ГЛАВА
СЕЛЬСКОГО ПОСЕЛЕНИЯ КРАСНЫЙ ЯР
МУНИЦИПАЛЬНОГО РАЙОНА КРАСНОЯРСКИЙ
САМАРСКОЙ ОБЛАСТИ

РАСПОРЯЖЕНИЕ

от «18» августа 2022 года № 53

Об утверждении документов по защите и обеспечению безопасности персональных данных при их обработке в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области

В целях осуществления мероприятий по защите и обеспечению безопасности персональных данных при их обработке в информационных системах Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, в соответствии с Федеральными законами от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных», постановлениями Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», 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», от 01.12.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», руководствуясь Уставом сельского поселения Красный Яр муниципального района Красноярский Самарской области:

1. Утвердить следующие документы по защите и обеспечению безопасности персональных данных при их обработке в Администрации

сельского поселения Красный Яр муниципального района Красноярский Самарской области:

1.1. Политику Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области в отношении обработки персональных данных в порядке, установленном Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (Приложение № 1).

1.2. Положение об обеспечении безопасности персональных данных в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области. (Приложение № 2).

1.3. Правила работы с обезличенными персональными данными в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области. (Приложение № 3).

1.4. Перечень персональных данных, обрабатываемых в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области. (Приложение №4).

1.5. Перечень должностей в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных (Приложение № 5).

1.6. Перечень должностей в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным (Приложение № 6).

1.7. Форма обязательства о неразглашении информации, содержащей персональные данные в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области. (Приложение № 7).

1.8. Типовая форма согласия на обработку персональных данных в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области. (Приложение № 8).

1.8.1. Типовая форма согласия на обработку персональных данных для реализации служебных (трудовых) отношений (Приложение 8.1.)

1.8.2. Согласие на обработку персональных данных, разрешённых субъектом персональных данных для распространения (Приложение 8.2.)

1.8.3. Согласие субъекта персональных данных на обработку персональных данных при предоставлении муниципальной услуги. (Приложение 8.3.)

1.9. Порядок доступа в помещения, в которых ведётся обработка персональных данных, в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области. (Приложение №9).

1.10. Правила рассмотрения запросов субъектов персональных данных или их представителей в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области. (Приложение №10).

1.11. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (Приложение № 11).

1.12. Инструкция по организации антивирусной защиты в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области. (Приложение №12).

1.13. Порядок учета, хранения и уничтожения носителей персональных данных в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области. (Приложение № 13).

1.14. Порядок реагирования на инциденты информационной безопасности в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области. (Приложение № 14).

1.15. Инструкция должностного лица, ответственного за организацию обработки персональных данных в информационных системах персональных данных (Приложение № 15).

1.16. Инструкция пользователя информационной системы персональных данных в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области (Приложение № 16).

1.17. Инструкция ответственного за обеспечение безопасности защиты персональных данных (Приложение № 17).

1.18. Инструкция по учету лиц, допущенных к работе с персональными данными в информационных системах персональных данных (Приложение № 18).

1.19. Инструкция по проведению инструктажа лиц, допущенных к работе с информационной системой персональных данных (Приложение № 19).

1.20. Порядок резервного копирования и восстановления данных (Приложение № 20).

1.21. Инструкция по действиям персонала во внештатных ситуациях при обработке конфиденциальной информации и персональных данных(Приложение № 21).

1.22. Модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Приложение № 22).

1.23. Утвердить форму договора получения на обработку персональных данных (Приложение № 23)

1.24. Утвердить перечень информационных систем персональных данных (Приложение № 24)

1.25. Утвердить Инструкцию по порядку учёта, хранения и уничтожения съёмных носителей персональных данных (Приложение № 25)

1.26. Утвердить форму журнала по учету обращений субъектов персональных данных о выполнении их законных прав в области защиты персональных данных, при обработке персональных данных, в том числе в информационных системах персональных данных(Приложение № 26).

1.27. Форму журнала учета лиц, допущенных к персональным данным (Приложение № 27)

1.28. Утвердить форму журнала учёта прохождения первичного инструктажа работниками, допущенными к работе с ПДН в ИСПДН (Приложение № 28)

1.29. Форму журнала учета нештатных ситуаций, фактов вскрытия и опечатывания пэвм, выполнения профилактических работ, установки и

модификации аппаратных и программных средств информационной системы персональных данных (Приложение № 29).

1.30. Положение об организации режима обеспечения безопасности помещений, в которых размещены информационные системы персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения и план-схему контролируемой зоны помещений по адресу: Самарская область, Красноярский район, село Красный Яр, улица Комсомольская, д.90 2 этаж. (Приложение № 30)

1.31. Инструкция по обращению с криптосредствами (Приложение № 31)

1.32. Инструкция по организации парольной защиты в информационных системах персональных данных (Приложение № 32)

1.33. Правила оценки вреда, который может быть причинён субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных (Приложение № 33)

1.34. Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные (Приложение № 34)

1.35. Положение об обработке и защите персональных данных посетителей веб-сайта администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области (Приложение № 35)

2. Разместить данное распоряжение и документы по защите и обеспечению безопасности персональных данных при их обработке в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области на сайте https://kryarposelenie.ru/ в разделе структура власти/ Администрация/персональные данные.

3. Заместителю Главы Ведерникову А.В. ознакомить муниципальных служащих и работников, занимающих должности, не отнесённых к должностям муниципальной службы, и осуществляющих обеспечение деятельности администрации поселения с данным распоряжение под подпись.

4. Распоряжение вступает в силу с 1 сентября 2022 года.

5. Контроль за исполнением распоряжения оставляю за собой.

Глава сельского поселения
Красный Яр муниципального района
Красноярский Самарской области А.Г. Бушов

Ведерников А.В.

Приложение № 1

УТВЕРЖДЕНА
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

ПОЛИТИКА АДМИНИСТРАЦИИ СЕЛЬСКОГО ПОСЕЛЕНИЯ КРАСНЫЙ ЯР МУНИЦИПАЛЬНОГО РАЙОНА КРАСНОЯРСКИЙ САМАРСКОЙ ОБЛАСТИ В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

ОПРЕДЕЛЕНИЯ

Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту 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 оператором 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 оператора.

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.

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

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Правовая основа

Политика Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области в отношении обработки персональных данных, в порядке, установленном Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее Политика):

- Трудового кодекса Российской Федерации;

- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ);

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

- 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 «Перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствие с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

Настоящая Политика устанавливает единый порядок обработки персональных данных в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области.

1.2. Цель Политики

Целью настоящей Политики является обеспечение безопасности персональных данных граждан от несанкционированного доступа, неправомерного их использования или утраты.

Настоящая Политика устанавливает и определяет:

- процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных;

- цели обработки персональных данных;

- перечень обрабатываемых персональных данных;

- категории субъектов, персональные данные которых обрабатываются;

- сроки обработки и хранения обрабатываемых персональных данных;

- порядок уничтожения обработанных персональных данных при достижении целей обработки или при наступлении иных законных оснований;

- правила рассмотрения запросов субъектов персональных данных или их представителей;

- правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к обеспечению безопасности персональных данных, установленных Федеральным законом № 152-ФЗ, принятыми в соответствии с ним нормативными правовыми актами и локальными актами Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области;

- правила работы с обезличенными данными;

- перечень информационных систем персональных данных;

- перечень должностей Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных;

- перечень должностей, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;

- ответственного за организацию обработки персональных данных;

- обязательство лица, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним трудового договора (контракта) прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей;

- типовую форму согласия на обработку персональных данных субъектов персональных данных;

- порядок доступа в помещения, в которых ведется обработка персональных данных.

1.3. Основные условия обработки персональных данных

Обработка персональных данных осуществляется после принятия необходимых мер по обеспечению безопасности персональных данных, а именно:

- после получения согласия субъекта персональных данных, в соответствии с частью 2 статьи 6 Федерального закона № 152-ФЗ;

- после направления уведомления об обработке персональных данных в Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, за исключением случаев, предусмотренных частью 2 статьи 22 Федерального закона от 27.07.2006 № 152-ФЗ;

Лица, допущенные к обработке персональных данных, под подпись знакомятся с настоящей Политикой и подписывают обязательство о неразглашении информации, содержащей персональные данные.

2. ПРОЦЕДУРЫ, НАПРАВЛЕННЫЕ НА ВЫЯВЛЕНИЕ И ПРЕДОТВРАЩЕНИЕ НАРУШЕНИЙ ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ПЕРСОНАЛЬНЫХ ДАННЫХ.

2.1. Меры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации

К мерам, направленным на выявление и предотвращение нарушений законодательства Российской Федерации в сфере обработки персональных данных относятся:

- назначение ответственного за организацию обработки персональных данных;
- применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии с частями 1 и 2 статьи 19 Федерального закона № 152-ФЗ;
- осуществление внутреннего контроля соответствия обработки персональных данных Федеральному закону № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами, требованиями к обеспечению безопасности персональных данных, политике и локальным актам Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области в отношении обработки персональных данных;
- оценка вреда, который может быть причинен субъектам персональным данных в случае нарушения законодательства Российской Федерации и настоящего Положения;
- ознакомление работников, непосредственно осуществляющих обработку персональных данных с положениями законодательства Российской Федерации о персональных данных и настоящим Положением;
- запрет на обработку персональных данных лицами, не допущенными к их обработке.

Документы, определяющие политику Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области в отношении обработки персональных данных, подлежат обязательному опубликованию.

2.2. Порядок обработки персональных данных в информационных системах персональных данных с использованием средств автоматизации

Обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации осуществляется в соответствии с требованиями постановления Правительства Российской Федерации от 01.10.2012 № 1119 «Об утверждении требований к защите персональных данных при обработке в информационных системах персональных данных», нормативных и руководящих документов уполномоченных федеральных органов исполнительной власти.

При эксплуатации автоматизированных систем необходимо соблюдать требования:

- к работе допускаются только лица, назначенные Распоряжением Главы сельского поселения Красный Яр муниципального района Красноярский Самарской области;
- на ПЭВМ, на которых обрабатываются и хранятся сведения о персональных данных, должны быть установлены пароли (идентификаторы);
- на период обработки защищаемой информации в помещении должны находиться только лица, допущенные в установленном порядке к обрабатываемой информации; допуск других лиц в указанный период может осуществляться с разрешения Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области.

2.3. Порядок обработки персональных данных без использования средств автоматизации

Обработка персональных данных без использования средств автоматизации (далее - неавтоматизированная обработка) может осуществляться в виде документов на бумажных носителях.

При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

При неавтоматизированной обработке персональных данных на бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо несовместимы;

- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

- документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;

- дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

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

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, 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 сельского поселения Красный Яр муниципального района Красноярский Самарской области способов обработки персональных данных;

- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, - при необходимости получение 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;

- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо несовместимы.

Документы и внешние электронные носители информации, содержащие персональные данные, должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

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, вымарывание).

При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

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

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

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, а том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

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.

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

3. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Целями обработки персональных данных являются:

- организация деятельности Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области для обеспечения соблюдения законов и иных нормативно-правовых актов, реализации права на труд;

- осуществления, возложенных на Администрацию сельского поселения Красный Яр муниципального района Красноярский Самарской области функций, полномочий и обязанностей в связи с оказанием услуг и осуществлением государственных или муниципальных функций.

4. СРОКИ ОБРАБОТКИ И ХРАНЕНИЯ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ.

4.1. Сроки обработки и хранения обрабатываемых персональных данных

Сроки обработки и хранения персональных данных определяются:

- Распоряжением Росархива от 20.12.2019 № 236 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения»;

- сроком исковой давности;

- иными требованиями законодательства Российской Федерации и нормативно-правовыми актами Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области.

4.2. Особенности хранения персональных данных

Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого 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.

