Муниципальное образование «Надеждинское сельское поселение»

Биробиджанского муниципального района

Еврейской автономной области

АДМИНИСТРАЦИЯ СЕЛЬСКОГО ПОСЕЛЕНИЯ

ПОСТАНОВЛЕНИЕ

05.06.2019 № 49

с. Надеждинское

Об утверждении организационных документов по защите персональных данных в администрации Муниципального образования «Надеждинское сельское поселение» Биробиджанского муниципального района Еврейской автономной области

В целях исполнения Федерального закона № 152-ФЗ от 27 июля 2006 года «О персональных данных», постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» администрация сельского поселения

ПОСТАНОВЛЯЕТ:

1. Утвердить прилагаемые:

1.1. Правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных в администрации Надеждинского сельского поселения.

1.2. Правила рассмотрения запросов субъектов персональных данных или их представителей в администрации Надеждинского сельского поселения.

1.3. Перечень информационных систем персональных данных в администрации Надеждинского сельского поселения.

1.4. Перечень персональных данных, обрабатываемых в администрации Надеждинского сельского поселения в связи с реализацией трудовых отношений, а также в связи с оказанием муниципальных услуг и осуществлением муниципальных функций.

1.5. Перечень должностей служащих администрации Надеждинского сельского поселения, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным.

1.6. Положение по обработке персональных данных без использования средств автоматизации в администрации Надеждинского сельского поселения.

1.7. Положение об организации и обеспечении защиты персональных данных при их обработке в информационных системах персональных данных администрации Надеждинского сельского поселения.

2. Настоящее постановление довести до ответственных лиц в части их касающейся.

3. Контроль за исполнением настоящего постановления оставляю за собой.

4. Настоящее постановление опубликовать в средствах массовой информации.

5. Настоящее постановление вступает в силу после дня его официального опубликования.

Глава сельского поселения Н.В. Красилова

УТВЕРЖДЕНЫ

постановлением администрации

сельского поселения

от 05.06.2019 г. № 49

**Правила**

**обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных в администрации Муниципального образования «Надеждинское сельское поселение» Биробиджанского муниципального района Еврейской автономной области**

**1. Общие положения.**

Настоящие Правила разработаны в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных, на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПД», приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей гостайну, содержащейся в государственных информационных системах», распорядительными и методическими документами ФСТЭК России, Трудовым кодексом Российской Федерации, Федеральным законом Российской Федерации от 02.03.2007 № 25-ФЗ «О муниципальной службе в Российской Федерации», Федеральным законом от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», Федеральным законом от 21.11.1996 № 129-ФЗ «О бухгалтерском учёте», Федеральным законом от 28.03.1998 № 53-ФЗ «О воинской обязанности и воинской службе», Федеральным законом от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления», Федеральным законом от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращения граждан Российской Федерации», Федеральным законом от 12.06.2002 № 67-ФЗ «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации», Федеральным законом от 21.07.2005 № 94- ФЗ «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд», Федеральным законом от 15.12.2001 № 167-ФЗ «Об обязательном пенсионном страховании в Российской Федерации», Федеральным законом от 16.07.1999 № 165-ФЗ «Об основах обязательного социального страхования», Федеральным законом от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации», Федеральным законом от 07.02.1992 № 2300-1 «О защите прав потребителей».

Данные Правила определяют порядок обработки персональных данных служащих администрации Надеждинского сельского поселения и третьих лиц, чьи персональные данные обрабатываются администрацией Надеждинского сельского поселения (далее администрация сельского поселения).

Правила являются внутренним нормативным документом, регламентирующим деятельность администрации сельского поселения в сфере обработки ПДн. Правила являются обязательными для выполнения всеми служащими, состоящими с администрацией сельского поселения в трудовых отношениях.

Защита персональных данных субъекта персональных данных от неправомерного их использования или утраты обеспечивается администрацией сельского поселения в порядке, установленном законодательством Российской Федерации, за счет своих средств.

**2. Понятие и состав персональных данных служащих администрации сельского поселения.**

Под персональными данными служащих администрации сельского поселения понимается информация, необходимая администрации сельского поселения в связи с возникновением трудовых отношений и касающаяся конкретного служащего администрации сельского поселения.

Субъектами ПДн, обработка персональных данных которых осуществляется администрацией сельского поселения, в соответствии с принципами работы, определенными в настоящих правилах, являются служащие администрации.

Целями получения и обработки ПДн служащих являются учет прохождения муниципальной службы сотрудниками администрации сельского поселения, формирование кадрового резерва для замещения должностей муниципальной службы, ведение трудовых книжек муниципальных служащих, ведение личных дел муниципальных служащих, ведение реестра муниципальных служащих, оформление и выдача служебных удостоверений муниципальных служащих, проведение конкурса на замещение вакантных должностей муниципальной службы и включение муниципальных служащих в кадровый резерв, проведение аттестации муниципальных служащих, проведение квалификационных экзаменов муниципальных служащих администрации в целях присвоения им классных чинов, установление надбавок за выслугу лет на муниципальной службе, присвоение иных надбавок и доплат, проверка достоверности и полноты сведений о доходах, об имуществе и обязательствах имущественного характера, представляемых муниципальными служащими администрации, чьи должности включены в утвержденный перечень должностей, поощрение и награждение муниципальных служащих, применении к ним дисциплинарных взысканий, заключение трудовых договоров с гражданами при приеме их на работу, составление табеля учета рабочего времени, графика ежегодных оплачиваемых отпусков, оформления документов для выезда в служебные командировки, определение стажа муниципальной службы, установления доплат к трудовым пенсиям муниципальным служащим, имеющим на это право, увольняемым из администрации, анализ уровня профессионального образования муниципальных служащих, его соответствия квалификационным требованиям, предъявляемым к замещаемым ими должностям муниципальной службы, в целях проведения работы по планированию направления муниципальных служащих для прохождения дополнительного профессионального образования, подготовка материалов по представлению к награждению государственными наградами Российской Федерации, области, главы муниципального района, главы сельского поселения, ведение учета лиц, награжденных наградами, бухгалтерский и налоговый учет, начисление и перечисления заработной платы.

Доступ к ПДн служащих администрации сельского поселения имеют:

-глава администрации сельского поселения;

-заместитель главы администрации сельского поселения;

-старший специалист первого разряда;

-специалист второго разряда;

-специалист-эксперт главный бухгалтер.

Информационные ресурсы, содержащие ПДн субъектов, создаются путём:

-копирования оригиналов документов, содержащих ПДн (например, паспорт, страховое свидетельство государственного пенсионного страхования);

-внесения сведений в учётные формы на бумажных носителях (личная карточка по форме Т-2ГС);

-внесения сведений в базы данных;

-получения оригиналов необходимых документов (трудовая книжка, автобиография, анкета, заявления).

К персональным данным служащих относятся:

1. Информация, содержащаяся в документах базы данных о служащих (заявлениях, ксерокопиях паспорта, военного билета, документах об образовании, документах о составе семьи; документах о состоянии здоровья; документах, подтверждающих право на дополнительные гарантии и компенсации; личном листке по учету кадров; анкете; резюме; обязательствах; контрольном листе прохождения инструктажа по технике безопасности, сведениях о доходах и др.).

2. Информация, содержащаяся в трудовой книжке служащего.

3. Информация, содержащаяся в служебном контракте и дополнительных соглашениях.

4. Информация, содержащаяся в личной карточке служащего (унифицированная форма Т-2ГС), личной карточке служащего (военнообязанного):

* фамилия, имя, отчество;
* дата рождения;
* место рождения;
* гражданство;
* знание иностранных языков;
* сведения о полученном образовании;
* профессия;
* стаж работы;
* состояние в браке;
* состав семьи;
* паспортные данные;
* адрес места жительства (по паспорту, фактический);
* номер домашнего телефона;
* сведения о воинском учете;
* сведения о приеме на работу и переводах на другую работу;
* сведения об аттестации;
* сведения о повышении квалификации;
* сведения о профессиональной переподготовке;
* сведения о поощрениях и наградах;
* сведения об отпусках;
* сведения о социальных льготах служащего;
* дата увольнения.

5. Информация, содержащаяся в приказах по личному составу, приказах о предоставлении отпусков, приказах о взысканиях, приказах о поощрении и премировании.

6.Информация, содержащаяся в графике отпусков, служебных характеристиках, рекомендациях и т.п.

**3. Обработка персональных данных служащих администрации** **сельского поселения.**

**3.1. Правила получения и обработки персональных данных служащих администрации сельского поселения**

Все персональные данные служащего получаются у него самого. Администрация сельского поселения сообщает служащему о целях получения персональных данных и последствиях отказа служащего дать письменное согласие на их получение.

Администрация сельского поселения не имеет права получать и обрабатывать персональные данные о политических, религиозных и иных убеждениях и частной жизни служащего. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации администрация сельского поселения вправе получать и обрабатывать данные о частной жизни служащего только с его письменного согласия.

Администрация сельского поселения не имеет права получать и обрабатывать персональные данные о членстве служащего в объединениях и/или его профсоюзной деятельности, за исключением случаев, предусмотренных Трудовым Кодексом Российской Федерации или иными федеральными законами.

Администрация сельского поселения не имеет права запрашивать информацию о состоянии здоровья служащего, за исключением тех сведений, которые относятся к вопросу о возможности выполнения служащим служебных обязанностей.

**4. Понятие и состав ПДн третьих лиц**

Под персональными данными третьих лиц понимается информация, необходимая администрации сельского поселения в связи с договорными отношениями, с оказанием муниципальных услуг или выполнением муниципальных функций и касающимися конкретного лица.

Субъектами ПДн, обработка персональных данных которых осуществляется администрацией сельского поселения, в соответствии с принципами работы, определенными в настоящем положении, являются:

- третьи лица – сотрудники МКУ «Централизованное хозяйственное учреждение» муниципального образования «Надеждинское сельское поселение» Биробиджанского муниципального района Еврейской автономной области, Собрание депутатов Надеждинского сельского поселения, руководители муниципальных учреждений, лица, претендующие на замещение должностей муниципальной службы;

-третьи лица – физические лица, юридические лица, индивидуальные предприниматели, отдельные граждане с которыми администрация имеет договорные отношения или чьи персональные данные обрабатываются администрацией сельского поселения в связи с оказанием муниципальных услуг или выполнением муниципальных функций.

Обработка ПДн третьих лиц может осуществляться только с целями, не выходящими за рамки обеспечения деятельности, указанной в настоящих Правилах.

