



«МБШ - Семинары» ЖШС

050059, Алматы, Өл-Фараби даңғ., 19,
«Нұрлы-Тау» БО, 16 қабат, 1604 кеңсе
Тел.: 8 (727) 311 09 11
Web: www.mbschool.kz

ТОО «МБШ - Семинары»

050059, Алматы, пр. Аль-Фараби, 19,
БЦ «Нурлы-Тау», 16 этаж, офис 1604
Тел.: 8 (727) 311 09 11
Web: www.mbschool.kz

ТОО «МБШ-Семинары» благодарит Вас за проявленный интерес и предлагает Вам рассмотреть ценовое предложение на корпоративное обучение по теме **«Руководитель службы безопасности (2 модуль)»**.

ТОО «МБШ-Семинары» имеет большой опыт в организации и проведении корпоративных тренингов/семинаров, как для мелких, так и для крупных компаний Казахстана на основе которого предлагает проведение тренинга/семинара и для Вашей Компании.

ТОО «МБШ-Семинары» приглашает Вас принять участие в тренинге/семинаре: **«Руководитель службы безопасности (2 модуль)»**.

Стоимость корпоративного обучения: 1 580 000 (один миллион пятьсот восемьдесят тысяч) тенге (Исполнитель не является плательщиком НДС) за 3 дня (24 академических часа) обучения.

Место проведения: РК, г. Нур-Султан конференц-зал отеля Best Western Plus Astana Hotel, ул. Достык 13А.

Дата проведения: по согласованию.

Время: с 10:00 до 17:30.

Тренер: Комаров Вадим Николаевич (Санкт - Петербург).

Количество участников: от 1 до 5 человек.

В стоимость обучения входит: обучение. Комплект обучающих материалов, блокноты, ручки, бейджи, сертификаты Moscow Business School на каждого участника тренинга/семинара (сертификаты входят в стоимость), удостоверение о повышении квалификации на каждого участника тренинга/семинара (при условии предоставления необходимого пакета документов и доплаты за каждого участника тренинга/семинара 12 000 (двенадцать тысяч) тенге без НДС). Перелет, проживание, трансфер тренера. Аренда конференц-зала, проектор, экран, флипчарт, маркеры, обеды, кофе-паузы.

Обратите внимание!

Программа тренинга/семинара стандартная и может быть адаптирована под специфику деятельности Заказчика, согласно подробной заявки Заказчика!

Возможна предварительная Skype – конференция с тренером.

Информация о компании.

Moscow Business School сегодня– это:

1. Профессиональный состав привлекаемых к процессу обучения преподавателей, успешных экспертов, консультантов, топ-менеджеров крупных корпораций;
2. Более 10 направлений семинаров, проходящих каждый месяц, 100%-ный тематический охват потребностей российского бизнеса в рамках краткосрочных программ профессионального обучения;
3. Дистанционные программы МВА, высокая эффективность которых обеспечивается за счет использования видеолекций, а также ряда иных учебных активностей, позволяющих максимально приблизить дистанционное обучение к очному (видеоконференции, вебинары, дискуссионные е-семинары, проводимые на форумной платформе);
4. Современная система дистанционного образования;
5. Интегрированный комплекс инструментов, технологий, методик и форматов обучения с выраженным прикладным, практически ориентированным обучением, направленным на решение практических задач менеджмента;
6. Ежемесячные матер-классы – бесплатные мероприятия - актуальный на сегодняшний момент формат для общения, обсуждения планов, высказывания предложений об услугах и рождения партнерских связей между компаниями и клиентами;
7. Более 100 мультимедийных тренингов в виде видеосеминаров в связке с системой дистанционного образования.

Учась в Moscow Business School, Вы получаете:

- престижные дипломы и сертификаты школы международного уровня;
- высокое качество сервиса во время обучения и индивидуальный подход;
- самые современные знания и навыки, новые полезные и интересные контакты со слушателями курса.

Обучение в Школе помогает структурировать реальный деловой опыт и выработать навыки системного подхода к решению бизнес-задач. Всё это способствует быстрому профессиональному и карьерному росту.

Программа тренинга/семинара.

«Руководитель службы безопасности (2 модуль)»

Резкое усложнение бизнес-среды, обострение конкурентной борьбы, возникновение новых видов угроз, высокой динамикой развития — все это потребовало от предприятий наличия сильных служб безопасности, способных эффективно действовать в чрезвычайных условиях. В связи с этим возрастают требования, предъявляемые к руководителям, менеджерам и специалистам, обеспечивающим безопасность.

