АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ ВЕРХНЕСТЕПНОВСКОГО СЕЛЬСОВЕТА СТЕПНОВСКОГО РАЙОНА СТАВРОПОЛЬСКОГО КРАЯ

РАСПОРЯЖЕНИЕ

21 января 2016 г. пос. Верхнестепной № 9-р

Об утверждении внутренних
нормативных правовых актов
по защите персональных данных

1. Для обеспечения безопасности персональных данных при их обработке в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края и во исполнение требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановления Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» утвердить прилагаемый перечень внутренних нормативных правовых актов:

1.1. Инструкцию системного администратора информационных систем персональных данных по обеспечению безопасности персональных данных в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края;

1.2. Инструкцию о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения и баз данных в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края;

1.3. Инструкцию ответственного за обработку персональных данных в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края;

1.4. Инструкцию по организации антивирусной защиты в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края;

1.5. Инструкцию по порядку учета и хранению документов, содержащих персональные данные в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края;

1.6. Инструкцию по обеспечению безопасности эксплуатации средств криптографической защиты информации (СКЗИ) в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края;

1.7. Инструкцию по порядку учета и хранению съемных носителей конфиденциальной информации (персональных данных) в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края;

1.8. Инструкцию пользователя информационных систем персональных данных по обеспечению безопасности персональных данных в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края;

1.9. Положение об обработке персональных данных в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края;

1.10. Порядок доступа сотрудников администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края в помещения, где ведётся обработка персональных данных;

1.11. Правила работы с обезличенными персональными данными в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края;

1.12. Регламент порядка действий сотрудников администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края, при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных;

1.13. Инструкцию осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края.

2. Управляющему делами администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края Муховской Е.И. довести до сведения всех сотрудников, обрабатывающих персональные данные, положения утверждаемых внутренних нормативных правовых актов.

3. Контроль за выполнением настоящего распоряжения оставляю за собой.

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

Глава муниципального образования
Верхнестепновского сельсовета
Степновского района
Ставропольского края Н.А.Капитонова

УТВЕРЖДЕНА
распоряжением администрации
муниципального образования
Верхнестепновского сельсовета
Степновского района
Ставропольского края
от 21 января 2016 г. № 9-р

ИНСТРУКЦИЯ
системного администратора информационных систем персональных данных по обеспечению безопасности персональных данных в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края

1. Общие положения

1.1. Настоящая Инструкция определяет обязанности, полномочия и ответственность системного администратора информационных систем персональных данных (ИСПДн) по обеспечению безопасности персональных данных в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края (далее – Администрация).

1.2. Администратор ИСПДн (далее – Администратор) назначается распоряжением Администрации.

1.3. Администратор ИСПДн подчиняется главе муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края.

1.4. Администратор ИСПДн в своей работе руководствуется настоящей Инструкцией и Положением о защите персональных данных, руководящими и нормативными документами ФСТЭК России и внутренними регламентирующими документами по защите информации в Администрации.

1.5. Администратор ИСПДн отвечает за обеспечение устойчивой работоспособности элементов ИСПДн и средств защиты, при обработке персональных данных.

2. Обязанности по обеспечению безопасности информации

Администратор ИСПДн обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Ознакомить всех пользователей ИСПДн с внутренними нормативными правовыми актами по обеспечению безопасности персональных данных (под роспись).

2.3. Обеспечивать установку, настройку и своевременное обновление элементов ИСПДн:

– программного обеспечения автоматизированных рабочих мест (далее – АРМ) и серверов (операционные системы, прикладное и специальное ПО);

– аппаратных средств;

– аппаратных и программных средств защиты.

2.4. Обеспечивать работоспособность элементов ИСПДн и локальной вычислительной сети.

2.5. Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов (если не назначен другой ответственный).

2.6. Обеспечивать функционирование и поддерживать работоспособность средств защиты.

2.7. В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.8. Осуществлять регистрацию пользователей, выдачу временных паролей пользователей, осуществлять контроль за правильностью использования пароля пользователем ИСПДн.

2.9. Обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации.

2.10. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.

2.11. Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт.

2.12. Присутствовать при выполнении технического обслуживания элементов ИСПДн сторонними физическими лицами и Компаниями.

2.13. Принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

3. Ответственность

3.1. В случае нарушения положений настоящей Инструкции Администратор несёт ответственность в соответствии с действующим законодательством.

_____

УТВЕРЖДЕНА
распоряжением администрации
муниципального образования
Верхнестепновского сельсовета
Степновского района
Ставропольского края
от 21 января 2016 г. № 9-р

ИНСТРУКЦИЯ
о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения и баз данных в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края

1. Назначение и область действия

1.1. Данная Инструкция определяет действия, связанные с мерами и средствами поддержания непрерывной работы и восстановления работоспособности информационных систем в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края (далее – Администрация).

1.2. Настоящая Инструкция регламентирует:

– меры защиты от потери информации;

– действия по восстановлению в случае потери информации.

1.3. Действие настоящей Инструкции распространяется на Администраторов информационных систем, ответственных за резервное копирование информации.

2. Меры обеспечения надежной работы и восстановления ресурсов при возникновении инцидентов

2.1. Технические меры.

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения Инцидентов, такие как:

– системы обеспечения отказоустойчивости;

– системы резервного копирования и хранения данных;

– системы контроля физического доступа.

Системы жизнеобеспечения ИСПДн включают:

– пожарные сигнализации и системы пожаротушения;

– системы вентиляции и кондиционирования;

– системы резервного питания.

Все критичные помещения (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

– локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;

– источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;

– резервные линии электропитания в пределах комплекса зданий;

Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на носитель (ленту, жесткий диск и т.п.).

2.2. Организационные меры.

2.2.1. Резервное копирование и хранение данных должно осуществлять на периодической основе:

– для обрабатываемых персональных данных – не реже раза в неделю или по требованию пользователя ИСПДн;

– для системной информации – не реже раза в месяц;

– эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн каждый раз при внесении изменений в эталонные копии (выход новых версий).

2.2.2. Данные о проведение процедуры резервного копирования должны отражаться в специально созданном Журнале учета.

2.2.3. Носители, на которые произведено резервное копирование, должны быть пронумерованы номером носителя, датой проведения резервного копирования.

2.2.4. Носители должны храниться в несгораемом шкафу или помещении, оборудованном системой пожаротушения.

2.2.5. Носители и резервные копии данных должны храниться не менее года для возможности восстановления данных.

3. Порядок проведения резервирования информации

3.1. Перед проведением процедуры резервного копирования необходимо убедиться в том, что все пользователи информационной системы завершили свою работу с информационной системой.

3.2. Резервирование информации в информационных системах персональных данных проводится при помощи штатных средств, поставляемых в составе специализированного программного обеспечения для построения информационной системы, либо, в случае отсутствия таковых, штатными средствами операционной системы или системы управления базами данных (при использовании таковой).

3.3. Все файлы, входящие в состав резервной копии, должны архивироваться в один архив с присвоением имени архива в формате время_дата (например, 18.00_21.11.2011).

3.4. Архивация может производиться как штатными средствами, поставляемыми в составе специализированного программного обеспечения для построения информационной системы, так и сторонним программным обеспечением (например, 7zip, WinRar).

3.5. Резервные копии должны сохраняться на носители, не входящие в состав технических средств информационной системы персональных данных (внешние жесткие диски, CD/DVD диски, flash диски).

3.6. После завершения процедуры резервного копирования информации и записи резервной копии на носитель, необходимо поместить носитель с резервной копией в специально отведённое для хранения место и проставить соответствующую отметку в Журнале.

4. Порядок проведения восстановления информации

4.1. Перед проведением процедуры восстановления информации необходимо убедиться в том, что все пользователи информационной системы завершили свою работу с информационной системой.

4.2. Восстановление информации следует проводить из наиболее актуальной резервной копии.

4.3. В случае, если специализированное программное обеспечение для построения информационной системы не позволяет работать с заархивированными резервными копиями, то перед восстановлением информации необходимо разархивировать файлы резервной копии при помощи стороннего программного обеспечения (например 7zip, WinRar).

4.4. Восстановление информации в информационных системах персональных данных проводится при помощи штатных средств, поставляемых в составе специализированного программного обеспечения для построения информационной системы, либо, в случае отсутствия таковых, штатными средствами операционной системы или системы управления базами данных (при использовании таковой).

4.5. После завершения процедуры восстановления необходимо убедиться в работоспособности информационной системы персональных данных.

4.6. В случае успешного восстановления оповестить пользователей информационной системы о возможности продолжения работы. В противном

случае необходимо изучить документацию, прилагаемую к программному обеспечению либо обратиться в службу технической поддержки.