Такими целями могут быть:

-формирование кадрового резерва для замещения должностей муниципальной службы;

-проведение конкурса на замещение вакантных должностей муниципальной службы и включение муниципальных служащих в кадровый резерв;

-проведение проверки достоверности ПДн и иных сведений, представляемых гражданами, претендующими на замещение должностей муниципальной службы, на замещение иных должностей назначение на которые и освобождение от которых, осуществляет глава сельского поселения;

-проведение проверки достоверности и полноты сведений о доходах, об имуществе и обязательствах имущественного характера, представляемых лицами, претендующими на замещение должностей муниципальной службы, а также сведений о доходах, об имуществе и обязательствах имущественного характера членов их семей;

-проведение проверки достоверности и полноты сведений о доходах, об имуществе и обязательствах имущественного характера, представляемых лицами, поступающими на работу, на должность руководителя муниципального учреждения сельского поселения, а также сведений о доходах, об имуществе и обязательства имущественного характера членов их семей;

-подготовка и уточнение общих и запасных списков кандидатов в присяжные заседатели по Биробиджанскому району для суда Еврейской автономной области и Дальневосточного военного суда;

-осуществление учета участников референдума, проживающих на территории муниципального образования «Надеждинское сельское поселение» Биробиджанского муниципального района Еврейской автономной области;

-приём граждан по жилищным вопросам;

-проведение спортивных мероприятий;

-организация награждения победителей и призеров, официальных физкультурно-спортивных мероприятий, физических лиц за высокие спортивные достижения на территории сельского поселения;

- заключение договоров на оказание услуг по спортивным, культурно-массовым мероприятиям;

-исполнение государственных полномочий по применению законодательства об административных правонарушениях;

-подготовка статистического отчета;

-рассмотрение жалоб и заявлений граждан сельского поселения,

-сбор и обработка данных об избирателях для последующей передачи их в территориальную избирательную комиссию муниципального района;

-подготовка и выдача разрешений на строительство, реконструкцию объектов капитального строительства;

-выдача документа, подтверждающего проведение основных работ по строительству (реконструкции) объекта индивидуального жилищного строительства, осуществляемому с привлечением средств материнского (семейного) капитала;

-подготовка, утверждение и выдача градостроительных планов земельных участков;

-подготовка и выдача разрешений на ввод объектов в эксплуатацию при осуществлении строительства, реконструкции объектов капитального строительства;

-кадровое делопроизводство на руководителей муниципальных учреждений;

-участия в расследованиях тяжелых, смертельных и групповых, с тяжелыми последствиями, несчастных случаев на производстве в администрации сельского поселения, муниципальных учреждениях;

-ведение банка данных по муниципальным учреждениям (о прохождении обучения по охране труда, о проведении специальной оценки условий труда в учреждениях);

-защита прав потребителей;

-заключение контрактов для муниципальных нужд;

-проверка соответствия требованиям, установленным в соответствии с законодательством РФ к лицам, осуществляющим поставку товара, выполнение работы, оказание услуги, являющихся объектом закупки;

-проверка правомочности участника закупки заключать контракт;

-проверка непроведения ликвидации участника закупки – юридического лица и отсутствия решения арбитражного суда о признании участника закупки – юридического лица или индивидуального предпринимателя несостоятельным (банкротом) и об открытии конкурсного производства;

-проверка неприостановления деятельности участника закупки в порядке, установленном Кодексом РФ об административных правонарушениях, на дату подачи заявки на участие в закупке;

-проверка отсутствия у участника закупки недоимки по налогам, сборам, задолженности по иным обязательным платежам в бюджеты бюджетной системы РФ;

-проверка отсутствия в реестре недобросовестных поставщиков (подрядчиков, исполнителей) информации об участнике закупки – юридическом лице, в том числе информации об учредителях, о членах коллегиального исполнительного органа, лице, исполняющем функции единоличного исполнительного органа участника закупки;

-проверка отсутствия у участника закупки – физического лица либо у руководителя, членов коллегиального исполнительного органа или главного бухгалтера юридического лица – участника закупки судимости за преступления в сфере экономики;

-проверка обладания участников закупки исключительными правами на результаты интеллектуальной деятельности;

-включение в реестр недобросовестных поставщиков (подрядчиков, исполнителей) информации об участниках закупок, уклонившихся от заключения контрактов, с которыми контракт был, расторгнут по решению суда или в связи с односторонним отказом Заказчика от исполнения контракта.

Доступ к ПДн третьих лиц, обрабатываемых в администрации муниципального района имеют:

-глава администрации сельского поселения;

-заместитель главы администрации сельского поселения;

-старший специалист первого разряда;

-специалист второго разряда;

-специалист-эксперт главный бухгалтер.

К персональным данным третьих лиц относятся:

1. Информация, содержащаяся в договоре и дополнительных соглашениях;

2. Информация, необходимая администрации сельского поселения для выполнения требований законодательства Российской Федерации и Еврейской автономной области: дата, месяц, год рождения; фамилия, имя, отчество; место рождения; адрес проживания; должность; сведения о составе семьи; сведения о рождении детей; сведения о заключении брака; сведения о признании за гражданином права пользования жилым помещением; сведения о праве пользования жилым помещением; сведения о доходах всех членов семьи за год; сведения из документа, удостоверяющего личность гражданина, подающего заявление о принятии на учёт, и из документов, удостоверяющих личность членов его семьи; сведения о наличии родственных отношений либо иных обстоятельств, свидетельствующих о принадлежности гражданина к семье заявителя; сведения о зарегистрированных по месту жительства гражданах; сведения из налоговых деклараций о доходах за расчетный период, заверенные налоговыми органами; сведения о размере пенсии; сведения о социальных выплатах, сведения о дееспособности/недееспособности; дата окончания срока отбывания наказания; о смерти, о судимости**.**

**5. Обработка персональных данных третьих лиц**

**5.1. Правила получения и обработки персональных данных третьих лиц**

Администрация сельского поселения получает персональные данные в рамках выполнения требований законодательства Российской Федерации и Еврейской автономной области с письменного согласия субъекта ПДн на обработку его персональных данных.

Администрация сельского поселения не имеет права получать и обрабатывать персональные данные о политических, религиозных и иных убеждениях и частной жизни третьих лиц. Администрация сельского поселения не имеет права получать и обрабатывать персональные данные о членстве третьих лиц в общественных объединениях и/или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

**6. Согласие субъекта ПДн на обработку его персональных данных**

Обработка персональных данных осуществляется только с письменного согласия субъекта ПД.

Письменное согласие на обработку своих персональных данных должно включать в себя:

-фамилию, имя, отчество, адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

-наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта ПДн;

-цель обработки персональных данных;

-перечень персональных данных, на обработку которых дается согласие субъекта ПДн;

-перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

-срок, в течение которого действует согласие, а также порядок его отзыва;

-подпись субъекта ПДн.

Согласие на обработку персональных данных может быть в любой момент отозвано.

**7. Организация работы с персональными данными в администрации сельского поселения**

Администрация сельского поселения обязана обеспечивать безопасность персональных данных при их обработке, осуществлять защиту персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

Создание, изменение и чтение персональных данных обрабатываемых в администрации сельского поселения доступно только служащим, определенным настоящими Правилами.

Документы, содержащие персональные данные в администрации сельского поселения создаются:

-в виде записей баз данных, ведущихся с использованием технических и программных средств автоматизированных систем, входящих в ИСПДн;

-в виде отдельных файлов (doc, xls и т.п.), создаваемых ответственными лицами;

-на бумажных носителях.

Доступ к техническим и программным средствам автоматизированных систем, входящих в ИСПДн предоставляется на основании распоряжения главы сельского поселения .

Создание и хранение документов с персональными данными в виде отдельных файлов (doc, xls и т.п.) допускается только на зарегистрированных отчуждаемых носителях ответственных лиц, с реализацией механизма разграничения доступа к ним.

**8. Организация хранения документов, содержащих персональные данные в администрации сельского поселения**

Бумажные документы, содержащие персональные данные, обязаны храниться в местах хранения, запирающихся на ключ, сейфах, металлических шкафах и т.п.

При работе с документами, содержащими персональные данные, запрещается:

-хранить документы в ящиках стола, оставлять без присмотра;

-брать документы для работы и на хранение домой;

-выносить документы из помещений администрации сельского поселения без разрешения главы администрации сельского поселения;

-держать документы вне сейфа без необходимости в процессе работы;

-передавать документы на хранение лицам, не имеющим права доступа к данным документам.

Текущее хранение кадровых документов, содержащих персональные данные, организует ответственный специалист администрации, назначаемый главой администрации сельского поселения.

Текущее хранение бухгалтерских документов, содержащих персональные данные, организует специалист-эксперт главный бухгалтер администрации сельского поселения.

Все остальные документы, содержащие персональные данные должны храниться в администрации сельского поселения с соблюдением номенклатурных сроков хранения.

Подготовка документов к последующему хранению включает экспертизу практической ценности документов, оформление и описание дел, составление актов о выделении к уничтожению документов и передачу их в архив.

Экспертизу документов проводит постоянная экспертная комиссия. Передача дел в архив осуществляется по графику, утвержденному главой сельского поселения не реже, чем один раз в три года.

**9. Уничтожение документов, содержащих персональные данные в администрации сельского поселения**

Документы, содержащие персональные данные временного хранения, как правило, в архив не передаются, а по истечении срока хранения уничтожаются.

К документам, содержащим ПДн, временного характера относятся документы, которые не должны храниться в архиве в обязательном порядке.

Для решения вопроса об уничтожении такого рода документов один раз в год собирается экспертная комиссия, определяемая распоряжением главы сельского поселения.

Итоги работы комиссии оформляются актами об уничтожении документов, содержащих персональные данные.

Уничтожение документов, содержащих персональные данные, производится любым способом, исключающим ознакомление посторонних лиц с уничтожаемыми материалами и возможность восстановления их текста. Акты составляются и подшиваются в дело.

**10. Распространение персональных данных администрацией сельского поселения**

**10.1. Доступ служащего к своим персональным данным**

По запросу служащего (приложение 1) администрация сельского поселения не позднее 3-х дней со дня получения такого запроса должна выдать служащему копии документов на бумажном носителе, связанные с работой (копии приказа о приеме на работу, приказов о переводах на другую работу, приказа об увольнении с работы, выписки из трудовой книжки, периода работы у данного работодателя и др.).

Предоставление ПДн служащих администрации сельского поселения фиксируются в журнале учета выдачи/передачи ПДн служащих администрации Надеждинского сельского поселения.

Копии документов, связанных с трудовой деятельностью в администрации сельского поселения, заверяются надлежащим образом и предоставляются служащему администрации сельского поселения безвозмездно.

**10.2. Доступ третьих лиц к своим персональным данным**

В случае получения от третьих лиц запроса установленной формы на предоставление его персональных данных администрация сельского поселения обязана предоставить такие персональные данные в сроки установленные «Правилами рассмотрения запросов субъектов персональных данных или их представителей в администрации Надеждинского сельского поселения».

**10.3. Передача персональных данных третьим лицам**

Передача персональных данных контрольно-надзорным органам и в государственные ИСПДн осуществляется в соответствии с действующим законодательством Российской Федерации.

Доступ к персональным данным на основании и во исполнение федеральных законов предоставляется:

-Федеральной инспекции труда и федеральным органам исполнительной власти, осуществляющим функции по контролю и надзору в установленной сфере деятельности;

-Федеральной налоговой службе и межрегиональным инспекциям и управлениям ФНС РФ по субъектам Российской Федерации;

-Федеральной службе государственной статистики и её территориальным органам;

-Федеральному фонду обязательного медицинского страхования и его территориальным органам;

-Военным комиссариатам;

-Фонду социального страхования РФ;

-Пенсионному фонду РФ.