Этот семинар является органичным продолжением семинара «Руководитель службы безопасности». Вместе с тем он имеет самостоятельный характер, не повторяет тем, рассмотренных в первом семинаре.

В результате обучения Вы

- познакомитесь с системой анализа и управления экономическими рисками
- изучите порядок взаимоотношений службы экономической безопасности с правовым подразделением компании по юридическому сопровождению взыскания задолженности
- освоите систему защитных мер от возможного враждебного поглощения
- изучите организацию системы внутреннего контроля
- познакомитесь с понятием «отката» и типологией «откатополучателей»
- рассмотрите порядок засекречивания и рассекречивания документов
- изучите виды ответственности за разглашение персональных данных, а также за ее незаконное получение
- познакомитесь с методикой проверки помещения на наличие каналов утечки информации
- освоите методику построения информационной безопасности компании
- изучите террористические и диверсионные угрозы промышленным объектам и освоите способы их предотвращения

Экономическая безопасность компании

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 рисков 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
- Определение объектов защиты от экономических рисков. Определение субъектов безопасности
- Аутсорсинговое обеспечение экономической безопасности компании
- Формирование нормативного обеспечения экономической безопасности бизнеса

Практикум: «Разработка модели угроз компании. Построение радаров внешних и внутренних рисков»

Взыскание дебиторской задолженности

- Понятие дебиторской задолженности. Виды дебиторской задолженности. Образование просроченной (безнадежной к получению) дебиторской задолженности
- Наличие дебиторской задолженности, как разновидность финансового риска. Влияние дебиторской задолженности на финансовую устойчивость компании
- Перечень превентивных воздействий службы экономической безопасности на возможных неплательщиков
- Информационно-аналитическая работа по определению нахождения должника, его активов, анализу его финансовой устойчивости, а также причин непогашения дебиторской задолженности
- Порядок взаимоотношений службы экономической безопасности с правовым подразделением компании по юридическому сопровождению взыскания задолженности. Судебные иски, арбитражное судебное производство и работа судебных приставов по взысканию дебиторской задолженности
- Порядок и особенности взаимоотношений службы экономической безопасности с правоохранительными органами в процессе взыскания дебиторской задолженности
- Организация и проведение переговоров с должниками. Психологические приемы, применяемые в процессе переговоров
- Имиджевые приемы воздействия, применяемые при работе с должниками. Законные способы формирования отрицательного имиджа компании-должника. Некоторые приемы «черного PR», применяемые на практике
- Работа коллекторских агентств для взыскания долга

Практикум: «Разработка сценария действий по нахождению должника, его активов»

Защита от рейдерства (враждебного поглощения)

- Гринмейл, или корпоративный шантаж. Сценарии действий гринмейлера. Возможности гринмейлера в зависимости от количества акций
- Рейдерские захваты. Цели (причины, мотивы) рейдерства. Виды рейдерства. Определение рейдерства (враждебного поглощения) в законодательстве России. Внутреннее и внешнее враждебное поглощение
- Типы и стратегии деятельности компаний-агрессоров. Сценарии рейдерских захватов (белые, серые и черные схемы)
- Возможности судебной защиты прав собственности на акции. Юридическая ответственность за враждебное поглощение. Изменения в уголовном законодательстве в части усиления ответственности за рейдерские захваты
- Превентивная система защитных мер от возможного враждебного поглощения. Классификация превентивных мер. Создание оборонного периметра компании
- Защита информационных ресурсов и атрибутов организации. Конкурентная разведка и иной мониторинг текущей ситуации. Защита реестра акционеров. Выстраивание отношений с правоохранительными органами и государственными органами в сфере экономической безопасности
- Формирование корпоративной культуры как элемента защиты от рейдерства. Проведение рекламной компании и PR-акций для формирования положительного

имиджа компании. Применение технологий «отравленных пилюль» и «золотых парашютов» в трудовых отношениях

- Признаки начавшегося враждебного поглощения. Защита компании от начавшегося враждебного поглощения
- Мероприятия, проводимые руководством, службой экономической безопасности, юристами компании при начавшемся враждебном поглощении. Перечень возможных организационных мер. Выстраивание общего плана защиты компании. Реорганизация компании. Возможность банкротства компании. Обеспечение информационно-аналитического сопровождения при начавшемся захвате

