РОССИЙСКАЯ ФЕДЕРАЦИЯ
РОСТОВСКАЯ ОБЛАСТЬ

Муниципальное образование «Краснолучское сельское поселение»
Администрация Краснолучского сельского поселения

РАСПОРЯЖЕНИЕ

01.07.2026 **№23** **х. Красный Луч**

Об утверждении внутренних нормативно-правовых актов по защите персональных данных

Для обеспечения безопасности персональных данных при их обработке в Администрации Краснолучского сельского поселения во исполнение требований Федерального закона от 27.06.2006 № 152 «О персональных данных», постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», руководствуясь Уставом муниципального образования «Краснолучское сельское поселение»:

1. Утвердить следующий перечень правовых актов:

1.1. Инструкцию администратора информационных систем персональных данных по обеспечению безопасности персональных данных в Администрации Краснолучского сельского поселения, согласно Приложению № 1;

1.2. Инструкцию о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения и баз данных в Администрации Краснолучского сельского поселения, согласно Приложению № 2;

1.3. Инструкцию ответственного за обработку персональных данных в Администрации Краснолучского сельского поселения, согласно Приложению № 3;

1.4. Инструкцию по организации антивирусной защиты в Администрации Краснолучского сельского поселения согласно Приложению № 4;

1.5. Порядок учета, хранения и уничтожения материальных носителей персональных данных в информационной системе персональных данных Администрации Краснолучского сельского поселения, согласно Приложению № 5;

1.6. Инструкцию пользователя информационных систем персональных данных по обеспечению безопасности персональных данных в Администрации Краснолучского сельского поселения, согласно Приложению № 6;

1.7. Положение об обработке персональных данных в Администрации Краснолучского сельского поселения, согласно Приложению № 7;

1.8. Порядок доступа сотрудников Администрации Краснолучского сельского поселения в помещения, где ведётся обработка персональных данных, согласно Приложению № 8;

1.9. Правила работы с обезличенными персональными данными в Администрации Краснолучского сельского поселения, согласно Приложению № 9;

1.10. Регламент порядка действий сотрудников Администрации Краснолучского сельского поселения, при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных, согласно Приложению № 10;

1.11. Политику обработки персональных данных в Администрации Краснолучского сельского поселения области, согласно Приложению № 11;

1.12. Инструкцию администратора безопасности информационных систем персональных данных Администрации Краснолучского сельского поселения, согласно Приложению № 12;

1.13. Инструкцию пользователя по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций в Администрации Краснолучского сельского поселения, согласно Приложению № 13;

1.14. Концепцию информационной безопасности информационных систем персональных данных в Администрации Краснолучского сельского поселения, согласно Приложению № 14;

1.15. Политику информационной безопасности в Администрации Краснолучского сельского поселения, согласно Приложению № 15;

1.16. Инструкцию по организации парольной защиты информационных систем персональных данных в Администрации Краснолучского сельского поселения, согласно Приложению № 16;

1.17. Инструкцию по организации защиты информации о событиях безопасности в информационных систем персональных данных в

Администрации Краснолучского сельского поселения, согласно Приложению № 17;

1.18. Инструкцию по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационной системы персональных данных в Администрации Краснолучского сельского поселения, согласно Приложению № 18;

1.19. Инструкцию по обеспечению защиты информации при выводе информационных систем персональных данных из эксплуатации или после принятия решения об окончании обработки информации в Администрации Краснолучского сельского поселения, согласно Приложению № 19;

1.20. Порядок уничтожения и блокирования персональных данных в Администрации Краснолучского сельского поселения, согласно Приложению № 20;

1.21. Положение об обработке персональных данных без использования средств автоматизации в Администрации Краснолучского сельского поселения, согласно Приложению № 21;

1.22. Лист ознакомления с законодательством в Администрации Краснолучского сельского поселения, согласно Приложению № 22;

1.23. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям безопасности информации в информационной системе персональных данных Администрации Краснолучского сельского поселения, согласно Приложению № 23;

2. Ответственному за организацию обработки персональных данных довести до сведения всех сотрудников, обрабатывающих персональные данные, положения утверждаемых нормативно-правовых актов.

3. Разместить Положение об обработке персональных данных и Политику обработки персональных данных на официальном сайте Администрации Краснолучского сельского поселения в информационно-телекоммуникационной сети «Интернет».

4. Признать утратившим силу распоряжение Администрации Краснолучского сельского поселения №8 от 27.02.2017 «Об утверждении внутренних нормативно-правовых актов по защите персональных данных».

5. Контроль за выполнением настоящего распоряжения оставляю за собой.

6. Распоряжение вступает в силу со дня его подписания.

Глава Администрации
Краснолучского сельского поселения  А.С. Шаблий

Приложение № 1
к распоряжению Администрации
Краснолучского сельского
поселения
от 01.07.2026 № 23

ИНСТРУКЦИЯ
администратора информационных систем персональных данных по обеспечению безопасности персональных данных в Администрации Краснолучского сельского поселения

1. Общие положения

1.1. Настоящая Инструкция определяет обязанности, полномочия и ответственность администратора информационных систем персональных данных (ИСПДн) по обеспечению безопасности персональных данных в Администрации Краснолучского сельского поселения (далее – Администрация).

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

1.3. Администратор ИСПДн подчиняется главе Администрации Краснолучского сельского поселения.

1.4. Администратор ИСПДн в своей работе руководствуется настоящей Инструкцией и Положением об обработке 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 нормативно-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.

Приложение № 2
к распоряжению Администрации
Краснолучского сельского
поселения
от 01.07.2026 №23 ___

ИНСТРУКЦИЯ
о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения и баз данных в Администрации Краснолучского сельского поселения

Назначение и область действия

Данная Инструкция определяет действия, связанные с мерами и средствами поддержания непрерывной работы и восстановления работоспособности информационных систем в Администрации Краснолучского сельского поселения (далее – Администрация).

Настоящая Инструкция регламентирует:

меры защиты от потери информации;

действия по восстановлению в случае потери информации.

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

Меры обеспечения надежной работы и восстановления ресурсов при возникновении инцидентов

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.).

Организационные меры.

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).

Данные о проведение процедуры резервного копирования должны отражаться в специально созданном Журнале учета (приложение 1).

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

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

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

Порядок проведения резервирования информации

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

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).

Все файлы, входящие в состав резервной копии, должны архивироваться в один архив с присвоением имени архива в формате время_дата (например, 18.00_21.05.2024).

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

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

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.

Порядок проведения восстановления информации

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

Восстановление информации следует проводить из наиболее актуальной резервной копии.

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).

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).

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

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.

Ответственность

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

Приложение 1

к Инструкции о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения и баз данных в Администрации Краснолучского сельского поселения

ЖУРНАЛ
учета резервного копирования и восстановления данных
№ ___

количество листов_____

начат_____

окончен_____

№ п.п.	Дата проведения резервного копирования/ восстановления	Наименование резервной копии	Наименование информационной системы/базы данных	ФИО и подпись ответственного
1.	2.	3.	4.	5.
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				

Приложение № 3
к распоряжению Администрации
Краснолучского сельского
поселения
от 01.07.2026_№23 ___

ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных в Администрации Краснолучского сельского поселения Ростовской области

1.Общие положения

1.1 Настоящая Инструкция разработана в соответствии со ст. 22.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и определяет обязанности, полномочия и ответственность лиц, ответственных за организацию обработки персональных данных в Администрации Краснолучского сельского поселения (далее – Администрация).

1.2 Ответственный за организацию обработки персональных данных назначается распоряжением Администрации Краснолучского сельского поселения из числа сотрудников Администрации.

1.3 Ответственный за организацию обработки персональных данных подчиняется главе Администрации Краснолучского сельского поселения.

1.4 Ответственный за организацию обработки персональных данных в своей работе руководствуется настоящей Инструкцией, Федеральными законами от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – ФЗ-№152 «О персональных данных»), от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлениями Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемых без использовании средств автоматизации», приказом Федеральной службы по техническому и экспортному контролю России от 18.02.2013 № 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.

1.5 Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения безопасности персональных данных и не исключает обязательного выполнения их требований.

2. Обязанности

2.1. Осуществлять внутренний контроль за соблюдением сотрудниками Администрации требований законодательства РФ при обработке персональных данных, внутренних положений, инструкций и других нормативно-правовых документов в области защиты информации.

2.2. Доводить до сведения работников Администрации (структурного подразделения) содержание положений законодательства Российской Федерации о персональных данных, внутренних нормативно-правовых актов Администрации по вопросам обработки персональных данных, требований по защите персональных данных.

2.3. 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 ФЗ-№152 «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;

такие 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).

2.4. 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.

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

3. Действия при обнаружении попыток несанкционированного доступа

3.1. К попыткам несанкционированного доступа относятся:

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

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

3.2. При выявлении факта несанкционированного доступа ответственный за организацию обработки персональных данных обязан:

прекратить несанкционированный доступ к персональным данным;

доложить главе Администрации служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

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

известить администратора безопасности ИСПДн о факте несанкционированного доступа;

составить акт о факте обнаружения попытки несанкционированного доступа (приложение 1).

4. Ответственность

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

Приложение 1
к Инструкции ответственного за
организацию обработки персональных
данных в Администрации
Краснолучского сельского поселения

АКТ
о факте обнаружения попытки несанкционированного доступа

Настоящий АКТ составлен в том, что «___» _____ 20__ года ответственным за организацию обработки и обеспечение безопасности ПДн, была обнаружена попытка несанкционированного доступа (НСД) к _____

_____
(наименование ИСПДн, базы данных)

Попытка НСД была выполнена под учетной записью пользователя:

_____

Статус НСД: _____
(успешный, неуспешный)

Принятые меры по устранению последствий НСД:

_____
_____
_____
_____
_____
_____
_____
_____
_____

Ответственный за организацию обработки и обеспечение безопасности ПДн

_____ _____ _____
(должность) (подпись) (фамилия и инициалы)

Приложение № 4
к распоряжению Администрации
Краснолучского сельского
поселения
от 01.07.2026 №23 ___

ИНСТРУКЦИЯ
по организации антивирусной защиты в Администрации Краснолучского сельского поселения

1. Общие положения

Настоящая Инструкция предназначена для организации порядка проведения антивирусного контроля в Администрации Краснолучского сельского поселения (далее – Администрация) и предотвращения возникновения фактов заражения вредоносным программным обеспечением.

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.

Приложение № 5

к распоряжению Администрации
Краснолучского сельского
поселения
от 01.07.2026 №23___

Порядок учета, хранения и уничтожения материальных носителей персональных данных в информационной системе персональных данных Администрации Краснолучского сельского поселения

1. Общие положения

1.1. Настоящий Порядок устанавливает организацию учета, хранения и уничтожения материальных носителей персональных данных (электронные, магнитные, оптические, бумажные) в информационной системе персональных (далее – ИСПДн**)** Администрации Краснолучского сельского поселения (далее – Администрация).

1.2. Настоящий Порядок разработан на основании следующих документов:

федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

постановление Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правыми актами;

постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК) Российской Федерации от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных».

2. Требования по обеспечению безопасности при использовании материальных носителей персональных данных

2.1 При обращении с материальными носителями персональных данных выполняются следующие основные правила:

– находящиеся на хранении и в обращении материальные носители персональных данных подлежат учёту;

– раздельному учету в журналах учета подлежат машинные носители, съемные машинные носители персональных данных (флэш-накопители, CD-диски и

т.п.), бумажные носители персональных данных (в соответствии с номенклатурой делопроизводства);

– пользователи для работы в ИСПДн могут использовать только учтенные материальные носители персональных данных;

– машинные носители персональных данных, срок эксплуатации которых истек, а также бумажные носители, потерявшие актуальность или необходимость их использования (достижение цели обработки, истечение срока хранения) уничтожаются в установленном порядке;

– все съемные машинные и бумажные носители информации хранятся в запираемых шкафах (сейфах), а также раздельно, в соответствии с целями обработки ПДн.

2.2. Ответственным за хранение, учет и выдачу съемных машинных носителей информации является администратор безопасности ИСПДн.

2.3. Порядок учета материальных носителей персональных данных.

Все находящиеся на хранении и в обращении материальные носители персональных данных учитываются в журнале учета машинных носителей персональных данных (форма журнала приведена в Приложении 1), журнале учета съемных машинных носителей персональных данных (форма журнала приведена в Приложении 2) и журнале учета бумажных носителей персональных данных (форма журнала приведена в Приложении 3).

Каждый материальный носитель персональных данных должен иметь уникальный регистрационный (учетный) номер. В качестве регистрационных номеров допускается использовать идентификационные (серийные) номера машинных носителей, присвоенные производителем этих машинных носителей, номера инвентарного учета, в т.ч. инвентарные номера технических средств, имеющих встроенные носители информации, учетные номера по номенклатуре дел для бумажных носителей и иные учетные номера.

Учет встроенных в стационарные технические средства машинных носителей персональных данных может вестись в журналах материально-технического учета в составе соответствующих технических средств. При использовании в составе одного технического средства информационной системы нескольких встроенных машинных носителей персональных данных, конструктивно объединенных в единый ресурс для хранения информации, допускается присвоение регистрационного номера техническому средству в целом.

Учет и выдачу съемных машинных носителей персональных данных осуществляет администратор безопасности ИСПДн. Факт выдачи и получения съемного машинного носителя конкретным сотрудником фиксируется в журнале учета съемных машинных носителей персональных данных.

Учет и выдачу бумажных носителей персональных данных осуществляет руководитель подразделения, сотрудник которого использует эти бумажные носители при работе в ИСПДн.

После окончания работ пользователь ИСПДн сдает материальный носитель, о чем делается соответствующая запись в соответствующем журнале учета материальных носителей персональных данных. При наличии личного сейфа у

пользователя ИСПДн допускается хранение учтенных материальных носителей в личных сейфах, в противном случае, материальные носители персональных данных должны храниться в сейфе у ответственного за учет материальных носителей персональных данных в ИСПДн.

В случае передачи материальных носителей между пользователями ИСПДн Администрации с разными правами доступа к персональным данным, при необходимости, должно обеспечиваться уничтожение (стирание) информации (на машинных и съемных машинных носителях), а также при передаче материальных носителей (машинных и съемных машинных) в сторонние организации для ремонта или утилизации, администратор безопасности ИСПДн должен осуществлять контроль уничтожения (стирания) информации на этих носителях. При этом, уничтожение (стирание) информации на материальных носителях должно исключать возможность восстановления защищаемой информации.

Сотрудникам запрещается подключать к ИСПДн неучтенные носители информации и информационно-телекоммуникационные средства.

2.4. Порядок уничтожения информации на материальных носителях персональных данных и уничтожения материальных носителей персональных данных.

В ИСПДн должны применяться следующие меры по уничтожению (стиранию) информации на материальных носителях персональных данных, исключающие возможность восстановления защищаемой информации:

– удаление файлов на машинном носителе (съемном машинном носителе) информации штатными средствами операционной системы и последующее форматирование машинного носителя (съемного машинного носителя) информации штатными средствами операционной системы;

– удаление файлов на машинном носителе (съемном машинном носителе) информации средствами гарантированного удаления информации (СЗИ Secret Net Studio, СЗИ Dallas Lock, средство гарантированного удаления Terrier и т.п.);

– «вымарывание» информации на бумажных носителях.

Материальные носители персональных данных, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению.

Уничтожение материальных носителей персональных данных осуществляется комиссией по уничтожению, назначаемой руководителем Администрации. Форма приказа о назначении комиссии по уничтожению материальных носителей информации представлена в Приложении 4.

Уничтожение материальных носителей персональных данных осуществляется механическим либо электромагнитным воздействием с помощью специализированных средств (шредер, уничтожитель оптических дисков и т.п.). Отобранные к уничтожению материалы измельчаются механическим способом до степени, исключающей возможность прочтения текста или сжигаются.

Уничтожение производится по мере необходимости, в зависимости от объемов накопленных для уничтожения документов, а также с учетом установленных законодательством сроков уничтожения персональных данных.

По результатам уничтожения комиссией составляется акт уничтожения материальных носителей персональных данных (Приложение 5), уничтоженные материальные носители персональных данных снимаются с материального учета (делается запись в журналах их учета и регистрации). В номенклатурах и описях дел проставляется отметка «Уничтожено. Акт №__(дата)».

В случае если обработка персональных данных осуществляется оператором с использованием средств автоматизации, документами, подтверждающими уничтожение персональных данных субъектов персональных данных, являются акт об уничтожении персональных данных и выгрузка из журнала регистрации событий в информационной системе персональных данных (далее - выгрузка из журнала) (Приложение 6).

В порядке, установленном законодательством Российской Федерации, для уничтожения материальных носителей и информации на материальных носителях может привлекаться подрядная организация, имеющая необходимую производственную базу для обеспечения установленного порядка уничтожения документов и носителей. В этом случае, уполномоченное должностное лицо Администрации, сопровождает материальные носители, содержащие персональные данные, до производственной базы подрядчика и присутствует при процедуре уничтожения материальных носителей (например, сжигание или химическое уничтожение). После уничтожения материальных носителей, уполномоченным должностным лицом Администрации и подрядчиком подписывается соответствующий акт в трех экземплярах.

Приложение 1
к Порядку обращения, хранения и
уничтожения материальных носителей
персональных данных в ИСПДн

Журнал учета машинных носителей персональных данных
в ИСПДн
(типовая форма)

Начат «____» _____ 20__ г.
Окончен «____» _____ 20__ г.
На _____листах

_____ _____
должность и Ф.И.О. ответственного за ведение и хранение журнала Подпись

№ п/п	Регистрационный номер	Дата учета	Тип/емкость носителя	Серийный номер	Отметка о постановке на учет (ФИО, подпись, дата)	Отметка о снятии с учета (ФИО, подпись, дата)	Местоположение носителя	Сведения об уничтожении носителя /стирании информации

Приложение 2
к Порядку обращения, хранения и
уничтожения материальных носителей
персональных данных в ИСПДн

Журнал учета съемных машинных носителей персональных данных
в ИСПДн
(типовая форма)

Начат «____» _____ 20__ г.
Окончен «____» _____ 20__ г.
На _____листах

_____ _____
должность и Ф.И.О. ответственного за ведение и хранение журнала Подпись

№ п/п	Регистрационный номер	Дата учета	Тип/емкость носителя	Серийный номер	Кому выдан (ФИО, должность, наименование группы пользователей)	Отметка о выдаче (ФИО, подпись, дата)	Отметка о получении (ФИО, подпись, дата)	Местоположение носителя (№ кабинета)	Отметка об обратном приеме (ФИО, подпись, дата)	Сведения об уничтожении носителя /стирании информации (№ и дата акта)

Приложение 3
к Порядку обращения, хранения и
уничтожения материальных носителей
персональных данных в ИСПДн

Журнал учета бумажных носителей персональных данных
в ИСПДн
(типовая форма)

Начат «____» _____ 20__ г.
Окончен «____» _____ 20__ г.
На _____листах

_____ _____
должность и Ф.И.О. ответственного за ведение и хранение журнала Подпись

№ п/п	Учетный номер	Дата учета	Тип носителя	Кому выдан (ФИО, должность, наименование группы пользователей)	Отметка о выдаче (ФИО, подпись, дата)	Отметка о получении (ФИО, подпись, дата)	Местоположение носителя (№ кабинета)	Отметка об обратном приеме (ФИО, подпись, дата)	Сведения об уничтожении носителя (№ и дата акта)

Приложение 4
к Порядку обращения, хранения и
уничтожения материальных носителей
персональных данных в ИСПДн

РОССИЙСКАЯ ФЕДЕРАЦИЯ
РОСТОВСКАЯ ОБЛАСТЬ

Муниципальное образование «Краснолучское сельское поселение»
Администрация Краснолучского сельского поселения

РАСПОРЯЖЕНИЕ

№ _

__.__._____ х. Красный Луч

О назначении комиссии по уничтожению
персональных данных

Во исполнение Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», в соответствии с Требованиями к подтверждению уничтожения персональных данных, утвержденных приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных»:

1. Назначить комиссию в составе:

председателя - главы Администрации Краснолучского сельского поселения

членов комиссии: Заместителя главы Администрации Краснолучского сельского поселения по вопросам ЖКХ, строительства и благоустройства;

ведущего специалиста по организационно-кадровой работе Администрации Краснолучского сельского поселения

начальника службы экономики и финансов Администрации Краснолучского сельского поселения

2. По результатам работ предоставить для утверждения акт об уничтожении машинных носителей персональных данных.

3. Контроль за исполнением постановления возложить на

_____

(Фамилия, инициалы) *(Занимаемая должность)*

Глава Администрации
Краснолучского сельского поселения

Приложение 5
к Порядку обращения, хранения и
уничтожения материальных
носителей персональных данных в ИСПДн

РАЗРЕШАЮ УНИЧТОЖИТЬ
Глава Администрации Краснолучского сельского поселения

_____ _____

«_____» _____202__ г.