Передача персональных данных страховым компаниям, банкам, благотворительным организациям, негосударственным пенсионным фондам, посольствам, другим организациям; родственникам, членам семьи и другим лицам осуществляется по письменному запросу о предоставлении персональных данных на имя главы сельского поселения с указанием цели предоставления и характера персональных данных. **Передача персональных данных осуществляется только при условии получения письменного согласия служащего, данные которого запрашиваются (отметка о согласии должна быть проставлена служащим на запросе), либо по письменному заявлению самого служащего.**

Обо всех запросах о предоставлении персональных данных должен быть уведомлен ответственный за организацию обработки персональных данных.

При передаче персональных данных третьих лиц должны соблюдаться следующие требования:

-передача персональных данных третьей стороне осуществляется на основании действующего законодательства Российской Федерации;

-существенным условием договора является обеспечение третьей стороной конфиденциальности персональных данных и безопасности персональных данных при их обработке (в договоре, если таковой имеется должны быть прописаны обязанности сторон по защите полученных ПДн);

- наличие письменного согласия субъекта ПДн.

Порядок действий с запросами от субъекта персональных данных или его законного представителя на подтверждение наличия, ознакомление, уточнение, уничтожение или отзыв согласия на обработку персональных данных дополнительно определен в Правилах рассмотрения запросов субъектов персональных данных или их представителей в администрации сельского поселения.

**11. Права субъектов ПДн в отношении своих персональных данных**

Субъекты ПДн в отношении своих персональных данных имеют право на:

-полную информацию о своих персональных данных и обработке этих данных;

-свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, за исключением случаев, предусмотренных федеральным законом;

-определение своих представителей для защиты своих персональных данных;

-требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований законодательства;

-требование об извещении администрацией сельского поселения всех лиц, которым ранее были извещены неверные или неполные персональные данные служащего, обо всех произведенных в них исключениях, исправлениях или дополнениях;

-обжалование в суде любых неправомерных действий или бездействия администрации сельского поселенияпри обработке или защите его персональных данных.

**11. Обязанности администрации сельского поселения при обработке ПДн**

При обработке ПДн администрация сельского поселения обязана:

-обеспечить защиту персональных данных от их неправомерного использования или утраты в порядке, установленном законодательством Российской Федерации и требованиями регулирующих органов;

-ознакомить субъекта ПДн или его законных представителей с его правами в области защиты персональных данных на веб-сайте www.br.eao.ru;

-осуществлять передачу ПДн третьих лиц только в соответствии с настоящими Правилами и законодательством Российской Федерации;

-обеспечить субъекту ПДн доступ к своим персональным данным.

Доступ в помещения, где осуществляется обработка персональных данных, ограничивается системой физической безопасности и организационно-распорядительными мерами.

Доступ к ИСПДн администрации сельского поселения осуществляется в соответствии с порядком, определенным в Положении об организации и обеспечении защиты персональных данных при их обработке в информационных системах персональных данных администрации сельского поселения.

Ответственным за предоставление доступа к ИСПДн администрации сельского поселения является назначенный главой администрации специалист.

Право внутреннего доступа к персональным данным имеют только те служащие администрации сельского поселения, которым это необходимо для выполнения своих должностных обязанностей в рамках служебного контракта с администрацией сельского поселения. Доступ к ИСПДн осуществляется на основании разрешительной системы доступа служащих администрации сельского поселения к ИСПДн. Ответственным за поддержание «Разрешительной системы допуска служащих администрации сельского поселения к ИСПДн» в актуальном состоянии является администратор ИСПДн.

Служащими администрации сельского поселения, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных.

Факт доступа служащих администрации сельского поселения к персональным данным, а также факты предоставления персональных данных по этим запросам регистрируются автоматизированными средствами ИСПДн.

При обнаружении нарушений порядка предоставления персональных данных субъекта ПДн служащий администрации сельского поселения незамедлительно приостанавливает предоставление персональных данных до выявления причин нарушений и устранения этих причин.

**12.** **Ответственность**

Пункты настоящих Правил обязательны для исполнения служащими администрации сельского поселения, в обязанности которых входит обработка и защита персональных данных.

Ознакомление служащих администрации сельского поселения с настоящими Правилами организует глава администрации сельского поселения.

Принципы работы с персональными данными в администрации сельского поселения:

-постоянный контроль за состоянием работы с персональными данными служащих администрации сельского поселения;

-персональная ответственность (служащие администрации сельского поселения, в обязанности которых входит обработка и защита персональных данных, несут личную ответственность за нарушение правил работы, определяемых настоящими Правилами).

Все служащие администрации сельского поселения, должностные обязанности которых подразумевают возможность ознакомления с ПДн, при приеме на работу обязаны подписывать Обязательство служащего администрации о неразглашении персональных данных, ставших ему известными в связи с исполнением должностных обязанностей (приложение 2).

Обязанность по исполнению требований по нераспространению сведений, содержащих персональные данные, сохраняется за бывшими служащими администрации сельского поселения в течение всего срока действия конфиденциальности сведений.

Ответственным за информационную безопасность является глава администрации сельского поселения, который также является гарантом соблюдения законодательства Российской Федерации о персональных данных.

На главу администрации возлагается:

-ведение, обеспечение нормального функционирования и контроль за работой средств защиты информации в составе системы защиты информационных систем персональных данных;

-выборочный периодический контроль за соблюдением порядка обмена электронными копиями файлов, содержащими персональные данные;

-учет фактов утраты документов и разглашения сведений, содержащих персональные данные, анализ причин и разработка мер по предупреждению таких инцидентов;

-обеспечение учета сейфов, металлических шкафов, специальных хранилищ и помещений (а также ключей к ним), в которых осуществляется хранение и работа с документами, содержащими персональные данные.

На муниципальных служащих администрации сельского поселения возлагается:

-персональная ответственность за организацию работы с информацией, содержащей персональные данные;

-принятие мер по предотвращению разглашения и утечки сведений, содержащих персональные данные;

-контроль за выполнением правил обращения с документами, содержащими персональные данные.

-контроль за соблюдением установленного порядка копирования документов, содержащих персональные данные; их учетом, хранением и использованием;

-контроль за соблюдением правил рассылки документов, содержащих персональные данные.

Служащие администрации сельского поселения, в обязанности которых входит обработка и защита персональных данных, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, могут быть привлечены к ответственности в соответствии с действующим законодательством Российской Федерации и административно-правовыми нормами, установленными в администрации сельского поселения.

**13. Взаимодействие с уполномоченными органами в области защиты персональных данных**

В соответствии с законодательством Российской Федерации в области обеспечения безопасности персональных данных функции контроля и надзора за соответствием порядка обработки персональных данных требованиям действующего законодательства возлагаются на федеральные органы исполнительной власти, уполномоченные в области обеспечения безопасности, противодействия техническим разведкам и технической защиты информации, контроля и надзора в сфере информационных технологий и связи.

Взаимодействие с уполномоченными органами организуется в пределах их полномочий:

1. С территориальными органами Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) по вопросам:

- предоставления информации, необходимой для реализации полномочий;

-осуществления проверочных и контрольных мероприятий в пределах предоставленных полномочий;

-выполнения требований об уточнении, блокировании или уничтожении недостоверных или полученных незаконным путем персональных данных;

-принятия в установленном законодательством Российской Федерации порядке мер по приостановлению или прекращению обработки персональных данных.

2. С территориальными органами ФСТЭК России по вопросам:

-предоставления информации, необходимой для реализации полномочий и осуществления проверочных и контрольных мероприятий;

-организации и проведения мероприятий, направленных на обеспечение безопасности персональных данных при их обработке в ИСПДн.

3. С территориальными органами ФСБ России по вопросам:

-предоставления информации, необходимой для реализации полномочий и осуществления проверочных и контрольных мероприятий;

-организации и обеспечения функционирования шифровальных (криптографических) средств, предназначенных для обеспечения безопасности персональных данных при их обработке в ИСПДн.

Организация взаимодействия с уполномоченными органами в области обеспечения безопасности персональных данных возлагается на главу администрации сельского поселения.

**14. Заключительные положения**

Настоящие Правила доводятся до всех служащих администрации сельского поселения под роспись при приеме на работу.

Приложение № 1

Главе администрации Надеждинского сельского поселения

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Имя, Отчество, Фамилия)

**ЗАПРОС**

Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(фамилия, имя, отчество полностью)

документ, удостоверяющий личность \_\_\_\_\_\_\_\_\_\_\_\_\_\_ серия \_\_\_\_\_\_\_\_\_\_\_ № \_\_\_\_\_\_\_\_\_\_\_\_\_ выдан\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(наименование органа, выдавшего документ и дата его выдачи)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

состою в трудовых отношениях с администрацией Надеждинского сельского поселения (трудовой договор № \_\_\_\_\_\_ от \_\_\_\_\_\_\_\_\_\_\_) и прошу вас предоставить мне следующую информацию:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

С целью: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(дата) (подпись)

Приложение № 2

Типовое обязательство служащего администрации сельского поселения, непосредственно осуществляющего обработку персональных данных, о неразглашении ставших известными ему в связи с исполнением должностных обязанностей в случае расторжения с ним трудового договора

Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(фамилия, имя, отчество)

оформляясь на должность \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

в \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(наименование организации)

будучи поставлен (а) в известность о том, что по роду своей деятельности и обязанностям буду допущен (а) к обработке персональных данных.

В соответствии с Законом Российской Федерации «О персональных данных» и иными нормативными правовыми актами о персональных данных, с которыми меня ознакомили, принимаю на себя обязательство по неразглашению доверенных мне сведений содержащих персональные данные сотрудников администрации и иных субъектов.

Принимаю на себя обязательства:

соблюдать требования законодательства Российской Федерации о персональных данных;

в случае попытки посторонних лиц получить информацию конфиденциального характера немедленно сообщить об этом главе администрации сельского поселения.

Я предупрежден (а) о том, что случае даже однократного нарушения принятых на себя обязательств буду отстранен (а) от работы со сведениями, содержащими персональные данные, а трудовой договор со мной может быть расторгнут.

Мне известно, что в случае отстранения от работы с персональными данными я не освобождаюсь от взятых обязательств по неразглашению сведений, содержащих персональные данные.

Обязуюсь добросовестно выполнять свои обязательства, строго охранять доверенные мне сведения, содержащие персональные данные.

Я предупрежден (а), что за разглашение сведений содержащих персональные данные, или утрату носителей сведений, содержащих персональные данные, а также за нарушение режима конфиденциальности буду привлечен (а) к ответственности в соответствии с законодательством Российской Федерации.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

«\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г.

УТВЕРЖДЕНЫ

постановлением

администрации

сельского поселения

от 05.06.2019 г. № 49

**ПРАВИЛА  
рассмотрения запросов субъектов персональных данных или их представителей в администрации Муниципального образования «Надеждинское сельское поселение» Биробиджанского муниципального района Еврейской автономной области**

**1. Область применения**

Настоящие Правила разработаны в соответствии с Конституцией РФ, Гражданским кодексом РФ, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и иными нормативными правовыми актами Российской Федерации в области защиты персональных данных, а также организационно-распорядительными документами администрации Надеждинского сельского поселения (далее администрация сельского поселения).