Практикум: «Разработка предложений по созданию оборонного периметра компании»

Борьба с корпоративными мошенничествами

Корпоративное мошенничество

- Мошенничество как разновидность преступления против собственности. Понятие и признаки мошенничества. Отличие мошенничества от иных преступлений против собственности
- Модель мошенника. Модель жертвы мошенничества. Мошенники и их мотивация, психологические приемы, применяемые мошенниками
- Модели мошеннических операций, виды и особенности корпоративного мошенничества. Общая характеристика и виды преступлений против собственности (кража, растрата, грабеж, разбой, вымогательство и т.д.)
- Юридическая ответственность за совершение мошеннических операций. Обзор судебной практики по применению судами решений по статье 159 Уголовного кодекса Российской Федерации
- Виды корпоративного мошенничества. Основные приемы и методы корпоративного мошенничества. Понятие «треугольник мошенничества» (давление внешних обстоятельств, возможность совершать мошенничество и возможность оправдывать мошеннические действия)
- Типичные сценарии корпоративного мошенничества со стороны наемных работников. Типичные сценарии корпоративного мошенничества со стороны руководителей. Признаки корпоративного мошенничества со стороны наемных работников и руководителей
- Сценарии корпоративного мошенничества, основанные на использовании новых информационных технологий
- Программа действий по борьбе с мошенничеством (предупреждение, обнаружение, расследование). Основные способы устранения возможностей корпоративного мошенничества
- Процедура проведения внутрикорпоративных расследований при выявлении факта мошенничества. Создание матрицы расследования. Методы и формы расследования. Процессуальные действия сотрудников службы экономической безопасности, направленные на сбор легитимных доказательств мошенничества

Практикум: «Рассмотрение различных методов корпоративного мошенничества»

Внутренний контроль

- Организация системы внутреннего контроля
- Организационные и контрольные меры по предупреждению корпоративного мошенничества

- Кадровые меры по предупреждению корпоративного мошенничества (проверка при приеме сотрудников, формирование корпоративной культуры, мотивация персонала и т.д.)
- Комплаенс как принцип ведения бизнеса в соответствии с применимым законодательством, правилами, кодексами и стандартами, установленными компетентными властями, профессиональными ассоциациями и внутренними документами учреждения
- Принципы организации комплаенса

Практикум: «Организация процесса комплаенса на предприятии»

Откаты

- Понятие «откат» в современных рыночных отношениях. Классификация откатов
- Избранные статьи УК Российской Федерации (коммерческий подкуп, получение и дача взятки, злоупотребление полномочиями)
- Типология «откатополучателей»
- Организация борьбы с откатами. Психологические приемы. Кадровая проверка потенциальных «откатополучателей»
- Создание корпоративного кодекса, включающего правила корпоративной этики
- Формализация внутренних правил, описывающих процедуру проведения закупок

Практикум: «Как выявить откатополучателя»

Противодействие экономическому шпионажу

Коммерческая тайна предприятия

- Режим коммерческой тайны. Нормативно-правовые акты Российской Федерации, определяющие понятие коммерческая тайна. Нормативно-правовые документы компании при введении режима коммерческой тайны
- Федеральный закон «О коммерческой тайне», основные нормы закона, применяемые термины и определения
- Порядок создания режима коммерческой тайны в компании. Перечень сведений, составляющих коммерческую тайну компании
- Ограничение доступа к информации, составляющей коммерческую тайну компании

Практикум: «Процедура создания перечня сведений, составляющих коммерческую тайну компании»

Организация конфиденциального делопроизводства

- Конфиденциальное делопроизводство как элемент защиты информации. Создание и функционирование конфиденциального делопроизводства в компании
- Принципы построения конфиденциального делопроизводства. Порядок взаимодействия открытого и конфиденциального делопроизводства
- Традиционный и электронный документооборот. Электронная цифровая подпись, как подтверждение авторства и подлинности электронного документа
- Определение порядка работы с конфиденциальными документами (создание, учет, хранение, перемещение и уничтожение)
- Порядок засекречивания и рассекречивания документов. Экспертные комиссии. Архив конфиденциальных документов

