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
info@intella.kz
www.intella.pro

ПРИГЛАШЕНИЕ

На обучающий тренинг:

IS4 Основы кибербезопасности

- **Тренер:** Специалист ИБ Игорь Савин
- **Статус:** Авторизованный курс Cisco Networking Academy
- **Длительность обучения** – 30 ак.часов (очно-заочная форма)
- **Форма обучения** – аудиторные занятия 2 дня (15 часов), дистанционное обучение (15 часов)
- **Место и даты проведения:** На базе центра повышения квалификации ТОО «INTELLA» (ведется набор)
  г. Алматы, ул. Ауэзова, 60, БЦ «Almaty Resdense» 6 этаж. Оф 17а
  г. Астана р-н Есиль ул. Д. Кунаева, 29/1, оф.1903
- **Расписание** – с 10.00 до 18.00, обед с 13.00 до 14.00

О курсе

Тренинг IS4 Основы кибербезопасности 1.0. разработан Cisco Networking Academy и дополнен практическими материалами INTELLA.

Цель курса

Курс «Основы кибербезопасности 1.0» готовит слушателей к более узкоспециализированным курсам по обеспечению безопасности. Этот вводный курс содержит восемь глав, в которых рассказывается о необходимости кибербезопасности, о видах инструментов, используемых для борьбы с киберугрозами, а также описываются карьерные возможности в этой области.

Тренинг ориентирован на: всех IT-специалистов заинтересованных в получении минимального набора знаний и навыков по основам кибербезопасности

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, питание и проживание

Контакты:

Диана Фролова df@intella.kz (Алматы) +7 (777) 552 74 22
(Астана) + 7 (7172) 28-00-82
Татьяна Бережная tb@intella.kz (Алматы) +7 (727) 355 02 34

IS4 Основы кибербезопасности

.

Модуль 1. Кибербезопасность. Мир мастеров, специалистов и преступников
Модуль 2. Выбор средств контроля
Модуль 3. Угрозы кибербезопасности, уязвимости системы кибербезопасности и атаки на нее
Модуль 4. Принципы криптографии
Модуль 5. Искусство обеспечения целостности данных
Модуль 6. Область применения концепции «пять девяток»
Модуль 7. Возведение укреплений

Курс Основы кибербезопасности 1.0 не имеет полного соответствия ни с одной сертификацией. Однако его содержание во многом совпадает с сертификацией CompTIA Security+, как указано в таблице.

Глава	**CompTIA Security+,**
1	Введение в кибербезопасность
	2.2. Последствия интеграции систем и данных с третьими сторонами в контексте информационной безопасности. 2.6. Особенности повышения уровня осведомленности об информационной безопасности 2.7. Ссредства обеспечения физической безопасности 3.2. Виды атак. 3.4. Виды атак на беспроводные сети. 3.7. Средства и приемы для обнаружения угроз безопасности и уязвимостей.
2	Выбор средств контроля
	2.9. Выбор средств контроля для достижения целей обеспечения информационной безопасности.
3	Угрозы кибербезопасности, уязвимости системы кибербезопасности и атаки на нее
	3.1. Виды вредоносных программ
	3.2. Виды атак
	3.3. Атаки с использованием социальной инженерии и их эффективность
	3.4. Виды атак на беспроводные сети
	3.5. Виды атак на уровне приложений
4	Принципы криптографии
	5.2. Средства управления аутентификацией, авторизацией или разграничения доступа
	6.1. Основные принципы криптографии
	6.2. Криптографические методы
5	Искусство обеспечения целостности данных
	2.9. Средства контроля для достижения целей обеспечения информационной безопасности. 6.3. Использование соответствующей инфраструктуры отрытых ключей (PKI), управление сертификатами
6	Область применения концепции «пять девяток»
	2.1. Значение понятий, связанных с риском. 2.5. Общие процедуры реагирования на нарушения безопасности 2.8. Лучшие практики управления рисками.
7	Система защиты (Возведение укреплений)
	1.1. Параметры безопасности на сетевых устройствах и других технических средствах. 1.4. Настройка общих протоколов и служб 2.4. Основные процедуры технической экспертизы 3.6. Анализ условий и выбор способов устранения угроз или средства сдерживания подходящего вида. 4.2. Суть основных понятий и технологий обеспечения информационной безопасности

	мобильных устройств. 4.3. Средства для обеспечения информационной безопасности хоста 4.4. Средства контроля для обеспечения безопасности данных 4.5. Альтернативные методы уменьшения рисков безопасности 5.3. Передовые методы установки и настройки средств контроля безопасности при управлении учетными записями 6.2. Использование криптографических методов

Пакет слушателя

- Электронный учебник
- Лабораторные работы
- Для получения свидетельства об окончании курса требуется успешно пройти модули разделов и принять участие в опросе по курсу.

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