Настоящие Правила регулирует отношения, возникающие при выполнении администрацией обязательств согласно требованиям статей 14, 20 и 21 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Положения настоящих Правил распространяются на действия администрации сельского поселения при обращении либо при получении запроса субъекта персональных данных или его представителя. Эти действия направлены на подтверждение наличия, ознакомление, уточнение, уничтожение или отзыв согласия на обработку персональных данных, а также на устранение нарушений законодательства, допущенных при обработке персональных данных.

**2. Ответственность**

Ответственность за корректировку, проверку и пересмотр настоящих Правил несет глава администрации сельского поселения.

Организация и проведение работ по ответам на запросы, устранению нарушений, а также уточнению, блокированию и уничтожению персональных данных возлагается на сотрудника, осуществляющего обработку ПДн. Ответственность за правильное применение настоящих Правил несут муниципальные служащие администрации сельского поселения.

**3. Действия в ответ на запросы по ПДн**

**3.1. Запрос субъекта ПДн или его представителя**

В случае поступления Запроса субъекта ПДн или его представителя по персональным данным необходимо выполнить следующие действия:

При получении запроса на наличие ПДн необходимо в течение 30 рабочих дней (согласно пункту 1 статьи 20 152-ФЗ) подтвердить обработку ПДн в случае ее осуществления. Если обработка ПДн субъекта не ведется, то в течение 30 рабочих дней (согласно пункту 2 статьи 20 152-ФЗ) необходимо отправить уведомление об отказе подтверждения обработки ПДн.

При получении запроса на ознакомление с ПДн необходимо в течение 30 рабочих дней (согласно пункту 1 статьи 20 152-ФЗ) предоставить для ознакомления ПДн в случае осуществления обработки этих ПДн. Если обработка ПДн субъекта не ведется, то в течение 30 рабочих дней (согласно пункту 2 статьи 20 152-ФЗ) необходимо отправить уведомление об отказе предоставления информации по ПДн.

Субъект ПДн или его представитель имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

1. подтверждение обработки ПДн, а также цель такой обработки;
2. способы обработки ПДн;
3. сведения о лицах, которые имеют доступ к ПДн;
4. перечень обрабатываемых ПДн и источник их получения;
5. сроки обработки ПДн, в том числе сроки их хранения;
6. юридические последствия для субъекта ПДн обработки его ПДн.

При получении запроса на уточнение ПДн в срок не превышающий 7 рабочих дней необходимо внести в них необходимые изменения, по предоставлению субъектом ПДн или его представителем сведений, подтверждающих, что ПДн, которые относятся к соответствующему субъекту и обработку которых осуществляет администрация сельского поселения, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки (согласно пункту 3 статьи 20 152-ФЗ) и отправить уведомление о внесенных изменениях. Если обработка ПДн субъекта не ведется или нет сведений, подтверждающих, что ПДн, которые относятся к соответствующему субъекту и обработку которых осуществляет администрация сельского поселения, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, то необходимо отправить уведомление об отказе осуществления изменения ПДн.

При получении запроса на уничтожение ПДн в срок, не превышающий 7 рабочих дней необходимо их уничтожить, по предоставлению субъектом ПДн или его представителем сведений, подтверждающих, что ПДн, которые относятся к соответствующему субъекту и обработку которых осуществляет администрация сельского поселения, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки (согласно пункту 3 статьи 20 152-ФЗ) и отправить уведомление об уничтожении. Если обработка ПДн субъекта не ведется или не были предоставлены сведения, подтверждающие, что ПДн, которые относятся к соответствующему субъекту и обработку которых осуществляет администрация сельского поселения, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также в силу необходимости обработки ПДн по требованиям иных законодательных актов, то необходимо отправить уведомление об отказе уничтожения ПДн.

При получении запроса на отзыв согласия на обработку ПДн в срок не превышающий 30 рабочих дней необходимо их уничтожить (согласно пункту 5 статьи 21 152-ФЗ) и отправить уведомление об уничтожении. Если обработка ПДн субъекта не ведется или не были предоставлены сведения, подтверждающие, что ПДн, которые относятся к соответствующему субъекту и обработку которых осуществляет администрация сельского поселения, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также в силу необходимости обработки ПДн по требованиям иных законодательных актов, то необходимо отправить уведомление об отказе уничтожения.

При выявлении недостоверности ПДн при обращении или по запросу субъекта ПДн или его представителя необходимо их блокировать с момента такого обращения или получения такого запроса на период проверки (согласно пункту 1 статьи 21 152-ФЗ). Если факт недостоверности ПДн подтвержден на основании документов, предоставленных субъектом ПДн или его законным представителем, необходимо уточнить ПДн и снять их блокирование. Если факт недостоверности ПДн не подтвержден, то необходимо отправить уведомление об отказе изменения ПДн.

При выявлении неправомерных действий с ПДн администрации сельского поселения при обращении или по запросу субъекта ПДн или его законного представителя необходимо их блокировать с момента такого обращения или получения такого запроса на период проверки (согласно пункту 1 статьи 21 152-ФЗ). Если факт неправомерности действий с ПДн подтвержден на основании документов, предоставленных субъектом ПДн или его законным представителем, необходимо в течение 3 рабочих дней (согласно пункту 3 статьи 21 152-ФЗ) устранить допущенные нарушения. Если невозможно устранить допущенные нарушения администрация сельского поселения в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с ПДн, необходимо уничтожить ПДн и отправить уведомление об уничтожении ПДн.

При достижении целей обработки ПДн администрация сельского поселения обязана незамедлительно прекратить обработку ПДн, уничтожить соответствующие ПДн в течение 30 рабочих дней с даты достижения цели обработки ПДн (согласно пункту 4 статьи 21 152-ФЗ), если иное не предусмотрено федеральными законами, и отправить уведомление об уничтожении ПДн.

**3.1. Запрос уполномоченного органа по защите прав Субъекта ПДн**

В случае поступления Запроса Уполномоченного органа по защите прав субъекта ПДн по персональным данным необходимо выполнить следующие действия:

При получении запроса необходимо в течение 30 дней (согласно пункту 4 статьи 20 152-ФЗ) предоставить информацию, необходимую для осуществления деятельности указанного органа.

При выявлении недостоверных ПДн при обращении или по запросу Уполномоченного органа по защите прав субъекта ПДн необходимо их блокировать с момента такого обращения или получения такого запроса на период проверки (согласно пункту 1 статьи 21 152-ФЗ). Если факт недостоверности ПДн подтвержден на основании документов, предоставленных субъектом ПДн или его представителем, необходимо уточнить ПДн и снять их блокирование. Если факт недостоверности ПДн не подтвержден, то необходимо отправить уведомление об отказе изменения.

При выявлении неправомерных действий с ПДн администрации сельского поселения при обращении или по запросу Уполномоченного органа по защите прав субъекта ПДн необходимо их блокировать с момента такого обращения или получения такого запроса на период проверки (согласно пункту 1 статьи 21 152-ФЗ). Если факт неправомерности действий с ПДн подтвержден на основании документов, предоставленных субъектом ПДн или его законным представителем, необходимо в течение 3 рабочих дней (согласно пункту 3 статьи 21 152-ФЗ) устранить допущенные нарушения. Если невозможно устранить допущенные нарушения администрация сельского поселения в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с ПДн, необходимо уничтожить ПДн и отправить уведомление об уничтожении ПДн.

При достижении целей обработки ПДн администрация сельского поселения обязана незамедлительно прекратить обработку ПДн, уничтожить соответствующие ПДн в течение 30 дней с даты достижения цели обработки ПДн (согласно пункту 4 статьи 21 152-ФЗ), если иное не предусмотрено нормативными правовыми документами Российской Федерации, и отправить уведомление об уничтожении ПДн.

**4. Прием запросов от субъекта ПДн или его представителей, а также от уполномоченного органа по защите прав субъектов ПДн**

При получении запросов, перечисленных в разделе 4 настоящих Правил служащие выполняют следующие действия:

В случае поступления запроса субъекта ПДн или его представителя необходимо зарегистрировать запрос в «Журнале учета входящей корреспонденции».

При личном обращении субъекта персональных данных в администрацию сельского поселения, администрация сельского поселения принимает запрос в произвольной форме. После принятия запроса служащий администрации сельского поселения сверяет сведения в запросе с предоставленными ему документами.

Необходимые сведения о субъекте ПДн, которые должны присутствовать в подаваемом запросе:

- Фамилия, имя и отчество субъекта ПДн;

- номер основного документа, удостоверяющего личность субъекта ПДн или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе, собственноручная подпись субъекта персональных данных или его законного представителя;

- состоит ли субъект ПДн в договорных отношения с администрацией сельского поселения;

- сведения о заключенных договорах между администрацией сельского поселения и субъектом ПДн.

- иные сведения о взаимоотношениях субъекта ПДн с администрацией сельского поселения.

В случае неправильной формы запроса или отсутствии документов, удостоверяющих личность субъекта ПДн или его представителя, служащий может отказать в приеме запроса и потребовать переделать запрос. При отказе субъекта ПДн или его представителя переделать запрос, служащий администрации сельского поселения района делает об этом запись в Журнале учета входящей корреспонденции».

Если запрос оформлен в соответствии с требованиями законодательства, он принимается к обработке и передается уполномоченному лицу в соответствии с разделом 3 настоящих Правил.

В случае поступления запроса уполномоченного органа по защите прав субъектов персональных данных необходимо зарегистрировать запрос в Журнале учета входящей корреспонденции».

Запрос принимается к обработке и передается уполномоченному лицу, в соответствии с разделом 3 настоящих Правил.

