№ 25379/IBA от 21.02.2024

Коммерческое предложение по обучению для компании ««»

По теме:

«УПРАВЛЕНИЕ КОМПЛЕКСНОЙ БЕЗОПАСНОСТЬЮ ПРЕДПРИЯТИЯ / CSO (CHIEF SECURITY OFFICER)»

От International Business Academy

2024

International Business Academy благодарит Вас за внимание к нашей компании и предлагает ознакомиться с коммерческим предложением по организации и проведению семинара

Наши конкурентные преимущества:

- **Индивидуальная разработка программ под заказ**
- **Mini ассессмент + отчет (по договорённости с клиентом)**
- **Большой выбор тренеров**
- **Персональный менеджер, курирующий проект**
- **Посттренинговая поддержка 6 месяцев**
- **Программы лояльности для постоянных клиентов**
- **Высокая репутация компании IBA и рекомендации от ведущих компаний Казахстана**
- **Обучение в рамках международных стандартов**

E-mail: info@iba.kz
Сайт: http://www.iba.kz/ Тел.: +7 (727) 328-02-02/03; Моб. тел.: +7 702 777 4411
Адрес: РК, г. Алматы ул. Жарокова 318 офис 23 (уг. проспекта Аль-Фараби)

INTERNATIONAL BUSINESS ACADEMY

УСЛОВИЯ СОТРУДНИЧЕСТВА:

ТОО «International Business Academy» приглашает Вас принять участие в обучении по теме: "Управление комплексной безопасностью предприятия / CSO (Chief Security Officer)".

Стоимость обучения: 495000 тенге без НДС (Исполнитель не является плательщиком НДС). Цена на 2025 год с учетом индексации 10% составит 544500 тенге без НДС (Исполнитель не является плательщиком НДС).

Место проведения: очно территория Поставщика/ онлайн платформа ZOOM

Даты проведения:

Онлайн:
1-5 апреля 2024
16-20 сентября 2024
9-13 декабря 2024
12-16 мая 2025
20-24 октября 2025
8-12 июня 2026
28 октября-1 ноября 2026

Продолжительность: 40 академических часов

Время: с 10:00 до 17:30.

Количество участников: 1 человек

В стоимость обучения входит: обучение, комплект эксклюзивных обучающих материалов, блокнот, ручка, сертификат International Business Academy, посттренинговая поддержка (6 месяцев), обед и 2 кофе-брейка в каждый день занятий (при условии, что обучение очное).

Просим заключить договор заранее как минимум за 1-2 месяца до начала обучения и забронировать даты с тренером.

Исполнитель: Батухтина Н.Е

E-mail: info@iba.kz
Сайт: http://www.iba.kz/ Тел.: +7 (727) 328-02-02/03; Моб. тел.: +7 702 777 4411
Адрес: РК, г. Алматы ул. Жарокова 318 офис 23 (уг. проспекта Аль-Фараби)

INTERNATIONAL BUSINESS ACADEMY

Информация о компании.

International Business Academy– это:

1. Рекомендации. Высокая репутация компании IBA и рекомендации от ведущих компаний Казахстана. Компания более 10 лет на рынке за это время зарекомендовала себя, как надежного поставщика услуг.

2. Персональный менеджер, курирующий проект. Каждый проект курирует отдельный менеджер, который закреплен за Вашей компанией

3. Лучшие эксперты. Профессиональный состав привлекаемых к процессу обучения преподавателей, успешных экспертов, консультантов, топ-менеджеров крупных корпораций.

4. Актуальность и польза. Наши программы отражают самые современные методики с учетом изменения рынка и законодательства.

5. Формат обучения. Мы предлагаем нашим клиентам несколько форматов обучения:
— Очный и Онлайн формат открытых, корпоративных и индивидуальных семинаров.

6. Пост-тренинговые анализ и поддержка в течении 6 месяцев. Мониторинг результатов тренингов в рабочем процессе, рекомендации от тренера.

