8 (495) 698-63-64
8 (800) 234-55-22
seminar@finkont.ru
www.finkont.ru

Политика безопасности предприятия

Слушатели программы получат практические знания о современных подходах построения и управления корпоративной безопасностью предприятия и основных подсистем – экономической, кадровой, информационной безопасностью. На занятиях будут рассматриваться как универсальные подходы к решению проблемы корпоративной безопасности, так и индивидуальные, основанные на специфике бизнеса.

Дата проведения: Открытая дата

Вид обучения: Курс повышения квалификации

Формат обучения: Дневной

Срок обучения: 5 дней

Продолжительность обучения: 40часов

Место проведения: г. Москва, ул. Золотая, д. 11, бизнес-центр «Золото», 5 этаж. Всем участникам высылается подробная схема проезда на семинар.

Для участников предусмотрено:

Методический материал, кофе-паузы.

Документ по окончании обучения: По итогам обучения слушатели, успешно прошедшие итоговую аттестацию по программе обучения, получают Удостоверение о повышении квалификации в объеме 40 часов (в соответствии с лицензией на право ведения образовательной деятельности, выданной Департаментом образования и науки города Москвы).

Для кого предназначен

Руководителей, директоров по безопасности, заместителей директора по безопасности, специалистов подразделений безопасности, внутренних аудиторов, директоров и специалистов по управлению персоналом, комплаенс-менеджеров, юристов.

Особенности программы

Корпоративная безопасность очень объемна по задачам, и быть узким специалистом по решению каждой из них невозможно. Но сотрудник, отвечающий за политику безопасности предприятия, и не должен быть узким специалистом во всех вопросах. Он должен уметь строить систему защиты, знать каких узких специалистов ему нужно найти, понимать, что нужно бизнесу от безопасности, применять на практике медицинский принцип «не навреди». Именно так. Безопасность не должна навредить бизнесу. И не должна существовать ради себя. Не должна раскручивать гендиректора на лишние деньги. Она должна быть оптимальна встроена в те бизнес-процессы, которые протекают в организации. И еще – безопасность не зарабатывает деньги, она их тратит, но позволяет защитить оставшуюся часть.
Политика безопасности строится на основе анализа рисков для организации, очень индивидуальна и стоит, как правило, из трех китах – политики экономической безопасности, политики кадровой безопасности и политики информационной безопасности. На этом пятидневном обучении каждый день будут закрывать одну тему, которая будет интересна как сотруднику, отвечающему за политику безопасности на предприятии, так и узкому специалисту по данному вопросу (риск-менеджеру, кадровику, юристу, специалисту по информационно-аналитической работе и т.д.). Слушателям будут выданы шаблоны локальных правовых актов по безопасности.

Это мероприятие можно заказать в корпоративном формате (обучение сотрудников одной компании).

Отдельные семинары в рамках курса

- Антикоррупционная политика предприятия. Предотвращение и урегулирование конфликтов интересов
- Кадровая безопасность предприятия

- Экономическая безопасность предприятия. Организация безопасной договорной работы

Участие возможно отдельно в каждом семинаре.

Программа обучения

День 1

Построение системы корпоративной безопасности. Безопасность как бизнес-функция.