5. Ответственность

5.1. Работники, нарушившие требования данной Инструкции, несут ответственность в соответствии с действующим законодательством.

УТВЕРЖДЕНА
распоряжением администрации
муниципального образования
Верхнестепновского сельсовета
Степновского района
Ставропольского края
от 21 января 2016 г. № 9-р

ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края

4. Общие положения

4.1. Настоящая Инструкция разработана в соответствии со статьей 22.1 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и определяет обязанности, полномочия и ответственность лиц, ответственных за организацию обработки персональных данных в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края (далее - Администрация).

4.2. Ответственный за организацию обработки персональных данных назначается распоряжением Администрации из числа сотрудников Администрации.

4.3. Ответственный за организацию обработки персональных данных подчиняется главе муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края.

4.4. Ответственный за организацию обработки персональных данных в своей работе руководствуется настоящей Инструкцией, Федеральными законами от 27 июля 2006 года №152-ФЗ «О персональных данных», от 27 июня 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства РФ от 15 сентября 2008 года № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемых без использовании средств автоматизации», Приказом федеральной службы по техническому и экспортному контролю России от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К) и внутренними документами Администрации по защите информации.

4.5. Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения безопасности

персональных данных и не исключает обязательного выполнения их требований.

5. Обязанности

5.1. Осуществлять внутренний контроль за соблюдением сотрудниками Администрации требований законодательства Российской Федерации при обработке персональных данных, внутренних положений, инструкций и других нормативных правовых документов в области защиты информации.

5.2. Доводить до сведения работников Администрации содержание положений законодательства Российской Федерации о персональных данных, внутренних нормативных правовых актов Администрации по вопросам обработки персональных данных, требований по защите персональных данных.

5.3. Организовать прием и обработку обращений и запросов субъектов персональных данных или их представителей и осуществлять контроль за приемом и обработкой таких обращений и запросов:

– в соответствии с Федеральным законом «О персональных данных» субъект персональных данных или его представитель имеет право на получение информации, касающейся обработки его персональных данных на основании обращения либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации;

– все обращения и запросы субъектов персональных данных подлежат обязательному учету;

– ответственный за организацию обработки обязан фиксировать все обращения и запросы в журнале учета обращений граждан (субъектов персональных данных).

5.4. Организовать прием и обработку обращений и запросов пользователей информационной системы на получение персональных данных, включая лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, а также факты предоставления персональных данных по этим запросам регистрировать в Журнале обращений.

5.5. Обеспечивать постоянный контроль выполнения установленного комплекса мероприятий по обеспечению безопасности информации пользователями информационной системы персональных.

6. Ответственность

3.1. В случае нарушения положений настоящей Инструкции ответственные за организацию обработки персональных данных лица несут ответственность в соответствии с действующим законодательством.

УТВЕРЖДЕНА
распоряжением администрации
муниципального образования
Верхнестепновского сельсовета
Степновского района
Ставропольского края
от 21 января 2016 г. № 9-р

ИНСТРУКЦИЯ
по организации антивирусной защиты в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края

1. Общие положения

1.1. Настоящая Инструкция предназначена для организации порядка проведения антивирусного контроля в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края (далее - Администрация) и предотвращения возникновения фактов заражения вредоносным программным обеспечением.

1.2. Данная Инструкция распространяется на всех пользователей и администраторов информационных систем персональных данных (далее – ИСПДн) в Администрации.

2. Установка и обновление антивирусных средств

2.1. Установка и настройка антивирусных средств осуществляются только Администратором информационной системы персональных данных.

2.2. Обновление антивирусных баз осуществляется по расписанию в автоматическом режиме, либо вручную при необходимости.

3. Требования к проведению мероприятий по антивирусной защите

3.1. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, flash дисках, CD-ROM и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

3.2. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие заражения вредоносным программным обеспечением.

3.3. Контроль информации на съёмных носителях производится непосредственно перед её использованием.

3.4. Особое внимание следует обратить на недопустимость использования съёмных носителей, принадлежащих лицам, временно

допущенным к работе на ЭВМ. Работа этих лиц должна проводиться под непосредственным контролем сотрудника или ответственного за информационную безопасность.

3.5. Ежедневно, в начале работы, должно выполняться обновление антивирусных баз и проводиться антивирусный контроль всех загружаемых в память файлов персонального компьютера.

3.6. Периодические проверки компьютеров должны проводиться не реже одного раза в неделю.

3.7. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться:

– Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка.

– При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.).

4. Действия сотрудников при обнаружении компьютерного вируса

4.1. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи обязаны:

– приостановить работу;

– немедленно поставить в известность о факте обнаружения зараженных вирусом файлов Администратора информационной системы персональных данных;

– провести лечение или уничтожение зараженных файлов.

4.2. При возникновении подозрения на наличие компьютерного вируса пользователь или Администратор информационной системы персональных данных должны провести внеочередной антивирусный контроль.

5. Ответственность при организации антивирусной защиты

5.1. Ответственность за организацию антивирусной защиты возлагается на Администратора информационной системы персональных данных.

5.2. Ответственность за выполнение требований данной Инструкции возлагается на Пользователей и Администратора информационной системы персональных данных.

5.3. Периодический контроль за соблюдением положений данной Инструкции возлагается на Администратора информационной системы персональных данных.

УТВЕРЖДЕНА
распоряжением администрации
муниципального образования
Верхнестепновского сельсовета
Степновского района
Ставропольского края
от 21 января 2016 г. № 9-р

ИНСТРУКЦИЯ
по порядку учета и хранению документов, содержащих персональные данные, в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края

1. Общие положения

1.1. Настоящая Инструкция разработана с целью обеспечения безопасности персональных данных при работе с документами, содержащими персональные данные.

1.2. Действие настоящей Инструкции распространяется на сотрудников администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края (далее – Администрация), допущенных к обработке персональных данных.

2. Порядок учета, хранения и обращения с документами, которые содержат персональные данные

2.1. Все находящиеся на хранении и в обращении документы с персональными данными в Администрации подлежат учёту.

2.2. Каждый документ, личное дело или журнал должны иметь уникальный учетный номер.

2.3. Учет и выдачу документов с персональными данными осуществляют сотрудники структурных подразделений, на которых возложены функции хранения документов, содержащих персональные данные. Факт выдачи документов фиксируется в журнале учета.

2.4. При работе с документами, которые содержат персональные данные необходимо:

2.4.1. Соблюдать требования настоящей Инструкции.

2.4.2. Использовать полученные документы исключительно для выполнения своих служебных обязанностей.

2.4.3. Ставить в известность ответственного за обработку персональных данных о любых фактах нарушения требований настоящей Инструкции.

2.4.4. Бережно относится к документам, содержащим персональные данные.

2.4.5. Обеспечивать физическую безопасность документов всеми разумными способами.

2.4.6. Обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

2.4.7. Извещать ответственного за организацию обработки персональных данных о фактах утраты (кражи) документов, содержащих персональные данные.

2.4.8. Осуществлять вынос документов с персональными данными для непосредственной передачи адресату только с письменного разрешения главы муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края.

2.4.9. При передаче персональных данных передаётся минимальный объем данных, который необходим для выполнения служебных обязанностей адресата.

2.4.10. В случае утраты или уничтожения документов, которые содержат персональные данные либо разглашении содержащихся в них сведений, немедленно ставится в известность руководитель Администрации. Отметки об утрате вносятся в журнал учета документов с персональными данными.

2.4.11. В случае увольнения или перевода работника в другое структурное подразделение, предоставленные документы с персональными данными информации изымаются.

3. Работа с журналом регистрации посетителей

3.1. Журнал регистрации посетителей необходим исключительно в целях контроля посещаемости.

3.2. В Журнале учёта посещаемости разрешается фиксация следующих персональных данных:

– Фамилия, Имя, Отчество;

– Наименование и номер документа, удостоверяющего личность (паспорт, водительское удостоверение, удостоверение личности и т.д.).

3.3. Порядок учёта, хранения и обращения с журналом регистрации посетителей осуществляется в соответствии с п. 2 настоящей инструкции.

3.4. В случае окончания журнала, его необходимо сдать в архив или уничтожить.

4. Запрещается

4.1. Использовать документы с персональными данными в личных целях.

4.2. Передавать документы с персональными данными третьим лицам без соответствующего разрешения руководителя Администрации.

4.3. Хранить документы с персональными данными вместе с документами с открытой информацией на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам.

4.4. Выносить документы с персональными данными из служебных помещений для работы с ними на дому и т. д.