Акт
об уничтожении персональных данных[1]
(типовая форма)

Комиссия, назначенная распоряжением Администрации Краснолучского сельского поселения от _____ № ____, в составе:

	Должность	Ф.И.О.
Председатель		
Члены комиссии		

провела отбор материальных носителей (бумажных, электронных, магнитных, оптических) персональных данных и установила, что информация, записанная на них в процессе эксплуатации ИСПДн, подлежит уничтожению в соответствии с действующим законодательством Российской Федерации и требованиями руководящих документов по защите информации:

№№ п/п	Наименование (тип) уничтожаемого носителя, содержащего персональные данные субъекта	Регистрационный (учетный) номер носителя	Количество листов (машинных носителей, съемных машинных носителей)	Фамилия, имя, отчество (при наличии) субъекта (субъектов) или иная информация, относящаяся к определенному (определенным) физическому (физическим) лицу (лицам), чьи персональные данные были уничтожены	Перечень категорий персональных данных	Причина уничтожения персональных данных[2]	Примечание

[1] Форма акта уничтожения материальных носителей персональных данных (на бумажных и машинных носителях информации) в соответствии Требованиями к подтверждению уничтожения персональных данных, утвержденных приказом Федеральной службы по надзору Федеральной службы по надзору в сфере связи , информационных технологий и массовых коммуникаций от 28.10.2022 № 179

[2] ПДн должны (могут) быть уничтожены в следующих случаях: если они собраны незаконно, истекли установленные сроки хранения, достигнута или изменилась цель их сбора, а также по требованию самого владельца данных. Кроме того, может быть принято решение об уничтожении материальных носителей ПДн, пришедших в негодность

Всего носителей _____
(цифрами и прописью)

Персональные данные уничтожены путем _____.
(стирания информации на машинном носителе средством гарантированного уничтожения в составе СЗИ от НСД Dallas Lock 8.0-К, уничтожения бумажного (машинного) носителя посредством измельчения, сжигания и т.п.)

«____» _____202___ г.
(дата уничтожения носителей персональных данных)

Председатель комиссии: _____ / И.О.Фамилия/
Члены комиссии: _____ / И.О.Фамилия/
_____ / И.О.Фамилия/

Отметки о списании материальных носителей персональных данных в книгах и журналах учета произведены
Ответственный за ведение учета материальных носителей сведений персональных данных:

_____	_____	_____
(должность)	**(подпись)**	**(фамилия и инициалы)**
_____	_____	_____
(должность)	**(подпись)**	**(фамилия и инициалы)**

«_____» _____202____г.

Приложение 6
к Порядку обращения, хранения и
уничтожения материальных
носителей персональных данных в ИСПДн

РАЗРЕШАЮ УНИЧТОЖИТЬ
Глава Администрации Краснолучского сельского поселения

_____ _____
«_____» _____202__ г.

Акт
об уничтожении персональных данных[3]
(типовая форма)

Комиссия, назначенная распоряжением Администрации Краснолучского сельского поселения от _____ №____, в составе:

	Должность	Ф.И.О.
Председатель		
Члены комиссии		

провела проверку информационных систем персональных данных, а также машинных носителей информации, содержащих персональные данные, установила, что информация, записанная на них в процессе эксплуатации ИСПДн, подлежит уничтожению в соответствии с действующим законодательством Российской Федерации и требованиями руководящих документов по защите информации:

№ п/п	Наименование информационной (информационных) системы (систем) персональных данных, из которой (которых) были уничтожены персональные данные субъекта (субъектов) персональных данных	Регистрационный (учетный) номер носителя с которого произведено уничтожение (стирание) (при наличии)	Фамилия, имя, отчество (при наличии) субъекта (субъектов) или иная информация, относящаяся к определенному (определенным) физическому (физическим) лицу (лицам), чьи персональные данные были уничтожены	Перечень категорий персональных данных	Причина уничтожения персональных данных[4]	Примечание

[3] Форма акта уничтожения персональных данных в электронной форме в случае их обработки с использованием средств автоматизации в соответствии Требованиями к подтверждению уничтожения персональных данных, утвержденных приказом Федеральной службы по надзору Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 № 179

[4] ПДн должны (могут) быть уничтожены в следующих случаях: если они собраны незаконно, истекли сроки хранения, достигнута или изменилась цель их сбора, а также по требованию самого владельца данных.

Персональные данные уничтожены путем _____.
(стирания информации на машинном носителе средством гарантированного уничтожения (TERRIER, в составе СЗИ от НСД Dallas Lock 8.0-К или Secret Net, неоднократного форматирования (3 и более раз) и т.п.)
«____» _____202___ г.
(дата уничтожения (стирания) персональных данных) [5]

Приложение: Выгрузка из журнала регистрации событий в информационной системе персональных данных, на _____лист__.

Председатель комиссии: _____ / И.О.Фамилия/
Члены комиссии: _____ / И.О.Фамилия/
_____ / И.О.Фамилия/

[5] Дата уничтожения может быть вставлена в таблицу

Приложение
к Акту об уничтожении персональных данных

Выгрузка[6]
из журнала регистрации событий в информационной системе персональных данных

№№ п/п	Фамилия, имя, отчество (при наличии) субъекта (субъектов) или иная информация, относящаяся к определенному (определенным) физическому (физическим) лицу (лицам), чьи персональные данные были уничтожены	Перечень категорий уничтоженных персональных данных субъекта (субъектов) персональных данных	Наименование информационной системы персональных данных, из которой были уничтожены персональные данные субъекта (субъектов) персональных данных	Причину уничтожения персональных данных	Дата уничтожения персональных данных субъекта (субъектов) персональных данных	Примечание

Председатель комиссии: _____ / И.О.Фамилия/
Члены комиссии: _____ / И.О.Фамилия/
_____ / И.О.Фамилия/

[6] В случае если выгрузка из журнала не позволяет указать отдельные сведения, предусмотренные в таблице, недостающие сведения вносятся в акт об уничтожении персональных данных.

Приложение № 6
к распоряжению Администрации
Краснолучского сельского
поселения
от 01.07.2026 №23 ___

ИНСТРУКЦИЯ
пользователя информационных систем персональных данных по обеспечению безопасности персональных данных в Администрации Краснолучского сельского поселения

Общие положения

Пользователь информационной системы персональных данных (далее – Пользователь) осуществляет обработку персональных данных в информационных системах персональных данных в Администрации Краснолучского сельского поселения (далее – Администрация).

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.

Пользователь несет персональную ответственность за свои действия.

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.

Обязанности пользователя

Пользователь обязан:

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

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

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.

Соблюдать требования парольной политики (Раздел 3).

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

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).

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

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

Пользователям запрещается:

– разглашать защищаемую информацию третьим лицам;

– копировать защищаемую информацию на внешние носители без письменного разрешения руководителя структурного подразделения или Администрации;

– 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.

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>.

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

Организация парольной защиты

Пароли доступа к элементам информационной системы персональных данных создаются Администратором безопасности информационной системы персональных данных.

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

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.

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.).

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.

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.

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

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

При работе в Сети запрещается:

– осуществлять работу при отключенных средствах защиты (антивирус и других).

– передавать по Сети защищаемую информацию без использования средств шифрования;

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

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

– запрещается нецелевое использование подключения к Сети.

Действия при обнаружении попыток несанкционированного доступа

При несанкционированном доступе к персональным данным (ПДн), а именно:

– выявление (обнаружение) сеансов работы с персональными данными незарегистрированных пользователей или пользователей, нарушивших

установленный порядок доступа, или превышающих свои полномочия по доступу к данным;

– выявление (обнаружение) действий постороннего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учётной записи пользователя ИСПДн, методом подбора пароля, использования пароля, разглашенного владельцем учётной записи или любым другим методом.

Пользователь обязан:

– известить администратора безопасности о факте несанкционированного доступа, от имени учётной записи, которого была осуществлена попытка;

– доложить ответственному за организацию обработки персональных данных Администрации о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях.

Ответственность

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

Приложение № 7
к распоряжению Администрации
Краснолучского сельского
поселения
от 01.07.2026 №23 ___

ПОЛОЖЕНИЕ
об обработке персональных данных в Администрации Краснолучского сельского поселения

1. Общие положения

Настоящее Положение об обработке персональных данных (далее — Положение) в Администрации Краснолучского сельского поселения (далее – Администрация) разработано в соответствии с Конституцией Российской Федерации, Федеральным законом «Об информации, информационных технологиях и о защите информации», Федеральным законом «О персональных данных».

1.1. 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.

1.2. Порядок ввода в действие и изменения Положения.

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

1.2.2. Все изменения в Положение вносятся распоряжениями главы Администрации.

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

1.4. 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 прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных;

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

– **оператор** - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

– **обработка персональных данных** - любое действие (операция) или совокупность действий (операций), 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;

– **автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;

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

– **предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

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

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

– **обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

– **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;

– **информационная система персональных данных** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

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

– **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 субъекте, в том числе о его фамилии, имени, отчестве, годе, месяце, дате и месте рождения, адресе, семейном, социальном, имущественном положении, образовании, профессии, доходах, паспортных данных, образовании, отношении к воинской обязанности, состоянии здоровья и другой информации, позволяющей 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, в целях обеспечения кадровой работы, в том числе в целях содействия сотруднику в прохождении гражданской (муниципальной) службы, обучении и должностном росте, обеспечения личной безопасности гражданского (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.

Персональные данные сотрудников обрабатываются до момента увольнения. Документы по личному составу, законченные делопроизводством до 1 января 2003 года, хранятся 75 лет, а документы по личному составу, законченные делопроизводством после 1 января 2003 года, хранятся 50 лет, после чего передаются на постоянное хранение в государственные архивные

фонды в соответствии со ст. 22.1 Федерального закона от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации».

Обработка персональных данных жителей района осуществляется в целях предоставления государственных и муниципальных услуг и исполнения муниципальных функций в соответствии с порядком работы с обращениями граждан в Администрации, утвержденными распоряжениями Администрации.

Персональные данные граждан, обратившихся в Администрацию лично, а также направивших индивидуальные или коллективные письменные обращения или обращения в форме электронного документа, обрабатываются в целях рассмотрения указанных обращений с последующим уведомлением заявителей о результатах рассмотрения.

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

Состав обрабатываемых персональных данных определяется в соответствии с перечнем персональных данных, обрабатываемых в Администрации Краснолучского сельского поселения Ростовской области (Приложение 1 к данному Положению).

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 Краснолучского сельского поселения Ростовской области (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 ст. 6 ФЗ-152 «О персональных данных» сотрудники Администрации при обработке персональных данных должны соблюдать следующие общие требования:

Обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных (Приложение 4 к данному Положению).

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.

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 27.07.2010 № 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.

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.

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.

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

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

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

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

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

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

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

– в иных случаях, предусмотренных частью 2 ст. 10 ФЗ-152 «О персональных данных».

Обработка персональных данных о судимости может осуществляться в случаях и в порядке, которые определяются в соответствии с федеральными законами.

Обработка специальных категорий персональных данных, осуществлявшаяся в случаях, предусмотренных в настоящем пункте, должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка, если иное не установлено федеральным законом.

4.2.4. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 ст. 11 ФЗ 10 ФЗ-152 «О персональных данных».

4.2.5. Автоматизированная обработка персональных данных разрешается в информационных системах персональных данных перечисленных в перечне информационных систем персональных данных, принадлежащих Администрации (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 нормативно-правовыми актами по защите информации.

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

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

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

6. Уничтожение персональных данных

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

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

документы, черновики документов, испорченные листы, варианты и неподписанные проекты документов уничтожаются 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 Краснолучского сельского поселения.

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.

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

8. Распространение персональных данных, в том числе в общедоступных источниках

В целях информационного обеспечения в Администрации могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги и т.п.). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных.

Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных (Приложение 4 к настоящему Положению). Администрация обязана обеспечить субъекту персональных данных возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

В случае раскрытия персональных данных неопределенному кругу лиц самим субъектом персональных данных без предоставления Администрации согласия, предусмотренного пунктом 8.3. Положения, обязанность

предоставить доказательства законности последующего распространения или иной обработки таких персональных данных лежит на каждом лице, осуществившем их распространение или иную обработку.

В случае, если персональные данные оказались раскрытыми неопределенному кругу лиц вследствие правонарушения, преступления или обстоятельств непреодолимой силы, обязанность предоставить доказательства законности последующего распространения или иной обработки таких персональных данных лежит на каждом лице, осуществившем их распространение или иную обработку.

В случае, если из предоставленного субъектом персональных данных согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, не следует, что субъект персональных данных согласился с распространением персональных данных, такие персональные данные обрабатываются Администрацией, без права распространения.

В случае, если из предоставленного субъектом персональных данных согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, не следует, что субъект персональных данных не установил запреты и условия на обработку персональных данных, предусмотренные пунктом 8.10 настоящего Положения, или если в предоставленном субъектом персональных данных таком согласии не указаны категории и перечень персональных данных, для обработки которых субъект персональных данных устанавливает условия и запреты в соответствии пунктом 8.10 Положения, такие персональные данные обрабатываются без передачи (распространения, предоставления, доступа) и возможности осуществления иных действий с персональными данными неограниченному кругу лиц.

Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, может быть предоставлено:

– непосредственно;

– использованием информационной системы уполномоченного органа по защите прав субъектов персональных данных.[7]

Молчание или бездействие субъекта персональных данных ни при каких обстоятельствах не может считаться согласием на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

В согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения, субъект персональных данных

---

[7] Правила использования информационной системы уполномоченного органа по защите прав субъектов персональных данных, в том числе порядок взаимодействия субъекта персональных данных с оператором, определены приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 21 июня 2021 г. № 106 "Об утверждении Правил использования информационной системы Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, в том числе порядка взаимодействия субъекта персональных данных с оператором"

вправе установить запреты на передачу (кроме предоставления доступа) этих персональных данных Администрацией неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц. Отказ в установлении субъектом персональных данных запретов и условий, предусмотренных настоящим пунктом, не допускается.

Администрация (оператор) обязана в срок не позднее трех рабочих дней с момента получения соответствующего согласия субъекта персональных данных опубликовать информацию об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных, разрешенных субъектом персональных данных для распространения.

Установленные субъектом персональных данных запреты на передачу (кроме предоставления доступа), а также на обработку или условия обработки (кроме получения доступа) персональных данных, разрешенных субъектом персональных данных для распространения, не распространяются на случаи обработки персональных данных в государственных, общественных и иных публичных интересах, определенных законодательством Российской Федерации.

Передача (распространение, предоставление, доступ) персональных данных, разрешенных субъектом персональных данных для распространения, должна быть прекращена в любое время по требованию субъекта персональных данных. Данное требование должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) субъекта персональных данных, а также перечень персональных данных, обработка которых подлежит прекращению. Указанные в данном требовании персональные данные могут обрабатываться только оператором, которому оно направлено.

Действие согласия субъекта персональных данных на обработку персональных данных, разрешенных субъектом персональных данных для распространения, прекращается с момента поступления в Администрацию требования, указанного в 8.13 Положения.

Субъект персональных данных вправе обратиться с требованием прекратить передачу (распространение, предоставление, доступ) своих персональных данных, ранее разрешенных субъектом персональных данных для распространения, к любому лицу, обрабатывающему его персональные данные, в случае несоблюдения положений настоящего пункта или обратиться с таким требованием в суд. Данное лицо обязано прекратить передачу (распространение, предоставление, доступ) персональных данных в течение трех рабочих дней с момента получения требования субъекта персональных данных или в срок, указанный во вступившем в законную силу решении суда, а если такой срок в решении суда не указан, то в течение трех рабочих дней с момента вступления решения суда в законную силу.

9. Правила работы с обезличенными данными

9.1. 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).

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

9.2. 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).

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

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

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, назначаемой руководителем Администрации не реже одного раза в 3 года.

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;

правильности 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;

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

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

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

соблюдения обязанностей Администрации, 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;

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

актуальности сведений, содержащихся в уведомлении Администрации об обработке персональных данных;

актуальности перечня информационных систем персональных данных в Администрации;

наличия и актуальности сведений, содержащихся в Правилах обработки персональных данных для каждой информационной системы персональных данных Администрации;

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

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

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

соблюдения сотрудниками Администрации конфиденциальности персональных данных;

актуальности локальных актов Администрации в области обеспечения безопасности персональных данных, в том числе в технических паспортах информационных систем персональных данных (при их наличии);

соблюдения сотрудниками Администрации требований по обеспечению безопасности персональных данных;

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

иных вопросов.

10.1. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, генеральному директору Администрации докладывает ответственный за организацию обработки персональных данных, либо председатель комиссии.

11. Права субъекта персональных данных

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

11.2. 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.

11.3. 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 ФЗ-№ 152 «О персональных данных»;

информацию об осуществленной или о предполагаемой трансграничной передаче данных;

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

иные сведения, предусмотренные ФЗ-№ 152 «О персональных данных» или другими федеральными законами.

11.4. 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.

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

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.

Приложение 1
к Положению об обработке персональных данных в Администрации Краснолучского сельского поселения

ПЕРЕЧЕНЬ
персональных данных, обрабатываемых в Администрации Краснолучского сельского поселения

В Администрации Краснолучского сельского поселения Ростовской области (далее – Администрация) обрабатывается следующий перечень персональных данных:

Персональные данные муниципальных служащих Администрации, членов их семей, лиц, претендующих на замещение должностей муниципальной службы в Администрации, членов их семей; иных сторонних лиц, обработка персональных данных которых осуществляется Администрацией в соответствии с законодательством Российской Федерации, законодательством Ростовской области и муниципальными нормативными правовыми актами Краснолучского сельского поселения.

1. Персональные данные главы Администрации (далее – выборного должностного лица), муниципальных служащих, замещающих должности муниципальной службы в Администрации (далее соответственно – муниципальные служащие, муниципальная служба), лиц, претендующих на замещение должностей муниципальной службы в Администрации, включают в себя следующую информацию:

1) фамилия, имя, отчество (в том числе предыдущие фамилия, имя, отчество в случае (ях) их изменения);

2) дата и место рождения;

3) гражданство (подданство) (в том числе предыдущее в случае (ях) его изменения), вид на жительство или иной документ, подтверждающий право на постоянное проживание гражданина Российской Федерации на территории иностранного государства);

4) паспортные данные (вид паспорта, серия, номер, кем и когда выдан);

5) адрес места жительства (адрес регистрации, адрес фактического проживания);

6) номер контактного телефона или сведения о других способах связи;

7) фотография;

8) сведения о семейном положении, о составе семьи, близких родственниках, свойственниках, о наличии иждивенцев;

9) сведения об образовании и (или) о квалификации (наименование и год окончания образовательной организации, наименование и реквизиты документа об образовании и о квалификации, документа о квалификации, подтверждающего повышение или присвоение квалификации по результатам дополнительного профессионального образования);

10) сведения о присвоении ученой степени, ученого звания;

11) сведения о трудовой деятельности;

12) страховой номер индивидуального лицевого счета;

13) идентификационный номер налогоплательщика;

14) номер страхового медицинского полиса обязательного медицинского страхования;

15) результаты психологического тестирования;

16) сведения о наличии государственных и иных наград;

17) сведения о воинском учете и реквизиты документов воинского учета;

18) информация о классном чине государственной гражданской службы Российской Федерации (в том числе дипломатическом ранге, воинском или специальном звании, классном чине юстиции, классном чине прокурорских работников, классном чине гражданской службы субъекта Российской Федерации), квалификационном разряде государственной гражданской службы (квалификационном разряде или классном чине муниципальной службы);

19) сведения о наличии или отсутствии судимости;

20) сведения об оформленных допусках к государственной тайне;

21) сведения о пребывании за границей Российской Федерации;

22) сведения о доходах, об имуществе и обязательствах имущественного характера, сведения о расходах;

23) медицинское заключение по установленной форме об отсутствии у гражданина заболевания, препятствующего поступлению на муниципальную службу или ее прохождению;

24) медицинское заключение по установленной форме об отсутствии медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну (при оформлении допуска к сведениям, составляющим государственную тайну);

25) документы, подтверждающие принадлежность налогоплательщика к категориям граждан, перечисленным в статье 218 Налогового кодекса Российской Федерации;

26) сведения о размере денежного содержания и иных выплат;

27) информация о ежегодных оплачиваемых отпусках, и иных отпусках в соответствии с законодательством Российской Федерации;

28) номер расчетного счета;

29) номер банковской карты;

30) информация, содержащаяся в трудовом договоре, дополнительных соглашениях к трудовому договору;

31) иные персональные данные, необходимые для достижения целей обработки персональных данных, предусмотренных положением об организации работы с персональными данными в Администрации Краснолучского сельского поселения, утверждаемым распоряжением Администрации Краснолучского сельского поселения.

2. Персональные данные членов семей выборного должностного лица, муниципальных служащих Администрации, лиц, претендующих на замещение должностей муниципальной службы в Администрации, членов семей муниципальных служащих в структурных подразделениях и членов семей лиц, претендующих на замещение должностей муниципальной службы в структурных подразделениях, включают в себя следующую информацию:

1) фамилия, имя, отчество (в том числе предыдущие фамилия, имя, отчество в случае (ях) их изменений);

2) дата и место рождения;

2[1]) данные свидетельства о рождении несовершеннолетнего ребенка, не имеющего паспорта (серия, номер, кем и когда выдано);

3) паспортные данные (вид паспорта, серия, номер, кем и когда выдан);

4) адрес места жительства (адрес регистрации, адрес фактического проживания);

5) сведения о семейном положении, о наличии детей;

6) место работы (наименование и адрес организации, занимаемая должность; в случае отсутствия основного места работы или службы - род занятий);

6[1]) страховой номер индивидуального лицевого счета;

7) сведения о доходах, об имуществе и обязательствах имущественного характера, а также о расходах (супруги (супруга) и несовершеннолетних детей);

8) иные персональные данные, необходимые для достижения целей обработки персональных данных, предусмотренных положением об организации работы с персональными данными в Администрации Краснолучского сельского поселения, утверждаемым распоряжением Администрации Краснолучского сельского поселения.