- Международные акты в сфере корпоративной безопасности. Законодательство РФ в области защиты предпринимательской деятельности. Ведомственные, отраслевые требования и стандарты в области защиты бизнеса.
- Понятие безопасность в российском бизнесе. Постановочные вопросы перед созданием системы защиты бизнеса. Определение объектов защиты. Построение системы корпоративной безопасности. Безопасность как бизнес-функция. Может ли безопасность зарабатывать деньги и быть прибыльной?
- Особенности построения корпоративной безопасности в публичных компаниях, организациях с государственным участием, а также в иностранных компаниях.
- Особенности построения корпоративной безопасности в экосистемах, холдингах, а также в организациях, имеющих сложную организационную (территориально разделенную) структуру.
- Особенности построения корпоративной безопасности в современной политической и экономической ситуации, а также в условиях санкционного давления. Проведение антикризисных мероприятий. На чем можно, а на чем нельзя экономить.
- Особенность построения корпоративной безопасности при дистанционной (удаленной) работе, а также при отсутствии «контура безопасности».
- Особенность построения корпоративной безопасности в период проведения специальной военной операции.
- Использование на практике теории хаоса в корпоративной безопасности. Принятие управленческих решений по безопасности в условиях неопределенности.
- Использование искусственного интеллекта для решения задач в области корпоративной безопасности. Может ли ИИ заменить безопасника?
- Риск-ориентированный подход при обеспечении безопасности предприятия. Экономические, политические, регуляторные, правовые, финансовые и иные риски. Составление карты рисков. Определение допустимых пределов риска и вероятности наступления. Построение системы управления экономическими рисками. Страхование рисков.
- Обеспечение корпоративной безопасности при цифровой трансформации бизнес-процессов предприятия. Обеспечение безопасности принятие управленческих решений в условиях избыточности информации, ее неточности и недостоверности.
- Методика проведения аудита безопасности предприятия. Составление плана аудита на основе карты экономических рисков и формирования моделей угроз. Оценка защищенности организационной структуры бизнеса и основных бизнес-процессов.
- Экспертные методы оценки защищенности предприятия. Оценка бесперебойности функционирования бизнес-процессов предприятия при наступлении внештатных ситуаций. Создание кризисных планов. Наличие мониторинга безопасности предприятия.
- Активы предприятия, как основной объект защиты. Материальные и нематериальные активы. Основные направления защиты товарно-материальных ценностей. Защита деловой репутации, имиджа, технологий и иных нематериальных активов.
- Понятие комплаенс в законодательстве. Комплаенс как функция по обеспечению соответствия деятельности организации требованиям, налагаемым на нее российским и зарубежным законодательством, оценки рисков и обеспечению комплексной защиты организации;
- Определение субъектов корпоративной безопасности. Свое подразделение безопасности или аутсорсинговое обслуживание. Плюсы и минусы обоих вариантов. Распределение полномочий и зон ответственности между безопасниками и иными должностными лицами предприятия.
- Понятие собственная безопасность. Подразделение собственной безопасности, его задачи и функционал.
- Особенности договорных отношений с аутсорсинговыми организациями, предлагающими услуги по корпоративной безопасности. Правовое обеспечение взаимодействия с адвокатами, частными охранными организациями, детективами и иными организациями (лицами, имеющими особый статус).
- Правовая сторона деятельности подразделения безопасности. Закон и этика в работе. Подчинение, финансирование и оценка эффективности работы подразделения безопасности. Взаимодействие с акционерами, владельцами и руководителями подразделений. Структура подразделения безопасности.
- Компетенции и навыки специалиста по безопасности, востребованные в современных условиях.
- Корпоративные стандарты безопасности предприятия (КСБ). Совместимость КСБ с иными стандартами, действующими на предприятии. Включение процесс защиты бизнеса в процесс менеджмента непрерывности бизнеса.
- Разработка локальных актов по обеспечению безопасности предприятия (политики, инструкции, регламенты и т.д.). Создание сводов правил и поведений сотрудников. Внедрение на предприятии культуры безопасности.
- Обучение персонала требованиям КСБ. Организация взаимодействия с контрагентами и партнерами по бизнесу в связи с внедрением КСБ. Выполнение требований по безопасности в договорной работе и при взаимодействии с государственными органами.

День 2

Экономическая безопасность предприятия. Организация безопасной договорной работы.