Приложение № 1

**Сводная таблица действий в ответ на запросы по ПДн**

| № | Запрос | Действия | Срок | Ответ |
| --- | --- | --- | --- | --- |
| 1.Запрос Субъекта ПДн или его Представителя | | | | |
| 1.1. | Наличие ПДн | Подтверждение обработки ПДн | 30 дней (пункт 1 статьи 20)\* | Подтверждение обработки ПДн |
| Отказ подтверждения обработки ПДн | 30 дней (пункт 2 статьи 20) | Уведомление об отказе подтверждения обработки ПДн |
| 1.2. | Ознакомление с ПДн | Предоставление информации по ПДн | 7 дней (пункт 3 статьи 20) | 1.Подтверждение обработки ПДн, а также цель такой обработки |
| 2.Способы обработки ПДн |
| 3.Сведения о лицах, которые имеют доступ к ПДн |
| 4.Перечень обрабатываемых ПДн и источник их получения |
| 5.Сроки обработки ПДн, в том числе сроки их хранения |
| 6.Юридические последствия для субъекта ПДн обработки его ПДн |
| Отказ предоставления информации по ПДн | 7 дней (пункт 3 статьи 20) | Уведомление об отказе предоставления информации по ПДн |
| 1.3. | Уточнение ПДн | Блокировка ПДн | Период проверки достоверности ПДн | Уведомление о внесенных изменениях |
| Изменение ПДн |
| Снятие блокировки ПДн |
| Отказ изменения ПДн | По предоставлению сведений по ПДн, подтверждающих неполноту, устаревание, недостоверность, незаконность получения или отсутствие необходимости для заявленных целей обработки | Уведомление об отказе предоставления изменения ПДн |
| 1.4. | Уничтожение ПДн | Блокировка ПДн | Период проверки достоверности ПДн | Уведомление об уничтожении |
| Уничтожение ПДн |
| Уведомление об отказе уничтожения ПДн |
| Отказ уничтожения ПДн |
| 1.5. | Отзыв согласия на обработку ПДн | Блокировка ПДн | 30 дней (пункт 5 статьи 21) | Уведомление о прекращении обработки и уничтожении ПДн |
| Уничтожение ПДн |
| Отказ прекращения обработки и уничтожения ПДн | 30 дней (пункт 5 статьи 21) | Уведомление об отказе прекращения обработки и уничтожения ПДн |
| 1.6. | Недостоверность ПДн Субъекта | Блокировка ПДн | Период проверки достоверности ПДн | Уведомление о внесенных изменениях |
| Изменение ПДн |
| Снятие блокировки ПДн |
| Отказ изменения ПДн | Период проверки достоверности ПДн | Уведомление об отказе изменения ПДн |
| 1.7. | Неправомерность действий с ПДн Субъекта | Устранение нарушений | 3 рабочих дня (пункт 3 статьи 21) | Уведомление об устранении нарушений |
| Уничтожение ПДн | 3 рабочих дня (пункт 3 статьи 21) | Уведомление об уничтожении ПДн |
| 1.8. | Достижение целей обработки ПДн Субъекта | Блокировка ПДн | 30 дней (пункт 4 статьи 21) | Уведомление об уничтожении ПДн |
| Уничтожение ПДн |
| 2. Запрос уполномоченного органа по защите прав Субъекта ПДн | | | | |
| 2.1. | Информация для осуществления деятельности уполномоченного органа | Предоставление затребованной информации по ПДн | 30 дней (пункт 4 статьи 20) | Предоставление затребованной информации по ПДн |
| 2.2. | Недостоверность ПДн Субъекта | Блокировка ПДн | Период проверки достоверности ПДн | Уведомление о внесенных изменениях |
| Изменение ПДн |
| Снятие блокировки ПДн |
| Отказ изменения ПДн | Период проверки достоверности ПДн | Уведомление об отказе изменения ПДн |
| 2.3. | Неправомерность действий с ПДн Субъекта | Устранение нарушений | 3 рабочих дня (пункт 3 статьи 21) | Уведомление об устранении нарушений |
| Уничтожение ПДн | 3 рабочих дня (пункт 3 статьи 21) | Уведомление об уничтожении ПДн |
| 2.4. | Достижение целей обработки ПДн Субъекта | Блокировка ПДн | 3 рабочих дня (пункт 4 статьи 21) | Уведомление об уничтожении ПДн |
| Уничтожение ПДн |

* ссылки на пункты и номера статей приведены для Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»

Приложение 2

к постановлению администрации

сельского поселения

от 05.06.2019 г. № 49

**Перечень**

**информационных систем персональных данных в администрации Надеждинского сельского поселения**

| №  п/п | Наименование ИС | Перечень ИСПДн,  входящих в состав ИС | Масштаб/количество АРМ в ИС | Адрес объекта |
| --- | --- | --- | --- | --- |
| 1 | «Бухгалтерия» | «Смета», «ДОК ПУ 5», «Налогоплательщик ЮЛ». | объектовый/4  АРМ № 1; № 2; № 3; № 4 | с. Надеждинское, ул. Центральная, д.35, кв.1 |
| 2 | «Кадры» | «Кадры» | объектовый/1  АРМ № 12 | с. Надеждинское, ул. Центральная, д.35, кв.1 |
| 3 | «Обращения граждан» | «Обращения граждан» | объектовый/2  АРМ № 13; № 14 | . Надеждинское, ул. Центральная, д.35, кв.1 |

Приложение 3

к постановлению администрации

сельского поселения

от 05.06.2019 г. № 49

**Перечень**

**персональных данных, обрабатываемых в администрации Надеждинского сельского поселения, в связи с реализацией трудовых отношений, а также в связи с оказанием муниципальных услуг и осуществлением муниципальных функций**

| №  п/п | Должность сотрудника, осуществляющего обработку ПДн | Способ обработки | Состав ПДн | Цель обработки | Основание обработки | Сроки обработки |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | Специалист - эксперт главный бухгалтер | Смешанный | ФИО, дата рождения, профессия, доходы, копия паспорта, сведения о рождении детей, должность, стаж работы, сведения о повышении квалификации, сведения о поощрениях, сведения об отпусках, сведения о социальных гарантиях, сведения из страхового свидетельства обязательного пенсионного страхования, сведения из свидетельства о постановке на учет в налоговом органе, сведения из налоговых деклараций о доходах за расчетный период, сведения о размере пенсии, ИНН, реквизиты банковских счетов | Бухгалтерский и налоговый учет. Заключение договоров, расчеты с контрагентами. | Трудовой кодекс, налоговый кодекс, ФЗ от 21.11.1996 № 129-ФЗ «О бухгалтерском учете», ФЗ от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в РФ», ФЗ от 15.12.2001 № 167-ФЗ «Об обязательном пенсионном страховании в РФ» | 75 лет  5 лет |
| 10 | Специалист второго разряда | Смешанный | ФИО, дата и место рождения, паспортные данные, сведения о регистрации по месту жительства и о временной регистрации по месту пребывания, сведения о воинском учете, сведения и призыве на военную службу, сведения о смерти, дата смерти, сведения о дееспособности/недееспособности | Осуществление учета участников референдума, проживающих на территории МО «Биробиджанский муниципальный район» ЕАО, сбор и обработка данных об избирателях для последующей передачи их в территориальную избирательную комиссию района | ФЗ от 12.06.2002 № 67-ФЗ «Об основных гарантиях прав и права на участие в референдуме граждан РФ», постановление губернатора ЕАО от 19.05.2011 № 179 «О мерах по реализации Положения о Государственной системе регистрации (учета) избирателей, участников референдума в Российской Федерации на территории ЕАО», постановление избирательной комиссии ЕАО от 28.04.2011 № 77/326 «Об обеспечении функционирования Государственной системы регистрации (учета) избирателей, участников референдума на территории ЕАО» | 5 лет |
| 12 | Глава администрации сельского поселения, Заместитель главы администрации сельского поселения | Смешанная | ФИО, дата рождения, место рождения, адрес, семейное положение, социальное положение, имущественное положение, образование, профессия, доходы, копия паспорта, паспортные данные, пол, гражданство, сведения о регистрации по месту жительства и временной регистрации по месту пребывания, номер телефона, адрес электронной почты, место работы или учебы членов семьи и родственников, должность, стаж работы, сведения о наградах (поощрениях), почетных званиях, сведения о социальных гарантиях, сведения о признании за гражданином права пользования жилым помещением, сведения о праве пользования жилым помещением, сведения о размере пенсии, сведения о социальных выплатах, о смерти, дата смерти, о судимости, сведения о дееспособности/недееспособности. | Работа с обращениями граждан | Конституция РФ, Устав МО «Биробиджанский муниципальный район», ФЗ от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в РФ», ФЗ от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан РФ», ФЗ от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» | Постоянно (предложения, письма творческого характера, заявления, жалобы содержащие сведения о серьезных недостатках и злоупотреблениях, коррупции.  5 лет  (личного характера) |
| 13 | Старший специалист первого разряда | Смешанная | ФИО, дата рождения, место рождения, адрес, семейное положение, социальное положение, имущественное положение, образование, профессия, доходы, копия паспорта, паспортные данные, пол, гражданство, сведения о регистрации по месту жительства и временной регистрации по месту пребывания, номер телефона, адрес электронной почты, место работы или учебы членов семьи и родственников, должность, стаж работы, сведения о наградах (поощрениях), почетных званиях, сведения о социальных гарантиях, сведения о признании за гражданином права пользования жилым помещением, сведения о праве пользования жилым помещением, сведения о размере пенсии, сведения о социальных выплатах, о смерти, дата смерти, о судимости, сведения о дееспособности/недееспособности. | Работа с обращениями граждан | Конституция РФ, Устав МО «Биробиджанский муниципальный район», ФЗ от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в РФ», ФЗ от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан РФ», ФЗ от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» | Постоянно (предложения, письма творческого характера, заявления, жалобы содержащие сведения о серьезных недостатках и злоупотреблениях, коррупции.  5 лет  (личного характера) |
| 14 | Заместитель главы администрации сельского поселения | Смешанная | ФИО, год рождения, месяц рождения, дата рождения, адрес, семейное положение, социальное положение, имущественное положение, образование, профессия, доходы, анкетные и биографические данные, сведения о рождении детей, паспортные данные, копия паспорта, фото на анкете в личном деле, пол, гражданство, сведения о регистрации по месту жительства и временной регистрации по месту пребывания, номер телефона, сведения о воинском учете, сведения о призыве на военную службу, специальность, место работы или учебы членов семьи и родственников, должность, стаж работы, сведения о повышении квалификации, сведения о профессиональной переподготовке, сведения о прохождении курсов подготовки специалистов, знание иностранного языка, сведения о наградах (поощрениях), почетных званиях, сведения об отпусках, сведения о социальных гарантиях, сведения из трудовой книжки, сведения из страхового свидетельства обязательного пенсионного страхования, сведения из свидетельства по постановке физического лица на учет в налоговом органе, медицинское заключение об отсутствии заболевания, препятствующего поступлению на муниципальную службу, сведения о доходах всех членов семьи за год, сведения из налоговых деклараций о доходах за расчетный период, сведения о социальных выплатах. | Учет прохождения муниципальной службы сотрудниками администрации сельского поселения . формирование кадрового резерва для замещения должностей муниципальной службы, ведение трудовых книжек муниципальных служащих, ведение личных дел муниципальных служащих, ведение реестра муниципальных служащих, оформление и выдача служебных удостоверений муниципальных служащих, проведение конкурса на замещение вакантных должностей муниципальной службы и включение муниципальных служащих в кадровый резерв, проведение аттестации муниципальных служащих, проведение квалификационных экзаменов муниципальных служащих администрации в целях присвоения им классных чинов, установление надбавок за выслугу лет на муниципальной службе, присвоение иных надбавок и доплат, проверка достоверности и полноты сведений о доходах, об имуществе и обязательствах имущественного характера, представляемых муниципальными служащими администрации, чьи должности включены в утвержденный перечень должностей, поощрение и награждение муниципальных служащих, применении к ним дисциплинарных взысканий, заключение трудовых договоров с гражданами при приеме их на работу, составление табеля учета рабочего времени, графика ежегодных оплачиваемых отпусков, оформления документов для выезда в служебные командировки, определение стажа муниципальной службы, установления доплат к трудовым пенсиям муниципальным служащим, имеющим на это право, увольняемым из администрации, анализ уровня профессионального образования муниципальных служащих, его соответствия квалификационным требованиям, предъявляемым к замещаемым ими должностям муниципальной службы, в целях проведения работы по планированию направления муниципальных служащих для прохождения дополнительного профессионального образования, подготовка материалов по представлению к награждению государственными наградами Российской Федерации, области и главы муниципального района, ведение учета лиц, награжденных наградами. Кадровое делопроизводство на руководителей муниципальных учреждений по договору. | Конституция РФ, трудовой кодекс РФ, гражданский кодекс РФ, налоговый кодекс РФ, Устав МО «Биробиджанский муниципальный район», ФЗ от 02.03.2007 № 25-ФЗ «О муниципальной службе», ФЗ от 28.03.1998 № 53-ФЗ «О воинской обязанности и воинской службе», ФЗ от 15.12.2001 № 167-ФЗ «Об обязательном пенсионном страховании в РФ», ФЗ от 16.07.1999 № 165-ФЗ «Об основах обязательного социального страхования», ФЗ от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в РФ. | 75 лет |

Приложение 4

к постановлению администрации

сельского поселения

от 0.5.06.2019 г. № 49

**Перечень**

**должностей служащих администрации Надеждинское сельское поселение, замещение которых предусматривает осуществление обработки ПДн либо осуществление доступа к персональным данным**

**Доступ к ПДн служащих администрации Надеждинского сельского поселения имеют:**

-глава администрации сельского поселения;

-заместитель главы администрации сельского поселения;

-старший специалист первого разряда;

-специалист второго разряда;

-специалист-эксперт главный бухгалтер.