4.5. Оставлять документы с персональными данными без присмотра.

4.6. Изготавливать и хранить копии паспортов или иных документов, удостоверяющих личность, за исключением случаев, предусмотренных законодательством.

5. Ответственность

5.1. Работники, нарушившие требования данной Инструкции, несут ответственность в соответствии с действующим законодательством.

УТВЕРЖДЕНА
распоряжением администрации
муниципального образования
Верхнестепновского сельсовета
Степновского района
Ставропольского края
от 21 января 2016 г. № 9-р

ИНСТРУКЦИЯ
по обеспечению безопасности эксплуатации средств криптографической защиты информации (СКЗИ) в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края

1. Общие положения

1.1. Настоящая Инструкция определяет порядок учета, хранения и использования средств криптографической защиты информации (СКЗИ) и криптографических ключей, а также порядок изготовления, смены, уничтожения и компрометации криптографических ключей в целях обеспечения безопасности эксплуатации в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края (далее – Администрация).

1.2. Пользователь должен выполнять все требования настоящей Инструкции, правила, изложенные в эксплуатационной документации на СКЗИ, а также другие документы, регламентирующие порядок работы с СКЗИ.

2. Обязанности Пользователя

2.1. Пользователь обязан соблюдать требования по обеспечению безопасности функционирования СКЗИ.

2.2. Пользователь обязан обеспечить конфиденциальность всей информации ограниченного распространения, доступной по роду выполняемых функциональных обязанностей.

2.3. Пользователь обязан сдать носители ключевой информации (далее – НКИ) при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ, ответственному за обработку персональных данных.

2.4. Пользователь обязан сдать носители ключевой информации (далее – НКИ) по окончании срока действия сертификата ключа, а также в случае компрометации ключа.

2.5. Пользователь обязан немедленно уведомлять Ответственного за обработку персональных данных о компрометации криптографических ключей.

2.6. Пользователь обязан немедленно уведомлять Ответственного за обработку персональных данных о фактах утраты или недостачи СКЗИ, НКИ.

3. Порядок обращения со средствами криптографической защиты информации

3.1. Монтаж и установка СКЗИ осуществляются только уполномоченным лицом, либо организацией, имеющей необходимые лицензии.

3.2. Все СКЗИ и НКИ должны учитываться в журнале.

3.3. Служебные помещения, в которых размещаются СКЗИ, должны оборудоваться охранной сигнализацией, по убытии сотрудников закрываться и сдаваться под охрану.

3.4. Для хранения носителей ключевой информации помещения обеспечиваются сейфами (металлическими шкафами).

3.5. Несанкционированное изготовление дубликатов ключей ЗАПРЕЩЕНО. В случае утери ключа механизм (секрет) замка (либо сам сейф) должен быть заменён.

3.6. К эксплуатации СКЗИ допускаются лица, изучившие правила пользования данным СКЗИ.

3.7. Все программное обеспечение ПЭВМ, предназначенной для установки СКЗИ, должно иметь соответствующие лицензии. Установка средств разработки и отладки программ на рабочую станцию, использующую СКЗИ, не допускается.

4. Порядок обращения с ключами ЭЦП

4.1. Криптографический ключ применяется для подписания (проверки электронной цифровой подписи) электронных документов до окончания срока его действия или наступления события, трактуемого как компрометация криптографических ключей.

4.2. Изготовление и выдача ключей ЭЦП осуществляется только Удостоверяющим центром.

4.3. Выработанные закрытые (конфиденциальные) криптографические ключи хранятся исключительно в электронном виде на цифровых носителях информации, которые получают статус НКИ.

4.4. НКИ являются объектами особой важности, т.к. они содержат информацию, предназначенную для гарантированной идентификации владельца ключа, защиты электронного документа от подделки и обеспечения конфиденциальности документа.

4.5. Владельцы ключей несут персональную ответственность за обеспечение конфиденциальности ключевой информации и защиту НКИ от несанкционированного использования.

4.6. Для хранения носителей ключевой информации Пользователь должен быть обеспечен личным сейфом.

5. Запрещается

5.1. Осуществлять несанкционированное и без учётное копирование ключевых данных.

5.2. Хранить НКИ вне сейфов и помещений, гарантирующих их сохранность и конфиденциальность.

5.3. Передавать НКИ третьим лицам.

5.4. Во время работы оставлять НКИ без присмотра (например, на рабочем столе или в разъеме системного блока ПЭВМ).

5.5. Хранить на НКИ какую-либо информацию, кроме ключевой.

5.6. Использование выведенных из действия криптографических ключей.

6. Действия при компрометации действующих ключей и восстановлении конфиденциальной связи

6.1. Под компрометацией криптографического ключа понимается утрата доверия к тому, что данный ключ обеспечивает однозначную идентификацию Владельца и конфиденциальность информации, обрабатываемой с его помощью. К событиям, связанным с компрометацией действующих криптографических ключей, относятся:

– Утрата (хищение) НКИ, в том числе – с последующим их обнаружением;

– Увольнение (переназначение) сотрудников, имевших доступ к ключевой информации;

– Передача закрытых (конфиденциальных) ключей по линии связи в открытом виде;

– Нарушение правил хранения криптографических ключей;

– Вскрытие фактов утечки передаваемой информации или её искажения (подмены, подделки);

– Отрицательный результат при проверке наложенной ЭЦП;

– Несанкционированное или без учётное копирование ключевой информации;

– Все случаи, когда нельзя достоверно установить, что произошло с НКИ (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута вероятность того, что данный факт произошел в результате злоумышленных действий).

6.2. При наступлении любого из перечисленных выше событий Владелец ключа должен немедленно прекратить связь с другими абонентами и сообщить о факте компрометации (или предполагаемом факте компрометации) в Удостоверяющий центр, производивший генерацию ключей ЭЦП.

6.3. При подтверждении факта компрометации действующих ключей Пользователь обязан обеспечить немедленное изъятие из обращения скомпрометированных криптографических ключей.

6.4. Для восстановления конфиденциальной связи после

компрометации действующих ключей Пользователь получает в Удостоверяющем центре новые ключи ЭЦП.

7. Ответственность Пользователя

7.1. Владелец ключа несет персональную ответственность за конфиденциальность личных ключевых носителей.

7.2. В случае неисполнения или ненадлежащего выполнения требований настоящей Инструкции Пользователь несёт ответственность в соответствии с действующим Законодательством Российской Федерации.

УТВЕРЖДЕНА
распоряжением администрации
муниципального образования
Верхнестепновского сельсовета
Степновского района
Ставропольского края
от 21 января 2016 г. № 9-р

ИНСТРУКЦИЯ
по порядку учета и хранению съемных носителей конфиденциальной информации (персональных данных) в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края

1. Общие положения

1.3. Настоящая Инструкция разработана с целью обеспечения безопасности персональных данных при их хранении на съемных носителях.

1.4. Действие настоящей Инструкции распространяется на сотрудников администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края (далее - Администрация), допущенных к обработке персональных данных.

2. Основные термины, сокращения и определения

2.1. Администратор информационной системы персональных данных – технический специалист, обеспечивает ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации ПО и оборудования вычислительной техники.

2.2. АРМ – автоматизированное рабочее место пользователя (ПК с прикладным ПО) для выполнения определенной производственной задачи.

2.3. ИБ – информационная безопасность – комплекс организационно-технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации.

2.4. ИС – информационная система – система, обеспечивающая хранение, обработку, преобразование и передачу информации с использованием компьютерной и другой техники.

2.5. Носитель информации – любой материальный объект, используемый для хранения и передачи электронной информации.

2.6. ПК – персональный компьютер.

2.7. ПО – программное обеспечение вычислительной техники.

2.8. ПО вредоносное – ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.

2.9. Пользователь – работник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработке

персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

3. Порядок использования носителей информации

3.1. Под использованием носителей информации в ИС понимается их подключение к инфраструктуре ИС с целью обработки, приема/передачи информации между ИС и носителями информации.

3.2. В ИС допускается использование только учтенных носителей информации, которые являются собственностью Администрации и подвергаются регулярной ревизии и контролю.

3.3. Носители конфиденциальной информации предоставляются сотрудникам Администрации на основании письменного разрешения руководителя Администрации при:

- необходимости выполнения вновь принятым работником своих должностных обязанностей;
- возникновения у сотрудника Администрации производственной необходимости.

4. Порядок учета, хранения и обращения со съемными носителями конфиденциальной информации (персональных данных), твердыми копиями и их утилизации

4.1. Все находящиеся на хранении и в обращении съемные носители с конфиденциальной информацией (персональными данными) в Администрации подлежат учёту.

