

## ПРИКАЗ

Дата **21.12.2021**

№ **19-од**

п.Тарасовский

Муниципальное  
автономное учреждение  
Тарасовского района  
«Многофункциональный  
центр предоставления  
государственных  
и муниципальных  
услуг»

### **О защите персональных данных в МАУ МФЦ Тарасовского района**

С целью обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, в целях регламентации процесса обработки персональных данных, обеспечения информационной безопасности информационных систем персональных данных в МАУ МФЦ Тарасовского района

### **ПРИКАЗЫВАЮ:**

Кирова ул., д.14  
п.Тарасовский,  
Ростовская область,  
346050  
Тел.(86386)31363  
Эл.почта:  
mfc\_tarasovskiy@  
donland.ru

1. Утвердить:
  - 1.1. Политику обработки персональных данных в МАУ МФЦ Тарасовского района согласно приложению 1 к приказу;
  - 1.2. Положение об обработке персональных данных в МАУ МФЦ Тарасовского района согласно приложению 1 к приказу;
  - 1.3. Положение об обработке персональных данных без использования средств автоматизации в МАУ МФЦ Тарасовского района согласно приложению 3 к приказу.
  - 1.4. Концепцию информационной безопасности информационных систем персональных данных согласно приложению 4 к приказу.
2. Довести содержание настоящего приказа до сведения всех сотрудников МАУ МФЦ Тарасовского района под личную подпись.
3. Разместить электронную версию приказа на странице МАУ МФЦ Тарасовского района на портале сети МФЦ Ростовской области ([www.mfc61.ru](http://www.mfc61.ru)) для свободного доступа с целью ознакомления всех заинтересованных лиц.
4. Контроль за исполнением настоящего приказа оставляю за собой.

Директор



Ю.С. Пташкина

**ПОЛИТИКА**  
**обработки персональных данных**  
**в муниципальном автономном учреждении Тарасовского района «Многофункциональный центр**  
**предоставления государственных и муниципальных услуг»**

**1. Общие положения**

Политика обработки персональных данных в Муниципальном автономном учреждении Тарасовского района «Многофункциональный центр предоставления государственных и муниципальных услуг» (далее — Политика) определяет основные принципы, цели, условия и способы обработки персональных данных, перечни субъектов и обрабатываемых в МАУ МФЦ Тарасовского района персональных данных, функции МАУ МФЦ Тарасовского района при обработке персональных данных, права субъектов персональных данных, а также реализуемые МАУ МФЦ Тарасовского района требования к защите персональных данных.

**Политика** разработана с учетом требований Конституции Российской Федерации, законодательных и иных нормативных правовых актов Российской Федерации в области персональных данных.

Положения Политики служат основой для разработки локальных нормативных актов, регламентирующих в МФЦ Тарасовского района вопросы обработки персональных данных МФЦ Тарасовского района и других субъектов персональных данных.

**2. Законодательные и иные нормативные правовые акты Российской Федерации, в соответствии с которыми определяется Политика обработки персональных данных в МФЦ Тарасовского района.**

2.1. Политика обработки персональных данных в МФЦ Тарасовского района определяется в соответствии со следующими нормативными правовыми актами:

- Трудовой кодекс Российской Федерации;
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»;
- Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства Российской Федерации от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
- Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказ Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;
- иные нормативные правовые акты Российской Федерации и нормативные документы уполномоченных органов государственной власти.

2.2. В целях реализации положений Политики в МФЦ Тарасовского района разрабатываются соответствующие локальные нормативные акты и иные документы, в том числе:

- Положение об обработке персональных данных в МФЦ Тарасовского района;
- Порядок доступа МФЦ Тарасовского района в помещения, где ведётся обработка персональных данных;
- Правила работы с обезличенными персональными данными в МФЦ Тарасовского района;
- Регламент порядка действий МФЦ Тарасовского района при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных;
- Инструкция осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в МФЦ Тарасовского района;
- иные локальные нормативные акты и документы, регламентирующие в МФЦ Тарасовского района вопросы обработки персональных данных.

**3. Основные термины и определения, используемые в локальных нормативных актах МФЦ Тарасовского района, регламентирующие вопросы обработки персональных данных**

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

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

**Оператор** — государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или

совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

**Обработка персональных данных** — любое действие (операция) или совокупность действий (операций), совершаемые 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.

**Автоматизированная обработка персональных данных** — обработка персональных данных с помощью средств вычислительной техники.

**Предоставление персональных данных** — действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

**Распространение персональных данных** — действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

**Трансграничная передача персональных данных** — передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

**Блокирование персональных данных** — временное прекращение обработки персональных данных (за исключением случаев, когда обработка необходима для уточнения персональных данных).

**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.

**Обезличивание персональных данных** — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

**Информационная система персональных данных** — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

#### **4. Принципы и цели обработки персональных данных**

4.1. МАУ МФЦ Тарасовского района, являясь оператором персональных данных, осуществляет обработку персональных данных МАУ МФЦ Тарасовского района и других субъектов персональных данных, не состоящих с МФЦ Тарасовского района в трудовых отношениях.

4.2. Обработка персональных данных в МАУ МФЦ Тарасовского района осуществляется с учетом необходимости обеспечения защиты прав и свобод МАУ МФЦ Тарасовского района и других субъектов персональных данных, в том числе защиты права на неприкосновенность частной жизни, личную и семейную тайну, на основе следующих принципов:

- обработка персональных данных осуществляется в МФЦ Тарасовского района на законной и справедливой основе;
- обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей;
- не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- обработке подлежат только персональные данные, которые отвечают целям их обработки;
- содержание и объем обрабатываемых персональных данных соответствует заявленным целям обработки;
- не допускается избыточность обрабатываемых персональных данных по отношению к заявленным целям их обработки;
- при обработке персональных данных обеспечиваются точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.
- МАУ МФЦ Тарасовского района принимаются необходимые меры либо обеспечивается их принятие по удалению или уточнению неполных или неточных персональных данных;
- хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем того требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;
- обрабатываемые персональные данные уничтожаются либо обезличиваются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4.3. Персональные данные обрабатываются в МАУ МФЦ Тарасовского района в целях:

- обеспечения соблюдения Конституции Российской Федерации, законодательных и иных нормативных правовых актов Российской Федерации, локальных нормативных актов МАУ МФЦ Тарасовского района;
- осуществления функций, полномочий и обязанностей, возложенных законодательством Российской Федерации на МАУ МФЦ Тарасовского района, в том числе по предоставлению персональных данных в органы государственной власти, в Пенсионный фонд Российской Федерации, в Фонд социального страхования Российской Федерации, в Федеральный фонд обязательного медицинского страхования, а также в иные государственные органы;
- регулирования трудовых отношений с сотрудниками МАУ МФЦ Тарасовского района (содействие в трудоустройстве, обучение и продвижение по службе, обеспечение личной безопасности, контроль количества и качества выполняемой

работы, обеспечение сохранности имущества);

- защиты жизни, здоровья или иных жизненно важных интересов субъектов персональных данных;
- подготовки, заключения, исполнения и прекращения договоров с контрагентами;
- обеспечения пропускного режима в МАУ МФЦ Тарасовского района;
- осуществления прав и законных интересов МФЦ Тарасовского района в рамках осуществления видов деятельности, предусмотренных Уставом и иными локальными нормативными актами МАУ МФЦ Тарасовского района, или третьих лиц либо достижения общественно значимых целей;
- в иных законных целях.

#### **5. Перечень субъектов, персональные данные которых обрабатываются в МАУ МФЦ Тарасовского района**

В МАУ МФЦ Тарасовского района обрабатываются персональные данные следующих категорий субъектов:

- сотрудников;
- иных граждан.

#### **6. Перечень персональных данных, обрабатываемых в МАУ МФЦ Тарасовского района**

Перечень персональных данных, обрабатываемых в МАУ МФЦ Тарасовского района, определяется в соответствии с законодательством Российской Федерации и локальными нормативными актами МАУ МФЦ Тарасовского района с учетом целей обработки персональных данных, указанных в разделе 4 Политики.

Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, в МФЦ Тарасовского района не осуществляется.

