ТОО «INTELLA»
010000, г. Астана, р-н Есиль
ул. Д. Кунаева, 29/1, оф.1903
БИН 080840000052

+ 7(7172) 28 00 82
+7(727) 355 02 34
www.intella.pro
info@intella.kz

ПРИГЛАШЕНИЕ

На обучающий тренинг:

IS070 Компьютерная криминалистика. Форензика

Домен знаний:	Информационная безопасность (IS)
Сертификация:	НОУ Академия информационных систем г.Москва
Статус тренинга:	авторизованный
Длительность обучения	4 (четыре) дня (36 ак.часов)
Форма обучения	аудиторные занятия
Место проведения	На базе центра повышения квалификации: «INTELLA» г.Алматы, ул.Ауэзова, 60 БЦ “Almaty Residense” 6 этаж офис 17а тел. +7 (727) 355 02 34 г.Астана, 010000, г. Астана, р-н Есиль ул. Д. Кунаева, 29/1, оф.1903 тел. +7 (7172) 28 00 82
Даты проведения	03 - 06.04.2019 Алматы (ведется набор)
Расписание	с 10.00 до 18.00, обед с 13.00 до 14.00.
В стоимость включено:	Раздаточный материал (в электронном и печатном виде) Кофе-брейки, обеды

СПЕЦИФИКАЦИЯ

Наименование курса	Стоимость за 1 участника, тенге без НДС
IS070 Компьютерная криминалистика (36 часов)	350 000

В стоимость включено:

- Раздаточный материал (в электронном и печатном виде)
- Кофе-брейки, обеды

Аннотация тренинга

Курс представляет собой сочетание теоретических лекций, практических занятий, самостоятельного исследования и тестов по результатам исследования. Программа курса построена таким образом, что каждый новый блок информации сопровождается практикумом, позволяющим слушателям лучше усвоить новый материал и получить навыки его применения в своей трудовой деятельности. Детальный групповой анализ полученных решений при участии преподавателя позволяет слушателям выявить допущенные ошибки и избежать их в будущем.

На итоговом занятии слушатели имеют возможность выбрать реальный бизнес-кейс, максимально отражающий специфику своей работы, либо по согласованию с преподавателям предоставить собственный.

Цели курса:

На занятиях курса Вы познакомитесь с методами и средствами по реагированию на инциденты информационной безопасности, по сбору цифровых доказательств и проведения компьютерных исследований. Вы научитесь определять тип инцидента, использовать специализированное криминалистическое ПО, расследовать различные типы атак.

По окончании курса Вы сможете:

- Организовать процесс реагирование на инциденты ИБ.
- Определить тип инцидента ИБ.
- Определить перечень необходимых к изъятию носителей информации
- Осуществить сбор цифровых доказательств и задокументировать их.
- Восстанавливать удаленную информацию
- В ходе проведения исследования – восстанавливать хронологию инцидента.
- Проводить исследование различных видов компьютерных атак.

Подготовить заключение специалиста по поводу проведенного исследования компьютерной информации

Целевая аудитория:

Курс рекомендован: руководителям отделов ИБ, специалистам отделов ИБ, компьютерным криминалистам и экспертам.

Пакет слушателя

- Электронный учебник
- Организационно-распорядительные и основные нормативно-правовые акты и методические материалы, на основе которых ведется обучение, дополнительная и справочная информация по тематике курса в электронном виде.

Дополнительно

- По окончании обучения и успешного прохождения итоговой аттестации слушатель получает Удостоверение о повышении квалификации Академии Информационных Систем.

Программа тренинга:

IS070 Компьютерная криминалистика

Модуль 1. Компьютерная криминалистика

- Компьютерная криминалистика
- Лаборатория компьютерной криминалистики
- Процесс расследования компьютерных инцидентов
- Первая реакция на инцидент
- Цифровые улики
- Сбор цифровых улик в Windows
- Устройства сбора данных и дублирования
- Практикум

Модуль 2. Практическое применение специализированного ПО

- Жесткие диски и файловые системы
- Восстановление удаленных файлов и удаленных разделов
- Исследование с использованием AccessData FTK

- Исследование с использованием EnCase
- Исследование стеганографии и изображений
- Взломщики паролей
- Исследование взлома мобильных устройств
- Исследование с использованием SANS SIFT
- Восстановление хронологии событий
- Практикум

Модуль 3. Компьютерные исследования при различных типах инцидентов

- Анализ журналов сетевых подключений и корреляции событий.
- Сетевые расследования, логи и дампы сетевого трафика
- Исследование при беспроводных атаках.
- Исследование при взломе веб-серверов.
- Исследование при взломе электронной почты
- Исследование при инцидентах в системах ДБО
- Практикум

Модуль 4. Самостоятельное реагирование на инцидент и проведение компьютерного исследования

- Практикум
- Тестовое задание
- Контроль
- Вопросы по курсу

Требования для прохождения практического курса:

Наличие Ноутбука желательно.

1. На ноутбуке должен быть установлен VMwareWorkstation 9 или более поздняя версия.
2. На VMwareWorkstation должен быть развернут 64-разрядный WindowsServer 2008 (с установленным пакетом обновлений 2 или более поздним) или WindowsServer 2012.

Требования к виртуальному серверу:

***a. Процессор*:** 64-разрядный процессор IntelPentium D или выше, с частотой 2,66 ГГц или выше;

b. Оперативная память: Не менее 2 Гб доступной оперативной памяти (рекомендуется не менее 4 Гб);

c. Жесткий диск: Не менее 100 Гб доступного дискового пространства.

Последующее обучение

VULMAN Построение комплексной системы управления уязвимостями

CRYPTO Проектирование защищенных комплексных систем с использованием криптографии

IS3 Управление инцидентами информационной безопасности