- Понятие «безопасная договорная работа» на предприятии исходя из требований Гражданского кодекса РФ и иного законодательства.
- Организация безопасной договорной работы на предприятии. Инструкция о договорной работе. Централизация или делегирование полномочий. Процедуры внутреннего согласования. Выдача доверенностей. Работа с допсоглашениями.
- Распределение зон ответственности между подразделениями и должностными лицами предприятия в договорной работе. Матрица компетенций.
- Информатизация и цифровая трансформация бизнес-процессов, связанных с договорной работой и сделками. Принципы работы Big Data в договорной работе. Применение технологий искусственного интеллекта в договорной работе.
- Особенности договорной работы в условиях санкционного давления и неопределенности, а также в процессе антикризисного управления. Минимизация издержек. Безопасность закупок при дистанционных (удаленных) методах работы.
- Особенность безопасной договорной работы в период проведения специальной военной операции. Взаимодействие с организациями из недружественных стран.
- Виды риска при заключении различных типов договоров (продажа, оказание услуг, закупка, ремонт, строительство и т.д.).
- Налоговые риски в договорной работе. Понятие «коммерческая осмотрительность» в спорах с налоговыми органами. Требования нормативных правовых актов ФНС России, по самостоятельной оценке, налоговых рисков в сделках.
- Риски получения низкокачественных товаров и услуг в договорных отношениях. Определение критериев качества и оценки эффективности траты денег.
- Риски завышения цены в закупочной деятельности. Методы ценообразования, а также расчета начальной максимальной цены. Понятие «цена владения».
- Понятие комплаенс-рисков в договорной работе. Требования международного законодательства к минимизации комплаенс рисков в договорной работе.
- Оценка коррупционных рисков в договорной работе. Требования законодательства РФ по принятию предприятиями мер по предупреждению и противодействию коррупции. Антикоррупционные оговорки в договорах.
- Риски аффилированности работников предприятия с контрагентами. Понятие «конфликт интересов» в договорной работе. Информационно-аналитические и психологические способы выявления личной заинтересованности в сделке. Основы оперативной психологии.
- Риски нарушения требований антимонопольного законодательства в договорной работе. Понятие недобросовестная конкуренция. Картельный сговор. Создание на предприятии антимонопольного комплаенс.
- Мошеннические риски в договорной работе. Мошеннические схемы, применяемые в гражданско-правовых отношениях. Особенность мошенничества в различных видах бизнеса.
- Риски нарушения информационной безопасности в договорной работе. Соглашения о конфиденциальности. Защита авторских прав, охрана интеллектуальной собственности и иных нематериальных прав при взаимоотношении с контрагентами.
- Риски, связанные с выполнением требований федерального закона № 115-ФЗ. Понятие «подозрительная сделка» в документах Центрального банка и Росфинмониторинга. Признаки, указывающие на необычный характер сделки.
- Организация конкурентных закупок на предприятии. Основные требования федеральных законов № 44-ФЗ и № 223-ФЗ к безопасной договорной работе.
- Особенности построения безопасной договорной работы при выполнении государственного оборонного заказа.
- Методы анализа надежности контрагента. Признаки опасности в деятельности организации. Применение метода Due Diligence при оценке компании. Методы оценки финансовой устойчивости и платежеспособности контрагента.
- Анализ безопасности коммерческих предложений. Изучение инициаторов проекта, их интересы и деловую репутацию. Верификация представителей. Изучение механизма получения прибыли. Анализ первого контакта. Поведенческие аспекты при оценке ненадежности контрагента.
- Правовая экспертиза как элемент безопасной договорной работы. Задачи правовой экспертизы. Стандартизация форм договора. Штрафные санкции за невыполнение условий договора. Типовые «подводные камни» в условиях договора.
- Противодействие откатам, неправомерному выводу активов, коммерческому подкупу и иным противоправным действиям в договорной работе.
- Организация контроля за выполнением условий договора как элемент безопасной договорной работы. Мониторинг информации по контрагентам. Создание алгоритмов реагирования на невыполнение контрагентами договорных обязательств.
- Ведение эффективной претензионно-исковой работы. Мониторинг неплатежей. Понятие форс-мажор в период кризиса и пандемии. Медиаторство как способ досудебного урегулирования спора. Психологические, юридические, имиджевые и иные способы воздействия на должника.
- Воздание эффективного внутреннего контроля за договорной работой на предприятии. Система внутреннего контроля по модели COSO. Компоненты по модели COSO. «Магический куб» COSO.
- Система внутренних проверок, финансовых расследований и иные процедуры в договорной работе.

День 3

Кадровая безопасность предприятия. Обеспечение безопасности при дистанционной (удаленной) работе.

- Понятие кадровая безопасность. Виды оформления юридических взаимоотношений организации и физических лиц.
- Актуальные изменения в трудовом и гражданском законодательстве, связанные с кадровой безопасностью.
- Основные требования безопасности при заключении гражданско-правовых договоров с физическими лицами. Особенность работы с «самозанятыми» и работниками, имеющими статус индивидуального предпринимателя. Аутстафинг (лизинг