#### **7. Функции МАУ МФЦ Тарасовского района при осуществлении обработки персональных данных**

7.1. МАУ МФЦ Тарасовского района при осуществлении обработки персональных данных:

- принимает меры, необходимые и достаточные для обеспечения выполнения требований законодательства Российской Федерации и локальных нормативных актов МАУ МФЦ Тарасовского района в области персональных данных;
- принимает правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;
- назначает лицо, ответственное за организацию обработки персональных данных в МАУ МФЦ Тарасовского района;
- издает локальные нормативные акты, определяющие политику и вопросы обработки и защиты персональных данных в МАУ МФЦ Тарасовского района;
- осуществляет ознакомление МАУ МФЦ Тарасовского района, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации и локальных нормативных актов МАУ МФЦ Тарасовского района в области персональных данных, в том числе требованиями к защите персональных данных, и обучение указанных сотрудников;
- публикует или иным образом обеспечивает неограниченный доступ к настоящей Политике;
- сообщает в установленном порядке субъектам персональных данных или их представителям информацию о наличии персональных данных, относящихся к соответствующим субъектам, предоставляет возможность ознакомления с этими персональными данными при обращении и (или) поступлении запросов указанных субъектов персональных данных или их представителей, если иное не установлено законодательством Российской Федерации;
- прекращает обработку и уничтожает персональные данные в случаях, предусмотренных законодательством Российской Федерации в области персональных данных;
- совершает иные действия, предусмотренные законодательством Российской Федерации в области персональных данных.

#### **8. Условия обработки персональных данных в МАУ МФЦ Тарасовского района**

8.1. Обработка персональных данных в МАУ МФЦ Тарасовского района осуществляется с согласия субъекта персональных данных на обработку его персональных данных, если иное не предусмотрено законодательством Российской Федерации в области персональных данных.

8.2. МАУ МФЦ Тарасовского района без согласия субъекта персональных данных не раскрывает третьим лицам и не распространяет персональные данные, если иное не предусмотрено федеральным законом.

8.3. МАУ МФЦ Тарасовского района вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных на основании заключаемого с этим лицом договора. Договор должен содержать перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели обработки, обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона «О персональных данных».

8.4. В целях внутреннего информационного обеспечения МАУ МФЦ Тарасовского района может создавать внутренние справочные материалы, в которые с письменного согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации, могут включаться его фамилия, имя, отчество, место работы, должность, год и место рождения, адрес, абонентский номер, адрес электронной почты, иные персональные данные, сообщаемые субъектом персональных данных.

8.5. Доступ к обрабатываемым в МАУ МФЦ Тарасовского района персональным данным разрешается только сотрудникам МАУ МФЦ Тарасовского района, согласно перечня должностей работников, допущенных к работе с

персональными данными и замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным в МАУ МФЦ Тарасовского района.

## **9. Перечень действий с персональными данными и способы их обработки**

9.1. МАУ МФЦ Тарасовского района осуществляет сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление и уничтожение персональных данных.

9.2. Обработка персональных данных в МАУ МФЦ Тарасовского района осуществляется следующими способами:

- неавтоматизированная обработка персональных данных;
- автоматизированная обработка персональных данных с передачей полученной информации по информационно-телекоммуникационным сетям или без таковой;
- смешанная обработка персональных данных.

## **10. Права субъектов персональных данных**

10.1. Субъекты персональных данных имеют право на:

- полную информацию об их персональных данных, обрабатываемых в МАУ МФЦ Тарасовского района;
- доступ к своим персональным данным, включая право на получение копии любой записи, содержащей их персональные данные, за исключением случаев, предусмотренных федеральным законом;
- уточнение своих персональных данных, их блокирование или уничтожение в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- отзыв согласия на обработку персональных данных;
- принятие предусмотренных законом мер по защите своих прав;
- обжалование действия или бездействия МФЦ Тарасовского района, осуществляемого с нарушением требований законодательства Российской Федерации в области персональных данных, в уполномоченный орган по защите прав субъектов персональных данных или в суд;
- осуществление иных прав, предусмотренных законодательством Российской Федерации.

## **11. Меры, принимаемые МАУ МФЦ Тарасовского района для обеспечения выполнения обязанностей оператора при обработке персональных данных**

11.1. Меры, необходимые и достаточные для обеспечения выполнения МАУ МФЦ Тарасовского района обязанностей оператора, предусмотренных законодательством Российской Федерации в области персональных данных, включают:

- наличие ответственного за обработку персональных данных;
- наличие администратора информационных систем персональных данных;
- наличие утвержденных инструкций, регламентирующих работу с персональными данными и информационными системами персональных данных;
- осуществление внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных;
- ознакомление всех сотрудников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику организации в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных под роспись;
- учет машинных носителей персональных данных;
- обеспечение восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- наличие правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных;
- определён перечень сотрудников, осуществляющих обработку персональных данных;
- сведения на бумажных носителях хранятся в сейфах или выделенных помещениях;
- определены места хранения персональных данных;
- ведётся учёт всех защищаемых носителей информации с помощью их маркировки и занесения учетных данных в журнал учета с отметкой об их выдаче (приеме);
- обеспечено раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.
- иные меры, предусмотренные законодательством Российской Федерации в области персональных данных.

11.2. Меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных устанавливаются в соответствии с локальными нормативными актами МАУ МФЦ Тарасовского района, регламентирующими вопросы обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных МФЦ Тарасовского района.

## **12. Контроль за соблюдением законодательства Российской Федерации и локальных нормативных актов МАУ МФЦ Тарасовского района в области персональных данных, в том числе требований к защите персональных данных.**

12.1. Контроль за соблюдением законодательства Российской Федерации и локальных нормативных актов МАУ МФЦ Тарасовского района в области персональных данных, в том числе требований к защите персональных данных, осуществляется с целью проверки соответствия обработки персональных данных в МАУ МФЦ Тарасовского района и локальным нормативным актам МФЦ Тарасовского района в области персональных данных, в том числе требованиям к

защите персональных данных, а также принятых мер, направленных на предотвращение и выявление нарушений законодательства Российской Федерации в области персональных данных, выявления возможных каналов утечки и несанкционированного доступа к персональным данным, устранения последствий таких нарушений.

12.2. Внутренний контроль за соблюдением законодательства Российской Федерации и локальных нормативных актов МАУ МФЦ Тарасовского района в области персональных данных, в том числе требований к защите персональных данных, осуществляется лицом, ответственным за организацию обработки персональных данных в МАУ МФЦ Тарасовского района.

12.3. Внутренний контроль соответствия обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, настоящей Политике, локальным нормативным актам МАУ МФЦ Тарасовского района осуществляет Ответственный за организацию обработки персональных данных.

12.4. Работники МАУ МФЦ Тарасовского района, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

**ПОЛОЖЕНИЕ**  
**об обработке персональных данных**  
**в муниципальном автономном учреждении Тарасовского района «Многофункциональный центр**  
**предоставления государственных и муниципальных услуг»**

**1. Общие положения**

1.1. Настоящее Положение об обработке персональных данных (далее — Положение) в муниципальном автономном учреждении Тарасовского района «Многофункциональный центр предоставления государственных и муниципальных услуг» (далее – МАУ МФЦ Тарасовского района) разработано в соответствии с Конституцией Российской Федерации, Федеральным законом «Об информации, информационных технологиях и о защите информации», Федеральным законом «О персональных данных».

1.2. Цель Положения — определение порядка обработки персональных данных в МАУ МФЦ Тарасовского района, обеспечение защиты прав и свобод субъектов персональных данных при обработке их персональных данных, а также установление ответственности работников, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3. Порядок ввода в действие и изменения Положения.

1.3.1. Настоящее Положение вступает в силу с момента его утверждения директором МАУ МФЦ Тарасовского района и действует в течение трёх лет, после чего должно быть пересмотрено.

1.3.2. Все изменения в Положение вносятся приказом.

1.4. Все работники МАУ МФЦ Тарасовского района, имеющие доступ к персональным данным, должны быть ознакомлены с настоящим Положением под роспись.

1.5. Режим конфиденциальности персональных данных снимается только в случаях их обезличивания.

**2. Основные понятия и состав персональных данных**

2.1. Для целей настоящего Положения используются следующие основные понятия:

**персональные данные** — любая информация, относящаяся к определенному или определяемому на основании такой информации субъекту, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и прочая дополнительная информация;

**обработка персональных данных** — сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных;

**конфиденциальность персональных данных** — обязательное требование для работника, получившего доступ к персональным данным, не допускать их распространения без согласия субъекта персональных данных или иного законного основания;

**распространение персональных данных** — действия, направленные на передачу персональных данных определенному кругу лиц или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

**использование персональных данных** — действия (операции) с персональными данными, совершаемые работниками в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъектов персональных данных либо иным образом затрагивающих их права и свободы или права и свободы других лиц;

**блокирование персональных данных** — временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

**уничтожение персональных данных** — действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

**обезличивание персональных данных** — действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

**общедоступные персональные данные** — персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

**информация** — сведения (сообщения, данные) независимо от формы их представления;

**документированная информация** — зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

2.2. В состав персональных данных входят сведения, содержащие информацию о паспортных данных, образовании, отношении к воинской обязанности, семейном положении, месте жительства, состоянии здоровья и другая информация, позволяющая идентифицировать субъекта персональных данных и получить о нём дополнительную информацию.