**Доступ к ПДн третьих лиц, обрабатываемых в администрации муниципального района имеют:**

-глава администрации сельского поселения;

-заместитель главы администрации сельского поселения;

-старший специалист первого разряда;

-специалист второго разряда;

-специалист-эксперт главный бухгалтер.

УТВЕРЖДЕНО

постановлением

администрации

сельского поселения

от 0.5.06.2019 г. № 49

**ПОЛОЖЕНИЕ**

**по обработке персональных данных без использования средств**

**автоматизации в администрации Надеждинского сельского поселения**

**1. Общие положения**

Настоящее Положение разработано в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», распорядительными и методическими документами ФСТЭК России, Трудовым Кодексом Российской Федерации, Федеральным законом Российской Федерации от 2 марта 2007 года № 25-ФЗ «О муниципальной службе в Российской Федерации», Федеральным законом от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации» и определяет порядок обработки персональных данных служащих администрации Надеждинского сельского поселения (далее администрация сельского поселения) третьих лиц, права и обязанности сторон трудовых отношений в связи с представлением, получением, хранением, комбинированием, передачей или любым другим использованием ими персональных данных, а также порядок защиты персональных данных служащих администрации сельского поселения и третьих лиц при их обработке без средств автоматизации.

Положение является внутренним нормативным документом, регламентирующим деятельность администрации сельского поселения в сфере защиты ПДн, обрабатываемых без использования средств автоматизации. Положение является обязательным для выполнения всеми служащими администрации сельского поселения.

Целью защиты ПДн, обрабатываемых без использования средств автоматизации, является предотвращение возможной утечки информации и (или) несанкционированного и непреднамеренного изменения или разрушения ПДн.

Обработка ПДн 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.

В администрации сельского поселения приняты следующие возможные методы неавтоматизированной обработки персональных данных:

-обработка персональных данных исключительно на бумажных носителях информации;

-обработка персональных данных с использованием средств вычислительной техники с выводом документа на бумажный носитель.

Защита ПДн при их неавтоматизированной обработке в администрации сельского поселения достигается выполнением комплекса организационных мероприятий и применением средств защиты информации от несанкционированного доступа с целью нарушения целостности (модификации, уничтожения) и доступности информации в процессе ее передачи и хранения.

Действие Положения не распространяется на устанавливаемый государственными органами режим защиты сведений, составляющих государственную тайну и иные виды тайн, защита которых определена отдельными законодательными и нормативно-методическими документами Российской Федерации.

**2. Требования к неавтоматизированной обработке персональных данных и мероприятия по их выполнению**

В администрации сельского поселения доступ к ПДн, обрабатываемым без использования средств автоматизации имеют:

-глава администрации сельского поселения;

-заместитель главы администрации сельского поселения;

-старший специалист первого разряда;

-специалист второго разряда;

-специалист-эксперт главный бухгалтер.

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).

Для выполнения данного требования при обработке персональных данных исключительно на бумажных носителях, хранение документов, содержащих персональные данные, осуществляется в специально отведенных местах.

Служащие администрации сельского поселения осуществляют обработку персональных данных в соответствии со своими должностными обязанностями.

Служащие администрации, сельского поселения осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации.

Служащие администрации сельского поселения, осуществляющие обработку персональных данных без использования средств автоматизации, в обязательном порядке должны быть ознакомлены с положениями настоящего положения.

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

-документы, разрабатываемые в процессе неавтоматизированной обработки персональных данных, должны печататься на фирменном бланке администрации муниципального района, либо содержать необходимые реквизиты. При этом цель, сроки обработки персональных данных должны содержаться в преамбуле документа. Перечень действий с персональными данными и способы обработки определены настоящим положением.

При неавтоматизированной обработке персональных данных осуществляется раздельное хранение документов, содержащих персональные данные субъекта, обрабатываемые в разных целях.

При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других, зафиксированных на том же носителе персональных данных, принимаются следующие мероприятия по обеспечению безопасности персональных данных:

-при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

-при необходимости уничтожения или блокирования части персональных данных, уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

-уничтожение 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).

Обработка персональных данных субъектов персональных данных, связанная с однократным пропуском субъекта на территорию администрации муниципального района, осуществляется при соблюдении следующих условий:

-необходимость ведения журнала учета посетителей должна быть зафиксирована нормативным актом администрации сельского поселения;

-в соответствии с данным нормативным актом копирование журнала учета посетителей должно быть запрещено;

- персональные данные субъекта заносятся в журнал не более одного раза в каждом случае пропуска субъекта на территорию администрации сельского поселения.

При необходимости изменения персональных данных, зафиксированных на бумажном носителе, осуществляется исправление персональных данных с использованием пишущей ручки или изготовлением нового документа.

Хранение персональных данных на бумажных носителях должно осуществляться в специально отведенных помещениях или в установленных в помещении надежных хранилищах (металлических шкафах, пеналах, сейфах).

При этом не допускается осуществлять совместное хранение персональных данных и документов, не относящихся к субъекту персональных данных.

**3. Правила приема и регистрации входящей корреспонденции содержащей персональные данные**

Прием, первичная обработка и регистрация входящей почтовой корреспонденции, содержащей персональные данные, осуществляется отделом организационно-контрольной работы и информационных технологий администрации сельского поселения, уполномоченным на эти действия, при этом проверяется правильность ее доставки, целостность вложений и наличие приложений.

На полученных документах, в правом нижнем углу лицевой стороны документа проставляется регистрационный штамп администрации муниципального района, с указанием даты поступления документа и его регистрационного номера.

Состав документа фиксируется в Журнале регистрации входящих документов.

Поступившие в администрацию сельского поселения машинные носители информации, содержащие персональные данные (в том числе сторонних организаций) учитываются как приложение к основному входящему документу в Журнале регистрации входящих документов.

После регистрации входящие документы передаются на рассмотрение руководству администрации сельского поселения в соответствии с распределением обязанностей.

Рассмотренный документ в соответствии с наложенной резолюцией передается под роспись исполнителю для использования в работе.

В случае, когда документ должен быть передан двум и более исполнителям, изготавливается необходимое количество копий документов, которые передаются под роспись исполнителям.

На подлиннике документа указывается дата, количество изготовленных копий, подпись и Ф.И.О. лица их изготовивших.

Корреспонденция, содержащая персональные данные, хранится в структурных подразделениях администрации сельского поселения в сформированных номенклатурных делах.

При отсутствии необходимости хранения копий документов содержащих персональные данные, копии уничтожаются, при этом на оригинале документа проставляется соответствующая отметка.

При обнаружении во входящей корреспонденции содержащей персональные данные повреждений или отсутствия указанных в корреспонденции вложенных документов, составляющих персональные данные, составляется акт в двух экземплярах:

* первый экземпляр направляется отправителю;
* второй экземпляр подшивается в дело.

При поступлении в администрацию сельского поселения корреспонденции в электронном виде, содержащей сведения, отнесенные к персональным данным, служащий, принявший корреспонденцию, обязан перенести документ на бумажный носитель или удалить входящее электронное письмо. Учет, первичная обработка и регистрация данного документа осуществляется установленным порядком.

Изготовление не учтенных (не зарегистрированных) копий документов, содержащих персональные данные, запрещается.

**4. Правила подготовки и отправки документов, содержащих персональные данные**

Исходящие документы готовятся на фирменных бланках администрации сельского поселения в соответствии с требованиями по делопроизводству, принятыми в администрации сельского поселения.

Подписанный уполномоченными лицами документ регистрируется Журнале регистрации исходящих документов и направляется адресату.

-при получении от исполнителей документов, предназначенных к отправке, проверяется наличие всех экземпляров и листов документа, приложений к нему, правильность оформления и адресования;

-перед отправкой необходимо выяснить способ отправки документа (пакет может быть доставлен адресату ценным, заказным письмом либо лично исполнителем при наличии такой возможности).

**5. Заключительные положения**

Настоящее Положение доводится до служащих администрации сельского поселения, в должностные обязанности которых входит обработка ПДн, под роспись при приеме на работу.

УТВЕРЖДЕНО

постановлением

администрации

сельского поселения

от 0.5.06.2019 г. № 49

**ПОЛОЖЕНИЕ**

**об организации и обеспечении защиты персональных данных при их обработке в информационных системах персональных данных администрации Надеждинского сельского поселения**

**1. Общие положения**

Настоящее Положение разработано в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21 марта 2012года № 211 «Об утверждении перечня мер, направленных, на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПД», приказ ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей гостайну, содержащейся в государственных информационных системах», распорядительными и методическими документами ФСТЭК России и определяет порядок обработки персональных данных служащих администрации Надеждинского сельского поселения (далее - администрация) и третьих лиц, права и обязанности сторон трудовых отношений в связи с представлением, получением, хранением, комбинированием, передачей или любым другим использованием ими персональных данных, а также порядок защиты персональных данных служащих администрации и третьих лиц, в том числе при их обработке в информационных системах персональных данных.

Положение является внутренним нормативным документом, регламентирующим деятельность администрации в сфере защиты ПДн, обрабатываемых в ИСПДн администрации. Положение является обязательным для выполнения всеми служащими администрации.

Целью защиты ПДн является предотвращение возможной утечки информации и (или) несанкционированного и непреднамеренного изменения или разрушения ПДн.

Защита ПДн в администрации достигается выполнением комплекса организационных мероприятий и применением средств защиты информации от несанкционированного доступа, с целью нарушения целостности (модификации, уничтожения) и доступности информации в процессе ее обработки, передачи и хранения, а также работоспособности технических средств.

