Бауманский учебный центр «Специалист»

Программа курса Стратегическая защита инфраструктуры предприятия

Код курса: **ССП2**

Тема	Ак. часов
Модуль 1. Криптография и защита данных • История криптографии • Математические функции в криптографии • Обмен закрытыми ключами • Обмен открытыми ключами • Аутентификация • **Практическая работа:** Изучение алгоритмов шифрования с помощью CrypTool	**8**
Модуль 2. Укрепление компьютеров работающих под Linux • Основы администрирования Linux • Процесс администрирования в Linux • Управление пользователями и защитой файловой системы • Настройка безопасности сетевых интерфейсов • Создание и защита скриптов для Linux • Средства безопасности Linux • **Практическая работа:** Применение мер безопасности в Suse Linux Enterprise Server	**8**
Модуль 3. Укрепление Windows Server • Концепции защиты инфраструктуры Windows Server • Основы аутентификации в Windows • Средства настройки безопасности Windows • Защита ресурсов Windows • Настройка аудита и ведение журналов в Windows • Настройка шифрующей файловой системы (EFS) • Методы защиты сетей Windows • **Практическая работа:** Применение мер безопасности Windows Server	**8**
Модуль 4. Техники атаки • Рекогносцировка сети • Создание карты сети • Определение рабочих станций сети • Сканирование сети • Сканирование уязвимостей • Вирусы, черви и троянские кони • Получение контроля над системой • Запись нажатий клавиш • Взлом зашифрованных паролей • Раскрытие скрытых паролей • Социальная инженерия • Получение несанкционированного доступа • Сокрытие атаки • Проведение DoS атаки • **Практическая работа:** Применение атакующих техник в лабораторном окружении	**4**

Модуль 5. Защита в Интернете и WWW • Основные компоненты Интернета • Защита DNS серверов • Идентификация техник Web-атак • Методы атак на пользователей Интернет • **Практическая работа:** Настройка безопасности серверов DNS, IIS, Apache	**5**
Модуль 6. Анализ рисков • Концепции анализа рисков • Методы анализа рисков • Процесс анализа рисков • Техники сведения рисков к минимуму • Непрерывная оценка рисков • **Практическая работа:** Анализ рисков компании ABC	**2**
Модуль 7. Создание политики безопасности • Концепции политик безопасности • Стандарты проектирования политики безопасности • Содержание политики • Пример политики • Реагирование на инциденты и эскалация • Политики коммуникаций со стратегическими партнерами • **Практическая работа:** Создание политики безопасности компании ABC	**2**
Модуль 8. Анализ подписей пакетов • Концепции анализа сигнатур пакетов TCP/IP • Общие уязвимости и раскрытия (CVE) • Концепции основных сигнатур злонамеренного трафика • Сигнатуры нормального трафика • Сигнатуры не нормального трафика • **Практическая работа:** Исследование сигнатур пакетов Snort	**3**
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