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 00 11
www.intella.kz
info@intella.kz

ПРИГЛАШЕНИЕ

На обучающий тренинг:

IS2 Комплексное обеспечение информационной безопасности в организации (30 часов)

Тренер: Специалист ИБ Игорь Савин
Статус: Авторский курс INTELLA
Длительность обучения – 3 (три) дня + видеокурс (40 ак.часов)
Форма обучения – аудиторные занятия
На базе центра повышения квалификации: «INTELLA»
Место и даты проведения – г.Алматы 27-29 августа 2018 г. (даты могут быть подвинуты на 10 дней, по согласованию с заказчиком)
Расписание – с 10.00 до 18.00, обед с 13.00 до 14.00.

СПЕЦИФИКАЦИЯ

Наименование курса	Ед.изм	Кол-во	Стоимость, тенге без НДС
IS2 Комплексное обеспечение информационной безопасности в организации (40 часов)	чел	1	300 000
IS2 Комплексное обеспечение информационной безопасности в организации (40 часов) *При регистрации на курс до 10 августа 2018г	чел	1	270 000*

Аннотация: Несмотря на кажущуюся проработанность темы обеспечения информационной безопасности организации как системы (СУИБ), вопросов в процессе совершенствования СУИБ всегда возникает много, особенно на этапе становления компании и осознания руководством значимости этого вопроса. Основная цель создания системы управления инцидентами как основы СУИБ — объективно идентифицировать и оценить наиболее значимые для бизнеса информационные риски, а также доказать адекватность используемых средств контроля и парирования рисков для оптимизации операционных затрат.

Сегодня не вызывает сомнений необходимость финансовых вложений в обеспечение информационной безопасности бизнеса. Для достижения максимальной эффективности этих инвестиций особенно важно направить их на адекватные инструменты контроля рисков. Обосновывая вложения и представляя руководству перечень существующих рисков, важно не только просто и коротко изложить информацию на понятном для менеджмента бизнес-языке, устранив таким образом коммуникационный барьер, но и четко сформулировать причинно-следственную связь между объемами вложений и достигаемыми результатами. Построение в организации системы управления информационными инцидентами позволяет оптимизировать финансы в сфере ИБ.

Очень важно отметить, что тренинг IS2 “Комплексное обеспечение информационной безопасности в организации” не привязан к программному или аппаратному обеспечению одного производителя.

Цель курса:

Ознакомление руководителей и специалистов департаментов и отделов информационной безопасности, защиты информации, информационных технологий, кадровых и юридических служб с актуальными вопросами обеспечения информационной безопасности в организации в соответствии с требованиями законодательства, а также приобретение практических навыков защиты информационных систем.

Тренинг ориентирован на: всех IT-специалистов заинтересованных в получении минимального набора знаний и навыков по основам информационной безопасности (далее ИБ)

Предварительный уровень подготовки:

Сертификаты по начальной подготовке ИБ, или эквивалентный набор знаний и навыков 2-летний опыт администрирования гетерогенной сети (Windows\Linux\Unix)

В стоимость включено:

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

В данную стоимость НЕ ВХОДИТ перелет и проживание

Исполнительный директор ТОО «INTELLA»
Диана Фролова

Контакты: Асель Муханмеджанова asel@pacifica.kz (Астана) + 7 (7172) 28-00-82
Татьяна Бережная tb@intella.kz (Алматы) +7 (727) 355 00 11

ПРОГРАММА КУРСА

РС002 “Комплексное обеспечение информационной безопасности в организации” рассчитан на четыре дня.

ДЕНЬ1**. Основы ИБ. Угрозы и уязвимости.**

ДЕНЬ 2. **Соответствие требованиям и безопасность операций. Контроль доступа и управление учетными данными.**

ДЕНЬ 3. **Криптография. Защита приложений, данных и хостов.**

ДЕНЬ 4. **Обеспечение безопасности компьютерных сетей. Итоговый тест. 100 вопросов.**

ОБЗОР ПЕРВОГО ДНЯ:

1 день	Время	Наименование
Модуль1. Угрозы и уязвимости.		
	10 час 00 мин	Знакомство с группой Преимущества курса. Приветствие и Введение.
	10 час 30 мин	Организационное обеспечение ИБ в компании
	11 час 00 мин	Элементы и технологии защиты
	11 час 30 мин	Кофе-Брейк
	11 час 45 мин	Угрозы и уязвимости. Риски ИБ и их оценка.
	12 час 30 мин	Виды мер минимизации рисков ИБ.
	13 час 00 мин	Принципы обеспечения ИБ. Базовые механизмы системы защиты.
	14 час 00 мин	Обед
	15 час 00 мин	Типы вредоносного кода. Разнообразные виды атак.
	15 час 30 мин	Социальная инженерия. Атаки на беспроводные сети.
	16 час 00 мин	Атаки на бизнес-приложения.
	16 час 30 мин	Лабораторная работа. Анализ сценариев, выбор и реализация контрмер для минимизации рисков атак.
	18 час 00 мин	Завершение дня занятий

Лабораторная работа 1. Анализ сценариев, выбор и реализация контрмер для минимизации рисков атак.

