

МУНИЦИПАЛЬНОЕ ОБРАЗОВАНИЕ

ХАНТЫ-МАНСИЙСКИЙ РАЙОН

Ханты-Мансийский автономный округ – Югра

**АДМИНИСТРАЦИЯ ХАНТЫ-МАНСИЙСКОГО РАЙОНА**

**П О С Т А Н О В Л Е Н И Е**

от 08.07.2016 № 218

*г. Ханты-Мансийск*

О системе технической

защиты информации

 В соответствии с постановлением Губернатора Ханты-Мансийского автономного округа от 17.07.2003 № 151 «О системе технической защиты информации», в целях создания единой системы технической защиты информации на территории муниципального образования Ханты-Мансийский район:

 1. Утвердить Положение о системе технической защиты информации согласно приложению.

 2. Признать утратившим силу постановление главы Ханты-Мансийского района от 24.04.2006 № 36 «О системе технической защиты информации».

 3. Рекомендовать главам сельских поселений Ханты-Мансийского района принять аналогичный правовой акт.

 4. Опубликовать настоящее постановление в газете «Наш район»
и разместить на официальном сайте администрации Ханты-Мансийского района.

 5. Настоящее постановление вступает в силу после его официального опубликования.

 6. Контроль за выполнением постановления возложить на заместителя главы администрации района, координирующего и курирующего деятельность отдела специальных мероприятий.

И.о. главы администрации

Ханты-Мансийского района Р.Н.Ерышев

Приложение

к постановлению администрации

Ханты-Мансийского района

от 08.07.2016 № 218

ПОЛОЖЕНИЕ

О СИСТЕМЕ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

В АДМИНСТРАЦИИ ХАНТЫ-МАНСИЙСКОГО РАЙОНА

I. Общие положения

 1. Настоящее Положение является документом, обязательным для исполнения органами администрации Ханты-Мансийского района и подведомственными учреждениями (далее – органы администрации и учреждения) при организации работ по технической защите сведений, составляющих государственную тайну, и конфиденциальной информации от ее утечки по техническим каналам, несанкционированного доступа к ней, а также от специальных воздействий на информационные ресурсы на предприятиях, в учреждениях и организациях государственной или муниципальной собственности.

 2. Положение определяет структуру системы технической защиты информации в органах администрации и учреждениях (далее – система ТЗИ в соответствующем падеже) как составной части окружной системы технической защиты информации, ее основные функции и задачи.

 3. Правовую основу работ по ТЗИ в органах администрации и учреждениях составляют Конституция РФ, законы РФ «О безопасности», «О государственной тайне», Федеральный закон «Об информации, информатизации и защите информации», другие федеральные законы и иные нормативные акты Российской Федерации, Ханты-Мансийского автономного округа – Югры.

 4. Деятельность системы ТЗИ осуществляется на основе следующих принципов:

 законности;

 разграничения полномочий;

 коллегиальности решений, принимаемых в интересах системы ТЗИ;

 взаимосвязи правовых организационных и технических методов защиты информации.

 5. Основными целями системы ТЗИ являются:

 предотвращение или существенное снижение ущерба органам администрации и учреждениям от утечки информации по техническим каналам и несанкционированного доступа к ней, преднамеренного воздействия на информацию с целью ее разрушения, уничтожения, модификации или блокирования;

 обеспечение условий, способствующих реализации государственной политики в сфере информационной безопасности в органах администрации и учреждениях.

 6. К основным объектам защиты в рамках системы ТЗИ относятся информационные ресурсы ограниченного доступа, обрабатываемые на объектах информатизации в органах администрации и учреждениях.

 7. Работы по ТЗИ в органах администрации и учреждениях являются составной частью управленческой, научной и производственной деятельности, осуществляются во взаимосвязи с другими мерами по обеспечению установленного режима секретности и конфиденциальности.

