ФИНКОНТ
учебный центр

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

seminar@finkont.ru
www.finkont.ru

Политика информационной безопасности предприятия

Вся корпоративная безопасность в настоящее время построена на основе работы с информацией и информационной безопасности. Сложность состоит в том, что информация – вещь нематериальная, представленная в разных материальных и нематериальных формах. 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. Да и само информационное поле чаще всего наполняются информацией, генерируемой ботами, а не человеком. Поэтому процесс защиты информации достаточно сложен и предполагает комплексное осуществление организационных, кадровых, режимных, правовых, технических и иных мероприятий.

Дата проведения: Открытая дата

Вид обучения: Курс повышения квалификации

Формат обучения: Дневной

Срок обучения: 3 дня

Продолжительность обучения: 24часа

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: Слушатели, успешно прошедшие итоговую аттестацию по программе обучения, получают Удостоверение о повышении квалификации в объеме 24 часов,(Лицензия на право ведения образовательной деятельности от 08 июня 2021 г. N041442, выдана Рособрнадзором).

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.

Цель обучения

- рассмотреть вопросы информационной безопасности, как составной части системы защиты бизнеса, а также предложить практические решения по защите от угроз и рисков, как внешних, так и внутренних.

Участники научатся:

- формировать политику безопасности, в соответствие с требованиями компании;
- готовить соответствующие пакеты документов;
- выбирать соответствующие средства для защиты информации от несанкционированного доступа;
- выбирать соответствующие средства для безопасной работы в сети.

Особенности программы

Особое внимание на курсе будет уделено противодействию разглашению информации через «человеческий фактор», особенно с применением фишинговых атак и методов социальной инженерии. При цифровой трансформации предприятия самым слабым звеном как всегда оказывается человек. Также участникам курса будут предоставлены методические пособия, информационные материалы с нормативной базой, методиками, алгоритмами действий, шаблонами локальных правовых актов по тематике курса.
Участникам курса будут предложены готовые алгоритмы действий и формы (образцы) необходимых нормативно-правовых документов.

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

Отдельные семинары в рамках курса

- Защита конфиденциальной информации предприятия
- Менеджмент информационной безопасности в условиях цифровой трансформации предприятия

Участие возможно отдельно в каждом семинаре.

Программа обучения

День 1. 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.
- Политика информационной безопасности как основа системы менеджмента ИБ. Цели и задачи Политики информационной безопасности. Общая структура политики информационной безопасности.
- Государственное регулирование в сфере информационной безопасности (ИБ). Российские и международные стандарты в области ИБ. Законодательство РФ, нормативно-правовые документы.
- 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.
- Государственные информационные системы. Первичность информации в государственных информационных реестрах. Отсутствие контура информационной безопасности в цифровом мире. Понятие цифровой след физического лица.
- Особенности документооборота в цифровом мире. Понятие электронный документ. Система электронного документооборота на предприятии. Цифровая подпись. Основные требованию к делопроизводству при цифровой трансформации предприятия.
- 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 культура 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, манипулированием информацией и иным действиям со стороны недобросовестных конкурентов.
- Методика разработки политики информационной безопасности на предприятии.
- Создание службы информационной безопасности. Разделение функций между службой информационной безопасности, службой безопасности и ИТ-подразделением. Место службы информационной безопасности в структуре предприятия.
- Понятие системы менеджмента информационной безопасности. Международные стандарты безопасности информационных систем. Основные требования стандарта менеджмента информационной безопасности ISO 27001.
- Аудит состояния информационной безопасности на предприятии. Порядок проведения аудита информационной безопасности предприятия.
- Основные требования международного и российского законодательства в области защиты персональных данных. Правовые акты регуляторов, определяющих политику по защите персональных данных в России.
- Права субъекта персональных данных и обязанности оператора персональных данных. Виды юридической ответственности за разглашение персональных данных, а также за невыполнение требований по их защите.

- Пошаговый алгоритм действий по созданию на предприятии системы обработки персональных данных, удовлетворяющей требованиям регуляторов.
- Изменения в законодательстве о персональных данных, вступивших в 2021 году. Особенности обработки персональных данных, разрешенных субъектом персональных данных для распространения.
- 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.
- Проведение внутренних проверок и расследований по инцидентам информационной безопасности на предприятии.

День 2. 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.

День 3. Обеспечение безопасности компьютерных систем и сетей.- Угрозы информационной безопасности.

- Угрозы и уязвимости автоматизированных информационных систем.
- Угрозы сетевой безопасности. Анализ угроз.
- Возможные последствия внешних атак и действий внутренних нарушителей.
- Возможные каналы несанкционированного доступа к важной информации.
- Новые классы угроз, связанные с использованием облачных вычислений и мобильных технологий.
- Системы обнаружения вторжений и ловушки.
- Защита виртуальной инфраструктуры.
- Оценка уровня защищённости информационных систем.
- Управление доступом. Требования к парольной защите. Безопасная работа в Интернет. Безопасная работа с электронной почтой. Безопасное хранение данных.
- Защита информации с использованием шифровальных (криптографических) средств. Криптографические методы защиты информации. Обеспечение применения электронной подписи и инфраструктуры открытого ключа с использованием сертифицированных средств.
- Социальная инженерия. Требования к антивирусной защите. Действия в нештатных ситуациях.
- Организационно-режимные меры. Экономические меры. Технические средства обеспечения безопасности

Практические занятия.

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.-