ФИНКОНТ
учебный центр

+7 (495) 698-63-64
8 (800) 234-55-22

seminar@finkont.ru
www.finkont.ru

Политика безопасности предприятия

Слушатели курса 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: 16 - 20 сентября 2024 с 10:00 до 17:30

Артикул: MC22030

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.

Стоимость участия: 63 900 руб.

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 курсе 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 курса будут выданы шаблоны локальных правовых актов по безопасности.

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

Отдельные семинары в рамках курса

- Экономическая безопасность предприятия. Организация безопасной договорной работы
- Антикоррупционная политика предприятия. Предотвращение и урегулирование конфликтов интересов
- Кадровая безопасность предприятия

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;
- международный опыт и корпоративные стандарты по защите компаний от экономических преступлений. Международные акты по борьбе с мошенничеством (UK Bribery Act, Foreign Corrupt Practices Act, Закон Сарбейнза — Оксли);
- 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;
- особенность построения корпоративной безопасности при дистанционной (удаленной) работе, а также при отсутствии «контура безопасности»;
- использование на практике теории хаоса в корпоративной безопасности. Принятие управленческих решений по безопасности в условиях неопределенности;
- 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;
- обеспечение безопасности предприятия в условиях кризиса и пандемии, а также при антикризисном управлении. На чем можно, а на чем нельзя экономить;
- 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 элементов искусственного интеллекта при выборе контрагента;
- 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;
- виды риска при заключении различных типов договоров (продажа, оказание услуг, закупка, ремонт, строительство и т.д.);
- налоговые риски в договорной работе. Понятие «должная 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;
- 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 форсмажор в период кризиса и пандемии. Медиаторство как способ досудебного урегулирования спора. Психологические, юридические, имиджевые и иные способы воздействия на должника;
- создание 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. Основные нормы трудового и гражданско-правового законодательства по вопросам кадровой безопасности.

- 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.
- Основные изменения трудового законодательства, вступившие в силу в 2023-2024 годах. Анализ рисков, связанных с частичной мобилизацией. Приостановка трудовых отношений с мобилизованными и добровольцами. Взаимоотношения предприятий и военных комиссариатов. Взаимоотношения предприятий с сотрудниками, покинувшими места постоянного проживания (релоцировавшимися).
- Особенность обеспечения кадровой безопасности в условиях проведения специальной военной операции и включения в состав России новых территорий. Особенности заключения трудовых и гражданско-правовых отношений с лицами, прибывающими с новых территорий.
- 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. 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 мероприятиях». Формирование модели потенциального нарушителя, применительно к различным должностям.
- Российское законодательство по обработке персональных данных. Алгоритм действий по выполнению на предприятии требований по защите персональных данных.
- Изменения в законодательстве о персональных данных, вступившие в силу в 2022-2023 годах. Понятие компрометация персональных данных работников и уведомление об этом Роскомнадзор. Особенности обработки персональных данных, разрешенных субъектом персональных данных для распространения.
- Особенности трансграничной передачи персональных данных, вступившие в силу с 1 марта 2023 года. Процедуры уведомления Роскомнадзора о трансграничной передаче персональных данных.
- Процедуры проведения внутренних расследований по фактам компрометации персональных данных работников.
- Превентивные мероприятия по предотвращению противоправных действий со стороны работников. Создание стимулов и мотивационных факторов, направленных на усиление лояльности. Реализация персональной ответственности.
- 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 руководства 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 предприятия. 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. Манипуляции в общении и технологии убеждения.
- Основные требования трудового законодательства при привлечении работника к дисци-плинарной ответственности.
- Привлечение работника к материальной ответственности. Процедуры и порядок проведения инвентаризации. Договор о полной материальной ответственности. Особенности проведения инвентаризации при дистанционной работе.
- 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 2022 – 2023 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, а также релоцировавшихся в другие страны работников;
- особенность-защиты конфиденциальной информации-в условиях 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 2022-2023 годах;
- новации в трансграничной передаче персональных данных, вступившие в силу с 1 марта 2023 года. 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;
- 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.