5. ПОРЯДОК УНИЧТОЖЕНИЯ ОБРАБОТАННЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Уничтожение обработанных персональных данных при достижении целей обработки или при наступлении иных законных оснований

Под уничтожением обработанных персональных данных понимаются действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Обрабатываемые персональные данные подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено действующим законодательством.

5.2. Порядок уничтожения обработанных персональных данных

Уничтожение обработанных персональных данных производится комиссией с составлением соответствующего акта.

6. ПРАВИЛА РАССМОТРЕНИЯ ЗАПРОСОВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

Правила рассмотрения запросов субъектов персональных данных оформляются отдельным документом и утверждаются Главой сельского поселения Красный Яр муниципального района Красноярский Самарской области .

7. ОТВЕТСТВЕННЫЙ ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Ответственный за организацию обработки персональных данных ответственный за организацию обработки персональных данных в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области назначается распоряжением Главы сельского поселения Красный Яр из числа сотрудников Администрации сельского поселения Красный Яр.

7.2. Инструкция ответственного за обработку персональных данных

Инструкция ответственного за обработку персональных данных утверждается распоряжением Главы сельского поселения Красный Яр. Ответственный за организацию обработки персональных под подпись знакомиться с инструкцией ответственного за организацию обработки персональных данных.

8. ПЕРЕЧЕНЬ ДОЛЖНОСТЕЙ, ОСУЩЕСТВЛЯЮЩИХ ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Перечень должностей

Перечень должностей служащие которых допускаются к обработке персональных данных и имеют доступ к персональным данным, утверждается распоряжением Главы сельского поселения Красный Яр муниципального района Красноярский Самарской области.

8.2. Обязательство о неразглашении персональных данных

Лица, допущенные к обработке персональных данных, в обязательном порядке под подпись знакомятся с настоящими Правилами и подписывают обязательство о неразглашении информации, содержащей персональные данные.

9. ПРАВИЛА РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ДАННЫМИ

Правила работы с обезличенными персональными данными утверждаются распоряжением Главы сельского поселения Красный Яр муниципального района Красноярский Самарской области.

10. ОТВЕТСТВЕННОСТЬ ЗА ПРОВЕДЕНИЕ МЕРОПРИЯТИЙ ПО ОБЕЗЛИЧИВАНИЮ ПЕРСОНАЛЬНЫХ ДАННЫХ

Перечень должностей, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных оформляется отдельным документом и утверждается распоряжением Главы сельского поселения Красный Яр муниципального района Красноярский Самарской области.

11. ПОРЯДОК ДОСТУПА В ПОМЕЩЕНИЯ, В КОТОРЫХ ВЕДЁТСЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

Порядок доступа в помещения, в которых ведётся обработка персональных данных оформляется в виде отдельного документа и утверждается распоряжением Главы сельского поселения Красный Яр муниципального района Красноярский Самарской области.

12. ПРАВИЛА ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ

Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к обеспечению безопасности персональных данных оформляются отдельным документом и утверждаются распоряжением Главы сельского поселения Красный Яр муниципального района Красноярский Самарской области.

Приложение № 2

УТВЕРЖДЕНО
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

ПОЛОЖЕНИЕ ОБ ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В АДМИНИСТРАЦИИ СЕЛЬСКОГО ПОСЕЛЕНИЯ КРАСНЫЙ ЯР МУНИЦИПАЛЬНОГО РАЙОНА КРАСНОЯРСКИЙ САМАРСКОЙ ОБЛАСТИ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем Положении использованы следующие термины и определения:

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.

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.

Вредоносное программное обеспечение: Программное обеспечение, предназначенное для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ к информации: Возможность получения информации и ее использования.

Защита информации: Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

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.

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 таковых средств.

Информационные технологии: Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способ осуществления таких процессов и методов.

Информация: Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

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.

Конфиденциальная информация: Информация, доступ к которой ограничивается в соответствии с действующим законодательством РФ, и иными регламентирующими документами.

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

Криптографическая защита: Защита информации от ее несанкционированной модификации и доступа посторонних лиц при помощи алгоритмов криптографического преобразования.

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.

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.

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.

Оператор персональных данных (оператор): Муниципальный орган, организующий и (или) осуществляющий обработку ПДн, а также определяющие цели и содержание обработки ПДн.

Персональные данные (ПДн): Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).

Предоставление информации: Действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

Разграничение доступа (правила разграничения доступа): Совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Распространение персональных данных: Действия, направленные на передачу ПДн 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.

Средство вычислительной техники: Совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Средство защиты информации: Техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Технические средства информационной системы персональных данных: Средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (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).

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 ИСПДн или в результате которых уничтожаются материальные носители персональных данных.

Целостность информации: Способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Шифрование: Процесс преобразования открытой информации с целью сохранения ее в тайне от посторонних лиц при помощи некоторого алгоритма, называемого шифром.

Электронный документ: Документ, в котором информация представлена в электронно-цифровой форме. Электронный документ может создаваться на основе документа на бумажном носителе, на основе другого электронного документа либо порождаться в процессе информационного взаимодействия.

Электронная подпись: Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ

В настоящем Положении использованы следующие сокращения, приведенные в Таблице 1:

Таблица 1. Сокращения

№ п/п	Сокращение	**Описание**
1.	ИСПДн	Информационная система персональных данных
2.	НСД	Несанкционированный доступ
3.	ПДн	Персональные данные
4.	СКЗИ	Средство криптографической защиты информации
5.	СЗПДн	Система защиты персональных данных

ОБЛАСТЬ ПРИМЕНЕНИЯ

Настоящее Положение об обеспечении безопасности персональных данных в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области (далее - Положение) предназначено для применения при организации и проведении работ по обеспечению безопасности персональных данных в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области

Требования настоящего Положения распространяются на работников Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, принимающих участие в обеспечении безопасности персональных данных.

ОБЩИЕ ПОЛОЖЕНИЯ

Настоящее Положение разработано в соответствии с распоряжением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Распоряжениеом ФСБ России 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 защищённости» и определяет содержание и

порядок осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных (ИСПДн) Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, представляющей собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку персональных данных как с использованием средств автоматизации, так и без использования таких средств.

Безопасность персональных данных при их обработке в ИСПДн достигается путем снижения вероятности осуществления НСД к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные действия.

При обработке персональных данных в ИСПДн Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области должно быть обеспечено:

- проведение мероприятий, направленных на предотвращение НСД к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов НСД к персональным данным;
- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие НСД к ним;
- непрерывный контроль и анализ уровня защищенности персональных данных.

Безопасность персональных данных при их обработке в ИСПДн обеспечивается с помощью системы защиты персональных данных (СЗПДн), включающей организационные мероприятия и средства защиты информации (в том числе криптографические средства, средства предотвращения НСД, программно-технических воздействий на технические средства обработки ПДн), а также используемые в ИСПД информационные технологии.

Обеспечение безопасности персональных данных в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области осуществляется на основе следующих принципов:

- соответствие мер и средств защиты актуальным угрозам безопасности,
- построение и модернизация СЗПДн в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области производится на основе анализа угроз безопасности персональных данных с учетом специфических особенностей ИСПДн;
- соответствие мер и средств защиты требованиям нормативных документов РФ - в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области используются меры и средства обеспечения безопасности персональных данных в строгом соответствии с действующими нормативными правовыми актами РФ в области обработки и защиты персональных данных;
- комплексность - с целью обеспечения безопасности персональных данных в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области используется совокупность организационных мер и технических средств защиты;
- патентная чистота - средства защиты информации, входящие в состав СЗПДн, отвечают требованиям по обеспечению патентной чистоты согласно действующим нормативным документам РФ. Используемое общесистемное, специальное и прикладное программное обеспечение имеет соответствующие лицензии производителей.
- удобство пользователей - при построении и модернизации СЗПДн учитываются и по возможности сводятся к минимуму возможные трудности пользователей в работе со средствами защиты и с основными процедурами обеспечения безопасности персональных данных;
- постоянное совершенствование - осуществляется регулярный внутренний контроль выполнения требований по обработке и обеспечению безопасности персональных данных, эффективности применяемых организационных мер и технических средств защиты и уровня защищенности персональных данных, а также регулярно пересматриваются состав угроз и

уровень защищенности ПДн, на основании чего принимаются меры по устранению выявленных недостатков и модернизации/совершенствованию СЗПДн.

Достаточность принятых мер по обеспечению безопасности персональных данных при их обработке в ИСПДн оценивается при проведении государственного контроля и надзора.

Мероприятия по обеспечению безопасности персональных данных при их обработке в ИСПДн Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области включают в себя:

- определение уровня защищенности обрабатываемых ПДн, в том числе отслеживание изменений состояния ИСПДн, которые могут повлиять на классификационные признаки ИСПДн (уровень защищенности ПДн);
- определение угроз безопасности персональных данных при их обработке в ИСПДн;
- разработка на основании определенных угроз и поддержание в актуальном состоянии частной модели безопасности угроз безопасности персональных данных при обработке их в ИСПДн;
- разработку на основе частной модели угроз системы защиты персональных данных (СЗПДн), обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для установленного уровня защищенности ПДн;
- установку и ввод в эксплуатацию СЗИ, входящих в состав СЗПДн, в соответствии с проектными решениями по созданию СЗПДн, эксплуатационной и технической документацией к данным СЗИ;
- обучение лиц, использующих СЗИ, входящие в состав СЗПДн, правилам работы с ними;
- учет применяемых СЗИ, входящих в состав СЗПДн, эксплуатационной и технической документации к ним;
- учет носителей персональных данных;
- учет лиц, допущенных к работе с персональными данными в ИСПДн;
- контроль соблюдения условий использования СЗИ, входящих в состав СЗПДн, предусмотренных эксплуатационной и технической документацией к ним;
- разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования СЗИ, входящих в состав СЗПДн, которые могут привести к нарушению заданных характеристик безопасности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработка и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
- описание состава и режима функционирования компонентов СЗПДн (описание СЗПДн).

Размещение компонентов ИСПДн, охрана помещений, в которых ведется работа с персональных данных, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и СЗИ, входящих в состав СЗПДн, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

Настоящее Положение должно быть доведено до всех работников Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, участвующих в обеспечении безопасности персональных данных, под подпись.

СТАДИИ СОЗДАНИЯ СЗПДН

В Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области обеспечение безопасности персональных данных осуществляется путем выполнения комплекса организационных и технических мероприятий, реализуемых в рамках следующих стадий создания и совершенствования СЗПДн:

- предпроектная стадия;
- стадия проектирования;
- стадия приемки и ввода в действие;
- модернизация СЗПДн.

СЗПДн включает организационные меры, технические средства защиты информации, а также используемые в ИСПДн информационные технологии, реализующие функции защиты информации.

Выполнение всех вышеуказанных стадий должно проходить по согласованию с должностным лицом, ответственным за организацию работ по обработке персональных данных.

Выполнение всех вышеуказанных стадий должно проходить под контролем должностного лица, ответственным за проведение работ по защите персональных данных.

5.1. Описание требований к предпроектной стадии создания СЗПДн

Целью предпроектной стадии создания СЗПДн является:

- определение категории субъектов персональных данных, чьи данные обрабатываются в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, состава и объема обрабатываемых персональных данных, а также цели и правовое основание обработки этих данных;
- определение должностных лиц, участвующих в обработке персональных данных;
- определение угроз безопасности персональных данных применительно к конкретным условиям функционирования ИСПДн;
- определение уровня защищенности ПДн.

Для достижения указанных целей проводится анализ информационных систем Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, содержащих персональные данные, и определяются все внутренние и внешние процессы обработки персональных данных, осуществляемые как с использованием средств автоматизации, так и без использования таковых.

По результатам предпроектной стадии определяется степень выполнения требований нормативно-правовых документов в области защиты персональных данных, а также разрабатывается план необходимых дальнейших организационных и технических мероприятий по реализации данных требований.

Должностное лицо, ответственное за проведение работ по защите персональных данных, определяет необходимость проведения тех или иных мероприятий, направленных на достижение перечисленных целей, и является ответственным за организацию и планирование действий, в результате которых достигаются цели предпроектной стадии.