### **3. Цели обработки персональных данных их состав и сроки обработки**

3.1. Обработка персональных данных сотрудников осуществляется в целях обеспечения соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации, предоставления образовательных услуг, ведения кадрового и бухгалтерского учета, и выполнения функций, возложенных законодательством Российской Федерации.

3.2. Состав обрабатываемых персональных данных определяется в соответствии с перечнем персональных данных, обрабатываемых в Муниципальном автономном учреждении Тарасовского района «Многофункциональный центр предоставления государственных и муниципальных услуг» (Приложение № 1 к данному Положению).

Персональные данные сотрудников обрабатываются до момента увольнения. Документы по личному составу, законченные делопроизводством до 1 января 2003 года, хранятся 75 лет, а документы по личному составу, законченные делопроизводством после 1 января 2003 года, хранятся 50 лет, после чего передаются на постоянное хранение в государственные архивные фонды в соответствии со ст. 22.1 Федерального закона от 22 октября 2004 г. № 125-ФЗ "Об архивном деле в Российской Федерации".

3.3. Персональные данные субъектов, не являющимися сотрудниками, в том числе персональные данные, полученные с формы обратной связи сайта МАУ МФЦ Тарасовского района, обрабатываются и хранятся до момента достижения цели обработки персональных данных, после чего уничтожаются.

3.4. Персональные данные иных субъектов, в том числе персональные данные, полученные с формы обратной связи сайта МАУ МФЦ Тарасовского района, обрабатываются и хранятся до момента достижения цели обработки персональных данных, после чего уничтожаются.

### **4. Сбор, обработка и защита персональных данных**

#### **4.1. Порядок получения персональных данных**

Доступ к персональным данным разрешен сотрудникам, указанным в перечне должностей работников, допущенных к работе с персональными данными, и замещение которых предусматривает осуществление обработки персональных данных либо, осуществление доступа к персональным данным, в муниципальном автономном учреждении Тарасовского района «Многофункциональный центр предоставления государственных и муниципальных услуг» (Приложение № 2 к данному Положению).

Перед допуском к работе с персональными данными, предоставлением персональных данных для выполнения служебных обязанностей с работника необходимо взять письменное обязательство о неразглашении персональных данных (Приложение № 3 к данному Положению).

Все персональные данные следует получать у субъекта персональных данных. Если персональные данные субъекта возможно получить только у третьей стороны, то субъект персональных данных должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Сотрудник МАУ МФЦ Тарасовского района должен сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа дать письменное согласие на их получение.

#### **4.2. Порядок обработки персональных данных.**

Субъект персональных данных предоставляет сотруднику МАУ МФЦ Тарасовского района достоверные сведения о себе. Сотрудник МАУ МФЦ Тарасовского района проверяет достоверность сведений, сверяя данные, предоставленные субъектом, с имеющимися у субъекта документами, удостоверяющими личность и иными документами подтверждающие достоверность сведений о субъекте персональных данных.

4.2.1. В соответствии со ст. 6 ФЗ-152 «О Персональных данных» сотрудники МАУ МФЦ Тарасовского района при обработке персональных данных должны соблюдать следующие общие требования:

4.2.1.1. Обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных. (Приложение № 4 к данному Положению).

4.2.1.2. Обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей.

4.2.1.3. Обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем.

4.2.1.4. Обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных.

4.2.1.5. Обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно.

4.2.2. Защита персональных данных от неправомерного их использования или утраты обеспечивается МАУ МФЦ Тарасовского района за счет средств МАУ МФЦ Тарасовского района в порядке, установленном законодательством.

Отказ гражданина от своих прав на сохранение и защиту тайны недействителен.

4.2.3. Обработка персональных данных субъекта о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни разрешается в случаях, если:

- субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;

- обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну.

4.2.4. Автоматизированная обработка персональных данных разрешается в информационных системах персональных данных перечисленных в перечне информационных систем персональных данных, принадлежащих Муниципальному автономному учреждению Тарасовского района «Многофункциональный центр предоставления государственных и муниципальных услуг» (Приложение № 5 к данному Положению).

## **5. Передача и хранение персональных данных**

5.1. При передаче персональных данных необходимо соблюдать следующие требования:

5.1.1. Не сообщать персональные данные субъекта третьей стороне без его письменного согласия, за исключением случаев, установленных федеральным законодательством.

5.1.2. Предупредить лиц, получивших персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц письменное подтверждение того, что это правило соблюдено. Лица, получившие персональные данные, обязаны соблюдать режим конфиденциальности. Данное Положение не распространяется на обмен персональными данными субъектов в порядке, установленном федеральными законами.

5.1.3. Осуществлять передачу персональных данных субъектов в пределах МАУ МФЦ Тарасовского района в соответствии с настоящим Положением и другими внутренними нормативно-правовыми актами по защите информации.

5.1.4. При передаче персональных данных за пределы МАУ МФЦ Тарасовского района в другие организации в целях выполнения производственных функций (аутсорсинг, аутстаффинг и т.п.) заключать договоры с указанием в них о том, что переданные персональные данные могут быть использованы только в целях, для которых они сообщены

5.1.5. Разрешать доступ к персональным данным субъектов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретной функции.

5.2. Персональные данные субъектов могут обрабатываться и храниться, как на бумажных носителях, так и в электронном виде.

## **6. Уничтожение персональных данных**

6.1. Уничтожение документов, содержащих персональные данные, в том числе черновиков, бракованных листов и испорченных копий, должно производиться комиссией.

6.2. Порядок уничтожения документов, черновиков, испорченных листов, неподписанных проектов документов, содержащих персональные данные:

- документы, черновики документов, испорченные листы, варианты и неподписанные проекты документов разрываются таким образом, чтобы было невозможно дальнейшее восстановление информации. В учетных данных документа (карточке, журнале) делается отметка об уничтожении черновика с указанием количества листов и проставлением подписи сотрудника и даты;

- уничтожение документов, содержащих персональные данные, производится в строгом соответствии со сроками хранения.

6.3. Уничтожение персональных данных в электронном виде осуществляется путём удаления информации со всех носителей и резервных копий без возможности дальнейшего восстановления.

6.4. Разрешение на уничтожение персональных данных дает руководитель МАУ МФЦ Тарасовского района.

## **7. Доступ к персональным данным**

7.1. Доступ сотрудников к персональным данным осуществляется на основании разрешительной системы доступа. 7.2. Копировать и делать выписки персональных данных разрешается исключительно в служебных целях с письменного разрешения директора МАУ МФЦ Тарасовского района.

7.3. Передача персональных данных третьей стороне возможна только при письменном согласии субъекта персональных данных, либо на основании законодательства Российской Федерации.

7.4. Передача персональных данных третьей стороне в случаях, не предусмотренных законодательством Российской Федерации осуществляется на договорной основе с указанием в договоре о том, что переданные персональные данные могут быть использованы только в целях, для которых они сообщены.

## **8. Правила работы с обезличенными данными**

8.1. Обезличиванием персональных данных называются действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных (например, статистические данные).

8.2. Обезличивание персональных данных в МАУ МФЦ Тарасовского района при обработке персональных данных с использованием средств автоматизации осуществляется с помощью специализированного программного обеспечения на основании нормативно правовых актов, правил, инструкций, руководств, регламентов, инструкций на такое программное обеспечение и иных документов для достижения заранее определенных и заявленных целей.

8.3. Допускается обезличивание персональных данных при обработке персональных данных без использования

средств автоматизации - производить способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

8.4. Работа с обезличенными данными осуществляется в порядке установленным законодательством Российской Федерации и внутренними нормативно-правовыми актами, регулирующими работу с персональными данными.

## **9. Порядок внутреннего контроля за соблюдением требований по обработке и обеспечению безопасности данных**

9.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в МАУ МФЦ Тарасовского района организуется проведение периодических проверок условий обработки персональных данных. Проверки осуществляются ответственным за организацию обработки персональных данных в МФЦ Тарасовского района либо комиссией, образуемой директором МФЦ Тарасовского района не реже одного раза в 3 года.

