ПРОЕКТ

РОССИЙСКАЯ ФЕДЕРАЦИЯ
ОРЛОВСКАЯ ОБЛАСТЬ
ГЛАЗУНОВСКИЙ РАЙОН

АДМИНИСТРАЦИЯ ОЧКИНСКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ

ПОСТАНОВЛЕНИЕ

_____2024г. №____

О порядке обработки персональных
данных в администрации
Очкинского сельского поселения

В соответствие с Федеральными законами от 27 июля 2006 года № 152-ФЗ «О персональных данных», от 2 марта 2007 года № 25-ФЗ «О муниципальной службе в Российской Федерации», Трудовым кодексом Российской Федерации, постановлениями Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», от 17 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», ПОСТАНОВЛЯЕТ:

1. Утвердить Положение о порядке обработки персональных данных в администрации Очкинского сельского поселения согласно приложению 1 к настоящему постановлению.

2. Утвердить Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных в администрации Очкинского сельского поселения согласно приложению 2 к настоящему постановлению.

3. Утвердить Инструкцию администратора безопасности информационной системы персональных данных (далее - ИСПДн), пользователей ИСПДн по обеспечению безопасности информации при обработке персональных данных в администрации Очкинского сельского поселения согласно приложение 3 к настоящему постановлению.

4. Ведущему специалисту по делопроизводству, организационной и кадровой работе администрации Очкинского сельского поселения:

- при выполнении работ руководствоваться Инструкцией администратора безопасности ИСПДн.

5. Постановление Очкинского сельского поселения от 29 декабря 2012г. № 53 «О порядке обработки персональных данных в администрации Очкинского сельского поселения признать утратившим силу.

6. Контроль за выполнением настоящего постановления оставляю за собой.

Глава Очкинского
сельского поселения О.И.Боева

Приложение 1 к постановлению администрации Очкинского сельского поселения «О порядке обработки

персональных данных в администрации Очкинского сельского поселения»

ПОЛОЖЕНИЕ
о порядке обработки персональных данных в администрации Очкинского сельского поселения

1. **Общие положения**

1.1. Положение о порядке обработки персональных данных в администрации Очкинского сельского поселения (далее – Положение) разработано на основании Конституции Российской Федерации, Трудового кодекса Российской Федерации, Федерального закона от 27 июля 2006 года № 152-ФЗ "О персональных данных" и других нормативно-правовых актов Российской Федерации.

1.2. Настоящее Положение устанавливает порядок приема, получения, поиска, сбора, систематизации, накопления, хранения, уточнения, обновления, изменения, использования, распространения (в том числе передачи), обезличивания, блокирования, уничтожения, учета документов, содержащих сведения, отнесенные к персональным данным субъектов персональных данных администрации Очкинского сельского поселения (далее – Администрации) с использованием средств автоматизации или без их использования.

1.3. Целью настоящего Положения является определение порядка обработки персональных данных в Администрации и защиты персональных данных субъектов персональных данных Администрации (далее – Субъектов) от несанкционированного доступа и разглашения, неправомерного их использования или утраты. Персональные данные являются конфиденциальной, строго охраняемой информацией.

1.4. Основные термины и определения, применяемые в настоящем Положении:

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

1.4.1.1 **Персональные данные**, разрешенные субъектом персональных данных для распространения, - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном настоящим Федеральным законом;

1.4.2. **Оператор** – Администрация, организующая и осуществляющая обработку персональных данных, и определяющая цели и содержание обработки персональных данных.

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

1.4.3.1 **Автоматизированная обработка персональных данн**ых - обработка персональных данных с помощью средств вычислительной техники;

1.4.4. **Распространение персональных данных** – распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;.

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

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

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

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

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

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

Обеспечение конфиденциальности персональных данных не требуется:

в случаях обезличивания персональных данных;

в отношении общедоступных персональных данных.

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

В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных (ПРИЛОЖЕНИЕ 1 к настоящему Положению) могут включаться фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные данным Субъектом.

Сведения о Субъекте могут быть в любое время исключены из общедоступных источников персональных данных по его требованию или по решению Оператора, либо по решению суда или иных уполномоченных государственных органов.

1.4.12.**Персональные данные конфиденциального характера** - персональные данные, внесенные в личные дела муниципальных служащих, иные сведения, содержащиеся в личных делах муниципальных служащих (за исключением сведений, которые в установленных федеральными законами случаях могут быть опубликованы в средствах массовой информации), а также персональные данные третьих лиц, предоставленные ими Администрации.

Средствам массовой информации (Интернет-портал администрации) предоставляются следующие сведения о доходах, имуществе и обязательствах имущественного характера муниципальных служащих с письменного согласия Субъекта (ПРИЛОЖЕНИЕ 2 к настоящему Положению):

а) декларированный годовой доход;

б) перечень объектов недвижимости, принадлежащих муниципальному служащему на праве собственности или находящихся в его пользовании, с указанием вида, площади и страны расположения каждого из них;

в) перечень транспортных средств.

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

1.4.14. **Работники** – лица, имеющие трудовые отношения с Оператором, либо кандидаты на вакантную должность, вступившие в отношения по поводу приема на работу.

1.5. **К субъектам персональных данных в Администрации (Субъектам)** относятся лица – носители персональных данных, передавшие свои персональные данные в Администрацию (как на добровольной основе, так и в рамках выполнения требований нормативно-правовых актов) для приема, получения, поиска, сбора, систематизации, накопления, хранения, уточнения, обновления, поиска, сбора, систематизации, накопления, хранения, уточнения, обновления, изменения, использования, распространения (в том числе передачи), обезличивания, в том числе:

муниципальные служащие, а также лица, выполняющие работы по договорам гражданско-правового характера и трудовым договорам;

иные лица, предоставляющие персональные данные Администрации.

По тексту Положения вид Субъекта персональных данных при необходимости может уточняться.

1.6.Персональные данные защищаются от несанкционированного доступа в соответствии с нормативно-правовыми актами Российской Федерации, нормативно-распорядительными актами и рекомендациями регулирующих органов в области защиты информации, а также утвержденными регламентами и инструкциями Администрации.

1.7.Сбор, хранение, использование и распространение персональных данных лица без письменного его согласия не допускаются. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75-летнего срока хранения, если иное не определено законом.

1.8.Должностные лица Администрации, в обязанности которых входит ведение персональных данных Субъектов, обязаны обеспечить каждому Субъекту возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

1.9.Персональные данные не могут быть использованы в целях:

причинения имущественного и морального вреда гражданам;

затруднения реализации прав и свобод граждан Российской Федерации.

1.10.Настоящее Положение и изменения к нему являются обязательными для исполнения всеми сотрудниками, имеющими доступ к персональным данным Субъектов Администрации. Все сотрудники Администрации должны быть ознакомлены под роспись с настоящим Положением в редакции, действующей на момент указанного ознакомления (ПРИЛОЖЕНИЕ 3 к настоящему Положению).

2. Принципы обработки персональных данных

2.1.Обработка персональных данных в Администрации осуществляется на основе следующих принципов:

законности целей и способов обработки персональных данных и добросовестности;

соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Оператора;

соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

2.2.Хранение персональных данных должно осуществляться в форме, позволяющей определить Субъекта, не дольше, чем этого требуют цели их обработки. Персональные данные подлежат уничтожению по достижению целей обработки или в случаях утраты необходимости в их достижении.

2.3.Субъект является собственником своих персональных данных и самостоятельно решает вопрос передачи Оператору своих персональных данных.

2.4.Держателем персональных данных является Администрация, которой Субъект передает во владение свои персональные данные с письменного согласия. Администрация выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством.

2.5.Потребителями (пользователями) персональных данных являются юридические и физические лица, обращающиеся к собственнику и (или) держателю персональных данных за получением необходимых сведений и пользующиеся ими без права передачи, разглашения.

2.6.Получение, хранение, комбинирование, передача или любое другое использование персональных данных Субъекта может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

3. Понятие и состав персональных данных.

3.1.Под персональными данными Субъектов понимается информация, необходимая Администрации в связи с трудовыми отношениями, в связи с исполнением своих административных обязанностей и касающаяся конкретного Субъекта (фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное и имущественное положение, образование, профессия, доходы), а также сведения о фактах, событиях и обстоятельствах жизни Субъекта, позволяющие идентифицировать его личность. Персональные данные являются конфиденциальной информацией. К персональным данным относятся следующие сведения и документы:

-анкетные и биографические данные;

-образование;

-сведения о трудовом и общем стаже;

-сведения о предыдущем месте работы работника;

-сведения о составе семьи;

-паспортные данные;

-сведения о воинском учете;

-сведения о заработной плате работника, иных выплатах Субъектам (включая стипендии);

-сведения о социальных льготах;

-специальность;

-занимаемая должность;

-наличие судимостей;

-адрес места жительства (пребывания), номер домашнего телефона;

-место работы или учебы членов семьи и родственников;

-содержание трудового договора (контракта);

-состав декларируемых сведений о доходах, об имуществе и обязательствах имущественного характера;

-подлинники и копии распоряжений по личному составу;

-основания к распоряжениям по личному составу;

-личные дела, личные карточки (форма Т-2 или Т-2 ГС) и трудовые книжки сотрудников;

-дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;

-анкеты, заполняемые Субъектами;
-копии документов об образовании;
-результаты медицинского обследования;
-рекомендации, характеристики;
-фотографии;
-копии отчетов, направляемые в органы статистики;
-документы о прохождении производственной практики студентами или слушателями ВУЗов, а также информация о выполнении ими учебных планов, успеваемости и т.п.

3.2.Документы, содержащие персональные данные, являются конфиденциальными, и содержат служебную информацию ограниченного распространения.

Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении срока хранения, если иное не определено законом.