3. Персональные данные иных сторонних лиц, обрабатываемые в соответствии с законодательством Российской Федерации, законодательством Ростовской области и муниципальными нормативными правовыми актами Краснолучского сельского поселения в рамках:

1) обеспечения реализации полномочий по представлению к государственным наградам Российской Федерации и наградам Ростовской области в соответствии с законодательством Российской Федерации и законодательством Ростовской области - включают в себя следующую информацию:

а) фамилия, имя, отчество;

б) дата и место рождения;

в) паспортные данные (вид паспорта, серия, номер, кем и когда выдан);

г) адрес места жительства (адрес регистрации, адрес фактического проживания);

д) место работы (наименование и адрес организации, занимаемая должность; в случае отсутствия основного места работы или службы - род занятий);

е) сведения о присвоении ученой степени, ученого звания;

ж) сведения о трудовой деятельности;

з) сведения о наличии государственных и иных наград;

и) информация о классном чине государственной гражданской службы Российской Федерации (в том числе дипломатическом ранге, воинском или специальном звании, классном чине правоохранительной службы, классном чине гражданской службы субъекта Российской Федерации), квалификационном разряде государственной гражданской службы (квалификационном разряде или классном чине муниципальной службы);

2) обеспечения реализации администрацией Краснолучского сельского поселения Ростовской области полномочий по осуществлению закупок товаров, работ, услуг для обеспечения муниципальных нужд Краснолучского сельского поселения Ростовской области, по которым она выступает заказчиком в соответствии с Федеральным законом «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» - включают в себя следующую информацию:

а) фамилия, имя, отчество;

б) паспортные данные (вид паспорта, серия, номер, кем и когда выдан);

в) адрес места жительства;

г) номер контактного телефона;

д) идентификационный номер налогоплательщика;

е) сведения об образовании и (или) о квалификации (наименование и год окончания образовательной организации, наименование и реквизиты документа об образовании и о квалификации, документа о квалификации, подтверждающего повышение или присвоение квалификации по результатам дополнительного профессионального образования);

3) осуществления работы по рассмотрению обращений граждан и организации личного приема граждан - включают в себя следующую информацию:

а) фамилия, имя, отчество (последнее при наличии);

б) почтовый адрес;

в) адрес электронной почты;

г) указанный в обращении контактный телефон;

д) иные персональные данные, указанные заявителем в обращении (жалобе), а также ставшие известными в ходе личного приема или в процессе рассмотрения поступившего обращения;

4) осуществления полномочий по решению вопросов местного значения, а также отдельных государственных полномочий, переданных администрации Краснолучского сельского поселения Ростовской области, включают в себя следующую информацию:

а) фамилия, имя, отчество;

б) дата и место рождения;

в) паспортные данные (вид паспорта, серия, номер, кем и когда выдан);

г) адрес места жительства (адрес регистрации, адрес фактического проживания);

д) место работы (наименование и адрес организации, занимаемая должность; в случае отсутствия основного места работы или службы - род занятий);

е) сведения о трудовой деятельности;

ж) сведения о национальности;

з) сведения о совершенном правонарушении;

и) сведения об алиментах;

к) сведения о лишении родительских прав.

5) предоставления государственных и муниципальных услуг в соответствии с Федеральным законом от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» включают в себя следующую информацию:

а) фамилия, имя, отчество;

б) дата и место рождения;

в) паспортные данные (вид паспорта, серия, номер, кем и когда выдан);

г) адрес места жительства (адрес регистрации, адрес фактического проживания);

д) место работы (наименование и адрес организации, занимаемая должность; в случае отсутствия основного места работы или службы - род занятий);

е) сведения о трудовой деятельности;

ж) номер контактного телефона или сведения о других способах связи.

6) при осуществлении деятельности по регистрации (учету) избирателей, участников референдума на территории Краснолучского сельского поселения включают в себя следующую информацию:

а) фамилия, имя, отчество;

б) дата и место рождения;

в) паспортные данные (вид паспорта, серия, номер, кем и когда выдан);

г) адрес регистрации.

Примечание. Сведения, о наличии или об отсутствии судимости, указанные в подпункте «19» пункта 1 настоящего Приложения, а также сведения, содержащиеся в медицинских заключениях по установленной форме об отсутствии у гражданина заболевания, препятствующего поступлению на муниципальную службу или ее прохождению, и об отсутствии медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну (при оформлении допуска к сведениям, составляющим государственную тайну), указанных в подпунктах «23» и «24» пункта 1 настоящего Приложения, в информационных системах, используемых при обработке персональных данных в Администрации, не обрабатываются.

Приложение 2
к Положению об обработке персональных данных в Администрации Краснолучского сельского поселения Ростовской области

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 Краснолучского сельского поселения

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

1. Глава Администрации Краснолучского сельского поселения.
2. Заместитель главы Администрации Краснолучского сельского поселения по вопросам ЖКХ, строительства и благоустройства.
3. Начальник финансово-экономической службы Администрации Краснолучского сельского поселения.
4. Главный бухгалтер Администрации Краснолучского сельского поселения.
5. Ведущий специалист экономист Администрации Краснолучского сельского поселения.
6. Ведущий специалист по организационно-кадровой работе Администрации Краснолучского сельского поселения.
7. Ведущий специалист по правовой работе Администрации Краснолучского сельского поселения.
8. Старший инспектор по земельным и имущественным отношениям Администрации Краснолучского сельского поселения.
9. Старший инспектор по муниципальному земельному контролю Администрации Краснолучского сельского поселения.
10. Старший инспектор по работе с молодежью, культуре и спорту Администрации Краснолучского сельского поселения.
11. Инспектор по архивной работе и работе с населением Администрации Краснолучского сельского поселения.
12. Инспектор - системный администратор Администрации Краснолучского сельского поселения.
13. Инспектор по пожарной безопасности Администрации Краснолучского сельского поселения.

Приложение 3
к Положению об обработке персональных данных в Администрации Краснолучского сельского поселения

ОБЯЗАТЕЛЬСТВО
о неразглашении персональных данных в Администрации Краснолучского сельского поселения

Я, _____
(ФИО сотрудника)

Паспорт серия _____ номер _____ выдан _____

_____

исполняющий(ая) должностные обязанности _____
(должность)

предупрежден(а) о том, что на период исполнения мною должностных обязанностей, мне будет предоставлен доступ к персональным данным.

Настоящим добровольно принимаю на себя обязательства:

1. Не передавать в любом виде и не разглашать третьим лицам и работникам Администрации Краснолучского сельского поселения, не имеющим на это право в силу выполняемых ими должностных обязанностей или в соответствии с решением руководителя, информацию содержащую персональные данные (за исключением собственных данных), которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей;

2. В случае попытки третьих лиц или работников Администрации Краснолучского сельского поселения, не имеющих на это право, получить от меня информацию, содержащую персональные данные, немедленно сообщить об этом факте своему непосредственному или (в случае отсутствия непосредственного) вышестоящему руководителю;

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

4. Выполнять требования закона и иных нормативных правовых актов Российской Федерации, а также внутренних документов администрации Краснолучского сельского поселения Ростовской области, регламентирующих вопросы защиты интересов субъектов персональных данных, порядка обработки и защиты персональных данных;

5. После прекращения моих прав на доступ к информации, содержащей персональные данные (переход на должность, не предусматривающую доступ к персональным данным либо прекращения Трудового договора), не обрабатывать, не разглашать и не передавать третьим лицам и неуполномоченным на это работникам Администрации Краснолучского сельского поселения, известную мне информацию, содержащую персональные данные.

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

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

Приложение № 4
к Положению об обработке персональных данных в Администрации Краснолучского сельского поселения

ТИПОВАЯ ФОРМА
согласия на обработку персональных данных работника (муниципального служащего) Администрации Краснолучского сельского поселения

Я, _____
(Ф.И.О. полностью)

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

с целью исполнения определенных сторонами условий трудового договора (трудоустройства) даю согласие Администрации Краснолучского сельского поселения, расположенной по адресу: 346488, Ростовская область, Октябрьский район, рх. Красный Луч, ул. Центральная, д. 58, на обработку нижеследующих персональных данных:

- фамилия, имя, отчество (в том числе предыдущие фамилия, имя, отчество в случае (ях) их изменения);
- дата и место рождения;
- гражданство (подданство) (в том числе предыдущее в случае (ях) его изменения), вид на жительство или иной документ, подтверждающий право на постоянное проживание гражданина Российской Федерации на территории иностранного государства);
- паспортные данные (вид паспорта, серия, номер, кем и когда выдан);
- адрес места жительства (адрес регистрации, адрес фактического проживания);
- номер контактного телефона или сведения о других способах связи;
- фотография;
- сведения о семейном положении, о составе семьи, близких родственниках, свойственниках, о наличии иждивенцев;
- сведения об образовании и (или) о квалификации (наименование и год окончания образовательной организации, наименование и реквизиты документа об образовании и о квалификации, документа о квалификации, подтверждающего повышение или присвоение квалификации по результатам дополнительного профессионального образования);
- сведения о присвоении ученой степени, ученого звания;
- сведения о трудовой деятельности;
- страховой номер индивидуального лицевого счета;

- идентификационный номер налогоплательщика;
- номер страхового медицинского полиса обязательного медицинского страхования;
- результаты психологического тестирования;
- сведения о наличии государственных и иных наград;
- сведения о воинском учете и реквизиты документов воинского учета;
- информация о классном чине государственной гражданской службы Российской Федерации (в том числе дипломатическом ранге, воинском или специальном звании, классном чине юстиции, классном чине прокурорских работников, классном чине гражданской службы субъекта Российской Федерации), квалификационном разряде государственной гражданской службы (квалификационном разряде или классном чине муниципальной службы);
- сведения о наличии или отсутствии судимости;
- сведения об оформленных допусках к государственной тайне;
- сведения о пребывании за границей Российской Федерации;
- сведения о доходах, об имуществе и обязательствах имущественного характера, сведения о расходах;
- медицинское заключение по установленной форме об отсутствии у гражданина заболевания, препятствующего поступлению на муниципальную службу или ее прохождению;
- медицинское заключение по установленной форме об отсутствии медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну (при оформлении допуска к сведениям, составляющим государственную тайну);
- документы, подтверждающие принадлежность налогоплательщика к категориям граждан, перечисленным в статье 218 Налогового кодекса Российской Федерации;
- сведения о размере денежного содержания и иных выплат;
- информация о ежегодных оплачиваемых отпусках, и иных отпусках в соответствии с законодательством Российской Федерации;
- номер расчетного счета;
- номер банковской карты;
- информация, содержащаяся в трудовом договоре, дополнительных соглашениях к трудовому договору;
- иные персональные данные, необходимые для достижения целей обработки персональных данных, предусмотренных положением об организации работы с персональными данными в Администрации Краснолучского сельского поселения, утверждаемым распоряжением Администрации Краснолучского сельского поселения.

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

(указать, в какие организации будут передаваться персональные данные)

_____

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

Данное согласие может быть отозвано по моему письменному заявлению.

_____ _____

(число, месяц, год) (подпись)

Приложение 5
к Положению об обработке
персональных данных в
Администрации Краснолучского
сельского поселения

ПЕРЕЧЕНЬ
информационных систем персональных данных, принадлежащих Администрации Краснолучского сельского поселения

В Администрации Краснолучского сельского поселения функционируют следующие информационные системы персональных данных (ИСПДн):

1. АРМ «Руководство Администрации».
2. АРМ «Бухгалтерия».
3. Официальный сайт.

Приложение 6
к Положению об обработке
персональных данных в
Администрации Краснолучского
сельского поселения

РАЗЪЯСНЕНИЕ
юридических последствий отказа субъекта персональных данных представить свои персональные данные и (или) дать согласие на их обработку
(типовая форма)

1. В соответствии с требованиями Федерального закона «О персональных данных» уведомляем Вас, что в случае Вашего отказа представить свои персональные данные и (или) дать согласие на их обработку Администрации Краснолучского сельского поселения (далее - Администрация) не сможет на законных основаниях осуществлять обработку Ваших персональных данных, что приведет к невозможности

_____
(указать конкретные последствия отказа в представлении персональных данных:

_____
невозможность поступления на муниципальную должность муниципальной службы

_____
Ростовской области в Администрации (далее – должность муниципальной

_____
службы),

1. В соответствии со статьями 57, 65 Трудового кодекса РФ субъект персональных данных, поступающий на работу, обязан предоставить определённый перечень персональных данных. Без предоставления персональных данных, необходимых для заключения трудового договора, субъекту персональных данных будет отказано в приёме на работу.

В случае непредставления гражданином персональных данных требуемых для предоставления государственных и муниципальных услуг, ему будет отказано в предоставлении такой услуги.

В случае непредставления гражданином персональных данных требуемых для постановки на военный учёт, ему будет отказано в постановке на учёт, что в свою очередь влечёт ответственность в соответствии с действующим законодательством.

В случае непредставления субъектом персональных данных, требуемых для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, в том числе в случае реализации оператором своего права на уступку прав (требований) по такому договору, а также для заключения договора по инициативе субъекта

персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем, данный договор заключен не будет.

2. В соответствии с законодательством Российской Федерации в области персональных данных Вы имеете право:

1) на получение сведений об Администрации, о месте его нахождения, о наличии в Администрации Ваших персональных данных, а также на ознакомление с такими персональными данными;

2) требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются соответственно неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законодательством Российской Федерации меры по защите своих прав;

3) на получение при обращении или при направлении запроса информации, касающейся обработки своих персональных данных;

4) на обжалование действия или бездействия Администрации в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

"___"_____ 20___ г. _____ _____

(подпись) (расшифровка подписи)

Приложение № 8
к распоряжению Администрации
Краснолучского сельского
поселения
от 01.07.2026 №23 ___

ПОРЯДОК
доступа сотрудников Администрации Краснолучского сельского поселения 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 Краснолучского сельского поселения (далее – Администрация), разработан 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 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

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 руководителем 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.

2.3. В нерабочее время, перед выходными и праздничными днями помещения опечатываются и сдаются под охрану. Ключи сдаются под роспись в журнале приема (сдачи) под охрану помещений, хранилищ, сейфов.

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.

Приложение № 9

к распоряжению Администрации
Краснолучского сельского
поселения
от 01.07.2026 №23 ___

ПРАВИЛА
работы с обезличенными персональными данными в Администрации Краснолучского сельского поселения

1. Общие положения

1.1. Настоящие Правила работы с обезличенными персональными данными в Администрации Краснолучского сельского поселения (далее – Администрация) разработаны в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

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

Приложение № 10

к распоряжению Администрации
Краснолучского сельского
поселения
от 01.07.2026 №23 ___

РЕГЛАМЕНТ
порядка действий сотрудников Администрации Краснолучского сельского поселения 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 РФ от 27.07.2006 № 152-ФЗ «О персональных данных».

Целью настоящего Регламента является:

обеспечение прав субъектов персональных данных на доступ к их персональным данным, которые обрабатываются в администрации Краснолучского сельского поселения (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 РФ от 27.07.2006 № 152-ФЗ «О персональных данных».

Общие положения

Настоящий Регламент использует следующие сокращения:

ПДн – персональные данные;

ИСПДн – информационная система персональных данных.

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

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.

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

В соответствии со ст. 14 Федерального закона РФ от 27.07.2006 № 152-ФЗ «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.

В соответствии со ст. 9 Федерального закона РФ от 27.07.2006 № 152-ФЗ «О персональных данных» субъект ПДн имеет право отозвать свое согласие на обработку ПДн.

В соответствии со ст.ст. 14, 20, 21 Федерального закона РФ 27.07.2006 № 152-ФЗ «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 ст. 14 Федерального закона РФ от 27.07.2006 № 152-ФЗ «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.

В соответствии с п. 3 ч. 5 ст. 14 Федерального закона РФ от 27.07.2006 № 152-ФЗ «О персональных данных» право субъекта ПДн на доступ к своим ПДн ограничивается в случае, если предоставление ПДн нарушает конституционные права и свободы других лиц.

Действия сотрудников Администрации при получении запроса субъекта ПДн

В соответствии с ч. 3 ст. 14 Федерального закона РФ от 27.07.2006 № 152-ФЗ «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.

В целях регистрации запросов субъектов ПДн и ответов на такие запросы в Администрации осуществляется ведение журнала регистрации запросов субъектов ПДн (приложение 1).

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

При получении запроса (обращения) физического лица, сотрудник Администрации, ответственный за прием и регистрацию входящей корреспонденции в Администрации, непосредственно в день получения устанавливает:

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;

Содержит ли почтовый адрес, по которому должен быть направлен

ответ;

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

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;

Отвечает ли такой запрос (обращение) требованиям, установленным ст. 14 Федерального закона РФ от 27.07.2006 № 152-ФЗ «О персональных данных», к запросу субъекта ПДн.

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.

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.

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

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.

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.

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.

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 п. 4 ч. 8 ст. 14 Федерального закона РФ от 27.07.2006 № 152-ФЗ «О персональных данных».

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

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

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

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 п. 2.3.

Администрация, в лице сотрудников, указанных в п. 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.

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 п. 4 настоящего Регламента для соответствующих действий (операций) в отношении ПДн (приложение 2).

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

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

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

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.

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

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.

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

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

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

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

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 порядка действий сотрудников Администрации Краснолучского сельского поселения при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных

ЖУРНАЛ
обращений субъектов персональных данных
№ _____

количество листов_____

начат_____

окончен_____

№ п.п.	ФИО субъекта персональных данных или его законного представителя	Входящий номер, дата обращения субъекта персональных данных	Исходящий номер, дата ответа на запрос субъекта персональных данных
1.	2.	3.	4.
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			

Приложение 2
к Регламенту порядка действий сотрудников Администрации Краснолучского сельского поселения при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных

Отзыв согласия на обработку персональных данных

«_____» _____ 202__ г.

Настоящим во исполнение положений Федерального закона РФ от 27.07.2006 № 152-ФЗ «О персональных данных» **я,**

_____
(фамилия, имя, отчество)

_____
(серия, номер паспорта, кем выдан)

_____
(место регистрации)

отзываю у Администрации Краснолучского сельского поселения свое **согласие на обработку персональных данных**. **Прошу прекратить обработку персональных данных** не позднее трех рабочих дней с даты поступления настоящего Отзыва, а также уничтожить всю персональную информацию, касающуюся меня лично.

Ф.И.О. Подпись

Приложение 3
к Регламенту порядка действий сотрудников Администрации Краснолучского сельского поселения при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных

Форма 1 «Запрос субъекта ПДн»

Главе Администрации
Краснолучского сельского поселения
_____

От
Паспорт серия номер

(Когда и кем выдан)

Проживающего по адресу:

Контактный номер телефона

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

1. Какова цель обработки моих персональных данных в Администрации Краснолучского сельского поселения?
2. Каковы способы обработки моих персональных данных, применяемые в Администрации Краснолучского сельского поселения, 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 Краснолучского сельского поселения, 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 4 к Регламенту порядка действий сотрудников Администрации Краснолучского сельского поселения при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных

Форма 2 «Ответ на запрос субъекта ПДн»

Исх №	От

Фамилия Имя Отчество
Адрес

Уважаемый _____!

Руководствуясь положениями ст. ст. 14, 20 Федерального закона РФ «О персональных данных» от 27 июля 2006 г. № 152-ФЗ сообщаем Вам, что Администрация Краснолучского сельского поселения 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;
Должность3.

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:

_____.

6. Источник получения персональных данных – _____.

7. Срок обработки Ваших персональных данных – _____.

8. Обработка Ваших персональных данных может повлечь следующие

юридические последствия –
_____.

_____

Фамилия И.О. (Подпись) (Дата)

Приложение 5
к Регламенту порядка действий сотрудников администрации Краснолучского сельского поселения при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных

Пример ответа на запрос субъекта ПДн

Исх. № __ от __.__.20__ г.

Иванову Ивану Ивановичу
Адрес

Уважаемый Иван Иванович!

Руководствуясь положениями ст. ст. 14, 20 Федерального закона РФ «О персональных данных» от 27 июля 2006 г. № 152-ФЗ сообщаем Вам, что Администрация Краснолучского сельского поселения обрабатывает Ваши персональные данные

1. Цель обработки Ваших персональных – бухгалтерский и кадровый учет, регистрация сведений, необходимых для оказания муниципальных услуг

2. Способы обработки Ваших персональных данных – смешанная обработка.

3. Лица, имеющие доступ к Вашим персональным данным:

Главный специалист;

Ведущий специалист.