1. Настройка и испытание системы регистрации и оперативного оповещения о событиях безопасности.
2. Минимизация поверхности атаки хоста
3. Настройка и проверка приемлемого уровня безопасности
4. Использование сканера безопасности

Тест домашнее задание 1. 20 вопросов

ОБЗОР ВТОРОГО ДНЯ:

2 день	Время	Наименование
Соответствие требованиям и безопасность операций. Контроль доступа и управление учетными данными.		
	10 час 00 мин	Приветствие и Введение

	10 час 15 мин	Источники требований к уровню ИБ в организации
	10 час 30 мин	Методологии аудита информационных систем и показатели уровня защищенности
	11 час 00 мин	Стандарты безопасности. Качественная и количественная оценка рисков.
	11 час 15 мин	Управление рисками. Виды мер минимизации рисков.
	11 час 30 мин	Кофе-Брейк
	11 час 45 мин	Административные меры. Технические меры защиты. Физические меры. Расследование инцидентов.
	12 час 30 мин	Управление непрерывностью бизнеса и восстановление после катастроф. Обязательства перед контрагентами.
	13 час 00 мин	Лабораторная работа 2. Разработка комплекса мер по обеспечению ИБ в организации.
	14 час 00 мин	Обед
	15 час 00 мин	Идентификация и система именования организации. Методы аутентификации.
	16 час 00 мин	Авторизация и модели контроля доступа. Аудит безопасности.
	16 час 30 мин	Контроль целостности системы защиты. Безопасное управление учетными данными.
	17 час 00 мин	Лабораторная работа 3. Настройка и использование механизмов контроля доступа.
	18 час 00 мин	Завершение дня занятий

Лабораторная работа 2. Разработка комплекса мер по обеспечению ИБ в организации.

1. Знакомство с типовым комплектом организационно-распорядительной документации по обеспечению ИБ
2. Расчет требуемого уровня доступности для критичной услуги автоматизированной системы и выбор комплекса мер по его обеспечению

Тест домашнее задание 2. 18 вопросов

Лабораторная работа 3. Настройка и использование механизмов контроля доступа.

1. Настройка и испытание системы аутентификации
2. Разграничение доступа к информационным ресурсам
3. Настройка подсистемы аудита и контроль целостности системы защиты
4. Реализация политики паролей

Тест домашнее задание 3. 15 вопросов

ОБЗОР ТРЕТЬЕГО ДНЯ:

3 день	Время	Наименование
Криптография. Защита приложений, данных и хостов.		
	10 час 00 мин	Вступительное слово преподавателя. Приветствие и вопросы безопасности.
	10 час 10 мин	Применение симметричной криптографии.
	11 час 00 мин	Асимметричная криптография как способ устранения недостатков симметричной.
	11 час 30 мин	Кофе-Брейк
	11 час 45 мин	Инфраструктура открытых ключей и электронные сертификаты
	13 час 00 мин	Лабораторная работа 4. Испытания средств защиты информации, использующих криптографические преобразования.
	14 час 00 мин	Обед

	15 час 00 мин	Сетевое оборудование и каналы связи. Базовые и системообразующие сетевые службы
	15 час 30 мин	Защита носителей сетевых служб. Протоколы туннелирования и удаленный доступ.
	16 час 00 мин	Система защиты периметра сети. Облачные службы
	16 час 20 мин	Кофе-Брейк
	16 час 40 мин	Лабораторная работа 8. Защита сетевой инфраструктуры
	17 час 10 мин	Итоговый тест. 100 вопросов

Криптография.

Лабораторная работа 4. Испытания средств защиты информации, использующих криптографические преобразования

1. Настройка шифрующей файловой системы в ОС Windows
2. Установка удостоверяющего центра и выдача электронного сертификата

Лабораторная работа 6. Защита сетевой инфраструктуры

1. Защита административного траффика
2. Организация безопасного удаленного доступа к сети организации

Питание входит в стоимость курса (обед, кофе-брейки)
Длительность курса: 3 дня + видеоматериал.

Пакет слушателя

- Фирменное учебное пособие.

Дополнительно

После успешной сдачи зачета выпускники получают сертификат Учебного центра

Выпускники могут получать бесплатные консультации специалистов Учебного центра по темам пройденного курса.

Последующее обучение

IS 03 «Управление инцидентами информационной безопасности»
IS 05 «Безопасность компьютерных систем и сетей на базе TCP/IP»
IS 05.2 «Технологии сетей и основы конфигурирования сетевых устройств»