- Формирование внутренней нормативной базы для обеспечения конфиденциального делопроизводства. Инструкция по конфиденциальному делопроизводству в компании
- Персональная ответственность сотрудников за сохранность конфиденциального документа и защиту информации, в нем содержащуюся. Порядок допуска сотрудников к работе с конфиденциальными документами. Обучение сотрудников компании правилам работы с конфиденциальными документами. Формирование культуры работы с конфиденциальными документами
- Контроль и учет документооборота в конфиденциальном делопроизводстве
- Контроль за размножением, тиражированием и уничтожением конфиденциальных документов
- Плановая и внеплановая проверка конфиденциального делопроизводства. Процедура проведения внутрикорпоративного расследования по факту нарушения правил работы с конфиденциальными документами или разглашению информации, содержащейся в конфиденциальных документах

Практикум: «Организация конфиденциального делопроизводства на малом предприятии»

Организация противодействию промышленному шпионажу на предприятии

- Правовые и организационные меры противодействия промышленному шпионажу. Юридическая ответственность за использование технических средств, предназначенных для негласного получения информации
- Классификация угроз. Модель угроз для предприятия. Источники угроз (конкуренты, криминал, общественные организации и др.). Модель «нарушителя». Внутренние и внешние нарушители.
- Элементы контрразведывательной работы на предприятии. Инсайдеры. Агенты влияния. Организация работы с добровольными помощниками. Взаимодействие между подразделениями предприятия по контрразведывательной деятельности. Понятие этики в контрразведке. Нормы законодательства РФ, позволяющие проводить контрразведывательные мероприятия на предприятии
- Противодействие техническим разведкам (ПДТР). Организационные, правовые, кадровые и технические мероприятия
- Естественные и искусственные каналы утечки информации. Технические каналы утечки информации (ТКУИ), их особенности и характеристики
- Обзор технических средств выявления и обнаружения ТКУИ. Обзор технических средств защиты конфиденциальной информации. Методика проверки помещения на наличие каналов утечки информации. Анализ отечественного рынка средств ПДТР

Практикум: «Проверка кабинета директора перед проведением закрытого совещания»

Информационная безопасность компании

Создание системы информационной безопасности в компании

- Политика информационной безопасности (ИБ). Методика построения политики информационной безопасности компании. Основные требования и принципы, учитываемые при разработке и внедрении политики ИБ
- Управление рисками информационной безопасности. Нормативное обеспечение управления рисками ИБ. Международные стандарты серии ISO/IEC 27000 «Информационные технологии. Методы обеспечения безопасности»
- Оценка рисков ИБ. Анализ рисков. Оценивание рисков. Обработка рисков

- Аудит информационной безопасности в компании. Внутренний аудит ИБ (цели и задачи внутренних аудитов ИБ, организационные принципы внутреннего аудита, обеспечение эффективности внутреннего аудита). Внешний аудит ИБ (принципы проведения внешнего аудита ИБ, этапы проведения, компетентность аудиторов)

Практикум: «Проведение внутреннего аудита»

Защита персональных данных

- Федеральный закон «О персональных данных», основные нормы закона, применяемые термины и определения. Трудовой кодекс Российской Федерации и иные нормативно-правовые акты Российской Федерации, регламентирующие вопросы персональных данных и их защиту
- Международные конвенции по защите персональных данных физических лиц
- Оператор персональных данных, его права и обязанности, порядок регистрации
- Формирование правового режима ограничения доступа и защиты персональных данных, порядок получения, формирования и обработки персональных данных, уведомление об обработке (о намерении осуществлять обработку) персональных данных
- Особенности обработки и защиты персональных данных, осуществляемой без использования средств автоматизации
- Особенности обработки и защиты персональных данных, осуществляемой с использованием средств автоматизации
- Порядок проведения классификации информационных систем персональных данных
- Необходимость и порядок получения лицензии на техническую защиту конфиденциальной информации
- Массивы биометрических персональных данных и требования к их защите
- Виды ответственности за разглашение персональных данных, а также за ее незаконное получение. Необходимые и достаточные условия для ее наступления

Практикум: «Реализация требований закона „О персональных данных“ для малого бизнеса»

Антитеррористическая защита объектов компании

Террористические и диверсионные угрозы промышленным объектам

- Некоторые характеристики и особенности террористической деятельности
- Террористические и диверсионные угрозы. Модель нарушителя
- Составление антитеррористического паспорта объекта
- Предотвращение террористических и диверсионных актов с использованием взрывных устройств, химических, бактериологических и радиоактивных веществ
- Примерное оснащение поста контроля персонала, посетителей, ручной клади
- Пост проверки почтовой корреспонденции. Признаки подозрительных почтовых отправлений
- Общие рекомендации по поведению персонала при наличии угрозы террористического акта
- Режим и охрана критически важных объектов