9.2. При осуществлении внутреннего контроля соответствия обработки персональных данных установленным требованиям в МАУ МФЦ Тарасовского района производится проверка:

- соблюдения принципов обработки персональных данных в МАУ МФЦ Тарасовского района;
- соответствия локальных актов в области персональных данных МАУ МФЦ Тарасовского района действующему законодательству Российской Федерации;
- выполнения сотрудниками МАУ МФЦ Тарасовского района требований и правил (в том числе особых) обработки персональных данных в информационных системах персональных данных МАУ МФЦ Тарасовского района;
- перечней персональных данных, используемых для решения задач и функций структурными подразделениями МАУ МФЦ Тарасовского района и необходимости обработки персональных данных в информационных системах персональных данных МАУ МФЦ Тарасовского района;
- правильность осуществления сбора, систематизации, сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения персональных данных в каждой информационной системе персональных данных МАУ МФЦ Тарасовского района;
- актуальность перечня должностей сотрудников МАУ МФЦ Тарасовского района, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;
- актуальность перечня должностей сотрудников МАУ МФЦ Тарасовского района, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных;
- соблюдение прав субъектов персональных данных, чьи персональные данные обрабатываются в информационных системах персональных данных МАУ МФЦ Тарасовского района;
- соблюдение обязанностей МАУ МФЦ Тарасовского района, предусмотренных действующим законодательством в области персональных данных;
- порядка взаимодействия с субъектами персональных данных, чьи персональные данные обрабатываются в информационных системах персональных данных МАУ МФЦ Тарасовского района, в том числе соблюдения сроков, предусмотренных действующим законодательством в области персональных данных, соблюдения требований по уведомлениям, порядка разъяснения субъектам персональных данных необходимой информации, порядка реагирования на обращения субъектов персональных данных, порядка действий при достижении целей обработки персональных данных и отзыве согласий субъектами персональных данных;
- наличие необходимых согласий субъектов персональных данных, чьи персональные данные обрабатываются в информационных системах персональных данных МАУ МФЦ Тарасовского района;
- актуальность сведений, содержащихся в уведомлении МАУ МФЦ Тарасовского района об обработке персональных данных;
- актуальность перечня информационных систем персональных данных в МАУ МФЦ Тарасовского района;
- наличие и актуальность сведений, содержащихся в Правилах обработки персональных данных для каждой информационной системы персональных данных МАУ МФЦ Тарасовского района;
- знания и соблюдение сотрудниками МФЦ Тарасовского района положений действующего законодательства Российской Федерации в области персональных данных;
- знания и соблюдение сотрудниками МАУ МФЦ Тарасовского района положений локальных актов МАУ МФЦ Тарасовского района в области обработки и обеспечения безопасности персональных данных;
- знания и соблюдение сотрудниками МАУ МФЦ Тарасовского района инструкций, руководств и иных эксплуатационных документов на применяемые средства автоматизации, в том числе программное обеспечение, и средства защиты информации;
- соблюдение сотрудниками МАУ МФЦ Тарасовского района конфиденциальности персональных данных;
- актуальность локальных актов МАУ МФЦ Тарасовского района в области обеспечения безопасности персональных данных, в том числе в Технических паспортах информационных систем персональных данных;
- соблюдение сотрудниками МФЦ Тарасовского района требований по обеспечению безопасности персональных данных;
- наличие локальных актов МФЦ Тарасовского района, технической и эксплуатационной документации технических и программных средств информационных систем персональных данных МФЦ Тарасовского района;
- иных вопросов.

9.3. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, директору

МАУ МФЦ Тарасовского района докладывает ответственный за организацию обработки персональных данных, либо председатель комиссии.

#### **10. Права субъекта персональных данных**

10.1. Субъект персональных данных имеет право получать доступ к своим персональным данным и ознакомление с ними, включая право на безвозмездное получение копий любой записи, содержащей его персональные данные.

10.2. Субъект персональных данных имеет право требовать от сотрудников МАУ МФЦ Тарасовского района уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющихся необходимыми для работы МФЦ Тарасовского района персональных данных.

10.3. Субъект персональных данных имеет право получать информацию, которая касается обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных;
- правовые основания и цели обработки персональных данных;
- цели и применяемые способы обработки персональных данных;
- наименование и место нахождения МАУ МФЦ Тарасовского района, сведения о лицах (за исключением работников МФЦ Тарасовского района), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных ФЗ-№ 152 «О персональных данных»;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные ФЗ-№ 152 «О персональных данных» или другими федеральными законами.

10.4. Субъект персональных данных имеет право требовать извещения сотрудниками МФЦ Тарасовского района всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.

#### **11. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных**

11.1. Работники МФЦ Тарасовского района, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

Директор Ю.С. Пташкина

**ПЕРЕЧЕНЬ**  
**персональных данных, обрабатываемых в муниципальном автономном учреждении Тарасовского района**  
**«Многофункциональный центр предоставления государственных и муниципальных услуг»**

В муниципальном автономном учреждении Тарасовского района «Многофункциональный центр предоставления государственных и муниципальных услуг» обрабатывается следующий перечень персональных данных:

**Персональные данные сотрудников:**

Фамилия, имя, отчество.  
Тип документа, удостоверяющего личность, серия и номер, дата выдачи, наименование органа, выдавшего документ и код его подразделения;  
Дата рождения.  
Место рождения.  
Адрес места жительства/регистрации.  
Идентификационный номер налогоплательщика (ИНН).  
Страховой номер индивидуального лицевого счета (СНИЛС).  
Сведения о гражданстве.  
Номер телефона.  
Адрес электронной почты.  
Семейное положение.  
Состав семьи, сведения о детях.  
Социальное положение.  
Образование.  
Профессия.  
Должность.  
Стаж.  
Сведения о доходах.  
Сведения о воинской обязанности и военной службе.  
Сведения об имуществе.  
Реквизиты лицевых счетов, банковских карт.

**Персональные данные субъектов, не являющихся сотрудниками:**

Фамилия, имя, отчество.  
Тип документа, удостоверяющего личность, серия и номер, дата выдачи, наименование органа, выдавшего документ и код его подразделения;  
Дата рождения.  
Место рождения  
Адрес места жительства/прописки.  
Идентификационный номер налогоплательщика (ИНН).  
Страховой номер индивидуального лицевого счета (СНИЛС).  
Сведения о гражданстве.  
Реквизиты лицевых счетов, банковских карт.  
Номер телефона.  
Адрес электронной почты.  
Семейное положение.  
Состав семьи, сведения о детях.  
Социальное положение.  
Образование.  
Профессия.  
Должность.  
Стаж.  
Сведения о доходах.  
Сведения о воинской обязанности и военной службе.  
Сведения об имуществе.

**ПЕРЕЧЕНЬ**  
**должностей работников, допущенных к работе с персональными данными, и замещение которых**  
**предусматривает осуществление обработки персональных данных либо осуществление доступа к**  
**персональным данным в муниципальном автономном учреждении Тарасовского района**  
**«Многофункциональный центр предоставления государственных и муниципальных услуг»**

Для обеспечения безопасности персональных данных при их обработке, хранении и передаче утверждаю следующий перечень должностей, допущенных к работе с персональными данными и замещение которых предусматривает осуществление обработки персональных данных либо, осуществление доступа к персональным данным:

- Директор.
- Заместитель директора.
- Главный бухгалтер.
- Главный специалист-юрист.
- Главные специалисты
- Ведущий специалисты
- Специалисты 1 категории.
- Специалисты 2 категории.

**ОБЯЗАТЕЛЬСТВО**  
**о неразглашении персональных данных**  
**в муниципальном автономном учреждении Тарасовского района «Многофункциональный центр**  
**предоставления государственных и муниципальных услуг»**

Я, \_\_\_\_\_  
(фамилия, имя, отчество работника)  
Паспорт гражданина РФ серия \_\_\_\_\_ номер \_\_\_\_\_, выдан \_\_\_\_\_,  
(орган, выдавший документ, удостоверяющий личность, дата выдачи)

исполняющий должностные обязанности \_\_\_\_\_  
(наименование должности работника)

предупрежден(а) о том, что на период исполнения мною должностных обязанностей по Трудовому договору, заключенному мною и муниципальным автономным учреждением Тарасовского района «Многофункциональный центр предоставления государственных и муниципальных услуг», и предусматривающих работу с персональными данными мне будет предоставлен доступ к информации.