Определение обрабатываемых персональных данных

В ходе предпроектной стадии по результатам анализа процессов обработки персональных данных в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области определяются состав, цели, правовое основание обработки персональных данных и сроки хранения обрабатываемых персональных данных.

На основании полученных данных формируется документ «Перечень персональных данных, обрабатываемых в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области ».

Определение перечня должностных лиц, допущенных к работе с персональными данными

В ходе предпроектной стадии по результатам анализа процессов обработки персональных данных в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области определяется перечень лиц, которым необходим доступ к персональных данных для выполнения трудовых обязанностей, а также перечень лиц, которые в рамках выполнения своих трудовых обязанностей имеют право доступа к ресурсам, содержащим персональные данные, без права ознакомления с персональными данными.

На основании полученных данных формируется перечень должностных лиц, допущенных в помещения и к работе со средствами вычислительной техники из состава ИСПДн Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, который утверждается соответствующим Распоряжением Главы сельского поселения Красный Яр муниципального района Красноярский Самарской области Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области.

Определение конфигурации и топологии ИСПДн

В ходе обследования информационных систем Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области определяются все базы данных (хранилища) и отчуждаемые носители информации и содержащиеся в них персональных данных. Кроме того, определяются конфигурация и топология ИСПДн в

целом и ее отдельных компонентов, а именно перечень серверного оборудования, автоматизированных рабочих мест, общесистемных и прикладных программных средств, задействованных при обработке персональных данных, перечень применяемых средств защиты информации, а также сетевая инфраструктура и перечень сетевого оборудования.

Определение угроз безопасности персональных данных

С целью определения необходимых мер и средств защиты, соответствующих актуальным угрозам безопасности персональных данных при их обработке в ИСПДн Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области , проводится анализ и оценка вероятности реализации и величины негативных последствий вследствие реализации угроз безопасности персональных данных при их обработке в ИСПДн.

В Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области составляется частная модель угроз безопасности персональных данных, которая разрабатывается на основании:

- ГОСТ Р 51275-2006 «Защита информации. Факторы, воздействующие на информацию. Общие положения»;
- Базовой модели угроз безопасности персональных данных при обработке в информационных системах персональных данных, утвержденной 15 февраля 2008 г. заместителем директора ФСТЭК России;
- Методики определения актуальных угроз безопасности персональных данных при обработке в информационных системах персональных данных, утвержденной 14 февраля 2008 г. заместителем директора ФСТЭК России;
- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 года № 149/54-144.

Определение уровня защищенности ПДн

Определение уровня защищенности ПДн осуществляется в соответствии с требованиями Постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». При определении уровня защищенности ПДн используется модель угроз безопасности ПДн, в которой проведен анализ актуальных угроз безопасности ПДн.

5.2. Стадия проектирования СЗПДн

Цели проектирования СЗПДн:

- определить требования по обеспечению безопасности персональных данных;
- определить структуру и характеристики создаваемой СЗПДн, состав технических средств защиты информации, предполагаемых к использованию в СЗПДн, требования к настройке и эксплуатации этих средств, параметры их взаимодействия, а также план мероприятий по подготовке СЗПДн к вводу в действие;
- определить требования и регламентировать деятельность работников Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области по организации легитимной обработки персональных данных и обеспечению безопасности персональных данных, обрабатываемых как с использованием средств автоматизации, так и без использования таковых.

Для достижения указанных целей в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области разрабатывается комплект организационно-распорядительных документов, определяющих требования и порядок действий при обработке и обеспечении безопасности персональных данных.

Должностное лицо, ответственное за проведение работ по защите персональных данных в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, определяет необходимость проведения мероприятий, направленных на достижение перечисленных целей, и является ответственным за организацию и планирование действий, в результате которых достигаются цели стадии проектирования СЗПДн.

Определение требований по обеспечению безопасности персональных данных

По результатам предпроектной стадии, в зависимости от определенного уровня защищенности ПДн и определенного перечня актуальных угроз безопасности персональных данных, задаются конкретные требования по обеспечению безопасности ПДн при их обработке в ИСПДн Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, выполнение которых обеспечивает минимизацию вероятности реализации предполагаемых угроз безопасности персональных данных.

Определение конфигурации СЗПДн

На основании требований, указанных выше, осуществляется проектирование СЗПДн, определяется состав и характеристики средств защиты информации, которые будут входить в состав создаваемой СЗПДн.

В Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области разрабатывается комплект организационно-распорядительной документации на СЗПДн, описывающей требования и процедуры по управлению и обеспечению безопасности персональных данных. За разработку и, при необходимости, пересмотр организационно-распорядительной документации на СЗПДн в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области отвечает должностное лицо, ответственное за проведение работ по обеспечению безопасности персональных данных.

5.3. Стадия ввода в действие СЗПДн

Цели стадии ввода в действие СЗПДн:

- внедрить технические средства защиты информации;
- проверить работоспособность средств защиты информации в составе ИСПДн;
- принять организационные меры по обеспечению безопасности персональных данных;
- ознакомить работников Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области с требованиями и обучить порядку обработки и обеспечения безопасности персональных данных.

Для достижения перечисленных целей выполняются следующие мероприятия:

- осуществляется закупка, установка и настройка средств защиты информации;
- проводятся опытная эксплуатация и приемо-сдаточные испытания средств защиты информации;
- утверждается и вводится в действие комплект организационно-распорядительных документов, определяющих требования и порядок действий при обработке и обеспечении безопасности персональных данных.
- проводится обучение работников по направлению обеспечения безопасности персональных данных.
- Должностное лицо, ответственное за проведение работ по защите персональных данных в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, определяет необходимость проведения тех или иных мероприятий, направленных на достижение перечисленных целей, и является ответственным за организацию и планирование действий, в результате которых достигаются цели стадии ввода в действие СЗПДн.

Внедрение средств защиты информации

Согласно требованиям, определенным в документации, осуществляется закупка, установка и настройка программных и технических средств защиты информации с составлением соответствующих актов установки.

Установка и ввод в эксплуатацию средств защиты информации осуществляется строго в соответствии с эксплуатационной и технической документации к ним. Перед установкой средств защиты информации проверяется их готовность к использованию, и составляются заключения о возможности их эксплуатации.

В Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области необходимо применять средства защиты информации, прошедшие в установленном порядке процедуру оценки соответствия и имеющие соответствующие сертификаты ФСТЭК и ФСБ России.

Внедрение организационных мер по обеспечению безопасности персональных данных

В Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области утверждается и вводится в действие комплект организационно-распорядительной документации на СЗПДн.

Все должностные лица, допущенные к обработке персональных данных, и лица, ответственные за обеспечение безопасности персональных данных, в обязательном порядке изучают организационно-распорядительные документы на СЗПДн в части их касающейся и руководствуются ими в своей работе.

Общий контроль над исполнением требований организационно-распорядительной документации на СЗПДн в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области возлагается на должностное лицо, ответственное за обеспечение безопасности ПДн.

Обучение работников по направлению обеспечения безопасности персональных данных

В Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области все работники, участвующие в обработке персональных данных, в обязательном порядке проходят обучение по следующим направлениям:

- общие вопросы обеспечения информационной безопасности;
- правила автоматизированной и неавтоматизированной обработки персональных данных и обеспечения безопасности персональных данных;
- правила использования прикладных систем и технических средств обработки персональных данных;
- правила использования средств защиты информации, входящих в состав СЗПДн;
- ответственность за нарушение правил обработки и обеспечения безопасности персональных данных.

Ответственным за организацию и контроль проведения обучения работников Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, участвующих в обработке и обеспечении безопасности персональных данных, является должностное лицо, ответственное за обеспечение безопасности персональных данных.

Обучение может проводиться как самим должностным лицом, ответственным за обеспечение безопасности персональных данных в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, так и с привлечением сторонних организаций.

Новые работники, принимаемые на работу, в обязательном порядке проходят первичный инструктаж. Ответственным за направление работника на первичный инструктаж является должностное лицо, ответственное за организацию работ по обработке персональных данных в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области.

Перед допуском работников Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области к работе с ПДн должностное лицо ответственное за обеспечение безопасности ПДн проводит ознакомление с нормативной документацией, утвержденной в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, в области безопасности ПДн.

5.4. Модернизация СЗПДн

В случаях изменения состава или структуры ИСПДн Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, состава угроз безопасности персональных данных или уровня защищенности ПДн, обработка которых осуществляется в ИСПДн Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области , проводится модернизация СЗПДн.

6. МЕРОПРИЯТИЯ ПО ОРГАНИЗАЦИИ И ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Под организацией обеспечения безопасности персональных данных при их обработке в ИСПДн Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области понимается формирование и реализация совокупности согласованных по целям, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности персональных данных.

Организационные мероприятия по обеспечению безопасности персональных данных в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области включает в себя:

- мероприятия по обеспечению охраны и физической защиты помещений, в которых расположены технические средства ИСПДн, исключающие несанкционированный доступ к техническим средствам ИСПДн, их хищение и нарушение работоспособности;
- обучение работников правилам обработки и защиты персональных данных.

В целях осуществления технического обеспечения безопасности персональных данных при их обработке в ИСПДн Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области реализовываются мероприятия по защите от НСД к ПДн.

Планирование мероприятий по обеспечению безопасности персональных данных осуществляется в соответствии с Разделом 8 настоящего Положения.

6.1. Мероприятия по обеспечению управления доступом

Общие требования

Для организации системы допуска и учета должностных лиц, допущенных к работе с персональными данными в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, должен быть определен перечень должностных лиц и утверждён соответствующим Распоряжением Главы сельского поселения Красный Яр муниципального района Красноярский Самарской области.

В Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области должна быть реализована разрешительная система допуска пользователей и разграничение прав доступа пользователей к информационным ресурсам, программным средствам обработки (передачи) и защиты информации с помощью функциональных возможностей операционной системы, прикладных систем обработки персональных данных либо специализированных средств защиты информации.

Работникам Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области предоставляется доступ к ПДн и средствам их обработки в объеме, минимально необходимом для выполнения их трудовых обязанностей.

Для идентификации и аутентификации пользователей ИСПДн Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области должны применяться пароли условно-постоянного действия. Требования к формированию пароли и периодичности их смены определены в эксплуатационной документации на СЗПДн (Руководство администратора информационной безопасности, и Инструкция работника по правилам обработки ПДн).

Порядок проведения мероприятий

Своевременное предоставление работникам Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области прав доступа к персональным данным и средствам их обработки, а также изменение их полномочий обеспечивает должностное лицо, ответственное за обеспечение безопасности ПДн в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области.

Порядок генерации, смены и прекращения действия паролей в ИСПДн Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области определен в эксплуатационной документации на СЗПДн).

6.2. Мероприятия по обеспечению регистрации и учета

Учет и хранение носителей ПДн

Требования

В Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области должен вестись учет как машинных, так и бумажных носителей ПДн. Также должно быть организовано хранение и использование этих носителей, исключающее их хищение, подмену и уничтожение.

В Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области учету подлежат следующие типы машинных носителей ПДн:

- отчуждаемые носители информации (внешние жесткие магнитные диски, гибкие магнитные диски, магнитные ленты, USB флеш-накопители, карты флеш-памяти, оптические носители (CD, DVD, BD и прочее);

- неотчуждаемые носители информации (жесткие магнитные диски).

Порядок проведения мероприятий

Порядок учета, хранения, использования носителей персональных данных (машинных и бумажных), а также порядок их уничтожения определены в документе «Порядок учета, хранения и уничтожения носителей персональных данных в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области ».

Ответственность за ведение учета машинных носителей персональных данных, организацию надлежащего хранения, а также уничтожение носителей персональных данных возлагается на должностное лицо, ответственное за защиту ПДн.

Контроль и ответственность за ведение учета бумажных носителей персональных данных, организацию надлежащего хранения, а также уничтожение носителей персональных данных возлагается на должностное лицо ответственное за организацию работ по обработке ПДн.

