

Инструкция
ответственного за обработку персональных данных
в Государственном бюджетном учреждении "Центр социального
обслуживания граждан пожилого возраста и инвалидов
Большемурашкинского района"

1. Общие положения

1.1. Настоящая Инструкция ответственного за обработку персональных данных государственного бюджетного учреждения "Центр социального обслуживания граждан пожилого возраста и инвалидов Большемурашкинского района" (далее - Инструкция) разработано в соответствии с Федеральным законом от 27.07.2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями), Федеральным законом от 27.07.2006г. № 152-ФЗ «О персональных данных» (с изменениями), постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства РФ от 15 сентября 2008 года № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации» и определяет обязанности, полномочия и ответственность лиц, ответственных за обработку персональных данных в государственном бюджетном учреждении "Центр социального обслуживания граждан пожилого возраста и инвалидов Большемурашкинского района" (далее - Учреждение).

1.2. Цель разработки Инструкции - обеспечение защиты персональных данных работников Учреждения при обработке их персональных данных, а также установление ответственности должностных лиц, имеющих доступ к персональным данным работников Учреждения, за невыполнение требований норм регулирующих обработку и защиту персональных данных.

1.3. Ответственный за обработку персональных данных назначается приказом директора Учреждения.

1.4. Ответственный за организацию обработки персональных данных обладает правами доступа к любым носителям персональных данных в Учреждении.

2. Термины и определения

2.1. **Автоматизированное рабочее место (АРМ)** - персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.

2.2. **Блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

2.3. **Доступ к информации** - возможность получения информации и её использования.

2.4. **Защита информации** - деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на информацию, то есть процесс, направленный на достижение информационной безопасности.

2.5. **Информация** - сведения (сообщения, данные) независимо от формы их представления.

2.6. **Информационная система персональных данных (ИСПДн)** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.7. **Несанкционированный доступ (НСД)** - доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций, путём изменения (повышения, фальсификации) своих прав доступа.

2.8. **Носитель информации** - любой материальный объект или среда, используемый для хранения или передачи информации.

2.9. **Обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.10. **Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

2.11. **Средство защиты информации (СЗИ)** – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

2.12.. **Пользователи** - работники Учреждения допущенные к обработке персональных данных согласно утвержденному приказом директора Учреждения перечню должностей.

2.13. **Угрозы безопасности персональных данных (УБПДн)** - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, предоставление,

распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных.

2.14. **Уничтожение персональных данных** - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

2. Обязанности ответственного за обработку персональных данных в Учреждении

Ответственный за обработку персональных данных обязан:

3.1. Знать перечень и условия обработки персональных данных в Учреждении.

3.2. Знать и предоставлять на утверждение директора Учреждения изменения к списку лиц, доступ которых к персональным данным необходим для выполнения ими своих служебных (трудовых) обязанностей.

3.3. Участвовать в определении полномочий пользователей ИСПДн (оформлении разрешительной системы доступа), минимально необходимых им для выполнения служебных (трудовых) обязанностей.

3.4. Осуществлять учёт документов содержащих персональные данные, их уничтожение, либо контроль процедуры их уничтожения.

3.5. Блокировать доступ к персональным данным при обнаружении нарушений порядка их обработки.

3.6. Реагировать на попытки несанкционированного доступа к информации в установленном ст.4 настоящей Инструкции порядке.

3.7. Контролировать осуществление мероприятий по установке и настройке средств защиты информации.

3.8. Проводить занятия и инструктажи с сотрудниками Учреждения о порядке работы с персональными данными и изучение руководящих документов в области обеспечения безопасности персональных данных.

3.9. Проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных.

3.10. Контролировать соблюдение сотрудниками локальных документов, регламентирующих порядок работы с программными, техническими средствами ИСПДн и персональными данными.

3.11. Вносить свои предложения по совершенствованию мер защиты персональных данных в ИСПДн, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищённости персональных данных.

3.12. Организовать учёт обращений субъектов персональных данных, контролировать заполнение «Журнала учета обращений субъектов персональных данных».

3.13. Знать законодательство РФ о персональных данных, следить за его изменениями.

3.14. Выполнять иные мероприятия, требуемые нормативными документами по защите персональных данных.

4. Действия при обнаружении попыток несанкционированного доступа

4.1 К попыткам несанкционированного доступа относятся:

4.1.1. сеансы работы с персональными данными незарегистрированных пользователей, или пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истёк, или превышающих свои полномочия по доступу к данным;

4.1.2. действия третьего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учётной записи администратора или другого пользователя ИСПДн, методом подбора пароля, использования пароля, разглашённого владельцем учётной записи или любым другим методом.

4.2. При выявлении факта несанкционированного доступа ответственный за обработку персональных данных обязан:

4.2.1. прекратить несанкционированный доступ к персональным данным;

4.2.2. доложить директору Учреждения о несанкционированном доступе, его результате (успешный, неуспешный) и предпринятых действиях;

4.2.3. известить руководителя структурного подразделения, в котором работает пользователь, от имени учётной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа.

5. Права

Ответственный за обработку персональных данных имеет право:

5.1. Требовать от сотрудников Учреждения выполнения локальных нормативно-правовых актов в части работы с персональными данными.

5.2. Блокировать доступ к персональным данным любых пользователей, если это необходимо для предотвращения нарушения режима защиты персональных данных.

5.3. Проводить служебные расследования и опрашивать пользователей по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с техническими и программными средствами ИСПДн, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных.

6. Ответственность

6.1. Ответственный за обработку персональных данных при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несёт дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.