Семинары Moscow Business School

Исходный URL: https://mbschool.ru/seminars/60132

Руководитель службы безопасности (1 модуль)

Потребность в руководителях службы безопасности существует как у предприятий малого и среднего бизнеса, так и у крупных холдинговых компаний. Руководители приходят к мысли, что им необходима служба, решающая задачи обеспечения безопасности предприятия. Возникает необходимость в человеке, который возьмет на себя работу по организации и управлению такой службой.

Расписание

Город: Нур-Султан

Дата:

- 9 – 13 сентября `19
- 16 – 20 марта `20
- 21 – 25 сентября `20

В результате обучения вы:

- проанализируете законодательство Российской Федерации в области корпоративной безопасности
- познакомитесь с особенностями проведения политики безопасности в условиях кризиса
- рассмотрите методы сбора информации и анализа конкурентной разведки
- изучите организацию защиты конфиденциальной информации при проведении закрытых мероприятий
- познакомитесь со структурой и принципами действия информационно-аналитической системы обеспечения безопасности бизнеса
- получите знания о правонарушениях и преступлениях в информационной сфере
- освоите системность в обеспечении личной безопасности первых лиц компании
- познакомитесь с ответственностью за нарушения в сфере информационной безопасности
- изучите правила работы с увольняющимися сотрудниками, имевшими доступ к конфиденциальной (опасной) информации
- рассмотрите порядок проведения внутрикорпоративных расследований службой безопасности по фактам совершения противоправных действий со стороны сотрудников компании
- изучите правовые основы деятельности частной охранной организации

Следующие темы возможно изучить отдельно:

Информационно-аналитическое обеспечение безопасности бизнеса

Практические методы защиты информации на предприятии

Программа семинара

День 1

Система корпоративной безопасности

Политика безопасности компании

- Основные понятия теории безопасности. Объект безопасности (Что защищаем?). Угроза (От чего защищаем?). Субъект безопасности (Кто защищает?)
- Угрозы безопасности. Риски. Ущербы
- Система безопасности бизнеса (структура, задачи, принципы построения)
- Служба безопасности — основа системы безопасности компании
- Политика безопасности бизнеса. Подходы к построению
- Особенности проведения политики безопасности в условиях кризиса. Участие СБ в антикризисных мероприятиях
- Особенности политики корпоративной безопасности в зарубежных странах
- Обеспечение безопасности бизнеса в представительствах иностранных компаний, действующих на территории России, холдингах, дочерних компаниях, в компаниях, имеющих сложную организационную (территориально разделенную) структуру

Практикум «Пошаговая методика разработки политики безопасности компании»

Правовая защита бизнеса как составная часть системы безопасности компании

- Законодательство Российской Федерации в области корпоративной безопасности. Новое в законодательстве Российской Федерации по вопросам охранной и детективной деятельности
- Основные направления работы СБ и юристов компании при проведении мероприятий по правовой защите бизнеса. Превентивные организационные приемы защиты при взаимодействии с государственными контролирующими и правоохранительными органами
- Виды проверок (налоговые, в рамках государственного контроля по выявлению административных правонарушений и т.д.). Права и обязанности государственных органов в процессе осуществления ими проверок и иных контрольных и надзорных мероприятий
- Действия сотрудников компании и СБ в ситуациях, возникших при проведении государственными органами проверок и иных контрольных и надзорных мероприятий
- Порядок составления протокола об административном правонарушении. Процедура наложения административного взыскания
- Методики взаимодействия с государственными контролирующими и правоохранительными органами, применяемые при защите интересов компании

Практикум «Разбор практик поведения сотрудников СБ при проверках компании государственными

контролирующими органами»

Служба безопасности компании

- Правовая сторона деятельности службы безопасности компании
- Место СБ в структуре компании. Взаимодействие с акционерами, владельцами и руководителями бизнеса
- Положение о службе безопасности компании
- Компетенции сотрудников СБ, их функции, права и обязанности
- Этический кодекс поведения сотрудников СБ компании. Мотивирование сотрудников
- Управление службой безопасности компании. Требования к начальнику СБ, черты характера, профессиональные качества, образовательный уровень, опыт работы

Практикум «Составление этического кодекса сотрудников СБ»