 8. Выполнение любых работ, связанных с использованием сведений, составляющих государственную тайну, и информации конфиденциального характера, без выполнения необходимых мероприятий по ТЗИ и противодействию иностранным техническим разведкам не допускается.

 9. Главными направлениями работ по ТЗИ в органах администрации и учреждениях являются:

 обеспечение эффективного управления системой ТЗИ;

 организационно-режимное обеспечение технической защиты сведений, составляющих государственную тайну, и конфиденциальной информации;

 обеспечение физической защиты объектов информации;

 обеспечение защиты информации от утечки по техническим каналам при ее обработке, хранении и передаче;

 обеспечение защиты информации от несанкционированного доступа к ней в автоматизированных информационных системах и локальных вычислительных сетях, а также от компьютерных вирусов;

 совершенствование методической базы обеспечения информационной безопасности органов администрации и учреждений;

 организация и проведение контроля системы ТЗИ;

 совершенствование организационно-штатной структуры подразделений, отвечающих за обеспечение информационной безопасности, и подготовка специалистов по данному профилю.

 10. Основными мероприятиями по ТЗИ в органах администрации и учреждениях являются:

 категорирование объектов защиты в зависимости от их важности, степени секретности защищаемой информации и условий эксплуатации, а также классификация автоматизированных систем по требованиям защищенности от несанкционированного доступа к информации;

 разработка и внедрение технических решений по защите информации при создании и эксплуатации объектов информатизации;

 реализация технических мер и применение средств защиты информации, исключающих перехват информации, передаваемой по каналам связи;

 применение информационных и автоматизированных систем управления в защищенном исполнении;

 организация аттестации объектов информатизации по требованиям безопасности информации.

 11. Конкретные мероприятия, методы и приемы по технической защите информации и противодействию иностранным техническим разведкам разрабатываются в зависимости от категории (класса) объекта защиты, опасных для него средств технической разведки, установленных для данного объекта требований по информационной безопасности и выделенных для этих целей средств.

II. Система технической защиты информации

 12. Систему ТЗИ образуют:

 глава администрации района;

 постоянно действующая техническая комиссия по защите государственной тайны;

 отдел специальных мероприятий;

 организации, выполняющие работы и оказывающие услуги в области технической защиты информации.

 13. Систему ТЗИ возглавляет глава администрации района.

 Непосредственная организация и руководство работами по защите информации возлагается на первого заместителя главы администрации района.

 14. В администрации Ханты-Мансийского района создана постоянно действующая техническая комиссия по защите государственной тайны (далее – ПДТК).

 15. ПДТК может заседать в расширенном составе в случае приглашения руководителей предприятий, учреждений и организаций или их заместителей, ответственных за организацию работ по защите информации и возглавляющих соответствующие ПДТК.

 16. В администрации Ханты-Мансийского района подразделением по технической защите информации и противодействию иностранным техническим разведкам, наделенным полномочиями по методическому руководству и контролю состояния защиты информации, является отдел специальных мероприятий.

 17. Основными функциями и задачами системы ТЗИ в органах администрации и учреждениях являются:

 проведение единой государственной политики, организация и координация работ по технической защите информации;

 исключение или существенное затруднение добывания информации средствами технической разведки;

 анализ состояния и прогнозирования источников угроз безопасности информации;

 контроль эффективности и анализ состояния информационной безопасности;

 выявление ключевых проблем в области безопасности информации, определение направлений развития системы ТЗИ;

 научно-техническое, нормативно-методическое и информационное обеспечение работ по информационной безопасности;

 организация специальных проверок и исследований объемов информации, а также их аттестация по требованиям безопасности информации;

 выявление технических каналов утечки информации, фактов несанкционированного доступа к ней, ее разрушения (уничтожения) или искажения, а также разработка мер по защите информации;

 проведение обучения и повышения квалификации специалистов по защите информации, руководителей, отвечающих за организацию работ по информационной безопасности.