Практикум: «Процедура проверки почтовых отправлений на наличие подозрительных предметов»

Информационные аспекты противодействия терроризму

- Кибертерроризм. Классификация деструктивных информационных воздействий на критически важные объекты. «Боевые вирусы». Программные закладки
- Модель нарушителя
- Информационная безопасность критически важных объектов
- Особенности организации процесса защиты информации автоматизированных систем управления технологическими процессами (АСУ ТП) на производстве

Практикум: «Оценка возможных ущербов связанных с уничтожением информационных объектов»

Резюме тренера.

Комаров Вадим Николаевич



Эксперт по корпоративной безопасности

Профессиональный опыт

- 2006 — по н.в. — ООО «Технологии Безопасности Бизнеса», генеральный директор
- 2002–2006 — ЗАО «Центр Безопасности Бизнеса», генеральный директор
- 1993–2002 — Гипермаркет «АШАН», торговая сеть «ТАТИ», Восточно-Европейский Инвестиционный Банк (ВЕИБ),

начальник службы безопасности

Профессиональные компетенции

- Организация и руководство службами безопасности. Проектирование систем комплексной безопасности для предприятий различного рода деятельности
- Разработка критериев и показателей эффективности системы безопасности. Осуществление практического руководства и контроля по их достижению
- Организация и проведение независимых конкурсов на поставку технических систем и физической охраны
- Организация систем экономической, кадровой и информационной безопасности с нуля
- Аудит экономической безопасности. Выявление и расчет экономических и хозяйственных рисков фирм
- Организация взаимодействия с силовыми и контролирующими государственными органами

Преподавательская деятельность

2002 – по н.в. – автор и ведущий семинаров по безопасности, докладчик на тематических конференциях по безопасности в России и за рубежом

Выступления и публикации

- Автор публикаций в профессиональных периодических СМИ: журнал «Мое дело», «Российская торговля», «Справочник руководителя торгового предприятия», «Газета Безопасность и Торговля», «Технологии Безопасности Бизнеса»
- Принимал участие в проектах на телевидении и радио по вопросам экономической и психологической безопасности

Образование

- 1998–2001 — Академия Предпринимательства и бизнеса при Правительстве г. Москвы, менеджер организации
- 1985–1989 — Полтавское Высшее Зенитное Ракетное Командное училище, инженер-радиотехник

Образец сертификата.



Moscow
Business School
Leadership Energy

СЕРТИФИКАТ

Настоящим удостоверяется, что

Иванов Иван Иванович

прошел обучение на семинаре
«Особенности продажи слонов
на среднерусской возвышенности»

Дата выдачи: 12.12.2016
Продолжительность курса: 16 часов

Руководитель:
А. Н. Самойловских

Преподаватель:
П. П. Петров

Образец удостоверения о повышении квалификации.

- Обратите внимание! Удостоверение о повышении квалификации выдается при предоставлении документов:
- Заполненная анкета с заявлением на имя ректора (по образцу)
- Копия диплома о высшем или среднем профессиональном образовании, с приложением (приложение- это документ, где указываются оценки)
- Копия паспорта (именно паспорта, не удостоверения личности)
- Документ о смене фамилии, если диплом о высшем или среднем профессиональном образовании выдан на другую фамилию, чем в паспорте
- Доплата 12 000 (двенадцать тысяч) тенге без НДС за одного участника

 MBS Удостоверение является документом о повышении квалификации	УДОСТОВЕРЕНИЕ О ПОВЫШЕНИИ КВАЛИФИКАЦИИ
	Настоящее удостоверение выдано _____ <small>(Фамилия, имя, отчество)</small>
	в том, что он (а) с " ____ " ____ г. по " ____ " ____ г. прошел (а) обучение в (на) _____ <small>(наименование образовательного учреждения (образователь) / наименование профессионального образования)</small>
	по _____ <small>(на программу профессионального образования)</small>
	в объеме _____ <small>(количество часов)</small>
Регистрационный номер _____	М.П. Ректор (директор) _____ Секретарь _____
	Город _____ год _____

Коммерческий директор МНПЦ Семьялы Василькина А.Д.