6.3. Мероприятия по обеспечению целостности

Требования

Сохранность и целостность программных средств ИСПДн и персональных данных являются обязательными и обеспечиваются в том числе за счет создания резервных копий. Резервному копированию подлежат все программные средства, архивы, журналы, информационные ресурсы (данные), используемые и создаваемые в процессе эксплуатации ИСПДн.

В Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области должен быть определен и документально зафиксирован состав и назначение ПО, используемого в ИСПДн. Порядок внесения изменений в установленное ПО ИСПДн, включая контроль действий программистов в процессе модификации ПО, должен быть регламентирован.

Эталонные копии ПО должны быть учтены, доступ к ним должен быть регламентирован.

С целью недопущения изменения состава ПО ИСПДн, из него должны быть исключены программные средства, предназначенные для разработки и отладки ПО (либо содержащие средства разработки, отладки и тестирования программно-аппаратного обеспечения).

Средства восстановления функций обеспечения безопасности персональных данных в ИСПДн должны предусматривать ведение не менее двух независимых копий программных средств.

В Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области должны быть реализованы механизмы восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним и/или возникновения форс-мажорных ситуаций или воздействия опасных факторов окружающей среды.

Требования к периодичности осуществления резервного копирования и требования к носителям, предназначенным для записи на них резервных копий, определены в документе «Порядок проведения резервного копирования персональных данных в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области».

Порядок проведения мероприятий

Порядок организации резервного копирования и восстановления массивов информации в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области определен в документе «Порядок проведения резервного копирования ПДн в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области ».

Ответственность за организацию своевременного резервного копирования и восстановления информации, а также за надлежащее хранение резервных носителей, содержащих резервные копии данных, возлагается на должностное лицо ответственное за защиту ПДн.

6.4. Мероприятия по обеспечению антивирусной защиты

Требования

Для предотвращения возможности внедрения в ИСПДн вредоносного программного обеспечения Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области должны применяться антивирусные средства:

Требования к настройке антивирусных средств защиты определены в проектной документации на СЗПДн, процедуры по управлению антивирусными средствами определены в эксплуатационной документации на СЗПДн (Руководство администратора информационной безопасности).

Порядок проведения мероприятий

Порядок использования антивирусных средств защиты определен в эксплуатационной документации на СЗПДн (Руководство администратора информационной безопасности).

Системный администратор Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области осуществляет:

- установку антивирусных средств защиты в соответствии с эксплуатационной и технической документацией к ним;
- настройку параметров антивирусных средств защиты согласно требованиям по обеспечению безопасности, определенным в проектной документации на СЗПДн;
- контроль эффективности работы антивирусных средств защиты;

Контроль соблюдения условий использования антивирусных средств защиты, предусмотренных эксплуатационной и технической документацией возлагается на должностное лицо ответственное за защиту ПДн.

6.5. Мероприятия по обеспечению криптографической защиты

Требования

В Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области должны применяться следующие типы средств криптографической защиты информации, сертифицированные ФСБ России:

- СКЗИ для обеспечения безопасности ПДн, передаваемых по каналам связи между Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области и ИС сторонних организаций;
- средства электронной подписи, т.е. шифровальные (криптографические) средства, используемые для подписания передаваемых документов и проверки электронной подписи получаемых документов.

СКЗИ, применяемые в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области для защиты ПДн, должны иметь класс, определенный в Частной модели угроз безопасности ПДн при их обработке в ИСПДн Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области.

Правила использования СКЗИ при обмене информацией со сторонними организациями СКЗИ должны быть определены условиями заключаемых договоров между Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области и данными организациями.

В Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области ведется учет всех применяемых СКЗИ, эксплуатационной и технической документации к ним, а также учет лиц, допущенных к работе с СКЗИ, предназначенными для обеспечения безопасности ПДн.

Требования к эксплуатации и учету применяемых в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области СКЗИ определены в документе «Порядок эксплуатации СКЗИ в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области».

Порядок проведения мероприятий

Порядок организации криптографической защиты в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, определен в документе «Порядок эксплуатации СКЗИ в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области ».

На должностное лицо, ответственное за выполнение работ по защите ПДн в Администрации сельского поселения Красный Яр муниципального района Красноярский

Самарской области, возлагается ответственность за обеспечение функционирования и безопасности СКЗИ согласно требованиям руководящих документов ФСБ России.

6.6. Мероприятия по обеспечению физической защиты

Основные требования по обеспечению физической защиты:

В целях предотвращения несанкционированного входа (вскрытия) в помещения, а также исключения возможности неконтролируемого проникновения в эти помещения посторонних лиц, в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области организуется и обеспечивается физическая охрана и техническая защита помещений Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, обеспечивающие сохранность технических средств обработки персональных данных, носителей персональных данных и средств защиты информации.

Защите подлежат следующие типы помещений:

- помещения, в которых осуществляется непосредственно обработка ПДн пользователями ИСПДн Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области;
- серверные помещения, в которых установлено серверное, сетевое оборудование и технические средства защиты информации;
- архивные помещения, в которых организовано хранение бумажных документов, содержащих ПДн.

Перечень лиц, которые допускаются в указанные помещения, определяется Распоряжением Главы сельского поселения Красный Яр муниципального района Красноярский Самарской области.

В целях обеспечения физической защиты помещений применяться следующие средства защиты и контроля за несанкционированным вскрытием:

- система охранной сигнализации;
- двери помещений оборудуются замками для защиты от несанкционированного проникновения и местами для их опечатывания и сдачи под охрану.
- устанавливаются металлические двери для защиты от несанкционированного проникновения в серверные и архивные помещения.

В целях организации противопожарной безопасности в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области устанавливается система пожарной сигнализации

Порядок проведения мероприятий по обеспечению физической защиты:

Контроль обеспечения безопасности помещений, в которых расположены компоненты ИСПДн, возлагается на должностное лицо ответственное за защиту ПДн.

Доступ в защищаемые помещения осуществляется согласно перечню утвержденного Распоряжением Главы сельского поселения Красный Яр муниципального района Красноярский Самарской области Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области.

Лица, не указанные в Перечне допущенных в защищаемые помещения, при наличии необходимости могут посещать помещения Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области только в сопровождении допущенных лиц.

Одиночное, бесконтрольное пребывание лиц, не допущенных к работе по обработке ПДн, в производственных помещениях - **СТРОГО ЗАПРЕЩЕНО.**

Пребывание посторонних лиц в серверных помещениях допускается в целях производственной необходимости, только в присутствии должностного лица, ответственного за защиту ПДн.

В случае утраты ключей (либо подозрении на утрату) к замкам в защищаемые помещения предпринимаются следующие меры:

- оповещаются должностные лица, ответственные за организацию работ по обработке ПДн за защиту ПДн служебной запиской;
- производится немедленная замена запираемых замков.
- назначается административная проверка всех режимных помещений с составлением акта и принятым мерам, виновные лица привлекаются к административной ответственности.

При возникновении форс-мажорных обстоятельств в защищаемых помещениях (возникновение пожара, затопление помещения, возгорание электропроводки и прочее) в отсутствии лиц, имеющих доступ в эти помещения, осуществляется вскрытие помещений с соблюдением следующих условий:

- оповещаются должностные лица ответственные за организацию работ по обработке и защите ПДн;
- помещения вскрываются группой в составе не менее двух человек;
- при вскрытии помещения составляется акт о вскрытии, в котором указываются должности и фамилии лиц, вскрывших помещение, дата, времяи причины вскрытия.

7. ОБЯЗАННОСТИ, ПРАВА И ОТВЕТСТВЕННОСТЬ ДОЛЖНОСТНЫХ ЛИЦ ПРИ ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ПДН

Обязанности, права и ответственность должностных лиц, участвующих в обеспечении безопасности ПДн в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области определены в соответствующих инструкциях.

8. ПЛАНИРОВАНИЕ РАБОТ ПО ЗАЩИТЕ ПДН

Планирование работ по защите информации, требования к содержанию плана, порядок разработки, согласования, утверждения и оформления плана, порядок отчетности и контроля над его выполнением определяются действующими нормативными документами РФ.

План определяет перечень основных проводимых организационно-технических мероприятий по защите информации (в том числе ПДн) в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области с указанием:

- сроков выполнения мероприятий;
- ответственных за выполнение соответствующих пунктов Плана работников.

В План включаются:

- мероприятия по контролю состояния защищенности ПДн;

План на очередной календарный год разрабатывается должностным лицом, ответственным за защиту информации в ИС ПДн, который осуществляет общий контроль над выполнением работ по защите информации.

Утвержденный план хранится у должностного лица ответственного за организацию работ по обработке ПДн.

Отчет о результатах выполнения запланированных мероприятий по обеспечению безопасности ПДнза текущий год формируется должностным лицом, ответственным за защиту ПДн, в рамках общего отчета работы за текущей год.

9. КОНТРОЛЬ СОСТОЯНИЯ ЗАЩИЩЕННОСТИ ПДН

Контроль состояния защищенности ПДн в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области осуществляется с целью своевременного выявления и предотвращения утечки конфиденциальной информации, отнесенной к категории ПДн, вследствие НСД к ней, преднамеренных программно-технических воздействий на персональные данные и оценки защищенности ПДн (далее по тексту - Контроль).

Контроль заключается в проверке выполнения требований действующих нормативных документов в области обработки и обеспечения безопасности ПДн, в оценке обоснованности и эффективности принятых мер по защите ПДн.

Контроль эффективности внедренных мер и СЗИ, входящих в состав СЗПДн, должен проводиться в соответствии с требованиями эксплуатационной документации на СЗПДн в целом на конкретные СЗИ, а также требованиями других нормативных документов не реже одного раза в год.

Обязательным является контроль СЗИ, входящих в состав СЗПДн, при вводе их в эксплуатацию после проведения ремонта таких средств, а также при изменении условий и расположения их эксплуатации.

Контроль обеспечения безопасности ПДн в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области организовывается должностным лицом, ответственным за проведение работ по защите ПДн в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области.

Контроль состояния и эффективности СЗПДн может осуществляться в соответствии с планом основных мероприятий по защите информации на текущий год или носить внеплановый характер.

Результаты периодического контроля оформляются отдельными протоколами или актами.

По всем выявленным нарушениям требований по защите ПДн должностное лицо, ответственное за обеспечение безопасности ПДн в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, в пределах предоставленных ему прав и своих функциональных обязанностей обязано добиваться их немедленного устранения.

Должностное лицо, ответственное за организацию работ по обработке ПДн в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, обязано принять все необходимые меры по немедленному устранению выявленных нарушений. При невозможности их немедленного устранения должна быть прекращена обработка ПДн и организованы работы по устранению выявленных нарушений.

Работники Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, осуществляющие обработку ПДн в ИСПДн, обязаны выполнять требования должностного лица ответственного за обеспечение безопасности ПДн, по устранению допущенных ими нарушений норм и требований по обработке и/или обеспечении безопасности ПДн. Также работники несут персональную ответственность за соблюдение требований по обеспечению безопасности ПДн в ходе проведения работ.

Учет, хранение и выдача работникам паролей и ключей для системы защиты ПДн от НСД, оперативный контроль действий работников, осуществляющих обработку ПДн, осуществляет должностное лицо ответственное за обеспечение безопасности ПДн.

10. УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области в целях своевременного устранения выявленных нарушений безопасности определен и задокументирован порядок действий при возникновении инцидентов информационной безопасности, связанных с нарушением требований по обработке и обеспечению безопасности ПДн.

10.1. Требования к мероприятиям

К инцидентам информационной безопасности, связанным с нарушением требований по обработке и обеспечению безопасности ПДн, относятся любые нарушения, приводящие к снижению уровня защищенности ИСПДн, в том числе несоблюдение условий хранения носителей ПДн и использования средств защиты информации, которые могут привести к нарушению конфиденциальности, целостности или доступности ПДн.

В Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области в случаях возникновения подобных инцидентов информационной безопасности проводятся разбирательства, составляются заключения по фактам возникновения инцидентов, разрабатываются и принимаются меры по предотвращению возможных последствий инцидентов.

10.2. Порядок проведения мероприятий

Организация и контроль процесса реагирования на инциденты информационной безопасности, связанные с обработкой и обеспечением безопасности ПДн, в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области возлагается на должностное лицо ответственное за обеспечение безопасности ПДн.

Процедура управления инцидентами информационной безопасности, связанными с нарушением требований по обработке и обеспечению безопасности ПДн, регламентирована в документе «Порядок реагирования на инциденты информационной безопасности в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области». Данный документ определяет порядок проведения следующих мероприятий:

- определение инцидента информационной безопасности;
- оповещение ответственного лица о возникновении инцидента;
- устранение последствий и причин инцидента;
- расследование инцидента;
- реализация необходимых корректирующих и превентивных мер.

Дополнительно порядок действий работников Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области в случаях возникновения инцидентов информационной безопасности определен в документе «Инструкция пользователю информационной системы ПДн в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области ».

11. МОДЕРНИЗАЦИЯ СИСТЕМЫ ЗАЩИТЫ ПДН

Для определения необходимости модернизации СЗПДн не реже одного раза в год должностным лицом ответственным за обеспечение безопасности ПДн проводится проверка состава и структуры СЗПДн, состава угроз и уровня защищенности ПДн, обработка которых осуществляется в ИСПДн Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области.

Модернизация СЗПДн в обязательном порядке проводится в случаях, если:

- изменился состав или структура самой ИСПДн или технические особенности ее построения (изменился состав обрабатываемых ПДн, состав или структура программного обеспечения, технических средств обработки ПДн, топологии ИСПДн и пр.);
- изменился состав угроз безопасности ПДн в ИСПДн;
- изменился уровень защищенности ПДн.

Выбор мер и СЗИ, входящих в состав СЗПДн, проводится на основании проведенного анализа угроз и проведенной классификации ИСПДн (определения уровня защищенности ПДн). Порядок проведения данных мероприятий определен в Разделах 5.1.4 «Определение угроз безопасности данных» и 5.1.5 «Определение уровня защищенности ПДн» настоящего Положения.

Должностное лицо ответственное за обеспечение безопасности ПДн ежегодно разрабатывает план работ по обеспечению безопасности ПДн в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, в котором определяется перечень необходимых мероприятий по обеспечению безопасности ПДн с учетом уже выполненных мероприятий.

В план работ по обеспечению безопасности ПДн включаются организационные и технические мероприятия, направленные на выполнение требований нормативно-правовых документов в области безопасности ПДн и на совершенствование СЗПДн, а также контрольные мероприятия и мероприятия по проведению обучения работников Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области. В плане указываются дата, сроки проведения мероприятий, их периодичность (разовые или регулярные) и назначаются ответственные за их организацию и выполнение лица.

Работники, участвующие в обеспечении безопасности ПДн в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области вправе формировать предложения по совершенствованию СЗПДн и направлять их на рассмотрение должностному лицу ответственному за защиту ПДн, которое в свою очередь формирует сводный перечень предложений по совершенствованию СЗПДн.

Ежегодно должностное лицо ответственное за защиту ПДн формирует отчет о проделанных мероприятиях по выполнению плана работ по обеспечению безопасности ПДн, обрабатываемых в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, и предоставляет его Главе Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области совместно со сводным перечнем предложений по совершенствованию СЗПДн.

Ежегодный отчет по выполнению плана работ включает в себя:

- результаты проведенной проверки состава и структуры, состава угроз и уровня защищенности ПДн;
- результаты проведенных контрольных мероприятий по защите ПДн;
- результаты проверок регулирующими органами;
- результаты анализа инцидентов информационной безопасности;
- результаты плановых мероприятий по обеспечению безопасности ПДн;
- предложения по совершенствованию СЗПДн на основе полученных результатов.

На основании решения, принятого Главой сельского поселения Красный Яр муниципального района Красноярский Самарской области, по результатам рассмотрения

ежегодного отчета и предложений по совершенствованию СЗПДн должностное лицо ответственное за защиту ПДн составляет план работ по обеспечению безопасности ПДн, обрабатываемых в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, на следующий год.

12. ПРИВЛЕЧЕНИЕ СТОРОННИХ ОРГАНИЗАЦИЙ ДЛЯ ПРОВЕДЕНИЯ МЕРОПРИЯТИЙ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПДН

В Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области могут привлекаться сторонние организации для проведения следующих мероприятий по обеспечению безопасности ПДн:

- разработка нормативно-методических материалов по вопросам обеспечения безопасности ПДн;
- поставка СЗИ и СКЗИ;
- выполнение организационных и технических мероприятий в области защиты ПДн, на проведение которых у Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области отсутствует соответствующее разрешение либо отсутствуют технические средства и подготовленные работники (специалисты);
- выполнение организационных и технических мероприятий в области защиты ПДн, выполнение которых силами Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области экономически нецелесообразно;
- подтверждение соответствия мер по защите ИСПДн требованиям нормативно-правовой базы РФ в области безопасности ПДн, путем проведения аттестационных испытаний ИСПДн Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области по требованиям безопасности информации;
- контроль и аудит эффективности проводимых мероприятий по защите ПДн.

Привлекаемые для оказания услуг в области защиты ПДн сторонние организации должны иметь лицензии на соответствующие виды деятельности.

Перечень совместно выполняемых организационных и технических мероприятий в области защиты ПДн определяется с учетом планируемых работ по созданию (реконструкции) ИСПДн и включается в План основных мероприятий по защите ПДн.

В данном разделе определен порядок взаимодействия с вышеперечисленными сторонними организациями.

12.1. Привлечение сторонних организаций для проведения мероприятий по созданию и модернизации СЗПДн и/или проведению контрольных мероприятий

Привлекаемая сторонняя организация должна обладать соответствующими, проводимым работам, лицензиями и сертификатами.

Должностное лицо, ответственное за обеспечение безопасности ПДн, является ответственным за выбор организации, привлекаемой для проведения мероприятий по созданию или модернизации СЗПДн и проведению контрольных мероприятий. Должностное лицо, ответственное за защиту ПДн, осуществляет подбор подходящих организаций и формирует предложения для согласования с Главой сельского поселения Красный Яр муниципального района Красноярский Самарской области.

Существенным условием договора является обязательство привлекаемой организации обеспечить конфиденциальность получаемой информации, ставшей известной в ходе выполнения работ по обеспечению безопасности ПДн в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области.

В случае привлечения сторонней организации для проведения мероприятий по созданию или модернизации СЗПДн в договоре прописываются обязательства привлекаемой организации по проведению необходимых организационно-технических мероприятий, включающих в себя:

- организацию и проведение работ по созданию СЗПДн;
- реализацию требований нормативно-правовых документов РФ в области обработки и защиты ПДн;
- своевременное совершенствование СЗПДн;
- поддержание работоспособности и сопровождение СЗПДн.

В случае привлечения сторонней организации для проведения контрольных мероприятий (аудит обеспечения безопасности ПДн) в договоре прописываются обязанности привлекаемой организации по выполнению необходимых работ, включающих в себя:

- проверку выполнения требований нормативно-правовых документов РФ в области обработки и защиты ПДн;
- оценку обоснованности и эффективности принятых в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области мер по обеспечению безопасности ПДн.

Должностное лицо, ответственное за обеспечение безопасности ПДн, осуществляет контроль над выполнением привлекаемой организацией взятых на себя обязательств.

12.2. Привлечение сторонних организаций для проведения обучения работников.

К организациям, привлекаемым для проведения обучения работников Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области по направлению обеспечения безопасности ПДн, предъявляются следующие требования:

- организация должна иметь лицензию на осуществление образовательной деятельности, выданную Министерством образования РФ, государственными органами управления образованием субъектов РФ или органами местного самоуправления, наделенными соответствующими полномочиями;
- предлагаемые организацией программы и курсы обучения должны быть согласованы с регулирующими и надзорными органами;
- по результатам проведенного обучения организация должна проводить итоговую аттестацию работников.

12.3. Привлечение сторонних организаций (подрядчиков) для ремонтно-восстановительных работ

Организацией обслуживания, настройки и ремонта средств обработки и СЗИ, входящих в состав СЗПДн, в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области занимается системный администратор Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области. В случае необходимости, ремонт технических средств может быть произведен с привлечением специалистов сторонних организаций на договорной основе с составлением актов выполненных работ.

Должностным лицом, ответственным за обеспечение безопасности ПДн, определяется порядок привлечения сторонних организаций (подрядчиков) для обслуживания, настройки и ремонта средств обработки и СЗИ, входящих в состав СЗПДн.

Сопровождение и контроль сторонних организаций (подрядчиков) обеспечивается должностным лицом, ответственным за обеспечение безопасности ПДн.

Обязательным условием при передаче технических средств обработки ПДн и машинных носителей ПДн для осуществления ремонтных работ сторонней организацией является удаление ПДн с носителей, установленных на передаваемых устройствах, либо извлечение носителей ПДн. Контроль исполнения данного требования возлагается на должностное лицо ответственное за защиту ПДн. В случае, когда выполнить данное требование не представляется возможным, должностным лицом, ответственным за защиту ПДн, составляется двусторонний протокол, в котором указано, что сторонняя организация осведомлена о том, какие именно персональные данные содержатся на носителе и обязана принять все необходимые меры по обеспечению их безопасности.

После проведения ремонта средств защиты или средств обработки ПДн, при изменении условий их расположения или эксплуатации обязательно осуществляется проверка готовности этих средств к использованию с составлением заключений о возможности их эксплуатации.

13. ПЕРЕСМОТР И ВНЕСЕНИЕ ИЗМЕНЕНИЙ

Настоящее Положение должно пересматриваться в случаях:

- изменения требований законодательства РФ, в области обработки и обеспечения информационной безопасности ПДн;
- изменением организационной и технологической инфраструктуры, в рамках которой обрабатываются ПДн;

- выявления снижения общего уровня информационной безопасности (по результатам регулярного мониторинга или аудита);

Ответственным за пересмотр настоящего Положения и составление рекомендаций по изменению является должностное лицо ответственное за обеспечение безопасности ПДн в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области.

Внесение изменений производится на основании соответствующего распоряжения Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области.

Приложение № 3

УТВЕРЖДЕНЫ
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

ПРАВИЛА РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ПЕРСОНАЛЬНЫМИ ДАННЫМИ В АДМИНИСТРАЦИИ СЕЛЬСКОГО ПОСЕЛЕНИЯ КРАСНЫЙ ЯР МУНИЦИПАЛЬНОГО РАЙОНА КРАСНОЯРСКИЙ САМАРСКОЙ ОБЛАСТИ

Статья 1. Условия обезличивания

Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса используемых информационных систем персональных данных и по достижению сроков обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законодательством Российской Федерации.

Статья 2. Способы обезличивания

К способам обезличивания персональных данных при условии дальнейшей обработки персональных данных относятся:

1) замена части сведений идентификаторами;

2) обобщение (понижение) точности некоторых сведений;

3) деление сведений на части и обработка их в разных информационных системах;

4) другие способы.

К способам обезличивания персональных данных в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

Статья 3. Правила работы с обезличенными данными

Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

При обработке обезличенных персональных данных с использованием средств автоматизации необходимо:

1) использование средств защиты информации;

2) использование антивирусных программ;

3) соблюдение правил доступа в помещение, в котором ведётся обработка персональных данных;

При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

1) хранения бумажных носителей в условиях, исключающих доступ к ним посторонних лиц;

2) соблюдение правил доступа в помещение, в котором ведётся обработка персональных данных.