4.2. Каждый съемный носитель с записанной на нем конфиденциальной информацией (персональными данными) должен иметь этикетку, на которой указывается его уникальный учетный номер.

4.3. Учет и выдачу съемных носителей конфиденциальной информации (персональных данных) осуществляет ответственный за организацию обработки персональных данных. Факт выдачи съемного носителя фиксируется в журнале учета съемных носителей конфиденциальной информации.

5. При использовании сотрудниками носителей конфиденциальной информации необходимо

5.1. Соблюдать требования настоящей Инструкции.

5.2. Использовать носители информации исключительно для выполнения своих служебных обязанностей.

5.3. Ставить в известность ответственного за обработку персональных данных о любых фактах нарушения требований настоящей Инструкции.

5.4. Бережно относится к носителям конфиденциальной информации (персональных данных).

5.5. Обеспечивать физическую безопасность носителей информации всеми разумными способами.

5.6. Извещать ответственного за обработку персональных данных о фактах утраты (кражи) носителей конфиденциальной информации.

5.7. Перед работой проверять носители конфиденциальной информации на наличие вредоносного ПО.

5.8. Осуществлять вынос съемных носителей конфиденциальной информации (персональных данных) для непосредственной передачи адресату только с письменного разрешения руководителя.

5.9. При отправке или передаче конфиденциальной информации (персональных данных) адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка конфиденциальной информации (персональных данных) адресатам на съемных носителях осуществляется в порядке, установленном для документов данного типа.

5.10. В случае утраты или уничтожения съемных носителей конфиденциальной информации (персональных данных) либо разглашении содержащихся в них сведений немедленно ставится в известность руководитель Администрации. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета съемных носителей конфиденциальной информации (персональных данных).

5.11. Съемные носители конфиденциальной информации (персональных данных), пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется «уполномоченной комиссией». По результатам уничтожения носителей составляется акт.

5.12. В случае увольнения или перевода работника в другое структурное подразделение, предоставленные носители конфиденциальной информации изымаются.

6. Запрещается

6.1. Использовать носители конфиденциальной информации в личных целях.

6.2. Передавать носители конфиденциальной информации другим лицам (за исключением администраторов ИС).

6.3. Хранить съемные носители с конфиденциальной информацией (персональными данными) вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

6.4. Выносить съемные носители с конфиденциальной информацией (персональными данными) из служебных помещений для работы с ними на дому и т. д.

7. Ответственность

7.1. Работники, нарушившие требования данной Инструкции, несут ответственность в соответствии с действующим законодательством.

_____

УТВЕРЖДЕНА
распоряжением администрации
муниципального образования
Верхнестепновского сельсовета
Степновского района
Ставропольского края
от 21 января 2016 г. № 9-р

ИНСТРУКЦИЯ
пользователя информационных систем персональных данных по обеспечению безопасности персональных данных в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края

1. Общие положения

1.1. Пользователь информационной системы персональных данных (далее – Пользователь) осуществляет обработку персональных данных в информационных системах персональных данных в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края (далее – Администрация).

1.2. Пользователем является каждый работник Администрации, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.3. Пользователь несет персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется настоящей Инструкцией, руководящими и нормативными документами Федеральной службы по техническому и экспортному контролю (ФСТЭК) России и другими внутренними нормативно - правовыми документами Администрации по защите информации.

2. Обязанности пользователя

Пользователь обязан:

2.1. Знать и выполнять требования настоящей Инструкции и других внутренних нормативно – правовых документов, по защите персональных данных.

2.2. Выполнять на автоматизированном рабочем месте (далее - АРМ) только те процедуры обработки персональных данных, которые определены для него должностной инструкцией.

2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности персональных данных, а также руководящих и организационно-распорядительных документов.

2.4. Соблюдать требования парольной политики (Раздел 3).

2.5. Соблюдать правила при работе в сетях общего доступа и международного обмена – Интернет (Раздел 4).

2.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на нём информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью в Администрации, а так же для получений консультаций по вопросам информационной безопасности, необходимо обратиться к Администратору информационной системы персональных данных или ответственном за обработку персональных данных.

2.8. Для получения консультаций по вопросам работы и настройке элементов информационной системы персональных данных необходимо обращаться к Администратору информационной системы персональных данных.

2.9. Пользователям запрещается:

– Разглашать защищаемую информацию третьим лицам;

– Копировать защищаемую информацию на внешние носители без письменного разрешения главы муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края;

– Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

– Несанкционированно открывать общий доступ к ресурсам;

– Запрещено подключать к АРМ и корпоративной информационной сети личные внешние носители и мобильные устройства;

– Отключать (блокировать) средства защиты информации;

– Обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к информационной системе персональных данных;

– Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам информационной системе персональных данных;

– Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с Администратором информационной системы персональных данных.

2.10. При отсутствии визуального контроля за рабочей станцией: доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>

2.11. Принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в рамках возложенных на него функций.

3. Организация парольной защиты

3.1. Личные пароли доступа к элементам информационной системы персональных данных создаются пользователем самостоятельно, за исключением временного пароля, который выдает Администратор информационной системы персональных данных.

3.2. Пользователь обязан сменить временный пароль, выданный Администратором информационной системы персональных данных при первом входе в систему.

3.3. Полная плановая смена паролей в информационной системе персональных данных проводится не реже одного раза в 3 месяца.

3.4. Правила формирования пароля:

– Пароль не может содержать имя учетной записи пользователя или какую-либо его часть.

– Пароль должен состоять не менее чем из 8 символов.

– В пароле должны присутствовать символы трех категорий из числа следующих четырех:

– прописные буквы английского алфавита от A до Z;

– строчные буквы английского алфавита от a до z;

– десятичные цифры (от 0 до 9);

– символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %).

– Запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а также имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе;

– Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

– Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

– Запрещается выбирать пароли, которые уже использовались ранее.

3.5. Правила ввода пароля:

– Ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан;

– Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

3.6. Правила хранения пароля:

– Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;

– Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем;

3.7. Лица, использующие паролирование, обязаны:

– Четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов по паролированию;

– Своевременно сообщать Администратору информационной системы персональных данных об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

4. Правила работы в сетях общего доступа и (или) международного обмена

4.1. Работа в сетях общего доступа и международного обмена (сети Интернет) (далее – Сеть) на элементах информационной системы персональных данных должна проводиться при служебной необходимости.

4.2. При работе в Сети запрещается:

– Осуществлять работу при отключенных средствах защиты (антивирус и других);

– Передавать по Сети защищаемую информацию без использования средств шифрования;

– Запрещается скачивать из Сети программное обеспечение и исполняемые файлы (файлы с расширением exe, dll, msi);

– Запрещается посещение сайтов сомнительной репутации (порно-сайты, сайты содержащие нелегально распространяемое ПО и другие);

– Запрещается нецелевое использование подключения к Сети.

5. Ответственность

5.1.Работники, нарушившие требования данной Инструкции, несут ответственность в соответствии с действующим законодательством.

УТВЕРЖДЕНО
распоряжением администрации
муниципального образования
Верхнестепновского сельсовета
Степновского района
Ставропольского края
от 21 января 2016 г. № 9-р

ПОЛОЖЕНИЕ
об обработке персональных данных в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края

1. Общие положения

1.1. Настоящее Положение об обработке персональных данных (далее — Положение) в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края (далее - Администрация) разработано в соответствии с Конституцией Российской Федерации, Федеральным законом «Об информации, информационных технологиях и о защите информации», Федеральным законом «О персональных данных».

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

1.3. Порядок ввода в действие и изменения Положения.

1.3.1. Настоящее Положение вступает в силу с момента его утверждения распоряжением Администрации и действует в течение трёх лет, после чего должно быть пересмотрено.

1.3.2. Все изменения в Положение вносятся распоряжением Администрации.

1.4. Все работники Администрации, имеющие доступ к персональным данным, должны быть ознакомлены с настоящим Положением под роспись.

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

2. Основные понятия и состав персональных данных

2.1. Для целей настоящего Положения используются следующие основные понятия:

– персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой информации субъекту, в том числе его фамилия, имя, отчество, год, месяц, дата и место

рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и прочая дополнительная информация;

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

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

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

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

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

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

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

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

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

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

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

3. Цели обработки персональных данных их состав и сроки обработки

3.1. Обработка персональных данных сотрудников осуществляется в целях обеспечения соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации, содействия сотруднику в прохождении муниципальной службы, обучении и должностном росте, обеспечения личной безопасности муниципального служащего и членов его семьи, а также в целях обеспечения сохранности принадлежащего ему имущества, учета результатов исполнения им должностных обязанностей, ведения кадрового и бухгалтерского учета, и выполнения функций, возложенных законодательством Российской Федерации.