Экономические аспекты обеспечения безопасности компании

- Анализ деятельности СБ компании. Аудит безопасности компании
- Оценка эффективности системы безопасности предприятия
- Методики оценки стоимости организационных, технических и иных методов обеспечения безопасности предприятия
- Финансирование службы безопасности компании

Практикум «Разбор кейса по аудиту безопасности компании (на примере конкретной компании)»

День 2

Информационно-аналитическое обеспечение безопасности бизнеса

Конкурентная разведка, противодействие экономическому шпионажу и черному PR

- Информационное пространство бизнеса. Цели и задачи системы информационного мониторинга
- Основные понятия конкурентной разведки. Стратегические и тактические задачи КР
- Правовые и этические нормы конкурентной разведки. Конкурентная разведка и промышленный шпионаж: сходство и различие. Этический кодекс
- Разведывательный цикл. Постановка задачи и планирование операций. Создание рубрикатора
- Метод раннего конкурентного предупреждения. «Треугольник Джилада»
- Организация службы КР на предприятии

Практикум «Разбор применения метода раннего конкурентного предупреждения для предприятий малого и среднего бизнеса»

Методы сбора и анализа информации в конкурентной разведке

- Классификация информации. Первичная и вторичная информация
- Качественные характеристики информации и источников информации (достоверность, надежность, актуальность и др.). Оценка информации по методу Кента
- Информационные источники. Классификация информационных источников
- Информационные помехи и информационное поле руководителя
- Методы сбора информации. Полевые и кабинетные методы
- Алгоритм анализа. Классификация методов
- Анализ конкурентной среды. Модель пяти сил Майкла Портера
- Методы анализа конкурентной разведки. Метод SWOT
- Причинно-следственный анализ. Контент-анализ. Ситуационный (Ивент) анализ
- Экспертные анализы. Диверсионный анализ
- Представление результатов КР лицу, принимающему решения. Типы аналитических документов

Практикум «Рассмотрение алгоритма диверсионного анализа при решении конкретной задачи»

Применение новых информационных технологий в деятельности службы безопасности

- Российские и зарубежные профессиональные базы данных. Краткий анализ. Интегрум. Интерфакс/СПАРК. Factiva. Lexis-Nexis
- Интернет-источники. Социальные сети как источник информации. Интернет-разведка
- Информационно-аналитические системы. Факт как основа ИАС. Принципы работы ИАС
- Классификация ИАС (Арион, Астарта, семейство I2, Palantir, Семантический архив, Аваланч и др.)
- Информационно-аналитическая система «Семантический архив». Структура. Принцип действия. Источники

Практикум «Сравнительный анализ различных информационно-аналитических систем (в зависимости от вида задачи)»

Анализ надежности контрагентов и безопасности коммерческих предложений

- Алгоритм определения надежности партнеров(физических и юридических лиц). Формирование матрицы действий по проверке компании в зависимости от суммы сделки, предоплаты и иных условий
- Применение метода Due Diligence в анализе компании
- Анализ финансовой устойчивости компании по представленным бухгалтерским отчетным документам (баланс, отчет о прибылях и убытках, отчет о движении капитала и т.д.). Анализ платежеспособности клиента
- Анализ возможных кризисных ситуаций в деятельности компании на основе статистических

методов, использующих информацию о времени деятельности компании, ее обороте и количестве работающих сотрудников
- Анализ учредительных документов компании с позиции безопасности. Анализ атрибутов компании и фирменного стиля компании
- Типы компаний, преследующие противоправные цели. Прогнозирование надежности организаций на основе растровых признаков опасности. Формирование рейтингов надежности партнеров
- Анализ безопасности коммерческих предложений и договоров. Изучение инициаторов проекта, их интересов и деловой репутации. Изучение механизма получения прибыли
- Анализ первого контакта. Поведенческие аспекты при выявлении ненадежного партнера

Практикум «Оценка возможностей применения новых информационных технологий (на примере системы СПАРК/Интерфакс) для проверки партнера»

День 3

Практические методы защиты информации на предприятии

Организационные и правовые методы защиты информации

- Основные понятия информационной безопасности. Термины и определения
- Правовые основы информационной безопасности. Концептуальные документы в области защиты информации
- Ответственность за нарушения в сфере информационной безопасности
- Методы и формы организационной защиты конфиденциальной информации
- Организация защиты конфиденциальной информации при проведении закрытых мероприятий