**Настоящим добровольно принимаю на себя обязательства:**

Не передавать в любом виде и не разглашать третьим лицам и работникам Муниципального автономного учреждения Тарасовского района «Многофункциональный центр предоставления государственных и муниципальных услуг», не имеющим на это право в силу выполняемых ими должностных обязанностей или в соответствии с решением руководителя, информацию содержащую персональные данные (за исключением собственных данных), которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей;

В случае попытки третьих лиц или работников Муниципального автономного учреждения Тарасовского района «Многофункциональный центр предоставления государственных и муниципальных услуг», не имеющих на это право, получить от меня информацию, содержащую персональные данные, немедленно сообщить об этом факте своему непосредственному или (в случае отсутствия непосредственного) вышестоящему руководителю;

Не использовать информацию, содержащую персональные данные с целью получения выгоды;

Выполнять требования закона и иных нормативных правовых актов Российской Федерации, а также внутренних документов Муниципального автономного учреждения Тарасовского района «Многофункциональный центр предоставления государственных и муниципальных услуг», регламентирующих вопросы защиты интересов субъектов персональных данных, порядка обработки и защиты персональных данных;

После прекращения моих прав на доступ к информации, содержащей персональные данные (переход на должность, не предусматривающую доступ к персональным данным либо прекращения Трудового договора), не обрабатывать, не разглашать и не передавать третьим лицам и неуполномоченным на это работникам Муниципального автономного учреждения Тарасовского района «Многофункциональный центр предоставления государственных и муниципальных услуг», известную мне информацию, содержащую персональные данные.

Я предупрежден(-а) о том, что в случае нарушения данного обязательства буду привлечен(-а) к дисциплинарной ответственности и/или иной ответственности в соответствии с действующим законодательством Российской Федерации.

\_\_\_\_\_  
(Дата)

\_\_\_\_\_  
(Подпись)

\_\_\_\_\_  
(Фамилия, Имя, Отчество)

**ТИПОВАЯ ФОРМА**  
**согласия на обработку персональных данных работника**  
**муниципального автономного учреждения Тарасовского района «Многофункциональный центр**  
**предоставления государственных и муниципальных услуг»**

Я, \_\_\_\_\_  
(Ф.И.О. полностью)

зарегистрированный(-ая) по адресу: \_\_\_\_\_

\_\_\_\_\_, паспорт серии \_\_\_\_\_ № \_\_\_\_\_

выдан \_\_\_\_\_

\_\_\_\_\_  
(орган, выдавший паспорт и дата выдачи)

с целью исполнения определенных сторонами условий трудового договора (трудоустройства) даю согласие муниципальному автономному учреждению Тарасовского района «Многофункциональный центр предоставления государственных и муниципальных услуг», расположенному по адресу: 346050, Ростовская область, п. Тарасовский, ул. Кирова, 14, на обработку нижеследующих персональных данных:

фамилия, имя, отчество;

тип, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;

дата рождения;

место рождения;

адрес места жительства/прописки;

идентификационный номер налогоплательщика (ИНН);

страховой номер индивидуального лицевого счета (СНИЛС);

номер телефона, адрес электронной почты;

сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании), о профессиональной переподготовке и повышении квалификации;

профессия, должность, стаж;

сведения о доходах;

семейное положение, состав семьи, сведения о детях;

сведения о воинской обязанности и военной службе и реквизиты документов воинского учета;

сведения об имуществе;

информация о наличии или отсутствии судимости;

информация о наличии или отсутствии административных правонарушений за употребление наркотических и психотропных веществ;

реквизиты расчетного счета, банковской карты.

Разрешаю размещение моих персональных данных в сети Интернет на сайте муниципального автономного учреждения Тарасовского района «Многофункциональный центр предоставления государственных и муниципальных услуг».

Разрешаю сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, обезличивание, блокирование, удаление, уничтожение, а также передачу третьим лицам.

Настоящее согласие вступает в силу с момента его подписания и действительно до моего увольнения.

Данное согласие может быть отозвано по моему письменному заявлению.

\_\_\_\_\_  
(Дата)

\_\_\_\_\_  
(Подпись)

\_\_\_\_\_  
(Фамилия, Имя, Отчество)

**ПЕРЕЧЕНЬ**  
**информационных систем персональных данных, принадлежащих**  
**муниципальному автономному учреждению Тарасовского района «Многофункциональный центр**  
**предоставления государственных и муниципальных услуг»**

В муниципальном автономном учреждении Тарасовского района «Многофункциональный центр предоставления государственных и муниципальных услуг» функционируют следующие информационные системы персональных данных (ИСПДн):

1. ИСПДн «ИИС ЕС МФЦ РО»;
2. ИСПДн 1С"Бухгалтерия".

## ПОЛОЖЕНИЕ

### об обработке персональных данных без использования средств автоматизации в муниципальном автономном учреждении Тарасовского района «Многофункциональный центр предоставления государственных и муниципальных услуг».

#### 1. Общие положения

1.1. Настоящее Положение об обработке персональных данных без использования средств автоматизации в муниципальном автономном учреждении Тарасовского района «Многофункциональный центр предоставления государственных и муниципальных услуг» (далее — Положение) применяется с учетом требований постановления Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

1.2. В настоящем Положении используются следующие определения:

**блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных) (статья 3 Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее — статья 3 Федерального закона № 152-ФЗ);

**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 (статья 3 Федерального закона № 152-ФЗ);

**обработка персональных данных без использования средств автоматизации** — обработка персональных данных, при которой такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека (Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденное постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687);

**персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (статья 3 Федерального закона № 152-ФЗ).

#### 2. Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации.

2.1. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков).

2.2. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

2.3. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники Муниципального автономного учреждения Тарасовского района «Многофункциональный центр предоставления государственных и муниципальных услуг» (далее – МАУ МФЦ Тарасовского района) или лица, осуществляющие такую обработку по договору с МАУ МФЦ Тарасовского района, должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется МАУ МФЦ Тарасовского района без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов, Российской Федерации, а также локальными правовыми актами МАУ МФЦ Тарасовского района.

2.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, наименование и адрес МФЦ Тарасовского района, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых МФЦ Тарасовского района способов обработки персональных данных;

- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;

- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в

документе, не нарушая прав и законных интересов иных субъектов персональных данных.

2.5. При ведении журналов (журналов регистрации, журналов посещений), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных в помещение МАУ МФЦ Тарасовского района или в иных аналогичных целях, должны соблюдаться следующие условия:

- необходимость ведения такого журнала должна быть предусмотрена актом МАУ МФЦ Тарасовского района, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных;
- копирование содержащейся в таких журналах информации не допускается;
- персональные данные каждого субъекта персональных данных могут заноситься в такой журнал не более 1 (одного) раза в каждом случае пропуска субъекта персональных данных.

2.6. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, зачеркивание, стирание).

2.7. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

### **3. Особенности обеспечения безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации**

3.1. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

3.2. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

3.3. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются приказом директора МАУ МФЦ Тарасовского района.

### **4. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных**

4.1. Ответственность за соблюдение требований по защите информации ограниченного доступа и надлежащего порядка проводимых работ возлагается на пользователей информационных систем персональных данных (далее — ИСПДн), администратора безопасности ИСПДн и ответственного за организацию обработки персональных данных МФЦ Тарасовского района.

4.2. Сотрудники МАУ МФЦ Тарасовского района, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

4.3. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим сотрудникам, не имеющим к ним доступ), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим Положением, локальными нормативно-правовыми актами (приказами) МАУ МФЦ Тарасовского района, влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Сотрудник МАУ МФЦ Тарасовского района, имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба МАУ МФЦ Тарасовского района (в соответствии с пунктом 7 статьи 243 Трудового кодекса Российской Федерации).

4.4. В отдельных случаях, при разглашении персональных данных, сотрудник, совершивший указанный проступок, несет ответственность в соответствии со статьей 13.14 Кодекса об административных правонарушениях Российской Федерации.

4.5. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со статьей 137 Уголовного кодекса Российской Федерации.

4.6. Сотрудники МАУ МФЦ Тарасовского района за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъектов, несут административную ответственность согласно статьям 5.27 и 5.39 Кодекса об административных правонарушениях Российской Федерации, а также возмещают субъекту ущерб, причиненный неправомерным использованием информации, содержащей персональные данные этого субъекта.

## **КОНЦЕПЦИЯ** **информационной безопасности информационных систем персональных данных**

### **1. Определения**

1.1. В настоящем документе используются следующие термины и их определения.

**Автоматизированная система** – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

**Аутентификация отправителя данных** – подтверждение того, что отправитель полученных данных соответствует заявленному.

**Безопасность персональных данных** – состояние защищенности персональных данных, характеризующееся способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

**Биометрические персональные данные** – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

**Блокирование персональных данных** – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

**Вирус (компьютерный, программный)** – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

**Вредоносная программа** – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

**Вспомогательные технические средства и системы** – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

**Доступ в операционную среду компьютера (информационной системы персональных данных)** – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ. Доступ к информации – возможность получения информации и ее использования.