3.2. Состав обрабатываемых персональных данных определяется в соответствии с перечнем персональных данных, обрабатываемых в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края (Приложение №1 к данному Положению).

3.3. Персональные данные сотрудников обрабатываются до момента увольнения после чего передаются в архив и хранятся в течение 75 лет.

3.4. С целью осуществления и выполнения, возложенных законодательством Российской Федерации функций и осуществления прав и законных интересов третьих лиц либо для достижения общественно значимых целей в Администрации обрабатывается следующий перечень персональных данных граждан:

1. Фамилия, Имя, Отчество
2. Серия, номер паспорта
3. Дата рождения
4. Адрес места жительства/прописки
5. Идентификационный номер налогоплательщика (ИНН)
6. Страховой номер индивидуального лицевого счета (СНИЛС)
7. Семейное положение
8. Профессия
9. Сведения о доходах
10. Состав семьи
11. Должность
12. Стаж
13. Сведения об имуществе
14. Образование
15. Номер телефона

3.5. Персональные данные граждан обрабатываются и хранятся до момента достижения цели обработки персональных данных, после чего уничтожаются.

4. Сбор, обработка и защита персональных данных

4.1. Порядок получения персональных данных

4.1.1. Доступ к персональным данным разрешен сотрудникам, указанным в перечне должностей работников, допущенных к работе с персональными данными и замещение которых предусматривает осуществление обработки персональных данных либо, осуществление доступа к персональным данным, в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края. (Приложение №2 к данному Положению).

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

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

4.2. Порядок обработки персональных данных.

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

4.2.2. В соответствии со статьей 6 Федерального закона «О персональных данных» сотрудники Администрации при обработке персональных данных должны соблюдать следующие общие требования:

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

4.2.2.2. Обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных

законодательством Российской Федерации на оператора функций, полномочий и обязанностей.

4.2.2.3. Обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг.

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

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

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

4.2.2.7. Защита персональных данных от неправомерного их использования или утраты обеспечивается Администрацией за счет средств Администрации в порядке, установленном законодательством.

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

4.2.3. Автоматизированная обработка персональных данных разрешается в информационных системах персональных данных перечисленных в перечне информационных систем персональных данных, принадлежащих администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края (Приложение №5 к данному Положению).

5. Передача и хранение персональных данных

5.1. При передаче персональных данных необходимо соблюдать следующие требования:

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

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

5.1.3. Осуществлять передачу персональных данных субъектов в пределах Администрации в соответствии с настоящим Положением и другими внутренними нормативными правовыми актами по защите информации.

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

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

6. Уничтожение персональных данных.

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

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

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

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

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

6.4. Разрешение на уничтожение персональных данных дает глава муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края.

7. Доступ к персональным данным

7.1. Доступ сотрудников к персональным данным осуществляется на основании разрешительной системы доступа.

7.2. Копировать и делать выписки персональных данных разрешается исключительно в служебных целях с письменного разрешения руководителя Администрации.

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

8. Правила работы с обезличенными данными

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

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

8.3. Допускается обезличивание персональных данных при обработке персональных данных без использования средств автоматизации - производить способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

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

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

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

9.2. При осуществлении внутреннего контроля соответствия обработки персональных данных установленным требованиям в Администрации производится проверка:

– соблюдения принципов обработки персональных данных в Администрации;

– соответствия локальных актов в области персональных данных Администрации действующему законодательству Российской Федерации;

– выполнения сотрудниками Администрации требований и правил (в том числе особых) обработки персональных данных в информационных системах персональных данных Администрации;

– перечней персональных данных, используемых для решения задач и функций структурными подразделениями Администрации и необходимости обработки персональных данных в информационных системах персональных данных Администрации;

– правильность осуществления сбора, систематизации, сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения персональных данных в каждой информационной системе персональных данных Администрации;

– актуальность перечня должностей сотрудников Администрации, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;

– актуальность перечня должностей сотрудников Администрации, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных;

– соблюдение прав субъектов персональных данных, чьи персональные данные обрабатываются в информационных системах персональных данных Администрации;

– соблюдение обязанностей Администрацией, предусмотренных действующим законодательством в области персональных данных;

– порядка взаимодействия с субъектами персональных данных, чьи персональные данные обрабатываются в информационных системах персональных данных Администрации, в том числе соблюдения сроков предусмотренных действующим законодательством в области персональных данных, соблюдения требований по уведомлениям, порядка разъяснения субъектам персональных данных необходимой информации, порядка реагирования на обращения субъектов персональных данных, порядка действий при достижении целей обработки персональных данных и отзыве согласий субъектами персональных данных;

– наличие необходимых согласий субъектов персональных данных, чьи персональные данные обрабатываются в информационных системах персональных данных Администрации;

– актуальность сведений, содержащихся в уведомлении Администрации об обработке персональных данных;

– актуальность перечня информационных систем персональных данных в Администрации;

– наличие и актуальность сведений, содержащихся в Правилах обработки персональных данных для каждой информационной системы персональных данных Администрации;

– знания и соблюдение сотрудниками Администрации положений действующего законодательства Российской Федерации в области персональных данных;

– знания и соблюдение сотрудниками Администрации положений локальных актов Администрации в области обработки и обеспечения безопасности персональных данных;

– знания и соблюдение сотрудниками Администрации инструкций, руководств и иных эксплуатационных документов на применяемые средства автоматизации, в том числе программное обеспечение, и средства защиты информации;

– соблюдение сотрудниками Администрации конфиденциальности персональных данных;

– актуальность локальных актов Администрации в области обеспечения безопасности персональных данных, в том числе в Технических паспортах информационных систем персональных данных;

– соблюдение сотрудниками Администрации требований по обеспечению безопасности персональных данных;

– наличие локальных актов Администрации, технической и эксплуатационной документации технических и программных средств информационных систем персональных данных Администрации;

– иных вопросов.

9.3. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, главе муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края докладывает ответственный за организацию обработки персональных данных, либо председатель комиссии.

10. Права субъекта персональных данных

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

10.2. Субъект персональных данных имеет право требовать от сотрудников Администрации уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных

или не являющих необходимыми для работы Администрации персональных данных.

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

– подтверждение факта обработки персональных данных;

– правовые основания и цели обработки персональных данных;

– цели и применяемые способы обработки персональных данных;

– наименование и место нахождения Администрации, сведения о лицах (за исключением работников Администрации), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

– обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

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

– порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;

– информацию об осуществленной или о предполагаемой трансграничной передаче данных;

– наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

– иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

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

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

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

_____

УТВЕРЖДЕН
распоряжением администрации
муниципального образования
Верхнестепновского сельсовета
Степновского района
Ставропольского края
от 21 января 2016 г. № 9-р

ПОРЯДОК
доступа сотрудников администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края в помещения, где ведётся обработка персональных данных

1. Общие положения

1.1. Настоящий Порядок доступа сотрудников в помещения, где ведётся обработка персональных данных в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края (далее - Администрация), разработано в соответствии с Конституцией Российской Федерации, Федеральным законом «Об информации, информационных технологиях и о защите информации», Федеральным законом «О персональных данных», постановлением Правительства РФ от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

1.2. Целью настоящего Порядка является исключение несанкционированного доступа в помещения, где ведётся обработка персональных данных и предотвращение нарушения конфиденциальности персональных данных.

2. Порядок доступа в помещения, где ведётся обработка персональных данных

2.1. Доступ сотрудников Администрации в помещения, в которых ведется обработка персональных данных, осуществляется по перечню должностей сотрудников Администрации в помещения, где ведется обработка персональных данных. Перечень готовится и уточняется лицом, ответственным за организацию обработки персональных данных в Администрации и утверждается распоряжением Администрации.

2.2. Допуск в помещения, в которых ведется обработка персональных данных, иных лиц, осуществляется сотрудниками, указанными в Разрешительной системе доступа сотрудников Администрации в помещения, в которых ведется обработка персональных данных. Пребывание посторонних лиц в кабинетах, в которых ведется обработка персональных данных, допускается только в присутствии сотрудников, указанных в

Разрешительной системе доступа сотрудников Администрации в помещения, в которых ведется обработка персональных данных.

3. Запрещается

3.1. Запрещается оставлять помещения, где ведётся обработка персональных данных, без присмотра сотрудников, имеющих допуск в помещения, где ведётся обработка персональных данных.