4. Получение, обработка и хранение персональных данных

4.1.Оператор получает сведения о персональных данных Субъектов из следующих документов:
-паспорта или иного документа, удостоверяющего личность;
-писем в адрес Администрации с указанными в них адресными данными;
-писем в адрес Администрации, содержащих сведения о персональных данных;
-трудовой книжки;
-страхового свидетельства государственного пенсионного страхования;
-свидетельства о постановке на учет в налоговом органе, содержащего сведения об идентификационном номере налогоплательщика;
-документов воинского учета, содержащих сведения о воинском учете военнообязанных и лиц, подлежащих призыву на военную службу;
-документов об образовании, содержащих сведения о профессии, о квалификации или о наличии специальных знаний, специальной подготовки;
-анкет, заполняемых собственноручно при приеме на работу, или при подаче документов на участие в конкурсе на замещение вакантных должностей, предполагающих конкурсный отбор;
-иных документов и сведений, предоставляемых субъектом персональных данных при приеме на работу, обучение, в процессе работы, обучения, а также в случае представления его к награждению.

Субъект обязан представлять администрации достоверные сведения о себе. Администрация имеет право проверять достоверность указанных сведений в порядке, не противоречащем законодательству Российской Федерации.

4.2.Обработка персональных данных Субъекта может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия в трудоустройстве, обучении, продвижении по службе, обеспечения личной безопасности, контроля количества и качества выполняемой работы, обеспечения сохранности имущества.

4.3.При определении объема и содержания обрабатываемых персональных данных Субъектов Оператор руководствуется Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами.

4.4.Все персональные данные Субъекта Администрация получает непосредственно у Субъекта. Сотрудник, ответственный за документационное обеспечение кадровой деятельности, принимает от Субъекта копии документов, сверяет их полноту и правильность указанных сведений с подлинниками.

4.4.1.При получении персональных данных без непосредственного участия Субъекта, например при подаче письменных или в электронной форме запросов, обращений и т.д. Администрация исходит из того, что Субъект, заполняя указанные

документы и внося в них свои персональные данные, а так же указывая в качестве их получателя Администрацию, добровольно дает свое согласие на их обработку.

4.5.Если персональные данные Субъекта возможно получить исключительно у третьей стороны, то Субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие (ПРИЛОЖЕНИЕ 4 к настоящему Положению). Оператор должен сообщить Субъекту о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа Субъекта представить письменное согласие на их получение (ПРИЛОЖЕНИЕ 5 к настоящему Положению).

4.6.Условием обработки персональных данных Субъекта является его письменное согласие (ПРИЛОЖЕНИЕ 6 к настоящему Положению), либо положения п.п. 4.4.1. настоящего Положения. Письменное согласие Субъекта на обработку его персональных данных должно включать в себя:

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

-наименование и адрес Оператора персональных данных получающего согласие Субъекта персональных данных;

-цель обработки персональных данных;

-перечень персональных данных, на обработку которых дается согласие Субъекта;

-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.

Согласие на обработку персональных данных может быть отозвано Субъектом в соответствии с положением ст.6 Условия обработки персональных данных Федерального закона «О персональных данных».

4.7.Согласия Субъекта на обработку его персональных данных не требуется в следующих случаях:

-обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;

-обработка персональных данных осуществляется в целях исполнения трудового или иного договора или соглашения между работником и администрацией;

-обработка персональных данных осуществляется для статистических целей при условии обязательного обезличивания персональных данных;

-обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов Субъекта, если получение его согласия при данных обстоятельствах невозможно;

-обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;

-осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами.

4.8.Для обработки персональных данных, содержащихся в согласии в письменной форме Субъекта на обработку его персональных данных, дополнительное согласие не требуется.

4.9.В случаи недееспособности Субъекта согласие на обработку его персональных данных в письменной форме дает его законный представитель.

В случаи смерти Субъекта согласие на обработку его персональных данных при необходимости дает в письменной форме один из его наследников, если такое согласие не было дано Субъектом при его жизни.

4.10.В случаях, если Администрация на основании договора поручает обработку персональных данных другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

4.11.Администрация не имеет права получать и обрабатывать персональные данные Субъекта о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни, за исключением, если:

Субъект дал согласие в письменной форме на обработку своих персональных данных;

персональные данные являются общедоступными;

обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством Российской Федерации.

В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни Субъекта только с его письменного согласия.

Обработка персональных данных, перечисленных в пункте 4.11. настоящего Положения, должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка.

4.12.Защита персональных данных Субъекта от неправомерного их использования или утраты должна быть обеспечена оператором за счет его средств в порядке, установленном федеральным законодательством РФ.

4.13.Субъекты персональных данных должны быть ознакомлены под роспись с правовыми актами Администрации, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области.

4.14.Основными источниками, содержащими персональные данные субъектов персональных данных в Администрации, являются их личные дела.

Личные дела хранятся уполномоченным лицом на бумажных носителях. Помимо этого персональные данные могут храниться в виде электронных документов, баз данных. Личное дело пополняется на протяжении всей трудовой деятельности работника Администрации.

Письменные доказательства получения Оператором согласия Субъекта персональных данных на их обработку хранятся в личном деле.

4.15.При обработке персональных данных Оператор вправе определять способы обработки, документирования, хранения и защиты персональных данных на базе современных информационных технологий.

4.16.Круг лиц, допущенных к работе с документами, содержащими персональные данные Субъектов, определяется распоряжением Администрации.

4.17.Прием, учет (регистрация), хранение и обработка документов, содержащих персональные данные сотрудников осуществляется отделом кадров управления по обеспечению деятельности администрации.

4.18.Методическое руководство и контроль за соблюдением требований по обработке персональных данных возлагается на главу администрации сельского поселения.

4.19.Обеспечение техническими средствами обработки (ПЭВМ, серверами и т.д.) и их организация их эксплуатации возлагается на специалиста администрации по делопроизводству, организационной и кадровой работе.

4.20.Помещения, в которых хранятся персональные данные Субъектов, оборудуются надежными замками на вскрытие помещений. Для хранения

персональных данных используются специально оборудованные шкафы или сейфы, которые запираются на ключ. Помещения, в которых хранятся персональные данные Субъектов, в рабочее время при отсутствии в них работников должны быть закрыты. Проведение уборки помещений, в которых хранятся персональные данные, должно производиться в присутствии ответственных работников.

5. Права и обязанности сторон в области защиты персональных данных

5.1.Субъект персональных данных - работник обязан передать Администрации или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен трудовым законодательством, иными законами Российской Федерации, включая сведения об образовании, специальных знаниях, стаже работы, отношении к воинской обязанности, гражданстве, месте жительства и др., в срок, не превышающий 5 рабочих дней, сообщать в отдел кадров управления по обеспечению деятельности администрации сведения об изменении своих персональных данных.

5.2.Субъект персональных данных имеет право:

5.2.1.На полную информацию о своих персональных данных и об их обработке.

5.2.2.На свободный бесплатный доступ к своим персональным данным, включая право на получение копии любой записи, содержащей персональные данные, за исключением случаев, предусмотренных федеральными законами. Доступ к своим персональным данным предоставляется Субъекту или его законному представителю при личном обращении либо при получении запроса (ПРИЛОЖЕНИЕ 7 к настоящему Положению). Запрос должен содержать номер основного документа, удостоверяющего личность Субъекта или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись Субъекта или его законного представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации.

Сведения о наличии персональных данных должны быть предоставлены Субъекту в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим Субъектам.

5.2.3.Требовать от Оператора исключения, исправления или уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также данных, обработанных с нарушением требований Трудового кодекса Российской Федерации, Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных». Указанное требование должно быть оформлено письменным заявлением Субъекта на имя главы сельского поселения.

Персональные данные оценочного характера Субъект имеет право дополнить заявлением, выражающим его собственную точку зрения.

5.2.4.Требовать об извещении Администрацией всех лиц, которым ранее были сообщены неверные или неполные персональные данные Субъекта, обо всех произведенных в них исключениях, исправлениях или дополнениях.

5.2.5.При отказе Оператора исключить или исправить персональные данные Субъекта, он имеет право заявить в письменной форме Оператору о своем несогласии с соответствующим обоснованием такого несогласия. При отклонении Оператором указанного обращения (несогласия) Субъект имеет право обжаловать действия Оператора в порядке, предусмотренном законодательством Российской Федерации.

5.2.6.Получать сведения об Администрации, о месте её нахождения, о наличии у Администрации персональных данных, относящихся к соответствующему Субъекту.

5.2.7.Получать информацию, касающуюся обработки его персональных данных, в том числе содержащую:

подтверждение факта обработки персональных данных Администрации, а также цель такой обработки;

способы обработки персональных данных, применяемые Оператором;

сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

перечень обрабатываемых персональных данных и источник их получения;

сроки обработки персональных данных, в том числе сроки их хранения;

сведения о том, какие юридические последствия для него может повлечь за собой обработка его персональных данных.

5.2.8. Обжаловать в судебном порядке любые неправомерные действия или бездействия Администрации при обработке и защите персональных данных.

5.3. Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении Субъекта или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных пунктом 5.4 настоящего Положения.

5.4. Решение, порождающее юридические последствия в отношении Субъекта или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия Субъекта в письменной форме (ПРИЛОЖЕНИЕ 6 к настоящему Положению) или в случаях, предусмотренных федеральными законами.

5.5. Администрация обязана разъяснить Субъекту порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты своих прав и законных интересов (приложение 7 к настоящему Положению).

5.6.Администрация обязана рассмотреть возражение Субъекта в течение семи рабочих дней со дня его получения и уведомить его о результатах рассмотрения такого возражения.

5.7.Если обязанность предоставления персональных данных Субъектом установлена федеральным законом (включая налоговое, трудовое право), администрация обязана разъяснить Субъекту юридические последствия отказа предоставить свои персональные данные.

5.8. Если персональные данные были получены не от Субъекта (за исключением случаев, если персональные данные были предоставлены Администрации на основании федерального закона или если персональные данные являются общедоступными), Администрация до начала обработки таких персональных данных обязана предоставить Субъекту следующую информацию (приложение 8 к настоящему Положению):

1) наименование (фамилия, имя, отчество) и адрес Оператора или его представителя;

2) цель обработки персональных данных и ее правовое основание;

3) предполагаемые пользователи персональных данных;

4) права Субъекта в области защиты персональных данных.