Объектами защиты в администрации являются персональные данные, средства и системы информатизации (СВТ, АС различного уровня и назначения на базе СВТ, в том числе информационно-вычислительные комплексы, сети и системы и другие технические средства обработки информации), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), используемые для обработки ПДн.

Действие Положения не распространяется на устанавливаемый государственными органами режим защиты сведений, составляющих государственную тайну и иные виды тайн, защита которых определена отдельными законодательными и нормативно-методическими документами Российской Федерации.

**2. Персональные данные, подлежащие защите**

Информационные ресурсы, содержащие ПДн, определяются Перечнем информационных систем персональных данных в администрации, утверждаемым постановлением администрации.

Информационные ресурсы, содержащие ПДн, расположены в ИСПДн администрации, состоящих из автоматизированных рабочих мест (АРМ) пользователей на базе ПЭВМ, серверов и отчуждаемых носителей информации.

В целях информационного обеспечения администрации могут создаваться общедоступные источники персональных данных (в том числе справочники, телефонные книги, адресные книги). Режим конфиденциальности для общедоступных источников персональных данных не устанавливается.

**3. Организационная система обеспечения безопасности ПДн**

Муниципальные служащие администрации несут персональную ответственность за обеспечение безопасности ПДн на участке деятельности подразделения, организуют выполнение установленных настоящим Положением требований по защите ПДн, принимают меры по максимальному ограничению возможности ознакомления с информацией служащих, которым по роду выполняемых ими должностных обязанностей она не требуется.

**3.1. Состав организационной системы обеспечения безопасности ПДн**

В организационную систему обеспечения безопасности ПДн администрации муниципального района входят:

-глава администрации сельского поселения;

--глава администрации сельского поселения;

-заместитель главы администрации сельского поселения;

-старший специалист первого разряда;

-специалист второго разряда;

-специалист-эксперт главный бухгалтер;

-старший специалист первого разряда;

-специалист второго разряда;

-специалист-эксперт главный бухгалтер.

Общее руководство организацией и координацией работ по защите ПДн осуществляет глава администрации сельского поселения.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Глава администрации  сельского поселения |  | |  |  |
|  |  |  | |  |  |
| заместитель главы администрации сельского поселения | старший специалист первого разряда | специалист второго разряда | специалист-эксперт главный бухгалтер | | |

Рис. 1 – Схема организационной системы обеспечения безопасности ПДн

Заместитель главы администрации сельского поселения осуществляет подготовку предложений по совершенствованию и реализации мероприятий по обеспечению безопасности ПДн в ИСПДн администрации, является администратором ИСПДн администрации, ведет контроль деятельности муниципальных служащих по выполнению ими установленных требований обеспечения безопасности ПДн в ИСПДн администрации.

Распоряжением администрации назначается администратор безопасности информационной безопасности в ИСПДн.

Права и обязанности администратора безопасности прописаны в Инструкции администратору ИСПДн в администрации.

Служащие администрации при осуществлении своих функциональных обязанностей с использованием ИСПДн администрации непосредственно реализуют требования безопасности информации, принятые для ИСПДн администрации, исполняют установленные режимы защиты ПДн, обеспечивают строгое исполнение предписанных правил безопасности информации.

**3.2. Права и обязанности лиц, ответственных за обеспечение безопасности ПДн**

Заместитель главы администрации сельского поселения:

- контролирует деятельность служащих подразделений администрации по вопросам обеспечения безопасности информации;

- требует прекращения обработки защищаемой информации в администрации при выявлении существенных нарушений в технологии обработки информации, при выходе из строя средств защиты информации и в других случаях выявления грубых нарушений требований по обеспечению информационной безопасности администрации;

- вносит на рассмотрение руководству администрации предложения по привлечению к материальной и дисциплинарной ответственности виновных в утечке информации, составляющей конфиденциальную информацию;

- участвует в работе экспертных комиссий при рассмотрении вопросов обеспечения информационной безопасности;

- привлекает в установленном порядке специалистов структурных подразделений администрации и сторонних организаций для проведения исследований, разработки решений, проведения мероприятий и разработки нормативно-методических документов по вопросам обеспечения безопасности информации;

- определяет необходимость и участвует в разработке нормативных документов, касающихся вопросов обеспечения информационной безопасности, включая документы, регламентирующие деятельность служащих подразделений администрации;

- осуществляет контроль за соблюдением режима физической охраны технических средств ИСПДн.

Методическое руководство деятельностью служащих администрации по организации и обеспечению безопасности информации осуществляется заместителем главы администрации сельского поселения.

Сотрудники администрации, вовлеченные в защиту ПДн в администрации, в пределах своих должностных обязанностей, обеспечивают соблюдение пользователями порядка и правил при работе с ПДн.

Пользователи ИСПДн администрации обязаны соблюдать требования внутренних нормативных документов, определяющих порядок обеспечения безопасности ПДн в ИСПДн.

Пользователи ИСПДн не имеют права использовать в неслужебных целях информационные ресурсы ИСПДн, обязаны хранить охраняемые законом ПДн и не разглашать ПДн, ставшие им известными в связи с исполнением должностных обязанностей.

**4. Порядок классификации ИСПДн и определение угроз безопасности ПДн при их обработке в ИСПДн**

Классификация ИСПДн проводится в соответствии с постановлением правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», с приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Устанавливается четыре класса защищенности информационной системы, определяющие уровни защищенности содержащейся в ней информации. Самый низкий – четвертый, самый высокий – первый.

Классификация ИСПДн проводится на этапе создания ИСПДн или в ходе их эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых ИСПДн) с целью установления методов и способов защиты информации, необходимых для обеспечения безопасности ПДн.

Класс защищенности определяется в зависимости от уровня значимости информации (УЗ), обрабатываемой в этой информационной системе, и масштаба информационной системы (федеральный, региональный, объектовый).

Уровень значимости информации определяется степенью возможного ущерба для обладателя информации (заказчика) и (или) оператора от нарушения конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), целостности (неправомерные уничтожение или модифицирование) или доступности (неправомерное блокирование) информации

УЗ = [(конфиденциальность, степень ущерба) (целостность, степень ущерба) (доступность, степень ущерба)].

где степень возможного ущерба может быть:

высокой, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять возложенные на них функции;

средней, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций;

низкой, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств.

Информация имеет высокий уровень значимости (УЗ 1), если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена высокая степень ущерба. Информации имеет средний уровень значимости (УЗ 2), если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена средняя степень ущерба и нет ни одного свойства для которого определена высокая степень ущерба. Информация имеет низкий уровень значимости (УЗ 3), если для всех свойств безопасности информации (конфиденциальности, целостности, доступности) определены низкие степени ущерба.

Информация имеет минимальный уровень значимости (УЗ 4), если обладателем информации (заказчиком) и (или) оператором степень ущерба от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности) не может быть определена, но при этом информация подлежит защите в соответствии с законодательством Российской Федерации.

При обработке в информационной системе двух и более видов информации уровень значимости определяется отдельно для каждого вида информации. Итоговый уровень значимости информации, обрабатываемой в информационной системе, устанавливается по наивысшим значениям степени возможного ущерба, определенным для конфиденциальности, целостности, доступности информации каждого вида информации.

Информационная система имеет федеральный масштаб, если она функционирует на территории Российской Федерации (в пределах федерального округа) и имеет сегменты в субъектах Российской Федерации, муниципальных образованиях и (или) организациях.

Информационная система имеет региональный масштаб, если она функционирует на территории субъекта Российской Федерации и имеет сегменты в одном или нескольких муниципальных образованиях и (или) подведомственных и иных организациях.

Информационная система имеет объектовый масштаб, если она функционирует на объектах одного федерального органа государственной власти, органа государственной власти субъекта Российской Федерации, муниципального образования и (или) организации и не имеет сегментов в территориальных органах, представительствах, филиалах, подведомственных и иных организациях.

Класс защищенности информационной системы определяется в соответствии с таблицей:

|  |  |  |  |
| --- | --- | --- | --- |
| Уровень значимости информации | Масштаб информационной системы | | |
| Федеральный | Региональный | Объектовый |
| УЗ 1 | К1 | К1 | К1 |
| УЗ 2 | К1 | К2 | К2 |
| УЗ 3 | К2 | К3 | К3 |
| УЗ 4 | К3 | К3 | К4 |

По результатам классификации ИСПДн оформляется акт классификации, утверждаемый главой администрации.

Класс защищенности информационной системы подлежит пересмотру при изменении масштаба информационной системы или значимости обрабатываемой в ней информации

Угрозы безопасности информации определяются по результатам оценки возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей, анализа возможных уязвимостей информационной системы, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

При определении угроз безопасности информации учитываются структурно-функциональные характеристики информационной системы, включающие структуру и состав информационной системы, физические, логические, функциональные и технологические взаимосвязи между сегментами информационной системы, с иными информационными системами и информационно-телекоммуникационными сетями, режимы обработки информации в информационной системе и в ее отдельных сегментах, а также иные характеристики информационной системы, применяемые информационные технологии и особенности ее функционирования.

По результатам определения угроз безопасности информации при необходимости разрабатываются рекомендации по корректировке структурно-функциональных характеристик информационной системы, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

Модель угроз безопасности информации должна содержать описание информационной системы и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

Для определения угроз безопасности информации и разработки модели угроз безопасности информации применяются методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085

**5. Требования по защите ПДн при их обработке в ИСПДн**

Администрация должна соблюдать режим конфиденциальности при обработке ПДн, за исключением случаев, когда обеспечение конфиденциальности ПДн не требуется.

Организационные и технические меры защиты информации, реализуемые в информационной системе в рамках ее системы защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационной системы должны обеспечивать:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;

- управление доступом субъектов доступа к объектам доступа;

- ограничение программной среды;

- защиту машинных носителей информации;

- регистрацию событий безопасности;

- антивирусную защиту;

- обнаружение (предотвращение) вторжений;

- контроль (анализ) защищенности информации;

- целостность информационной системы и информации;

- доступность информации;

- защиту среды виртуализации;

- защиту технических средств;

- защиту информационной системы, ее средств, систем связи и передачи данных.

Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

Меры по защите машинных носителей информации (средства обработки (хранения) информации, съемные машинные носители информации) должны исключать возможность несанкционированного доступа к машинным носителям и хранящейся на них информации, а также несанкционированное использование съемных машинных носителей информации.

Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) информацию в целях ее добывания, уничтожения, искажения и блокирования доступа к информации, а также реагирование на эти действия.

Меры по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности информации, содержащейся в информационной системе, путем проведения мероприятий по анализу защищенности информационной системы и тестированию ее системы защиты информации.

Меры по обеспечению целостности информационной системы и информации должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащейся в ней информации, а также возможность восстановления информационной системы и содержащейся в ней информации.

Меры по обеспечению доступности информации должны обеспечивать авторизованный доступ пользователей, имеющих права по такому доступу, к информации, содержащейся в информационной системе, в штатном режиме функционирования информационной системы.

