Кожухова О.В

АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ «ГЛИНКОВСКИЙ РАЙОН» СМОЛЕНСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

от 18 мая 2012 г. № 146

Об утверждении Положения
о порядке организации и проведении
работ по защите конфиденциальной
информации

В целях выполнения «Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К)», утверждённых приказом Гостехкомиссии России от 30.08.2002 года № 282

Администрация п о с т а н о в л я е т:

1. Утвердить прилагаемое Положение о порядке организации и проведении работ по защите конфиденциальной информации в Администрации муниципального образования «Глинковский район» Смоленской области.
2. Данное постановление довести до структурных подразделений Администрации.
3. Контроль за исполнением настоящего постановления возложить на начальника отдела по информационной политике Администрации (О.В. Кожухова).

Глава Администрации
муниципального образования
«Глинковский район»
Смоленской области

Н.А.Шарабуров

Администрация муниципального образования «Глинковский район» Смоленской области
"Для документов"

Верно
Управляющий делами Администрации
18 МАЙ 2012
Н. Н. Макаренкова

Утверждено постановлением
Администрации муниципального
образования «Глинковский
район» Смоленской области
от «18» мая 2012 г. № 146

Положение
о порядке организации и проведении работ по защите конфиденциальной информации в Администрации муниципального образования «Глинковский район» Смоленской области.

1. Общие положения.

1.1. Настоящее Положение определяет порядок организации и проведения работ по защите конфиденциальной информации в Администрации муниципального образования «Глинковский район» Смоленской области и её структурных подразделениях (далее – Администрация).

1.2. Мероприятия по защите конфиденциальной информации, проводимые в Администрации, являются составной частью управленческой и иной служебной деятельности и осуществляются во взаимосвязи с мерами по обеспечению установленной конфиденциальности проводимых работ.

1.3. Уровень технической защиты конфиденциальной информации, а также перечень необходимых мер защиты определяется дифференцировано по результатам обследования объекта информатизации, с учетом соотношения затрат на организацию технической защиты конфиденциальной информации и величины ущерба, который может быть нанесен собственнику конфиденциальной информации при ее разглашении, утрате, уничтожении и искажении.

Системы и средства информатизации и связи, предназначенные для обработки (передачи) конфиденциальной информации, должны быть аттестованы в реальных условиях эксплуатации на предмет соответствия принимаемых мер и средств защиты требуемому уровню безопасности информации.

Проведение любых мероприятий и работ с конфиденциальной информацией, без принятия необходимых мер технической защиты информации не допускается.

1.4. Объекты защиты в Администрации:

- средства и системы информатизации и связи (средства вычислительной техники, локальная вычислительная сеть (ЛВС), средства и системы связи и передачи информации, переговорные устройства, средства изготовления и тиражирования документов), используемые для обработки, хранения и передачи информации, содержащей конфиденциальную информацию - далее основные технические средства и системы (ОТСС);
- технические средства и системы, не обрабатывающие информацию, но размещенные в помещениях, где обрабатывается конфиденциальная информация - далее вспомогательные технические средства и системы (ВТСС);

1.5. Ответственность за выполнение требований настоящего Положения возлагается на управляющего делами Администрации, руководителей структурных подразделений, а также на специалистов, допущенных к обработке, передаче и

хранению в технических средствах информации, содержащей конфиденциальную информацию.

2. Охраняемые сведения.

2.1. Сведения, составляющие конфиденциальную информацию, определяются Перечнем сведений конфиденциального характера, утвержденным нормативным правовым актом Администрации в соответствии с Указом Президента РФ от 6 марта 1997 года № 188.

Перечень сведений конфиденциального характера включает:

- Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.
- Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом РФ и федеральными законами (служебная тайна).

3. Технические каналы утечки конфиденциальной информации, несанкционированного доступа и специальных воздействий на нее.

3.1. Доступ к конфиденциальной информации, нарушение ее целостности и доступности возможно реализовать за счет:

– несанкционированного доступа к конфиденциальной информации при ее обработке в информационных системах и ресурсах;

– утечки конфиденциальной информации по техническим каналам.

