения данных • Постоянная защита файлов для систем хранения данных • **Лабораторная работа 18.** Защитите хранилище на платформе NetApp Clustered Data ONTAP • Защита от шифрования для NetApp • **Лабораторная работа 19.** Настройте компонент Защита от шифрования для NetApp	**1**
Модуль 11. Дополнительные настройки • Защита общих ресурсов кластера • Управление сетевым экраном • Интеграция с SIEM • Управление приложением • Сбор диагностической информации • Наблюдение за состоянием защиты (Health Check)	**1**
Аудиторная нагрузка в классе с преподавателем	**16 ак.ч. + 16 ак.ч. самостоятельно**

По окончании обучения на курсе проводится итоговая аттестация. Аттестация проводится в виде теста на последнем занятии или на основании оценок практических работ, выполняемых во время обучения на курсе.

Контакты центра

Для частных лиц
+7 (495) 232-32-16

Для организаций
+7 (495) 780-48-44

E-mail
info@specialist.ru