

Защита конфиденциальной информации предприятия

На семинаре будет сделан акцент на обучение работе по стандартам информационной безопасности, создании режима коммерческой тайны на предприятии и обработке персональных данных в соответствии с требованиями регуляторов. Также особое внимание будет уделено противодействию разглашения информации через «человеческий фактор», особенно с применением фишинговых атак и методов социальной инженерии. Также участникам семинара будет предоставлено методическое пособие по корпоративной безопасности, а также информационные материалы с нормативной базой, методиками, алгоритмами действий, шаблонами локальных правовых актов по тематике семинара.

Дата проведения: Открытая дата

Вид обучения: Семинар

Формат обучения: Онлайн-трансляция

Срок обучения: 1 день

Продолжительность обучения: 8 часов

Для участников предусмотрено:

Методический материал.

Документ по окончании обучения: Сертификат об участии в семинаре.

Для кого предназначен

Руководителей (заместителей руководителей) организаций и структурных подразделений; работников подразделений безопасности; работников, ответственных за цифровую трансформацию предприятия; работников, участвующих в менеджменте информационной безопасности; специалистов ИТ подразделений, подразделений ИТ безопасности и кибербезопасности; работников HR подразделений; корпоративных юристов.

Особенности программы

В условиях цифровой трансформации экономики и предприятия остро стоит вопрос об информационной безопасности и защите конфиденциальной информации. Законодательство РФ относит определенную информацию к конфиденциальной. Есть конфиденциальная информация, которую организации обязаны защищать (например, персональные данные или государственная тайна), а есть информация, которую предприятие может по своему усмотрению относить к конфиденциальной и имеет право защищать. Например, коммерческая тайна. В чем сложность защиты конфиденциальной информации? В первую очередь в том, что информация нематериальна. Конфиденциальная информация может быть в материальных документах, в электронных документах, в информационных реестрах, в головах работников и т.д. Кроме того, в условиях цифровой трансформации предприятия теряется сам контур информационной безопасности, то есть отсутствует физическое место нахождения информации. Не ясно, где находится то, что нужно защищать.

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

Мероприятие проходит в рамках курса повышения квалификации:

- Политика информационной безопасности предприятия

Программа обучения

Защита конфиденциальной информации предприятия.

- 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 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;
- порядок и-процедуры защиты конфиденциальной информации при использовании дистанционных работников;
- 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. Режим служебной тайны 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;
- 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 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.

Преподаватели

ПРЕПОДАВАТЕЛЬ

К.т.н., доцент кафедры информационных технологий и систем безопасности. Член правления клуба ИТ директоров Санкт-Петербурга, председатель конференции по ИБ по СЗФО.

ПРЕПОДАВАТЕЛЬ

Эксперт-практик в области корпоративной безопасности. Бизнес-консультант по вопросам безопасности международного делового сотрудничества.-

ПРЕПОДАВАТЕЛЬ

Специалист в области безопасности бизнеса, полковник юстиции. Заведующий кафедрой безопасности Университета государственного и муниципального управления.-