4. Доступ к Вашим персональным данным может быть предоставлен заместителю главы. 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: фамилия, имя, отчество, серия и номер паспорта, дата рождения, адрес места рождения, адрес места жительства/прописки, ИНН, СНИЛС, номер телефона, семейное положение, состав семьи, образование, профессия, должность, стаж, сведения о воинской обязанности, сведения об имуществе, национальность. Источник получения персональных данных – документы, предъявляемые Вами при устройстве на работу.

6. Срок обработки Ваших персональных данных – до момента Вашего увольнения, до момента прекращения оказания Вам муниципальных услуг.

7. Обработка Ваших персональных данных влечет для Вас в качестве юридических последствий возникновение у Вас прав, присущих субъекту ПДн и предусмотренных ст. 14 ФЗ «О персональных данных», а именно: право на доступ к своим ПДн, право на получение сведений об операторе, право требовать уточнения, блокирования или уничтожения ПДн, право отозвать согласие на обработку ПДн и т.п.

Фамилия И.О.	(Подпись)	(Дата)

Приложение № 11
к распоряжению Администрации
Краснолучского сельского
поселения
от 01.07.2026 №23 ___

ПОЛИТИКА
обработки персональных данных в Администрации Краснолучского сельского поселения

1. Общие положения

1.1. Политика обработки персональных данных в Администрации Краснолучского сельского поселения (далее – Политика) определяет основные принципы, цели, условия и способы обработки персональных данных, перечни субъектов и обрабатываемых в Администрации Краснолучского сельского поселения (далее – Администрация) персональных данных, функции Администрации при обработке персональных данных, права субъектов персональных данных, а также реализуемые Администрацией требования к защите персональных данных.

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

1.3. Положения Политики служат основой для разработки локальных нормативных актов, регламентирующих в Администрации вопросы обработки персональных данных сотрудников Администрации и других субъектов персональных данных.

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

2.1. Политика обработки персональных данных в Администрации определяется в соответствии со следующими нормативными правовыми актами:

Трудовой кодекс Российской Федерации;

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера»;

Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

Постановление Правительства Российской Федерации от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

Приказ Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;

иные нормативные правовые акты Российской Федерации и нормативные документы уполномоченных органов государственной власти.

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

Положение об обработке персональных данных в Администрации;

Порядок доступа Администрации в помещения, где ведётся обработка персональных данных;

Правила работы с обезличенными персональными данными в Администрации;

Регламент порядка действий Администрации при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных;

Инструкция осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Администрации;

иные локальные нормативные акты и документы, регламентирующие в Администрации вопросы обработки персональных данных.

3. Основные термины и определения, используемые в локальных нормативных актах Администрации, регламентирующие вопросы обработки персональных данных

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

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

Оператор — государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими

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

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

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

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

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

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

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

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

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

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

4. Перечень субъектов, персональные данные которых обрабатываются в Администрации

4.1. Администрация является оператором, организующим и осуществляющим в соответствии с Федеральным законом «О персональных

данных» обработку персональных данных следующих субъектов персональных данных:

1) глава Администрации Краснолучского сельского поселения (далее - выборное должностное лицо), муниципальные служащие, замещающие должности муниципальной в Администрации (далее соответственно - должности муниципальной службы, муниципальная служба, муниципальные служащие Администрации), члены их семей, лица, претендующие на замещение должностей муниципальной службы в Администрации, члены их семей;

2) работники Администрации, не являющиеся муниципальными служащими Администрации, а также члены их семей;

3) иные сторонние лица, обработка персональных данных которых осуществляется Администрацией в соответствии с законодательством Российской Федерации и законодательством Ростовской области (далее - иные сторонние лица).

5. Принципы и цели обработки персональных данных

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

обработка персональных данных осуществляется в Администрации на законной и справедливой основе;

обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей;

не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

обработке подлежат только персональные данные, которые отвечают целям их обработки;

содержание и объем обрабатываемых персональных данных соответствует заявленным целям обработки. Не допускается избыточность обрабатываемых персональных данных по отношению к заявленным целям их обработки;

при обработке персональных данных обеспечиваются точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Администрацией принимаются необходимые меры либо обеспечивается их принятие по удалению или уточнению неполных или неточных персональных данных;

хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем того требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;

обрабатываемые персональные данные уничтожаются либо обезличиваются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

5.2. Персональные данные обрабатываются в Администрации в следующих целях:

5.2.1. Персональные данные выборного должностного лица, муниципальных служащих Администрации, членов их семей, лиц, претендующих на замещение должностей муниципальной службы в Администрации, членов их семей, муниципальных служащих в структурных подразделениях, членов их семей, лиц, претендующих на замещение должностей муниципальной службы в структурных подразделениях, и членов их семей обрабатываются в целях:

1) формирования кадровых документов для поступления на выборную должность и ее замещение, на должности муниципальной службы, прохождения муниципальной службы, для выполнения связанных с этих требований трудового законодательства Российской Федерации, законодательства Российской Федерации о муниципальной службе и о противодействии коррупции;

2) осуществления действий, связанных с обеспечением выборному должностному лицу, муниципальным служащим условий труда, предоставлением гарантий и компенсаций, обязательным социальным страхованием, осуществлением расчетов по оплате труда и иным выплатам, связанным с замещением должности муниципальной службы, иных действий, связанных с замещением должности муниципальной службы, представлением к государственным наградам Российской Федерации и наградам Ростовской области и направленных на реализацию положений Трудового кодекса Российской Федерации, федеральных законов «О муниципальной службе в Российской Федерации» и «О противодействии коррупции», распоряжения Правительства Российской Федерации от 26 мая 2005 г. № 667-р «Об утверждении формы анкеты, представленной гражданином Российской Федерации, поступающим на государственную гражданскую службу Российской Федерации или на муниципальную службу Российской Федерации», иных нормативных правовых актов Российской Федерации, Закона Ростовской области «О муниципальной службе в Ростовской области» и муниципальных нормативных правовых актов Краснолучского сельского поселения в области муниципальной службы, трудовых правоотношений и наград;

3) ведения реестра муниципальных служащих и осуществления всех действий, связанных с реализацией полномочий по организации муниципальной службы;

4) включения в кадровый резерв на муниципальной службе в администрации Краснолучского сельского поселения в соответствии с нормативными правовыми актами Краснолучского сельского поселения в области организации работы с кадровым резервом на муниципальной службе.

5) выполнения требований законодательства Российской Федерации и законодательства Ростовской области о противодействии коррупции.

5.2.2. Персональные данные иных сторонних лиц обрабатываются в целях:

1) обеспечения реализации полномочий по представлению к государственным наградам Российской Федерации и наградам Ростовской области в соответствии с законодательством Российской Федерации и законодательством Ростовской области;

2) осуществления работы по рассмотрению обращений граждан и организации личного приема граждан в соответствии с Федеральным законом «О порядке рассмотрения обращений граждан Российской Федерации», Областным законом Ростовской области «Об обращениях граждан»;

3) включения в кадровый резерв на муниципальной службе в администрации Краснолучского сельского поселения в соответствии с нормативными правовыми актами Краснолучского сельского поселения в области организации работы с кадровым резервом на муниципальной службе;

4) осуществления полномочий по решению вопросов местного значения, а также отдельных государственных полномочий, переданных Администрации Краснолучского сельского поселения;

5) предоставления государственных и муниципальных услуг в соответствии с Федеральным законом от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;

6) при осуществлении деятельности по регистрации (учету) избирателей, участников референдума на территории Краснолучского сельского поселения;

7) обеспечения реализации администрацией Краснолучского сельского поселения полномочий по осуществлению закупок товаров, работ, услуг для обеспечения муниципальных нужд Краснолучского сельского поселения , по которым она выступает заказчиком в соответствии с Федеральным законом «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».

6. Перечень персональных данных, обрабатываемых в Администрации

6.1. Перечень персональных данных, обрабатываемых в Администрации, определяется в соответствии с законодательством Российской Федерации и локальными нормативными актами Администрации

с учетом целей обработки персональных данных, указанных в разделе 4 Политики.

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

7. Функции Администрации при осуществлении обработки персональных данных

7.1. Администрация при осуществлении обработки персональных данных:

принимает меры, необходимые и достаточные для обеспечения выполнения требований законодательства Российской Федерации и локальных нормативных актов Администрации в области персональных данных;

принимает правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;

назначает лицо, ответственное за организацию обработки персональных данных в Администрации;

издает локальные нормативные акты, определяющие политику и вопросы обработки и защиты персональных данных в Администрации;

осуществляет ознакомление сотрудников Администрации, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации и локальных нормативных актов Администрации в области персональных данных, в том числе требованиями к защите персональных данных, и обучение указанных сотрудников;

публикует или иным образом обеспечивает неограниченный доступ к настоящей Политике;

сообщает в установленном порядке субъектам персональных данных или их представителям информацию о наличии персональных данных, относящихся к соответствующим субъектам, предоставляет возможность ознакомления с этими персональными данными при обращении и (или) поступлении запросов указанных субъектов персональных данных или их представителей, если иное не установлено законодательством Российской Федерации;

прекращает обработку и уничтожает персональные данные в случаях, предусмотренных законодательством Российской Федерации в области персональных данных;

совершает иные действия, предусмотренные законодательством Российской Федерации в области персональных данных.

8. Условия обработки персональных данных в Администрации

8.1. Обработка Администрацией персональных данных осуществляется с письменно оформленного согласия субъекта персональных данных на обработку персональных данных в соответствии с типовой формой такого согласия согласно приложению 4 к Положению об обработке персональных данных в Администрации (далее - письменное согласие на обработку персональных данных), за исключением случаев, когда законодательством Российской Федерации установлена иная форма такого согласия или такое согласие не требуется в соответствии с законодательством Российской Федерации и настоящей Политикой.

8.2. В зависимости от целей, указанных в пункте 5.2. настоящей Политики Администрация осуществляет сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение и распространение персональных данных.

8.3. Обработка персональных данных осуществляется как с использованием, так и без использования средств автоматизации.

8.4. Принятие решений, порождающих юридические последствия в отношении лиц, указанных в подпунктах «1» - «3» пункта 4.1 настоящей Политики, или иным образом затрагивающих их права и законные интересы, на основании исключительно автоматизированной обработки их персональных данных, осуществляется при условии получения их письменного согласия в соответствии с типовой формой такого согласия согласно приложению 4 к Положению об обработке персональных данных в Администрации (далее – Положение).

8.5. Обработка персональных данных субъектов персональных данных, указанных в пункте 4.1. настоящей Политики, в соответствии с пунктом 2 части 1 статьи 6 и частью 2 статьи 11 Федерального закона «О персональных данных» осуществляется без их письменного согласия на обработку персональных данных в рамках целей обработки персональных данных, указанных в пункте 5.2. настоящей Политики.

8.6. Обработка специальных категорий персональных данных субъектов персональных данных, указанных в пункте 4.1. настоящей Политики, осуществляется без их письменного согласия на обработку персональных данных в рамках целей обработки персональных данных, указанных в подпункте 5.2.1. пункта 5.2. настоящей Политики, в соответствии с подпунктом 2.3, 6, 7, 8 части 2 статьи 10 Федерального закона «О персональных данных» и положениями Трудового кодекса Российской Федерации, федеральных законов «О муниципальной службе в Российской

Федерации», «О противодействии коррупции», за исключением случаев получения персональных данных соответствующего субъекта персональных данных у третьих лиц.

8.7. Персональные данные субъектов персональных данных, указанных в подпунктах «1» и «2» пункта 4.1. настоящей Политики, Администрация получает лично у субъектов персональных данных. В случае возникновения необходимости получения персональных данных такого субъекта персональных данных у третьей стороны Администрация обязана известить об этом субъект персональных данных заранее, получить его письменное согласие и сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных.

8.8. Уполномоченные лица Администрации с учетом установленной компетенции сообщают субъекту персональных данных о составе персональных данных, обрабатываемых в Администрации, и целях их обработки. Разъяснение юридических последствий отказа субъекта персональных данных представить свои персональные данные и (или) дать согласие на их обработку доводится до сведения субъектов персональных данных в соответствии с типовой формой такого разъяснения согласно приложению 6 к Положению.

8.9. Передача персональных данных субъектов персональных данных третьим лицам не допускается без письменного согласия субъекта персональных данных на передачу персональных данных третьим лицам в соответствии с типовой формой такого согласия согласно приложению 4 к Положению, за исключением случаев, установленных законодательством Российской Федерации.

Распространение персональных данных субъекта персональных данных осуществляется Администрацией с письменного согласия субъекта персональных данных.

Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных в соответствии с типовой формой такого согласия согласно приложению 4 к Положению.

Трансграничная передача персональных данных в Администрации не осуществляется. В случае необходимости трансграничной передачи персональных данных она должна проводиться с учетом требований статьи 12 Федерального закона «О персональных данных».

8.10. Администрация вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных на основании заключаемого с этим лицом договора. Договор должен содержать перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели обработки, обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке,

а также требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона «О персональных данных».

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

8.12. Доступ к обрабатываемым в Администрации персональным данным разрешается только сотрудникам Администрации, согласно перечня должностей работников, допущенных к работе с персональными данными и замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным в Администрации в соответствии с приложением 2 к Положению.

8.13. Защита персональных данных субъектов персональных данных и иных сторонних лиц от несанкционированного доступа, неправомерного использования или утраты обеспечивается Администрацией в порядке, установленном законодательством Российской Федерации.

8.14. Обеспечение безопасности персональных данных субъектов персональных данных при их обработке в информационных системах Администрации осуществляется отделом цифрового развития Администрации Краснолучского сельского поселения путем исключения несанкционированного, в том числе случайного, доступа к персональным данным субъектов персональных данных, указанным в пункте 4.1. настоящей Политики, а также принятия следующих мер по обеспечению безопасности персональных данных:

1) применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах Администрации, необходимых для выполнения требований к защите персональных данных;

2) применение средств защиты информации, установленных законодательством Российской Федерации в области персональных данных;

3) оценка эффективности принимаемых мер по обеспечению безопасности персональных данных в информационных системах Администрации;

4) учет машинных носителей персональных данных;

5) обнаружение фактов несанкционированного доступа к персональным данным и принятие соответствующих мер в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы администрации и по реагированию на компьютерные инциденты в них;

6) контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровней защищенности информационных систем

Администрации;

7) принятие иных мер, предусмотренных законодательством Российской Федерации в области персональных данных.

8.15. Хранение персональных данных субъектов персональных данных, указанных в пункте 4.1 настоящей Политики, должно осуществляться в форме, позволяющей определить субъекта персональных данных или иного стороннего лица, не дольше чем это требуют цели их обработки.

Сроки обработки и хранения персональных данных субъектов персональных данных, указанных в пункте 4.1 настоящей Политики, в администрации определяются в соответствии с трудовым законодательством Российской Федерации, законодательством Российской Федерации о муниципальной службе и архивном деле в Российской Федерации.

8.16. В случае достижения целей обработки персональных данных субъекта персональных данных или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством Российской Федерации в области персональных данных, а также в случае отзыва субъектом персональных данных письменного согласия на обработку его персональных данных Администрация обязана незамедлительно прекратить обработку персональных данных соответствующего субъекта персональных данных и уничтожить их в срок, не превышающий 30 дней со дня достижения целей обработки персональных данных (поступления отзыва субъектом персональных данных письменного согласия на обработку его персональных данных), если иное не предусмотрено законодательством Российской Федерации в области персональных данных.

9. Порядок уничтожения обработанных персональных данных в Администрации

9.1 Уничтожение обработанных персональных данных в Администрации в целях исключения их дальнейшей обработки осуществляется в сроки, установленные законодательством Российской Федерации.

9.2. Документы, содержащие персональные данные, наряду с иными документами формируются в дела в структурных подразделениях Администрации в соответствии с номенклатурой дел и передаются на хранение в архивный сектор администрации в порядке, установленном Инструкцией по делопроизводству в Администрации.

9.3. Выделение документов с истекшими сроками хранения, в том числе документов, содержащих персональные данные и подлежащих уничтожению, осуществляется экспертной комиссией Администрации. По результатам такой работы ежегодно составляется акт о выделении к уничтожению дел, не подлежащих хранению, включающий в себя наряду с иными документами документы, содержащие персональные данные (далее - дела, не подлежащие хранению).

9.4. Акт о выделении к уничтожению дел, не подлежащих хранению, ежегодно рассматривается на заседании экспертной комиссии Администрации.

По итогам рассмотрения на заседании экспертной комиссии Администрации акта о выделении к уничтожению дел, не подлежащих хранению, экспертная комиссия Администрации согласовывает его, направляет на согласование ответственному лицу и главе Администрации для подготовки его к согласованию экспертно-проверочной комиссией комитета по управлению архивным делом Ростовской области.

9.5. Акт о выделении к уничтожению дел, не подлежащих хранению, согласованный экспертной комиссией администрации и экспертно-проверочной комиссией комитета по управлению архивным делом Ростовской области, утверждается главой Администрации. На основании такого акта осуществляется уничтожение дел, не подлежащих хранению, в соответствии с порядком их уничтожения, утверждаемым распоряжением Администрации.

9.6. Уничтожение обработанных персональных данных из информационных систем Администрации осуществляется в соответствии с пунктом 8.16 настоящей Политики в порядке, утверждаемом распоряжением Администрации.

10. Перечень действий с персональными данными и способы их обработки

10.1. Администрация осуществляет сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), распространение, обезличивание, блокирование, удаление и уничтожение персональных данных.

10.2. Обработка персональных данных в Администрации осуществляется следующими способами:

неавтоматизированная обработка персональных данных;

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

смешанная обработка персональных данных.

11. Права субъектов персональных данных

11.1. Субъекты персональных данных имеют право на:

полную информацию об их персональных данных, обрабатываемых в Администрации;

доступ к своим персональным данным, включая право на получение копии любой записи, содержащей их персональные данные, за исключением случаев, предусмотренных федеральным законом;

уточнение своих персональных данных, их блокирование или уничтожение в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

отзыв согласия на обработку персональных данных;

принятие предусмотренных законом мер по защите своих прав;

обжалование действия или бездействия Администрации, осуществляемого с нарушением требований законодательства Российской Федерации в области персональных данных, в уполномоченный орган по защите прав субъектов персональных данных или в суд;

осуществление иных прав, предусмотренных законодательством Российской Федерации.

12. Меры, принимаемые Администрацией для обеспечения выполнения обязанностей оператора при обработке персональных данных

12.1. Меры, необходимые и достаточные для обеспечения выполнения Администрацией обязанностей оператора, предусмотренных законодательством Российской Федерации в области персональных данных, наряду с указанными в пункте 8.14. настоящей Политики включают:

наличие ответственного за обработку персональных данных;

наличие администратора информационных систем персональных данных;

наличие утвержденных инструкций, регламентирующих работу с персональными данными и информационными системами персональных данных;

осуществление внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных;

ознакомление всех сотрудников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику организации в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных под роспись;

учет машинных носителей персональных данных;

обеспечение восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

наличие правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных;

определение перечня сотрудников, осуществляющих обработку персональных данных;

обеспечение хранения сведений на бумажных носителях в сейфах или выделенных помещениях;

определение мест хранения персональных данных;

ведение учёта всех защищаемых носителей информации с помощью их маркировки и занесения учетных данных в журнал учета с отметкой об их выдаче (приеме);

обеспечение раздельного хранения персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

иные меры, предусмотренные законодательством Российской Федерации в области персональных данных.

12.2. Меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных устанавливаются в соответствии с локальными нормативными актами Администрации, регламентирующими вопросы обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных Администрации.

13. Контроль за соблюдением законодательства Российской Федерации и локальных нормативных актов Администрации в области персональных данных, в том числе требований к защите персональных данных.

13.1. Контроль за соблюдением законодательства Российской Федерации и локальных нормативных актов Администрации в области персональных данных, в том числе требований к защите персональных данных, осуществляется с целью проверки соответствия обработки персональных данных в Администрации и локальным нормативным актам Администрации в области персональных данных, в том числе требованиям к защите персональных данных, а также принятых мер, направленных на предотвращение и выявление нарушений законодательства Российской Федерации в области персональных данных, выявления возможных каналов утечки и несанкционированного доступа к персональным данным, устранения последствий таких нарушений.

13.2. Внутренний контроль за соблюдением законодательства Российской Федерации и локальных нормативных актов Администрации в области персональных данных, в том числе требований к защите персональных данных, осуществляется лицом, ответственным за организацию обработки персональных данных в Администрации, а также специально назначаемой комиссией.

13.3. Внутренний контроль соответствия обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите

персональных данных, настоящей Политике, локальным нормативным актам Администрации осуществляет Ответственный за организацию обработки персональных данных.

13.4. 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.

Приложение № 12
к распоряжению Администрации
Краснолучского сельского
поселения
от 01.07.2026 №23___

ИНСТРУКЦИЯ
администратора безопасности информационных систем персональных данных в Администрации Краснолучского сельского поселения

1. Общие положения

1.1. Администратор безопасности ИСПДн (далее – Администратор безопасности) назначается распоряжением Администрации Краснолучского сельского поселения (далее – Администрация).

1.2. Администратор безопасности подчиняется главе Администрации.

1.3. Администратор безопасности в своей работе руководствуется настоящей инструкцией, Концепцией и Политикой информационной безопасности, руководящими и нормативными документами ФСТЭК России и регламентирующими документами Администрации.