персонала) как вариант кадрового обеспечения предприятия.
- Основные риски и угрозы, исходящие от работников, варианты их реализации и возможные направления защиты. Противоправные действия, ответственность за которые предусмотрена законодательством и основные способы защиты от них.
- Анализ кадровых рисков, связанных с проведением специальной военной операции. Приостановка трудовых отношений с мобилизованными и добровольцами. Безопасные отношения с участниками СВО. Взаимоотношения предприятий с сотрудниками, покинувшими места постоянного проживания (релоцировавшимися).
- Особенность обеспечения кадровой безопасности в условиях включения в состав России новых территорий. Особенности заключения трудовых и гражданско-правовых отношений с лицами, прибывающими с новых территорий.
- Актуальные изменения в воинском учете для организаций. Пошаговый алгоритм действий по формированию воинского учета на предприятии, исходя из новых требований.
- Основные нормы трудового законодательства, в части регламентации труда дистанционных (удаленных) работников. Обеспечение кадровой безопасности при дистанционных (удаленных) методах работы.
- Кадровая безопасность в условиях проведения антикризисных мероприятий и кадрового голода. Требования государственных органов по сохранению кадрового потенциала предприятий;
- Порядок взаимодействия структурных подразделений и должностных лиц предприятия по вопросам кадровой безопасности. Зоны ответственности подразделений (матрица компетенций).
- Создание и актуализация локальной правовой базы предприятия. Ознакомление и получение согласия от работника. Нормы трудового договора по вопросам кадровой безопасности.
- Проверка персонала при приеме на работу. Сбор и анализ информации о кандидате по методу SMICE. Порядок анализа резюме, трудовой книжки, дипломов, характеристик и иных официальных документов. Анкеты для кандидатов на работу;
- Официальные и неофициальные источники по сбору информации о кандидатах на работу. Использование ресурсов Интернета для сбора информации о кандидате.
- Процедуры принятия на работу лиц, ранее занимавших должности государственной и муниципальной службы. Уведомление и получение согласия на их трудоустройство.
- Правила проведения индивидуальных бесед с кандидатами на работу. Формирование психологических портретов. Психологические особенности кандидатов, представляющих опасность для предприятия. Использование ролевых игр для моделирования поведения человека в различных ситуациях.
- Признаки опасности у кандидата на работу. На что обратить внимание в «проверочных меро-приятиях». Формирование модели потенциального нарушителя, применительно к различным должностям.
- Российское и международное законодательство по обработке персональных данных. Алгоритм действий по выполнению на предприятии требований по обработке и защите персональных данных.
- Актуальные изменения в законодательстве о персональных данных. Особенности обработки персональных данных, разрешенных субъектом персональных данных для распространения. Введение уголовной ответственности за незаконную обработку персональных данных.
- Процедуры проведения внутренних расследований по фактам разглашения (утечки) персональных данных работников.
- Превентивные мероприятия по предотвращению противоправных действий со стороны работников. Создание стимулов и мотивационных факторов, направленных на усиление лояльности. Реализация персональной ответственности.
- Выполнение требований законодательства по противодействию коррупции. Антикоррупцион-ная политика предприятия. Принятие кодекса этики и служебного поведения работников как элемент кадровой безопасности. Формирование корпоративной культуры.
- Понятие конфликт интересов в трудовых отношениях. Меры по предупреждению и урегулированию конфликта интересов на предприятии.
- Повышение профессионализма работников как элемент кадровой безопасности. Независимые центры оценки квалификации. Процедуры аттестации работников.
- Создание системы обучения работников действиям во внештатных и чрезвычайных ситуациях (пожар, стихийное бедствие, теракт, диверсия и др.).
- Построение кадровой безопасности с различными группами риска. Работа с «жалобщиками» и иными работниками, злоупотребляющими своими правами.
- Оценка стиля работы должностных лиц с позиции кадровой безопасности.
- Комплаенс-контроль работников, занимающих должности с коррупционными рисками. Анализ полномочий и результатов работы персонала на предприятии. Политика кадровой безопасности по минимизации комплаенс-рисков.
- Создание обратной связи на предприятии. Организация телефонов доверия и горячей линии. Применение методов «тайного покупателя».
- «Оперативная психология». Анализ личности человека и формирование моделей его поведения. Методы выявления лжи в процессе коммуникаций (профайлинг). Анализ языка тела. Ма-нейруляции в общении и технологии убеждения.
- Основные требования трудового законодательства при привлечении работника к дисциплинарной ответственности.
- Привлечение работника к материальной ответственности. Процедуры и порядок проведения инвентаризации. Договор о полной материальной ответственности. Особенности проведения инвентаризации при дистанционной работе.
- Особенность проведения внутренних проверок и расследований по наиболее характерным противоправным действиям сотрудников (хищение, «откат», мошенничество, разглашение информации, конфликт интересов, увод клиентов и т.д.).
- Использование полиграфа (детектора лжи) при проведении внутренних проверок и расследований. Правовая и организационная сторона вопроса. Можно ли обмануть полиграф?
- Документальное оформление результатов внутренних проверок и расследований. Возможность использования результатов в качестве доказательства вины работника. Взаимоотношение с правоохранительными органами при возбуждении уголовных

дел.
- Процедуры увольнения работников с позиции безопасности. Особенности увольнения работников, которые могут представлять угрозу для организации после увольнения.
- Трудовые споры. Безопасные взаимоотношения с трудовой инспекцией и прокуратурой по вопросам нарушения трудового законодательства. Судебная защита интересов предприятия при конфликтах с работниками.
- Позиции судов при рассмотрении трудовых споров о неправомерном увольнении. Обзор судебной практики 2025 – 2026 годов. Методы, применяемые адвокатами для защиты своих клиентов в трудовых спорах.