3.2. Запрещается оставлять без присмотра находящихся в помещении, где ведётся обработка персональных данных, посторонних лиц, а также, сотрудников, не имеющих допуск в помещения, где ведётся обработка персональных данных.

4. Внутренний контроль

4.1. Внутренний контроль за соблюдением порядка доступа в помещения, где ведётся обработка персональных данных, осуществляется лицом, ответственным за обработку персональных данных.

5. Ответственность

5.1. Сотрудники, нарушившие нормы настоящего Порядка, несут ответственность в соответствии с действующим законодательством.

УТВЕРЖДЕНЫ
распоряжением администрации
муниципального образования
Верхнестепновского сельсовета
Степновского района
Ставропольского края
от 21 января 2016 г. № 9-р

ПРАВИЛА
работы с обезличенными персональными данными в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края

1. Общие положения

1.1. Настоящие Правила работы с обезличенными персональными данными в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края (далее - Администрация) разработаны в соответствии с Федеральным законом от 27 июля 2006 г. №152-ФЗ «О персональных данных», постановлением Правительства РФ от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

1.2. Настоящие Правила определяют порядок работы с обезличенными персональными данными в Администрации.

2. Термины и определения

2.1. Персональные данные – любая информация, относящаяся прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных).

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

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

2.4. Обезличивание персональных данных проводится с целью ведения статистических данных и снижения ущерба от разглашения защищаемых персональных данных.

3. Способы обезличивания персональных данных

3.1. Уменьшение перечня обрабатываемых сведений (например, исключить место жительства субъекта персональных данных).

3.2. Замена части сведений идентификаторами (например, заменить Фамилию, Имя, Отчество порядковым номером по табелю).

3.3. Обобщение – понижение точности некоторых сведений (например, «Место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только город).

3.4. Деление сведений на части и обработка в разных информационных системах.

3.5. Возможны другие способы обезличивания, исключающие возможность определения принадлежности персональных данных определённому субъекту персональных данных.

4. Порядок работы с обезличенными персональными данными

4.1. Мероприятия по обезличиванию персональных данных проводят сотрудники, ответственные за обработку персональных данных.

4.2. Обезличенные персональные данные могут обрабатываться как автоматизированным, так и не автоматизированным способами.

4.3. Обработка обезличенных персональных данных осуществляется с соблюдением конфиденциальности.

4.4. При работе с обезличенными персональными данными в автоматизированном и не автоматизированном режимах необходимо соблюдать правила и требования по обеспечению безопасности персональных данных, действующие в Администрации.

4.5. Передача обезличенных персональных данных третьим лицам разрешается с письменного разрешения руководителя Администрации, либо без такового в случаях, предусмотренных действующим законодательством.

5. Ответственность

5.1. Лица, нарушившие настоящие Правила, несут ответственность в соответствии с действующим законодательством.

УТВЕРЖДЕН
распоряжением администрации
муниципального образования
Верхнестепновского сельсовета
Степновского района
Ставропольского края
от 21 января 2016 г. № 9-р

a.

b. РЕГЛАМЕНТ

c. порядка действий сотрудников администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных

Настоящий Регламент разработан на основании и во исполнение Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Целью настоящего Регламента является:

– обеспечение прав субъектов персональных данных на доступ к их персональным данным, которые обрабатываются в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края (далее - Администрация);

– обеспечение прав уполномоченного органа по защите прав субъектов персональных данных на получение информации, необходимой ему для реализации полномочий по защите прав субъектов персональных данных;

– упорядочение действий сотрудников Администрации при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных.

Настоящий Регламент распространяется на сотрудников Администрации, которые в рамках исполнения своих должностных обязанностей осуществляют прием и регистрацию обращений (запросов) субъектов персональных данных, а также уполномоченного органа по защите прав субъектов персональных данных, осуществляют рассмотрение обращений (запросов), подготовку и направление ответов на них.

Настоящий Регламент подлежит применению исключительно в случаях обращений либо при получении запросов субъектов персональных данных или их законных представителей, а также уполномоченного органа по защите прав субъектов персональных данных в рамках Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

1. Общие положения

1.1. Настоящий Регламент использует следующие сокращения:

ПДн – персональные данные;

ИСПДн – информационная система персональных данных.

1.2. Субъект ПДн – это физическое лицо, определенное или определяемое на основании любой относящейся к нему информации.

1.3. Законный представитель субъекта ПДн – это гражданин, который в силу закона выступает во всех учреждениях и организациях от имени и в защиту личных и имущественных прав и законных интересов недееспособных, ограниченно дееспособных граждан, либо дееспособных, но в силу своего физического состояния (по старости, болезни и т. п.) не могущих лично осуществлять свои права и выполнять свои обязанности. В качестве законных представителей выступают родители, усыновители, опекуны и попечители.

1.4. Далее по тексту настоящего Регламента под субъектом ПДн будет подразумеваться также законный представитель субъекта ПДн.

1.5. В соответствии со статьей 14 Федерального закона «О персональных данных» субъект ПДн имеет право:

– на получение сведений об Администрации, как операторе ПДн, в т.ч. о месте его нахождения;

– на получение сведений о наличии у Администрации ПДн, относящихся к соответствующему субъекту персональных данных;

– на ознакомление с такими ПДн;

– требовать уточнения своих ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

– на получение при обращении или при получении запроса информации, касающейся обработки его ПДн, в том числе содержащей:

– подтверждение факта обработки персональных данных Администрацией, а также цель такой обработки;

– способы обработки персональных данных, применяемые Администрацией;

– 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 субъекта персональных данных может повлечь за собой обработка его персональных данных.

1.6. В соответствии со статьей 9 Федерального закона «О персональных данных» субъект ПДн имеет право отозвать свое согласие на обработку ПДн.

1.7. В соответствии со статьями 14, 20, 21 Федерального закона «О персональных данных» Администрация, как оператор ПДн, в случае поступления соответствующего запроса от субъекта ПД обязан:

– предоставить субъекту ПДн в доступной форме сведения о наличии его ПДн (при этом указанные сведения не должны содержать ПДн, относящиеся к другим субъектам ПДн);

– сообщить субъекту ПДн информацию о наличии ПДн, относящихся к соответствующему субъекту ПДн, и другие сведения, право на получение которых субъектом ПДн предусмотрено статьей 14 Федерального закона «О персональных данных»;

– предоставить возможность ознакомления с ПДн без взимания платы за это;

– внести в ПДн необходимые изменения, уничтожить или блокировать соответствующие ПДн по предоставлении субъектом ПДн сведений, подтверждающих, что ПДн, которые относятся к соответствующему субъекту и обработку которых осуществляет Администрация, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

– прекратить обработку ПДн и уничтожить их в случае отзыва субъектом ПДн согласия на обработку своих ПДн;

– о внесенных изменениях и предпринятых мерах уведомить субъекта ПДн и третьих лиц, которым ПДн этого субъекта были переданы;

– уведомить субъекта ПДн об уничтожении ПДн;

1.8. В соответствии с пунктом 3 части 5 статьи 14 Федерального закона «О персональных данных» право субъекта ПДн на доступ к своим ПДн ограничивается в случае, если предоставление ПДн нарушает конституционные права и свободы других лиц.

2. Действия сотрудников Администрации при получении запроса субъекта ПДн

2.1. В соответствии с частью 3 статьи 14 Федерального закона «О персональных данных» запрос должен содержать номер основного документа, удостоверяющего личность субъекта ПДн или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта ПДн или его законного представителя.

2.2. В целях регистрации запросов субъектов ПДн и ответов на такие запросы в Администрации осуществляется ведение журнала регистрации запросов субъектов ПДн.

2.3. Ответственный за организацию обработки ПДн осуществляет прием и регистрацию запросов субъектов ПДн, а также рассмотрение, подготовку, регистрацию и направление ответов на такие запросы.

2.4. При получении запроса (обращения) физического лица, сотрудник

Администрации, ответственный за прием и регистрацию входящей корреспонденции в Администрации, непосредственно в день получения устанавливает:

2.4.1. Содержит ли запрос фамилию, имя, отчество (последнее при его наличии) гражданина или его законного представителя, номер основного документа, удостоверяющего личность гражданина или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе;

2.4.2. Содержит ли почтовый адрес, по которому должны быть направлены ответ;

2.4.3. Имеется ли собственноручная подпись, а если запрос направлен в электронной форме, то имеется ли электронная цифровая подпись;

2.4.4. Сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором;

2.4.5. Отвечает ли такой запрос (обращение) требованиям, установленным статьей 14 Федерального закона РФ «О персональных данных» к запросу субъекта ПДн.