1.4. Администратор безопасности отвечает за поддержание необходимого уровня безопасности объектов защиты.

1.5. Администратор безопасности является ответственным должностным лицом Администрации, уполномоченным на проведение работ по технической защите информации и поддержанию достигнутого уровня защиты ИСПДн и ее ресурсов на этапах промышленной эксплуатации и модернизации.

1.6. Администратор безопасности должен иметь специальное рабочее место, размещенное в здании Администрации так, чтобы исключить несанкционированный доступ к нему посторонних лиц и других пользователей.

1.7. Рабочее место Администратора безопасности должно быть оборудовано средствами физической защиты (личный сейф, железный шкаф или другое), подключением к ИСПДн, а также средствами контроля за техническими средствами защиты.

1.8. Администратор безопасности осуществляет методическое руководство Операторов и Администраторов ИСПДн, в вопросах обеспечения безопасности персональных данных.

1.9. Требования администратора информационной безопасности, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми пользователями ИСПДн.

1.10. Администратор безопасности несет персональную ответственность за качество проводимых им работ по контролю действий

пользователей при работе в ИСПДн, состояние и поддержание установленного уровня защиты ИСПДн.

2. Должностные обязанности

Администратор безопасности обязан:

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

2.2. Осуществлять установку, настройку и сопровождение технических средств защиты.

2.3. Участвовать в контрольных и тестовых испытаниях и проверках элементов ИСПДн.

2.4. Участвовать в приемке новых программных средств.

2.5. Обеспечить доступ к защищаемой информации пользователям ИСПДн согласно их правам доступа при получении оформленного соответствующим образом разрешения.

2.6. Уточнять в установленном порядке обязанности пользователей ИСПДн по обработке объектов защиты.

2.7. Вести контроль над процессом осуществления резервного копирования объектов защиты.

2.8. Осуществлять контроль над выполнением Плана мероприятий по защите персональных данных.

2.9. Анализировать состояние защиты ИСПДн и ее отдельных подсистем.

2.10. Контролировать неизменность состояния средств защиты их параметров и режимов защиты.

2.11. Контролировать физическую сохранность средств и оборудования ИСПДн.

2.12. Контролировать исполнение пользователями ИСПДн введенного режима безопасности, а также правильность работы с элементами ИСПДн и средствами защиты.

2.13. Контролировать исполнение пользователями парольной политики.

2.14. Контролировать работу пользователей в сетях общего пользования и (или) международного обмена.

2.15. Своевременно анализировать журнал учета событий, регистрируемых средствами защиты, с целью выявления возможных нарушений.

2.16. Не допускать установку, использование, хранение и размножение в ИСПДн программных средств, не связанных с выполнением функциональных задач.

2.17. Не допускать к работе на элементах ИСПДн посторонних лиц.

2.18. Осуществлять периодические контрольные проверки рабочих станций и тестирование правильности функционирования средств защиты ИСПДн.

2.19. Оказывать помощь пользователям ИСПДн в части применения средств защиты и консультировать по вопросам введенного режима защиты.

2.20. Периодически представлять руководству отчет о состоянии защиты ИСПДн и о нештатных ситуациях на объектах ИСПДн и допущенных пользователями нарушениях установленных требований по защите информации.

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

2.22. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, фактов обнаружения несанкционированного доступа к персональным данным с целью ликвидации их последствий.

3. Ответственность

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

С настоящей Инструкцией ознакомлен:

№	Должность сотрудника	Фамилия, имя, отчество	Дата и подпись
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			

Приложение № 13
к распоряжению Администрации
Краснолучского сельского
поселения
от 01.07.2026 №23 ___

ИНСТРУКЦИЯ
пользователя по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций в Администрации Краснолучского сельского поселения

1. Назначение и область действия

1.1. Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием ИСПДн Администрации Краснолучского сельского поселения (далее – Администрация), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций.

1.2. Целью настоящего документа является превентивная защита элементов ИСПДн от прерывания в случае реализации рассматриваемых угроз.

1.3. Задачей данной Инструкции является:

определение мер защиты от прерывания;

определение действий восстановления в случае прерывания.

1.4. Действие настоящей Инструкции распространяется на всех пользователей Администрации, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

системы жизнеобеспечения;

системы обеспечения отказоустойчивости;

системы резервного копирования и хранения данных;

системы контроля физического доступа.

1.5. Пересмотр настоящего документа осуществляется по мере необходимости, но не реже одного раза в два года.

2. Порядок реагирования на аварийную ситуацию

2.1. Действия при возникновении аварийной ситуации

В настоящем документе под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн. Аварийная ситуация становится возможной в результате реализации одной из угроз, приведенных в приложении 1.

Все действия в процессе реагирования на аварийные ситуации должны документироваться ответственным за реагирование сотрудником в «Журнале по учету мероприятий по контролю».

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники Администрации (Администратор безопасности, Администратор и Оператор ИСПДн) предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

2.2. Уровни реагирования на инцидент

При реагировании на инцидент, важно, чтобы пользователь правильно классифицировал критичность инцидента. Критичность оценивается на основе следующей классификации:

Уровень 1 – **Незначительный инцидент**. Незначительный инцидент определяется как локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств защиты. Эти инциденты решаются ответственными за реагирование сотрудниками.

Уровень 2 – **Авария**. Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты. Эти инциденты выходят за рамки управления ответственными за реагирование сотрудниками.

К авариям относятся следующие инциденты:

Отказ элементов ИСПДн и средств защиты из-за:

повреждения водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения), а также подтопления в период паводка или проливных дождей;

сбоя системы кондиционирования.

Отсутствие Администратора ИСПДн и Администратора безопасности более чем на сутки из-за:

химического выброса в атмосферу;

сбоев общественного транспорта;

эпидемии;

массового отравления персонала;

сильного снегопада;

торнадо;

сильных морозов.

Уровень 3 – **Катастрофа**. Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, а также к угрозе жизни пользователей ИСПДн, классифицируется как катастрофа. Обычно к катастрофам относят обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к работоспособности ИСПДн и средств защиты на сутки и более.

К катастрофам относятся следующие инциденты:

пожар в здании;
взрыв;
просадка грунта с частичным обрушением здания;
массовые беспорядки в непосредственной близости от Объекта.

3. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций

3.1. Технические меры

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

системы жизнеобеспечения;
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 Администрации (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Порядок предотвращения потерь информации и организации системы жизнеобеспечения ИСПДн описан в Инструкции о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения и баз данных.

3.2. Организационные меры

Ответственные за реагирование сотрудники ознакомляют всех сотрудников Администрации, находящихся в их зоне ответственности, с данной инструкцией в срок, не превышающий трех рабочих дней с момента выхода нового сотрудника на работу.

По окончанию ознакомления сотрудник расписывается в инструкции.

Приложение 1
к инструкции пользователя по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций в Администрации Краснолучского сельского поселения

ИСТОЧНИКИ УГРОЗ

Технологические угрозы	
1	Пожар в здании
2	Повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения)
3	Взрыв (бытовой газ, теракт, взрывчатые вещества или приборы, работающие под давлением)
4	Химический выброс в атмосферу
Внешние угрозы	
5	Массовые беспорядки
6	Сбои общественного транспорта
7	Эпидемия
8	Массовое отравление персонала
Стихийные бедствия	
9	Удар молнии
10	Сильный снегопад
11	Сильные морозы
12	Просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением здания
13	Затопление водой в период паводка
14	Наводнение, вызванное проливным дождем
15	Торнадо
16	Подтопление здания (воздействие подпочвенных вод, вызванное внезапным и непредвиденным повышением уровня грунтовых вод)

Телеком и ИТ угрозы	
17	Сбой системы кондиционирования
18	Сбой ИТ – систем
Угроза, связанная с человеческим фактором	
19	Ошибка персонала, имеющего доступ к серверной
20	Нарушение конфиденциальности, целостности и доступности конфиденциальной информации
Угрозы, связанные с внешними поставщиками	
21	Отключение электроэнергии
22	Сбой в работе интернет-провайдера
23	Физически разрыв внешних каналов связи

Приложение № 14
к распоряжению Администрации
Краснолучского сельского
поселения
от 01.07.2026 №23 ___

КОНЦЕПЦИЯ
информационной безопасности информационных систем персональных данных

1. Определения

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

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

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

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

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

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

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

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

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

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

Доступ к информации – возможность получения информации и ее использования.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу

Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

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

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

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

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

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

2. Обозначения и сокращения

АВС – антивирусные средства.
АРМ – автоматизированное рабочее место.
ВТСС – вспомогательные технические средства и системы.
ИСПДн – информационная система персональных данных.
КЗ – контролируемая зона.
ЛВС – локальная вычислительная сеть.
МЭ – межсетевой экран.
НСД – несанкционированный доступ.
ОС – операционная система.
ПДн – персональные данные.
ПМВ – программно-математическое воздействие.
ПО – программное обеспечение.
ПЭМИН – побочные электромагнитные излучения и наводки.
САЗ – система анализа защищенности.
СЗИ – средства защиты информации.
СЗПДн – система (подсистема) защиты персональных данных.
СОВ – система обнаружения вторжений.
ТКУИ – технические каналы утечки информации.
УБПДн – угрозы безопасности персональных данных.

3. Введение

3.1. Настоящая Концепция информационной безопасности ИСПДн администрации Краснолучского сельского поселения (далее – Администрация) является официальным документом, в котором определена система взглядов на обеспечение информационной безопасности Администрации.

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

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

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

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

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

3.7. Концепция является методологической основой для:

– формирования и проведения единой политики в области обеспечения безопасности ПДн в ИСПДн Администрации;

– принятия управленческих решений и разработки практических мер по воплощению политики безопасности ПДн и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление,

отражение и ликвидацию последствий реализации различных видов угроз ПДн;

– координации деятельности структурных подразделений Администрации при проведении работ по развитию и эксплуатации ИСПДн с соблюдением требований обеспечения безопасности ПДн;

– разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности ПДн в ИСПДн Администрации.

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

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

4. Общие положения

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

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

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

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

4.5. Эти меры призваны обеспечить:

– **конфиденциальность** информации (защита от несанкционированного ознакомления);

– **целостность** информации (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);

– **доступность** информации (возможность за приемлемое время получить требуемую информационную услугу).

4.6. Стадии создания СЗПДн включают:

– предпроектную стадию, включающую предпроектное обследование ИСПДн, разработку технического (частного технического) задания на ее создание;

– стадию проектирования (разработки проектов) и реализации ИСПДн, включающую разработку СЗПДн в составе ИСПДн;

– стадию ввода в действие СЗПДн, включающую опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку соответствия ИСПДн требованиям безопасности информации.

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

– инструкции администратора информационных систем персональных данных по обеспечению безопасности персональных данных;

– инструкции о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения и баз данных;

– инструкции ответственного за обработку персональных данных;

– инструкции по организации антивирусной защиты;

– инструкции по порядку учета и хранению документов, содержащих персональные данные;

– инструкции по обеспечению безопасности эксплуатации средств криптографической защиты информации (СКЗИ);

– инструкции по порядку учета и хранения машинных носителей конфиденциальной информации (персональных данных);

– инструкции пользователя информационных систем персональных данных по обеспечению безопасности персональных данных;

– инструкции по осуществлению внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных;

– инструкции пользователя по обеспечению безопасности обработки персональных данных, при возникновении внештатных ситуаций.

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

4.9. Перечень необходимых мер защиты информации определяется по результатам внутренней проверки безопасности ИСПДн Администрации.

5. Задачи СЗПДн

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

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

защиту от вмешательства в процесс функционирования ИСПДн посторонних лиц (возможность использования АС и доступ к ее ресурсам должны иметь только зарегистрированные установленным порядком пользователи);

разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам ИСПДн (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям ИСПДн для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа:

к информации, циркулирующей в ИСПДн;

средствам вычислительной техники ИСПДн;

аппаратным, программным и криптографическим средствам защиты, используемым в ИСПДн.

регистрацию действий пользователей при использовании защищаемых ресурсов ИСПДн в системных журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов;

контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;

защиту от несанкционированной модификации и контроль целостности используемых в ИСПДн программных средств, а также защиту системы от внедрения несанкционированных программ;

защиту ПДн от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;

защиту ПДн, хранимой, обрабатываемой и передаваемой по каналам связи, от несанкционированного разглашения или искажения;

обеспечение живучести криптографических средств защиты информации при компрометации части ключевой системы;

своевременное выявление источников угроз безопасности ПДн, причин и условий, способствующих нанесению ущерба субъектам ПДн, создание механизма оперативного реагирования на угрозы безопасности ПДн и негативные тенденции;

создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление

негативного влияния и ликвидация последствий нарушения безопасности ПДн.

6. Объекты защиты

6.1. Перечень информационных систем.

В Администрации производится обработка персональных данных в информационных система обработки персональных данных (ИСПДн).

Перечень ИСПДн определяется на основании внутреннего обследования.

6.2. Перечень объектов защиты.

Объектами защиты являются – информация, обрабатываемая в ИСПДн, и технические средства ее обработки и защиты. Перечень персональных данных, подлежащие защите, определен в Перечне персональных данных, обрабатываемых в Администрации.

Объекты защиты включают:

обрабатываемую информацию;

технологическую информацию;

программно-технические средства обработки;

средства защиты ПДн;

каналы информационного обмена и телекоммуникации;

объекты и помещения, в которых размещены компоненты ИСПДн.

7. Классификация пользователей ИСПДн

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

7.2. Пользователи ИСПДн делятся на три основные категории:

7.2.1. Администратор ИСПДн - сотрудник Администрации, который занимается настройкой, внедрением и сопровождением системы. Администратор ИСПДн обладает следующим уровнем доступа:

обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;

обладает полной информацией о технических средствах и конфигурации ИСПДн;

имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;

обладает правами конфигурирования и административной настройки технических средств ИСПДн.

7.2.2. Администратор безопасности ИСПДн - сотрудник Администрации или сторонних организаций, который занимается разработкой программного обеспечения. Администратор безопасности ИСПДн обладает следующим уровнем доступа:

обладает информацией об алгоритмах и программах обработки информации на ИСПДн;

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

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

7.2.3. Пользователь ИСПДн - сотрудник Администрации, участвующий в процессе эксплуатации ИСПДн. Пользователь ИСПДн обладает следующим уровнем доступа:

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

располагает конфиденциальными данными, к которым имеет доступ.

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

7.4. Все выявленные группы пользователей отражаются в Перечне должностей работников, допущенных к работе с персональными данными и замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным в Администрации Краснолучского сельского поселения. На основании обследования определяются права доступа к элементам ИСПДн для всех групп пользователей и отражаются в Разрешительной системе доступа сотрудников к ресурсам информационных систем персональных данных, принадлежащих Администрации.

8. Основные принципы построения системы комплексной защиты информации

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

законность;

системность;

комплексность;

непрерывность;

своевременность;

преемственность и непрерывность совершенствования;

персональная ответственность;
минимизация полномочий;
взаимодействие и сотрудничество;
гибкость системы защиты;
открытость алгоритмов и механизмов защиты;
простота применения средств защиты;
научная обоснованность и техническая реализуемость;
специализация и профессионализм;
обязательность контроля.

8.2. Законность.

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

8.2.2. Пользователи и обслуживающий персонал ПДн ИСПДн Администрации должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за защиты ПДн.

8.3. Системность.

8.3.1. Системный подход к построению СЗПДн Администрации предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ПДн ИСПДн Администрации.

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

8.4. Комплексность.

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

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

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

8.5. Непрерывность защиты ПДн.

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

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

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

8.6. Своевременность.

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

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

8.7. Преемственность и совершенствование.

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

8.8. Персональная ответственность.

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

8.9. Принцип минимизации полномочий.

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

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

8.10. Взаимодействие и сотрудничество.

8.10.1. Предполагает создание благоприятной атмосферы в коллективах подразделений, обеспечивающих деятельность ИСПДн Администрации, для снижения вероятности возникновения негативных действий, связанных с человеческим фактором.

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

8.11. Гибкость системы защиты ПДн.

Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования.

8.12. Открытость алгоритмов и механизмов защиты.

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

8.13. Простота применения средств защиты.

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

8.13.2. Должна достигаться автоматизация максимального числа действий пользователей и администраторов ИСПДн.

8.14. Научная обоснованность и техническая реализуемость.

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

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

8.15. Специализация и профессионализм.

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

8.16. Обязательность контроля.

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

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

9. Меры, методы и средства обеспечения требуемого уровня защищенности

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

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

9.2. Законодательные (правовые) меры защиты.

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

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

9.3. Морально-этические меры защиты.

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

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

9.4. Организационные (административные) меры защиты.

9.4.1. Организационные (административные) меры защиты – это меры организационного характера, регламентирующие процессы функционирования ИСПДн, использование ресурсов ИСПДн, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с ИСПДн таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

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

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

9.4.4. К административному уровню относятся решения руководства, затрагивающие деятельность ИСПДн в целом. Эти решения закрепляются в

Политике информационной безопасности. Примером таких решений могут быть:

принятие решения о формировании или пересмотре комплексной программы обеспечения безопасности ПДн, определение ответственных за ее реализацию;

формулирование целей, постановка задач, определение направлений деятельности в области безопасности ПДн;

принятие решений по вопросам реализации программы безопасности, которые рассматриваются на уровне Администрации в целом;

обеспечение нормативной (правовой) базы вопросов безопасности и т.п.

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

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

какова область применения политики безопасности ПДн;

каковы роли и обязанности должностных лиц, отвечающие за проведение политики безопасности ПДн, а также их установить ответственность;

кто имеет права доступа к ПДн;

какими мерами и средствами обеспечивается защита ПДн;

какими мерами и средствами обеспечивается контроль за соблюдением введенного режима безопасности.

9.4.7. Организационные меры должны:

предусматривать регламент информационных отношений, исключающих возможность несанкционированных действий в отношении объектов защиты;

определять коалиционные и иерархические принципы и методы разграничения доступа к ПДн;

определять порядок работы с программно-математическими и техническими (аппаратные) средствами защиты и криптозащиты и других защитных механизмов;

организовать меры противодействия НСД пользователями на этапах аутентификации, авторизации, идентификации, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

9.4.8. Организационные меры должны состоять из:

регламента доступа в помещения ИСПДн;

порядок допуска сотрудников к использованию ресурсов ИСПДн Администрации;

регламента процессов ведения баз данных и осуществления модификации информационных ресурсов;

регламента процессов обслуживания и осуществления модификации аппаратных и программных ресурсов ИСПДн;

инструкций пользователей ИСПДн (администратора ИСПДн, пользователя ИСПДн);

инструкция пользователя при возникновении внештатных ситуаций.

9.5. Физические меры защиты.

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

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

9.6. Аппаратно-программные средства защиты ПДн.

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

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

средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей ИСПДн;

средства разграничения доступа зарегистрированных пользователей системы к ресурсам ИСПДн Администрации;

средства обеспечения и контроля целостности программных и информационных ресурсов;

средства оперативного контроля и регистрации событий безопасности;

криптографические средства защиты ПДн.

9.6.3. Успешное применение технических средств защиты на основании принципов (раздел 8) предполагает, что выполнение перечисленных ниже требований обеспечено организационными

(административными) мерами и используемыми физическими средствами защиты:

обеспечена физическая целостность всех компонент ИСПДн;

каждый сотрудник (пользователь ИСПДн) или группа пользователей имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;

все изменения конфигурации технических и программных средств ИСПДн производятся строго установленным порядком (регистрируются и контролируются) только на основании распоряжений руководства Администрации;

сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (специальных помещениях, шкафах и т.п.).

специалистами Администрации осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

10. Контроль эффективности системы защиты

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

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

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

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

11. Сферы ответственности за безопасность ПДн

11.1. Ответственным за разработку мер и контроль над обеспечением безопасности персональных данных является глава Администрации

Краснолучского сельского поселения. Он может делегировать часть полномочий по обеспечению безопасности персональных данных.

11.2. Сфера ответственности главы Администрации включает следующие направления обеспечения безопасности ПДн:

планирование и реализацию мер по обеспечению безопасности ПДн;

анализ угроз безопасности ПДн;

разработку, внедрение, контроль исполнения и поддержание в актуальном состоянии политик, руководств, концепций, процедур, регламентов, инструкций и других организационных документов по обеспечению безопасности;

контроль защищенности ИТ инфраструктуры Администрации от угроз ИБ путем эмуляции действий потенциального злоумышленника по преодолению механизмов защиты;

обучение и информирование пользователей ИСПДн, о порядке работы с ПДн и средствами защиты;

предотвращение, выявление, реагирование и расследование нарушений безопасности ПДн.

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

12. Модель нарушителя безопасности

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

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

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

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

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

13. Модель угроз безопасности

13.1. Для ИСПДн Администрации выделяются следующие основные категории угроз безопасности персональных данных:

13.1.1. Угрозы от утечки по техническим каналам.

13.1.2. Угрозы несанкционированного доступа к информации:

угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн;

угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);

угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера;

угрозы преднамеренных действий внутренних нарушителей;

угрозы несанкционированного доступа по каналам связи;

описание угроз, вероятность их реализации, опасность и актуальность представлены в Модели угроз безопасности персональных данных каждой ИСПДн.

