

Антивирусное администрирование McAfee GroupShield

Этот курс позволит приобрести практический опыт в установке и настройке продуктов McAfee для сканирования на уровне серверов электронной почты: McAfee GroupShield 6.0 и McAfee SpamKiller 2.1. С помощью детальных лабораторных работ слушатели курса научатся развертывать и администрировать данные продукты, обеспечивая защиту сети от вирусов, распространяющихся по электронной почте, других потенциальных угроз и спама.



Необходимые навыки

Практические знания в области сетевых технологий, а также общее понимание серверных операционных систем Windows, приложений Microsoft Exchange 2000 и 2003.

Лабораторные работы

Все темы сопровождаются лабораторными упражнениями, специально разработанными для увеличения отдачи от курса. Лабораторные работы в классе предоставляют основной практический опыт, необходимый для установки, настройки и управления антивирусными продуктами McAfee.

Материалы курса

- Учебное пособие

Продолжительность

- 2 дня

После прохождения курса слушатели смогут

- Определять, как вирусы могут воздействовать на сеть, проходя через сервер электронной почты или шлюз
- Понимать важность многоуровневой системы защиты
- Устанавливать GroupShield 6.0 для Microsoft Exchange
- Понимать, как GroupShield взаимодействует с Microsoft Exchange 2000 и 2003
- Понимать возможности GroupShield 6.0 для Microsoft Exchange
- Настраивать политики антивирусного сканирования GroupShield 6.0
- Настраивать политики контентного сканирования GroupShield 6.0
- Устанавливать и настраивать SpamKiller 2.1 для Microsoft Exchange
- Настраивать ePolicy Orchestrator для управления GroupShield 6.0 и SpamKiller 2.1
- Осуществлять поиск неисправностей GroupShield 6.0

Рекомендуемые следующие курсы

Для расширения знаний и навыков по управлению антивирусными продуктами McAfee рекомендуется пройти следующие учебные курсы:

- Защита внутренней сети: McAfee VirusScan Enterprise 8.0i и ePolicy Orchestrator 3.5 (TRN-AVD-101-TCL)
- Антивирусное администрирование McAfee WebShield (TRN-AVD-301-TCL)

Контактная информация

Associates
Телефон: +7 (095) 730 7476
E-mail: education@associates.ru

Программа курса

День первый

GroupShield Exchange

- Основы MS Exchange
- Понимание антивирусного сканирования в Microsoft Exchange
- Методы сканирования в GroupShield 6.0 для Microsoft Exchange
- Общие возможности
- Защита данных почтового ресурса и ресурса коллективной работы
- Системные требования для установки GroupShield 6.0 для Microsoft Exchange
- Методы установки GroupShield 6.0 для Microsoft Exchange
- Изменения в системе
- Сервисы GroupShield
- Поддержка, включая обновление, восстановление и удаление
- *Лабораторная работа: создание и настройка группы рассылки для администраторов*
- Возможности GroupShield 6.0
- Компоненты GroupShield 6.0
- Дополнительные модули GroupShield 6.0
- Интерфейс GroupShield: локальный, удаленный, веб-интерфейс
- Использование различных интерфейсов GroupShield
- Настройка прав доступа к интерфейсу GroupShield
- *Лабораторная работа: установка GroupShield 6.0 для Microsoft Exchange*
- *Лабораторная работа: настройка и проверка доступа к интерфейсу GroupShield*
- *Лабораторная работа: удаленный доступ к интерфейсу GroupShield*
- *Лабораторная работа: доступ к веб-интерфейсу GroupShield*
- Понятие угроз для организации
- Понятие политик GroupShield
- Настройка глобальных политик для антивируса, контентного сканирования, фильтрации файлов, шифрования, управления сканером и подписанных сообщений
- Настройка текста официальной оговорки в политиках
- Настройка фильтра по размеру сообщений
- Понятия групп правил и контентных правил
- Настройка групп правил
- Настройка контентных правил
- Назначение групп правил группам политик
- Понятие и настройка групп политик
- Настройка уведомлений в GroupShield 6.0
- *Лабораторная работа: настройка глобальных политик для антивируса, контентного сканирования, фильтрации файлов, создание группы правил, создание контентного правила*
- *Лабораторная работа: проверка глобальной политики фоновое сканирование*
- *Лабораторная работа: создание группы политик*
- *Лабораторная работа: создание политики для группы политик и ее проверка*
- Понятие и настройка параметров фоновое сканирование для VSAPI или транспортного сканирования
- Различия между VSAPI 2.0 и VSAPI 2.5
- База данных обнаружений
- Новые возможности обновления в GroupShield 6.0
- Создание сканирования по запросу в политиках GroupShield
- *Лабораторная работа: настройка обновления DAT-файлов*

Outbreak Manager и Alert Manager

- Концепция
- Правила: триггер, порог, реакция и ответное действие
- Просмотр состояния правила
- Просмотр активности эпидемии
- *Лабораторная работа: настройка набор правил Outbreak Manager*
- *Лабораторная работа: настройка политик Outbreak Manager в GroupShield 6.0*
- *Лабораторная работа: имитация эпидемии и проверка правил Outbreak Manager*

День второй

SpamKiller

- Основы SpamKiller
- Общие системные требования
- Возможности продукта
- Методы обнаружения спама
- Консоль SpamKiller и настройки
- Действия и правила SpamKiller
- Черный и белый списки
- Задачи управления
- Веб-интерфейс
- *Лабораторная работа: установка SpamKiller*
- *Лабораторная работа: настройка SpamKiller*
- *Лабораторная работа: тестирование SpamKiller*
- *Лабораторная работа: глобальный черный список*
- *Лабораторная работа: глобальный белый список*
- *Лабораторная работа: веса спама*
- *Лабораторная работа: настройка пользовательских черных и белых списков*
- *Лабораторная работа: удаление SpamKiller*

GroupShield и ePolicy Orchestrator

- Обзор установки
- Настройка GroupShield
- Добавление GroupShield в ePO
- Применение политик
- Сходства политик GroupShield и ePO
- Различия политик GroupShield и ePO
- *Лабораторная работа: добавление NAP-файлов GroupShield в ePO*
- *Лабораторная работа: развертывание агента ePO на сервере GroupShield*
- *Лабораторная работа: установка GroupShield 6.0 и SpamKiller через ePO*
- *Лабораторная работа: использование ePO для установки и применения политик GroupShield*
- *Лабораторная работа: использование ePO для установки и применения политик SpamKiller*
- *Лабораторная работа: генерация и просмотр оповещений в ePO*
- *Лабораторная работа: отчеты GroupShield в ePO*

Мониторинг и поиск неисправностей GroupShield 6.0

- Просмотр журналов
- Просмотр карантина
- Монитор производительности
- Инструменты поиска неисправностей
- Требования для обращения в техническую поддержку McAfee