АННОТАЦИЯ

Программа повышения квалификации

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ОРГАНАХ ГОСУДАРСТВЕННОЙ ВЛАСТИ».

Актуальность. В связи с развитием информационных технологий и компьютеризацией экономики одним из важнейших вопросов в деятельности органов государственной власти становится обеспечение информационной безопасности. Специфика информационного взаимодействия органов государственной власти, органов местного самоуправления состоит в том, что в их информационных системах накапливается и обрабатывается информация, которая в соответствии с действующим законодательством классифицируется как конфиденциальная. Государственная политика обеспечения информационной безопасности Российской Федерации определяет основные направления деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации в этой области, порядок закрепления их обязанностей по защите интересов Российской Федерации в информационной сфере в рамках направлений их деятельности и базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере.

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

Модули программы:

Требования законодательства РФ, нормативно-методических документов к обеспечению защиты конфиденциальной информации и персональных данных в органах государственной власти.

Угрозы и риски информационной безопасности (ИБ) в органах государственного и муниципального управления. Анализ актуальных угроз и оценка рисков ИБ. Возможные последствия внешних атак и действий внутренних нарушителей. Новые классы угроз, связанные с использованием облачных вычислений и мобильных технологий.

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

Применение электронной подписи с использованием сертифицированных средств. Сертификат ключа проверки подлинности электронной подписи.

Организационно-правовые вопросы технической защиты информации. Организационно-технические вопросы реализации угроз конфиденциальности, доступности и целостности информации ограниченного доступа; порядок выявления угроз безопасности информации ограниченного доступа, обусловленный реализацией технических каналов утечки информации; средства контроля эффективности защиты информации.

Технические средства защиты информации

Аттестация объектов информатизации по требованиям безопасности информации. Классификация объектов информатизации. Порядок проведения аттестации объектов информатизации. Содержание этапов аттестационных испытаний. Организация контроля защищенности информации ограниченного доступа на этапе эксплуатации объектов информатизации.

Компетенции и ответственность руководителей органов государственной власти в сфере обеспечения информационной безопасности.

Защита персональных данных. Возможные каналы несанкционированного распространения персональных данных. Необходимые организационные и технические меры по защите ПД в соответствии с требованиями Постановлений Правительства РФ, приказов ФСТЭК и с рекомендациями Роскомнадзора.

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.