АННОТАЦИЯ

Программа повышения квалификации

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ».

Актуальность. В связи с развитием информационных технологий и компьютеризацией экономики одним из важнейших вопросов в деятельности компании становится обеспечение информационной безопасности.

Информация – это один из самых ценных и важных активов любого предприятия и должна быть надлежащим образом защищена.

Программа предназначена для руководителей и специалистов подразделений служб безопасности, информационных технологий, всех заинтересованных специалистов.

Модули программы:

Государственное регулирование в сфере информационной безопасности (ИБ). Российские и международные стандарты в области ИБ. Законодательство РФ, руководящие, нормативно-методические документы, требования и рекомендации регуляторов к обеспечению защиты конфиденциальной информации: коммерческой, служебной тайны и персональных данных. Действующая в РФ система сертификация средств и аттестации объектов информатизации

Угрозы информационной 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. Меры по обеспечению информационной безопасности. Разработка политики информационной безопасности в организации.

Защита конфиденциальной информации предприятия. Выбор поставщиков технических средств защиты информации. Типичные ошибки проектов защиты информации.

Технические и программные средства обеспечения информационной безопасности компании. Средства защиты информации, критерии выбора решения, сравнительная оценка. Практика внедрения средств защиты, возможные проблемы и пути их решения.

Средства мониторинга и аудита информационной безопасности. Нормативно-правовое основание аудита информзащиты. Содержание и последовательность основных этапов аудита. Выбор технических средств активного аудита.

Защита персональных данных (ПД). Рекомендации регуляторов по защите ПД. Возможные каналы несанкционированного распространения персональных данных. Необходимые организационные и технические меры по защите ПД. В соответствии с требованиями приказов ФСТЭКи с рекомендациями Роскомнадзора.

«Человеческий фактор» и социальная инженерия. Организационные и технические меры по противодействию угрозам. Виды угроз негативного воздействия на персонал. Способы формирования и трансформации убеждений и ценностей персонала. Новые угрозы, связанные с популярностью социальных сетей.

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.

Требования к слушателям: к освоению программы допускаются лица, имеющие/получающие среднее профессиональное и (или) высшее образование.

Срок обучения: не менее 1 месяца (72 часа). Периодичность обучения определяется при формировании групп обучающихся, по желанию слушателей.

Форма обучения: заочная с применением дистанционных образовательных технологий.

В результате обучения Вы получаете удостоверение о повышении квалификации установленного образца.