INTERNATIONAL BUSINESS ACADEMY
www.iba.kz | info@iba.kz | +7 702 777 4411
г. Алматы ул. Шашкина 24 (БЦ K Plaza) офис 1

№ 77507/IBA от 08.11.2026

CENTRAL ASIAN ASSOCIATION FOR ACCREDITATION OF EDUCATION

International Business Academy обладает международной институциональной аккредитацией в сфере образования, подтверждающей соответствие международным стандартам качества образовательной деятельности

Коммерческое предложение для компании «»

Условия сотрудничества

«International Business Academy» приглашает Вас принять участие в обучении по теме: «Современные методики противодействия и снижение уровня рисков безопасности. Методы борьбы с мошенничеством, хищениями на предприятии. Порядок проведения внутренних проверок и расследований».

Стоимость обучения: 296500 тенге без НДС. Цена на 2027 год с учетом индексации 10% составит 326150 тенге без НДС.

*Компания ИП International Business Academy с 2026 года работает на общеустановленном режиме налогообложения с НДС.

*НДС 16% будет добавлен в счет на оплату.

Место проведения: очно территория Поставщика/ онлайн платформа ZOOM

Количество участников: 1 человек

Продолжительность обучения: 2 дня (16 академ.часов)

Даты проведения:

Алматы: 9-10 сентября 2026, 11-12 ноября 2026, 15-16 февраля 2027, 12-13 апреля 2027, 9-10 июня 2027, 9-10 августа 2027, 18-19 октября 2027, 8-9 декабря 2027, 17-18 января 2028, 20-21 марта 2028, 15-16 мая 2028, 10-11 июля 2028, 4-5 сентября 2028, 6-7 ноября 2028

Онлайн: 8-9 октября 2026, 28-29 декабря 2026, 21-22 января 2027, 18-19 марта 2027, 20-21 мая 2027, 1-2 июля 2027, 13-14 сентября 2027, 8-9 ноября 2027, 7-8 февраля 2028, 3-4 апреля 2028, 19-20 июня 2028, 21-22 августа 2028, 23-24 октября 2028, 4-5 декабря 2028

* даты требуют дополнительного согласования

Расписание: с 10:00 - 17.30

В стоимость обучения входит: обучение, комплект эксклюзивных обучающих материалов, блокнот, ручка, сертификат International Business Academy, посттренинговая поддержка (3 месяца), обед и кофе-брейк в каждый день занятий (при условии, что обучение очное).

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

Исполнитель:



Руководитель Батухтина Н.Е.

International Business Academy — обучение, ориентированное на практический результат, развитие сотрудников и рост эффективности бизнеса.

Описание программы:

1 день

Система анализа и управления экономическими рисками в компании

- Виды экономических рисков. Внешние и внутренние риски
- Создание системы анализа и управления экономическими рисками
- Методики оценки и измерения рисков
- Анализ угроз и оценка их уровня
- Мониторинг рисков. Радары и матрицы управления рисками
- Прогнозирование рисковой ситуации. Определение источников информации, которые позволяют выявить причины риска и возможные его виды. Выяснение источников риска
- Прогнозирование основных видов риска
- Применяемые методы управления экономическими рисками. Методы минимизации и методы возмещения потерь. Методы упреждения и методы уклонения от риска. Методы локализации и методы распределения риска

Защита информации как составная часть общей системы безопасности организации

- Понятие информационной безопасности. Наиболее распространенные угрозы. Основные определения и критерии классификации угроз.
- Основные направления защиты информации.
- Понятие системы менеджмента информационной безопасности. Недостатки проектного подхода к построению системы управления информационной безопасностью. Процессный подход к обеспечению информационной безопасности.
- 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 Компании.

