Бауманский учебный центр «Специалист»

Программа курса KL 007.1 Kaspersky NGFW

Код курса: **КЛ007**

Тема	Ак. часов
Модуль 1. Введение • Вызовы. • Решение от Kaspersky. • Принцип работы KSN.	**1**
Модуль 2. Базовая настройка NGFW	**2**
Модуль 3. Архитектура • Пакет и поток. • Межсетевой экран и App-control. • Межсетевой экран, App-control и DNS security. • Межсетевой экран, App-control и глубокий анализ трафика. • Межсетевой экран, App-control и SSL-inspection. • Общая схема обработки трафика.	**4**
Модуль 4. Модули безопасности • Сегментация и изоляция. • User awareness. • Межсетевой экран. • Deep packet inspection. • SSL-inspection. • Группы профилей безопасности. • DNS security. • Web control. • Antivirus. • IDPS. • Менеджер сессий.	**4**
Модуль 5. Модули, функции и компоненты • NAT. • Кластер. • Агенты настройки. • Агенты настройки: KLNAGENT. • Агенты настройки: KNBEagent. • Мониторинг с помощью Zabbix. • Работа с конфигурацией. • Взаимодействие с внешними системами. • Автоматическое создание правил NGFW. • Обновление. • Поиск и устранение неисправностей.	**4**
Модуль 6. Спецификации • Платформы. • Лицензии.	**1**
Модуль 7. Лабораторные работы **Лабораторная работа № 1. Развернуть управляющие и служебные системы** • Задание А: Настройте платформу OSMP	

- Задание B: Разверните оркестратор KNBE
- Задание C: Настройте оркестратор KNBE
- Задание D: Разверните службу UAWS
- Задание E: Настройте службу UAWS

Лабораторная работа № 2. Базовая настройка межсетевого экрана Kaspersky NGFW

- Задание A: Запуск всех виртуальных машин и подключение к консоли NGFW
- Задание B: Настройка и проверка сетевых параметров NGFW
- Задание C: Подключение межсетевого экрана к платформе OSMP
- Задание D: Подключение межсетевого экрана к оркестратору KNBE и службе UAWS
- Задание E: Подключение межсетевого экрана к системе мониторинга Zabbix
- Задание F: Управление сетевыми настройками NGFW
- Задание H: Создание группы управляемых устройств и перемещение NGFW в состав группы Задание L: Создание политики межсетевого экрана
- Задание G: Настройка передачи журнала сетевых соединений в KUMA OSMP
- Задание I: Создание сетевых объектов

Лабораторная работа № 3. Управление правилами фильтрации и контроль приложений

- Задание A: Создание правил фильтрации с журналированием сетевых соединений
- Задание B: Создание правила FW с детектированием сервисов

Лабораторная работа № 4. Настройка NAT

- Задание A: Настройка NAT для выхода из LAN и MGMT в WAN
- Задание B: Настройка Static NAT для отдельного сервиса

Лабораторная работа № 5. Настройка контроля приложений

- Задание A: Создайте правило для блокировки протокола SSH

Лабораторная работа № 6. Настройка контроля приложений на основе SNI

- Задание A: Создание правила для блокирования трафика приложения Telegram
- Задание B: Использование FQDN в правилах фильтрации
- Задание C: Использование доменных учетных записей и групп в правилах фильтрации

Лабораторная работа № 7. Настройка системы обнаружения и предотвращения вторжений (IDPS)

- Задание A: Предотвращение сетевого сканирования
- Задание B: Блокирование атак на основе уязвимостей

Лабораторная работа № 8. Расшифровка и инспектирование трафика TLS

- Задание A: Настройка расшифровки и инспектирование трафика TLS
- Задание B: Добавление сертификата MITM с помощью групповой политики
- Задание C: Использование исключений

Лабораторная работа № 9. Настройка фильтрации веб-приложений

- Задание A: Создание правила для блокировки доступа к Dropbox
- Задание B: Проверка работы правила блокировки

Лабораторная работа № 10. Защита от вредоносных программ и URL-адресов

- Задание A: Блокирование загрузки вредоносных программ
- Задание B: Блокирование вредоносных и потенциально опасных URL-адресов. Использование исключений

Лабораторная работа № 11. Настройка фильтрации Веб-трафика "Web control"

- Задание A: Настройка правила Web Control
- Задание B: Проверка работы Web Control

Лабораторная работа № 12. Настройка инспектирования DNS трафика • Задание A: Создание и применение профиля DNS Security к групповому профилю безопасности • Задание B: Проверка работы инспектирования, фильтрации DNS-запросов и информации о событиях DNS Security **Лабораторная работа № 13. Настройка response на алерт из KUMA** • Задание A: Настройка response на событие из KUMA • Задание B: Проверка работы алерта и плейбука, а также автоматическое создание правила межсетевого экрана **Лабораторная работа № 14. Базовая настройка протокола динамической маршрутизации BGP**	
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