5.9. Администрация обязана безвозмездно предоставить Субъекту возможность ознакомления с персональными данными, относящимися к соответствующему Субъекту, а также внести в них необходимые изменения, уничтожить или блокировать соответствующие персональные данные по предоставлении Субъектом сведений, подтверждающих, что персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах Оператор обязан в срок не превышающий 3 дней уведомить соответствующего Субъекта персональных данных и третьих лиц, которым персональные данные этого Субъекта были переданы (ПРИЛОЖЕНИЕ 9 к настоящему Положению).

Администрация обязана сообщить в уполномоченный орган по защите прав Субъектов по его запросу информацию, необходимую для осуществления деятельности указанного органа, в установленные нормативно-правовыми актами Российской Федерации сроки.

5.10. В случаях выявления недостоверных персональных данных или неправомерных действий с ними Администрация обязана осуществить блокирование персональных данных, относящихся к соответствующему Субъекту, с момента получения такой информации на период проверки. В случаях подтверждения факта недостоверности персональных данных Администрация на основании соответствующих документов обязана уточнить персональные данные и снять их блокирование.

5.11. В случаях выявления неправомерных действий с персональными данными Администрация в срок, не превышающий трех рабочих дней с даты такого выявления, обязана устранить допущенные нарушения. В случаях невозможности устранения допущенных нарушений Администрация в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, обязана уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных Администрация обязана уведомить Субъекта или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав Субъектов, - также указанный орган (ПРИЛОЖЕНИЕ 9 к настоящему Положению).

5.12.В случаях достижения цели обработки персональных данных Администрация обязана незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами, и уведомить об этом субъекта персональных данных (ПРИЛОЖЕНИЕ 9 к настоящему Положению).

5.13.В случаях отзыва Субъектом согласия на обработку своих персональных данных (ПРИЛОЖЕНИЕ 10 к настоящему Положению) Администрация обязана прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением сторон и (или) федеральным законом. Об уничтожении персональных данных Оператор в срок не превышающий 3 дней обязан уведомить Субъекта персональных данных (ПРИЛОЖЕНИЕ 9 к настоящему Положению).

5.14.До начала обработки персональных данных Администрация обязана уведомить уполномоченный орган по защите прав Субъектов о своем намерении осуществлять обработку персональных данных, за исключением случаев обработки персональных данных:

относящихся к Субъектам, которых связывают с Администрацией трудовые отношения;

полученных Администрацией в связи с заключением договора, стороной которого является Субъект, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия Субъекта и используются Администрацией исключительно для исполнения указанного договора и заключения договоров с Субъектом;

относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующим общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме Субъектов;

являющиеся общедоступными персональными данными;

включающих в себя только фамилии, имена и отчества Субъектов;

необходимых в целях однократного пропуска Субъекта на территорию, на которой находится Администрация, или в аналогичных целях;

включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус федеральных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

обрабатываемых без использования средств автоматизации в соответствии с федеральными законами и иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных.

5.15.Уведомление, указанное в п. 5.14, должно быть направлено в письменной форме и подписано уполномоченным лицом или направлено в электронной форме и подписано электронной цифровой подписью в соответствии с законодательством Российской Федерации. Уведомление должно содержать следующие сведения:

наименование, адрес Оператора;

цель обработки персональных данных;

категории персональных данных;

категории Субъектов, персональные данные которых обрабатываются;

правовое основание обработки персональных данных;

перечень действий с персональными данными, общее описание используемых Оператором способов обработки персональных данных;

описание мер, которые Оператор обязуется осуществлять при обработке персональных данных по обеспечению безопасности персональных данных при их обработке;

дата начала обработки персональных данных;

срок и условия прекращения обработки персональных данных.

6. Доступ к персональным данным Субъекта и их передачи

6.1.Внутренний доступ (доступ внутри Администрации) к персональным данным Субъектов имеют сотрудники, которым эти данные необходимы для выполнения должностных обязанностей.

6.1.1.Право доступа к персональным данным Субъекта имеют:

Глава сельского поселения;

непосредственно Субъект;

другие сотрудники Администрации, которые имеют доступ к персональным данным Субъекта с письменного согласия самого Субъекта персональных данных.

После прекращения юридических отношений с Субъектом персональных данных, его персональные данные, хранятся в Администрации в течение сроков, установленных архивным и иным законодательством РФ.

При достижении целей обработки персональных данных Субъекта персональных данных они должны быть уничтожены согласно действующим требованиям.

6.2.Внешний доступ.

6.2.1.К числу массовых потребителей персональных данных вне Администрации относятся следующие государственные и негосударственные структуры:

налоговые органы;

правоохранительные органы;

органы лицензирования и сертификации;

органы прокуратуры и ФСБ;

органы статистики;

страховые агентства;

военкоматы;

органы социального страхования;

пенсионные фонды;

6.2.2.Надзорно-контрольные органы имеют доступ к информации исключительно в сфере своей компетенции.

6.3.Внешний доступ со стороны третьих лиц к персональным данным Субъекта осуществляется с его письменного согласия за исключением случаев, когда такой доступ необходим в целях предупреждения угрозы жизни и здоровью Субъекта или других лиц, и иных случаев, установленных законодательством.

6.4.Оператор обязан сообщать персональные данные Субъекта по надлежащим оформленным запросам суда, прокуратуры и иных правоохранительных органов.

6.5.Персональные данные Субъекта могут быть предоставлены другой организации только на основании письменного запроса на бланке организации с приложением копии заявления Субъекта.

6.6.Персональные данные Субъекта могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого Субъекта.

6.7.При передаче персональных данных Администрация должна соблюдать следующие требования:

6.7.1.Не сообщать персональные данные Субъекта третьей стороне без его письменного согласия за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью Субъекта, а также в случаях, установленных федеральными законами.

6.7.2.Не сообщать персональные данные Субъекта в коммерческих целях без его письменного согласия.

6.7.3.Предупреждать лиц, получающих персональные данные Субъекта, 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, получающие персональные данные, обязаны соблюдать режим конфиденциальности. Данное положение не распространяется на обмен персональными данными в порядке, установленном федеральными законами.

6.7.4.Не запрашивать информацию о состоянии здоровья Субъекта, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.

6.7.5.Передавать персональные данные Субъекта исключительно в порядке, установленном Трудовым кодексом Российской Федерации и Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Потребители персональных данных должны подписать обязательство о неразглашении персональных данных (ПРИЛОЖЕНИЕ 11 к настоящему Положению).

6.8.Передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

6.9.Не допускается отвечать на вопросы, связанные с передачей персональной информации, по телефону.

6.10.Сведения передаются в письменной форме и должны иметь гриф конфиденциальности «Для служебного пользования» и регистрироваться соответствующим образом. В сопроводительном письме к таким документам указывается, что в прилагаемых документах содержатся персональные данные Субъектов персональных данных.

6.11.Трансграничная передача персональных данных.

6.11.1.До начала осуществления трансграничной передачи персональных данных Оператор обязан убедиться, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав Субъекта.

6.11.2.Трансграничная передача персональных данных на территории иностранных государств, обеспечивающих защиту персональных данных,

осуществляется в соответствии с ФЗ «О персональных данных» и может быть запрещена или ограничена в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства.

6.11.3.Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты персональных данных Субъектов, может осуществляться в случаях:

наличия согласия Субъекта в письменной форме;

предусмотренных международными договорами Российской Федерации об оказании правовой помощи по гражданским, семейным и уголовным делам;

предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства;

исполнения договора, стороной которого является Субъект персональных данных;

защиты жизни, здоровья, иных жизненно важных интересов Субъекта или других лиц при невозможности получения согласия в письменной форме.

7. Защита персональных данных

7.1.Комплекс мер по защите персональных данных направлен на предупреждение нарушений доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечивает безопасность информации в процессе управленческой и производственной деятельности администрации.

7.2.Защита персональных данных, обрабатываемых с использованием или без использования ЭВМ, осуществляется в соответствии с Инструкциями, утвержденными Главой сельского поселения.

7.3. Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий в соответствии с требованиями к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, требованиями к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных, установленными Правительством Российской Федерации.

7.4. Мероприятия по защите персональных данных подразделяются на внутреннюю и внешнюю защиту.

7.4.1. «Внутренняя защита» включает следующие организационно-технические мероприятия:

7.4.1.1. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководством и специалистами Администрации.

7.4.1.2. Для защиты персональных данных в Администрации применяются следующие принципы и правила:

ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют доступа к информации, содержащей персональные данные;

строгое избирательное и обоснованное распределение документов и информации между сотрудниками;

рациональное размещение рабочих мест сотрудников, при котором исключалось бы бесконтрольное использование защищаемой информации;

знание сотрудниками требований нормативно-методических документов по защите персональных данных;

наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;

определение и регламентация состава сотрудников, имеющих право доступа (входа) в помещение, в котором находится соответствующая вычислительная техника;

организация порядка уничтожения информации;

своевременное выявление нарушений требований разрешительной системы доступа сотрудниками Администрации;

воспитательная и разъяснительная работа с сотрудниками Администрации по предупреждению утраты ценных сведений при работе с конфиденциальными документами;

защита паролями доступа персональных компьютеров, на которых содержатся персональные данные.

7.4.1.3.Личные дела работников могут выдаваться на рабочие места только главе сельского поселения, и в исключительных случаях, по письменному разрешению главы Администрации, сотрудникам Администрации.

7.4.2.«Внешняя защита» включает следующие организационно-технические мероприятия:

7.4.2.1.Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией.