День 4

Защита конфиденциальной информации на предприятии. Цифровая трансформация информационной безопасности.

- Особенности деятельности предприятия в условиях цифровой трансформации экономики. Защита информации, защита информационной инфраструктуры и информационное противоборство как три составляющих безопасности в цифровом мире.
- Понятие критическая информационная инфраструктура в российском законодательстве, процедуры категорирования и основные требования по ее защите.
- Защита конституционных прав физических лиц при цифровой трансформации. Неприкосновенность частной жизни, тайна телефонных переговоров, почтовых и иных сообщений. Процедуры использования технических средств, предназначенных для негласного получения информации.
- Понятие культура информационной безопасности при цифровой трансформации. Культура информационной безопасности как составная часть корпоративной безопасности. Этические нормы в менеджменте информационной безопасности.
- Политика информационной безопасности как основа системы менеджмента ИБ. Цели и задачи Политики информационной безопасности. Общая структура политики информационной безопасности.
- Законодательство РФ в области защиты информации. Понятие конфиденциальная информация и конфиденциальность информации. Информация, доступ к которой не может быть ограничен.
- Источники конфиденциальной информации. Виды и формы представления конфиденциальной информации.
- Основные направления защиты конфиденциальной информации. Системный подход к защите информации.
- Правовые, организационные, режимные и инженерно-технические мероприятия по защите конфиденциальной информации. Кибербезопасность предприятия. Создание внутриобъектового и пропускного режимов на предприятии. Физическая защита охраняемых информационных ресурсов.
- Работники организации как основной канал утечки конфиденциальной информации. Политика кадровой безопасности. Мероприятия по предотвращению разглашения работниками конфиденциальной информации.
- Особенность защиты информации при использовании на предприятии дистанционных (удаленных) работников.
- Особенность защиты конфиденциальной информации в условиях проведения специальной военной операции, санкционного давления и программ импортозамещения.
- Требования по защите конфиденциальной информации в гражданско-правовых отношениях. Соглашение о конфиденциальности перед проведением переговоров.
- Виды юридической ответственности за разглашение конфиденциальной информации, а также за ее незаконное получение. Уголовная, административная и гражданско-правовая ответственность. Обзор судебной практики.
- Профессиональная тайна как составная часть конфиденциальной информации Законодательство РФ в области защиты профессиональных тайн (врачебная тайна, нотариальная тайна, банковская тайна, адвокатская тайна и т.д.).
- Служебная тайна как составная часть конфиденциальной информации. Законодательство РФ в области защиты служебной тайны. Правовой режим применения ограничения доступа к служебной информации. Правила работы с документами «ДСП» в коммерческих структурах.
- Защита коммерческой информации на предприятии. Процедуры создания режима коммерческой тайны. Понятие обладатель коммерческой тайны, его права и обязанности.
- Понятие разглашение коммерческой тайны в российском законодательстве. Обязательства работников по сохранению коммерческой тайны предприятия и отказ от использования ее в личных целях. Сохранность коммерческих секретов работниками после увольнения.
- Ограничение доступа к коммерческой тайне и защита информации как обязательный элемент режима коммерческой тайны. Системный подход к защите информации. Организационные, кадровые, технические, режимные и иные мероприятия по защите коммерческой тайны.
- Особенность работы с коммерческой информацией, представленной в электронном виде. Понятие электронный документ. Электронная подпись. Процесс цифровизации коммерческой тайны.
- Соблюдение режима коммерческой тайны в договорных отношениях с юридическими и физическими лицами. Конфиденциальность полученной контрагентом информации как условие договора. Компенсация ущерба и штрафные санкции за разглашение коммерческой тайны или незаконное использование ее в личных целях.
- Процедуры предоставления информации, составляющей коммерческую тайну предприятия государственным органам. Понятие мотивированное требование государственного органа. Обязанность государственных органов по охране конфиденциальности полученной информации.
- Защита персональных данных на предприятии. Основные требования ФЗ «О персональных данных» и нормативных актов регуляторов (Роскомнадзор, ФСТЭК России, ФСБ России и т.д.), регламентирующие порядок обработки персональных данных. Изменения в требованиях по обработке персональных данных, принятых в 2025 году.
- Новации в трансграничной передаче персональных данных. Процедуры уведомления Роскомнадзора о трансграничной передаче персональных данных.

