

# АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ

## «ГЛИНКОВСКИЙ район» Смоленской области

**П О С Т А Н О В Л Е Н И Е**

от 30 июля 2018 г. № 251

|  |  |
| --- | --- |
| Об утверждении Положения о порядке организации и проведения работ по защите конфиденциальной информации в Администрации муниципального образования «Глинковский район» Смоленской области |  |

В целях выполнения требований руководящих документов в области защиты информации ограниченного распространения

Администрация муниципального образования «Глинковский район» Смоленской области 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. Руководителям структурных подразделений Администрации ознакомить всех сотрудников с указанным Положением и обеспечить его исполнение.

3. Контроль за исполнением настоящего постановления возложить на начальника отдела по информационной политике Администрации муниципального образования «Глинковский район» Смоленской области О.В. Кожухову.

4. Постановление Администрации муниципального образования «Глинковский район» Смоленской области от 18.05.2012 г. № 146 «Об утверждении Положения о порядке организации и проведения работ по защите конфиденциальной информации» признать утратившим силу.

Глава муниципального образования

«Глинковский район»

Смоленской области М.З. Калмыков

|  |  |
| --- | --- |
|  | Приложение к постановлению Администрации муниципального образования «Глинковский район» Смоленской области  от 30 июля 2018 г. № 251 |

# Положение

# о порядке организации и проведения работ по защите конфиденциальной информации в Администрации муниципального образования «Глинковский район» Смоленской области

# Общие положения

* 1. Настоящее Положение определяет порядок организации и проведения работ по защите конфиденциальной информации в Администрации муниципального образования «Глинковский район» Смоленской области (далее – Администрация).
  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.
  3. Информационные системы и ресурсы Администрации района подлежат обязательному учету и защите.

1.4. Конфиденциальная информация должна обрабатываться (передаваться) с использованием защищенных систем и средств информатизации и связи или с использованием технических и программных средств технической защиты конфиденциальной информации.

1.5. 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. Для сведений, составляющих служебную тайну, не ниже требований, установленных данным документом и государственными стандартами Российской Федерации.

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. Объектами защиты в Администрации являются:

- 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);

- помещения (служебные кабинеты, актовые, конференц-залы и т.п.), специально предназначенные для проведения конфиденциальных мероприятий – защищаемые помещения (ЗП).

* 1. Ответственность за выполнение требований настоящего Положения возлагается на управляющего делами Администрации, руководителей структурных подразделений Администрации, а также на специалистов Администрации, допущенных к обработке, передаче и хранению в технических средствах информации, содержащей конфиденциальную информацию.

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

2.1. 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.

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

# 3. Оценка возможностей технических разведок и других источников

# угроз безопасности конфиденциальной информации

3.1**.** Для добывания конфиденциальных сведений могут использоваться:

- портативная возимая (носимая) аппаратура радио, акустической, визуально-оптической и телевизионной разведки, а также разведки побочных электромагнитных излучений и наводок (ПЭМИН);

- автономная автоматическая аппаратура акустической и телевизионной разведки, а также разведки ПЭМИН;

- компьютерная разведка, использующая различные способы и средства несанкционированного доступа к информации и специальных воздействий на нее.

Угроза компьютерной разведки объектам защиты возможна в случае подключения АС, обрабатывающим информацию ограниченного доступа, к внешним, в первую очередь, глобальным сетям.

Портативная возимая аппаратура разведки может применяться из ближайших зданий и автомобилей на стоянках вблизи зданий.

Портативная носимая аппаратура имеет ограниченные возможности и может быть использована лишь для уточнения данных или перехвата информации в непосредственной близости от защищаемых объектов.

Автономная автоматическая аппаратура радио, акустической, телевизионной, а также разведки ПЭМИН используется для длительного наблюдения за объектом защиты.

3.2. Несанкционированный доступ (далее - НСД) к информации и специальные воздействия на нее могут осуществляться при ее обработке на отдельных автоматизированных рабочих местах, в локальных вычислительных сетях, в распределенных телекоммуникационных системах.

3.3. Кроме перехвата информации техническими средствами возможно непреднамеренное попадание защищаемой информации к лицам, не допущенным к ней, но находящимся в пределах контролируемой зоны (далее - КЗ). Это возможно, например, вследствие:

* непреднамеренного прослушивания без использования технических средств конфиденциальных разговоров из-за недостаточной звукоизоляции ограждающих конструкций, защищаемых помещений и их инженерно-технических систем;
* случайного прослушивания телефонных разговоров при проведении профилактических работ в сетях телефонной связи;
* некомпетентных или ошибочных действий пользователей и администраторов АС при работе вычислительных сетей;
* просмотра информации с экранов дисплеев и других средств ее отображения.

3.4. Оценка возможностей средств технической разведки осуществляется с использованием нормативных документов ФСТЭК России.

Наиболее опасной является аппаратура портативной (возимой и носимой) разведки электромагнитных излучений и аппаратура акустической речевой разведки, которая может применяться с прилегающей к зданиям администрации территорий, а также автономная автоматическая аппаратура акустической речевой разведки, скрытно устанавливаемая внутри помещений.

3.5. Оценка возможности НСД к информации в средствах вычислительной техники и автоматизированных системах осуществляется с использованием руководящих документов ФСТЭК России.

НСД к информации и специальные воздействия на нее реально возможны, если не выполняются требования перечисленных выше документов, дифференцированные в зависимости от степени конфиденциальности обрабатываемой информации, уровня полномочий пользователей по доступу к конфиденциальной информации и режимов обработки данных в автоматизированных системах.

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

4.1. Разработка мер и обеспечение 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. Объекты информатизации должны быть аттестованы по требованиям безопасности информации в соответствии с нормативными документами ФСТЭК России.

4.4. Ответственность за обеспечение требований по технической защите конфиденциальной информации возлагается на должностное лицо, эксплуатирующее объекты информатизации.

4.5. Порядок организации антивирусной защиты конфиденциальной информации при ее обработке техническими средствами в Администрации определен инструкцией по организации антивирусной защиты информации в АС органов местного самоуправления муниципального образования «Глинковский район» Смоленской области.

4.6. Порядок организации парольной защиты конфиденциальной информации при ее обработке техническими средствами в Администрации определен инструкцией по организации парольной защиты в АС Администрации муниципального образования "Глинковский район» Смоленской области.

# Обязанности и права должностных лиц

5.1. Руководство технической защитой конфиденциальной информации в Администрации возлагается на ответственного за защиту информации.

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

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

5.4. 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.

**6. Контроль состояния технической защиты конфиденциальной информации**

6.1. Основными задачами контроля состояния технической защиты конфиденциальной информации являются оценка уровня и эффективности принятых мер защиты, своевременное выявление и предотвращение утечки по техническим каналам информации, составляющей конфиденциальную или служебную тайну, НСД к информации, преднамеренных программно-технических воздействий на информацию с целью ее уничтожения, искажения, блокирования, нарушения правового режима использования информации.

6.2. Контроль заключается в проверке выполнения актов законодательства Российской Федерации по вопросам защиты конфиденциальной информации, решений ФСТЭК России, наличия соответствующих документов по технической защите конфиденциальной информации.