ПРИГЛАШЕНИЕ

На обучающий тренинг:

IS-CRYPTO Основы криптографии. Certified Cryptography Specialist IS-CRYPTO

- **Домен знаний:** Информационная безопасность (CISSP in Deep)
- **Сертификация: Certified Cryptography Specialist IS-CRYPTO**
- **Связанные сертификации: CISSP, CISM, SSCP, CCNA/CCNP Security**
- **Тренер:** Алексей Зайончковский
- **Статус тренинг:** авторизованный
- **Длительность обучения** – 2 (два) дня 18 ак.часа
- **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** - 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

Аннотация тренинга

Концепция тренинга – это всенаправленные знания по современной криптографии на уровне её использования для решения задач информационной безопасности. Мы подготовили тренинг, который предоставит наиболее полные знания необходимые для работы и сдачи экзаменов, при этом не перегружая специалистов лишней информацией.

Основные преимущества:

1) Тренинг не привязан к какому-либо производителю
2) Материал подается в нескучном формате без лишней теории и сложной математики
3) В тренинге половина времени отводится на практику
4) Вмещает весь материал, который необходим как часть других программ обучения
5) Тренинг вмещает глубокий разбор материала домена криптография CISSP
6) Основной задачей тренинга поставлено понимание материала, а не зазубривание

Тренинг предназначен для:

Системных администраторов, аналитиков безопасности, аудиторов, менеджеров безопасности

Требование к слушателю

Знание основ информационной безопасности, знание основ сетевых технологий.

Последующее обучение

Построение сетей VPN, Microsoft PKI, другие домены информационной безопасности

По окончанию обучения

Вы приобретете знания по:

- основным алгоритмам шифрования
- методикам по безопасному обмену ключами
- методикам атак на шифры
- стандартам шифрования
- методикам стеганографии

Вы сможете:

- проектировать защищенные комплексные системы с использованием криптографии
- адекватно применять различные средства криптографической защиты для поставленных задач

ПРОГРАММА ТРЕНИНГА

iS-CRYPTO «Основы криптографии»

День первый	
Основная терминология криптографии	10.00 – 10.30
Зарождение криптографии	10.30 – 10.50
Шифр Цезаря	11.00 – 11.05
Практическая работа по зашифровке, расшифровке	11.05 – 11.20
Эра механики	11.20 – 11.40
Современная криптография	11.40 – 11.50
Применение криптографии	12.00 – 12.10
Типы шифров	12.10 – 12.30
Нулевые шифры	12.30 – 12.35
Шифры подстановки	12.35 – 12.40
Симметричное шифрование	12.40 – 12.50
Обед	13.00 – 14.00
Ассиметричное шифрование	14.00 – 14.15
Diffie-Hellmann	14.15 – 14.30
Практическая работа по безопасному обмену ключами	14.30 – 14.50
RSA	15.00 – 15.05
El Gamal	15.05 – 15.10
ECC	15.10 – 15.15
Контроль целостности	15.15 – 15.25
MD5	15.25 – 15.30
SHA-1,-3	15.30 – 15.40
HAVAL	15.40 – 15.45
RIPEMD-160	15.45 – 15.50

Цифровая подпись	16.00 – 16.20
Практическая работа по анализу шифров	16.20 – 16.40
Защищенное хранение данных	16.40 – 16.50
Защищенная передача данных	17.00 – 17.10
Использование для 3-х «китов»	17.10 – 17.25
Практическая работа по анализу использования алгоритмов шифрования	17.25 – 17.50
День 2	
Дополнительные методы применения криптографии	10.00 – 10.10
Аутентификация и контроль доступа с помощью криптографии	10.10 – 10.20
Управление ключами	10.20 – 10.40
Пара слов о PKI	10.40 – 10.50
Криптоанализ и атаки на шифры	11.00 – 11.20
Статистический анализ	11.20 – 11.30
Практическая работа – взлом шифра с помощью статистического анализа	11.30 – 11.50
Стеганография и её типы	12.00 – 12.20
Использование стеганографии для сокрытия информации	12.20 – 12.30
Практическая работа по использованию стеганографии	12.30 – 12.50
Обед	13.00 – 14.00
Обзор водных знаков	14.00 – 14.10
Обзор стандартов информационной безопасности с позиции криптографии	14.10 – 14.30
Применение средств криптографии в корпоративной среде	14.30 – 14.50
Протоколы и стандарты	15.00 – 15.20
Решения для защиты данных	15.20 – 15.50
Практическая работа – сценарий по защите корпоративной информации	16.00 – 17.30
Проверка знаний и подготовка к сдаче экзамена	17.30 – 17.50

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

- Для получения Сертификата об окончании курса требуется успешно пройти модули разделов и принять участие в опросе по курсу.
- Точное место и способ проведения тренинга уточняйте у менеджера по обучению
- При группах от 3 человек стоимость и место проведения тренинга по согласованию с Заказчиком
- Тренинги могут проводиться в г. Алматы, г. Астан, г. Москва или дистанционно

В стоимость включено:

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

Контакты:

Исполнительный директор ТОО «INTELLA» Диана Фролова df@intella.kz +7 777 552 74 22

Асель Муханмеджанова asel@pacifica.kz (Астана) + 7 (7172) 28-00-82

Татьяна Бережная tb@intella.kz (Алматы) +7 (727) 355 02 34