7.4.2.2.Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Администрации, посетители, сотрудники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе кадров, управлении бухгалтерского учета и отчетности, других подразделений, использующих персональные данные

7.4.2.3.Для защиты персональных данных соблюдается ряд мер организационно-технического характера:

порядок приема, учета и контроля деятельности посетителей;

технические средства охраны, сигнализации;

порядок охраны территории, зданий, помещений, транспортных средств;

требования к защите информации при интервьюировании и собеседованиях.

8. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

8.1.Персональная ответственность является одним из главных требований к организации функционирования системы защиты персональных данных и обязательным условием обеспечения эффективности функционирования данной системы.

8.2.Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

8.3.Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

8.4.Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных Субъекта, несут дисциплинарную, административную,

гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

8.5.Каждый сотрудник Администрации, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность полученной информации.

8.6.Должностные лица, в обязанность которых входит ведение персональных данных, обязаны обеспечить каждому Субъекту, возможность ознакомления с документами и материалами, если иное не предусмотрено законом.

Неправомерный отказ в предоставлении собранных в установленном порядке персональных данных, либо несвоевременное их предоставление в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации влечет наложение на должностных лиц административного наказания в порядке, установленном Кодексом Российской Федерации об административных правонарушениях.

8.7.В соответствии с Гражданским кодексом РФ лица, незаконными методами получившие информацию, составляющую персональные данные, обязаны возместить причиненные убытки; такая же обязанность возлагается и на работников, не обладающих правом доступа к персональным данным.

8.8.Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения влечет наложение наказания в порядке, предусмотренном Уголовным кодексом Российской Федерации.

Приложение 2 к постановлению администрации Очкинского сельского поселения «О порядке обработки персональных данных в администрации Очкинского сельского поселения»

ПОЛОЖЕНИЕ
об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных в администрации Очкинского сельского поселения

1. Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных в администрации Очкинского сельского поселения (далее – Положение) разработано на основании постановления Правительства Российской Федерации от 17 ноября 2007 года №781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

2. Настоящее Положение устанавливает требования к обеспечению безопасности персональных данных (далее – ПДн) при их обработке в информационных системах персональных данных (далее – ИСПДн) администрации Очкинского сельского поселения, представляющих собой совокупность ПДн, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПДн с использованием средств автоматизации (далее – информационные системы).

Под техническими средствами, позволяющими осуществлять обработку ПДн, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

3. Безопасность ПДн достигается путем исключения несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение,

изменение, блокирование, копирование, распространение ПДн, а также иные несанкционированные действия.

Безопасность ПДн при их обработке в информационных системах обеспечивается с помощью системы защиты ПДн, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Для обеспечения безопасности ПДн при их обработке в информационных системах осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

4. Методы и способы защиты информации в ИСПДн устанавливаются Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

Достаточность принятых мер по обеспечению безопасности ПДн при их обработке в информационных системах оценивается при проведении государственного контроля и надзора.

5. Работы по обеспечению безопасности ПДн при их обработке в информационных системах являются неотъемлемой частью работ по созданию информационных систем.

6. Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия.

7. Ответственный за выполнение работы по обеспечению безопасности ИСПДн организует разработку организационной, технической документации на ИСПДн и подготовку информационной системы к аттестации.

8. Порядок проведения классификации ИСПДн устанавливается совместно Федеральной службой по техническому и экспортному контролю, Федеральной службой безопасности Российской Федерации и Министерством информационных технологий и связи Российской Федерации.

9. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств.

10. Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с ПДн, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей ПДн и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

11. Возможные каналы утечки информации при обработке ПДн в информационных системах определяются Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

12. Пользователями ИСПДн (далее – Пользователи) являются сотрудники администрации Очкинского сельского поселения, обрабатывающие ПДн в информационной системе, отвечающие за обеспечение конфиденциальности ПДн и безопасности ПДн в информационной системе на своем рабочем месте.

13.При обработке ПДн в информационной системе ответственный за выполнение работы по обеспечению безопасности ИСПДн обеспечивает:

а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;

б) своевременное обнаружение фактов несанкционированного доступа к ПДн;

в) недопущение воздействия на технические средства автоматизированной обработки ПДн в результате которого может быть нарушено их функционирование;

г) возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

д) постоянный контроль за обеспечением уровня защищенности ПДн.

14.При обработке ПДн в информационной системе Пользователи ИСПДн обеспечивают:

а) проведение мероприятий, направленных на предотвращение передачи ПДн лицам, не имеющим права доступа к такой информации;

б) недопущение воздействия на технические средства автоматизированной обработки ПДн в результате которого может быть нарушено их функционирование;

в) своевременное обнаружение фактов несанкционированного доступа к ПДн;

г) постоянный контроль за обеспечением уровня защищенности ПДн.

14.Мероприятия по обеспечению безопасности ПДн при их обработке в информационных системах организуются и проводятся ответственным за выполнение работы по обеспечению безопасности ИСПДн и включают в себя:

а) определение угроз безопасности ПДн при их обработке, формирование на их основе модели угроз;

б) разработку на основе модели угроз системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса информационных систем;

в) проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

г) установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

д) обучение Пользователей ИСПДн, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;

ж) учет Пользователей ИСПДн, допущенных к работе с ПДн в информационной системе;

з) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

и) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей ПДн, использования средств защиты информации, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

к) описание системы защиты ПДн.

15.Сотрудники администрации Очкинского сельского поселения, доступ которых к ПДн, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим ПДн на основании списка, утвержденного Главой администрации Очкинского сельского поселения.

16.Запросы Пользователей информационной системы на получение ПДн, включая лиц, указанных в пункте 15 настоящего Положения, а также факты предоставления ПДн по этим запросам регистрируются в журнале обращений. Содержание журнала обращений периодически проверяется ответственным за выполнение работы по обеспечению безопасности ИСПДн.

17.При обнаружении нарушений порядка предоставления ПДн ответственный за выполнение работы по обеспечению безопасности ИСПДн незамедлительно приостанавливает предоставление ПДн пользователям информационной системы до выявления причин нарушений и устранения этих причин.

18.Реализация требований по обеспечению безопасности информации в средствах защиты информации возлагается на их разработчиков.

В отношении разработанных шифровальных (криптографических) средств защиты информации, предназначенных для обеспечения безопасности ПДн при их обработке в информационных системах, проводятся тематические исследования и контрольные тематические исследования в целях проверки выполнения требований по безопасности информации. При этом под тематическими исследованиями понимаются криптографические, инженерно-криптографические и специальные исследования средств защиты информации и специальные работы с техническими средствами информационных систем, а под контрольными тематическими исследованиями - периодически проводимые тематические исследования.

Конкретные сроки проведения контрольных тематических исследований определяются Федеральной службой безопасности Российской Федерации.

19.Результаты оценки соответствия и (или) тематических исследований средств защиты информации, предназначенных для обеспечения безопасности ПДн при их обработке в информационных системах, оцениваются в ходе экспертизы, осуществляемой Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

20.К средствам защиты информации, предназначенным для обеспечения безопасности ПДн при их обработке в информационных системах, прилагаются правила пользования этими средствами, согласованные с Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

Изменение условий применения средств защиты информации, предусмотренных указанными правилами, согласовывается с этими федеральными органами исполнительной власти в пределах их полномочий.

21.Средства защиты информации, предназначенные для обеспечения безопасности ПДн при их обработке в информационных системах, подлежат учету с использованием индексов или условных наименований и регистрационных номеров. Перечень индексов, условных наименований и регистрационных номеров определяется Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

22.Особенности разработки, производства, реализации и эксплуатации шифровальных (криптографических) средств защиты информации и предоставления услуг по шифрованию ПДн при их обработке в информационных системах устанавливаются Федеральной службой безопасности Российской Федерации.

Приложение 3 к постановлению администрации Очкинского сельского поселения «О порядке обработки персональных данных в администрации Очкинского сельского поселения»

Инструкция администратора безопасности ИСПДн, пользователей ИСПДн по обеспечению безопасности информации при обработке персональных данных в администрации Очкинского сельского поселения

1. Общие положения

1.1. Инструкция администратора безопасности ИСПДн, пользователей ИСПДн по обеспечению безопасности информации при обработке персональных данных в администрации Очкинского сельского поселения (далее – Инструкция) разработана в соответствии с типовой инструкцией, одобренной решением Межведомственной комиссии по защите государственной тайны от 9 октября 2009 года № 172.

1.2. В настоящей Инструкции используются следующие основные понятия:

Автоматизированная система (АС) – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций. АС может состоять из одного либо нескольких автоматизированных рабочих мест (АРМ);

Администратор безопасности информационных систем персональных данных (Администратор безопасности ИСПДн) – технический специалист, ответственный за выполнение работ по обеспечению безопасности персональных данных при их обработке в ИСПДн, содержащих информационные системы персональных данных;

Аттестация объектов информатизации – комплексная проверка (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации с целью оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности информации;

Безопасность информации – состояние защищенности информации, обрабатываемой средствами вычислительной техники и средствами автоматизации от внутренних и внешних угроз;

Вспомогательные технические средства и системы (ВТСС) - технические средства и системы, не предназначенные для передачи, обработки и хранения информации, содержащей персональные данные, устанавливаемые совместно с основными техническими средствами;

Доступ к информации (доступ) – ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации;

Защита информации - деятельность по предотвращению утечки защищаемой информации, несанкционированных, преднамеренных и непреднамеренных воздействий на защищаемую информацию, в том числе на персональные данные;

Информационные ресурсы - отдельные документы и отдельные массивы документов, документы и массивы документов, содержащиеся в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах), а также машинные носители информации (жёсткие магнитные диски, гибкие магнитные диски, оптические диски и т.п.);

Информационные системы персональных данных (ИСПДн) - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

Контролируемая зона (КЗ) - пространство (территория, здание, часть здания и т.п.), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или временного пропуска;

Мероприятия по защите информации - совокупность действий, направленных на разработку и/или практическое применение методов, способов и средств защиты информации;

Несанкционированный доступ к информации (НСД) - доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами;

