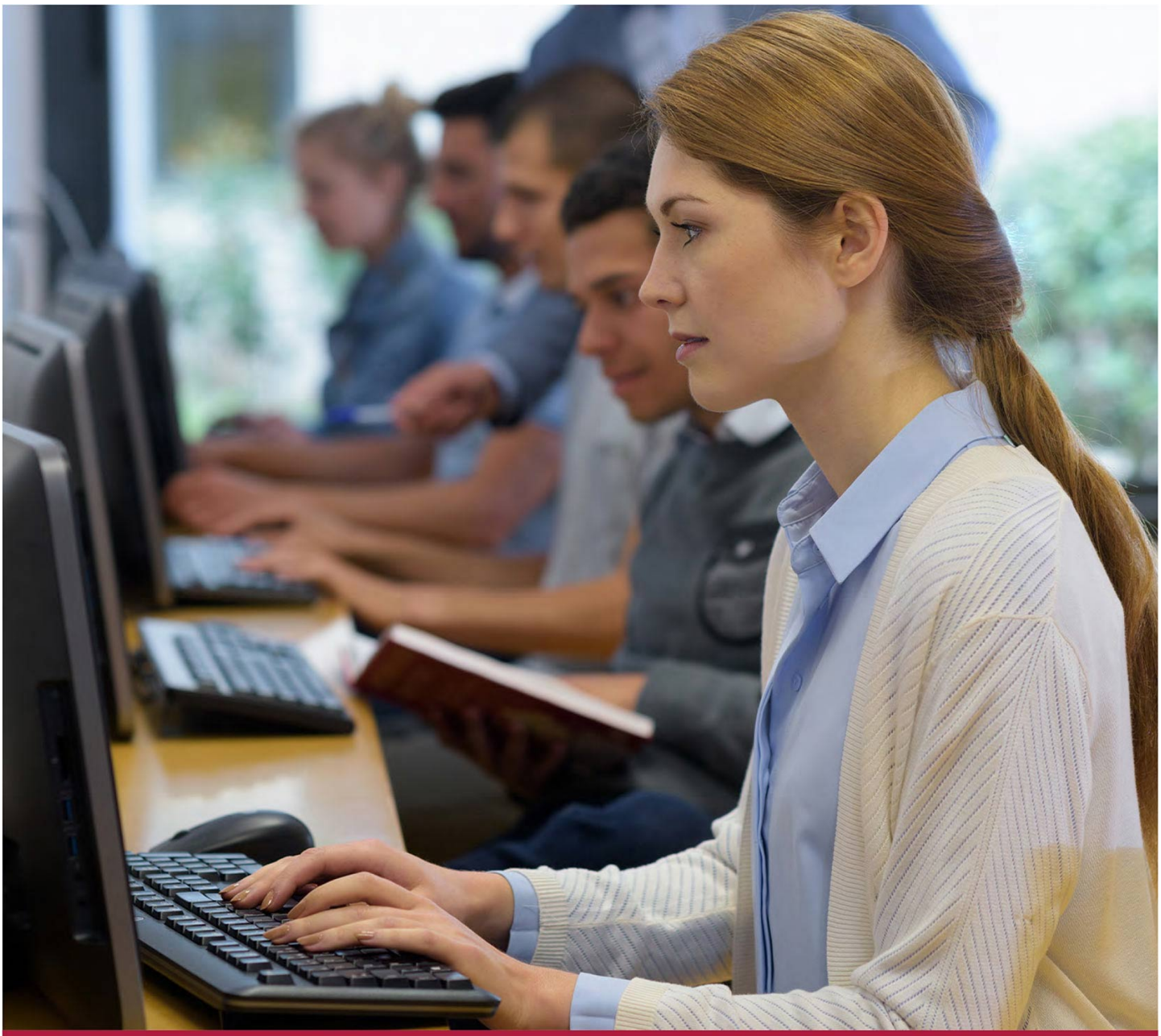
Академия АйТи
a Softline Company



Компьютерная криминалистика и расследование инцидентов информационной безопасности

Код курса: Forensica

+7 (495) 150 96 00 | academy@academyit.ru | academyit.ru

Компьютерная криминалистика и расследование инцидентов информационной безопасности

Код курса: Forensica

Длительность	40 ак. часов
Формат	
Разработчик курса	Академия АйТи
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

В данном курсе рассматривается методика производства компьютерно-технических экспертиз и расследования инцидентов информационной безопасности. В ходе изучения программы слушатель освоит правовые основы назначения и производства компьютерно-технических экспертиз, основные программные и аппаратно-программные средства исследования носителей информации.