Приложение № 4

УТВЕРЖДЕН
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

ПЕРЕЧЕНЬ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В АДМИНИСТРАЦИИ СЕЛЬСКОГО ПОСЕЛЕНИЯ КРАСНЫЙ ЯР МУНИЦИПАЛЬНОГО РАЙОНА КРАСНОЯРСКИЙ САМАРСКОЙ ОБЛАСТИ

Таблица 1. Перечень обрабатываемых персональных данных

Группа персональных данных	Состав персональных данных	Цели обработки персональных данных
1. Обработка персональных данных обращений граждан		
Общие сведения о гражданах	Фамилия, имя, отчество, дата и место рождения, адрес регистрации, адрес фактического проживания, семейное положение, социальное положение, сведения об образовании, имущественное положение, доходы, паспортные данные, данные ИНН, данные Пенсионного страхового свидетельства, сведения о рождении детей, о заключении/расторжении брака, место работы, должность, состав семьи, телефоны домашний и сотовый, сведения о трудовой деятельности, сведения о ближайших родственниках (фамилия, имя, отчество, дата рождения, степень родства), фотография	Прием и регистрация обращений (или запросов) граждан, организаций и общественных объединений, поступивших в администрацию сельского поселения Красный Яр муниципального района Красноярский Самарской области
2. Обработка персональных данных в ИС «Парус», 1С, «Контур», ГИС ГМП		
Общие сведения о работниках	Фамилия, имя, отчество, дата рождения, место рождения, гражданство, фотография, адрес регистрации, адрес фактического проживания, номер телефона (либо иной вид связи); данные паспорта или документа, его заменяющего (серия, номер, кем и когда выдан);сведения об образовании (наименование учебного заведения, дата окончания учебного заведения, номер диплома, направление подготовки или специальность по диплому, квалификация по диплому);послевузовское профессиональное образование: аспирантура, адъюнктура, докторантура (наименование образовательного или научного учреждения, год окончания, ученая степень, ученое звание (дата присвоения, номера дипломов, аттестатов);сведения о наличии (отсутствии) классного чина федеральной гражданской службы, дипломатического ранга, воинского или специального звания, классного чина правоохранительной службы, классного чина гражданской службы субъекта Российской Федерации, квалификационного разряда государственной службы, квалификационного разряда или классного чина муниципальной службы (кем и когда присвоены);сведения о владении	Реализация кадровой и бухгалтерской политики

Группа персональных данных	Состав персональных данных	Цели обработки персональных данных
	иностранными языками; сведения о судимости, когда и за что; сведения о допуске к государственной тайне, оформленном за период работы, службы, учебы, его форма, номер и дата; сведения о выполняемой работе с начала трудовой деятельности (наименование организации, ее адреса, месяца и года поступления и ухода, должности, включая учебу в высших и средних специальных учебных заведениях, военную службу, работу по совместительству, предпринимательскую деятельность и т.п.);сведения о наличии государственных наград, иных наград и знаков отличия, почетных званиях и поощрениях; сведения о близких родственниках (отец, мать, братья, сестры и дети, а также муж (жена), в том числе бывшие) с указанием степени родства, фамилии, имени, отчества (в том числе предыдущие в случае их изменения), даты и места рождения, места работы (наименование и адрес организации), должности, домашнего адреса (адрес регистрации, фактического проживания);сведения о близких родственниках (отец, мать, братья, сестры и дети, а также муж (жена), в том числе бывшие), постоянно проживающих за границей и (или) оформляющих документы для выезда на постоянное место жительства в другое государство; сведения о пребывании за границей (когда, где, с какой целью);данные о наличии заграничного паспорта (серия, номер, кем и когда выдан);номер страхового свидетельства обязательного пенсионного страхования (далее - СНИЛС); реквизиты страхового медицинского полиса обязательного медицинского страхования; реквизиты свидетельства государственной регистрации актов гражданского состояния; сведения из реестра дисквалифицированных лиц; идентификационный номер налогоплательщика (далее - ИНН);сведения о реквизитах и (или) копии иных документов, выданных на имя муниципального служащего; материалы и результаты аттестации муниципального служащего; сведения о повышении квалификации, профессиональной переподготовке; сведения об отпусках; сведения о реквизитах банковских счетов для выплаты денежного содержания и о размере денежного содержания муниципального служащего; сведения о занимаемой должности; отношение к воинской обязанности; сведения о воинском учете: воинское звание, категория запаса, военно-учетная специальность, категория годности к воинской службе, наименование военного комиссариата по месту жительства, состояние на воинском учете; сведения о социальном положении (в том числе о социальных льготах);сведения о семейном положении; сведения о составе семьи; содержащиеся в выписке из домовой книги, копиях финансового лицевого счета, свидетельства о браке, свидетельства о рождении ребенка (детей), трудовой книжки; сведения из заключения медицинского учреждения о наличии (отсутствии) заболевания, препятствующего	

Группа персональных данных	Состав персональных данных	Цели обработки персональных данных
	прохождению муниципальной службы; сведения о доходах, об имуществе, о денежных средствах, находящихся на счетах в банках и иных кредитных организациях, о ценных бумагах, об обязательствах имущественного характера, прочих обязательствах муниципального служащего, его супруги (супруга), несовершеннолетних детей; сведения о расходах муниципального служащего, его супруги (супруга), несовершеннолетних детей по каждой сделке по приобретению земельного участка, другого объекта недвижимости, транспортного средства, ценных бумаг, акций (долей участия, паев в уставных (складочных) капиталах организаций) и об источниках получения средств, за счет которых совершена указанная сделка, если сумма сделки превышает общий доход данного лица и его супруги (супруга) за три последних года, предшествующих совершению сделки; содержащиеся в документах о наличии в собственности муниципального служащего и (или) членов его семьи жилых помещений; сведения о размерах начисленных, удержанных и оплаченных налогов, в т.ч. налога на доходы физических лиц; сведения о взносах во внебюджетные фонды Российской Федерации, в т.ч. в Пенсионный фонд Российской Федерации, Фонд обязательного медицинского страхования Российской Федерации, Фонд социального страхования Российской Федерации; сведения, указанные в оригиналах и копиях распоряжение по личному составу и материалах к ним; материалы по служебным проверкам в отношении муниципального служащего; сведения о временной нетрудоспособности муниципального служащего; табельный номер муниципального служащего (работника).	
3. Обработка персональных данных при ведении похозяйственных книг		
Общие сведения о собственных и зарегистрированных (проживающих) лицах	Фамилия, имя, отчество члена хозяйства, пол, дата рождения адрес проживания Члены хозяйства, совместно проживающие с главой хозяйства и (или) совместно осуществляющие с ним ведение хозяйства, место работы, должность, состав семьи, телефоны домашний и сотовый,	В соответствии с Федеральным законом от 07 июля 2003 года № 112-ФЗ «О личном подсобном хозяйстве», распоряжением Минсельхоза России от 11 октября 2010 года № 345 «Об утверждении формы и порядка ведения похозяйственных книг органами местного самоуправления поселений и органами местного самоуправления городских округов».
4. Обработка персональных данных при оказании муниципальных услуг и муниципальном контроле		
Общие сведения	Фамилия, имя, отчество, адрес проживания, телефоны домашний и сотовый, паспортные данные заменяющего (серия, номер, кем и когда выдан),	

Таблица 2. Правовое основание обработки персональных данных и сроки их хранения

Группа персональных данных	Основание для обработки персональных данных
1. Обработка персональных данных обращений граждан 2.	
Сведения о гражданах	Федеральный закон от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»
3. Обработка персональных данных в ИС «Парус», 1С, «Контур», ГИС ГМП, УРМ	
Сведения о работнике	Статьи 85-90 Трудового кодекса Российской Федерации, Налоговый кодекс Российской Федерации.
Сведения о родственниках работника	
4. Обработка персональных данных при ведении похозяйственных книг БАРС ЭПК Электронная похозяйственная книга	
Сведения о гражданах	Федеральным законом от 07 июля 2003 года № 112-ФЗ «О личном подсобном хозяйстве», распоряжением Минсельхоза России от 11 октября 2010 года № 345 «Об утверждении формы и порядка ведения похозяйственных книг органами местного самоуправления поселений и органами местного самоуправления городских округов».

Приложение № 5

УТВЕРЖДЕН
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

ПЕРЕЧЕНЬ ДОЛЖНОСТЕЙ В АДМИНИСТРАЦИИ СЕЛЬСКОГО ПОСЕЛЕНИЯ КРАСНЫЙ ЯР МУНИЦИПАЛЬНОГО РАЙОНА КРАСНОЯРСКИЙ САМАРСКОЙ ОБЛАСТИ, ОТВЕТСТВЕННЫХ ЗА ПРОВЕДЕНИЕ МЕРОПРИЯТИЙ ПО ОБЕЗЛИЧИВАНИЮ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ, В СЛУЧАЕ ОБЕЗЛИЧИВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

- Глава поселения;
- Заместитель Главы;
- Ведущий специалист;
- Специалист (контрактный управляющий);
- Главный бухгалтер;
- Заместитель Главного бухгалтера;
- Специалист;
- Специалист-техник;
- Инструктор по физической культуре;
- Инструктор по работе с несовершеннолетними;
- Заведующий хозяйством.

Приложение № 6

УТВЕРЖДЕН
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

ПЕРЕЧЕНЬ ДОЛЖНОСТЕЙ В АДМИНИСТРАЦИИ СЕЛЬСКОГО ПОСЕЛЕНИЯ КРАСНЫЙ ЯР МУНИЦИПАЛЬНОГО РАЙОНА КРАСНОЯРСКИЙ САМАРСКОЙ ОБЛАСТИ , ЗАМЕЩЕНИЕ КОТОРЫХ ПРЕДУСМАТРИВАЕТ ОСУЩЕСТВЛЕНИЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ЛИБО ОСУЩЕСТВЛЕНИЕ ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ

- Глава поселения;
- Заместитель Главы;
- Ведущий специалист;
- Специалист (контрактный управляющий);
- Главный бухгалтер;
- Заместитель Главного бухгалтера;
- Специалист;
- Специалист-техник;
- Инструктор по физической культуре;
- Инструктор по работе с несовершеннолетними;
- Заведующий хозяйством.

Приложение № 7

УТВЕРЖДЕНА
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

Форма обязательства о неразглашении информации, содержащей персональные данные

Я, _____
(фамилия, имя, отчество лица, допущенного к обработке персональных данных)
_____,
исполняющий(ая) должностные обязанности
_____
_____
_____,
предупрежден(а) о том, что на период исполнения должностных обязанностей мне будет предоставлен допуск к информации, содержащей персональные данные.

Настоящим добровольно принимаю на себя обязательства:

1. Не передавать и не разглашать третьим лицам информацию, содержащую персональные данные, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей.
2. В случае попытки третьих лиц получить от меня информацию, содержащую персональные данные, сообщать непосредственному начальнику.
3. Не использовать информацию, содержащую персональные данные, с целью получения выгоды.
4. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.
5. В случае расторжения договора (контракта) и (или) прекращения права на допуск к информации, содержащей персональные данные, не разглашать и не передавать третьим лицам известную мне информацию, содержащую персональные данные.

Я предупрежден(а) о том, что нарушение данного обязательства является основанием привлечения к дисциплинарной и(или) иной ответственности в соответствии с законодательством Российской Федерации.

«____» _____ 20 г _____/_____
(подпись) (расшифровка подписи)

Приложение № 8

УТВЕРЖДЕНО
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

Согласие на обработку персональных данных

_____
(Наименование (Ф.И.О.) оператора, получающего согласие субъекта персональных данных)

_____
(Адрес оператора)

_____
(Ф.И.О. субъекта персональных данных)

_____
(Адрес, где зарегистрирован субъект персональных данных)

_____
(Номер основного документа, удостоверяющего его личность, сведения о дате выдачи документа и выдавшем его органе)

Даю своё согласие на обработку следующих персональных данных:
_____
(Перечень персональных данных)

с целью:_____
(Указывается цель обработки персональных данных)

Даю своё согласие на совершение следующих действий с моими персональными данными (**ненужное зачеркнуть**): сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Даю своё согласие на использование следующих способов обработки моих персональных данных (**ненужное зачеркнуть**):
- с использованием средств автоматизации (автоматизированная обработка);
- без использования средств автоматизации (неавтоматизированная обработка);
- смешанная обработка.