- Понятие оператор персональных данных, его права и обязанности, порядок регистрации. Реестр операторов, осуществляющих обработку персональных данных. Уведомление об обработке (о намерении осуществлять обработку) персональных данных.
- Понятие субъект персональных данных, его права и обязанности в соответствии с российским законодательством.
- Формирование правового режима защиты персональных данных. Перечень мер по защите персональных данных.
- Пошаговый алгоритм действий по выполнению предприятием требований законодательства по обработке персональных данных.
- Требования к обеспечению безопасности персональных данных, при их обработке в информационных системах персональных данных, в зависимости от типа угроз.
- Административный регламент исполнения государственной функции по осуществлению государственного контроля за соответствием обработки персональных данных требованиям законодательства.
- Введение уголовной ответственности за незаконную обработку персональных данных и административную ответственность за утечки персональных данных у оператора.
- Методики проведения внутренних расследований по инцидентам, связанным с нарушением конфиденциальности информации на предприятии. Плановые и внеплановые проверки.
- Виды юридической ответственности (уголовная, гражданско-правовая, дисциплинарная и иная) за разглашение конфиденциальной информации, использование ее в личных целях, а также за ее незаконное получение. Необходимые и достаточные условия для наступления ответственности.

День 5

Антикоррупционная политика предприятия. Предотвращение и урегулирование конфликтов интересов.

- Понятие «коррупция» в международном законодательстве. Конвенции ООН по противодействию коррупции и подкупу должностных лиц.
- Основные требования международного стандарта ИСО 37001 - 2025 «Системы менеджмента противодействия коррупции – требования и рекомендации по применению» и ИСО 37301 «Система управления соответствием – требования с руководством по применению».
- Понятие «коррупция» и «коррупционное правонарушение» в российском законодательстве. Положения ФЗ «О противодействии коррупции», являющиеся обязательными для выполнения организациями, независимо от формы собственности. Методические рекомендации по их выполнению. Новации антикоррупционного законодательства 2025-2026 годов.
- Особенности исполнения обязанностей, соблюдения ограничений и запретов в области противодействия коррупции отдельными категориями граждан в период проведения специальной военной операции, предусмотренные Указом Президента РФ от 29.12.2022 года № 968.
- Меры по предупреждению коррупции и трудовое законодательство РФ. Различия в правовом статусе работников организаций частного и государственного секторов, обуславливающие недопустимость отдельных мер по предупреждению коррупции в организациях частного сектора в связи с положениями трудового законодательства РФ.
- Основные требования профессионального стандарта "Специалист в сфере предупреждения коррупционных правонарушений», утвержденного приказом Минтруда России от 08.08.2022 № 472н. Образование, компетенции и навыки работника, ответственного за противодействие коррупции в организации.
- Меры по предупреждению коррупции и законодательство РФ о персональных данных. Особенности построения мер по предупреждению коррупции в организации с учетом требований законодательства РФ о персональных данных.
- Основные нормы Антикоррупционной хартии российского бизнеса и ее дорожная карта. Порядок и процедуры присоединения к хартии.
- Понятие «комплаенс» в международном и российском законодательстве. Требования приказов Росимущества по комплаенс процедурам в акционерных обществах с государственным участием.
- Институциональный статус подразделения (должностного лица) по профилактике коррупционных и иных правонарушений. Подчинение, основные права и обязанности. Взаимодействие с риск-менеджерами, службой внутреннего контроля и аудита, и иными подразделениями.
- Примерный перечень действий должностных лиц организации, которые могут квалифицироваться как коррупция и коррупционное правонарушение по международному и российскому законодательству.
- Антикоррупционные требования и ограничения, налагаемые на бывших государственных и муниципальных служащих при заключении ими трудовых или гражданско-правовые договоров.
- Ответственность юридических и физических лиц за коррупционные правонарушения и непринятия мер по противодействию коррупции. Возможность привлечения к дисциплинарной ответственности работника за нарушение антикоррупционного законодательства.
- Методики оценки бизнес-процессов с позиции коррупционных рисков. Составление карты коррупционных рисков в организации. Разработка и введение специальных антикоррупционных процедур.
- Антикоррупционные коллегиальные органы в организации, порядок формирования и принятия решений. Организационно-техническое и документационное обеспечение деятельности органа.
- Формирование антикоррупционной политики организации. Особенности проведения антикоррупционной политики на предприятиях различных сфер бизнеса.
- Планирование деятельности в области противодействия коррупции в организации. Подготовка локальных нормативных правовых и иных актов в области противодействия коррупции.
- Использование искусственного интеллекта и иных информационных технологий в выявлении коррупционных схем и минимизации коррупционных рисков. Новеллы информационной политики в сфере противодействия коррупции. Технические средства контроля за действиями персонала, позволяющие вычислять личную заинтересованность и иные коррупционные признаки.

