Бауманский учебный центр «Специалист»

Программа курса KL 038.4.5: Kaspersky Industrial CyberSecurity. Administration

Код курса: **КЛ038**

Тема	Ак. часов
Модуль 1. Kaspersky Security Center Базовая информация о Kaspersky Security Center • Состав и архитектура Kaspersky Security Center. • Функции Kaspersky Security Center. • MMC-консоль Kaspersky Security Center. • Web-консоль Kaspersky Security Center. • Плагин управления. • Политики. • Задачи. • Установка. • Активация и обновление баз.	**3**

Модуль 2. Kaspersky Industrial CyberSecurity for Networks Развертывание Kaspersky Industrial CyberSecurity for Networks • Архитектура и принцип работы. • Подготовка к установке. • Установка. • **Лабораторная работа 1.** Установить сервер KICS for Networks. • Первоначальная настройка. • **Лабораторная работа 2.** Активировать и обновить KICS for Networks. • **Лабораторная работа 3.** Включить перехват трафика. • Интеграция с Kaspersky Security Center. Инвентаризация сети • Технологии инвентаризации. • Инвентаризация устройств. • **Лабораторная работа 4.** Включить обнаружение активности устройств. • **Лабораторная работа 5.** Включить обнаружение информации об устройствах. • **Лабораторная работа 6.** Выполнить активный опрос устройств. • Анализ промышленных протоколов. • **Лабораторная работа 7.** Включить обнаружение устройств для контроля процесса. • **Лабораторная работа 8.** Включить контроль проектов ПЛК и распознавание параметров (тегов) проектов ПЛК. • **Лабораторная работа 9.** Включить контроль команд. • **Лабораторная работа 10.** Выполнить контроль конфигурации ПЛК. • **Лабораторная работа 11.** Включить контроль параметров промышленного процесса. • Обнаружение сетевых взаимодействий. • Карта сети. • **Лабораторная работа 12.** Включить контроль целостности сети. • **Лабораторная работа 13.** Настроить карту сети. Обслуживание Kaspersky Industrial CyberSecurity for Networks • Мониторинг состояния продукта. • Отчеты. • Журналы продукта. • Хранение и ротация служебных данных. • Сбор информации для обращения в поддержку. • **Лабораторная работа 14.** Завершить настройку KICS for Networks. Интеграции Kaspersky Industrial CyberSecurity for Networks • Возможности интеграции. • Интеграция с Kaspersky Security Center. • **Лабораторная работа 15.** Настроить отображение данных из KICS for Networks в Kaspersky Security Center. • Интеграция с другими системами. • Интеграция по REST API. • Интеграция с KICS for Nodes. • **Лабораторная работа 16.** Собрать информацию о работе программы.	**7**

Модуль 3. Kaspersky Industrial CyberSecurity for Nodes Развертывание Kaspersky Industrial CyberSecurity for Nodes • Область применения KICS for Nodes. • Состав и архитектура KICS for Nodes. • Требования к оборудованию. • Комплект поставки. • Способы установки. • Порядок развертывания KICS for Nodes. • Результаты установки. • **Лабораторная работа 17.** Подготовить инфраструктуру к развертыванию KICS for Nodes. • **Лабораторная работа 18.** Развернуть Агент администрирования Kaspersky Security Center и KICS for Nodes. • Консоль управления KICS for Nodes. • **Лабораторная работа 19.** Установить Консоль управления KICS for Nodes. • **Лабораторная работа 20.** Подключить KICS for Nodes к KICS for Networks. Защита узлов промышленной сети с помощью Kaspersky Industrial CyberSecurity for Nodes • Меры, реализуемые KICS for Nodes для защиты узлов сети. • Как вредоносные программы попадают на устройства. • Что вредоносные программы делают на узлах АСУ ТП. • Типы защит KICS for Nodes. • Бессигнатурная защита. • Контроль запуска программ. • **Лабораторная работа 21.** Настроить Контроль запуска программ в KICS for Nodes для работы в неблокирующем режиме. • **Лабораторная работа 22.** Заблокировать запуск неавторизованных приложений на узлах АСУ ТП. • Контроль устройств. • Контроль Wi-Fi соединений. • Управление сетевым экраном. • Контроль технологического процесса. • Мониторинг файловых операций. • **Лабораторная работа 23.** Настроить Мониторинг файловых операций KICS for Nodes для контроля файлов АСУ ТП. • Анализ журналов. • Мониторинг доступа к реестру. • Контроль целостности ПЛК. • **Лабораторная работа 24.** Настроить проверку целостности проектов ПЛК. Интеграции Kaspersky Industrial CyberSecurity for Nodes • Передача данных в SCADA при помощи Kaspersky Security Gateway. • Интеграция с SIEM. Обслуживание Kaspersky Industrial CyberSecurity for Nodes • Настройка прав доступа к программе. • Наблюдаем за состоянием защиты (Health Check). • Сбор диагностической информации. • **Лабораторная работа 25.** Завершить настройку KICS for Nodes.	**7**

Модуль 4. Kaspersky Industrial CyberSecurity for Linux Nodes Почему Linux требует защиты • Компоненты KICS for Linux Nodes. • **Лабораторная работа 26.** Настроить Kaspersky Security Center Linux. • **Лабораторная работа 27.** Установить KICS for Linux Nodes на управляемые устройства. Как защитить устройства • Как защититься от сетевых атак? • Как защититься от вредоносного ПО? • **Лабораторная работа 28.** Настроить базовую защиту компьютера с операционной системой Linux. • **Лабораторная работа 29.** Настроить расширенную защиту сервера с операционной системой Linux. • Как укрепить компьютер. • **Лабораторная работа 30.** Работа с контролем безопасности на компьютере с ОС Linux. Управление KICS for Linux Nodes при помощи утилиты kics-control • Зачем использовать командную строку? • Как узнать статус приложения KICS for Linux Nodes? • Как управлять задачами? • Работа с событиями. • **Лабораторная работа 31.** Управление защитой с помощью kics-control. • **Лабораторная работа 32.** Управление учетными записями в Linux и администрирование устройств.	**7**
Аудиторная нагрузка в классе с преподавателем	**24 ак.ч. + 24 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