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

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

Курс обучения «Основы криптографии»

СПЕЦИФИКАЦИЯ

Наименование курса	Стоимость за 1 участника, тенге без НДС
Основы криптографии	100 000

- **Длительность обучения** – 2 дня (20 ак. часов)
- **Форма обучения** – аудиторные занятия на русском языке
- **Место проведения:** на базе центра повышения квалификации ТОО «INTELLA» г. Нур-Султан, р-н Есиль ул. Д. Кунаева, 29/1, оф.1903
- **Форма обучения -** аудиторные занятия
- **Расписание -** с 10.00 до 18.00, обед с 13.00 до 14.00.
- **Преподаватель:** сертифицированный тренер ТОО «ПАЦИФИКА» Игорь Савин.

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

Целевая аудитория

Тренинг предназначен для:
Системных администраторов, аналитиков безопасности, аудиторов, менеджеров безопасности

Пакет слушателя

В стоимость включено:

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

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

Контакты:

Асель Муханмеджанова asel@intella.kz (г.Алматы) +7 (727) 355 02 34
(г.Нур-Султан) +7 (7172) 28 00 82

ПРОГРАММА ТРЕНИНГА

Основы криптографии

День	Время	Тема
1 день	10.00 – 10.30	Основная терминология криптографии
	10.30 – 10.50	Зарождение криптографии
	11.00 – 11.05	Шифр Цезаря
	11.05 – 11.20	Практическая работа по зашифровке, расшифровке
	11.20 – 11.40	Эра механики
	11.40 – 11.50	Современная криптография
	12.00 – 12.10	Применение криптографии
	12.10 – 12.30	Типы шифров
	12.30 – 12.35	Нулевые шифры
	12.35 – 12.40	Шифры подстановки
	12.40 – 12.50	Симметричное шифрование
	13.00 – 14.00	Обед
	14.00 – 14.15	Ассиметричное шифрование
	14.15 – 14.30	Diffie-Hellmann
	14.30 – 14.50	Практическая работа по безопасному обмену ключами
	15.00 – 15.05	RSA
	15.05 – 15.10	El Gamal
	15.10 – 15.15	ECC
	15.15 – 15.25	Контроль целостности
	15.25 – 15.30	MD5
	15.30 – 15.40	SHA-1,-3
	15.40 – 15.45	HAVAL
	15.45 – 15.50	RIPEMD-160
	16.00 – 16.20	Цифровая подпись
	16.20 – 16.40	Практическая работа по анализу шифров
	16.40 – 16.50	Защищенное хранение данных
	17.00 – 17.10	Защищенная передача данных
	17.10 – 17.25	Использование для 3-х «китов»
	17.25 – 17.50	Практическая работа по анализу использования алгоритмов шифрования
2 день	10.00 – 10.10	Дополнительные методы применения криптографии
	10.10 – 10.20	Аутентификация и контроль доступа с помощью криптографии
	10.20 – 10.40	Управление ключами
	10.40 – 10.50	Пара слов о PKI
	11.00 – 11.20	Криптоанализ и атаки на шифры
	11.20 – 11.30	Статистический анализ
	11.30 – 11.50	Практическая работа – взлом шифра с помощью статистического анализа
	12.00 – 12.20	Стеганография и её типы
	12.20 – 12.30	Использование стеганографии для сокрытия информации
	12.30 – 12.50	Практическая работа по использованию стеганографии
	13.00 – 14.00	Обед
	14.00 – 14.10	Обзор водных знаков
	14.10 – 14.30	Обзор стандартов информационной безопасности с позиции криптографии
	14.30 – 14.50	Применение средств криптографии в корпоративной среде
	15.00 – 15.20	Протоколы и стандарты

День	Время	Тема
	15.20 – 15.50	Решения для защиты данных
	16.00 – 17.30	Практическая работа – сценарий по защите корпоративной информации
	17.30 – 17.50	Проверка знаний

- ✓ Два коротких перерыва будут предусмотрены в удобное время утром и днем.
- ✓ Один час будет предоставлен для обеденного перерыва.
- ✓ Дополнительные перерывы могут быть организованы по согласованию участников и преподавателя, при условии, что цели обучения будут выполнены.