Меры по защите среды виртуализации должны исключать несанкционированный доступ к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, а также воздействие на информацию и компоненты, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей.

Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту информации при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы, проектных решений по ее системе защиты информации, направленных на обеспечение защиты информации.

Выбор мер защиты информации для их реализации в информационной системе в рамках ее системы защиты информации включает:

определение базового набора мер защиты информации для установленного класса защищенности информационной системы в соответствии с базовыми наборами мер защиты информации;

адаптацию базового набора мер защиты информации применительно к структурно-функциональным характеристикам информационной системы, информационным технологиям, особенностям функционирования информационной системы (в том числе предусматривающую исключение из базового набора мер защиты информации мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе);

уточнение адаптированного базового набора мер защиты информации с учетом не выбранных ранее мер защиты информации, в результате чего определяются меры защиты информации, обеспечивающие блокирование (нейтрализацию) всех угроз безопасности информации, включенных в модель угроз безопасности информации;

дополнение уточненного адаптированного базового набора мер защиты информации мерами, обеспечивающими выполнение требований о защите информации, установленными иными нормативными правовыми актами в области защиты информации, в том числе в области защиты персональных данных.

Для выбора мер защиты информации для соответствующего класса защищенности информационной системы применяются методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085.

**6. Организационные меры по защите ПДн при их обработке в ИСПДн**

**6.1. Требования к оборудованию помещений и рабочих мест пользователей ИСПДн**

Все технические средства ИСПДн администрации должны находиться в пределах контролируемых зон, исключающих неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Размещение технических средств, обрабатывающих ПДн, должно осуществляться с учетом требования минимизации доступа в рабочие помещения лиц, не связанных с обслуживанием оборудования.

Размещение устройств отображения и печати информации, используемых в составе АРМ пользователей ИСПДн администрации, должно осуществляться с учетом максимального затруднения визуального просмотра информации посторонними лицами. Кроме того, должны приниматься дополнительные меры, исключающие подобный просмотр (шторы, жалюзи на окнах, непрозрачные экраны).

Неиспользуемые в процессе обработки ПДн устройства ввода/вывода АРМ пользователей ИСПДн (СОМ, LPT, НГМД, CD, USB) необходимо отключить либо опечатать (опломбировать) в случае, если данные функции нельзя реализовать с помощью СЗИ на программном уровне.

Серверы и коммуникационное оборудование ИСПДн должны располагаться в отдельном опломбированном помещении с прочной запираемой дверью. Перечень лиц, имеющих право доступа в указанные помещения, утверждается отдельным списком. Ключи от дверей данных помещений должны быть только у лиц, имеющих право доступа в них. Допускается устанавливать коммуникационное оборудование в отдельных запираемых и опечатываемых металлических шкафах, размещаемых в охраняемых помещениях.

**6.2. Требования к процедуре получения доступа в ИСПДн**

Предоставление доступа к ПДн, обрабатываемым в ИСПДн осуществляется на основании распоряжения администрации.

Администратором безопасности информации должна проводиться периодическая проверка прав пользователей ИСПДн следующим образом:

- проверка прав пользователей должна проводиться на периодической основе или после каждого изменения в системе. При этом проверка прав пользователей, имеющих особые привилегии для доступа в систему, должна проводиться с меньшей периодичностью;

- должна быть предусмотрена регулярная проверка адекватности назначенных привилегий с целью исключения получения кем-либо из пользователей излишних прав.

**7. Технические требования по защите ПДн при их обработке в ИСПДн**

Технические меры защиты информации реализуются посредством применения средств защиты информации, имеющих необходимые функции безопасности.

В этом случае в информационных системах 1 и 2 класса защищенности применяются:

средства вычислительной техники не ниже 5 класса;

системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса;

межсетевые экраны не ниже 3 класса в случае взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и не ниже 4 класса в случае отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена.

В информационных системах 3 класса защищенности применяются:

средства вычислительной техники не ниже 5 класса;

системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса в случае взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и не ниже 5 класса в случае отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена;

межсетевые экраны не ниже 3 класса в случае взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и не ниже 4 класса в случае отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена.

В информационных системах 4 класса защищенности применяются:

средства вычислительной техники не ниже 5 класса;

системы обнаружения вторжений и средства антивирусной защиты не ниже 5 класса; межсетевые экраны не ниже 4 класса.

В информационных системах 1 и 2 классов защищенности применяются средства защиты информации, программное обеспечение которых прошло проверку не ниже чем по 4 уровню контроля отсутствия недекларированных возможностей.

**7.1. Требования к резервированию**

Для обеспечения возможности быстрого восстановления ПДн и средств их обработки в случае повреждения (утраты) рабочей копии в ИСПДн администрации муниципального района должны выполняться следующие требования:

-резервные копии информационных ресурсов, содержащих ПДн, и инструкции по их восстановлению должны храниться в специально выделенном месте, территориально отдаленном от места обработки самой информации;

-для обеспечения сохранности резервных копий должен быть применён комплекс организационных и технических мер защиты;

-носители, на которые осуществляется резервное копирование, должны регулярно проверяться на работоспособность;

-должны быть предусмотрены регулярные проверки процедур восстановления.

**7.2. Обеспечение безопасности ПДн при передаче**

При передаче ПДн субъекта должны соблюдаться следующие требования:

-не сообщать ПДн субъекта третьей стороне без его письменного согласия, за исключением случаев, предусмотренных действующим законодательством Российской Федерации;

-предупреждать лиц, получивших ПДн, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получившие ПДн, обязаны соблюдать режим конфиденциальности;

-разрешать доступ к ПДн только специально уполномоченным на это служащим, при этом указанные служащие должны иметь право получать только те ПДн, которые необходимы для выполнения ими должностных обязанностей;

-передавать ПДн субъектов их представителям в порядке, установленном действующим законодательством Российской Федерации, и ограничивать эту информацию только теми ПДн, которые необходимы для выполнения указанными представителями их должностных функций;

-передача ПДн третьим лицам может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

Трансграничная передача ПДн на территорию иностранного государства допускается только с согласия субъекта или в случаях, определенных законодательством Российской Федерации.

**7.3. Обеспечение безопасности при хранении ПДн**

Полный перечень информационных систем ПДн администрации утвержден постановлением администрации.

Круг лиц, допущенных к работе с документами, содержащими ПДн служащих, утверждается постановлением администрации.

Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки. ПДн подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении, поэтому для каждой системы ПДн в обязательном порядке устанавливается срок хранения ПДн и осуществляется регулярное уничтожение, а также обезличивание ПДн при наличии такой возможности.

**8. Планирование и контроль обеспечения безопасности ПДн**

Планирование работ по защите информации проводится в целях выявления и устранения недостатков в системе защиты информации, разработки предложений по ее совершенствованию. В администрации разрабатывается утверждаемый главой администрации План мероприятий по защите информации ПДн, включающий следующие основные мероприятия:

- разработка (модернизация) систем защиты информации;

- контроль защищенности информации в ИСПДн;

- контроль организации защиты информации;

- устранение недостатков по результатам ранее проведенных проверок и контрольных мероприятий.

План включает в себя перечень мероприятий, подразделения, ответственные за проведение работ, сроки выполнения мероприятий и состав отчетных документов, оформляемых по результатам их реализации.

План мероприятий по защите персональных данных разрабатывается ежегодно.

С целью изучения, анализа и оценки фактического состояния безопасности ПДн, выявления недостатков и нарушений режима конфиденциальности в работе с персональными данными, предпосылок к возникновению этих нарушений, установления их причин и выработки необходимых предложений для их устранения, а также для своевременного выявления и предотвращения утечки информации, содержащей ПДн, в ИСПДн должен проводиться периодический (не реже 1 раза в год) контроль состояния защиты ПДн, который заключается в оценке:

- соблюдения требований руководящих и нормативно-методических документов по защите ПДн;

- работоспособности применяемых средств защиты информации в соответствии с их эксплуатационной документацией;

- знаний и выполнения персоналом своих функциональных обязанностей в части защиты ПДн.

Контроль осуществляется путем проведения плановых и внеплановых проверок. Плановые проверки пользователей ИСПДн, технических средств и систем проводятся комиссиями, назначаемыми распоряжением администрации. План внутренних проверок состояния защиты ПДн в ИСПДн составляется на 12 месяцев.

Результаты работы оформляются актом в произвольной форме. В акте указываются рекомендации по закрытию возможных каналов утечки информации.

Проверка технических средств и систем проводится не реже одного раза в год, а также дополнительно при изменении состава технических средств и систем, условий обработки информации, содержащей ПДн.

Все работы по контролю должны проводиться при строгом соблюдении мер безопасности, исключающих разглашение сведений о проводимых работах, местах размещения технических средств и систем, используемых СЗИ и возможных каналах утечки информации, содержащей ПДн.

В случаях обнаружения нарушений при обработке ПДн в ИСПДн администрации ответственный за обработку ПДн обязан:

-немедленно прекратить обработку ПДн в ИСПДн, где обнаружены нарушения, и принять меры к их устранению;

-организовать в установленном порядке расследование причин и условий появления нарушений с целью недопущения их в дальнейшем и привлечения к ответственности виновных лиц.

Возобновление работ разрешается только после устранения нарушений и проверки достаточности и эффективности принятых мер, соответствия их требованиям нормативных документов по защите ПДн.

**9. Ответственность**

**9.1. Ответственность за обеспечение безопасности ПДн**

Лица, виновные в нарушении нормативных правовых актов и внутренних актов администрации, регулирующих обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

Администрация, как владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения, реализующее полномочия владения, пользования, распоряжения конфиденциальной информацией в пределах, установленных законом, несет ответственность за использование персональных данных в целях причинения имущественного и морального вреда субъектов ПДн, затруднения реализации их прав и свобод. Ограничение прав субъектов ПДн на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено.

**9.2. Ответственность за неразглашение информации, содержащей ПДн**

Под разглашением информации, содержащей ПДн, понимается действие или бездействие должностных лиц, в результате которых информация, содержащая ПДн, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

Утрата документов, содержащих ПДн, – это выход (в том числе и временный) документов из владения ответственного за их сохранность служащего, которому они были доверены, вследствие чего эти документы, а равно содержащиеся в них сведения, стали, либо могли стать достоянием посторонних лиц.

Разглашение информации, содержащей ПДн, или утрата документов, содержащих таковую, относится к числу грубых нарушений служебного контракта.

За разглашение информации, содержащей ПДн, утрату документов, содержащих такие сведения, а также за иные нарушения режима защиты ПДн виновные лица несут дисциплинарную, административную или уголовную ответственность в соответствии с действующим законодательством Российской Федерации.

**9.3. Ответственность за нарушение требований настоящего Положения**

Служащие администрации несут персональную ответственность за соблюдение настоящего Положения.

Служащие администрации несут ответственность по действующему законодательству Российской Федерации за разглашение сведений, составляющих ПДн, ставших известными им случайно или по роду работы.

**10. Заключительные положения**

Настоящее Положение доводится до служащих администрации, в должностные обязанности которых входит обработка ПДн, под роспись при приеме на работу.