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

Информационная безопасность в условиях цифровой трансформации предприятия

На курсе слушатели узнают, как защитить предприятие от потери корпоративной информации, повреждения информационных систем, как проводить технический аудит информационной среды, как определить необходимые технические средства защиты информации, разработать стратегию защиты с четким планом и бюджетом, как не допустить утечку конфиденциальной информации, как правильно организовать работу с персональными данными и выстроить эффективную систему информационной безопасности.

Дата проведения: Открытая дата

Вид обучения: Курс повышения квалификации

Формат обучения: Дневной

Срок обучения: 3 дня

Продолжительность обучения: 24часа

Место проведения: г. Санкт-Петербург, Лиговский проспект, 266с1, Бизнес Центр Премьер Лига (3 очередь), 4 этаж, из лифта направо. Станции метро «Московские ворота», «Технологический институт», «Обводный канал».

Для участников предусмотрено: Методический материал, кофе-паузы.

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, директоров по безопасности, руководителей и специалистов служб безопасности, специалистов по информационной безопасности, сотрудников, ответственных за цифровую трансформацию предприятия, специалистов ИТ подразделений и кибербезопасности, руководителей комплаенс-подразделений.

Цель обучения

Получить практические рекомендации по созданию эффективной системы информационной безопасности предприятия, применению современных методов и технических средств защиты информации.
Это мероприятие можно заказать в корпоративном формате (обучение сотрудников одной компании).

Программа обучения

День-1.

Защита конфиденциальной информации. Режим коммерческой тайны.

- Законодательство РФ-в-области защиты 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.

День-2.

Защита персональных данных своими силами.

- ФЗ-«О-персональных данных», основные нормы закона, применяемые термины и-определения. Изменения в-законодательстве, вступившие в-силу в-2021-2022-годах. Трудовой кодекс-РФ, иные нормативные акты, регламентирующие вопросы обработки персональных данных в-рамках трудовых отношений.
- Основные положения нормативных актов регуляторов (Роскомнадзор, ФСТЭК России, ФСБ России и-т.д.), регламентирующие требования к-обработке персональных данных.
- Виды юридической ответственности за-разглашение персональных данных, несоблюдение требований по-их-защите, а-также за-их-незаконное получение. Необходимые и-достаточные условия для наступления ответственности. Обзор судебной практики.
- 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.
- Специальные категории персональных данных и-особенности их-обработки.
- Особенности обработки персональных данных, разрешенных субъектом персональных данных для распространения.
- Порядок получения, хранения, предоставления и-уничтожения (обезличивания) персональных данных.
- Формирование правового режима защиты персональных данных. Перечень мер по-защите персональных данных.
- Пошаговый алгоритм действий по-выполнению предприятием требований законодательства по-обработке персональных данных.
- Организационные и-правовые мероприятия по-защите персональных данных. Создание политики обработки персональных данных и-иных организационно-распорядительных документов.
- Обработка персональных данных, осуществляемой без использования средств автоматизации и-их-защита.
- Порядок проведения кадровых мероприятий по-защите персональных данных. Определение цели и-получение согласия на-обработку персональных данных.
- Порядок и-процедуры работы с-персональными данными при дистанционной (удаленной) работе.
- Особенности получения (предоставления) аутсорсинговых услуг по-обработке персональных данных. Трансграничная передача персональных данных.
- Требования к-материальным носителям биометрических персональных данных и-технологиям их-хранения вне информационных систем персональных данных.
- Создание информационных систем персональных данных. Формирование модели угроз безопасности персональных данных при их-обработке в-информационных системах персональных данных. Методика определения актуальных угроз.

- 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.
- Права и-обязанности должностных лиц, осуществляющих государственный контроль и-лиц, в-отношении которых осуществляются мероприятия по-контролю. Состав, последовательность и-сроки выполнения административных процедур.
- Типичные нарушения операторами требований законодательства по-обработке персональных данных.

День-3.

Обеспечение безопасности компьютерных систем и-сетей.

- 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.
- Криптографические методы защиты информации. Алгоритмы шифрования, хеширования, электронной подписи. Средства криптографической защиты информации и-их-применение в-корпоративной информационной системе (КИС). Криптопровайдеры. Сервисы, необходимые для функционирования PKI (CRL, OCSP, TSP). Интеграция PKI в-КИС. Защита данных с-помощью блокчейна. Применение электронной подписи с-использованием сертифицированных средств. Сертификат ключа проверки подлинности электронной подписи. Удостоверяющий центр. Хранение электронных юридически значимых документов.
- Социальная инженерия. Требования к-антивирусной защите. Действия в-нештатных ситуациях.
- Организационно-режимные меры. Экономические меры. Технические средства обеспечения безопасности.
- Создание автоматизированной системы защиты информации в-соответствии с-рекомендациями комплекса стандартов ISO 27001-2013.
- Оценка экономической эффективности мер защиты информации. Анализ рисков-ИБ и-выбор стратегии управления ими. Обоснование инвестиций на-информационную защиту.
- Средства мониторинга и-аудита информационной безопасности. Нормативно-правовое основание аудита информационной безопасности. Содержание и-последовательность основных этапов аудита. Выбор технических средств активного аудита.

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

ПРЕПОДАВАТЕЛЬ

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