Семинары Moscow Business School

Исходный URL: https://mbschool.ru/seminars/7728

Технологии управления службой безопасности компании

Продолжительность обучения: 80 академических часов аудиторных занятий.

Полученные знания дают возможность создать и эффективно управлять службой безопасности предприятия. Вы не только существенно расширите свои компетенции, но и сможете внедрить новые инструменты деятельности и управления данной структурой.

Расписание

Город: Москва

Дата:

- 12 – 16 августа `19
- 16 – 20 сентября `19
- 11 – 15 ноября `19
- 16 – 20 декабря `19
- 17 – 21 февраля `20
- 23 – 27 марта `20
- 18 – 22 мая `20
- 22 – 26 июня `20
- 10 – 14 августа `20

В результате обучения вы:

- изучите современные приемы управления системами безопасности компании, а также рассмотрите опыт их создания в коммерческих структурах
- проанализируете проблемы безопасности бизнеса и подготовите алгоритмы их решений
- научитесь правильному составлению нормативных правовых документов компании, которые позволят обеспечивать должный уровень безопасности
- усовершенствуете навыки оперативной работы с персоналом
- сумеете организовывать результативное функционирование систем безопасности в организации. Научитесь правильной организации режима и охраны компании
- оцените современное состояние российского рынка средств безопасности

Программа семинара

Модуль 1

- Продолжительность: 5 дней
- Тренеры: Креопалов Владимир Владиславович, Панкратьев Вячеслав Вячеславович, Баяндин Николай Иванович
- Расписание: с 10:00 до 17:30

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»

Модуль 2

- Продолжительность: 5 дней
- Тренеры: Креопалов Владимир Владиславович, Панкратьев Вячеслав Вячеславович, Баяндин Николай Иванович
- Расписание: с 10:00 до 17:30

День 1

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 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
- 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 радара 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»

День 2

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 треугольника 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»

День 3

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 содержащейся в нем информации. 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»

День 4

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»

День 5

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»

Стоимость участия

Стоимость участия в семинаре составляет **110000 руб.** с учетом всех налогов.

В стоимость обучения входит:

- Комплект авторских материалов
- Кофе-паузы
- Сертификат Moscow Business School
- Удостоверение о повышении квалификации

Преподаватели семинара

- **Креопалов Владимир Владиславович**

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

- **Панкратьев Вячеслав Вячеславович**

  Специалист в области корпоративной безопасности компании и управлении экономическими рисками

- **Баяндин Николай Иванович**

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