14. Механизм реализации Концепции

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

федеральных законов в области обеспечения информационной безопасности и защиты информации;

постановлений Правительства Российской Федерации;

руководящих, организационно-распорядительных и методических документов ФСТЭК России;

потребностей ИСПДн в средствах обеспечения безопасности информации.

15. Ожидаемый эффект от реализации Концепции

15.1. Реализация Концепции безопасности ПДн в ИСПДн позволит:

оценить состояние безопасности информации ИСПДн, выявить источники внутренних и внешних угроз информационной безопасности, определить приоритетные направления предотвращения, отражения и нейтрализации этих угроз;

разработать распорядительные и нормативно-методические документы применительно к ИСПДн;

провести классификацию и сертификацию ИСПДн;

провести организационно-режимные и технические мероприятия по обеспечению безопасности ПДн в ИСПДн;

обеспечить необходимый уровень безопасности объектов защиты.

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

16. Список использованных источников

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

Федеральный Закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»), устанавливающий основные принципы и условия обработки ПДн, права, обязанности и ответственность участников отношений, связанных с обработкой ПДн;

«Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденное Постановлением Правительства РФ от 01.11.2012 № 1119;

«Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденное Постановлением Правительства РФ от 15.09.2008 № 687;

«Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», утвержденные Постановлением Правительства РФ от 06.07.2008 № 512.

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

приказ ФСТЭК России от 18.02.2013 № 21 (в ред. от 14.05.2020) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

Методический документ. Методика оценки угроз безопасности информации (утв. ФСТЭК России 05.02.2021).

Приложение № 15
к распоряжению Администрации
Краснолучского сельского
поселения
от 01.07.2026_№23 ___

ПОЛИТИКА
информационной безопасности информационных систем персональных данных администрации Краснолучского сельского поселения

1. Определения

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

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

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

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

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

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

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

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

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими

средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

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

Доступ к информации – возможность получения информации и ее использования.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2. Обозначения и сокращения

АВС – антивирусные средства
АРМ – автоматизированное рабочее место
ВТСС – вспомогательные технические средства и системы
ИСПДн – информационная система персональных данных
КЗ – контролируемая зона
ЛВС – локальная вычислительная сеть
МЭ – межсетевой экран
НСД – несанкционированный доступ
ОС – операционная система
ПДн – персональные данные
ПМВ – программно-математическое воздействие
ПО – программное обеспечение
ПЭМИН – побочные электромагнитные излучения и наводки
САЗ – система анализа защищенности
СЗИ – средства защиты информации
СЗПДн – система (подсистема) защиты персональных данных
СОВ – система обнаружения вторжений
ТКУИ – технические каналы утечки информации
УБПДн – угрозы безопасности персональных данных

3. Введение

3.1. Настоящая Политика информационной безопасности администрации Краснолучского сельского поселения (далее – Администрация) является официальным документом.

3.2. Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных изложенных в Концепции информационной безопасности ИСПДн Администрации.

3.3. Политика разработана в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», на основании:

Рекомендации Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 31.07.2017 «Рекомендации по составлению документа, определяющего политику оператора в отношении обработки персональных данных, в порядке, установленном Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18.02.2013 № 21;

Требований по безопасности информации к системам управления базами данных, утвержденных приказом ФСТЭК России от 14.04.2023 № 64;

Методического документа «Методика оценки угроз безопасности информации», утвержденного ФСТЭК России 05.02.2021;

Приказа ФСБ от 10.07.2014 № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

Приказа ФСБ России от 09.02.2005 № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденной приказом ФАПСИ от 13.06.2001 № 152;

Методических рекомендаций по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные

при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденных руководством 8 Центра ФСБ России (№ 149/7/2/6-432 от 31.03.2015).

3.4. В Политике определены требования к персоналу ИСПДн, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в ИСПДн Администрации.

4. Общие положения

4.1. Целью настоящей Политики является обеспечение безопасности объектов защиты Администрации от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн).

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

4.3. Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБПДн.

4.4. Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

4.5. Состав объектов защиты представлен в Перечне персональных данных, подлежащих защите.

4.6. Состав ИСПДн, подлежащих защите, представлен в Перечне ИСПДн.

5. Область действия

5.1. Требования настоящей Политики распространяются на всех сотрудников Администрации (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

5.2.

6. Система защиты персональных данных

6.1. Система защиты персональных данных (СЗПДн), строится на основании:

перечня персональных данных, подлежащих защите;

акта классификации информационной системы персональных данных;

модели угроз безопасности персональных данных;

положения о разграничении прав доступа к обрабатываемым персональным данным;

руководящих документов ФСТЭК и ФСБ России.

6.2. На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн Администрации. На основании анализа актуальных угроз безопасности ПДн, описанного в Модели угроз, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в Плане мероприятий по обеспечению защиты ПДн.

6.3. Для каждой ИСПДн должен быть составлен список используемых технических средств защиты, а также программного обеспечения, участвующего в обработке ПДн, на всех элементах ИСПДн:

АРМ пользователей;

сервера приложений;

СУБД;

границе ЛВС;

каналов передачи в сети общего пользования и (или) международного обмена, если по ним передаются ПДн.

6.4. В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства:

антивирусные средства для рабочих станций пользователей и серверов;

средства межсетевого экранирования;

средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

6.5. Также в список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты. Список функций защиты может включать:

управление и разграничение доступа пользователей;

регистрацию и учет действий с информацией;

обеспечение целостности данных;

обнаружение вторжений.

6.6. Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения должны быть внесены в Список и утверждены главной Администрации или лицом, ответственным за обеспечение защиты ПДн.

7. Требования к подсистемам СЗПДн

7.1. СЗПДн включает в себя следующие подсистемы:

управления доступом, регистрации и учета;

обеспечения целостности и доступности;

антивирусной защиты;

межсетевого экранирования;

анализа защищенности;

обнаружения вторжений;

криптографической защиты.

7.2. Подсистемы СЗПДн имеют различный функционал в зависимости от уровня защищенности ИСПДн, определенного в Акте классификации информационной системы персональных данных.

7.3. Подсистемы управления доступом, регистрации и учета.

Подсистема управления доступом, регистрации и учета предназначена для реализации следующих функций:

идентификации и проверка подлинности субъектов доступа при входе в ИСПДн;

идентификации терминалов, узлов сети, каналов связи, внешних устройств по логическим именам;

идентификации программ, томов, каталогов, файлов, записей, полей записей по именам;

регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее останова.

регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;

регистрации попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.

Подсистема управления доступом может быть реализована с помощью штатных средств обработки ПДн (операционных систем, приложений и СУБД). Так же может быть внедрено специальное техническое средство или их комплекс осуществляющие дополнительные меры по аутентификации и контролю. Например, применение единых хранилищ учетных записей пользователей и регистрационной информации, использование биометрических и технических (с помощью электронных пропусков) мер аутентификации и других.

7.4. Подсистема обеспечения целостности и доступности.

Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств ИСПДн Администрации, а также средств защиты, при случайной или намеренной модификации.

Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а также резервированием ключевых элементов ИСПДн.

7.5. Подсистема антивирусной защиты.

Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей ИСПДн Администрации.

Средства антивирусной защиты предназначены для реализации следующих функций:

резидентный антивирусный мониторинг;

антивирусное сканирование;

скрипт-блокирование;

централизованную/удаленную установку/деинсталляцию антивирусного продукта, настройку, администрирование, просмотр отчетов и статистической информации по работе продукта;

автоматизированное обновление антивирусных баз;

ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;

автоматический запуск сразу после загрузки операционной системы.

Подсистема реализуется путем внедрения специального антивирусного программного обеспечения на все элементы ИСПДн.

7.6. Подсистема межсетевого экранирования.

Подсистема межсетевого экранирования предназначена для реализации следующих функций:

фильтрации открытого и зашифрованного (закрытого) IP-трафика по следующим параметрам;

фиксации во внутренних журналах информации о проходящем открытом и закрытом IP-трафике;

идентификации и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ;

регистрации входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова;

контроля целостности своей программной и информационной части;

фильтрации пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

фильтрации с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;

регистрации и учета запрашиваемых сервисов прикладного уровня;

блокирования доступа неидентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату;

контроля за сетевой активностью приложений и обнаружения сетевых атак.

Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования на границе ЛВС, классом не ниже 4.

7.7. Подсистема анализа защищенности.

Подсистема анализа защищенности, должна обеспечивать выявления уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

7.8. Подсистема обнаружения вторжений.

Подсистема обнаружения вторжений, должна обеспечивать выявление сетевых атак на элементы ИСПДн подключенные к сетям общего пользования и (или) международного обмена.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

7.9. Подсистема криптографической защиты.

Подсистема криптографической защиты предназначена для исключения НСД к защищаемой информации в ИСПДн Администрации, при ее передаче по каналам связи сетей общего пользования и (или) международного обмена.

Подсистема реализуется внедрения криптографических программно-аппаратных комплексов.

8. Пользователи ИСПДн

8.1. В Концепции информационной безопасности определены основные категории пользователей. На основании этих категории должна быть произведена типизация пользователей ИСПДн, определен их уровень доступа и возможности.

8.2. В ИСПДн Администрации можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

администратор ИСПДн;

пользователь ИСПДн.

8.3. Данные о группах пользователях, уровне их доступа и информированности должен быть отражен в Разрешительной системе доступа сотрудников к ресурсам информационных систем персональных данных, принадлежащих Администрации Краснолучского сельского поселения Ростовской области .

8.4. Администратор ИСПДн.

Администратор ИСПДн, сотрудник Администрации, ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного Пользователя ИСПДн к элементам, хранящим персональные данные.

Администратор ИСПДн обладает следующим уровнем доступа и знаний:

обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;

обладает полной информацией о технических средствах и конфигурации ИСПДн;

имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;

обладает правами конфигурирования и административной настройки технических средств ИСПДн.

8.5. Пользователь ИСПДн.

Пользователь ИСПДн – сотрудник Администрации, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Пользователь ИСПДн не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Пользователь ИСПДн обладает следующим уровнем доступа и знаний:

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

располагает конфиденциальными данными, к которым имеет доступ.

9. Требования к персоналу по обеспечению защиты ПДн

9.1. Все сотрудники Администрации, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

9.2. При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

9.3. Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

9.4. Сотрудники Администрации, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а также возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

9.5. Сотрудники Администрации должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

9.6. Сотрудники Администрации должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

9.7. Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.

9.8. Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами Администрации, третьим лицам.

9.9. При работе с ПДн в ИСПДн сотрудники Администрации обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

9.10. При завершении работы с ИСПДн сотрудники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

9.11. Сотрудники Администрации должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.

9.12. Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

10. Должностные обязанности пользователей ИСПДн

10.1. Должностные обязанности пользователей ИСПДн описаны в следующих документах:

инструкция администратора ИСПДн;

инструкция пользователя ИСПДн;

инструкция о порядке резервирования и восстановления;

инструкция по антивирусной защите;

инструкция пользователя СКЗИ;

инструкция по работе с документами с ПДн;

инструкция по учету машинных носителей;

регламент реагирования на запрос субъекта ПДн;

инструкция пользователя при возникновении внештатных ситуаций;

инструкция по организации парольной защиты;

инструкция по организации защиты информации о событиях безопасности в ИСПДн;

инструкция по установке и модификации по;

инструкция по обеспечению защиты информации при выводе ИСПДн из эксплуатации.

11. Ответственность сотрудников

11.1. В соответствии со ст. 24 Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

11.2. Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272, 273 и 274 УК РФ).

11.3. Администратор ИСПДн несет ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

11.4. При нарушениях сотрудниками Администрации – пользователей ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

11.5. Приведенные выше требования нормативных документов по защите информации должны быть отражены в Положениях о подразделениях Администрации, осуществляющих обработку ПДн в ИСПДн и должностных инструкциях сотрудников Администрации.

11.6. Необходимо внести в Положения о подразделениях Администрации, осуществляющих обработку ПДн в ИСПДн сведения об ответственности их руководителей и сотрудников за разглашение и несанкционированную модификацию (искажение, фальсификацию) ПДн, а также за неправомерное вмешательство в процессы их автоматизированной обработки.

12. Список использованных источников

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

Федеральный Закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»), устанавливающий основные принципы и условия обработки ПДн, права, обязанности и ответственность участников отношений, связанных с обработкой ПДн;

«Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденное Постановлением Правительства РФ от 01.11.2012 № 1119;

«Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденное Постановлением Правительства РФ от 15.09.2008 № 687;

«Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», утвержденные Постановлением Правительства РФ от 06.07.2008 № 512.

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

приказ ФСТЭК России от 18.02.2013 № 21 (в ред. от 14.05.2020) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

Требования по безопасности информации к системам управления базами данных, утвержденные приказом ФСТЭК России от 14.04.2023 № 64;

методический документ «Методика оценки угроз безопасности информации».

12.3 Нормативно-методические документы Федеральной службы безопасности Российской Федерации (далее - ФСБ России) по обеспечению безопасности ПДн при их обработке в ИСПДн (только при использовании СКЗИ):

приказ ФСБ от 10.07.2014 № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

приказ ФСБ России от 09.02.2005 № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом ФАПСИ от 13.06.2001 № 152;

Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденных руководством 8 Центра ФСБ России (№ 149/7/2/6-432 от 31.03.2015).

Приложение № 16
к распоряжению Администрации
Краснолучского сельского
поселения
от 01.07.2026 №23 ___

ИНСТРУКЦИЯ
по организации парольной защиты информационных систем персональных данных в Администрации Краснолучского сельского поселения

1. Общие положения

1.1. Настоящая Инструкция предназначена для организации парольной защиты информационных систем персональных данных в Администрации Краснолучского сельского поселения (далее – Администрация).

1.2. Действие настоящей Инструкции распространяется на всех пользователей информационных систем персональных данных (далее – Пользователь).

1.3. 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.

2. Организация парольной защиты

2.1. Пароли доступа к элементам информационной системы персональных данных создаются Администратором безопасности информационной системы персональных данных.

2.2. Правила смены личных паролей:

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

Внеплановая смена (удаление) личного пароля любого пользователя информационных систем персональных данных в случае прекращения его полномочий (увольнение, либо переход на другую работу внутри банка) должна производится немедленно после окончания последнего сеанса работы данного пользователя системы.

Внеплановая полная смена всех паролей должна производится в случае прекращения полномочий (увольнение, переход на другую должность и другие обстоятельства) администраторов информационных систем персональных данных и других сотрудников, которым по роду работы были предоставлены либо полномочия по управлению автоматизированной системой в целом, либо полномочия по управлению подсистемой защиты

информации данной системы, а значит, кроме личного пароля им могут быть известны пароли других пользователей системы.

Администратор безопасности информационной системы персональных данных оказывает необходимую помощь пользователям в процессе смены пароля.

2.3. 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.

2.4. Правила ввода пароля:

ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан и с учётом текущей раскладки клавиатуры;

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

2.5. 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.

2.6. Действия в случае утери и компрометации пароля:

в случае утери пароля сотрудник получает у Администратора безопасности информационной системы персональных данных новый пароль;

в случае компрометации пароля (подсматривание кем-либо, разглашение пароля и др.) пароль необходимо сменить в соответствии с вышеуказанными требованиями.

2.7. Лица, использующие паролирование, обязаны:

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

своевременно сообщать Администратору безопасности информационной системы персональных данных об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей;

по первому требованию Администратора безопасности информационной системы персональных данных предъявлять значения действующего личного пароля для контроля соответствия установленным требованиям, а после проверки провести немедленную его смену.

3. Ответственность

3.1. Ответственность за организацию парольной защиты в подразделении возлагается на Администратора безопасности информационной системы персональных данных.

3.2. Периодический контроль за соблюдением требований данной инструкции возлагается на Администратора безопасности информационной системы персональных данных.

3.3. Владельцы паролей должны быть ознакомлены с данной инструкцией под расписку.

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

Лист ознакомления

№ п/п	Должность	Ф.И.О.	Дата и подпись
1.	Глава Администрации Краснолучского сельского поселения	Шаблий А.С.	
2.	Заместитель главы Администрации по вопросам ЖКХ, строительства и благоустройства	Евтухов Д.П.	
3.	Начальник финансово-экономической службы	Уманчук О.В.	
4.	Главный бухгалтер	Голубева Е.А	
5.	Ведущий специалист экономист	Роман Я.В.	
6.	Ведущий специалист по организационно-кадровой работе	Гетманова М.И.	
7.	Старший инспектор по работе с молодежью, культуре и спорту	Кувардина К.В.	
8.			

Приложение № 17
к распоряжению Администрации
Краснолучского сельского
поселения
от 01.07.2026 №23 ___

ИНСТРУКЦИЯ
по организации защиты информации о событиях безопасности в информационных систем персональных данных в Администрации Краснолучского сельского поселения

1. Общие положения

1.1. Настоящая Инструкция предназначена для организации защиты информации о событиях безопасности в информационных систем персональных данных в Администрации Краснолучского сельского поселения (далее – Администрация).

1.2. Действие настоящей Инструкции распространяется на Администратора безопасности информационных систем персональных данных (далее – Администратор).

2. События безопасности

2.1. К событиям безопасности, подлежащим регистрации в информационных системах персональных данных, принадлежащих Администрации, должны быть отнесены любые проявления состояния информационных систем персональных данных и системы защиты информации, указывающие на возможность нарушения конфиденциальности, целостности или доступности информации, доступности компонентов информационных систем персональных данных, нарушения процедур, установленных организационно-распорядительными документами по защите информации, а также на нарушение штатного функционирования средств защиты информации.

2.2. В информационных системах персональных данных Администрации подлежат регистрации следующие события:

вход/выход, а также попытки входа пользователей в информационные системы персональных данных и загрузки/останова операционной системы;

подключение машинных носителей информации и вывод информации на носители информации;

запуск/завершение программ и процессов (заданий, задач), связанных с обработкой защищаемой информации;

попытки доступа программных средств к определяемым оператором защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам,

файлам, записям, полям записей) и иным объектам доступа;

попытки удаленного доступа.

2.3. Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны обеспечивать возможность идентификации типа события безопасности, даты и времени события безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности.

2.3.1. При регистрации входа/выхода пользователей в информационные системы персональных данных и загрузки/останова операционной системы состав и содержание информации должны, как минимум, включать дату и время входа/выхода в систему/из системы или загрузки/останова операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки/останова операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа.

2.3.2. При регистрации подключения машинных носителей информации и вывода информации на носители информации состав и содержание регистрационных записей должны, как минимум, включать дату и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации.

2.3.3. При регистрации запуска/завершения программ и процессов (заданий, задач), связанных с обработкой защищаемой информации состав и содержание регистрационных записей должны, как минимум, включать дату и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный).

2.3.4. При регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам состав и содержание регистрационных записей должны, как минимум, включать дату и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип).

2.3.5. При регистрации попыток доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, записям, полям записей) состав и содержание информации должны, как минимум, включать дату и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого объекта доступа (логическое имя (номер).

2.3.6. При регистрации попыток удаленного доступа к информационной системе состав и содержание информации должны, как минимум, включать дату и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к информационной системе.

3. Защита информации о событиях безопасности

3.1. В информационных системах персональных данных Администрации должна обеспечиваться защита информации о событиях безопасности.

3.2. Защита информации о событиях безопасности (записях регистрации (аудита)) обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

3.3. Доступ к записям аудита и функциям управления механизмами регистрации (аудита) должен предоставляться только уполномоченным должностным лицам.

3.4. Требования к защите информации о событиях безопасности**:**

в информационных системах персональных данных обеспечивается резервное копирование записей регистрации (аудита);

в информационных системах персональных данных обеспечивается резервное копирование записей регистрации (аудита) на носители однократной записи (неперезаписываемые носители информации);

в информационных системах персональных данных для обеспечения целостности информации о зарегистрированных событиях безопасности должны применяться в соответствии с законодательством Российской Федерации криптографические методы;

оператор предоставляет доступ к записям регистрации событий безопасности (аудита) ограниченному кругу сотрудников.

4. Ответственность

4.1. Ответственность за организацию парольной защиты в подразделении возлагается на Администратора безопасности информационной системы персональных данных.

4.2. Периодический контроль за соблюдением требований данной инструкции возлагается на Администратора безопасности информационной системы персональных данных.

Приложение № 18
к распоряжению Администрации
Краснолучского сельского
поселения
от 01.07.2026_№23 ___

ИНСТРУКЦИЯ
по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационной системы персональных данных Администрации Краснолучского сельского поселения

1. Общие положения

1.1. Инструкция по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем персональных данных Администрации Краснолучского сельского поселения (далее – Администрация), включает в себя описание комплекса организационно-технических мер по проведению работ по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем персональных данных.

1.2. Требования настоящей Инструкции распространяются на всех должностных лиц и сотрудников Администрации, использующих в работе информационные систем персональных данных, в которых осуществляется обработка информации ограниченного доступа, не составляющей государственной тайны.

1.3. Должностные лица Администрации, задействованные в обеспечении функционирования информационных систем персональных данных Администрации, знакомятся с основными положениями и приложениями Инструкции в части, их касающейся, по мере необходимости.

1.4. Ознакомление с требованиями Инструкции пользователей информационных систем персональных данных осуществляет Администратор безопасности информационных систем персональных данных под роспись с выдачей электронных копий соответствующих приложений и разделов Инструкции непосредственно для повседневного использования в работе.