- Порядок проведения антикоррупционных мероприятий в процессе антикризисного управления. Минимизация издержек. Минимизация коррупционных рисков при использовании дистанционных (удаленных) работников.
- Понятие «конфликт интересов» в антикоррупционном и ином законодательстве. Кто обязан предпринимать меры по предотвращению и урегулированию конфликтов интересов. Декларации о конфликте интересов.
- Методика анализа ситуации, попадающей под понятие «конфликт интересов». Применение мер дисциплинарного воздействия, включая увольнение, к участникам конфликта интересов.
- Кодекс этики и корпоративного поведения в организации как составная часть антикоррупционной политики на предприятии. Этичность в действиях работника при выполнении должностных обязанностей, общении с клиентами и контрагентами, а также в межличностном общении в коллективе.
- Понятие профессиональной этики в законодательстве РФ. Требования кодексов профессиональной этики, применительно к различным профессиям.
- Культура информационной безопасности как элемент этики и корпоративного поведения. Конфиденциальность и этика при распространении информации в социальных сетях и иных информационных ресурсах интернета.
- Правила, регламентирующие обмен подарками и знаками делового гостеприимства;
- Минимизация коррупционных рисков при управлении персоналом. Процедуры приема-увольнения работников. Политика кадровой безопасности. Антикоррупционные процедуры при делегировании полномочий и трудоустройстве родственников.
- Минимизация коррупционных рисков в закупках. Регламентация процедур выбора контрагентов и взаимоотношения с ними. Проверки контрагентов (Due diligence). Вычисление аффилированности и личной заинтересованности в сделках. Антикоррупционный аудит отдельных операций и сделок.
- Антикоррупционная экспертиза проектов нормативных правовых актов организации. Включение антикоррупционных оговорок и положений в гражданско-правовые и трудовые договора.
- Создание процедур информирования работодателя о ставшей известной работнику информации о случаях совершения коррупционных правонарушений другими работниками, контрагентами предприятия или иными лицами. Защита лиц, сообщивших о коррупционных правонарушениях.
- Возможные подходы к информированию, обучению и консультированию работников в рамках профилактики коррупции.
- Организация системы внутреннего контроля и аудита как элемент антикоррупционной политики организации. Проведение внутренних расследований по фактам нарушения антикоррупционной политики организации.
- Противодействие фальсификации бухгалтерской (финансовой) отчетности как средство противодействия коррупции.
- Деятельность органов прокуратуры по надзору за исполнением законодательства о противодействии коррупции. Деятельность Минтруда РФ в сфере методического обеспечения противодействия коррупции.
- Взаимодействие предприятия с государственными правоохранительными, надзорными и иными государственными органами, а также общественно-политическими организациями по вопросам профилактики и противодействия коррупции.

Преподаватели

КОМАРОВ Вадим Николаевич

Эксперт по корпоративной безопасности. Один из ведущих экспертов в России и СНГ по экономической, кадровой, психологической, информационной безопасности предприятий.
В настоящее время является советником по безопасности ГК «Невада», ГК «РобоФинанс», ОАО «ВРХ», ТОО «Тоймаркет». Более четырех лет работает на рынке консалтинга в сфере обеспечения безопасности. Является квалифицированным экспертом по системам безопасности предприятий.
Входит в список рейтинга «5000 наиболее популярных и узнаваемых лиц в России» по мнению Аналитического центра Brand Analytics.