2.5. В случае если при приеме запроса (обращения) физического лица будет установлено, что он содержит в себе все сведения, перечисленные в п. 2.4. настоящего то такой запрос подлежит приему и регистрации в журнале регистрации запросов субъектов ПДн в тот же день.

2.6. В случае, если при приеме запроса (обращения) физического лица будет установлено, что он не содержит в себе сведений, перечисленных в п. 2.4. настоящего Регламента, то такой запрос подлежит приему и регистрации в порядке, предусмотренном Администрацией для приема и регистрации прочей входящей корреспонденции.

2.7. Запросы субъектов ПДн, зарегистрированные в соответствии с п. 2.5. настоящего Регламента, в день регистрации подлежат передаче сотруднику (сотрудникам) Администрации, указанному (ным) в пункте 2.3. настоящего Регламента.

2.8. Сотрудники Администрации, ответственные за рассмотрение запросов субъектов персональных данных, обязаны рассмотреть запрос субъекта ПДн и подготовить ответ на него в письменной форме в течение десяти рабочих дней с даты получения Администрацией указанного запроса.

2.9. В случае если в запросе субъект ПДн изъявил желание ознакомиться со своими ПДн, возможность такого ознакомления должна быть предоставлена субъекту ПДн в течение десяти рабочих дней с даты получения Администрацией указанного запроса.

2.10. Письменный ответ на запрос субъекта ПДн должен быть направлен в его адрес заказным письмом с уведомлением о вручении в течение десяти рабочих дней с даты получения Администрацией указанного

запроса.

2.11. Если при рассмотрении запроса субъекта ПДн будет установлено, что предоставление ПДн нарушает конституционные права и свободы других лиц, Администрация сообщает ему об отказе в предоставлении информации о ПДн либо таких ПДн, о чем в срок, не превышающий семи рабочих дней со дня получения запроса субъекта ПДн в адрес субъекта ПДн направляется мотивированный ответ в письменной форме, содержащий ссылку на положение пункта 4 части 8 статьи 14 Федерального закона «О персональных данных».

2.12. Для обработки персональных данных, содержащихся в обращении в письменной форме субъекта ПД, дополнительного согласия не требуется.

3. Действия сотрудников Администрации при получении запроса уполномоченного органа по защите прав субъектов персональных данных

3.1. Прием и регистрация запросов уполномоченного органа по защите прав субъектов ПДн осуществляется Администрацией в порядке, установленном для приема и регистрации входящей корреспонденции.

3.2. При получении запроса уполномоченного органа по защите прав субъектов ПДн сотрудники Администрации, ответственные за прием и регистрацию входящей корреспонденции, в тот же день осуществляют регистрацию такого запроса и передают его сотрудникам указанным в пункте 2.3.

3.3. Администрация, в лице сотрудников, указанных в пункте 2.3. настоящего Регламента, сообщает в уполномоченный орган по защите прав субъектов ПДн по его запросу информацию, необходимую для осуществления деятельности указанного органа, а также направляет истребуемые им документы в течение семи рабочих дней с даты получения такого запроса.

3.4. В случае выявления уполномоченным органом по защите прав субъектов ПДн фактов недостоверности ПДн или неправомерных действий с ними, уточнение, блокирование или уничтожение таких ПДн осуществляется в порядке и сроки, предусмотренные пунктом 4 настоящего Регламента для соответствующих действий (операций) в отношении ПДн.

4. Действия сотрудников Администрации при получении требования субъекта ПДн об уточнении своих ПДн, их блокировании или уничтожении; в случае выявления при обращении или по запросу субъекта ПДн фактов недостоверности ПДн или неправомерных действий с ними; в случае отзыва субъектом ПДн согласия на их обработку

4.1. При получении требований субъектов ПДн об уточнении своих ПДн, их блокировании, уничтожении прием и регистрация таких требований осуществляется в порядке, предусмотренном пунктом 2 настоящего Регламента.

4.2. Требования субъектов ПДн в тот же день передаются сотрудникам Администрации, указанным в пункте 2.3.

4.3. Полномочные сотрудники Администрации вносят в ПДн субъекта необходимые изменения, уничтожают или блокируют соответствующие ПДн по предоставлении субъектом ПДн сведений, подтверждающих, что ПДн, которые относятся к соответствующему субъекту и обработку которых осуществляет Администрация, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

4.4. О внесенных изменениях и предпринятых мерах Администрация обязана уведомить субъекта ПДн и третьих лиц, которым ПДн этого субъекта были переданы.

4.5. В случае если факт недостоверности ПДн или неправомерных действий с ними будет выявлен при обращении или по запросу субъекта ПДн Администрация обязана осуществить блокирование ПДн, относящихся к соответствующему субъекту ПДн, с момента такого обращения или получения такого запроса на период проверки.

4.6. В случае подтверждения факта недостоверности ПДн Администрация на основании документов, представленных субъектом ПДн, или иных необходимых документов обязана уточнить ПДн и снять их блокирование.

4.7. В случае выявления неправомерных действий с ПДн Администрация в срок, не превышающий трех рабочих дней с даты такого выявления, обязана устранить допущенные нарушения.

4.8. В случае невозможности устранения допущенных нарушений Администрация в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с ПДн, обязана уничтожить ПДн.

4.9. Об устранении допущенных нарушений или об уничтожении ПДн Администрация обязана уведомить субъекта ПДн.

4.10. В случае отзыва субъектом ПДн согласия на обработку своих ПДн Администрация обязана прекратить обработку ПДн и уничтожить их в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено федеральным законодательством. Об уничтожении ПДн Администрация обязана уведомить субъекта ПДн.

Приложение № 1 к Регламенту
Форма 1 «Запрос субъекта ПДн»

Главе муниципального образования
Верхнестепновского сельсовета
Степновского района
Ставропольского края

От

Паспорт серия номер

(Когда и кем выдан)

Проживающий по адресу:

Контактный номер телефона

Руководствуясь статьей 14 Федерального закона «О персональных данных», прошу Вас предоставить мне следующую информацию:

1. Какова цель обработки моих персональных данных в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края;
2. Каковы способы обработки моих персональных данных, применяемые в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края, как оператором персональных данных;
3. Какие лица имеют доступ к моим персональным данным и каким лицам может быть предоставлен такой доступ;
4. Каков перечень обрабатываемых в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края принадлежащих мне персональных данных и каков источник их получения;
5. Каковы сроки обработки моих персональных данных и каковы сроки их хранения;
6. Какие юридические последствия для меня, как для субъекта персональных данных, может повлечь за собой обработка моих персональных данных.

Фамилия И.О. (Подпись) (Дата)

Приложение № 2 к Регламенту
Форма 2 «Ответ на запрос субъекта ПДн»

Бланк администрации
поселения

Дата, исходящий номер

_____
(Фамилия, Имя, Отчество)
_____
(адрес заявителя)

Уважаемый _____!

Руководствуясь положениями статей 14, 20 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» сообщаем Вам, что администрация муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края обрабатывает Ваши персональные данные

1.Цель обработки Ваших персональных –
_____
(указать цель, заранее определенную до начала обработки)

2. Способы обработки Ваших персональных данных – автоматизированная обработка, неавтоматизированная обработка, смешанная обработка.

3.Лица, имеющие доступ к Вашим персональным данным:

- Должность1;
- Должность2;

4.Доступ к Вашим персональным данным может быть предоставлен:_____.
Также, по основаниям, предусмотренным действующим законодательством, доступ к Вашим персональным данным может быть предоставлен органам, осуществляющим оперативно-розыскную деятельность, органам дознания, следствия, суда.

5.Перечень обрабатываемых персональных данных: _____ Источник получения персональных данных – _____

6.Срок обработки Ваших персональных данных – _____

7.Обработка Ваших персональных данных может повлечь следующие юридические последствия – обработка Ваших ПДн влечет для Вас в качестве юридических последствий возникновение у Вас прав, присущих субъекту ПДн и предусмотренных статьей 14 Федерального закона «О персональных данных»).

Глава муниципального образования
Верхнестепновского сельсовета
Степновского района
Ставропольского края _____ _____
/подпись/ *М.П.* */И.О. Фамилия/*

УТВЕРЖДЕН
распоряжением администрации
муниципального образования
Верхнестепновского сельсовета
Степновского района
Ставропольского края
от 21 января 2016 г. № 9-р

ИНСТРУКЦИЯ
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края

1. Общие положения

1.1. Настоящая Инструкция осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края (далее - Администрация) разработана с учетом Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним внутренними нормативными правовыми актами.

