

Комплексное обеспечение безопасности предприятия

Слушатели курса получают практические знания о современных подходах при построении корпоративной безопасности предприятия, по управлению экономическими рисками, выявлению конфликтов интересов в закупках, противодействию недобросовестной конкуренции, защите активов, методам построения безопасной договорной работы на предприятии в условиях санкционного давления и кризисных явлений в экономике, обеспечению кадровой безопасности при дистанционной (гибридной) работе и информационной безопасности в условиях цифровой трансформации предприятия.

Дата проведения: 9 - 14 июня 2024 с 10:00 до 17:30

Артикул: MC22400

Вид обучения: Курс повышения квалификации

Формат обучения: Выездной

Срок обучения: 6 дней

Продолжительность обучения: 24 часа

Место проведения:

[Sea Galaxy Hotel Congress & SPA 4*](#), г. Сочи, ул. Черноморская, дом 4.

Стоимость участия: 100 200 руб.

Для участников предусмотрено:

В стоимость обучения входит: Обучение по программе курса; методические материалы; размещение в 2-местных номерах «Стандарт» (в номере: спутниковое телевидение, телефон, фен, набор фирменных банных принадлежностей, тапочки, услуга "Будильник"), питание ВВ (завтраки). Бесплатно: WI-FI, охраняемая парковка, посещение Wellness центра, услуги прачечной, швейная мастерская, сейф-ячейка, экскурсионная программа.

По желанию участников, за дополнительную плату, могут быть забронированы одноместные номера или номера других категорий, а также проживание с сопровождающими лицами. Доплата за одноместное размещение составляет 24 500 рублей. В стоимость не включен проезд до отеля.

Стоимость участия без проживания: 49 900 рублей.

Документ по окончании обучения: По итогам обучения слушатели, успешно прошедшие итоговую аттестацию по программе обучения, получают Удостоверение о повышении квалификации в объеме 24 часов (в соответствии с лицензией на право ведения образовательной деятельности, выданной Департаментом образования и науки города Москвы).

Для кого предназначен

Руководителей предприятий и организаций, директоров по безопасности, руководителей и специалистов служб безопасности, специалистов по экономической безопасности, риск-менеджеров, внутренних контролеров.

Цель обучения

Научить разрабатывать и реализовывать комплексные программы мероприятий по минимизации угроз финансовым, материальным, информационным и кадровым ресурсам организации.

Особенности программы

Слушателям курса будет предоставлено авторское методическое пособие по корпоративной безопасности, а также информационные материалы с нормативной базой, методиками, алгоритмами действий, шаблонами локальных правовых актов по тематике курса.

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

Программа обучения

День-1.

Заезд слушателей (после 14.00), регистрация.

14.00— 15.00-Обед. Свободное время.

18.00— 20.00-Ужин. Свободное время.

День-2, 3, 4, 5.

8.00— 10.00-Завтрак.

10.00— 14.00-Обучение.

14.00— 15.00-Обед. Свободное время.

19.00— 20.00-Ужин. Свободное время.

День-6.

8.00— 10.00-Завтрак.

Отъезд участников (до-12.00).

ПРОГРАММА

Современные подходы при построении корпоративной безопасности. Тенденции 2023-2024-годов.

- 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.
- 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 принятия управленческих решений в-условиях избыточности информации, ее-неточности и-недоверности.
- 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.

- Особенности договорных отношений с-аутсорсинговыми организациями, предлагающими услуги по-корпоративной безопасности. Взаимодействия с-адвокатами, частными охранными организациями, детективами и-иными организациями (лицами, имеющими особый статус) при решении вопросов корпоративной безопасности.
- 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 правил поведения 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.

Организация безопасной договорной работы в-условиях санкционного давления и-неопределенности. Управление рисками в-закупочной деятельности.

- Организация безопасной договорной работы на-предприятии. Инструкция о-договорной работе. Централизация или делегирование полномочий. Процедуры внутреннего согласования. Выдача доверенностей. Работа с-договорами.
- Распределение зон ответственности между подразделениями и-должностными лицами предприятия в-договорной работе. Матрица компетенций.
- Особенности договорной работы в-условиях санкционного давления и-неопределенности, а-также в-процессе антикризисного управления. Минимизация издержек. Безопасность закупок при дистанционных (удаленных) методах работы.
- Особенности 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 российского и-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.
- Корректировка критериев оценки надежности контрагента в-современных политических и-экономических условиях. 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. Понятие форсмажор.
- 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. Медиаторство как способ досудебного урегулирования спора. Психологические, юридические, имиджевые и-иные способы воздействия на-должника.

Обеспечение кадровой безопасности предприятия при дистанционной (гибридной) работе и в период проведения специальной военной операции.