Носитель информации - физическое лицо или материальный объект, в том числе физические поля, в которых информация находит своё отображение в виде символов, образов, сигналов, технических решений, процессов и количественных характеристик физических величин;

Объект информатизации - совокупность информационных ресурсов, основных технических средств и систем обработки информации, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, средств), в которых они установлены;

Обработка информации - совокупность операций сбора, накопления, ввода-вывода, приема-передачи, записи, хранения, регистрации, уничтожения, преобразования и отображения, осуществляемых над информацией;

Объект защиты информации - информация, носитель информации или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации;

Организационно-технические мероприятия по обеспечению защиты информации - совокупность действий, направленных на применение организационных мер и программно-технических способов защиты информации, на объекте информатизации;

Основные технические средства и системы (ОТСС) технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи информации, содержащей персональные данные;

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

Пользователь ИСПДн – сотрудник администрации Очкинского сельского поселения, работающий в АС администрации, обрабатывающий и пользующийся информацией (персональными данными), полученной от её собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации;

Пользователь АС - сотрудник администрации Очкинского сельского поселения, работающий в АС администрации. Пользователь АС может не иметь допуска к работе в ИСПДн администрации;

Режимное помещение - помещение, в котором располагается АС, содержащая ИСПД и/или хранятся в нерабочее время носители сведений, составляющие конфиденциальную информацию, и обеспечивается сохранность указанных сведений;

Система защиты информации ИСПДн - совокупность технических, программных и программно-технических средств защиты информации и средств контроля эффективности защиты информации;

Средства вычислительной техники (СВТ) - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем;

Средства защиты информации (СЗИ) - технические, криптографические, программные и другие средства, предназначенные для защиты информации в ИСПДн, в которых они реализованы, также средства контроля эффективности защиты информации.

Положения настоящей Инструкции распространяются на АС администрации Очкинского сельского поселения в целом и входящие в её состав ИСПДн.

Должностные обязанности администратора безопасности ИСПДн распространяются так же и на работу в АС в целом.

1.3.Инструкция определяет обязанности должностных лиц, а также требования к содержанию и порядку осуществления мероприятий по обеспечению защиты информации в АС, применительно к следующим категориям сотрудников:

специалисты администрации Очкинского сельского поселения, ведущие обработку ПДн в ИСПДн;

пользователи ИСПДн.

1.4. Инструкция устанавливает единый порядок и основные требования к защите информации при подготовке к обработке и при обработке информации в ИСПДн администрации Очкинского сельского поселения (далее **–** Администрация).

1.5.Ознакомиться с настоящей Инструкцией в полном объёме обязаны все должностные лица Администрации и пользователи ИСПДн.

1.5.1.Ознакомление с настоящей Инструкцией, в полном объеме, необходимо всем должностным лицам и пользователям ИСПДн Администрации для понимания своей роли и места в системе защиты конфиденциальной информации, в т.ч. персональных данных при работе в ИСПДн администрации Очкинского сельского поселения.

1.6.Обработка информации в ИСПДн осуществляется на аттестованной по требованиям безопасности информации АС, реализующей заданную технологию обработки информации. Опытную эксплуатацию ИСПДн допускается осуществлять без проведения аттестации, но с обязательным выполнением мероприятий по обеспечению защиты информации, изложенных в настоящей инструкции.

1.7.Основные мероприятия по обеспечению защиты в ИСПДн, проводятся в соответствии с Нормативно-методическим документом «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)» (Гостехкомиссия России, 2002), «Положением о методах и способах защиты информации в информационных системах персональных данных», утвержденных Федеральной службой по техническому и экспортному контролю (Гостехкомиссия России) Приказом от 5 февраля 2010 года №58.

1.8.Ответственность за обеспечение безопасности персональных данных при её обработке в ИСПДн Администрации, возлагается на специалиста по делопроизводству, организационной и кадровой работе (далее - специалист).

1.9. Ответственными за осуществление мероприятий по защите информации в ИСПДн, при её обработке в Администрации назначаются следующие должностные лица:

специалист по делопроизводству, организационной и кадровой работе администрации (далее - администратор безопасности);

1.10.Должностные лица, допустившие нарушения требований руководящих и нормативных документов по вопросам защиты (обеспечения безопасности)

информации в ИСПДн, привлекаются к дисциплинарной, административной или уголовной ответственности в соответствии с законодательством Российской Федерации.

1.11.По фактам и попыткам несанкционированного доступа к информации в ИСПДн, а также случаям утечки обрабатываемой с использованием СВТ информации, должны проводиться служебные расследования. До завершения служебного расследования обработка информации в АС запрещается.

1.12.В случае невозможности приостановки обработки информации в АС, при возникновении указанных в п.1.11. инцидентов, администратор безопасности ИСПДн обязан предпринять все необходимые мероприятия, в рамках своей компетенции, по обеспечению сохранности регистрационной информации в АС и обеспечению безопасной обработки ПДн.

1.13. При невозможности своими силами провести расследование указанных в п.1.11. инцидентов, администратор безопасности ИСПДн обязан поставить об этом в известность главу в администрации района.

2. Требования к содержанию и порядку осуществления мероприятий по защите (обеспечению безопасности) информации в ИСПДн администрации Очкинского сельского поселения

2.1.Организацию подготовки АС, предназначенной для обработки информации в ИСПДн, к аттестации по требованиям безопасности информации осуществляет администратор безопасности ИСПДн.

2.2.Состав программного обеспечения, технических средств и средств автоматизации, предназначенных для обработки информации в ИСПДн, должен соответствовать номенклатуре, объёму и сложности задач, решаемых с использованием СВТ, а также в соответствии с классом ИСПДн. Соответствие классу ИСПДн должно подтверждаться сертификатами ФСТЭК России – средства защиты информации (за исключением криптографических средств защиты информации) и ФСБ России – криптографические средства защиты информации, на программное и аппаратное обеспечение, участвующее в обработке персональных данных.

2.3.В состав программного обеспечения АС, предназначенной для обработки информации в ИСПДн, помимо общего (операционные системы, текстовые и графические редакторы, средства архивации данных, средства доступа к файловой системе, средства мультимедиа и др.) и специального (прикладного) программного обеспечения обязательно включается сертифицированный по требованиям безопасности информации антивирусный программный продукт.

2.4.Из состава технических средств и систем АС, предназначенных для обработки информации в ИСПДн должны быть исключены (заблокированы) избыточные элементы и, в первую очередь, устройства ввода/вывода информации на внешние носители.

2.5.Размещение и монтаж ОТСС, предназначенных для отображения и создания копий документов на бумажных носителях (видеотерминалов, печатающих устройств, графопостроителей и т.п.) необходимо проводить с учётом максимального затруднения визуального просмотра информации посторонними лицами (шторы и/или жалюзи на окнах, непрозрачные экраны и т.п.).

2.6.АС, предназначенные для обработки информации в ИСПДн класса 1 и 2, должны пройти оценку соответствия требованиям по защите информации (аттестацию).

2.7.На АС, содержащих ИСПДн класса 3, в соответствии с «Положением о методах и способах защиты информации в информационных системах персональных данных», утвержденного приказом Федеральной службой по техническому и экспортному контролю от 5 февраля 2010 года №58 должны быть проведены соответствующие мероприятия по защите информации и утверждена Декларация соответствия АС требованиям безопасности (далее Декларация) (ПРИЛОЖЕНИЕ 1 к настоящей Инструкции). Декларацию утверждает комиссия по приведению объекта информатизации «Администрация Очкинского сельского поселения» и входящих в его

состав информационных систем персональных данных в соответствие с требованиями Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных» (далее - Комиссия по безопасности информации).

2.8.Защита информации в ИСПДн, обрабатываемой с использованием АС, должна осуществляться посредством выполнения комплекса мероприятий по предотвращению утечки информации за счёт несанкционированного доступа к ней, а также по предупреждению преднамеренных программно-технических воздействий на информацию с целью нарушения её конфиденциальности и доступности в процессе её обработки, передачи и хранения.

2.9.Отладочные и экспериментальные работы (опробование программ, формирование массивов информации и др.) проводятся до ввода автоматизированной системы в эксплуатацию под руководством администратора безопасности ИСПДн.

2.10. Все СЗИ, применяемые для защиты информации в ИСПДн, должны иметь сертификаты соответствия по требованиям безопасности информации, а эффективность применяемых технических и/или организационных решений, направленных на обеспечение конфиденциальности, целостности и доступности информации, должна быть подтверждена результатами аттестационных испытаний АС.

2.11. Технические и организационные решения для конкретной информационной технологии разрабатываются организацией, имеющей соответствующие лицензии органа, уполномоченного на ведение лицензионной деятельности.

2.12. При проведении технического обслуживания и ремонта СВТ непосредственно на объекте информатизации допуск сотрудников сервисных (ремонтных) организаций осуществляется в установленном порядке при наличии у них соответствующей лицензии и предписания на осуществление работ (услуг). Сотрудники сервисных (ремонтных) организаций до начала работ должны дать подписку о неразглашении сведений конфиденциального характера, ставшим им известных в ходе выполнения работ (ПРИЛОЖЕНИЕ 2 к настоящей Инструкции).

2.12.1. Порядок допуска сотрудников сервисных (ремонтных) организаций к производству работ определяется «Инструкцией администратору безопасности ИСПДн по организации технических (регламентных) работ в АС администрации» (ПРИЛОЖЕНИЕ 3 к настоящей Инструкции).

2.13.При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям любые узлы и блоки с элементами накопления и хранения информации, входящие в состав АС администрации, в том числе и не содержащие ПДн. Вышедшие из строя элементы и блоки СВТ заменяются на элементы и блоки согласно акту (ПРИЛОЖЕНИЕ 4 к настоящей Инструкции), с внесением их технических характеристик и учетных номеров в технический паспорт АС, при необходимости проводится переаттестация АС по требованиям безопасности информации.

