# АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ

## «ВЕЛИЖСКИЙ район»

**ПОСТАНОВЛЕНИЕ**

от 22.05.2020 № 223

|  |  |
| --- | --- |
| Об утверждении Положения о порядке организации и проведения работ по защите информации ограниченного доступа в Администрации муниципального образования «Велижский район» |  |

В целях выполнения требований руководящих документов в области защиты информации ограниченного допуска Администрация муниципального образования «Велижский район»

ПОСТАНОВЛЯЕТ:

# 1. Утвердить прилагаемое Положение о порядке организации и проведении работ по защите информации органичного доступа в Администрации муниципального образования «Велижский район».

2. Руководителям структурных подразделений Администрации муниципального образования «Велижский район» ознакомить всех сотрудников с указанным Положением и обеспечить его исполнение.

3. Контроль за исполнением настоящего постановления возложить на заместителя Главы муниципального образования «Велижский район» Е.А. Шаловскую.

4. Настоящее постановление вступает в силу со дня его подписания.

Глава муниципального образования

«Велижский район» В.В. Самулеев

|  |  |
| --- | --- |
|  | Приложение  Утверждено  постановлением Администрации муниципального образования «Велижский район»  от 22.05.2020 № 223 |

# ПОЛОЖЕНИЕ

# о порядке организации и проведение работ по защите информации ограниченного доступа в Администрации муниципального образования «Велижский район»

# Общие положения

* 1. Настоящее Положение определяет порядок организации и проведения работ по защите информации ограниченного доступа в Администрации муниципального образования «Велижский район» (далее – Администрация).
  2. Мероприятия по защите информации ограниченного доступа, 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 подлежат обязательному учету и защите.

1.4. Информация ограниченного доступа должна обрабатываться (передаваться) с использованием защищенных систем и средств информатизации и связи или с использованием технических и программных средств технической защиты информации ограниченного доступа.

1.5. Уровень технической защиты информации ограниченного доступа, а также перечень необходимых мер защиты определяется дифференцировано по результатам обследования объекта информатизации, с учетом соотношения затрат на организацию технической защиты информации ограниченного доступа 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) информации ограниченного доступа, должны быть аттестованы в условиях эксплуатации на предмет соответствия принимаемых мер и средств защиты требуемому уровню безопасности информации.

Проведение любых мероприятий и работ с информацией ограниченного доступа 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 (далее - ЛВС), средства и системы связи и передачи информации, переговорные устройства, средства изготовления и тиражирования документов, используемые для обработки, хранения и передачи информации, содержащей информацию ограниченного доступа - далее основные технические средства и системы;

- технические средства и системы, не обрабатывающие информацию, но размещенные в помещениях, где обрабатывается информация ограниченного доступа

- далее вспомогательные технические средства и системы;

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

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

2.1. Доступ к информации ограниченного доступа, нарушение ее целостности и доступности возможно реализовать за счет:

* несанкционированного доступа к информации ограниченного доступа при ее обработке в информационных системах и ресурсах;
* утечки информации ограниченного доступа по техническим каналам.

# 3. Оценка возможностей технических разведок и других источников

# угроз безопасности информации ограниченного доступа

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 к автоматизированной системе, 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 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. 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 несанкционированного доступа к информации в средствах вычислительной техники и автоматизированных системах осуществляется с использованием руководящих документов ФСТЭК России.

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

4.1. Разработка мер и обеспечение защиты информации ограниченного доступа осуществляют системные администраторы Администрации.

4.2. Для защиты информации ограниченного доступа 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 информации ограниченного доступа возлагается на должностное лицо, эксплуатирующее объекты информатизации.

4.5. Порядок организации антивирусной защиты информации ограниченного доступа при ее обработке техническими средствами в Администрации определен инструкцией по организации антивирусной защиты автоматизированной системы в Администрации муниципального образования «Велижский район» утверждённый постановлением Администрации муниципального образования «Велижский район» от 21.05.2020 № 219.

4.6. Порядок организации парольной защиты информации ограниченного доступа при ее обработке техническими средствами в Администрации определен инструкцией по организации парольной защиты информационных систем персональных данных в Администрации муниципального образования «Велижский район» утверждённый постановлением Администрации муниципального образования «Велижский район» от 21.05.2020 № 218.

# Обязанности и права должностных лиц

5.1. Руководство технической защитой информации ограниченного доступа 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 основных технических средств и систем обеспечивают уровень технической защиты информации в соответствии с требованиями (нормами), установленными в нормативных документах.

5.4. Руководители структурных подразделений, владельцы и пользователи основных технических средств и систем 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 информации ограниченного доступа**

6.1. Контроль состояния защиты информации осуществляет ответственный за защиту информации, содержащей персональные данные на объектах информатизации в Администрации в целях предотвращения утечки информации по техническим каналам, несанкционированного доступа к информации, хищения технических средств и носителей информации.

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