1.2. Настоящая Инструкция определяет порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

2. Тематика внутреннего контроля

2.1. Тематика проверок обработки персональных данных с использованием средств автоматизации:

– Соответствие полномочий пользователя разрешительной системе доступа;

– Соблюдение пользователями информационных систем персональных данных парольной политики;

– Соблюдение пользователями информационных систем персональных данных антивирусной политики;

– Соблюдение пользователями информационных систем персональных данных правил работы со съемными носителями персональных данных;

– Соблюдение правил работы с средствами криптографической защиты;

– Соблюдение порядка доступа в помещения, где расположены элементы информационных систем персональных данных;

– Соблюдение порядка резервирования баз данных и хранения резервных копий;

– Соблюдение порядка работы со средствами защиты информации.

2.2. Соблюдение правил хранения и работы с бумажными носителями персональных данных.

3. Порядок проведения внутренних проверок

3.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям Администрация организует проведение периодических проверок условий обработки персональных данных.

3.2. Проверки осуществляются ответственным за организацию обработки персональных данных (далее - Ответственный) либо комиссией, образуемой распоряжением Администрации.

3.3. Внутренние проверки проводятся в соответствии с Планом внутренних проверок, составленным Ответственным либо Председателем комиссии и утвержденным распоряжением Администрации. Форма Плана приведена в Приложении 1 к настоящей Инструкции. При необходимости План может быть изменен.

3.4. План внутренних проверок составляется в декабре текущего года на следующий год и включает в себя все тематики проверок, равномерно распределенные на весь год.

3.5. Очередность и объем проверок определяется Ответственным либо Председателем комиссии самостоятельно.

3.6. Проверки осуществляются Ответственным либо комиссией непосредственно на месте обработки персональных данных путем опроса, либо, при необходимости, путем осмотра рабочих мест сотрудников, участвующих в процессе обработки персональных данных.

3.7. Для каждой проверки составляется Протокол проведения внутренней проверки. Форма Протокола приведена в Приложении 2 к настоящей Инструкции.

3.8. При выявлении нарушений в ходе проверки Ответственным либо Председателем комиссии в Протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.

3.9. Протоколы хранятся у Ответственного либо Председателя комиссии в течение текущего года. Уничтожение Протоколов проводится Ответственным либо комиссией самостоятельно в январе следующего за проверочным годом.

3.10. О результатах проверки и мерах, необходимых для устранения нарушений, руководителю докладывает Ответственный либо Председатель комиссии.

Приложение №1
ФОРМА

ПЛАН
внутренних проверок условий обработки персональных данных

№	Тема проверки	Нормативный документ предъявляющий требования	Срок проведения	Исполнитель
1.	Соответствие полномочий пользователя разрешительной системе доступа	Разрешительная система доступа		
2.	Соблюдение пользователями информационных систем персональных данных парольной политики	Инструкция пользователя		
3.	Соблюдение пользователями информационных систем персональных данных антивирусной политики	Инструкция по антивирусной защите		
4.	Соблюдение пользователями информационных систем персональных данных правил работы со съемными носителями персональных данных	Инструкция по работе со съёмными носителями		
5.	Соблюдение правил работы с средствами криптографической защиты	Инструкция по работе с средствами криптографической защиты		
6.	Соблюдение порядка доступа в помещения, где расположены элементы информационных систем персональных данных	Порядок доступа сотрудников в помещения где ведётся обработка персональных данных		
7.	Соблюдение порядка резервирования баз данных и хранения резервных копий	Инструкция о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения и баз данных		

№	Тема проверки	Нормативный документ предъявляющий требования	Срок проведения	Исполнитель
8.	Соблюдение порядка работы со средствами защиты информации	Инструкция пользователя информационных систем персональных данных, инструкция администратора информационных систем персональных данных по обеспечению безопасности персональных данных		
9.	Соблюдение правил хранения и работы с бумажными носителями персональных данных.	Инструкция по порядку учета и хранению документов, содержащих персональные данные		

Приложение 2
ФОРМА

Протокол
проведения внутренней проверки условий обработки персональных данных

Настоящий Протокол составлен в том, что __.__.201_ ответственным за организацию обработки персональных данных/ комиссией по внутреннему контролю проведена проверка

_____
(тема проверки)

Проверка осуществлялась в соответствии с требованиями

_____
_____.
(название документа)

В ходе проверки проверено:

_____
_____
_____
_____
_____
_____
_____

Выявленные нарушения:

_____
_____
_____
_____.

Меры по устранению нарушений:

_____
_____
_____
_____
_____

Срок устранения нарушений: _____.
Должность Ответственного _____И.О. Фамилия
либо
Председатель комиссии _____И.О. Фамилия
Члены комиссии:
Должность _____И.О. Фамилия
Должность _____И.О. Фамилия
Должность _____И.О. Фамилия

Приложение № 1
к Положению об обработке
персональных данных в администрации
муниципального образования
Верхнестепновского сельсовета
Степновского района
Ставропольского края

ПЕРЕЧЕНЬ
персональных данных, обрабатываемых в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края

Персональные данные сотрудников:

1. Фамилия, Имя, Отчество
2. Серия, номер паспорта
3. Дата рождения
4. Адрес места жительства/прописки
5. Идентификационный номер налогоплательщика (ИНН)
6. Страховой номер индивидуального лицевого счета (СНИЛС)
7. Семейное положение
8. Профессия
9. Сведения о доходах
10. Состав семьи
11. Должность
12. Стаж
13. Сведения об имуществе
14. Образование

Персональные данные жителей муниципального образования:

1. Фамилия, Имя, Отчество
2. Серия, номер паспорта
3. Дата рождения
4. Адрес места жительства/прописки
5. Образование
6. Состав семьи
7. Должность
8. Сведения об имуществе
9. Семейное положение
10. Номер телефона

_____

Приложение № 2
к Положению об обработке
персональных данных в администрации
муниципального образования
Верхнестепновского сельсовета
Степновского района
Ставропольского края

Перечень
должностей работников, допущенных к работе с персональными данными и замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края

1. Глава муниципального образования
2. Управляющий делами
3. Главный специалист - главный бухгалтер
4. Ведущий специалист
5. Специалист 1 категории
6. Бухгалтер
7. Старший инспектор военно-учетного стола
8. Старший инженер

_____

Приложение № 3
к Положению об обработке
персональных данных в администрации
муниципального образования
Верхнестепновского сельсовета
Степновского района
Ставропольского края

ОБЯЗАТЕЛЬСТВО
о неразглашении персональных данных в администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края

Я, _____
(ФИО сотрудника)

Паспорт серия _____ номер _____ выдан _____

_____

исполняющий(ая) должностные обязанности _____
(должность)

предупрежден(а), что на период исполнения должностных обязанностей мне будет предоставлен допуск к персональным данным. Настоящим добровольно принимаю на себя обязательства:

1. Не разглашать третьим лицам персональные данные, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.

2. В случае попытки третьих лиц получить от меня персональные данные, сообщать непосредственному руководителю.

3. Не использовать персональные данные с целью получения выгоды.

4. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.

5. После прекращения права на допуск к персональным данным не разглашать и не передавать третьим лицам известные мне персональные данные.

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

_____ _____ _____
(Фамилия, Имя, Отчество) (Дата) (Подпись)

Приложение № 4
к Положению об обработке
персональных данных в администрации
муниципального образования
Верхнестепновского сельсовета
Степновского района
Ставропольского края

Согласие на обработку персональных данных

Я,
_____
(Ф.И.О. полностью)

зарегистрированный(ая) по адресу:
_____
_____
__,
паспорт серии _____№_____
выдан_____
_____
__,
(орган, выдавший паспорт и дата выдачи)

даю согласие администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края, расположенной по адресу: 357937, Ставропольский край, Степновский район, пос. Верхнестепной, ул. Советская, 7, на обработку моих персональных, а именно:

_____
(указать перечень персональных данных)
_____
_____
_____

с целью
_____
(указать цель обработки)
_____
_____

разрешаю
_____
(указать перечень действий с персональными данными)
_____
_____

настоящее согласие вступает в силу с момента его подписания и действительно до

_____
(дата или условие прекращения обработки персональных данных)
_____
_____

Данное согласие может быть отозвано по моему письменному заявлению.

«____»_____20___г.

_____

(подпись и фамилия, имя, отчество прописью полностью)

Приложение № 5
к Положению об обработке
персональных данных в администрации
муниципального образования
Верхнестепновского сельсовета
Степновского района
Ставропольского края

Перечень
информационных систем персональных данных, принадлежащих администрации муниципального образования Верхнестепновского сельсовета Степновского района Ставропольского края

1. «1С: Бухгалтерия»
2. «Хозяйство»
3. «Находка-ЗАГС»

_____