Практикум «Алгоритм организации проведения совещания, на котором будут обсуждаться конфиденциальные планы предприятия, например, по выходу на новые рынки»

Угрозы и уязвимости. Модель нарушителя

- Правонарушения и преступления в информационной сфере
- Каналы утечки информации
- Обзор и классификация угроз информации, обрабатываемой СВТ и АС
- Классификация компьютерных атак
- Компьютерные вирусы и программные закладки
- Модели нарушителей
- Методы социальной инженерии

Практикум «Разбор алгоритма составления модели нарушителя для предприятий малого и среднего бизнеса»

Программно-аппаратные методы защиты информации

- Перечень аппаратно-программных средств защиты компьютерной информации
- Защита внешнего контура. DLP-системы
- Идентификация и аутентификация пользователей. Пароли. Биометрические методы
- Антивирусные программы
- Криптографические средства защиты информации
- Межсетевое экранирование
- VPN-технологии

Практикум «Оценка российского рынка средств защиты информации»

Служба комплексной защиты информации компании

- Место службы защиты информации (IT-Security) в структуре системы безопасности предприятия
- Нормативные акты, регламентирующие деятельность IT-Security
- Лицензирование и сертификация средств защиты информации. Аттестация объектов информатизации
- Компетенции руководителя и сотрудников службы защиты информации

Практикум «Алгоритм получения лицензии на производство средств защиты информации»

День 4

Кадровая безопасность компании

Персонал как объект защиты и как источник угрозы

- Классификация угроз в отношении персонала
- Организационные и правовые методы защиты персонала
- Виды угроз, исходящих от сотрудников компании, варианты их реализации и возможные направления защиты
- Противоправные действия сотрудников, ответственность за которые предусмотрена в Российской Федерации (УК, КоАП, Трудовой Кодекс и др.)
- Корпоративный кодекс, возможные действия сотрудников компании, нарушающие его нормы. Привлечение сотрудников к ответственности за нарушения корпоративного кодекса

Практикум «Составление матрицы уязвимости компании с учетом угроз кадровой безопасности, исходящих от собственных сотрудников»

Проверка кандидатов для работы в компании. Прием сотрудников

- Процедура сбора информации о кандидатах на работу в компании. Оформление согласия на сбор персональных данных. Возможность использования детективов для сбора информации
- Сбор информации о кандидате. Порядок анализа резюме. Анкеты для кандидатов на работу. Официальные источники по сбору информации
- Использование интернета для сбора информации о кандидате на работу в компанию
- Возможность легализации полученной информации о кандидате. Юридическое оформление отказа в приеме на работу
- Растровые признаки опасности у кандидата на работу. На что обратить внимание в проверочных мероприятиях
- Применение современных методов и технологий при проверках кандидатов на работу (полиграф, психозондирование)
- Формирование модели потенциального правонарушителя, применительно к различным должностям
- Особенности приема отдельных категорий персонала (топ-менеджеры; лица, назначаемые на должности, связанные с мошенническими рисками и т.д.)

Практикум «Правила приема сотрудников на должности, связанные с обработкой конфиденциальной информации»

Управление кадровой безопасностью в компании

- 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
- Создание системы персональной ответственности сотрудников компании
- Порядок проведения службой безопасности внутрикорпоративных расследований по фактам совершения противоправных действий со стороны сотрудников компании
- Использование полиграфа (детектора лжи) при проведении внутрикорпоративных расследований. Правовая и организационная сторона вопроса
- Применение методов психозондирования при расследовании противоправных действий
- Процессуальное оформление результатов внутрикорпоративных расследований
- Взаимодействие СБ с правоохранительными органами при расследовании противоправных действий

Практикум «Алгоритм действий сотрудников СБ при внутрикорпоративном расследовании (на конкретном примере)»

Увольнение персонала

- Обеспечение лояльности увольняющихся сотрудников
- Правила работы с увольняющимися сотрудниками, имевшими доступ к конфиденциальной