- Требования законодательства РФ по проведению антикоррупционной политики в организациях. Основные положения ФЗ «О противодействии коррупции» и Национального плана противодействия коррупции на 2021-2024 годы утвержденного Указом Президента РФ от 16.08.2021 № 478.
- 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.
- Институциональный статус подразделений (должностных лиц) по профилактике коррупционных и иных правонарушений. Подчинение, основные права и обязанности. Взаимодействие с риск-менеджерами, службой внутреннего контроля и аудита, и иными подразделениями.
- Анализ коррупционных рисков в организациях. Методики оценки коррупционных рисков. Процесс управления коррупционными рисками. Составление карты коррупционных рисков. Определение «критических точек» и «коррупциогенных факторов».
- Примерный перечень действий должностных лиц организаций, которые могут квалифицироваться как коррупция по российскому и международному законодательству.
- Определение антикоррупционных мер и формирование антикоррупционной политики в организациях. Привязка антикоррупционных мер к реальным коррупционным схемам.
- Использование цифровых технологий в противодействии коррупции. Новеллы информационной политики в сфере противодействия коррупции. Технические средства контроля за действиями персонала, позволяющие вычислять личную заинтересованность и иные коррупционные признаки.
- Понятие «конфликт интересов» в антикоррупционном и ином законодательстве. Обязанность отдельных должностных лиц принимать меры по предотвращению и урегулированию конфликта интересов.
- Методика анализа ситуации, попадающей под понятие «конфликт интересов». Порядок предотвращения и урегулирования конфликта интересов. Применение мер дисциплинарного воздействия к его участникам.
- Права должностных лиц организаций по сбору, накоплению и обработке персональных данных, позволяющих вычислять личную заинтересованность у работников и иных лиц, которая может привести к конфликту интересов.
- Понятие профессиональной этики в законодательстве РФ. Требования кодексов профессиональной этики, применительно к различным профессиям.
- Создание кодека этики и служебного поведения, положения о конфликте интересов, положения о подарках и знаках делового гостеприимства и иных локальных актов, регламентирующих антикоррупционную политику.
- Возможные подходы к профилактике коррупционных правонарушений при осуществлении закупок товаров, работ, услуг, проводимых в соответствии с требованиями федеральных законов от 05.04.2013 г. № 44-ФЗ и от 18.07.2011 г № 223-ФЗ. Антикоррупционный аудит отдельных операций и сделок с повышенными коррупционными рисками. Антикоррупционная оговорка в текстах договоров.
- Минимизация коррупционных рисков в кадровой работе и принятии управленческих решений. Антикоррупционные процедуры при делегировании полномочий и трудоустройстве родственников. Антикоррупционные положения в трудовых договорах работников.
- Методика проведения антикоррупционной экспертизы нормативных правовых актов (проектов актов) в организациях с государственным участием.
- Каналы получения информации и защита заявителей, сообщивших о фактах коррупции. Организация работы горячей линии и телефонов доверия.
- Организация системы внутреннего контроля и аудита как элемент антикоррупционной политики.
- Специальные обязанности отдельных должностных лиц, предусмотренные антикоррупционным и трудовым законодательством. Уведомление об обращениях в целях склонения к совершению коррупционных правонарушений.
- Представление отдельными должностными лицами организаций сведений о доходах (расходах), об имуществе и обязательствах имущественного характера. Методические рекомендации Минтруда России по вопросам представления сведений и заполнения декларации.
- Запреты и ограничения, предусмотренные антикоррупционным законодательством для отдельных должностных лиц организаций.
- Антикоррупционные требования и ограничения, налагаемые на бывших государственных и муниципальных служащих при заключении ими трудовых или гражданско-правовые договоров.
- Порядок проведения внутренних проверок и расследований по фактам совершения работниками коррупционных правонарушений или нарушения требований антикоррупционного законодательства.

- Меры ответственности за коррупционные правонарушения и непринятие мер по противодействию коррупции. Порядок привлечения к ответственности должностных лиц организаций.
- Порядок контроля и надзора за соблюдением законодательства о противодействии коррупции. Полномочия органов прокуратуры по надзору за исполнение антикоррупционного законодательства. Деятельность Минтруда РФ в сфере методического обеспечения противодействия коррупции.

Преподаватели

ВЛАСЕНКО Михаил Николаевич

Независимый эксперт Минюста России по антикоррупционной экспертизе. Эксперт Международной контртеррористической тренинговой ассоциации (МКТА) International Counter Terror Training Association (INT 12671).

