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

Обеспечение информационной безопасности предприятия

Программа рассматривает системный подход к обеспечению информационной безопасности на предприятии,дает понимание, как выстраивать комплексную защиту данных, информационных систем и инфраструктуры в условиях цифровых угроз. На обучении разбираются современные требования законодательства в области информационной безопасности и защиты персональных данных, принципы построения системы информационной безопасности и подготовка необходимых документов,модели угроз и нарушителей, каналы несанкционированного доступа к информации, техническиеи программные средства защиты информации,методы защиты сетей и корпоративных систем, криптографические средства, реагирование на инциденты и основы компьютерной криминалистики, оценка рисков и экономическое обоснование выбора мер противодействия, кадровая безопасность и культура информационной безопасности.

Дата проведения: 15 - 19 марта 2027 с 10:00 до 17:30

Артикул: СП14911

Вид обучения: Курс повышения квалификации

Формат обучения: Онлайн-трансляция

Срок обучения: 5 дней

Продолжительность обучения: 40часов

Стоимость участия: 61 900 руб.

Для участников предусмотрено: Методический материал.

Документ по окончании обучения: Удостоверение о повышении квалификации в объеме 40 часов (в соответствии с лицензией на право ведения образовательной деятельности, выданной Департаментом образования и науки города Москвы).

Для кого предназначен

Директоров по безопасности, руководителей и специалистов подразделений информационной безопасности, информационных технологий, департаментов цифрового развития, руководителей и специалистов IT подразделений.

Результат обучения

В результате обучения на программе слушатели узнают:

- Актуальную нормативно-правовую базу в области информационной безопасности.
- Основные угрозы и уязвимости в современных информационных системах.
- Принципы построения комплексной системы защиты информации.
- Порядок проведения аудита информационной безопасности и реагирования на инциденты.
- Обеспечение защиты персональных данных и конфиденциальной информации.
- Методы и средства криптографической защиты данных.
- Технологии обеспечения безопасности компьютерных сетей и веб-приложений.
- Управление рисками информационной безопасности и создание политик безопасности.

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

Программа обучения

День 1

Законодательное и нормативно-правовое регулирование в сфере информационной безопасности (ИБ). Указ Президента РФ от 01.05.2022 № 250, Указ Президента РФ от 30 марта 2022 № 166, приказ Минцифры от 17 августа 2023 г. №720. Основные требования указов Президента и приказа Минцифры. Нормативно-правовые акты ФСТЭК и ФСБ в области защиты КИИ. Общие требования и рекомендации регуляторов к обеспечению защиты информации, персональных данных и конфиденциальной информации. Система сертификации средств и аттестации объектов информатизации. Международные стандарты в области информационной безопасности ISO/IEC 27001:2022. Ответственность за правонарушения в области информационной безопасности.

Информационная безопасность как составной элемент системы безопасности предприятия.

Концепция безопасности и принципы построения комплексной системы обеспечения информационной безопасности. Деление информации по уровням конфиденциальности. Виды тайн. Современные угрозы информационной безопасности и методы противодействия им. Принципы построения подразделения комплексной системы защиты информации предприятия. Функциональные обязанности работников подразделения информационной безопасности. Отличие информационной безопасности от кибербезопасности.

Организационные методы обеспечения информационной безопасности. Политики информационной безопасности предприятия и разработка внутренних организационно-распорядительных документов. Основные тактики и техники внешних кибератак и действий внутренних нарушителей. Анализ и оценка рисков информационной безопасности. Наиболее распространенные каналы утечки информации. Несанкционированный доступ к базам данных предприятия и варианты противодействия.

Обеспечение безопасности объектов критической информационной инфраструктуры (КИИ). Требования законодательства по защите объектов КИИ, 187-ФЗ «О безопасности критической информационной инфраструктуры РФ». Понятие КИИ в информационной безопасности, какие сведения относятся к КИИ. Категорирование объектов КИИ, порядок составления Акта категорирования, категории значимости объектов. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры. Полномочия ФСТЭК и ФСБ России в области защиты КИИ. Отличие ведомственных сертификатов. Киберразведка на объектах КИИ. Влияние импортозамещения в информационной безопасности на защиту объектов КИИ.

День 2

Обеспечение защиты 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 информации 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.

Расследование хакерских атак и-реагирование на-инциденты информационной безопасности.-Реагирование на-инциденты информационной безопасности. Требования и рекомендации нормативных актов ФСБ – ФСТЭК по-реагированию на-инциденты (2022-2026 гг.) -Организация взаимодействия с-ГосСОПКА.

День 3

Технические и программные средства защиты информации. Средства защиты информации на рабочих станциях. Обеспечение безопасности центров обработки данных. Организация удаленной работы пользователей с соблюдением требований ИБ. Средства многофакторной аутентификации (MFA). Обеспечение безопасности информации при использовании мобильных устройств. Построение корпоративной инфраструктуры открытых ключей (PKI). Системы централизованного управления учетными записями и правами доступа. Средства автоматизации анализа журналов, выявления инцидентов ИБ и мониторинга действий пользователей.