**Закладочное устройство** – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

**Защищаемая информация** – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

**Идентификация** – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

**Информативный сигнал** – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

**Информационная система персональных данных (ИСПДн)** – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

**Информационные технологии** – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

**Использование персональных данных** – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

**Источник угрозы безопасности информации** – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

**Контролируемая зона** – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

**Конфиденциальность персональных данных** – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

**Межсетевой экран** – локальное (однокомпонентное) или функционально-распределенное программное (программноаппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

**Нарушитель безопасности персональных данных** – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

**Неавтоматизированная обработка персональных данных** – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

**Недекларированные возможности** – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

**Несанкционированный доступ (несанкционированные действия)** – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

**Носитель информации** – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

**Обезличивание персональных данных** – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

**Обработка персональных данных** – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

**Общедоступные персональные данные** – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

**Оператор (персональных данных)** – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

**Технические средства информационной системы персональных данных** – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

**Перехват (информации)** – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

**Персональные данные** – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

**Побочные электромагнитные излучения и наводки** – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

**Политика «чистого стола»** – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

**Пользователь информационной системы персональных данных** – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

**Правила разграничения доступа** – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

**Программная закладка** – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, заблокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) заблокировать аппаратные средства.

**Программное (программно-математическое) воздействие** – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

**Раскрытие персональных данных** – умышленное или случайное нарушение конфиденциальности персональных данных.

**Распространение персональных данных** – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации,

размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

**Ресурс информационной системы** – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

**Специальные категории персональных данных** – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

**Средства вычислительной техники** – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

**Субъект доступа (субъект)** – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

**Технический канал утечки информации** – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

**Трансграничная передача персональных данных** – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

**Угрозы безопасности персональных данных** – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

**Уничтожение персональных данных** – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

**Утечка (защищаемой) информации по техническим каналам** – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

**Уязвимость** – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

**Целостность информации** – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

## **2. Обозначения и сокращения**

АВС – антивирусные средства.

АРМ – автоматизированное рабочее место.

ВТСС – вспомогательные технические средства и системы.

ИСПДн – информационная система персональных данных.

КЗ – контролируемая зона.

ЛВС – локальная вычислительная сеть.

МЭ – межсетевой экран.

НСД – несанкционированный доступ.

ОС – операционная система.

ПДн – персональные данные.

ПМВ – программно-математическое воздействие.

ПО – программное обеспечение.

ПЭМИН – побочные электромагнитные излучения и наводки.

САЗ – система анализа защищенности.

СЗИ – средства защиты информации.

СЗПДн – система (подсистема) защиты персональных данных.

СОВ – система обнаружения вторжений.

ТКУИ – технические каналы утечки информации.

УБПДн – угрозы безопасности персональных данных.

## **3. Введение**

3.1. Настоящая Концепция информационной безопасности ИСПДн муниципального автономного учреждения Тарасовского района «Многофункциональный центр предоставления государственных и муниципальных услуг» (далее – МАУ МФЦ Тарасовского района) является официальным документом, в котором определена система взглядов на обеспечение информационной безопасности МАУ МФЦ Тарасовского района.

3.2. Необходимость разработки Концепции обусловлена стремительным расширением сферы применения новейших информационных технологий и процессов при обработке информации вообще, и персональных данных в частности.

3.3. Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (СЗПДн) МАУ МФЦ Тарасовского района. Концепция определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

3.4. Концепция разработана в соответствии с системным подходом к обеспечению информационной безопасности. Системный подход предполагает проведение комплекса мероприятий, включающих исследование угроз информационной безопасности и разработку системы защиты ПДн, с позиции комплексного применения технических и

организационных мер и средств защиты.

3.5. Под информационной безопасностью ПДн понимается защищенность персональных данных и обрабатывающей их инфраструктуре от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам (субъектам ПДн) или инфраструктуре. Задачи информационной безопасности сводятся к минимизации ущерба от возможной реализации угроз безопасности ПДн, а также к прогнозированию и предотвращению таких воздействий.

3.6. Концепция служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности МАУ МФЦ Тарасовского района, а также нормативных и методических документов, обеспечивающих ее реализацию, и не предполагает подмены функций государственных органов власти Российской Федерации, отвечающих за обеспечение безопасности информационных технологий и защиту информации.

3.7. Концепция является методологической основой для:

- формирования и проведения единой политики в области обеспечения безопасности ПДн в ИСПДн МАУ МФЦ Тарасовского района;
- принятия управленческих решений и разработки практических мер по воплощению политики безопасности ПДн и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз ПДн;
- координации деятельности структурных подразделений МАУ МФЦ Тарасовского района при проведении работ по развитию и эксплуатации ИСПДн с соблюдением требований обеспечения безопасности ПДн;
- разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности ПДн в ИСПДн МФЦ Тарасовского района.

3.8. Область применения Концепции распространяется на все подразделения МАУ МФЦ Тарасовского района, в которых осуществляется автоматизированная обработка ПДн, а также на подразделения, осуществляющие сопровождение, обслуживание и обеспечение нормального функционирования ИСПДн.

3.9. Правовой базой для разработки настоящей Концепции служат требования действующих в России законодательных и нормативных документов по обеспечению безопасности персональных данных (ПДн).

#### **4. Общие положения**

4.1. Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (СЗПДн) МФЦ Тарасовского района, в соответствии с Перечнем ИСПДн. Концепция определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

4.2. СЗПДн представляет собой совокупность организационных и технических мероприятий для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий с ними.

4.3. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

4.4. Структура, состав и основные функции СЗПДн определяются исходя из класса ИСПДн. СЗПДн включает организационные меры и технические средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн), а также используемые в информационной системе информационные технологии.

4.5. Эти меры призваны обеспечить:

- конфиденциальность информации (защита от несанкционированного ознакомления);
- целостность информации (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);
- доступность информации (возможность за приемлемое время получить требуемую информационную услугу).

4.6. Стадии создания СЗПДн включают:

- предпроектная стадия, включающая предпроектное обследование ИСПДн, разработку технического (частного технического) задания на ее создание;
- стадия проектирования (разработки проектов) и реализации ИСПДн, включающая разработку СЗПДн в составе ИСПДн;
- стадия ввода в действие СЗПДн, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку соответствия ИСПДн требованиям безопасности информации.

4.7. Организационные меры предусматривают создание и поддержание правовой базы безопасности ПДн и разработку (введение в действие) предусмотренных Политикой информационной безопасности ИСПДн следующих организационно-распорядительных документов:

- инструкцию администратора информационных систем персональных данных по обеспечению безопасности персональных данных;
- инструкцию о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения и баз данных;
- инструкцию ответственного за обработку персональных данных;

- инструкцию по организации антивирусной защиты;
- инструкцию по порядку учета и хранению документов, содержащих персональные данные;
- инструкцию по обеспечению безопасности эксплуатации средств криптографической защиты информации (СКЗИ);
- инструкцию по порядку учета и хранению машинных носителей конфиденциальной информации (персональных данных);
- инструкцию пользователя информационных систем персональных данных по обеспечению безопасности персональных данных;
- инструкцию осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных;
- инструкцию пользователя по обеспечению безопасности обработки персональных данных, при возникновении внештатных ситуаций.

4.8. Технические меры защиты реализуются при помощи соответствующих программно-технических средств и методов защиты.

Перечень необходимых мер защиты информации определяется по результатам внутренней проверки безопасности ИСПДн МФЦ Тарасовского района.

## **5. Задачи СЗПДн**

5.1. Основной целью СЗПДн является минимизация ущерба от возможной реализации угроз безопасности ПДн.

5.2. Для достижения основной цели система безопасности ПДн ИСПДн должна обеспечивать эффективное решение следующих задач:

- защиту от вмешательства в процесс функционирования ИСПДн посторонних лиц (возможность использования АС и доступ к ее ресурсам должны иметь только зарегистрированные установленным порядком пользователи);
- разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам ИСПДн (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям ИСПДн для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа:
  - к информации, циркулирующей в ИСПДн;
  - средствам вычислительной техники ИСПДн;
  - аппаратным, программным и криптографическим средствам защиты, используемым в ИСПДн.
- регистрацию действий пользователей при использовании защищаемых ресурсов ИСПДн в системных журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов;
- контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;
- защиту от несанкционированной модификации и контроль целостности используемых в ИСПДн программных средств, а также защиту системы от внедрения несанкционированных программ;
- защиту ПДн от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;
- защиту ПДн, хранимой, обрабатываемой и передаваемой по каналам связи, от несанкционированного разглашения или искажения;
- обеспечение живучести криптографических средств защиты информации при компрометации части ключевой системы;
- своевременное выявление источников угроз безопасности ПДн, причин и условий, способствующих нанесению ущерба субъектам ПДн, создание механизма оперативного реагирования на угрозы безопасности ПДн и негативные тенденции;
- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности ПДн.