Подробная информация

Профиль аудитории:

- сотрудники экспертно-криминалистических подразделений государственных правоохранительных органов;
- негосударственные судебные эксперты;
- специалисты негосударственных служб безопасности;
- специалисты по информационной безопасности;
- специалисты аудиторских компаний.

Предварительные требования:

- базовые знания об устройстве компьютера;
- базовые знания о носителях информации;
- базовые сведения об администрировании ОС семейства Windows и Linux.

По окончании курса слушатели изучат:

- правовые основы назначения и производства судебных компьютерно-технических экспертиз;
- основные методы обеспечения доказательственного значения проведённой экспертизы;
- аппаратную часть компьютера, идентификацию специальных типов компьютеров;
- основные программные и аппаратно-программные средства производства компьютерно-технических экспертиз;
- основные принципы осмотра объектов и изъятия компьютерного оборудования;
- практические методы доступа к зашифрованным данным;

- способы исследования мобильных телефонов и смартфонов;
- методику расследования инцидентов информационной безопасности.

Программа курса

Модуль 1 «Общие сведения о компьютерной технике»

- Устройство компьютера. Основные носители информации. Оперативная память, HDD и SSD диски. Типы материнских плат, основные разъёмы для плат расширения (ISA, PCI, PCI-E, AGP). Как определить рабочую станцию, невыделенный сервер, компьютер для майнинга, тонкого клиента и т.д.
- Операционные системы Windows и Linux. Способы хранения информации на жёстких дисках. Что такое файловая система, системы FAT, NTFS, HPFS, Ext (2-4), Btrfs. Разбиение жёсткого диска, что такое файл подкачки и swap-партиция. Что такое RAID-массив.
- Защита компьютера. Пароль на BIOS, электронные замки, шифрование жёсткого диска. Способы преодоления этих защитных мер. Получение прямого доступа к жёстким дискам и оперативной памяти.
- Сетевое оборудование. Концентраторы, коммутаторы, маршрутизаторы, беспроводные точки доступа и роутеры. Возможности доступа к этим устройствам. Использование их для негласного получения информации.
- Устройство смартфона. Системы iOS и Android. Возможность снятия информации со смартфона.

Модуль 2 «Производство компьютерно-технических экспертиз»

- Правовые основы производства экспертизы. Правовая регламентация производства экспертиз по гражданским и уголовным делам. Процессуальный статус эксперта и соблюдение норм законодательства.
- Обеспечение доказательственного значения экспертизы и основные ошибки экспертов. Требования к экспертному заключению. Допрос эксперта в суде.
- Возможные виды проводимых исследований. Планирование экспертизы в зависимости от вопросов, сформулированных следователем.

Модуль 3 «Forensica - цифровая криминалистика»

- Производство компьютерно-технической экспертизы. Основное оборудование и программные средства, необходимые для производства экспертизы. Блокираторы записи и дубликаторы. Экспертные системы.
- Исследование дампов оперативной памяти.
- Поиск уликовой информации на компьютерах. Основные принципы изъятия компьютерной техники.
- Работа с российскими экспертными системами
- Поиск сообщений электронной почты. Основные почтовые программы и где они сохраняют данные. Структура почтового сообщения. Анализ служебной информации.
- Исследование подозрительных программ. Использование сторонних сервисов для исследования. Применение результатов исследования в компьютерно-технической экспертизе.
- Работа с криптографией. Основные средства криптографической защиты. AES, EFS, PGP, архиваторы с шифрованием, офисные пакеты, базы данных. Основы поиска зашифрованных данных.

- Вскрытие защищённых данных. Специальное программное обеспечение. Извлечение паролей из браузеров, программ для мгновенного обмена сообщениями и других программ.
- Исследование мобильных телефонов. Экспертные системы. Снятие информации с телефона. Использование результатов исследования компьютера для доступа к мобильному телефону.

Модуль 4 «Расследование инцидентов информационной безопасности»

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

Модуль 5 «Аудит информационной системы на соответствие требованиям технического задания»

- Требование к техническому заданию. Конкретность. Отсутствие бланкетных положений. Минимизация отсылочных положений.
- Аудит проекта ИС на соответствие требованиям технического задания.
- Предварительное оформление процедуры приёмо-сдаточных испытаний при приёмке системы в эксплуатацию.
- Оформление условий авторского надзора и технической поддержки системы.
- Превентивные меры защиты от претензий со стороны заказчика.

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Академии АйТи

+7 (495) 150 96 00 | academy@academyit.ru