Режим коммерческой тайны. Конфиденциальное делопроизводство

- Коммерческая тайна. Понятие «коммерческой тайны» в предпринимательской деятельности. Нормативно-правовые акты РК, определяющие понятие коммерческая тайна.
- Порядок создания режима коммерческой тайны в Компании.
- Составление и применение перечня сведений, составляющих коммерческую тайну Компании, рекомендуемая информация, которая должна составлять коммерческую тайну компании.
- Процедура ограничения доступа к информации, составляющей коммерческую тайну Компании.
- Внутренние нормативные документы, регламентирующие деятельность Компании в области защиты коммерческой тайны. Изменения и дополнения, вносимые в нормативно-правовые документы компании при введении режима коммерческой тайны.
- Обязательство работника по сохранению коммерческой тайны Компании.
- Соблюдение режима коммерческой тайны в договорной работе.
- Процедура передачи государственным органам информации, составляющей коммерческую

тайну Компании.
- Виды юридической ответственности за разглашение коммерческой тайны, а также за незаконное получение информации.
- Конфиденциальное делопроизводство — составная часть системы безопасности Компании. 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.

Информационная безопасность Компании

- Электронная цифровая подпись как базовый механизм обеспечения юридической силы документа при электронном документообороте и наиболее эффективное средство подтверждения авторства и подлинности электронного документа.
- 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 Компании.

Кадровая безопасность Компании

- Внутренние угрозы организации со стороны «человеческого фактора».
- Угрозы кадровой безопасности со стороны конкурентов и преступных формирований.
- Психологические особенности сотрудников, представляющих опасность для организации. Схема проверки кандидатов (соискателей) на работу.
- Превентивные мероприятия, проводимые Службой безопасности компании по предотвращению противоправных действий со стороны сотрудников Компании.
- Различные варианты создания стимулов и мотивационных факторов, направленных на усиление лояльности сотрудников Компании.
- Выстраивание отношений между Службой безопасности и персоналом Компании. Что эффективней — компромат или взаимопомощь?
- Создание системы персональной ответственности сотрудников Компании.
- «Растровые признаки опасности», на что обратить внимание в проверочных мероприятиях.
- Досье сотрудника. Правила при работе с досье.

2 день

Корпоративное мошенничество

- 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 Компании?
- 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

- Оценка стоимости ущерба (убытков) для предприятия при наличии «откатов» или «коммерческого подкупа»
- Методика проведение анти-откатного аудита на предприятии. Определение бизнес-процессов и должностей с откатными рисками. Анализ работы подразделения снабжения
- 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
- Вычисление личной заинтересованности работника при анализе договорной работы на предприятии. Косвенные признаки откатов при анализе взаимоотношений с контрагентами
- 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 анти-откатной и анти-мошеннической 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

Управление силами охраны на предприятии. Система видеонаблюдения

- Эффективная организация и управление службой охраны и видеонаблюдения для предотвращения несанкционированного вторжения на охраняемые объекты, предупреждение краж и других инцидентов на предприятии
- Координация действий персонала охраны и видеонаблюдения при аварийных и чрезвычайных событиях
- Координация действий службы безопасности с руководителями объектов, группой управления аварийными ситуациями, Пожарно-аварийной службой (ПАС)

Физическая защита объектов передприятия

- Методы и технологии обеспечения контроль доступа на охраняемые объекты авторизованного персонала, визитеров и автотранспорта

- Защита товарно-материальных ценностей компании от краж и вандализма
- Современные методы обеспечения физической защиты объектов предприятий уязвимых в террористическом отношении
- Элементы физической безопасности, как части совокупной системы общей безопасности: обнаружение уязвимостей и уменьшение рисков и выработка мер по противодействию потенциальным угрозам

Современные методы проведения внутренних проверок и расследований на предприятии краж ТМЦ, мошенничеств, вандализма

- Этапы подготовки отчетов по результатам внутренних проверок и расследований инцидентов
- Возмещение ущерба причиненного предприятию в результате противоправных действий
- Взаимодействие Группы внутренних расследований с отделами предприятия и правоохранительными органами для профилактики инцидентов, обеспечения безопасности персонала и имущества
    - Порядок проведения ВСР и ВСП по фактам совершения противоправных действий со стороны сотрудников Компании
    - Использование полиграфа (детектора лжи) при проведении ВСР. Правовая и организационная сторона вопроса. Возможно ли, обмануть полиграф?
    - Процессуальное оформление результатов ВСР
    - Взаимодействие Службы безопасности с правоохранительными органами при расследовании противоправных действий