## **6. Объекты защиты**

### **6.1. Перечень информационных систем.**

В Муниципальном автономном учреждении Тарасовского района «Многофункциональный центр предоставления государственных и муниципальных услуг» производится обработка персональных данных в информационных системах обработки персональных данных (ИСПДн).

Перечень ИСПДн определяется на основании внутреннего обследования.

### **6.2. Перечень объектов защиты.**

Объектами защиты являются – информация, обрабатываемая в ИСПДн, и технические средства ее обработки и защиты. Перечень персональных данных, подлежащие защите, определен в Перечне персональных данных, обрабатываемых в Муниципальном автономном учреждении «Многофункциональный центр предоставления государственных и муниципальных услуг» Тарасовского района.

Объекты защиты включают:

- обрабатываемая информация;
- технологическая информация;
- программно-технические средства обработки;
- средства защиты ПДн;
- каналы информационного обмена и телекоммуникации;
- объекты и помещения, в которых размещены компоненты ИСПДн.

## 7. Классификация пользователей ИСПДн

7.1. **Пользователем ИСПДн** является лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования. Пользователем ИСПДн является любой сотрудник МАУ МФЦ Тарасовского района, имеющий доступ к ИСПДн и ее ресурсам в соответствии с установленным порядком, в соответствии с его функциональными обязанностями.

7.2. Пользователи ИСПДн делятся на три основные категории:

7.2.1. **Администратор ИСПДн** – сотрудники МАУ МФЦ Тарасовского района, который занимается настройкой, внедрением и сопровождением системы. Администратор ИСПДн обладает следующим уровнем доступа:

- обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;
- обладает полной информацией о технических средствах и конфигурации ИСПДн;
- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;
- обладает правами конфигурирования и административной настройки технических средств ИСПДн.

7.2.2. **Администратор безопасности ИСПДн** - сотрудник МАУ МФЦ Тарасовского района или сторонних организаций, который занимается разработкой программного обеспечения. Администратор безопасности ИСПДн обладает следующим уровнем доступа:

обладает информацией об алгоритмах и программах обработки информации на ИСПДн;

– обладает возможностями внесения ошибок, недеklarированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;

- может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.

7.2.3. **Пользователь ИСПДн** - сотрудник МФЦ Тарасовского района, участвующий в процессе эксплуатации ИСПДн. Пользователь ИСПДн обладает следующим уровнем доступа:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;

- располагает конфиденциальными данными, к которым имеет доступ.

7.2.4. Категории пользователей должны быть определены для каждой ИСПДн. Должно быть уточнено разделение сотрудников внутри категорий, в соответствии с типами пользователей определенными в Политике информационной безопасности.

7.2.5. Все выявленные группы пользователей отражаются в Перечне должностей работников, допущенных к работе с персональными данными и замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным в Муниципальном автономном учреждении Тарасовского района «Многофункциональный центр предоставления государственных и муниципальных услуг». На основании обследования определяются права доступа к элементам ИСПДн для всех групп пользователей и отражаются в Разрешительной системе доступа сотрудников к ресурсам информационных систем персональных данных, принадлежащих Муниципальному автономному учреждению Тарасовского района «Многофункциональный центр предоставления государственных и муниципальных услуг».

## 8. Основные принципы построения системы комплексной защиты информации

8.1. Построение системы обеспечения безопасности ПДн ИСПДн МАУ МФЦ Тарасовского района и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

- законность;
- системность;
- комплексность;
- непрерывность;
- своевременность;
- преемственность и непрерывность совершенствования;
- персональная ответственность;
- минимизация полномочий;
- взаимодействие и сотрудничество;
- гибкость системы защиты;
- открытость алгоритмов и механизмов защиты;
- простота применения средств защиты;
- научная обоснованность и техническая реализуемость;
- специализация и профессионализм;
- обязательность контроля.

### 8.2. Законность.

Предполагает осуществление защитных мероприятий и разработку СЗПДн МАУ МФЦ Тарасовского района в соответствии с действующим законодательством в области защиты ПДн и других нормативных актов по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции.

Пользователи и обслуживающий персонал ПДн ИСПДн МАУ МФЦ Тарасовского района должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за защиты ПДн.

### 8.3. Системность.

Системный подход к построению СЗПДн МАУ МФЦ Тарасовского района предполагает учет всех взаимосвязанных,

взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ПДн ИСПДн МАУ МФЦ Тарасовского района.

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки ПДн, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и НСД к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

#### **8.4. Комплексность.**

Комплексное использование методов и средств защиты предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

Защита должна строиться эшелонировано. Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Создание защитных рубежей осуществляется с учетом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невязанно связанных областях.

Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Одним из наиболее укрепленных рубежей призваны быть средства криптографической защиты, реализованные с использованием технологии VPN. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

#### **8.5. Непрерывность защиты ПДн.**

Защита ПДн – не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИСПДн.

ИСПДн должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода ИСПДн в незащищенное состояние.

Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная техническая и организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных "закладок" и других средств преодоления системы защиты после восстановления ее функционирования.

#### **8.6. Своевременность.**

Предполагает упреждающий характер мер обеспечения безопасности ПДн, то есть постановку задач по комплексной защите ИСПДн и реализацию мер обеспечения безопасности ПДн на ранних стадиях разработки ИСПДн в целом и ее системы защиты информации, в частности.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

#### **8.7. Преемственность и совершенствование.**

Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования ИСПДн и ее системы защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

#### **8.8. Персональная ответственность.**

Предполагает возложение ответственности за обеспечение безопасности ПДн и системы их обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

#### **8.9. Принцип минимизации полномочий.**

Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью, на основе принципа «все, что не разрешено, запрещено».

Доступ к ПДн должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

#### **8.10. Взаимодействие и сотрудничество.**

Предполагает создание благоприятной атмосферы в коллективах подразделений, обеспечивающих деятельность ИСПДн МАУ МФЦ Тарасовского района, для снижения вероятности возникновения негативных действий, связанных с человеческим фактором.

В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности подразделений технической защиты информации.

#### **8.11. Гибкость системы защиты ПДн.**

Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования

уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования.

#### **8.12. Открытость алгоритмов и механизмов защиты.**

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Однако, это не означает, что информация о конкретной системе защиты должна быть общедоступна.

#### **8.13. Простота применения средств защиты.**

Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).

Должна достигаться автоматизация максимального числа действий пользователей и администраторов ИСПДн.

#### **8.14. Научная обоснованность и техническая реализуемость.**

Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности ПДн.

СЗПДн должна быть ориентирована на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

#### **8.15. Специализация и профессионализм.**

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности ПДн, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами МАУ МФЦ Тарасовского района.

#### **8.16. Обязательность контроля.**

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности ПДн на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

### **9. Меры, методы и средства обеспечения требуемого уровня защищенности**

9.1. Обеспечение требуемого уровня защищенности должно достигаться с использованием мер, методов и средств безопасности. Все меры обеспечения безопасности ИСПДн подразделяются на:

- законодательные (правовые);
- морально-этические;
- организационные (административные);
- физические;
- технические (аппаратные и программные).

#### **9.2. Законодательные (правовые) меры защиты.**

К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с ПДн, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию ПДн и являющиеся сдерживающим фактором для потенциальных нарушителей.

Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

#### **9.3. Морально-этические меры защиты.**

9.3.1. К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения ЭВМ в стране или обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписанные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писанные, то есть оформленные в некоторый свод (устав) правил или предписаний.

9.3.2. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений. Морально-этические меры защиты снижают вероятность возникновения негативных действий, связанных с человеческим фактором.

#### **9.4. Организационные (административные) меры защиты.**

9.4.1. Организационные (административные) меры защиты – это меры организационного характера,

регламентирующие процессы функционирования ИСПДн, использование ресурсов ИСПДн, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с ИСПДн таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

9.4.2. Главная цель административных мер, предпринимаемых на высшем управленческом уровне – сформировать Политику информационной безопасности ПДн (отражающую подходы к защите информации) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

9.4.3. Реализация Политики информационной безопасности ПДн в ИСПДн состоят из мер административного уровня и организационных (процедурных) мер защиты информации.