Срок, в течение которого действует согласие: _____
(Указывается срок действия согласия)

В случае неправомерных действий или бездействия оператора настоящее согласие может быть отозвано мной заявлением в письменном виде.

Дата:_____ _____ _____
(подпись) (инициалы, фамилия)

Приложение № 8.1

УТВЕРЖДЕНА
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

Типовая форма согласия на обработку персональных данных для реализации служебных (трудовых) отношений

с.Красный Яр «___» _____ 20__ г.

Я,_____
(фамилия, имя, отчество)
зарегистрированная по адресу: _____, _____паспорт _____ № _____ выдан_____, свободно, по своей воле и в своем интересе даю согласие оператору - администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области (местонахождение: Самарская область, Красноярский район, с. Красный Яр, кл. Комсомольская, д. 90, на обработку (любое действие (операцию) 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), а также передачу иным лицам для реализации функций оператора в целях обеспечения функционирования и безопасности информационной системы следующих персональных данных:

фамилия, имя, отчество (в том числе предыдущие в случае их изменения), пол, дата и место рождения, гражданство, фотография, домашний адрес (адрес регистрации, фактического проживания), номер телефона (либо иной вид связи);

данные паспорта или документа, его заменяющего (серия, номер, кем и когда выдан);

сведения об образовании (наименование учебного заведения, дата окончания учебного заведения, номер диплома, направление подготовки или специальность по диплому, квалификация по диплому);

послевузовское профессиональное образование: аспирантура, адъюнктура, докторантура (наименование образовательного или научного учреждения, год окончания, ученая степень, ученое звание (дата присвоения, номера дипломов, аттестатов);

сведения о наличии (отсутствии) классного чина федеральной гражданской службы, дипломатического ранга, воинского или специального звания, классного чина правоохранительной службы, классного чина гражданской службы субъекта Российской Федерации, квалификационного разряда государственной службы, квалификационного разряда или классного чина муниципальной службы (кем и когда присвоены);

сведения о владении иностранными языками;

сведения о судимости, когда и за что;

сведения о допуске к государственной тайне, оформленном за период работы, службы, учебы, его форма, номер и дата;

сведения о выполняемой работе с начала трудовой деятельности (наименование организации, ее адреса, месяца и года поступления и ухода, должности, включая учебу в высших и средних специальных учебных заведениях, военную службу, работу по совместительству, предпринимательскую деятельность и т.п.);

сведения о наличии государственных наград, иных наград и знаков отличия, почетных званиях и поощрениях;

сведения о близких родственниках (отец, мать, братья, сестры и дети, а также муж (жена), в том числе бывшие) с указанием степени родства, фамилии, имени, отчества (в том числе предыдущие в случае их изменения), даты и места рождения, места работы (наименование и адрес организации), должности, домашнего адреса (адрес регистрации, фактического проживания);

сведения о близких родственниках (отец, мать, братья, сестры и дети, а также муж (жена), в том

числе бывшие), постоянно проживающих за границей и (или) оформляющих документы для выезда на постоянное место жительства в другое государство;

сведения о пребывании за границей (когда, где, с какой целью);

данные о наличии заграничного паспорта (серия, номер, кем и когда выдан);

номер страхового свидетельства обязательного пенсионного страхования (далее - СНИЛС);

реквизиты страхового медицинского полиса обязательного медицинского страхования;

реквизиты свидетельства государственной регистрации актов гражданского состояния;

сведения из реестра дисквалифицированных лиц;

идентификационный номер налогоплательщика (далее - ИНН);

сведения о реквизитах и (или) копии иных документов, выданных на имя муниципального служащего;

материалы и результаты аттестации муниципального служащего;

сведения о повышении квалификации, профессиональной переподготовке;

сведения об отпусках;

сведения о реквизитах банковских счетов для выплаты денежного содержания и о размере денежного содержания муниципального служащего;

сведения о занимаемой должности;

отношение к воинской обязанности;

сведения о воинском учете: воинское звание, категория запаса, военно-учетная специальность, категория годности к воинской службе, наименование военного комиссариата по месту жительства, состояние на воинском учете;

сведения о социальном положении (в том числе о социальных льготах);

сведения о семейном положении;

сведения о составе семьи, содержащиеся в выписке из домовой книги, копиях финансового лицевого счета, свидетельства о браке, свидетельства о рождении ребенка (детей), трудовой книжки;

сведения из заключения медицинского учреждения о наличии (отсутствии) заболевания, препятствующего прохождению муниципальной службы;

сведения о доходах, расходах, об имуществе, о денежных средствах, находящихся на счетах в банках и иных кредитных организациях, о ценных бумагах, об обязательствах имущественного характера, прочих обязательствах муниципального служащего, его супруги (супруга), несовершеннолетних детей;

сведения, содержащиеся в документах о наличии в собственности муниципального служащего и (или) членов его семьи жилых помещений;

сведения о размерах начисленных, удержанных и оплаченных налогов, в т.ч. налога на доходы физических лиц;

сведения о взносах во внебюджетные фонды Российской Федерации, в т.ч. в Пенсионный фонд Российской Федерации, Фонд обязательного медицинского страхования Российской Федерации, Фонд социального страхования Российской Федерации;

сведения, указанные в оригиналах и копиях распоряжениеов по личному составу и материалах к ним;

материалы по служебным проверкам в отношении муниципального служащего;

сведения о временной нетрудоспособности;

табельный номер.

Вышеуказанные персональные данные предоставляются для обработки в целях обеспечения соблюдения в отношении меня законодательства Российской Федерации в сфере отношений, связанных с поступлением на муниципальную службу и работу в администрации сельского поселения Красный Яр муниципального района Красноярский (работу), ее прохождением и прекращением (трудовых и непосредственно связанных с ними отношений) для реализации функций, возложенных на Администрацию сельского поселения Красный Яр муниципального района Красноярский Самарской области действующим законодательством.

Я ознакомлен(а), что:

1) согласие на обработку персональных данных действует с даты подписания настоящего согласия в течение всего срока прохождения муниципальной службы (работы) в администрации сельского поселения Красный Яр муниципального района Красноярский;

2) согласие на обработку персональных данных может быть отозвано на основании письменного заявления в произвольной форме;

3) в случае отзыва согласия на обработку персональных данных администрация сельского поселения Красный Яр муниципального района Красноярский Самарской области прекращает обработку персональных данных в течение 10 дней с даты получения отзыва. Указанный срок может быть продлен не более чем на пять рабочих дней по мотивированному уведомлению, которое оператор должен направить в адрес субъекта ПД (ч. 5.1 ст. 21 Закона о ПД в новой ред.). Администрация сельского поселения Красный Яр вправе продолжить обработку персональных данных при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

4) после увольнения с муниципальной службы (прекращения трудовых отношений) персональные данные хранятся в администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области в течение срока хранения документов, предусмотренного действующим законодательством Российской Федерации;

5) персональные данные, предоставляемые в отношении третьих лиц, будут обрабатываться только в целях осуществления и выполнения функций, возложенных законодательством Российской Федерации на администрацию сельского поселения Красный Яр муниципального района Красноярский Самарской области.

Дата начала обработки персональных данных:

_____ _____

(число, месяц, год) (подпись)

Зарегистрировано в журнале учета документов
о согласии на обработку персональных данных
«___» _____ 20___ № _____

Приложение № 8.2

УТВЕРЖДЕНО
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

Администрация сельского поселения Красный Яр
Адрес организации: 446370, Самарская область,
Красноярский район, с. Красный Яр, ул. Комсомольская, д. 90
от _____
(Фамилия Имя Отчество)
адрес регистрации:_____
_____

Согласие на обработку персональных данных, разрешённых субъектом персональных данных для распространения

Настоящим я, _____,
руководствуясь статьей 10.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», заявляю о согласии на распространение Администрацией сельского поселения Красный Яр моих персональных данных с целью размещения информации обо мне на официальном сайте ttps://kryarposelenie.ru/ в следующем порядке:

Категория персональных данных	Перечень персональных данных	Разрешаю к распространению (да/нет)	Разрешаю к распространению неограниченному кругу лиц (да/нет)	Условия и запреты	Дополнительные условия
Общие персональные данные	Фамилия				
	Имя				
	Отчество				
	Год рождения				
	Месяц рождения				
	Дата рождения				
	Место рождения				
	Адрес				
	Семейное положение				
	Образование				
	Профессия				
Специальные категории персональных данных	Состояние здоровья				
	Сведения о судимости				
Биометрические персональные данные	Цветное цифровое фотографическое изображение лица				

Сведения об информационных ресурсах учреждения, посредством которых будут осуществляться предоставление доступа неограниченному кругу лиц и иные действия с персональными данными:

Информационный ресурс	Действия с персональными данными
https://kryarposelenie.ru/ https://vk.com/aspkrasnyar	Предоставление сведений неограниченному кругу лиц

Настоящее согласие дано мной добровольно и действует до отзыва.
Оставляю за собой право потребовать прекратить распространять мои персональные данные. В случае получения требования учреждение обязано немедленно прекратить распространять мои персональные данные, а также сообщить мне перечень третьих лиц, которым персональные данные были переданы.

_____ _____ _____
Дата *подпись* *Фамилия Инициалы*

Приложение № 8.3.

УТВЕРЖДЕНО
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

СОГЛАСИЕ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ПРЕДОСТАВЛЕНИИ МУНИЦИПАЛЬНОЙ УСЛУГИ

Я, _____
субъект персональных данных (его представитель)
проживающий (ая) по адресу: _____
паспорт: _____
в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» даю свое согласие администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области (далее - Оператор), расположенной по адресу: 446370, Самарская область, Красноярский район, с. Красный Яр, ул. Комсомольская, д.90 на обработку своих персональных данных. Обработка вышеуказанных персональных данных будет осуществляться путем смешанной обработки (сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в случаях прямо предусмотренных действующим законодательством РФ), блокирование, уничтожение. Я подтверждаю, что ознакомлен (а) с порядком предоставления истребуемой муниципальной услуги, а также с правилами обработки персональных данных Оператором, осуществляемой на бумажном и электронном носителях с использованием автоматизированных систем.

Целью предоставления и обработки персональных данных является:

1. Определение возможности предоставления муниципальной услуги;
2. Предоставление муниципальной услуги;

Согласие на обработку персональных данных в целях, указанных в пункте 1, действительно с момента предоставления настоящего согласия и в течение всего срока рассмотрения документов и принятия решения о предоставлении (отказе от предоставления) соответствующей муниципальной услуги. Согласие на обработку персональных данных в целях, указанных в пункте 2, действует в течение всего срока предоставления муниципальной услуги, а также 5 (пяти) лет с момента предоставления результата муниципальной услуги. Я уведомлен (а) о своем праве отозвать согласие путем подачи Оператору письменного заявления. Отказ от предоставления своих персональных данных влечет невозможность Оператора исполнить муниципальную услугу. Подтверждаю, что ознакомлен (а) с положениями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», права и обязанности в области защиты персональных данных мне разъяснены.

Кроме того, я уведомлен, что Оператор имеет право предоставлять информацию по официальному запросу третьих лиц только в установленных законом случаях.

_____	_____	_____
Дата	Подпись	Ф.И.О.
_____	_____	_____
Дата	Подпись	Ф.И.О. ответственного сотрудника Оператора: сотрудника, принявшего данное согласие)

Приложение № 9

УТВЕРЖДЕН
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

ПОРЯДОК ДОСТУПА В ПОМЕЩЕНИЯ, В КОТОРЫХ ВЕДЁТСЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ, В АДМИНИСТРАЦИИ СЕЛЬСКОГО ПОСЕЛЕНИЯ КРАСНЫЙ ЯР МУНИЦИПАЛЬНОГО РАЙОНА КРАСНОЯРСКИЙ САМАРСКОЙ ОБЛАСТ**И**

1. Настоящая инструкция определяет порядок доступа сотрудников Администрацией сельского поселения Красный Яр (далее - Администрация) и других лиц в помещения, предназначенные для обработки персональных данных.

