ПРОГРАММА ОБУЧЕНИЯ

по курсу «Компьютерная криминалистика»

Модуль 1. Что такое компьютерная криминалистика, ее роль в обеспечении информационной безопасности.

Модуль 2. Расследование инцидентов информационной безопасности:

- Цели расследования инцидентов информационной безопасности;
- Основные субъекты таких расследований;
- Неотложные действия после инцидента информационной безопасности;
- Последовательность действий при расследовании.

Модуль 3. Работа с лог-файлами:

- Анализ лог-файлов сетевого трафика;
- Что такое сервис whois;
- Утилита tracert;
- Какую информацию может дать провайдерская компания.

Модуль 4. Правовые основы производства экспертиз:

- Правовая регламентация производства экспертиз по гражданским и уголовным делам;
- Процессуальный статус эксперта и соблюдение норм законодательства;
- Требования к экспертному заключению;
- Допрос эксперта в суде.

Модуль 5. Производство компьютерно-технической экспертизы:

- Основное оборудование и программные средства, необходимые для производства экспертизы;
- Блокираторы записи и дубликаторы;
- Экспертные системы – Belkasoft Evidence Center, Belkasoft Acquisition Tool, Belkasoft Live RAM Capturer, Forensic Toolkit, OSForensics, FTK Imager и другие;
- Возможные виды проводимых исследований;
- Планирование экспертизы в зависимости от вопросов, сформулированных следователем.

Модуль 6. Поиск уликовой информации на компьютерах:

- Основные принципы изъятия компьютерной техники;
- В каких объектах содержится уликовая информация;
- Методы сокрытия таких данных от обнаружения.

Модуль 7. Артефакты ОС Windows:

- Исследование реестра ОС;
- Системы сбора и анализа журналов ОС;
- Корреляция событий;
- Создание и исследование Timeline.

Модуль 8. Исследование дампов оперативной памяти:

- Утилиты volatility, redline и др.

Модуль 9. Работа с системой Paraben Commander:

- Поиск информации с помощью системы Paraben Commander.

Модуль 10. Поиск сообщений электронной почты:

- Основные почтовые программы и места, где они сохраняют данные;
- Чтение почты с помощью Paraben Commander;
- Структура почтового сообщения;
- Анализ служебной информации.

Модуль 11. Работа с криптографией:

- Основные средства криптографической защиты. AES, EFS, PGP, архиваторы с шифрованием, офисные пакеты, базы данных;
- Основы поиска зашифрованных данных;
- Вскрытие защищённых данных;
- Программное обеспечение Passware Forensic Kit и ElcomSoft Password Recovery Bundle;

- Взлом хешей MD5, SHA-1, SHA-256, LM, NTLM и т.д.;
- Извлечение паролей из браузеров, программ для мгновенного обмена сообщениями и других программ.