7. Индивидуальный подход. Все, начиная от содержания, места и времени проведения тренингов может быть настроено в соответствии Вашим потребностями.

8. Принципиально высокий уровень сервиса. Мы создали все условия для максимального вовлечения в обучение: от удобных кресел и современного презентационного оборудования, до удобной локации.

9. Международные стандарты обучения. Обучение в рамках международных стандартов, с адаптаций под реалии казахстанского бизнеса.

ОПИСАНИЕ ПРОГРАММЫ:

1 день

Общие вопросы построения системы корпоративной безопасности

- Что такое политика (концепция) безопасности. Постановочные вопросы перед созданием системы защиты бизнеса
- Что мы будем защищать (определение объектов безопасности)
- Кто будет обеспечивать безопасность бизнеса (определение субъектов безопасности). Служба

безопасности предприятия или аутсорсинговое обслуживание. Что выбрать. Плюсы и минусы обоих вариантов
- Правовая сторона деятельности Службы безопасности предприятия. Подчинение Службы безопасности. Взаимодействие с акционерами, владельцами и руководителями бизнеса. Положение о Службе безопасности предприятия. Выстраивание взаимоотношений Службы безопасности с иными подразделениями предприятия
- От каких угроз будем защищать бизнес (внешние/внутренние, постоянные/ временные, мониторинг угроз, определение вероятности наступления, оценка возможного ущерба).
- Как будем строить систему безопасности бизнеса
- Принципы построения корпоративной безопасности
- Направления по обеспечению безопасности бизнеса
- Структура системы безопасности организации
- Критерии оценки эффективности деятельности системы обеспечения безопасности организации
- Способы проверки эффективности мер по обеспечению безопасности
- Подготовка к созданию системы безопасности
- Формирование нормативного (правового) обеспечения безопасности бизнеса. Концепция (политика) обеспечения безопасности предприятия, инструкции, регламенты и алгоритмы
- Управление корпоративной безопасностью в кризисных ситуациях. Участие службы безопасности в проведении антикризисных мероприятий
- Управленческо-организационные меры по обеспечению безопасности в условиях работы в кризисной ситуации, при угрозе нападения на организацию и террористического акта

Методика проведения аудита безопасности предприятия

- Основные понятия и виды аудита. Критерии аудита
- Организация процесса аудита. Контрольные процедуры внутреннего аудита. Профессиональная квалификация аудитора
- Методики комплексной оценки обеспечения безопасности предприятия

Система анализа и управления рисками на предприятии

- Виды экономических рисков
- Создание системы анализа и управления экономическими рисками. Участие службы безопасности в управлении экономическими рисками
- Прогнозирование рисковой ситуации. Определение источников информации, которые позволяют выявить причины риска и возможные его виды. Выяснение источников риска. Прогнозирование основных видов риска. Определение объектов, на которые воздействует тот или иной вид риска
- Процесс управления рисками
- Методы, используемые для диагностики рисков
- Идентификация рисков
- Методы расчета рисков. Сравнение количественных и качественных методов расчета
- Этапы проведения диагностики рисков
- Оценка рисков. Определение допустимых пределов риска
- Приемлемость риска. Формирование карты рисков

- Формирование отчета о рисках
- Разработка программы мероприятий по управлению рисками
- Мониторинг
- Использование риск-менеджмента при принятии решений. Необходимость использования риск-менеджмента. Особенности рассмотрения рисков при принятии решений
- Организационные аспекты управления рисками. Требования по внедрению системы управления рисками. Возможная структура управления рисками. Исполнение функции риск-менеджмента

Управление инцидентами на предприятии

- Основы инцидент-менеджмента
    - Планирование и подготовка
    - Обнаружение и оповещение о событиях безопасности
    - Оценка и принятие решений по событиям безопасности
    - Реагирование на инциденты безопасности
    - Анализ
    - Улучшение
- Организация инцидент-менеджмента в компании
    - Этапы управления инцидентами
    - Внедрение системы инцидент-менеджмента
- Взаимосвязь инцидент-менеджмента и риск-менеджмента
- Общий алгоритм действий при наступлении инцидента