Средства защиты АСУ ТП и «Интернета вещей» (IoT). Практика внедрения средств защиты, возможные проблемы и пути их решения. Типичные ошибки проектов защиты информации.

День 4

Управление безопасностью в-виртуальной и-облачной среде.-Типичные атаки на облачные инфраструктуры. Ошибки конфигурации, которые могут привести к утечке данных. Как правильно выстраивать защиту в облаке. Шифрование данных и-управление ключами. Многофакторная аутентификация. Критерии выбора облачного провайдера. Оценка надежности и-безопасности. Процедуры реагирования на-инциденты в облаках.

Применение DLP-решений-для защиты конфиденциальной информации.

Криптографические методы защиты информации.-Алгоритмы шифрования, хеширования, электронной подписи. Средства криптографической защиты информации и-их-применение в-корпоративной информационной системе (КИС). Криптопровайдеры.

Методы и-средства обеспечения информационной безопасности-в-соответствии с-рекомендациями комплекса стандартов ГОСТ ИСО/МЭК 27001–2021.

День 5

Защита корпоративной информации при использовании на предприятии дистанционных (удаленных) работников. Практики настройки удаленного доступа и VPN для сотрудников в России и за рубежом. Удаленные рабочие столы и минусы дистанционной работы с позиции безопасности. Сотрудник за рубежом: варианты обеспечения информационной безопасности. Проблемы и их решения: взлом через домашние устройства связи; использование домашних компьютеров, зараженных вредоносным ПО.

Оценка экономической эффективности мер защиты информации.-Анализ рисков-информационной безопасности и-выбор стратегии управления ими. Обоснование инвестиций на-информационную защиту.

Аудит информационной безопасности. Виды и формы аудита информационной безопасности.-Нормативно-правовое основание аудита информационной безопасности. Содержание и-последовательность основных этапов аудита.

Социальная инженерия.-Виды и тактика атак с-использованием «человеческого фактора» и методов социальной инженерии. Рекомендуемые организационные мероприятия и-неотложные технические меры по-противодействию этим угрозам. Способы формирования и трансформации убеждений и ценностей персонала. Угрозы, связанные с популярностью социальных сетей.

Преподаватели

ЛОБАКОВ Валентин Викторович

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

Сфера профессиональных интересов:

- Разработка стратегии корпоративной безопасности предприятия.
- Нормативно-правовое обеспечение деятельности служб корпоративной защиты хозяйствующих субъектов.
- Организация обеспечения безопасности предприятий ТЭК (в соответствии с ФЗ-256 от 21.07.2011, Постановлениями Правительства РФ №№ 458-460, 993, Методическими рекомендации Минэнерго-2012 и пр.).
- Разработка и внедрение системы обеспечения безопасности хозяйствующих субъектов от угроз террористического характера и актов незаконного вмешательства.
- Построение эффективной системы безопасности предприятий, имеющих заграничные филиалы.
- Введение в специальность «Конкурентная разведка».
- Кадровая безопасность на предприятии. Ее организация, формы и методы обеспечения.
- Организация проведения служебных расследований (разбирательств) на предприятии.
- Договорная работа на предприятии и вопросы обеспечения экономической безопасности.
- Безопасное проведение предприятием конкурсных процедур (по ФЗ №№ 44 и 223).
- Организация взаимодействия подразделений и служб по противодействию поступления на предприятие контрафактной, фальсифицированной и некачественной продукции.
- Организация и обеспечение пропускного и внутриобъектового режима на предприятии.

Преподавательская деятельность:

Проводит обучающие программы для владельцев, топ-менеджеров и руководителей в бизнес-школах по дисциплинам, связанными с корпоративной безопасностью предприятий различных форм собственности.

Образование:

1981 г. Ленинградский государственный университет им. А.А. Жданова.
1985 г. Академия-(г. Москва)

Опыт работы:

- 2005-2017 гг. ПАО «Газпром», заместитель начальника Управления корпоративной защиты ООО «Газпром трансгаз Санкт-Петербург».
- 2001-2005 гг. Акционерный Банк «Россия», холдинговая структура безопасности, заместитель гендиректора.
- 1994-2001 гг. Начальник отдела службы безопасности (коммерческие банки, Центральный Банк Российской Федерации).
- 1981-994 гг. Государственная служба.

Корпоративные клиенты:

Газпром, Газпром нефть, Роснефть, Лукойл, Транснефть, Башнефть, Татнефть, Росатом, Ростех, Россети, Аэрофлот, Северсталь, Норильский никель, Фосагро, Газпромбанк, АБ «Россия», СГС, Строймонтаж, Мегафон, МТС, Билайн (всего около 200).

ПРЕПОДАВАТЕЛЬ

Преподаватель-практик в области информационной безопасности, эксперт по кибербезопасности в государственных и коммерческих организациях. Более 20 лет практического опыта в информационной безопасности на стыке с IT. Сфера профессиональных компетенций: вопросы связанные с кибербезопасностью и информационной безопасностью, защита инфраструктуры и объектов информатизации. Опыт взаимодействия с регуляторами ФСТЭК, ФСБ, Морской регистр.
Образование: специалитет - специалист по комплексной защите объектов информатизации, аспирантура - информационные системы и процессы.