2.13.1.Необходимость проведения переаттестации АС определяется «Инструкцией по проведению оценки соответствия АС после проведения технических (регламентных) работ» (ПРИЛОЖЕНИЕ 5 к настоящей Инструкции).

2.14.Допуск пользователей ИСПДн к работе на аттестованной по требованиям безопасности информации АС осуществляется после ввода её в эксплуатацию распоряжением Администрации и назначения лиц, ответственных за эксплуатацию АС.

2.14.1.Режим работы в ИСПДн АС до аттестации на соответствие требованиям по безопасности информации и ввода её в эксплуатацию в установленном порядке, определяется как режим опытной эксплуатации ИСПДн и должен осуществляться с соблюдением требований по безопасности информации согласно «Инструкции администратора безопасности ИСПДн администрации по проведению опытной эксплуатации ИСПДн АС» (ПРИЛОЖЕНИЕ 6 к настоящей Инструкции).

2.15. Контроль допуска к автоматизированной обработке информации осуществляет администратор безопасности ИСПДн, согласно «Инструкции администратора безопасности ИСПДн администрации по контролю допуска пользователей к автоматизированной обработке информации в ИСПДн администрации» (ПРИЛОЖЕНИЕ 7 к настоящей Инструкции), с регистрацией в «Журнале учета лиц, допущенных к работе с персональными данными в ИСПДн».

2.16. После решения задач с использованием АС вся информация в ИСПДн, не предназначенная для дальнейшего использования, должна быть стёрта со всех машинных носителей информации с оформлением соответствующего акта (ПРИЛОЖЕНИЕ 8 к настоящей Инструкции). Стирание информации должно производиться либо специальными программами, сертифицированными по требованиям безопасности информации, либо средствами, входящими в состав сертифицированных средств защиты информации, обеспечивающими невозможность восстановления и просмотра информации с помощью любых программных средств, на штатном оборудовании аттестованной по требованиям безопасности информации АС. 2.17. При эксплуатации АС, предназначенной для обработки информации в ИСПДн, пользователям ИСПДн запрещается:

проводить обработку информации без наличия специального допуска;

подключать к АС неучтенные СВТ (ноутбуки, ЭВМ, мониторы, принтеры, коммутационное оборудование);

проводить обработку информации с нарушением технологии её обработки и с отступлением от должностных инструкций;

проводить обработку информации без выполнения обязательных мероприятий по её защите в пределах своих должностных инструкций;

вносить изменения в состав, конструкцию, конфигурацию и размещение технических средств;

вносить изменения в состав программного обеспечения, структуру файловой системы АС;

осуществлять попытки несанкционированного доступа к резервам информационной системы и других пользователей;

подключать АС к информационным сетям общего пользования и другим АС;

отключать (блокировать) средства защиты информации АС;

использовать неисправные машинные носители информации для её хранения и обработки;

производить запуск АС с системных дискет или загрузочных CD дисков и флэш - накопителей;

пользоваться неучтенными специальным образом съемными электронными носителями информации;

сообщать свои идентификационные и авторизационные данные третьим лицам;

проводить обработку информации без контроля и ограничения физического и визуального допуска к ней третьих лиц, не допущенных к её обработке;

разглашать сведения о реализованном в АС комплексе средств защиты информации;

накапливать на машинных носителях информации данные, надобность в которых миновала;

хранить машинные носители информации вблизи сильных источников электромагнитных излучений;

оставлять АС при выходе из помещения, в котором она установлена, не убедившись, что она заблокирована средствами защиты или отключена.

2.18.При внесении изменений в состав программного обеспечения, структуру файловой системы АС, содержащей ИСПД класса 3, необходимо провести дополнительные мероприятия по защите информации, внести изменения в Декларацию и утвердить ее повторно Комиссией по безопасности информации.

2.19.При внесении изменений в состав программного обеспечения, структуру файловой системы АС, содержащей ИСПД класса 1 и 2, специалистами организаций, имеющих соответствующие лицензии проводится переаттестация АС.

3. Должностные обязанности сотрудников администрации Очкинского сельского поселения, ответственных за осуществление мероприятий по обеспечению защиты информации в ИСПДн

3.1.Администратор безопасности ИСПДн отвечает за соблюдение на объекте информатизации требований по обеспечению безопасности информации и правильность применения средств защиты информации от НСД.

В обязанности Администратора безопасности ИСПДн входит:

осуществление контроля за выполнением требований по защите ПДн согласно «Инструкции о проведении контроля за выполнением требований по защите ПДн» (ПРИЛОЖЕНИЕ 9 к настоящей Инструкции);

разработка предложений по составу общесистемных программных средств, обеспечивающих функционирование АС, подлежащей аттестации по требованиям безопасности информации;

разработка и поддержка в актуальном состоянии матрицы доступа пользователей к защищаемым информационным ресурсам ИСПДн, подлежащей аттестации по требованиям безопасности информации (ПРИЛОЖЕНИЕ 10 к настоящей Инструкции);

определение класса ИСПДн, подлежащей аттестации по требованиям безопасности информации, от НСД (ПРИЛОЖЕНИЕ 11 к настоящей Инструкции);

составление и представление на утверждение Главе администрации списка сотрудников, доступ которых к персональным данным, обрабатываемым в ИСПДн, необходим для выполнения служебных (трудовых) обязанностей;

осуществление контроля за ведением «Журнала учета лиц, допущенных к работе с персональными данными в ИСПДн»;

участие и контроль за проведением аттестационных испытаний АС;

знание способов, методов и средств защиты информации в ИСПДн от НСД, знание перечня задач, решаемых с использованием АС и пользователей ИСПДн, допущенных к их решению;

осуществление допуска пользователей к техническим средствам АС и информации в соответствии с разрешительной системой доступа;

ежегодно проведение занятий, доведение до пользователей ИСПДн основных положений нормативных, правовых и руководящих документов по вопросам защиты (обеспечения безопасности) информации в ИСПДн;

проведение разбирательств по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных;

осуществление контроля за своевременным представлением списков пользователей, допускаемых к защищаемым ресурсам АС, с целью закрепления за ними паролей, а также прав пользования ресурсами СВТ;

ведение учёта, хранения, закрепления и выдачи паролей доступа к техническим средствам и информационным ресурсам АС согласно «Инструкции по организации парольной защиты» (ПРИЛОЖЕНИЕ 12 к настоящей инструкции);

обеспечение смены и ввода пароля разграничения доступа к информационным ресурсам пользователей ИСПДн с периодичностью не реже одного раза в квартал;

периодически, не реже двух раз в год, тестирование всех функции системы разграничения доступа к информации, обрабатываемой с использованием АС;

планирование мероприятий по обеспечению защиты (обеспечению безопасности) информации в ИСПДн;

планирование и проведение внутренних проверок режима защиты информации;

осуществление визуального контроля целостности компонентов СВТ, а также целостность элементов контроля НСД (наклеек, пломб, защитных знаков) к внутренним узлам и блокам СВТ;

организация проверок АС на наличие компьютерных «вирусов» согласно «Инструкции по антивирусной защите АС» (ПРИЛОЖЕНИЕ 13 к настоящей Инструкции);

своевременное обновление базы антивирусных программ;

организация докладов Главе администрации о нарушениях или невыполнении пользователями ИСПДн требований по защите (обеспечению безопасности) информации и правил обращения со съёмными машинными носителями информации;

разработка (уточнение) настоящей Инструкции и обеспечение её выполнения;

приостановка предоставления персональных данных пользователям информационной системы при обнаружении нарушений порядка их предоставления;

регулярное создание резервных копий системных файлов и обрабатываемых данных, подлежащих хранению, на специально учтённых в режимном помещении съёмных машинных носителях информации, согласно «Инструкции по резервному копирования и хранению информации в АС» (ПРИЛОЖЕНИЕ 14 к настоящей Инструкции);

поддержка в актуальном состоянии технической документацию на АС и ИСПДн.

3.2. Глава администрации отвечает за соблюдение на объекте информатизации требований по обеспечению безопасности информации, а также составляют списки пользователей ИСПДн, допущенных к обработке ПД на АС и представляют их на согласование администратору безопасности ИСПДн;

3.3.Пользователь ИСПДн отвечает за техническое состояние АС, установленный порядок использования программного обеспечения, а также применение технических и программных СЗИ.

Он обязан:

знать перечень задач, решаемых с использованием аттестованных по требованиям безопасности информации АС, сроки их выполнения;

вести учёт аттестованных по требованиям безопасности информации объектов информатизации, СВТ и оргтехники, имеющих предписания на эксплуатацию, находящихся на его рабочем месте;

знать требования руководящих документов по защите (обеспечению безопасности) информации и Инструкции;

осуществлять работы с использованием АС только после получения разрешения администратора безопасности ИСПДн на автоматизированную обработку информации;

соблюдать утверждённую матрицу доступа пользователей к защищаемым информационным ресурсам ИСПДн, обрабатываемой с использованием АС;

осуществлять визуальный контроль целостности компонентов АС, а также целостность элементов контроля НСД (наклеек, пломб, защитных знаков) к внутренним узлам и блокам СВТ;

докладывать администратору безопасности ИСПДн о выявленных изменениях в конфигурации технических средств и программного обеспечения АС;

немедленно докладывать и информировать Главу администрации Очкинского сельского поселения о фактах и попытках НСД к обрабатываемой (хранящейся) в АС информации

Приложение 3 к постановлении администрации Очкинского сельского поселения «О порядке обработки персональных данных в администрации Очкинского сельского поселения»

ПЛАН МЕРОПРИЯТИЙ
по защите персональных данных в информационных системах персональных данных администрации Очкинского сельского поселения

