8 (495) 698-63-64
8 (800) 234-55-22
seminar@finkont.ru
www.finkont.ru

Менеджмент информационной безопасности в условиях цифровой трансформации предприятия

На сегодняшний день, работу предприятий трудно представить без информационных и коммуникационных технологий. Информация — неотъемлемый компонент всех сфер деятельности предприятия, средство, без которого невозможно решать множество усложняющихся задач, стоящих перед предприятием. Информация обладает несколькими характеристиками, и одна из важнейших — безопасность.

Дата проведения: Открытая дата

Вид обучения: Семинар

Формат обучения: Дневной

Срок обучения: 1 день

Продолжительность обучения: 8часов

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: 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.

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.

Особенности программы

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.На семинаре будут рассмотрены вопросы организации информационной безопасности и практические меры, которые должны быть запланированы и внедрены в каждой конкретной организации для

обеспечения режима информационной безопасности.

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

Мероприятие проходит в рамках курса повышения квалификации:

- Политика информационной безопасности предприятия

Программа обучения

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.

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.-