Одобрено на заседании

Совета по вопросам технической защиты информации

в Ханты-Мансийском автономном округе – Югре

Протокол от 29.05.2017 № 3/17

Типовые функции и задачи структурного подразделения (штатного специалиста, ответственного за реализацию мероприятий) по защите информации в исполнительном органе государственной власти (органе местного самоуправления) Ханты-Мансийского автономного округа – Югры

1. Основные задачи:

участие в анализе и выявлении возможных каналов утечки информации и воздействия на информационные ресурсы и процессы на объектах информатизации;

организация классификации автоматизированных систем (далее – АС) и определение уровня защищенности информации, обрабатываемой в информационных системах органа власти;

организация выполнения организационно-технических мер защиты информации на объектах информатизациии аттестации объектов информатизации требованиям безопасности информации;

организация внедрения и эксплуатация средств защиты информации систем информатизации и связи;

разработка на базе руководящих и методических документов по технической защите информации внутреннихорганизационно- распорядительных документов, определяющих порядок и мероприятия по защите информации на объектах информатизации;

контроль выполнения требований по защите информации при эксплуатации объектов информатизации.

2. Основные функции:

планирование работ по защите информации воргане власти*,* контроль выполнения запланированных мероприятий, подготовку и представление отчета о мероприятиях по защите информации в Управления защиты информации и специальной документальной связи Аппарата Губернатора автономного округа;

определение возможностей по получению охраняемых сведений техническими средствами разведки иностранных государств и криминальных структур;

определение технических каналов утечки информации, возможностей несанкционированного доступа к информационным ресурсам и процессам и воздействия на них с целью разрушения (уничтожения) или искажения;

подготовка предложений по классификации АСпо уровню их защиты от несанкционированного доступа к информационным ресурсам и процессам;

разработка предложений по организационно-техническим мероприятиям защиты информации на объектах информатизации*;*

организация подготовки объектов информатизации, обрабатывающих информацию ограниченного доступа к аттестации, организация и участие в разработке необходимой документации, в том числе технических паспортов на объекты информатизации;

формирование предложений в план закупки и внедрения новых технических средств в области защиты информации, внесение предложений по финансированию работ, связанных с обеспечением защиты информации, обрабатываемой на объектах информатизации*,* исходя из требований;

организация аттестации объектов информатизации по требованиям безопасности информации;

разработка предложений по организации и совершенствованию системы защиты информации воргане власти;

разработка воргане власти руководящих и организационных документов по защите информации в соответствии с требованиями настоящего Руководства;

организация и проведение периодического контроля эффективности проводимых мероприятий и принимаемых мер по защите информации, учет и анализ результатов контроля;

организация в установленном порядке расследований причин и условий появления нарушений в области защиты информации и разработка предложений по устранению недостатков и предупреждению подобного рода нарушений, а также осуществление контроля за устранением этих нарушений;

организация и проведение занятий с сотрудниками органа власти по вопросам защиты информации;

вести учет лиц, допущенных к работе с конфиденциальной информацией в информационных системах;

определять угрозы безопасности информации, формирование на их основе модели угроз и модели нарушителя безопасности информации в ИС;

разрабатывать на основе модели угроз СЗИ ИС, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты информации, предусмотренных для соответствующего класса информационных систем;

осуществлять контроль соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

незамедлительно сообщать руководителю органа власти (лицу, ответственному за руководство работами по защите информации) об имевших место попытках несанкционированного доступа к конфиденциальной информации, а также принимать необходимые меры по их недопущению;

знать перечень СВТ и АС в ИС органа власти и перечень задач, решаемых с их использованием;

обеспечить соблюдение требований по обеспечению информационной безопасности при проведении технического обслуживания и ремонтных работ в информационной системе (СВТ);

проводить инструктаж работников органа власти по правилам работы с используемыми аппаратно-программными средствами защиты информации;

осуществлять повседневный контроль за действиями пользователей при работе с паролями, соблюдением порядка их смены, хранения и использования;

предоставлять в отдел технической защиты информации Управления специальных мероприятий Аппарата Губернатора автономного округа необходимую информацию в части возложенных на него полномочий и обязанностей в пределах своей компетенции.

3. Работникиподразделения (штатный специалист) по защите информации органа власти имеют право:

выходить с предложениями к руководствупо совершенствованию системы защиты информации воргане власти и привлечении к проведению работ по защите информации на договорной основе предприятий и организаций, имеющих лицензии на соответствующий вид деятельности;

контролировать выполнение требований по защите информации при эксплуатации объектов информатизации;

вносить предложения руководству о прекращении обработки информации на объектах информатизации при выявлении нарушений, приводящих к утечке информации.