**Программа повышения квалификации в форме профессионального тренинга**

«КВАЛИФИКАЦИОННЫЙ ТРЕНИНГ. ПРАКТИКА РЕШЕНИЯ ЗАДАЧ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ В УСЛОВИЯХ ВНУТРЕННИХ И ВНЕШНИХ АТАК РАЗЛИЧНЫХ КЛАССОВ»

**I-й уровень**

**Целевая установка:** Поэтапное тестирование и обучение практическим навыкам защиты корпоративной ИТ-инфраструктуры и информационных ресурсов от внутренних и внешних атак различных классов.

**Категория слушателей**: Руководители и специалисты подразделений информационной безопасности и другие категории сотрудников, связанные с защитой ИТ-инфраструктуры и корпоративной информации.

**Содержание программы:**

|  |  |
| --- | --- |
| Наименование тем и учебных вопросов | Кол-во часов |
| **Модуль 1. Создание защищенной ИТ-инфраструктуры для различных категорий корпоративных информационных ресурсов.** Формирование сегментов автоматизированной обработки корпоративной информации и доступа к ресурсам сети Интернет. Предоставление прав доступа пользователей к корпоративным информационным ресурсам.  | 4 |
| **Модуль 2. Формирование модели угроз корпоративным информационным ресурсам и изучение потенциальных сценариев их реализации.** Угрозы и сценарии нарушений политики информационной безопасности со стороны сотрудников. Угрозы и сценарии внешних сетевых вторжений. Угрозы и сценарии социальной инженерии. Тестирование ИТ-инфраструктуры на проникновение. | 8 |
| **Модуль 3. Конфигурирование средств локальной и периметровой защиты ИТ-инфраструктуры и корпоративной информации.** Настройка политик и конфигурирование локальных и периметровых средств защиты информации (систем регистрации и учета, контроля целостности, антивирусной защиты, обнаружения атак, межсетевого экранирования). Создание системы резервирования и архивирования информационных ресурсов. | 12 |
| **Модуль 4. Криптографические средства защиты ИТ-инфраструктуры и корпоративной информации.** Экспресс-обзор и демонстрация на учебной ИТ-инфраструктуре возможностей современных средств криптографической защиты. Создание защищенной корпоративной телекоммуникационной системы на основе криптографических защищенных соединений с применением аппаратных и программных средств криптографической защиты. | 8 |
| **Модуль 5. Мониторинг безопасности доступа к локальным и сетевым ресурсам защищенной инфраструктуры.** Решение задач обнаружения злоупотреблений пользователей и сетевых вторжений на основе консолидированного анализа данных регистрационных журналов и применения средств анализа уязвимостей | 8 |