9.4.4. К административному уровню относятся решения руководства, затрагивающие деятельность ИСПДн в целом. Эти решения закрепляются в Политике информационной безопасности. Примером таких решений могут быть:

- принятие решения о формировании или пересмотре комплексной программы обеспечения безопасности ПДн, определение ответственных за ее реализацию;
- формулирование целей, постановка задач, определение направлений деятельности в области безопасности ПДн;
- принятие решений по вопросам реализации программы безопасности, которые рассматриваются на уровне МАУ МФЦ Тарасовского района в целом;
- обеспечение нормативной (правовой) базы вопросов безопасности и т.п.

9.4.5. Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности ПДн, определить какими ресурсами (материальные, персонал) они будут достигнуты и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью ИСПДн.

9.4.6. На организационном уровне определяются процедуры и правила достижения целей и решения задач Политики информационной безопасности ПДн. Эти правила определяют:

- какова область применения политики безопасности ПДн;
- каковы роли и обязанности должностных лиц, отвечающие за проведение политики безопасности ПДн, а также их установить ответственность;
- кто имеет права доступа к ПДн;
- какими мерами и средствами обеспечивается защита ПДн;
- какими мерами и средствами обеспечивается контроль за соблюдением введенного режима безопасности.

9.4.7. Организационные меры должны:

- предусматривать регламент информационных отношений, исключающих возможность несанкционированных действий в отношении объектов защиты;
- определять коалиционные и иерархические принципы и методы разграничения доступа к ПДн;
- определять порядок работы с программно-математическими и техническими (аппаратные) средствами защиты и криптозащиты и других защитных механизмов;
- организовать меры противодействия НСД пользователями на этапах аутентификации, авторизации, идентификации, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

9.4.8. Организационные меры должны состоять из:

- регламента доступа в помещения ИСПДн;
- порядок допуска сотрудников к использованию ресурсов ИСПДн МАУ МФЦ Тарасовского района;
- регламента процессов ведения баз данных и осуществления модификации информационных ресурсов;
- регламента процессов обслуживания и осуществления модификации аппаратных и программных ресурсов ИСПДн;
- инструкций пользователей ИСПДн (администратора ИСПДн, пользователя ИСПДн);
- инструкция пользователя при возникновении внештатных ситуаций.

## 9.5. Физические меры защиты.

9.5.1. Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

9.5.2. Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации, исключающими нахождение внутри контролируемой (охраняемой) зоны технических средств разведки.

## 9.6. Аппаратно-программные средства защиты ПДн.

9.6.1. Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав ИСПДн и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

9.6.2. С учетом всех требований и принципов обеспечения безопасности ПДн в ИСПДн по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

- средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей ИСПДн;
- средства разграничения доступа зарегистрированных пользователей системы к ресурсам ИСПДн МАУ МФЦ Тарасовского района;

- средства обеспечения и контроля целостности программных и информационных ресурсов;
- средства оперативного контроля и регистрации событий безопасности;
- криптографические средства защиты ПДн.

9.6.3. Успешное применение технических средств защиты на основании принципов (раздел 8) предполагает, что выполнение перечисленных ниже требований обеспечено организационными (административными) мерами и используемыми физическими средствами защиты:

- обеспечена физическая целостность всех компонент ИСПДн;
- каждый сотрудник (пользователь ИСПДн) или группа пользователей имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;
- все изменения конфигурации технических и программных средств ИСПДн производятся строго установленным порядком (регистрируются и контролируются) только на основании приказов руководства МАУ МФЦ Тарасовского района;
- сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (специальных помещениях, шкафах и т.п.);
- специалистами МАУ МФЦ Тарасовского района осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

#### **10. Контроль эффективности системы защиты**

10.1 Контроль эффективности СЗПДн должен осуществляться на периодической основе. Целью контроля эффективности является своевременное выявление ненадлежащих режимов работы СЗПДн (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), а также прогнозирование и превентивное реагирование на новые угрозы безопасности ПДн.

10.2. Контроль может проводиться как администраторами ИСПДн (оперативный контроль в процессе информационного взаимодействия в ИСПДн), так и привлекаемыми для этой цели компетентными организациями, имеющими лицензию на этот вид деятельности, а также ФСТЭК России и ФСБ России в пределах их компетенции.

10.3. Контроль может осуществляться администратором ИСПДн как с помощью штатных средств системы защиты ПДн, так и с помощью специальных программных средств контроля.

10.4. Оценка эффективности мер защиты ПДн проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

#### **11. Сферы ответственности за безопасность ПДн**

11.1. Ответственным за разработку мер и контроль над обеспечением безопасности персональных данных является Директор. Директор может делегировать часть полномочий по обеспечению безопасности персональных данных.

11.2. Сфера ответственности руководителя учреждения включает следующие направления обеспечения безопасности ПДн:

- планирование и реализация мер по обеспечению безопасности ПДн;
- анализ угроз безопасности ПДн;
- разработка, внедрение, контроль исполнения и поддержание в актуальном состоянии политик, руководств, концепций, процедур, регламентов, инструкций и других организационных документов по обеспечению безопасности;
- контроль защищенности ИТ инфраструктуры МФЦ Тарасовского района от угроз ИБ путем;
- обучение и информирование пользователей ИСПДн, о порядке работы с ПДн и средствами защиты;
- предотвращение, выявление, реагирование и расследование нарушений безопасности ПДн.

11.3. При взаимодействии со сторонними организациями в случаях, когда сотрудникам этих организаций предоставляется доступ к объектам защиты (раздел 6), с этими организациями должно быть заключено «Соглашение о конфиденциальности», либо «Соглашение о соблюдении режима безопасности ПДн при выполнении работ в ИСПДн».

#### **12. Модель нарушителя безопасности**

12.1. Под нарушителем в МАУ МФЦ Тарасовского района понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб объектам защиты (раздел 6).

12.2. Нарушители подразделяются по признаку принадлежности к ИСПДн. Все нарушители делятся на две группы:

- внешние нарушители – физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн;
- внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн.

12.3. Классификация нарушителей представлена в Модели угроз безопасности персональных данных каждой ИСПДн.

#### **13. Модель угроз безопасности**

13.1. Для ИСПДн МАУ МФЦ Тарасовского района выделяются следующие основные категории угроз безопасности персональных данных:

13.1.1. Угрозы от утечки по техническим каналам.

13.1.2. Угрозы несанкционированного доступа к информации:

- угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн;
- угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);
- угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в

ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера;

- угрозы преднамеренных действий внутренних нарушителей;
- угрозы несанкционированного доступа по каналам связи;
- описание угроз, вероятность их реализации, опасность и актуальность представлены в Модели угроз безопасности персональных данных каждой ИСПДн.

#### **14. Механизм реализации Концепции**

14.1. Реализация Концепции должна осуществляться на основе перспективных программ и планов, которые составляются на основании и во исполнение:

- федеральных законов в области обеспечения информационной безопасности и защиты информации;
- постановлений Правительства Российской Федерации;
- руководящих, организационно-распорядительных и методических документов ФСТЭК России;
- потребностей ИСПДн в средствах обеспечения безопасности информации.

#### **15. Ожидаемый эффект от реализации Концепции**

15.1. Реализация Концепции безопасности ПДн в ИСПДн позволит:

- оценить состояние безопасности информации ИСПДн, выявить источники внутренних и внешних угроз информационной безопасности, определить приоритетные направления предотвращения, отражения и нейтрализации этих угроз;
- разработать распорядительные и нормативно-методические документы применительно к ИСПДн;
- провести классификацию и сертификацию ИСПДн;
- провести организационно-режимные и технические мероприятия по обеспечению безопасности ПДн в ИСПДн;
- обеспечить необходимый уровень безопасности объектов защиты.

15.2. Осуществление этих мероприятий обеспечит создание единой, целостной и скоординированной системы информационной безопасности ИСПДн и создаст условия для ее дальнейшего совершенствования.

#### **16. Список использованных источников**

16.1. Основными нормативно-правовыми и методическими документами, на которых базируется настоящее Положение являются:

- Федеральный Закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»), устанавливающий основные принципы и условия обработки ПДн, права, обязанности и ответственность участников отношений, связанных с обработкой ПДн.
- «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденное Постановлением Правительства РФ от 1.11.2012 г. № 1119.
- «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденное Постановлением Правительства РФ от 15.09.2008 г. № 687.
- «Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», утвержденные Постановлением Правительства РФ от 06.07.2008 г. № 512.

16.2. Нормативно-методические документы Федеральной службы по техническому и экспертному контролю Российской Федерации (далее – ФСТЭК России) по обеспечению безопасности ПДн при их обработке в ИСПДн:

- Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.2008 г. (ДСП).
- Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.2008 г. (ДСП).
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.2008 г. (ДСП).
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.2008 г. (ДСП).