Программа повышения квалификации в форме профессионального тренинга

КВАЛИФИКАЦИОННЫЙ ТРЕНИНГ

«ПРАКТИКА РЕШЕНИЯ ЗАДАЧ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ В УСЛОВИЯХ ВНУТРЕННИХ И ВНЕШНИХ АТАК РАЗЛИЧНЫХ КЛАССОВ»

Целевая установка:

Поэтапное тестирование и обучение практическим навыкам управления системой обеспечения информационной безопасности предприятия в условиях внутренних и внешних атак различных классов.

Категория слушателей: руководители и специалисты подразделений информационной безопасности и другие категории сотрудников, связанные с решением задач управления защитой ИТ-инфраструктуры и корпоративной информации и успешно прошедшие обучение по программе первого уровня.

Содержание программы:

Наименование тем и учебных вопросов	Кол-во часов
Модуль 1. Закрепление навыков первого уровня на основе решения задач защиты ИТ-инфраструктуры и корпоративной информации повышенной сложности. Тестирование защищенности ИТ-инфраструктуры и корпоративной информации с использованием расширенных возможностей инструментария этичного хакинга. Создание пользовательских правил обнаружения новых уязвимостей средствами редактора скриптов систем анализа уязвимостей. Использование возможностей предпроцессоров систем обнаружения вторжений. Автоматизация сбора регистрационной информации на основе скриптов PowerShell и Bash.	8
Модуль 2. Анализ данных устройств хранения и оперативной памяти. Создание образов дисков и дампов памяти. Поиск и анализ цифровых отпечатков злоупотреблений пользователей и кибератак в дампах памяти и устройствах хранения данных.	8
Модуль 3. Практика применения DLP- и SIEM-систем, средств визуализации и инструментария OSINT при решении задач контроля информационной безопасности, выявления и расследования инцидентов. Конфигурирование DLP- и SIEM-систем, формирование эффективных политик контроля и правил корреляции событий. Поиск, визуализация и анализ данных при решении задач управления информационной безопасностью в открытых источниках.	8
Модуль 4. Расследование инцидентов информационной безопасности. Решение задач выявления цифровых отпечатков реализации внутренних и внешних атак различных классов. Реконструкция сценариев нарушения информационной безопасности. Анализ цифровых улики иной информации для доказательства причастности злоумышленников к умышленным противоправным действиям и киберпреступлениям.	8
Итоговое квалификационное испытание профессиональных навыков и умений. Поддержание защищенности инфраструктуры и информационных ресурсов в условиях внутренних и внешних атак различных классов. Сертификация выпускников второго уровня.	8