1.5. Непосредственное исполнение настоящей Инструкции определяется Администратором безопасности информационных систем персональных данных по согласованию с ответственным за организацию обработки безопасности персональных данных Администрации.

2. Порядок проведения работ

2.1. Все изменения конфигурации технических и программных средств рабочих станций Администрации должны производиться только на основании заявок, согласованных с Администратором безопасности информационных систем персональных данных.

2.2. Все изменения конфигурации технических и программных средств рабочих станций и серверов, входящих в состав аттестованных по требованиям безопасности информационных систем персональных данных Администрации, должны производиться только на основании заявок, согласованных с руководством Администрации и Администратором безопасности информационных систем персональных данных. При этом необходимо уведомить об осуществленных изменениях организацию, производившую аттестацию, которая принимает решение о необходимости проведения контроля эффективности аттестованного объекта информатизации.

2.3. Все изменения конфигурации технических и программных средств, входящих в состав аттестованных по требованиям безопасности информационных систем персональных данных Администрации, отражаются в Техническом паспорте объекта информатизации. Запрещается изменение состава (в том числе ввод новых) программных средств, осуществляющих обработку ПДн на объектах информатизации, аттестованных по требованиям безопасности информации, без уведомления об предполагаемых изменениях организацию, производившую аттестацию.

2.4. В заявке указываются наименование компьютера и ответственный за него сотрудник. После чего заявка передается Администратору безопасности информационных систем персональных данных для исполнения работ по внесению изменений в конфигурацию программного обеспечения и аппаратных средств информационных систем персональных данных Администрации.

2.5. Право внесения изменений в конфигурацию аппаратно-программных средств информационных систем персональных данных Администрации предоставляется Администратору безопасности информационных систем персональных данных, Администратору информационных систем персональных данных, а также ответственному за организацию обработки персональных данных. Изменение конфигурации аппаратно-программных средств рабочих станций и серверов кем-либо без согласования с Администратором безопасности информационных систем персональных данных и/или ответственным за организацию обработки персональных данных запрещено.

2.6. Установка и настройка программного средства осуществляются Администратором безопасности информационных систем персональных данных и/или Администратором информационных систем персональных данных согласно эксплуатационной документации.

2.7. Запрещается установка и использование на персональных электронных вычислительных машинах (серверах) программного обеспечения, не входящего в Перечень программного обеспечения, разрешенного к использованию в информационных систем персональных данных Администрации Краснолучского сельского поселения (приложение 1).

2.8. Администратор безопасности информационных систем персональных данных Администрации осуществляет контроль за отсутствием на компьютерах сотрудников программного обеспечения и данных, не связанных с выполнением должностных обязанностей.

2.9. Установка (обновление) программного обеспечения (системного, тестового и т.п.) на средствах вычислительной техники производится с эталонных копий программных средств, хранящихся у Администратора информационных систем персональных данных. Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, а также отсутствие вредоносного программного кода.

2.10. После установки (обновления) программного обеспечения Администратор информационных систем персональных данных должен произвести настройку средств управления доступом к компонентам данной задачи (программного средства) в соответствии с требованиями к системе защиты информации и совместно с пользователем компьютера проверить правильность настройки средств защиты.

2.11. После завершения работ по внесению изменений в состав аппаратных средств рабочей станции ее системный блок должен закрываться Администратором безопасности информационных систем персональных данных на ключ (при наличии штатных механических замков) и опечатываться (пломбироваться, защищаться специальной наклейкой).

2.12. Администратор безопасности информационных систем персональных данных должен произвести соответствующую запись в «Журнале фактов вскрытия и опечатывания рабочих станций и серверов, выполнения профилактических работ, установки и модификации программных средств на элементах в ИСПДн» (приложение 2).

2.13. В случае обнаружения недекларированных (не описанных в документации) возможностей программного средства, сотрудники немедленно докладывают Администратору безопасности информационных систем персональных данных. Использование программного средства до получения специальных указаний запрещается.

2.14. Оригиналы заявок (документов) или приказы, на основании которых производились изменения в составе технических или программных средств персональных электронных вычислительных машин с отметками о внесении изменений в состав аппаратно-программных средств должны храниться у Администратора безопасности информационных систем персональных данных Администрации.

3. Порядок пересмотра инструкции

3.1. Инструкция подлежит полному пересмотру при изменении перечня решаемых задач, состава технических и программных средств информационных систем персональных данных Администрации, приводящих к существенным изменениям технологии обработки информации.

3.2. Инструкция подлежит частичному пересмотру в остальных случаях. Частичный пересмотр проводится ответственным за организацию обработки персональных данных в Администрации.

3.3. Полный пересмотр данного документа проводится ответственным за организацию обработки персональных данных Администрации с целью проверки соответствия положений данного документа реальным условиям применения их в информационных систем персональных данных Администрации.

3.4. Вносимые изменения не должны противоречить другим положениям Инструкции.

4. Ответственные за организацию и контроль выполнения инструкции

4.1. Ответственность за организацию контрольных и проверочных мероприятий по вопросам установки, модификации технических и программных средств возлагается на Администратора безопасности информационных систем персональных данных.

4.2. Ответственность за общий контроль информационной безопасности возлагается на ответственного за организацию обработки персональных данных Администрации.

Приложение 1
к инструкции по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационной системы персональных данных Администрации Краснолучского сельского поселения Ростовской области

Перечень программного обеспечения, разрешенного к использованию в информационных систем персональных данных Администрации Краснолучского сельского поселения

– Microsoft Office (OpenOffice, L) – набор программ для работы с текстовыми документами, электронными таблицами, презентациями;

– программа просмотра PDF-документов;

– программа для работы с электронными архивами;

– антивирусный пакет;

– правовые системы (Гарант, Консультант-плюс);

– система электронного делопроизводства и документооборота «ДЕЛО»;

– программное обеспечение для кадрового и бухгалтерского учета «1С: Зарплата и кадры государственного учреждения»;

– дополнительное программное обеспечение, требуемое для выполнения специализированных задач – данное программное обеспечение устанавливается сотрудниками Администрации по предварительной заявке пользователя с учётом наличия официально приобретённой или бесплатно распространяемой версии данной программы и рассмотрения возможности установки её на компьютер пользователя.

Приложение 2
к инструкции по установке,
модификации и техническому
обслуживанию программного
обеспечения и аппаратных средств
информационной системы
персональных данных Администрации
Краснолучского сельского поселения

Журнал фактов вскрытия и опечатывания рабочих станций и серверов, выполнения профилактических работ, установки и модификации программных средств на элементах в ИСПДн

№ п.п	Дата	Описание выполненной работы	ФИО исполнителей и их подписи	ФИО пользователя, подпись
1	2	3	4	5
1.				
2.				
3.				

Приложение № 19
к распоряжению Администрации
Краснолучского сельского
поселения
от 01.07.2026 №23 ___

ИНСТРУКЦИЯ
по обеспечению защиты информации при выводе информационных систем персональных данных из эксплуатации или после принятия решения об окончании обработки информации в Администрации Краснолучского сельского поселения

1. Общие положения

1.1. Настоящая Инструкция разработана с целью обеспечения защиты информации при выводе информационных систем персональных данных из эксплуатации или после принятия решения об окончании обработки информации в Администрации Краснолучского сельского поселения (далее – Администрация).

1.2. Действие настоящей Инструкции распространяется на Администратора безопасности информационных систем персональных данных Администрации (далее – Администратор).

2. Порядок защиты информации

2.1. Обеспечение защиты информации при выводе из эксплуатации информационных систем персональных данных или после принятия решения об окончании обработки информации осуществляется Администратором в соответствии с эксплуатационной документацией на систему защиты информации информационной системы и организационно-распорядительными документами по защите информации и включает:

архивирование информации, содержащейся в информационной системе;

уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

2.2. Архивирование информации, содержащейся в информационной системе, должно осуществляться при необходимости дальнейшего использования информации в деятельности Администрации.

2.3. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации при необходимости передачи машинного носителя информации другому пользователю информационной системы персональных данных или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения производится комиссией, назначенной распоряжением Администрации.

2.4. При выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка информации, в случае, когда их

дальнейшее использование не предполагается или хранение не требуется осуществляется физическое уничтожение этих машинных носителей информации.

2.5. Факт уничтожения персональных данных и/или машинных носителей на которых производилась их обработка и/или хранение оформляется актом. Формы акта приведены в приложении 1.

3. Ответственность

3.1. Ответственность за обеспечение защиты информации при выводе информационных систем персональных данных из эксплуатации или после принятия решения об окончании обработки информации в Администрации возлагается на Администратора.

Приложение 1
к Инструкции

Разрешаю уничтожить
Глава Администрации Краснолучского сельского поселения _____

«_____» _____202__ г.

Акт
об уничтожении персональных данных[8]
(типовая форма)

Комиссия, назначенная распоряжением Администрации от _____ № ____, в составе:

	Должность	Ф.И.О.
Председатель		
Члены комиссии		

провела отбор материальных носителей (бумажных, электронных, магнитных, оптических) персональных данных и установила, что информация, записанная на них в процессе эксплуатации ИСПДн, подлежит уничтожению в соответствии с действующим законодательством Российской Федерации и требованиями руководящих документов по защите информации:

[8] Форма акта уничтожения материальных носителей персональных данных (на бумажных и машинных носителях информации) в соответствии Требованиями к подтверждению уничтожения персональных данных, утвержденных приказом Федеральной службы по надзору Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 № 179

№№ п/п	Наименование (тип) уничтожаемого носителя, содержащего персональные данные субъекта	Регистрационный (учетный) номер носителя	Количество листов (машинных носителей, съемных машинных носителей)	Фамилия, имя, отчество (при наличии) субъекта (субъектов) или иная информация, относящаяся к определенному (определенным) физическому (физическим) лицу (лицам), чьи персональные данные были уничтожены	Перечень категорий персональных данных	Причина уничтожения персональных данных[9]	Примечание

Всего носителей _____
(цифрами и прописью)

Персональные данные уничтожены путем _____.
(стирания информации на машинном носителе средством гарантированного уничтожения в составе СЗИ от НСД Dallas Lock 8.0-К, уничтожения бумажного (машинного) носителя посредством измельчения, сжигания и т.п.)

«____» _____202___ г.
(дата уничтожения носителей персональных данных)

Председатель комиссии: _____ / И.О.Фамилия/
Члены комиссии: _____ / И.О.Фамилия/
_____ / И.О.Фамилия/

Отметки о списании материальных носителей персональных данных в книгах и журналах учета произведены
Ответственный за ведение учета материальных носителей сведений персональных данных:

_____ _____ _____
(должность) (подпись) (фамилия и инициалы)

_____ _____ _____
(должность) (подпись) (фамилия и инициалы)

«_____» _____202____г.

[9] ПДн должны (могут) быть уничтожены в следующих случаях: если они собраны незаконно, истекли установленные сроки хранения, достигнута или изменилась цель их сбора, а также по требованию самого владельца данных. Кроме того, может быть принято решение об уничтожении материальных носителей ПДн, пришедших в негодность

Утверждаю

Разрешаю уничтожить
Глава Администрации Краснолучского сельского поселения _____

«_____» _____202__ г.

Акт
об уничтожении персональных данных[10]
(типовая форма)

Комиссия, назначенная распоряжением Администрации от _____ № ____, в составе:

	Должность	Ф.И.О.
Председатель		
Члены комиссии		

провела проверку информационных систем персональных данных, а также машинных носителей информации, содержащих персональные данные, установила, что информация, записанная на них в процессе эксплуатации ИСПДн, подлежит уничтожению в соответствии с действующим законодательством Российской Федерации и требованиями руководящих документов по защите информации:

[10] Форма акта уничтожения персональных данных в электронной форме в случае их обработки с использованием средств автоматизации в соответствии Требованиями к подтверждению уничтожения персональных данных, утвержденных приказом Федеральной службы по надзору Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 № 179.

№ п/п	Наименование информационной (информационных) системы (систем) персональных данных, из которой (которых) были уничтожены персональные данные субъекта (субъектов) персональных данных	Регистрационный (учетный) номер носителя с которого произведено уничтожение (стирание) (при наличии)	Фамилия, имя, отчество (при наличии) субъекта (субъектов) или иная информация, относящаяся к определенному (определенным) физическому (физическим) лицу (лицам), чьи персональные данные были уничтожены	Перечень категорий персональных данных	Причина уничтожения персональных данных[11]	Примечание

Персональные данные уничтожены путем _____.
(стирания информации на машинном носителе средством гарантированного уничтожения (TERRIER, в составе СЗИ от НСД Dallas Lock 8.0-К или Secret Net, неоднократного форматирования (3 и более раз) и т.п.)
«____» _____202___ г.
(дата уничтожения (стирания) персональных данных) [12]

Приложение: Выгрузка из журнала регистрации событий в информационной системе персональных данных, на _____лист__.

Председатель комиссии: _____ / И.О.Фамилия/
Члены комиссии: _____ / И.О.Фамилия/
_____ / И.О.Фамилия/

[11] ПДн должны (могут) быть уничтожены в следующих случаях: если они собраны незаконно, истекли сроки хранения, достигнута или изменилась цель их сбора, а также по требованию самого владельца данных.
[12] Дата уничтожения может быть вставлена в таблицу

Приложение
к Акту об уничтожении персональных данных

Выгрузка[13]
из журнала регистрации событий в информационной системе персональных данных

№№ п/п	Фамилия, имя, отчество (при наличии) субъекта (субъектов) или иная информация, относящаяся к определенному (определенным) физическому (физическим) лицу (лицам), чьи персональные данные были уничтожены	Перечень категорий уничтоженных персональных данных субъекта (субъектов) персональных данных	Наименование информационной системы персональных данных, из которой были уничтожены персональные данные субъекта (субъектов) персональных данных	Причину уничтожения персональных данных	Дата уничтожения персональных данных субъекта (субъектов) персональных данных	Примечание

Председатель комиссии: _____ / И.О.Фамилия/
Члены комиссии: _____ / И.О.Фамилия/
_____/И.О.Фамилия/

[13] В случае если выгрузка из журнала не позволяет указать отдельные сведения, предусмотренные в таблице, недостающие сведения вносятся в акт об уничтожении персональных данных.

Приложение № 20
к распоряжению Администрации
Краснолучского сельского
поселения
от 01.07.2026_№23 ___

ПОРЯДОК
уничтожения и блокирования персональных данных в Администрации Краснолучского сельского поселения

1. Общие положения

1.1. Настоящий Порядок уничтожения и блокирования персональных данных (далее – Порядок) Администрации Краснолучского сельского поселения (далее – Администрация) определяет условия и способы уничтожения:

бумажных носителей (документов), содержащих персональные данные по достижению цели обработки этих персональных данных;

персональных данных в машинных носителях информации, в том числе персональных данных, и при необходимости самих машинных носителей информации.

2. Блокирование и уничтожение персональных данных, содержащихся в машинных носителях информации

2.1. Блокирование информации, содержащей персональные данные субъекта персональных данных, производится в случаях:

если персональные данные являются неполными, устаревшими, недостоверными;

если сведения являются незаконно полученными или не являются необходимыми для заявленной оператором персональных данных цели обработки.

2.2. В случае подтверждения факта недостоверности персональных данных работник, ответственный за организацию обработки персональных данных (далее – Ответственный), на основании документов, представленных субъектом персональных данных, обязан уточнить персональные данные и принять меры к их блокированию.

2.3. В случае выявления неправомерных действий с персональными данными Ответственный обязан устранить (организовать устранение) допущенные нарушения. В случае невозможности устранения допущенных нарушений необходимо в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, уничтожить персональные данные.

2.4. Об устранении допущенных нарушений или об уничтожении персональных данных Ответственный обязан уведомить субъекта персональных данных, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также уведомить указанный орган.

2.5. Ответственный обязан уничтожить персональные данные субъекта персональных данных в случаях:

достижения цели обработки персональных данных;

отзыва субъектом персональных данных согласия на обработку своих персональных данных;

в случае, указанном в п. 2.3. настоящего Порядка.

2.6. Уничтожение персональных данных должно быть осуществлено в течение трех дней с момента наступления таких случаев.

2.7. В согласии субъекта персональных данных на обработку его персональных данных могут быть установлены иные сроки уничтожения персональных данных при достижении цели обработки персональных данных.

3. Работа с бумажными носителями (документами)

3.1. Виды и периоды уничтожения бумажных носителей, содержащих персональные данные, представлены в таблице 1.

Таблица 1

Виды и периоды уничтожения бумажных носителей, содержащих персональные данные

№ п/п	Документ	Срок хранения	Действия по окончании срока хранения
1.	Документы (сведения, содержащие персональные данные о работниках Оператора), переданные и сформированные при трудоустройстве работника	законченные делопроизводством до 1 января 2003 года, хранятся 75 лет законченные делопроизводством после 1 января 2003 года, хранятся 50 лет	Сдача в архив
2.	Документы, содержащие персональные данные субъекта, не являющегося сотрудником	Установленные для данных документов сроки хранения	Уничтожение
3.	Иные документы (журналы учёта, списки и т.п.)	Хранятся до замены на новые, если не указан конкретный срок хранения	Уничтожение

3.2. По окончании срока хранения документы, указанные в п. 3.1. Порядка передаются в архив либо уничтожаются путём сжигания, измельчения на мелкие части (или иным способом), исключающие возможность последующего восстановления информации или сжигаются.

4. Работа с машинными носителями информации

4.1. Виды и периоды уничтожения персональных данных, хранимых в электронном виде («файлах») на жестком диске компьютера (далее – НЖМД) и машинных носителях: компакт дисках (далее – CD-R/RW, DVD-R/RW в зависимости от формата), FLASH-накопителях.

4.2. Пример видов и периодов уничтожения персональных данных, хранимых в электронном виде на НЖМД, представлен в таблице 2.

Таблица 2

Виды и периоды уничтожения персональных данных, хранимых в электронном виде на жестком диске компьютера

№ п/п	Информация, вид носителя	Срок хранения	Действия по окончании срока хранения
1.	База данных автоматизированной информационной системы Оператора Носитель: файлы на НЖМД	До достижения целей обработки или утраты необходимости в достижении указанных целей До создания более актуальной копии	Повторное использование носителя для записи очередной резервной копии БД, в случае невозможности – уничтожение носителя; удаление архивных файлов с НЖМД
2.	База данных информационной системы « 1С: Зарплата и кадры государственного учреждения»	До достижения целей обработки или утраты необходимости в достижении указанных целей До создания более актуальной копии	Повторное использование носителя для записи очередной резервной копии БД, в случае невозможности – уничтожение носителя; удаление архивных файлов с НЖМД
3.	База данных информационной системы «Система электронного делопроизводства и документооборота «ДЕЛО»	До достижения целей обработки или утраты необходимости в достижении указанных целей До создания более актуальной копии	Повторное использование носителя для записи очередной резервной копии БД, в случае невозможности – уничтожение носителя; удаление архивных файлов с НЖМД

4.3. Машинные носители информации (за исключением НЖМД), перечисленные в п. 4.1. Порядка должны находиться в сейфе, опечатываемом печатью (кроме формируемых или обрабатываемых в данный момент на рабочем месте).

4.4. По окончании сроков хранения, машинные носители информации, подлежащие уничтожению, физически уничтожаются с целью невозможности восстановления и дальнейшего их использования. Это достигается путём деформирования, нарушения единой целостности носителя или его сжигания.

4.5. Подлежащие уничтожению файлы, расположенные на жестком диске ПЭВМ, удаляются средствами операционной системы с последующим «очищением корзины» либо с использованием программных средств гарантированного стирания информации, сертифицированных ФСТЭК России.

4.6. В случае допустимости повторного использования носителя формата CD-RW, DVD-RW, FLASH применяется программное удаление («затирание») содержимого диска путём его форматирования с последующей записью новой информации на данный носитель или использования программных средств гарантированного стирания информации, сертифицированных ФСТЭК России.

5. Порядок оформления и хранения документов об уничтожении персональных данных, а также их носителей

5.1. Уничтожение (стирание) персональные данных, а также их материальных носителей осуществляет специальная Комиссия, создаваемая распоряжением главы Администрации.

5.2. В ходе процедуры уничтожения носителей персональных данных необходимо присутствие членов Комиссии, осуществляющей уничтожение персональных данных и иной конфиденциальной информации, находящейся на технических средствах.

5.3. В случае если обработка персональных данных осуществляется оператором без использования средств автоматизации, документом, подтверждающим уничтожение персональных данных субъектов персональных данных, является акт об уничтожении персональных данных (Приложение 1).

5.4. В случае если обработка персональных данных осуществляется оператором с использованием средств автоматизации, документами, подтверждающими уничтожение персональных данных субъектов персональных данных, являются акт об уничтожении персональных данных и выгрузка из журнала регистрации событий в информационной системе персональных данных (далее - выгрузка из журнала) (Приложение 2).

5.5. Акт об уничтожении персональных данных (Приложения 1, 2), составляется и подписывается Комиссией и утверждается главой Администрации. Выгрузка из журнала (Приложение 2) подписывается Комиссией и прилагается к акту.

