14-15 августа 2025 года

Online-обучение, повышение квалификации (16 часов), код: 783-ФР

НОВЫЕ ТРЕБОВАНИЯ ЗАКОНОДАТЕЛЬСТВА ПО СОЗДАНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИЯХ В 2025 ГОДУ: КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ, КОММЕРЧЕСКАЯ И СЛУЖЕБНАЯ ТАЙНЫ, ВИДЫ ЮРИДИЧЕСКОЙ ОТВЕТСТВЕННОСТИ

ПРЕПОДАВАТЕЛИ ОБУЧЕНИЯ

ПАНКРАТЬЕВ Вячеслав Вячеславович – полковник юстиции в запасе, заведующий кафедрой безопасности в Университете государственного и муниципального управления, эксперт в области корпоративной безопасности и управлению рисками. Независимый консультант в области корпоративной безопасности. Разработчик методик аудита безопасности предприятия и создания КСБ – корпоративных стандартов безопасности

ПРОГРАММА ОБУЧЕНИЯ

Ключевые положения законодательства РФ в области защиты информации, действующие в 2025 году. Указ Президента РФ от 01.05.2022 №250 (в ред. от 13.06.2024). Термины и определения. Правовые основы наличия на предприятии конфиденциальной информации. 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.

Принятие управленческих решений в условиях избыточности информации, ее неточности и недостоверности. Принципы работы Big Data. Применение элементов искусственного интеллекта в деятельности предприятия. Наличие черного пиара и фейковых новостей в информационном поле. Понятие культура информационной безопасности при цифровой трансформации предприятия. Культура информационной безопасности, как составная часть корпоративной безопасности. Этические нормы в менеджменте информационной безопасности.

Государственные информационные системы. Первичность информации в государственных информационных реестрах. Отсутствие контура информационной безопасности в цифровом мире. Понятие цифровой след физического лица.

Особенности ведения документооборота. Система электронного документооборота на предприятии. Цифровая подпись. Основные требованию к делопроизводству при цифровой трансформации предприятия.

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 системы менеджмента информационной безопасности. Международные стандарты безопасности информационных систем. Основные требования стандарта менеджмента информационной безопасности ISO 27001. 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.

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. ИТ мероприятия по защите конфиденциальной информации. Защита компьютерных сетей. Применение средств криптографической защиты информации. Правовые мероприятия по защите конфиденциальной информации. Создание правовых режимов по защите информации.

Особенность защиты информации при использовании на предприятии дистанционных (удаленных) 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.

Основные требования международного и российского законодательства в области защиты персональных данных. Правовые акты регуляторов, определяющих политику по защите персональных данных в России. Пошаговый алгоритм действий по созданию на предприятии системы обработки персональных данных, удовлетворяющей требованиям регуляторов. Виды юридической ответственности за нарушение правил обработки персональных данных, утечки персональных данных, несоблюдение требований по их защите, а также за их незаконное получение. Уголовная ответственность за незаконную обработку 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.

Проведение внутренних проверок и расследований по инцидентам информационной безопасности на предприятии.

УСЛОВИЯ УЧАСТИЯ

Стоимость участия в повышении квалификации одного слушателя – **16 000 рублей** (НДС не облагается).
При оплате до **13 августа 2024 года** специальная цена – **11 000 рублей** (НДС не облагается).
! При регистрации и оплате одного сотрудника от организации, участие второго сотрудника от данной организации предоставляется бесплатно.
Возможно корпоративное участие специалистов по специальным ценам: **20 000 рублей** (5 человек); **30 000 рублей** (10 человек).

В стоимость включено:
Обучение на дистанционной платформе с выдачей Удостоверения о повышении квалификации (16 часов).
Предоставление доступа к видеозаписи обучения и методическим материалам в электронном виде.
**Организатор оставляет за собой право вносить изменения в заявленную программу*

РЕГИСТРАЦИЯ ПО ТЕЛ. +7 (906) 090-63-93, E-MAIL: M.CENTRA@MTSDPO.RU