№ п\п	Наименование мероприятия	Срок выполнения	Ответственный за выполнение	Примечание
1.	Оформление правового основания обработки персональных данных (ПДн)	При вводе информационной системы персональных данных (ИСПДн) в эксплуатацию	Глава сельского поселения	При создании ИСПДн необходимо оформить приказ о вводе ее в эксплуатацию. Приказ оформляется руководителем организации.
2.	Направление в уполномоченный орган (Роскомнадзор) уведомления о своем намерении осуществлять обработку ПДн с использованием средств автоматизации	При необходимости	Глава сельского поселения	Уведомление направляется при вводе в эксплуатацию новых информационных систем персональных данных, либо при внесении изменений в существующие
3.	Документальное регламентирование работы с ПДн	При необходимости	Глава сельского поселения	Разработка положения по обработке и защите персональных данных, регламента специалиста ответственного за безопасность персональных данных, либо внесение изменений в существующие
4.	Получение письменного согласия субъектов ПДн (физических лиц)	Постоянно	Сотрудники администрации Очкинского сельского	Письменное согласие получается при передаче ПДн субъектами для

	на обработку ПДн в случаях, когда этого требует законодательство		поселения	обработки в ИСПДн, либо для обработки без использования средств автоматизации. Форма согласия приведена в Положении об обработке и защите ПДн.
5.	Пересмотр договора с субъектами ПДн в части обработки ПДн	При необходимости	Глава сельского поселения	Пересмотр договоров проводится при необходимости и оставляется на усмотрение организации – оператора ПДн
6.	Установка сроков обработки ПДн и процедуры их уничтожения по окончании срока обработки	При необходимости	Глава сельского поселения	Для каждой ИСПДн организацией - оператором ПДн должны быть установлены сроки обработки ПДн, что должно быть документально подтверждено в паспорте на ИСПДн. При пересмотре сроков – необходимые изменения должны быть внесены в паспорт ИСПДн
7.	Ограничение доступа работников к ПДн	При необходимости (при создании ИСПДн)	Глава сельского поселения	В случае создания ИСПДн, а также приведения имеющихся ИСПДн в соответствии с требованиями закона необходимо разграничить доступ к ПДн сотрудников организации согласно матрице доступа(сотрудники наделяются минимальными полномочиями доступа, необходимыми для выполнения ими своих обязанностей, например, могут иметь права только на просмотр ПДн) Матрица доступа утверждается руководителем организации. При необходимости пересматривается (увольнение, прием новых сотрудников и прочее), подшивается в паспорт

				ИСПДн
8.	Повышение квалификации сотрудников в области защиты ПДн	Постоянно	Глава сельского поселения	Ответственных за выполнение работ – не менее раз в два года, повышение осведомленности сотрудников – постоянно
9.	Инвентаризация информационных ресурсов с целью выявления присутствия и обработки в них ПДн	Раз в полгода	Глава сельского поселения	
10.	Классификация ИСПД	При необходимости	Глава сельского поселения	Классификация проводится при создании ИСПДн, при выявлении в информационных системах ПДн, при изменении состава, структуры самой ИСПДн или технических особенностей ее построения
11.	Выявление угроз безопасности и разработка моделей угроз и нарушителя	При необходимости	Глава сельского поселения	Разрабатывается при создании системы защиты ИСПДн
12.	Аттестация (сертификация) средств защиты ПДн или декларирование соответствия по требованиям безопасности ПДн	При необходимости	Глава сельского поселения	Проводится совместно с лицензиатами ФСТЭК
13.	Эксплуатация ИСПД и контроль безопасности ПДн	Постоянно	Глава сельского поселения	

Приложение 4 к постановлению администрации Очкинского сельского поселения «О порядке обработки персональных данных в администрации Очкинского сельского поселения»

План внутренних проверок режима защиты персональных данных в администрации Очкинского сельского поселения

Мероприятие	Периодичность	Исполнитель
Контроль за соблюдением режима обработки персональных данных, в т.ч. технологий обработки, соблюдения должностных инструкций.	Еженедельно	Глава сельского поселения
Контроль за реализацией режима защиты персональных данных использующимися программно-техническими средствами защиты информации, в т.ч. средствами защиты от несанкционированного доступа, межсетевыми экранами, средствами криптографической защиты информации, антивирусными средствами	Ежедневно	Глава сельского поселения
Контроль за соблюдением режима защиты при подключении к сетям общего пользования и (или) международного обмена	Еженедельно	Глава сельского поселения
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты персональных данных	Ежемесячно	Глава сельского поселения
Контроль за обновлениями программного обеспечения и единообразия применяемого программного обеспечения на всех элементах информационных систем персональных данных	Еженедельно	Глава сельского поселения
Контроль за обеспечением резервного копирования	Еженедельно	Глава сельского поселения
Организация анализа и пересмотра имеющихся угроз безопасности персональных данных, а так же предсказание появления новых, еще неизвестных угроз	Ежеквартально	Глава сельского поселения
Поддержание в актуальном состоянии нормативно-организационных документов	Ежемесячно	Глава сельского поселения
Контроль за разработкой и	Ежемесячно	Глава сельского поселения

внесением изменений в программное обеспечение собственной разработки или штатное программное обеспечение специально дорабатываемое собственными разработчиками или сторонними организациями.		

План внутренних проверок режима защиты персональных данных, содержит перечень внутренних проверок режима защиты персональных данных.

План внутренних проверок распространяется на все информационные системы персональных данных администрации Очкинского сельского поселения.

ПРИЛОЖЕНИЕ 1
к Положению о порядке обработки
персональных данных в администрации
Очкинского сельского поселения

Согласие Субъекта персональных данных на включение информации о его персональных данных в

_____.
(справочник, каталог и др. общедоступные источники)

Я, субъект персональных данных: _____ (Ф.И.О. полностью), основной документ, удостоверяющий личность: _____ (наименование, серия, номер, дата выдачи, выдавший орган), зарегистрированного(-ой) по адресу: _____, в лице представителя субъекта персональных данных (заполняется в случае получения согласия от представителя субъекта персональных данных) _____ (Ф.И.О. полностью), основной документ, удостоверяющий личность: _____ (наименование, серия, номер, дата выдачи, выдавший орган), зарегистрированный(-ая) по адресу: _____, _____ (реквизиты доверенности или иного документа, подтверждающего полномочия представителя), в соответствии со ст. 9 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" даю конкретное, предметное, информированное, сознательное и однозначное согласие на обработку своих персональных данных _____ (наименование или Ф.И.О., ИНН и (или) ОГРН (ОГРНИП) оператора) (далее - оператор), находящемуся по адресу: _____ (адрес оператора), с целью включения в корпоративный справочник _____
следующей информации, содержащей мои персональные данные:

Перечень моих персональных данных, на обработку которых я даю согласие: фамилия, имя, отчество, гражданство, пол, возраст, дата и место рождения, номер основного документа, удостоверяющего личность, сведения о дате выдачи указанного документа и выдавшем его органе, адрес регистрации по месту жительства, адрес фактического проживания, идентификационный номер налогоплательщика, страховой номер индивидуального лицевого счета, номер телефона, адрес электронной почты, _____ (иные данные).

Разрешаю оператору производить автоматизированную, а также осуществляемую без использования средств автоматизации обработку моих персональных данных, а именно: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

Лицо, осуществляющее обработку персональных данных по поручению оператора (если обработка будет поручена такому лицу): _____ (наименование или Ф.И.О., ИНН и (или) ОГРН (ОГРНИП)), находящееся по адресу: _____ (адрес).

Согласие действует до "__"_____ ____ г. Субъект персональных данных вправе отозвать настоящее согласие на обработку своих персональных данных, письменно уведомив об этом оператора.

Приложение:

Доверенность представителя (иные документы, подтверждающие полномочия представителя) от "__"_____ ____ г. N __ (если согласие подписывается представителем субъекта персональных данных).

Субъект персональных данных (представитель):

_____ /_____/
(подпись) (Ф.И.О.)

"__"_____ ____ г.

ПРИЛОЖЕНИЕ 2
к Положению о порядке обработки персональных данных в администрации Очкинского сельского поселения

Заявление

Я_____,
(фамилия, имя, отчество).

проживающий(ая) по адресу
_____
_____
паспорт серии ____№_____,выдан_____.

Даю согласие на обработку моих сведений о доходах, об имуществе и обязательствах имущественного характера за период с «__» января 20__ г. по 31 декабря 20__ г. и размещение на официальном Интернет-портале администрации Очкинского сельского поселения в порядке, утвержденном постановлением администрации Очкинского сельского поселения от «___» _____ г. № ____ «Об утверждении Положения о представлении гражданами, претендующими на замещение должностей муниципальной службы, и муниципальными служащими администрации Очкинского сельского поселения сведений о доходах, об имуществе и обязательствах имущественного характера» следующих сведений:

а) перечень объектов недвижимого имущества, принадлежащих мне на праве собственности или находящихся в их пользовании, с указанием вида, площади и страны расположения каждого из них;

б) перечень транспортных средств, с указанием вида и марки, принадлежащих мне на праве собственности;

в) мой годовой доход.

_____ _____ _____
дата подпись расшифровка подписи

ПРИЛОЖЕНИЕ 3
к Положению о порядке обработки персональных данных в администрации Очкинского сельского поселения

Расписка
об ознакомлении Субъекта персональных данных с «Положением о защите персональных данных в администрации Очкинского сельского поселения»

Я, _____,
(должность, Ф.И.О.)

ознакомлен (на) с «Положением о защите персональных данных в администрации Очкинского сельского поселения»

_____ _____ _____
дата подпись расшифровка подписи

ПРИЛОЖЕНИЕ 4
к Положению о порядке обработки
персональных данных в администрации
Очкинского сельского поселения

Письменное согласие Субъекта персональных данных на получение его персональных данных у третьих лиц

Я, субъект персональных данных: _____ (Ф.И.О. полностью), основной документ, удостоверяющий личность: _____ (наименование, серия, номер, дата выдачи, выдавший орган), зарегистрированного(-ой) по адресу: _____, в лице представителя субъекта персональных данных (заполняется в случае получения согласия от представителя субъекта персональных данных) _____ (Ф.И.О. полностью), основной документ, удостоверяющий личность: _____ (наименование, серия, номер, дата выдачи, выдавший орган), зарегистрированный(-ая) по адресу: _____, _____ (реквизиты доверенности или иного документа, подтверждающего полномочия представителя), в соответствии со ст. 9 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" даю конкретное, предметное, информированное, сознательное и однозначное согласие Оператором (администрация Очкинского сельского поселения) **на получение его персональных данных у третьих лиц** .

