Курс PC 5 Предотвращение и расследование киберпреступлений

г.Алматы 2017 год

В ходе изучения данного курса слушатели приобретают практические навыки поиска цифровых следов в компьютерных системах, фиксации этих следов в качестве доказательств по гражданским и уголовным делам; научатся анализировать собранные материалы с целью выявления источника атаки и восстановления работоспособности системы, а также документировать противоправные действия злоумышленников.

По окончании курса слушатели научатся:

- Определять последовательности действий при расследовании
- Правильно писать экспертное заключение
- Выявлять объекты, содержащие уличающую информацию
- Самостоятельно разбираться с хронологией событий при инциденте
- Определять различные методы сокрытия данных от обнаружения
- Выявлять все следы совершения преступления и найти виновных лиц
- Анализировать собранные материалы
- Основным принципам изъятия компьютерной техники
- Применять полученные знания на практике

Аудитория:
Специалисты, уже имеющие опыт практического использования современных технологий в сфере информационной безопасности.

Длительность обучения – 4 дня (32академических часа)
Форма обучения – аудиторные занятия
Тренеры курса: Ведущий преподаватель направлений «Информационная безопасность» города Алматы.
Стоимость курса: с одного слушателя 350 000 тг. с учетом НДС
На базе центра повышения квалификации: ТОО «ПАЦИФИКА»
Место проведения – г. Астана либо г.Алматы

В стоимость курса входит:

- Раздаточные материалы
- кофе-брейки.

Дополнительная информация по телефону: +7 (727) 334-15-74
al@pacifica.kz
Менеджер ТОО «ПАЦИФИКА», Леонтьева Анастасия

Программа курса

	Описание курса	Время
День 1	• Информация и ее роль. Основные понятия в сфере оборота информации. • Факторы угроз для информации и их классификация. • Понятие компьютерного инцидента (КИ). Некоторые примеры инцидентов. • Цели расследования инцидентов информационной безопасности. • Основные субъекты таких расследований. • Неотложные действия после инцидента информационной безопасности. • Последовательность действий при расследовании.	С 10 час. 00 мин. До 18 час. 00 мин.
День 2	• Правовая регламентация производства экспертиз по гражданским и уголовным делам. • Процессуальный статус эксперта и соблюдение норм законодательства. • Правовой статус специалиста. • Методика изъятия компьютерной техники и носителей информации. • Обеспечение доказательственного значения изъятых материалов. • Программное средство EnCase.	С 10 час. 00 мин. До 18 час. 00 мин.
День 3	• Основное оборудование и программные средства, необходимые для производства экспертизы. ▪ Блокираторы записи и дубликаторы. • В каких объектах содержится уликовая информация. ▪ Методы сокрытия таких данных от обнаружения. ▪ Исследование реестра ОС. Системы сбора и анализа журналов ОС. ▪ Корреляция событий. Создание и исследование Timeline.	С 10 час. 00 мин. До 18 час. 00 мин.
День 4	• Структура почтового сообщения. • Анализ служебной информации. • Основы поиска зашифрованных данных. • Вскрытие защищённых данных. • Программное обеспечение Passware Forensic Kit. • Программное обеспечение ElcomSoft Password Recovery Bundle. • Извлечение паролей из браузеров, программ для мгновенного обмена сообщениями и других программ. • Использование технических средств и организация поисковых мероприятий в сети Интернет.	С 10 час. 00 мин. До 18 час. 00 мин.

По окончании тренинга выдается сертификат обучающего центра.