3.2. Детальное описание возможных технических каналов утечки информации, несанкционированного доступа к информации и специальных воздействий на нее содержится в Модели угроз безопасности информации Администрации.

4. Организационные и технические мероприятия по технической защите конфиденциальной информации.

4.1. Разработка мер по обеспечению защиты конфиденциальной информации осуществляются отделом по информационной политике Администрации.

4.2. Для защиты конфиденциальной информации, используются сертифицированные по требованиям безопасности технические средства защиты.

4.3. Организация и проведение работ по антивирусной защите информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, при ее обработке техническими средствами определяются настоящим документом, действующими государственными стандартами и другими нормативными и методическими документами Гостехкомиссии России.

Организации антивирусной защиты информации на объектах информатизации достигается путём:

- установки и применения средств антивирусной защиты информации;
- обновления баз данных средств антивирусной защиты информации;
- действий работников Администрации при обнаружении заражения информационно-вычислительных ресурсов программными вирусами.

4.3.1. Организация работ по антивирусной защите информации возлагается отдел по информационной политике Администрации и руководителей структурны. подразделений.

4.3.2. Защита информации от воздействия программных вирусов на объектах информатизации должна осуществляться посредством применения средств антивирусной защиты. Порядок применения средств антивирусной защиты устанавливается с учетом следующих требований:

- обязательный входной контроль на отсутствие программных вирусов на всех поступающих на объект информатизации носителей информации, информационных массивов, программных средств общего и специального назначения;
- периодическая проверка пользователями жестких магнитных дисков (не реже одного раза в неделю) и обязательная проверка используемых в работе носителей информации перед началом работы с ними на отсутствие программных вирусов;
- внеплановая проверка носителей информации на отсутствие программных вирусов в случае подозрения на наличие программного вируса;
- восстановление работоспособности программных средств и информационных массивов в случае их повреждения программными вирусами.

4.3.3. К использованию допускается только лицензированные, сертифицированные по требованиям ФСТЭК России антивирусные средства.

4.3.4. Порядок применения средств антивирусной защиты во всех случаях устанавливается с учетом следующих требований:

- входной антивирусный контроль всей поступающей на внешних носителях информации и программных средств любого назначения;
- входной антивирусный контроль всей информации, поступающей с электронной почтой;
- входной антивирусный контроль всей поступающей информации из сети «Интернет»;
- выходной антивирусный контроль всей исходящей информации на любых внешних носителях, а так же передача информации посредством электронной почты;
- обязательная антивирусная проверка используемых в работе внешних носителей информации;
- обеспечение получения обновлений антивирусных программ в автоматическом режиме, включая обновления вирусных баз и непосредственно новых версий программ;
- внеплановая антивирусная проверка внешних носителей на отсутствие компьютерных вирусов в случае подозрения на наличие компьютерного вируса;

4.3.5. О факте обнаружения программных вирусов сообщается в орган, от которых поступили зараженные файлы, для принятия мер по локализации и устранению программных вирусов.

Перед отправкой информации и программных средств, осуществляется ее проверка на наличие программных вирусов.

При обнаружении программных вирусов пользователь обязан немедленно прекратить все работы на АРМ и принять меры к их локализации и удалению с помощью имеющихся антивирусных средств защиты.

4.3.6. Необходимо постоянно осуществлять обновление вирусных баз. Частоту обновления устанавливать в зависимости от используемых антивирусных средств и частоты выпуска обновления указанных баз.

5. Обязанности должностных лиц.

5.1. Руководители структурных подразделений Администрации организуют и обеспечивают техническую защиту информации, циркулирующую в технических средствах и помещениях подчиненных им подразделений.

5.2. Владельцы и пользователи ОТСС обеспечивают уровень технической защиты информации в соответствии с требованиями (нормами), установленными в нормативных документах.

5.3. Руководители подразделений, владельцы и пользователи ОТСС обязаны вносить предложения о приостановке работ с использованием сведений, составляющих конфиденциальную или служебную тайну, в случае обнаружения утечки (или предпосылок к утечке) этих сведений.