- 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. Особенности работы с «самозанятыми» и работниками, имеющими статус индивидуального предпринимателя. Аутстафing (лизинг персонала) как вариант кадрового обеспечения предприятия.
- Основные изменения трудового законодательства, вступившие в силу в 2022-2024-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).
- Особенности 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 изменения в трудовых и гражданско-правовых отношениях с отдельными категориями граждан, произошедшие в 2022-2024 годах на примере изменения требований к персоналу объектов топливно-энергетического комплекса, участвующих в работах по обеспечению безопасности объектов ТЭК.
- 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;
- 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.
- Признаки опасности у кандидата на работу. На что обратить внимание в «проверочных мероприятиях». Формирование модели потенциального нарушителя, применительно к различным должностям.
- Российское и международное 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 2022-2024-годах. Понятие компрометация персональных данных работников и уведомление об этом Роскомнадзор. Особенности обработки персональных данных, разрешенных субъектом персональных данных для распространения.
- 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. Антикоррупционная 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.
- Построение кадровой безопасности с различными группами риска. Работа с «жалобщиками» и иными работниками, злоупотребляющими своими правами.
- Комплаенс-контроль работников, занимающих должности с коррупционными рисками. Анализ полномочий и результатов работы персонала на предприятии. Политика кадровой безопасности по минимизации комплаенс-рисков.
- 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.
- Особенности проведения внутренних проверок и расследований по наиболее характерным противоправным действиям сотрудников (хищение, «откат», мошенничество, разглашение информации, конфликт интересов, уход клиентов и т.д.).
- 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 2022— 2024-годов. Методы, применяемые адвокатами для защиты своих клиентов в трудовых спорах.

Менеджмент информационной безопасности в условиях цифровой трансформации предприятия.

- 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 предприятия. Неприкосновенность частной жизни, тайна телефонных переговоров, почтовых и иных сообщений. Процедуры использования технических средств,

предназначенных для негласного получения информации.

- Понятие культуры информационной безопасности при цифровой трансформации предприятия. Культура информационной безопасности, как составная часть корпоративной безопасности. Этические нормы в менеджменте информационной безопасности.
- Информация как нематериальный актив предприятия. Противодействие черному пиару, манипулированию информацией и иным действиям со стороны недобросовестных конкурентов.
- Политика информационной безопасности как основа системы менеджмента ИБ. Цели и задачи Политики информационной безопасности. Общая структура Политики информационной безопасности.
- Аудит состояния информационной безопасности на-предприятии. Порядок проведения аудита информационной безопасности предприятия.
- Законодательство РФ в-области защиты информации. Термины и-определения. Правовые основы наличия на-предприятии конфиденциальной информации.
- Основные источники конфиденциальной информации на-предприятии. Автоматизация процессов обмена информацией между ними. Основные каналы утечки конфиденциальной информации при цифровой трансформации предприятия.
- Основные направления защиты конфиденциальной информации. Системный подход к-защите информации. Особенности информационной безопасности в-условиях санкционного давления и-программ импортозамещения.
- Организационные мероприятия по-защите конфиденциальной информации. Анализ информационных ресурсов предприятия. Оптимизация информационных потоков. Определение формы представления информационных ресурсов, подлежащих защите.
- Режимные, технические и-инженерно-технические мероприятия по-защите конфиденциальной информации. Создание внутриобъектового и-пропускного режимов. Физическая защита охраняемых информационных ресурсов.
- Кадровые мероприятия по-защите конфиденциальной информации. Распределение прав доступа к-информации. Разглашение информации через «человеческий фактор», как основной канал утечки конфиденциальной информации. Защита от-фишинговых атак и-методов социальной инженерии.
- Правовые мероприятия по-защите конфиденциальной информации. Создание правовых режимов по-защите информации.
- Особенность защиты информации при использовании на-предприятии дистанционных (удаленных) работников, а-также релоцировавшихся в-другие страны работников.
- Виды юридической ответственности за-разглашение конфиденциальной информации, использование ее в-личных целях или неправомерному доступу к-ней. Уголовная, административная, дисциплинарная и-гражданско-правовая ответственность. Обзор судебной практики.
- Изменения в-законодательстве о-персональных данных, вступивших в-силу в-2023-2024-годах. Особенности обработки персональных данных, разрешенных субъектом персональных данных для распространения. Процедуры трансграничной передачи персональных данных.
- Создание режима коммерческой тайны на-предприятии. Методика составления перечня сведений, составляющих коммерческую тайну. Основные организационные, правовые и-технические меры по-защите коммерческой тайны.
- Обязательства работников по-сохранению коммерческой тайны на-предприятии. Понятие «разглашение коммерческой тайны». Виды юридической ответственности за-разглашение коммерческих секретов предприятия.
- Понятие «служебная тайна» в-российском законодательстве. Особенность работы с-документами, имеющими ограничительную пометку «для служебного пользования». Ответственность за-разглашение служебной тайны.
- Перечень сведений в-области военной, военно-технической деятельности-РФ, которые при их-получении иностранными источниками могут быть использованы против безопасности-РФ и-порядок работы с-информацией, входящей в-этот перечень.

Преподаватели

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). Опубликовано методические пособия «Практическое пособие по информационной безопасности предпринимательской деятельности», «Практические рекомендации по безопасности бизнеса».