Название: **КВАЛИФИКАЦИОННЫЙ ТРЕНИНГ. ПРАКТИКА РЕШЕНИЯ ЗАДАЧ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ В УСЛОВИЯХ ВНУТРЕННИХ И ВНЕШНИХ АТАК РАЗЛИЧНЫХ КЛАССОВ**

Категория: программа повышения квалификации с выдачей удостоверения установленного законодательством РФ образца. Интенсивное практическое обучение с сочетанием учебных и реальных исходных данных и практических примеров.

Форма проведения: практические занятия в компьютерном классе

с предустановленным программным обеспечением.

Продолжительность обучения: 5 дней.

Объем учебных часов: 40 часов.

Категория обучаемых: руководители и специалисты подразделений информационной безопасности и другие категории сотрудников, связанные с защитой ИТ-инфраструктуры и корпоративной информации.
Целевая установка: поэтапное тестирование и обучение практическим навыкам защиты корпоративной ИТ-инфраструктуры и информационных ресурсов от внутренних и внешних атак различных классов.
Краткая аннотация. Уникальная программа экспресс-обучения и тестирования квалификационных навыков специалистов в области информационной безопасности, проводимая в формате киберучений, включающая решение в рамках единого игрового сценария задач создания защищенной инфраструктуры, мониторинга и выявления уязвимостей, тестирования на проникновение, оперативного изменения конфигурации системы защиты, аналитического расследования инцидентов. При решении задач используется весь спектр современных технологий и средств обеспечения информационной безопасности и управления защищенностью корпоративных компьютерных сетей.

Содержание программы:

Модуль 1. Создание защищенной ИТ-инфраструктуры для различных категорий корпоративных информационных ресурсов (8 часов).

- Формирование сегментов автоматизированной обработки информации, составляющей коммерческую тайну, персональных данных, внутрикорпоративной информации, технологических данных АСУТП и сегмента корпоративной информации, доступной из сети Интернет.

- Предоставление прав доступа пользователей к корпоративным информационным ресурсам.
- Настройка политик и конфигурирование локальных и периметровых средств защиты информации.
- Создание системы резервирования и архивирования информационных ресурсов.

Модуль 2. Формирование модели угроз корпоративным информационным ресурсам и изучение потенциальных сценариев их реализации (8 часов).

- Угрозы и сценарии нарушений политики информационной безопасности со стороны сотрудников.
- Угрозы и сценарии внешних сетевых вторжений.
- Угрозы и сценарии социальной инженерии.

Модуль 3.Мониторинг и управление безопасностью доступа к локальным и сетевым ресурсам защищенной инфраструктуры (12 часов).

- Решение задач поиска потенциально опасного кода в приложениях управления операционными и технологическими процессами и восстановление их безопасности.
- Выявлении и устранение уязвимостей различных классов.
- Решение задач обнаружения злоупотреблений пользователей и сетевых вторжений в сетях административного и технологического управления в режиме реального времени.
- Профилактика утечек «чувствительной» информации.
- Анализа корреляции событий безопасности.

Модуль 4. Расследование инцидентов информационной безопасности (8 часов).

- Решение задач выявления цифровых отпечатков реализации внутренних и внешних атак различных классов.
- Реконструкция сценария нарушений информационной безопасности.
- Формирование визуальной схемы расследования.

Модуль 5. Итоговое квалификационное испытание профессиональных навыков и умений (4 часа).

- Поддержание защищенности инфраструктуры и информационных ресурсов предприятия в условиях внутренних и внешних атак различных классов.
- Оперативное реконфигурирование защищенной инфраструктуры и средств защиты, восстановление целостности и доступности информационных ресурсов.