Опыт работы:

- 2006- н.в. — ЗАО «Технологии Безопасности Бизнеса», генеральный директор.
- 2002–2006 гг. — ЗАО «Центр Безопасности Бизнеса», генеральный директор.
- 1993–2002гг. — Гипермаркет «Ашан», торговая сеть «Тати», Восточно-Европейский Инвестиционный Банк (ВЕИБ), начальник службы безопасности.

Сфера профессиональных компетенций:

Организация и руководство службами безопасности и внутреннего контроля; проектирование систем комплексной безопасности для предприятий различного рода деятельности; разработка и обоснование системы внутреннего контроля предприятия (аудит, ревизии, инвентаризации, управленческий контроль); организация с нуля системы информационной и кадровой безопасности на предприятии; оценка системы внешних и внутренних рисков и угроз; нормативное обеспечение деятельности подразделений безопасности и внутреннего контроля; информационно-аналитическое обеспечение деятельности системы безопасности и системы внутреннего контроля; организация системы предотвращения внутрикорпоративного мошенничества и хищений на предприятии; разработка систем экономической разведки и контрразведки на предприятии.

Публикации:

Автор публикаций в профессиональных периодических СМИ: журналы «Директор по безопасности», «Мое дело», «Российская торговля», «Справочник руководителя предприятия», газеты «Безопасность и торговля», «Технологии Безопасности Бизнеса».

Корпоративные клиенты:

Энергетическая Корпорация «ОЭК» (Москва), Холдинг «Инвенсис» (Лондон, Москва), Топливно – энергетическая Корпорация ДТЭК (Донецк), Топливно – энергетическая Корпорация «Метинвест» (Донецк), Холдинг «РЕННА» (Москва, Краснодар, Белгород), Холдинг «АБИ-Продакт» (Владимир, Калининград), ОАО «ВРХ» (Кострома, Москва), Банк «Пробизнесбанк» (Москва), Банк «Росэксимбанк» (Москва), ГК "Национальный Кредит" (Москва), Компания «Ямское Поле» (Москва), Компания "Яндекс" (Москва, Рязань), Завод «Сан-Гобен-Вебер» (Подольск), Комбинат АКК (Белгород), Завод «Моссельмаш» (Москва), Автомобильный завод «Урал» (Миасс, Челябинская обл.), Деревообрабатывающий завод «Ресурс» (Тамбов), Деревообрабатывающий комбинат «Солдек» (Вологда), Климовский трубный завод (Климовск), Компания БиЛайн (Москва), Комбинат «Муром» (Муром), Торговая компания «Магнум» (Алматы), Торговая компания «Сибпластком» (Новосибирск), Торговая компания «КВАДРАТ» (Киров), Торговая компания «Стар» (Ереван), Торговая компания «Золотое яблоко» (Екатеринбург), Торговая компания «Л Этуаль» (Москва), Торговая компания «Ижтрейдинг» (Ижевск), Торговая компания "М-видео" (Москва).

ПАНКРАТЬЕВ Вячеслав Вячеславович

Полковник юстиции в запасе, заведующий кафедрой безопасности в Университете государственного и муниципального управления, эксперт в области корпоративной безопасности и управлению рисками, преподаватель-консультант, автор и ведущий обучающих программ (MBA, Executive MBA, открытые семинары, корпоративные мероприятия, индивидуальные консультации) по проблемам защиты бизнеса более чем в десяти учебных заведениях России.Автор книг и методических пособий по безопасности предпринимательской деятельности. Независимый консультант в области корпоративной безопасности. Разработчик методик аудита безопасности предприятия и создания КСБ – корпоративных стандартов безопасности.

Образование:

Окончил Академию ФСБ, Высшее военно-политическое училище пограничных войск КГБ СССР.

Опыт работы:

Имеет 28-тилетний опыт работы в спецслужбах КГБ, ФАПСИ, ФСО.

Корпоративные клиенты:

Среди корпоративных клиентов такие компании как: ОАО «Газпром» (корпоративный университет), ОАО «МТС» (корпоративный университет), ОАО «Мегафон», ОАО «Электрокабель», Группа компаний Armadillo, Группа компаний «Биотек», Группа компаний БТБ (Безопасные Технологии Бизнеса), Группа компаний Белагро, АФК «Система», FM Логистик, Московский залоговый банк.

Публикации:

Имеет публикации на тему защиты информации, (издательство «Арсин», данное издательство специализируется на выпуске спецлитературы). Опубликованы методические пособия «Практическое пособие по информационной безопасности предпринимательской деятельности», «Практические рекомендации по безопасности бизнеса».