Бауманский учебный центр «Специалист»

Программа курса Тактическая периметровая защита предприятия

Код курса: **ССП1**

Тема	Ак. часов
Модуль 1. Основы защиты сети • Обзор защиты сети • Технологии защиты сети • Цели управления доступом • Влияние уровневой защиты на работу сети • Концепции сетевого аудита • **Практическая работа:** Изучение основ защиты сети	**2**
Модуль 2. Изучение TCP/IP • Ключевые концепции TCP/IP • Установка Wireshark - версии 4/3/2 • Анализ сеансов TCP • Анализ IP пакета • Анализ сообщений ICMP • Анализ заголовков TCP • Анализ заголовков UDP • Анализ фрагментации пакетов • Анализ целого сеанса • **Практическая работа:** Исследование структуры TCP/IP пакетов с помощью Wireshark	**6**
Модуль 3. Маршрутизаторы и списки контроля доступа • Настройка основной безопасности маршрутизаторов • Принципы маршрутизации • Удаление неиспользуемых протоколов и служб • Создание списков контроля доступа • Применение списков контроля доступа • Концепции ведения журналов • **Практическая работа:** Администрирование и настройка мер безопасности на маршрутизаторах Cisco	**6**
Модуль 4. Проектирование межсетевых экранов • Основные принципы проектирования и реализации фаерволлов • Создание политики фаерволлов • Создание набора правил для фильтрации пакетов • Функции прокси-сервера • Бастионные хосты • Функции honeypot в сетевом окружении • **Практическая работа:** Изучение вариантов применения фаерволлов	**2**
Модуль 5. Настройка фаерволлов • Основные функции и общие методы применения фаерволлов • Настройка и мониторинг фаерволлов Microsoft • Концепции IP таблиц • Настройка iptables в Linux • Применение технологий фаерволлов • **Практическая работа:** Конфигурирование правил ISA, iptables, MikroTik	**4**

Модуль 6. Применение IPSec и VPN • Функции IPSec • Управление политиками IPSec • Настройка IPSec в режиме AH • Комбинирование AH и ESP в IPSec • Основы VPN • Туннельные протоколы • Проектирование и архитектура VPN • Безопасность VPN • Настройка VPN на Windows Server • **Практическая работа:** Реализация шифрования и подписывания трафика с помощью IPSec	**4**
Модуль 7. Проектирование системы обнаружения вторжения (IDS) • Цели IDS • Технологии и техники обнаружения вторжений • Обнаружение вторжения на уровне хостов • Обнаружение вторжения на уровне сети • Принципы анализа данных для обнаружения вторжения • Использование IDS • Чего не может IDS • **Практическая работа:** Изучение вариантов применения систем обнаружения вторжений	**2**
Модуль 8. Настройка IDS • Принципы работы Snort • Установка Snort - последняя версия, которая поддерживает интеграцию с SQL • Правила Snort • Настройка Snort на использование базы данных • Настройка IDS под Linux • **Практическая работа:** Настройка и тестирование системы обнаружения вторжений Snort	**6**
Модуль 9. Защита беспроводных сетей • Основы беспроводной связи • Основы беспроводных сетей (WLAN) • Безопасность беспроводных сетей • Аудит беспроводных сетей • Доверенные беспроводные сети • **Практическая работа:** Захват, анализ и защита трафика беспроводной сети	**8**
Аудиторная нагрузка в классе с преподавателем	**40 ак.ч. + 40 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