В случае если выгрузка из журнала не позволяет указать отдельные сведения, предусмотренные Приложением 2, недостающие сведения вносятся в акт об уничтожении персональных данных (Приложение 2).

Приложение 1
к Порядку

Разрешаю уничтожить
Глава Администрации Краснолучского сельского поселения

_____

«_____» _____202__ г.

Акт
об уничтожении персональных данных[14]
(типовая форма)

Комиссия, назначенная распоряжением Администрации от _____ № ____, в составе:

	Должность	Ф.И.О.
Председатель		
Члены комиссии		

провела отбор материальных носителей (бумажных, электронных, магнитных, оптических) персональных данных и установила, что информация, записанная на них в процессе эксплуатации ИСПДн, подлежит уничтожению в соответствии с действующим законодательством Российской Федерации и требованиями руководящих документов по защите информации:

№№ п/п	Наименование (тип) уничтожаемого носителя, содержащего персональные данные субъекта	Регистрационный (учетный) номер носителя	Количество листов (машинных носителей, съемных машинных носителей)	Фамилия, имя, отчество (при наличии) субъекта (субъектов) или иная информация, относящаяся к определенному (определенным) физическому (физическим) лицу (лицам), чьи персональные данные были уничтожены	Перечень категорий персональных данных	Причина уничтожения персональных данных[15]	Примечание

Всего носителей _____

[14] Форма акта уничтожения материальных носителей персональных данных (на бумажных и машинных носителях информации) в соответствии Требованиями к подтверждению уничтожения персональных данных, утвержденных приказом Федеральной службы по надзору Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 № 179

[15] ПДн должны (могут) быть уничтожены в следующих случаях: если они собраны незаконно, истекли установленные сроки хранения, достигнута или изменилась цель их сбора, а также по требованию самого владельца данных. Кроме того, может быть принято решение об уничтожении материальных носителей ПДн, пришедших в негодность

(цифрами и прописью)

Персональные данные уничтожены путем _____.
(стирания информации на машинном носителе средством гарантированного уничтожения в составе СЗИ от НСД Dallas Lock 8.0-К, уничтожения бумажного (машинного) носителя посредством измельчения, сжигания и т.п.)
«____» _____202___ г.
(дата уничтожения носителей персональных данных)

Председатель комиссии: _____ / И.О.Фамилия/
Члены комиссии: _____ / И.О.Фамилия/
_____ / И.О.Фамилия/

Отметки о списании материальных носителей персональных данных в книгах и журналах учета произведены
Ответственный за ведение учета материальных носителей сведений персональных данных:

_____	_____	_____
(должность)	(подпись)	(фамилия и инициалы)
_____	_____	_____
(должность)	(подпись)	(фамилия и инициалы)

«_____» _____202____г.

Приложение 2
к Порядку

Разрешаю уничтожить
Глава Администрации Краснолучского сельского поселения

_____

«_____» _____202__ г.

Акт
об уничтожении персональных данных[16]
(типовая форма)

Комиссия, назначенная распоряжением Администрации от _____ № ____, в составе:

	Должность	Ф.И.О.
Председатель		
Члены комиссии		

провела проверку информационных систем персональных данных, а также машинных носителей информации, содержащих персональные данные, установила, что информация, записанная на них в процессе эксплуатации ИСПДн, подлежит уничтожению в соответствии с действующим законодательством Российской Федерации и требованиями руководящих документов по защите информации:

[16] Форма акта уничтожения персональных данных в электронной форме в случае их обработки с использованием средств автоматизации в соответствии Требованиями к подтверждению уничтожения персональных данных, утвержденных приказом Федеральной службы по надзору Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 № 179.

№ п/п	Наименование информационной (информационных) системы (систем) персональных данных, из которой (которых) были уничтожены персональные данные субъекта (субъектов) персональных данных	Регистрационный (учетный) номер носителя с которого произведено уничтожение (стирание) (при наличии)	Фамилия, имя, отчество (при наличии) субъекта (субъектов) или иная информация, относящаяся к определенному (определенным) физическому (физическим) лицу (лицам), чьи персональные данные были уничтожены	Перечень категорий персональных данных	Причина уничтожения персональных данных[17]	Примечание

Персональные данные уничтожены путем _____.
(стирания информации на машинном носителе средством гарантированного уничтожения (TERRIER, в составе СЗИ от НСД Dallas Lock 8.0-К или Secret Net, неоднократного форматирования (3 и более раз) и т.п.)
«____» _____202___ г.
(дата уничтожения (стирания) персональных данных) [18]

Приложение: Выгрузка из журнала регистрации событий в информационной системе персональных данных, на _____лист__.

Председатель комиссии: _____ / И.О.Фамилия/
Члены комиссии: _____ / И.О.Фамилия/
_____ / И.О.Фамилия/

[17] ПДн должны (могут) быть уничтожены в следующих случаях: если они собраны незаконно, истекли сроки хранения, достигнута или изменилась цель их сбора, а также по требованию самого владельца данных.
[18] Дата уничтожения может быть вставлена в таблицу

Приложение
к Акту об уничтожении персональных данных

Выгрузка[19]
из журнала регистрации событий в информационной системе персональных данных

№№ п/п	Фамилия, имя, отчество (при наличии) субъекта (субъектов) или иная информация, относящаяся к определенному (определенным) физическому (физическим) лицу (лицам), чьи персональные данные были уничтожены	Перечень категорий уничтоженных персональных данных субъекта (субъектов) персональных данных	Наименование информационной системы персональных данных, из которой были уничтожены персональные данные субъекта (субъектов) персональных данных	Причину уничтожения персональных данных	Дата уничтожения персональных данных субъекта (субъектов) персональных данных	Примечание

Председатель комиссии: _____ / И.О.Фамилия/
Члены комиссии: _____ / И.О.Фамилия/
_____/И.О.Фамилия/

[19] В случае если выгрузка из журнала не позволяет указать отдельные сведения, предусмотренные в таблице, недостающие сведения вносятся в акт об уничтожении персональных данных.

Приложение № 21
к распоряжению Администрации
Краснолучского сельского
поселения
от 01.07.2026 №23 ___

ПОЛОЖЕНИЕ
об обработке персональных данных без использования средств автоматизации в администрации Краснолучского сельского поселения

1. Общие положения

1.1. Настоящее Положение об обработке персональных данных без использования средств автоматизации администрации Краснолучского сельского поселения (далее — Положение) применяется с учетом требований постановления Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

1.2. В настоящем Положении используются следующие определения:

блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных) (статья 3 Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» (далее — статья 3 Федерального закона № 152-ФЗ);

обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных (статья 3 Федерального закона № 152-ФЗ);

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

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

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

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

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

2.3. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники Администрации Краснолучского сельского поселения далее – Администрация) или лица, осуществляющие такую обработку по договору с Администрацией, должны быль проинформированы о факте обработки ими персональных данных, обработка которых осуществляется Администрацией без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов, Российской Федерации, а также локальными правовыми актами Администрации.

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

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

типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку

персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;

типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных.

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

необходимость ведения такого журнала должна быть предусмотрена актом Администрации, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных;

копирование содержащейся в таких журналах информации не допускается;

персональные данные каждого субъекта персональных данных могут заноситься в такой журнал не более 1 (одного) раза в каждом случае пропуска субъекта персональных данных.

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

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

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

3.1. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения

персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

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

3.3. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются распоряжением Администрации Краснолучского сельского поселения.

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

4.1. Ответственность за соблюдение требований по защите информации ограниченного доступа и надлежащего порядка проводимых работ возлагается на сотрудников Администрации, имеющих доступ к такой информации.

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

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

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

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

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

Приложение № 22
к распоряжению Администрации
Краснолучского сельского
поселения
от 01.07.2026 №23 ___

ЛИСТ ОЗНАКОМЛЕНИЯ
с положениями законодательства Российской Федерации о персональных данных, локальными актами по вопросам обработки персональных данных, требованиями к защите персональных данных в Администрации Краснолучского сельского поселения

Я _____
(Фамилия Имя Отчество)
подтверждаю, что ознакомлен(а) с действующими на момент подписания нижеперечисленными нормативными правовыми актами, локальными нормативными актами, требованиями. Их текст мною прочитан, содержание понятно.

№ п/п	Нормативные правовые акты, локальные нормативные акты, требования	Дата ознакомления	подпись
1.	Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных; Глава 14 Трудового кодекса Российской Федерации; Постановление Правительства РФ от 06.07.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»; Постановление Правительства РФ от 21.03.2012 №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными и муниципальными органами»; Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных		

	при их обработке и информационных системах персональных данных»;		
2.	План мероприятий по обеспечению защиты персональных данных в информационных системах персональных данных, утвержденный распоряжением Администрации Краснолучского сельского поселения от _____ №_____; Иные порядки, положения, регламенты и инструкции по защите персональных данных, утвержденные в Администрации Краснолучского сельского поселения.		

Приложение № 23
к распоряжению Администрации
Краснолучского сельского
поселения
от 01.07.2026 №23 ___

Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям безопасности информации в информационной системе персональных данных Администрации Краснолучского сельского поселения

1. Общие положения

Настоящими правилами осуществления внутреннего контроля соответствия обработки персональных данных, требованиям безопасности информации в информационной системе персональных данных (далее – ИСПДн) Администрации Краснолучского сельского поселения (далее – Администрация), определяются процедуры, направленные на выявление и предотвращение нарушений установленных требований по защите информации в ИСПДн.

Настоящие правила определяют порядок внутреннего контроля соответствия обработки защищаемой информации, в т. ч. персональных данных, требованиям безопасности информации в ИСПДн и действуют постоянно.

2. Требования к организации внутреннего контроля

В целях осуществления внутреннего контроля обеспечения безопасности информации в ИСПДн организуется проведение периодических проверок условий обработки защищаемой информации.

Проверка включает в себя:

контроль реализации правил разграничения доступа, полномочий пользователей в ИСПДн;

контроль соблюдения пользователями ИСПДн правил организации парольной защиты;

контроль соблюдения пользователями ИСПДн установленных правил антивирусной защиты;

контроль соблюдения установленных в ИСПДн правил работы с материальными носителями информации;

контроль соблюдения порядка доступа в помещения, где расположены элементы ИСПДн и ведется обработка защищаемой информации;

контроль соблюдения порядка резервирования информации и хранения резервных копий;

контроль соблюдения порядка работы со средствами защиты информации;

контроль знания и соблюдения пользователями ИСПДн внутренних документов по защите информации.

Проверки осуществляются ответственным за защиту информации совместно с администратором ИСПДн (далее - комиссия).

Проверки проводятся на основании утвержденного главой Администрации Плана мероприятий по защите персональных данных, содержащего Перечень мероприятий по контролю за обеспечением безопасности информации, в т. ч. персональных данных, в ИСПДн (приложение 1).

При проведении проверки обеспечения безопасности информации в ИСПДн установленным требованиям должны быть полностью объективно и всесторонне установлены:

порядок и условия применения организационных и технических мер по защите информации, исполнение которых обеспечивает установленный уровень защищенности ПДн в ИСПДн;

соответствие состава и структуры программно-технических средств ИСПДн документированному составу и структуре средств, представленному в техническом паспорте ИСПДн;

порядок и условия применения средств защиты информации;

порядок и условия допуска лиц в помещения, где размещены средства ИСПДн;

порядок организации и правильности учета машинных носителей информации;

соблюдение установленных правил доступа субъектов доступа к объектам доступа;

соблюдение установленного порядка использования мобильных технических средств;

наличие (отсутствие) фактов несанкционированного доступа к информации и принятие необходимых мер;

соблюдение установленных правил организации парольной и антивирусной защиты;

знание персоналом базы нормативно-методических документов по защите информации.

При проведении внутренней проверки комиссия имеет право:

запрашивать у сотрудников Администрации, допущенных к работе в ИСПДн, информацию, необходимую для реализации полномочий;

принимать меры по приостановлению или прекращению обработки защищаемой информации, осуществляемой с нарушением требований законодательства Российской Федерации;

вносить главе Администрации предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности информации;

вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в области защиты информации.

Мероприятия, проведенные в ходе внутреннего контроля, должны быть занесены в журнал учета мероприятий по контролю за обеспечением защиты информации в ИСПДн (приложение 2).

В отношении информации, ставшей известной комиссии в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность.

Проверка должна быть завершена не позднее чем через месяц со дня принятия решения о её проведении. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений составляется протокол (приложение 3), который должен быть представлен главе Администрации для ознакомления.

Приложение 1
к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям безопасности информации в информационной системе персональных данных Администрации Краснолучского сельского поселения

Перечень
мероприятий по контролю за обеспечением безопасности персональных данных в информационных системах персональных данных Администрации Краснолучского сельского поселения

Мероприятие	Периодичность	Исполнитель
Проверка работоспособности и контроля соблюдения правил эксплуатации СКЗИ, в соответствии с эксплуатационной документацией на СКЗИ	1 раз в месяц	Ответственный за обеспечение функционирования и безопасности криптографических средств
Проверка соответствия состава и структуры программно-технических средств ИСПДн документированному составу и структуре средств, представленному в техническом паспорте ИСПДн	1 раз в 6 месяцев	Ответственный за организацию обработки и обеспечение безопасности персональных данных Администратор ИСПДн
Проверка выполнения требований по условиям расположения СВТ в помещениях, в которых размещены элементы ИСПДн	1 раз в 6 месяцев	Ответственный за организацию обработки и обеспечение безопасности персональных данных Администратор ИСПДн
Проверка целостности опечатывания системных блоков и	1 раз в 6 месяцев	Администратор безопасности ИСПДн

Мероприятие	Периодичность	Исполнитель
других ТС, участвующих в обработке информации		
Проверка организации допуска лиц в помещения, где размещены средства ИСПДн, в т. ч. перечня лиц, имеющих право доступа в помещения ИСПДн	1 раз в 3 месяца	Ответственный за организацию обработки и обеспечение безопасности персональных данных Администратор ИСПДн
Проверка актуальности перечня лиц, допущенных к работе в ИСПДн	1 раз в 3 месяца	Ответственный за организацию обработки и обеспечение безопасности персональных данных Администратор безопасности ИСПДн
Проверка соответствия реального уровня полномочий по доступу к информации различных пользователей, установленному в матрице доступа	1 раз в 3 месяца	Администратор безопасности ИСПДн
Проверка организации учета средств защиты информации, используемых в ИСПДн	1 раз в 6 месяцев	Ответственный за организацию обработки и обеспечение безопасности персональных данных
Проверка наличия документов, подтверждающих возможность применения технических и программных средств защиты информации (сертификатов соответствия и других документов)	1 раз в 6 месяцев	Ответственный за организацию обработки и обеспечение безопасности персональных данных Администратор безопасности ИСПДн
Проверка неизменности настроенных параметров средств	1 раз в месяц	Администратор безопасности

Мероприятие	Периодичность	Исполнитель
защиты информации, используемых в ИСПДн		
Контроль состава программного обеспечения	1 раз в 3 месяца	Администратор ИСПДн
Контроль правил заведения и удаления учетных записей пользователей	1 раз в 6 месяцев	Ответственный за организацию обработки и обеспечение безопасности персональных данных Администратор безопасности ИСПДн
Проверка соблюдения установленных правил организации парольной защиты	1 раз в 6 месяца	Администратор ИСПДн, Администратор безопасности ИСПДн
Контроль соблюдения установленных правил организации антивирусной защиты	1 раз в 3 месяца	Администратор ИСПДн, Администратор безопасности ИСПДн
Проверка работоспособности системы резервного копирования	1 раз в 6 месяцев	Администратор ИСПДн
Проверка организации учета и условий хранения материальных носителей информации	1 раз в 6 месяцев	Ответственный за организацию обработки и обеспечение безопасности персональных данных Администратор безопасности ИСПДн
Проверка знаний персоналом базы нормативно-методических документов по защите информации	1 раз в 6 месяцев	Ответственный за организацию обработки и обеспечение безопасности персональных данных
Организация анализа и пересмотра имеющихся угроз безопасности информации ИСПДн, а также	Не реже 1 раза в год	Ответственный за организацию обработки и обеспечение

Мероприятие	Периодичность	Исполнитель
предсказание появления новых, еще неизвестных, угроз		безопасности персональных данных Администратор ИСПДн

План
мероприятий по контролю за обеспечением безопасности персональных данных в информационных системах персональных данных Администрации Краснолучского сельского поселения Ростовской области на 2026 год

Мероприятие	Дата	Исполнитель	Отметка о выполнении
Проверка работоспособности и соблюдения правил эксплуатации СКЗИ, в соответствии с эксплуатационной документацией на СКЗИ	25.12.2026	Ответственный за обеспечение функционирования и безопасности криптографических средств	
Проверка соответствия состава и структуры программно-технических средств ИСПДн документированному составу и структуре средств, представленному в техническом паспорте ИСПДн	25.12.2026	Ответственный за организацию обработки и обеспечение безопасности персональных данных Администратор ИСПДн	
Проверка выполнения требований по условиям расположения СВТ в помещениях, в которых размещены элементы ИСПДн	25.12.2026	Ответственный за организацию обработки и обеспечение безопасности персональных данных Администратор ИСПДн	
Проверка целостности опечатывания системных блоков и других ТС, участвующих в обработке информации	25.12.2026	Администратор безопасности ИСПДн	
Проверка организации допуска лиц в помещения, где размещены средства ИСПДн, в т. ч. Перечня лиц, имеющих право	25.12.2026	Ответственный за организацию обработки и обеспечение безопасности	

Мероприятие	Дата	Исполнитель	Отметка о выполнении
доступа в помещения ИСПДн		персональных данных Администратор ИСПДн	
Проверка актуальности перечня лиц, допущенных к работе в ИСПДн	25.12.2026	Ответственный за организацию обработки и обеспечение безопасности персональных данных Администратор безопасности ИСПДн	
Проверка соответствия реального уровня полномочий по доступу к информации различных пользователей, установленному в матрице доступа	25.12.2026	Администратор безопасности ИСПДн	
Проверка организации учета средств защиты информации, используемых в ИСПДн	25.12.2026	Ответственный за организацию обработки и обеспечение безопасности персональных данных	
Проверка наличия документов, подтверждающих возможность применения технических и программных средств защиты информации (сертификатов соответствия и других документов)	25.12.2026	Ответственный за организацию обработки и обеспечение безопасности персональных данных Администратор безопасности ИСПДн	
Проверка неизменности настроенных параметров средств защиты	25.12.2026	Администратор безопасности	

Мероприятие	Дата	Исполнитель	Отметка о выполнении
информации, используемых в ИСПДн			
Контроль состава программного обеспечения	25.12.2026	Администратор ИСПДн	
Контроль правил заведения и удаления учетных записей пользователей	25.12.2026	Ответственный за организацию обработки и обеспечение безопасности персональных данных Администратор безопасности ИСПДн	
Проверка соблюдения установленных правил организации парольной защиты	25.12.2026	Администратор ИСПДн, Администратор безопасности ИСПДн	
Контроль соблюдения установленных правил организации антивирусной защиты	25.12.2026	Администратор ИСПДн, Администратор безопасности ИСПДн	
Проверка работоспособности системы резервного копирования	25.12.2026	Администратор ИСПДн	
Проверка организации учета и условий хранения материальных носителей информации	25.12.2026	Ответственный за организацию обработки и обеспечение безопасности персональных данных Администратор безопасности ИСПДн	
Проверка знаний персоналом базы нормативно-методических документов по защите информации	25.12.2026	Ответственный за организацию обработки и обеспечение безопасности	

Мероприятие	Дата	Исполнитель	Отметка о выполнении
		персональных данных	
Организация анализа и пересмотра имеющихся угроз безопасности информации ИСПДн, а также предсказание появления новых, еще неизвестных, угроз	25.12.2026	Ответственный за организацию обработки и обеспечение безопасности персональных данных Администратор ИСПДн	

Приложение 2
к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям безопасности информации в информационной системе персональных данных Администрации Краснолучского сельского поселения

Журнал учета мероприятий по контролю за обеспечением защиты информации в ИСПДн
(типовая форма)

Начат «____» _____ 20__ г.

Окончен «____» _____ 20__ г.

На _____листах

_____ _____
должность и Ф.И.О. ответственного за ведение и хранение журнала Подпись

№ п/п	Мероприятие	Дата	Исполнитель	Результат

Приложение 3

к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям безопасности информации в информационной системе персональных данных Администрации Краснолучского сельского поселения

А К Т
результатов проведения внутренней проверки
обеспечения безопасности информации в ИСПДн

Настоящий АКТ составлен в том, что «___» _____ 20__ года комиссией в составе: ответственного за организацию обработки и обеспечение безопасности ПДн, администратора ИСПДн, администратора безопасности ИСПДн, была проведена плановая внутренняя проверка обеспечения безопасности информации в ИСПДн.

Проверка осуществлялась в соответствии с требованиями _____

название внутреннего локального акта

Проверено:

_____

_____

Выявлено:

_____

_____

Меры по устранению нарушений:

_____

_____

Срок устранения нарушений: _____.

Проверку провели:

_____ _____ /_____/

_____ _____ /_____/

_____ _____ /_____/

«___» _____ 20__ года

С результатами проверки ознакомлен:

Глава Администрации Краснолучского сельского поселения _____ /_____/

«___» _____ 20__ года