Независимый консультант по реинжинирингу и построению систем корпоративной безопасности. Кандидат экономических наук, доцент, профессор РАЕ, доцент кафедры «Безопасности и информационных технологий» Национального исследовательского университета МЭИ, доцент кафедры «Анализа рисков и экономической безопасности» Финансового университета при Правительстве РФ, полковник запаса.

Сфера профессиональных компетенций:

- Построение системы экономической безопасности компании, холдинга, отрасли.
- Экономика безопасности организации. Повышение эффективности системы экономической безопасности компании.
- Оптимизация функционирования систем безопасности различного уровня.
- Информационная и бизнес-аналитика.
- Создание эффективных систем управления персоналом.
- Психология безопасности, снижение и профилактика конфликтов.
- Противодействие корпоративному мошенничеству.
- Расследования корпоративных происшествий.
- Анализ и оценка рисков в деятельности организации. Создание систем риск-менеджмента.
- Обеспечение защиты информации от утечки по техническим каналам. Инженерно-техническая защита объектов экономической деятельности.

Образование:

2009 — Аспирантура ВГНА Минфина России.
Кандидат экономических наук (08.00.05).
2006 — Московский энергетический институт. «Экономика и управление на предприятии».
1994 — Военная академия им. Ф.Э. Дзержинского, г. Москва.
1986 — Рязанское ВВКУС им. Маршала М.В. Захарова.
За время научно-педагогической и консультационной деятельности прошел 14 курсов повышения квалификации и профессиональной переподготовки по родственной тематике.

Опыт работы:

2016–2006 — ВГНА Минфина России, далее Финансовый университет при Правительстве РФ. Доцент кафедры.
2016–2000 — Национальный исследовательский университет МЭИ. Доцент кафедры, помощник директора.
С 1999 по настоящее время – независимый эксперт МКТА.
2000–2006 — Директор охранно-сыскного агентства, руководитель департамента экономической безопасности машиностроительного холдинга, крупной торговой сети.
1986–2000 — Прохождение военной службы на командных должностях в ВС СССР и ВС РФ.

Публикации:

Публикации на темы региональной и корпоративной безопасности, в издательстве «ЮРАЙТ».

Методические пособия «Экономика безопасности», «Экономика защиты информации», «Управления рисками предприятия», «Кадровая безопасность», «Экономическая безопасность», «Подготовка специалистов в сфере экономической безопасности», всего более 20.

Более 50 статей и опубликованных тезисов выступлений по профильной тематике.

Корпоративные клиенты:

ЦБ РФ, «Сбербанк России», Министерство экономики МО, ОАО «Газпром», АФК «Система», «РусГидро», «Федеральное агентство по туризму», ОАО «Норильский никель», «Роснефть», «Московский метрополитен», «Мосгортранс» и многие другие.

КРЕОПАЛОВ Владимир Владиславович

Кандидат технических наук, эксперт-практик в области безопасности предпринимательской деятельности, доцент кафедры информационной безопасности Московского государственного университета экономики.

Сфера профессиональных интересов:

- Обеспечение личной охраны, проверка персонала компании, информационно-аналитическая работа.
- Обеспечение и контроль безопасности бизнеса и личности.
- Организация служб безопасности в частных структурах.
- Конкурентная разведка.
- Информационная безопасность.

Образование:

2008 г. — Центральный научно-исследовательский институт экономики, информатики и систем управления, аспирантура.
2004 г. — Институт безопасности бизнеса и личности Московского энергетического института, управление экономической безопасностью на предприятии.
2008 г. — Центральный научно-исследовательский институт экономики, информатики и систем управления, аспирантура, диссертация по специальности: «Системный анализ, управление и обработка информации», аспирантура.
1990 г. — Высшее техническое.

Опыт работы:

2002-— н.-в. —-ФНПЦ ОАО «Красногорский завод-им. С.-А.-Зверева», помощник заместителя генерального директора по-безопасности и-режиму, руководитель подразделения экономической безопасности.

1998-— Частное охранное предприятие, руководитель.

Преподавательская деятельность:

Автор и преподаватель курсов по практическим аспектам комплексной безопасности предпринимательской деятельности, автоматизированных систем, экономическим аспектам и методам защиты информации.

Публикации:

Автор ряда статей по вопросам конкурентной разведки и организации соответствующих служб на промышленных предприятиях.

Автор учебных пособий по курсу «Информационная безопасность».

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».