Перечень моих персональных данных, на обработку которых я даю согласие: фамилия, имя, отчество, гражданство, пол, возраст, дата и место рождения, номер основного документа, удостоверяющего личность, сведения о дате выдачи указанного документа и выдавшем его органе, адрес регистрации по месту жительства, адрес фактического проживания, идентификационный номер налогоплательщика, страховой номер индивидуального лицевого счета, номер телефона, адрес электронной почты, _____ (иные данные).

Разрешаю оператору производить автоматизированную, а также осуществляемую без использования средств автоматизации обработку моих персональных данных, а именно: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

Лицо, осуществляющее обработку персональных данных по поручению оператора (если обработка будет поручена такому лицу): _____ (наименование или Ф.И.О., ИНН и (или) ОГРН (ОГРНИП)), находящееся по адресу: _____ (адрес).

Согласие действует до "__"_____ ____ г. Субъект персональных данных вправе отозвать настоящее согласие на обработку своих персональных данных, письменно уведомив об этом оператора.

Приложение:

Доверенность представителя (иные документы, подтверждающие полномочия представителя) от "__"_____ ____ г. N __ (если согласие подписывается представителем субъекта персональных данных).

Субъект персональных данных (представитель):

_____ /_____/

(подпись) (Ф.И.О.)

"__" _____ ____ г.

ПРИЛОЖЕНИЕ 5
к Положению о порядке обработки персональных данных в администрации Очкинского сельского поселения

Уведомление

Уважаемый _____!
(Ф.И.О.)

В связи с

_____
(указать причину)

у администрации Очкинского сельского поселения возникла необходимость получения следующей информации, составляющей Ваши персональные данные:

_____
(перечислить информацию)

_____
_____.

Просим Вас предоставить указанные сведения

_____
_____
(кому)

в течение трех рабочих дней с момента получения настоящего уведомления.
В случаи невозможности предоставить указанные сведения просим в указанный срок дать письменное согласие на получение Оператором (администрацией Очкинского сельского поселения) необходимой информации из следующих источников

_____,
(указать источники)

следующими способами:

_____.
(автоматизированная обработка, иные способы)

По результатам обработки указанной информации Оператором планируется принятие следующих решений, которые будут доведены до Вашего сведения_____

_____.
(указать решения и иные юридические последствия обработки информации)

Против принятого решения Вы имеете право заявить свои письменные возражения в срок до_____.
Информируем Вас о последствиях Вашего отказа дать письменное согласие на получение оператором указанной информации

_____
(перечислить последствия)

Информируем Вас о Вашем праве в любое время отозвать свое письменное согласие на обработку персональных данных.

_____ _____ _____
дата подпись расшифровка подписи

Настоящее уведомление на руки получил:

_____ _____ _____
дата подпись расшифровка подписи

ПРИЛОЖЕНИЕ 6
к Положению о порядке обработки персональных данных в администрации Очкинского сельского поселения

СОГЛАСИЕ
на обработку персональных данных

Я, субъект персональных данных: _____ (Ф.И.О. полностью), основной документ, удостоверяющий личность: _____ (наименование, серия, номер, дата выдачи, выдавший орган), зарегистрированного(-ой) по адресу: _____, в лице представителя субъекта персональных данных (заполняется в случае получения согласия от представителя субъекта персональных данных) _____ (Ф.И.О. полностью), основной документ, удостоверяющий личность: _____ (наименование, серия, номер, дата выдачи, выдавший орган), зарегистрированный(-ая) по адресу: _____, _____ (реквизиты доверенности или иного документа, подтверждающего полномочия представителя), в соответствии со ст. 9 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" даю конкретное, предметное, информированное, сознательное и однозначное согласие на обработку своих персональных данных _____ (наименование или Ф.И.О., ИНН и (или) ОГРН (ОГРНИП) оператора) (далее - оператор), находящемуся по адресу: _____ (адрес оператора), с целью обработки персональных данных.

Перечень моих персональных данных, на обработку которых я даю согласие: фамилия, имя, отчество, гражданство, пол, возраст, дата и место рождения, номер основного документа, удостоверяющего личность, сведения о дате выдачи указанного документа и выдавшем его органе, адрес регистрации по месту жительства, адрес фактического проживания, идентификационный номер налогоплательщика, страховой номер индивидуального лицевого счета, номер телефона, адрес электронной почты, _____ (иные данные).

Разрешаю оператору производить автоматизированную, а также осуществляемую без использования средств автоматизации обработку моих персональных данных, а именно: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

Лицо, осуществляющее обработку персональных данных по поручению оператора (если обработка будет поручена такому лицу): _____ (наименование или Ф.И.О., ИНН и (или) ОГРН (ОГРНИП)), находящееся по адресу: _____ (адрес).

Согласие действует до "__"_____ ____ г. Субъект персональных данных вправе отозвать настоящее согласие на обработку своих персональных данных, письменно уведомив об этом оператора.

Приложение:

Доверенность представителя (иные документы, подтверждающие полномочия представителя) от "__"_____ ____ г. N __ (если согласие подписывается представителем субъекта персональных данных).

Субъект персональных данных (представитель):

_____ /_____/
(подпись) (Ф.И.О.)

"__"_____ ____

ПРИЛОЖЕНИЕ 7
к Положению о порядке обработки персональных данных в администрации Очкинского сельского поселения

Запрос о доступе Субъекта персональных данных к своим персональным данным

В_____.
(наименование и адрес Оператора)

От
_____
_____
_____
_____.
(Ф.И.О., номер основного документа, удостоверяющего личность Субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе)

Прошу предоставить мне для ознакомления следующую информацию (документы), составляющие мои персональные данные:
_____.
(перечислить)

_____ _____ _____
дата подпись расшифровка подписи

ПРИЛОЖЕНИЕ 8
к Положению о порядке обработки персональных данных в администрации Очкинского сельского поселения

Уведомление

Уважаемый_____!
(Ф.И.О.)

на основании _____
администрация Очкинского сельского поселения (Оператор) получила от:

_____
(наименование организации, адрес)

следующую информацию, содержащую Ваши персональные данные:

_____.
(перечислить)

Указанная информация будет обработана и использована Оператором в целях:_____
_____.

Вы имеете право на полную информацию о своих персональных данных, содержащуюся у Оператора, свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей Ваши персональные данные, за исключением случаев, предусмотренных действующим законодательством; требовать от Оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав, получать иную информацию, касающуюся обработки Ваших персональных данных.

_____ _____ _____
дата подпись расшифровка подписи

Настоящее уведомление на руки получил:

_____ _____ _____
дата подпись расшифровка подписи

ПРИЛОЖЕНИЕ 9
к Положению о порядке обработки персональных данных в администрации Очкинского сельского поселения

Уведомление

о _____
(уничтожении, изменении, прекращении обработки, устранении нарушений персональных данных)

Уважаемый _____!
(Ф.И.О.)

В связи с _____
(недостоверностью, выявлением неправомерных действий с Вашими персональными данными, достижением цели обработки, отзывом Вами согласия на обработку, другие причины) сообщаем Вам, что обработка Ваших персональных данных о

_____
_____
(перечислить)

прекращена и указанная информация подлежит уничтожению (изменению).

_____ _____ _____
дата подпись расшифровка подписи

Настоящее уведомление на руки получил:

_____ _____ _____
дата подпись расшифровка подписи

ПРИЛОЖЕНИЕ 10
к Положению о порядке обработки персональных данных в администрации Очкинского сельского поселения

[наименование (Ф. И. О.) и адрес оператора,
получившего согласие субъекта персональных данных]
[полное наименование организации (обособленного подразделения), Ф. И. О. индивидуального предпринимателя, физического лица]
ИНН/КПП [значение]
[адрес нахождения организации (обособленного подразделения)/адрес постоянного
места жительства индивидуального предпринимателя, физического лица]

Отзыв согласия на обработку персональных данных

Настоящим, в соответствии с требованиями Федерального закона "О персональных данных" от 27.07.2006 года № 152-ФЗ, в связи с [указать причину], [наименование организации (обособленного подразделения)/я] отзывает(ю) у [наименование (Ф. И. О.) оператора] свое согласие на обработку персональных данных, данное [число, месяц, год] в целях [вписать нужное].

Прошу прекратить обработку персональных данных в срок, не превышающий
трех рабочих дней с даты поступления настоящего отзыва.

[Число, месяц, год] [подпись] [Ф. И. О.]

ПРИЛОЖЕНИЕ 11
к Положению о порядке обработки персональных данных в администрации Очкинского сельского поселения

ОБЯЗАТЕЛЬСТВО.
о неразглашении конфиденциальной информации
(персональных данных)
.

Я,_____
(ФИО муниципального служащего)

исполняющий(ая) должностные обязанности по занимаемой должности

_____
_____
(должность)

предупрежден(а), что на период исполнения должностных обязанностей в соответствии с должностным регламентом, мне будет предоставлен допуск к конфиденциальной информации (персональным данным), не содержащим сведений, составляющих государственную тайну. Настоящим добровольно принимаю на себя обязательства:

1. Не разглашать третьим лицам конфиденциальные сведения, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.
2. Не передавать и не раскрывать третьим лицам конфиденциальные сведения, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.
3. В случае попытки третьих лиц получить от меня конфиденциальные сведения, сообщать непосредственному руководителю.
4. Не использовать конфиденциальные сведения с целью получения выгоды.
5. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты конфиденциальных сведений.
6. В течение года после прекращения права на допуск к конфиденциальным сведениям не разглашать и не передавать третьим лицам известные мне конфиденциальные сведения.

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

_____ _____
(фамилия, инициалы) (подпись)

«_____»_____20___г.