2 день

Информационная безопасность

- Защита информации как составная часть общей системы безопасности организации. Понятие информационного общества. Понятие информационной безопасности. Наиболее распространенные угрозы. Основные определения и критерии классификации угроз. Основные направления защиты информации
- Уровни формирования режима ИБ. Законодательный уровень
- Административный уровень. Понятие системы менеджмента информационной безопасности. Недостатки проектного подхода к построению системы управления информационной безопасностью. Процессный подход к обеспечению информационной безопасности. Международные стандарты безопасности информационных систем. Стандарт, базирующиеся на процессном подходе к обеспечению информационной безопасности — ISO 27001. ISO 27001 и национальные нормативные документы по ИБ. Требования ISO 27001. Политика информационной безопасности как основа системы менеджмента ИБ. Цели и задачи Политики информационной безопасности. Общая структура Политики информационной безопасности. Аудит состояния информационной безопасности на предприятии. Порядок проведения аудита информационной безопасности в организации
- Программно-технический уровень. Понятие авторизации, идентификации и аутентификации пользователей. Разграничение доступа. Технологии защиты информации:

криптографические методы защиты, электронная цифровая подпись как базовый механизм обеспечения юридической силы документа при электронном документообороте и наиболее эффективное средство подтверждения авторства и подлинности электронного документа. межсетевое экранирование, VPN (виртуальная частная сеть), активный аудит (DLP-системы, вредоносное программное обеспечение и антивирусные программы)

- Службы интернета
- Социальная инженерия
- Противодействие промышленному шпионажу. Техническая защита информации.Классификация технических каналов утечки информации. Технические каналы утечки акустической информации. Защита акустической (речевой) информации. Средства и методы обнаружения технических каналов утечки информации. Мероприятия по выявлению технических каналов утечки информации. Оценка защищенности информации от утечки по ТКУИ
- Режим коммерческой тайны. Конфиденциальное делопроизводство.Понятие «коммерческой тайны» в предпринимательской деятельности. Нормативно-правовые акты РК, определяющие понятие коммерческая тайна. Порядок создания режима коммерческой тайны в организации. Составление и применение перечня сведений, составляющих коммерческую тайну организации, рекомендуемая информация, которая должна составлять коммерческую тайну организации. Процедура ограничения доступа к информации, составляющей коммерческую тайну организации. Внутренние нормативные документы, регламентирующие деятельность организации в области защиты коммерческой тайны. Изменения и дополнения, вносимые в нормативно-правовые документы организации при введении режима коммерческой тайны. Обязательство работника по сохранению коммерческой тайны организации. Соблюдение режима коммерческой тайны в договорной работе. Процедура передачи государственным органам информации, составляющей коммерческую тайну организации. Виды ответственности за разглашение коммерческой тайны, а также за незаконное получение информации
- Конфиденциальное делопроизводство — составная часть системы безопасности организации. Конфиденциальное делопроизводство как элемент режима защиты коммерческой тайны. Принципы построения конфиденциального делопроизводства. Порядок взаимодействия открытого и конфиденциального делопроизводства. Этапы создания конфиденциального делопроизводства, практические рекомендации по порядку создания
- Подразделение информационной безопасности. Какой быть структуре эффективного подразделения информационной безопасности? Место подразделения ИБ в структуре организации. Разделение функций между подразделением ИБ и IT-подразделением. Организация взаимодействия с руководством подразделения информационной безопасности и руководителями структурных IT-подразделений организации

3 день

Кадровая безопасность

- Внутренние угрозы предприятию со стороны «человеческого фактора»
- Мотивированное и немотивированное разглашение информации
- Психологические особенности сотрудников, представляющих опасность для предприятия
- Проверки кандидатов (соискателей) на работу