(опасной) информации
- Правила проведения индивидуальных бесед с увольняющимися сотрудниками. Что предпринять, чтобы сотрудник после увольнения не представлял опасность
- Имиджевые и репутационные аспекты воздействия на увольняющегося сотрудника
- Определение истинных причин увольнения сотрудника
- Процессуальное оформление увольнения с точки зрения безопасности. Как лучше расставаться с «нехорошими» людьми
- Алгоритм передачи дел и должности. Превентивная работа с контрагентами. Что сделать, чтобы увольняющийся сотрудник не увел клиентов

Практикум «Правила увольнения сотрудника с должности, связанной с обработкой конфиденциальной информации»

День 5

Организация проведения охранных мероприятий на объекте

Внутриобъектовый и пропускной режимы в компании

- Вневедомственная и ведомственная охрана, правовые основы их деятельности, особенности работы с данными подразделениями
- Негосударственная охрана в Российской Федерации, частные охранные организации как разновидность негосударственных охранных структур
- Правовые основы деятельности частной охранной организации. Новое в законодательстве Российской Федерации
- Виды оружия (гражданское, служебное, боевое) в соответствии с законодательством Российской Федерации
- Создание внутриобъектового и пропускного режимов в компании. Защита персональных данных при осуществлении пропускного режима
- Подготовка договора на оказание охранных услуг
- Создание схемы охраны объекта
- Деятельность субъектов охранной деятельности по охране и сопровождению грузов

Практикум «Алгоритм организации пропускного режима на вновь создаваемом предприятии»

Инженерно-техническая безопасность компании

- Система инженерно-технической безопасности. Перечень инженерно-технических мероприятий по оборудованию защищаемого объекта
- Противопожарная безопасность компании
- Системы охраны периметров объектов. Принципы работы систем охраны периметров
- Системы охранного телевидения (видеонаблюдения). Правовые основы использования видеонаблюдения на объектах

- Обзор технических средств охранных сигнализаций (инфракрасные, радиоволновые, ультразвуковые, магнитно-контактные, акустические, ударно-контактные, емкостные, вибрационные охранные извещатели)
- Системы контроля и управления доступом. Перечень организационных, правовых, кадровых и технических мероприятий

Практикум «Разработка нормативных документов, регламентирующих организационные, правовые, кадровые и технические мероприятия на защищаемом объекте. Общие подходы»

Организация личной безопасности персонала

- Перечень мероприятий по обеспечению личной безопасности (физическая защита, юридическая защита, психологическая защита и т.д.)
- Планирование охранных мероприятий по физической защите человека
- Порядок приобретения, хранения, ношения и применения (использования) оружия физическими лицами
- Некоторые правила общения с людьми, представляющими опасность
- Использование понятия «необходимая оборона» для самозащиты физического лица и освобождения от уголовной ответственности за причинение вреда нападавшему

Практикум «Алгоритм планирования охранных мероприятий по защите сотрудников предприятия при угрозах чрезвычайных ситуаций»

Организация защиты первых лиц компании

- Системность в обеспечении личной безопасности первых лиц компании
- Правовые особенности работы телохранителей в России. Законодательство Российской Федерации об охранной деятельности (государственная охрана, ведомственная охрана, вневедомственная охрана, частная охрана). Что нужно знать физическому лицу, нанимающему телохранителей
- Организация охранных мероприятий по физической защите руководителя (дом, офис, перемещение в городе, перемещение по стране и т.д.)
- Информационно-аналитическая работа как составная часть работы телохранителей

Практикум: «Рассмотрение правил подбора телохранителей»

Стоимость участия

Стоимость участия в семинаре составляет **225600 тенге** с учетом всех налогов.

В стоимость обучения входит:

- Комплект авторских материалов

- Кофе-паузы, обеды
- Сертификат Moscow Business School
- Удостоверение о повышении квалификации*
- Диплом о профессиональной переподготовке**

Преподаватели семинара

- **Баяндин Николай Иванович**

  Профессор Академии безопасности, обороны и правопорядка, эксперт Российского общества профессионалов конкурентной разведки

- **Панкратьев Вячеслав Вячеславович**

  Специалист в области корпоративной безопасности компании и управлении экономическими рисками

- **Креопалов Владимир Владиславович**

  Кандидат технических наук, эксперт-практик в области безопасности предпринимательской деятельности

- **Комаров Вадим Николаевич**

  Эксперт по корпоративной безопасности. Один из ведущих экспертов в России и СНГ по экономической, кадровой, психологической, информационной безопасности предприятий