- Превентивные мероприятия, проводимые Службой безопасности компании по предотвращению утечки информации со стороны работников предприятия
- Различные варианты создания стимулов и мотивационных факторов, направленных на усиление лояльности работников предприятия
- «Растровые признаки опасности» у работников. На что обратить внимание в проверочных мероприятиях
- Технические средства контроля за работниками
- Тестирование (оценка) работников
- Досье работников. Правила при работе с досье
- Приём персонала на работу. Методы обеспечения безопасности при приёме персонала
- Проверка кандидата при приёме на работу
- Способы получения информации о кандидате
- Проверка сотрудника во время работы (испытательного срока)
- Безопасное увольнение работников. Угрозы при увольнении работников
- Признаки неудовлетворённости сотрудников перед увольнением
- Правила при увольнении работников
- Мероприятия, проводимые Службой безопасности при увольнении работников
- Процедура проведения внутрикорпоративной проверки (расследования) по фактам противоправных действий со стороны персонала
- Использование полиграфа (детектора лжи) при проведении внутрикорпоративных проверок (расследований). Правовая и организационная сторона вопроса. Возможно ли обмануть полиграф?
- Применение методов психозондирования при расследовании противоправных действий
- Процессуальное оформление результатов внутрикорпоративных проверок (расследований)
- Взаимодействие Службы безопасности с правоохранительными органами при расследовании противоправных действий

4 день

Экономическая безопасность

Корпоративное мошенничество. Противоправные действия

- Что такое корпоративное мошенничество? Общая характеристика и виды преступлений против собственности. Понятие и признаки мошенничества. Отличие мошенничества от иных видов преступлений против собственности. Уголовная ответственность за мошенничество
- Элементы мошенничества. Мошенники и их мотивация, психологические приемы, применяемые мошенниками
- Структура мошеннической операции, формы и сценарии мошенничества в различных видах бизнеса
- Как корпоративное мошенничество влияет на предприятие?
- Как отличить неэффективность от мошенничества?
- Цикл управления риском корпоративного мошенничества: обзор
- Стратегии управления риском мошенничества
- Предотвращение: основные мероприятия (система внутренних контролей, проверка

контрагентов и потенциальных сотрудников)
- Обнаружение: основные способы (горячая линия, отслеживание индикаторов в поведении, аналитические способы)
- Расследование: на что обратить внимание (юридическая сторона вопроса)
- Реагирование: что делать по результатам
- Какие навыки необходимы для эффективного противодействия мошенничеству
- Создание на предприятии системы предупреждения и защиты от мошеннических операций

Противодействие откатам и коммерческому подкупу в договорной работе предприятия

- Понятие «откат» и «коммерческий подкуп» в законодательстве РК, а также в обычаях делового оборота. Состав правонарушений и типовые схемы откатов
- Виды юридической ответственности за действия, классифицирующиеся как «откат» и «коммерческий подкуп». Юридические особенности увольнения работника, замешанного в откатах
- Риски откатов
- Способы вычисления откатов
- Способы предотвращения откатов через регламентацию бизнес-процессов
- Способы предотвращения откатов через безопасную кадровую политику
- Схемы избавления от неугодных работников
- Сбор и анализ информации по работникам с «откатными» рисками. Использование технических средств (видео, аудио, DLP систем) для доказательства заинтересованности в сделке и неофициальных договоренностей с контрагентом. Сбор компромата по работникам, используя информационные ресурсы Интернета. Способы легализации «оперативной» информации
- Методика тайного покупателя при оценке заинтересованности работников и объективности ценовой политики при выборе контрагента
- Создание системы «обратной связи» на предприятии. Телефоны доверия, беседы с увольняющимися сотрудниками, контакты с несостоявшимися поставщиками и иные способы получения обратной связи
- Юридическое оформление антиоткатной политики на предприятии. Включение антикоррупционных оговорок в трудовые и гражданско-правовые договора. Декларирование политики «добросовестной организации». Создание локальной нормативно-правовой базы по противодействию и профилактики откатам и коммерческому подкупу
- Введение элементов коллегиальности принятия решения в договорной работе. Организация процедур согласования и проведения конкурсных процедур при выборе контрагентов

Антикоррупционный комплаенс

- Что такое комплаенс. Виды комплаенс
- Комплаенс и безопасность: в чем разница
- Комплаенс-контроль — что это? Почему комплаенс-контроль важен для бизнеса. Два подхода к комплаенс-контролю. Инструменты комплаенс-контроля
- Комплаенс-риск. Классификация комплаенс-рисков. Типы комплаенс-рисков. Как управлять комплаенс-рисками
- Комплаенс-менеджер: функционал

- Внедрение комплаенс
- Антикоррупционный комплаенс
- Комплаенс как система эффективного управления
- ISO 37301:2021 «Системы менеджмента комплаенса — Требования и руководство по применению»
- Алгоритм действий по разработке комплаенс-программы
- Оценка коррупционных рисков
- Разработка антикоррупционных мер
- Разработка антикоррупционных локальных документов предприятия
- Реализация антикоррупционных мер

5 день

Разведка и контрразведка как инструменты снижения рисков и управления на предприятии

Базовые принципы разведки и контрразведки

- Принципы добывания информации. Промышленный шпионаж, разведка и контрразведка. Добросовестная и недобросовестная конкуренция. Разведка и контрразведка как органы безопасности. Функции и задачи разведки и контрразведки. Основные задачи разведки. Виды разведки. Способы несанкционированного доступа к конфиденциальной информации. Назначение и виды операций. Факторы успеха бизнес-разведки. Контрразведка. Основные направления контрразведки. Предмет деятельности контрразведки. Деловая разведка (ДР) противника как угроза безопасности предприятия. Задачи внешней контрразведки
- Этапы деловой разведки. Правовые и этические нормы ведения деловой разведки. Разведывательный цикл
- Постановка задачи и планирование операции. Составление плана. Создание системы деловой разведки. Структура и функции подразделения ДР. Формирование команды исполнителей
- Сбор информации. Характеристики и требования к информации. Особенности восприятия человеком информации. Ценностные характеристики информации. Источники информации. Методы сбора информации. Методы верификации информации. Информационная матрица. Информационные ресурсы для деловой разведки
- Анализ информации. Методы анализа
- Представление результатов
- Новые информационные технологии при решении задач деловой разведки

Методики определения надежности контрагентов и безопасности коммерческих предложений

- Понятие «должная осмотрительность», процедура Due Diligence
- Признаки, свидетельствующие о неблагонадежности контрагента
- Изучение контрагентов. Безопасность при договорной работе. Риски, связанные с недобросовестным партнерством
- Ключевые показатели (индикаторы) для оценки партнера
- Источники информации, используемые при изучении контрагентов

- Автоматизация процедур проверки контрагентов. Практическая работа с источниками информации
- Особенности получения информации по физическим лицам

Добывание информации «оперативными» методами (получение информации, используя «человеческий фактор»). Мотивация человека на передачу (разглашение) информации

- **Оценка личности**. Общая схема оценки личности (схема изучения личности). Оценка личности в процессе общения. Оценка личности по внешним признакам. Методы оценки личности
- **Установление и развитие психологических контактов**. Общая схема психологического контакта. Заведение знакомства (выбор предлога; формирование первого впечатления; учет перцептивных особенностей объекта; привлечение внимания). Формирование интереса (возбуждение «симпатии»; вовлечение в беседу; умение слушать). Установление доверительности (особенности доверительного общения; формирование доверительности; преодоление барьера доверительности)
- **Выведывание информации**. Психологические основы выведывания. Методика выведывания информации
- **Психологическое воздействие на личность**. Убеждение — главный метод воздействия. Метод принуждения. Метод внушения