2. Ответственность за обеспечение исполнения требований настоящей инструкции несет ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных.

3. Для помещений, в которых обрабатываются персональные данные, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей персональных данных и средств защиты информации, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц. При хранении материальных носителей персональных данных должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.

4. В помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации, допускаются только сотрудники и должностные лица, получившие доступ к персональным данным.

5. Нахождение в помещениях, в которых ведется обработка персональных данных лиц, не являющихся сотрудниками и должностными лицами, получившими доступ к персональным данным, возможно только в присутствии сотрудников и должностных лиц, получивших доступ к персональным данным на время, ограниченное необходимостью решения вопросов, связанных с исполнением должностных функций.

6. Присутствие других лиц в данных помещениях допускается в той мере, в какой этого требуют технологические процессы обработки персональных данных. Доступ в помещения Администрации осуществляется только в сопровождении сотрудника Администрации, который предварительно производит оценку целесообразности и требуемого времени нахождения лица в помещении, а также проверяет документы, удостоверяющие личность.

7. Сотрудники и должностные лица, получившие доступ к персональным данным не должны покидать помещение, в котором ведется обработка персональных данных, оставляя в нем без присмотра посторонних лиц, включая сотрудников, не уполномоченных на обработку персональных данных.

8. Доступ в помещения, в которых осуществляется обработка персональных данных, разрешается только в рабочее время.

9. Доступ в помещения, в которых осуществляется обработка персональных данных, в нерабочее время возможен только по письменной заявке работника, согласованной с его непосредственным Главой и имеющей разрешающую резолюцию Главы поселения. Данные заявки хранятся у лица, ответственного за организацию обработки персональных данных в Администрации.

10. В помещениях, в которых происходит обработка и хранение персональных данных, запрещено использование не предусмотренных служебными обязанностями технических устройств, фотографирование, видеозапись, звукозапись, в том числе с использованием мобильных телефонов.

11. Для предотвращения несанкционированного доступа к информации, содержащей ПДн, осуществляется контроль деятельности рабочих. Рабочие и специалисты ремонтно-строительных организаций пропускаются в помещение для проведения ремонтно-строительных работ на основании заявок, подписанных Главой поселения или его заместителями. Работы проводятся под контролем сотрудников Администрации.

12. Для исключения несанкционированного доступа к информации, содержащей ПДн, организована охрана помещений Администрации. Режим работы охраны устанавливается локальными актами Администрации.

13. Уборка помещения выполняется обслуживающим персоналом под контролем сотрудников, имеющих право доступа в данное помещение. Во время уборки в помещении должна быть приостановлена работа с ПДн, должны быть выключены все АРМ, на которых хранятся ПДн, носители, содержащие ПДн должны быть убраны в сейф.

14. После окончания рабочего дня дверь каждого помещения закрывается на ключ, при этом запрещается оставлять ключ в замке помещения.

15. В нерабочее время помещения, в которых ведется обработка персональных данных, хранятся документы, содержащиеся персональные данные, должны закрываться на ключ.

16. По окончании рабочего дня помещения, в которых ведется обработка ПДн, и установленные в них хранилища должны быть закрыты, хранилища опечатаны.

17. При утрате ключа от хранилища или от входной двери в помещение, в котором ведется обработка ПДн, замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить. Порядок хранения ключевых и других документов в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает ответственный за безопасность персональных данных.

18. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному за безопасность персональных данных. Ответственный за безопасность персональных данных должен составить акт и принять, при необходимости, меры к локализации последствий несанкционированного доступа к ПДн.

19. Контроль соблюдения настоящего Порядка осуществляется лицом, ответственным за организацию обработки персональных данных Администрации.

20. Лицо, ответственное за организацию обработки персональных данных, в случае установления факта нарушения сотрудником Администрации настоящего Порядка проводит с ним разъяснительную работу, а в случае неоднократного нарушения – уведомляет Главу поселения.

Приложение № 10

УТВЕРЖДЕНЫ
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

ПРАВИЛА РАССМОТРЕНИЯ ЗАПРОСОВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ ИЛИ ИХ ПРЕДСТАВИТЕЛЕЙ В АДМИНИСТРАЦИИ СЕЛЬСКОГО ПОСЕЛЕНИЯ КРАСНЫЙ ЯР МУНИЦИПАЛЬНОГО РАЙОНА КРАСНОЯРСКИЙ САМАРСКОЙ ОБЛАСТИ

ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила определяют порядок рассмотрения запросов субъектов персональных данных (далее ПДн) или их представителей в организации «наименование» (далее – Организация).

1.2. Настоящие Правила разработаны в соответствии с:

1.2.1. Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее Федеральный закон №152-ФЗ).

1.2.2. Федеральным законом от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации».

1.3. Основные понятия и термины, используемые в настоящих Правилах, применяются в значениях, определенных статьей 3 Федерального закона № 152-ФЗ.

ПРАВИЛА РАССМОТРЕНИЯ ЗАПРОСОВ

1.4. Субъект ПДн имеет право на получение информации в Организации касающейся обработки его ПДн (часть 7 статьи 14 Федерального закона №152-ФЗ), в том числе содержащей:

1.4.1. Подтверждение факта обработки ПДн Организацией.

1.4.2. Правовые основания и цели обработки ПДн.

1.4.3. Цели и применяемые Организацией способы обработки ПДн.

1.4.4. Наименование и место нахождения Организации, сведения о лицах (за исключением работников оператора), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Организацией или на основании федерального закона.

1.4.5. Обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом.

1.4.6. Сроки обработки ПДн, в том числе сроки их хранения.

1.4.7. Порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом № 152-ФЗ.

1.4.8. Информацию об осуществленной или о предполагаемой трансграничной передаче ПДн.

1.4.9. Наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Организации, если обработка поручена или будет поручена такому лицу.

1.4.10. Иные сведения, предусмотренные Федеральным законом № 152-ФЗ или другими федеральными законами.

1.5. Сведения, указанные в п. 2.1, должны предоставляться субъекту ПДн или его представителю Организацией при обращении либо при получении запроса субъекта ПДн или его представителя.

1.6. Запрос субъекта ПДн должен содержать:

1.6.1. Номер основного документа, удостоверяющего личность субъекта ПДн или его представителя.

1.6.2. Сведения о дате выдачи указанного документа и выдавшем его органе.

1.6.3. Сведения, подтверждающие участие субъекта ПДн в отношениях с Организацией (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения).

1.6.4. Вместо сведений, указанных в пункте 2.3.3 допустимы сведения, иным образом подтверждающие факт обработки ПДн Организацией;

1.6.5. Подпись субъекта ПДн или его представителя.

В Организации разработаны и используются соответствующие бланки с формами обращений субъектов ПДн (ПРИЛОЖЕНИЯ №1, №2, №3 и №4 к настоящим Правилам).

1.7. Запрос может быть, также, направлен субъектом ПДн в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

1.8. Сведения, указанные в п. 2.1, должны быть предоставлены субъекту ПДн Организацией в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.

1.9. Субъект ПДн вправе требовать от Организации уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

1.10. Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с частью 8 статьи 14 Федерального закона №152-ФЗ.

1.11. Запросы, поступающие в Организацию, должны обрабатываться в соответствии с требованиями Федерального закона №152-ФЗ и рассматриваться в соответствии с требованиями Федерального закона от 02 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» и локальными актами Администрации в течение десяти рабочих дней с момента обращения (получения оператором соответствующего запроса). Указанный срок может быть продлен не более чем на пять рабочих дней по мотивированному уведомлению, которое оператор должен направить в адрес субъекта ПД. Сведения предоставляются в той форме, в которой направлено соответствующее обращение (запрос), если в нем не указано иное (ч. 3 ст. 14 Закона о ПД в новой ред.)

1.12. Все поступившие запросы регистрируются в день их поступления. На запросе указывается входящий номер и дата регистрации. В Организации разработана и используется соответствующая форма журнала регистрации запросов субъектов ПДн (ПРИЛОЖЕНИЕ №5 к настоящим Правилам).

1.13. Рассмотрение запросов и подготовка ответов осуществляется по поручению Главы поселения или его заместителя.

1.14. Рассмотрение запросов и подготовку ответов могут осуществлять сотрудники Администрации поселения, обрабатывающие ПДн, в соответствии с их должностным регламентом (инструкцией).

1.15. Ответы субъекту ПДн направляются в виде уведомлений. В Организации разработаны и используются соответствующие формы бланков уведомлений (ПРИЛОЖЕНИЯ №6, №7, №8, №9, №10, №11 к настоящим Правилам).

1.16. Сотрудники Организации, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящими Правилами, в пределах, определенных действующим законодательством Российской Федерации.

ПРИЛОЖЕНИЕ № 1
к «Правилам рассмотрения
запросов субъектов ПДн»

Вх. №_____ дата _____

Администрация сельского поселения Красный Яр
Адрес организации: 446370, Самарская область,
Красноярский район, с. Красный Яр, ул. Комсомольская, д. 90
от _____
(Фамилия Имя Отчество)
адрес регистрации:_____
_____

ЗАПРОС НА ПРЕДОСТАВЛЕНИЕ ИНФОРМАЦИИ ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ.

От _____
(фамилия, имя, отчество)

паспорт _____ выданный _____
(номер) (дата выдачи)

_____
(место выдачи п спорта)

Адрес: _____
(адрес места жительства)

Основания, по которым лицо выступает в качестве законного представителя субъекта персональных данных:

_____

Сведения, подтверждающие факт обработки персональных данных в организации «наименование»:

_____

В соответствии со ст. 14 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» прошу предоставить мне следующую информацию, касающуюся обработки моих персональных данных:

- подтвердить факт обработки моих персональных данных;
- правовые основания и цели обработки моих персональных данных;
- наименование и местонахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к моим персональным данным или которым могут быть раскрыты мои персональные данные на основании договора или на основании федерального закона;
- относящиеся ко мне обрабатываемые персональные данные, источник их получения;
- сроки обработки моих персональных данных, в том числе сроки их хранения;
- порядок осуществления мной прав, предусмотренных Федеральным законом «О персональных данных»;
- информацию об осуществленной или предполагаемой трансграничной передаче моих персональных данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку моих персональных данных если обработка поручена или будет поручена такому лицу
- _____.
(иные сведения)

Данный запрос является первичным / повторным, на основании того, что:

_____
(ОБЯЗАТЕЛЬНО: указать причину направления повторного запроса)

Указанные сведения прошу предоставить по адресу:

_____

_____ _____
(дата) (подпись)

ПРИЛОЖЕНИЕ № 2
к «Правилам рассмотрения
запросов субъектов ПДн»

_____

Вх. №_____ дата _____

Администрация сельского поселения Красный Яр
Адрес организации: 446370, Самарская область,
Красноярский район, с. Красный Яр, ул. Комсомольская, д. 90
от _____
(Фамилия Имя Отчество)
адрес регистрации:_____
_____

ЗАЯВЛЕНИЕ

об отзыве согласия на обработку персональных данных.

От _____
(фамилия, имя, отчество)

паспорт _____ выданный _____
(номер) (дата выдачи)

_____
(место выдачи паспорта)

Адрес: _____
(адрес места жительства)

Основания, по которым лицо выступает в качестве законного представителя субъекта персональных данных:
_____

Сведения, подтверждающие факт обработки персональных данных в организации «наименование»:
_____

Прошу прекратить обработку моих персональных данных, осуществляемую в целях:
_____
(цели обработки персональных данных, в отношении которых отзывается согласие)

по причине:
_____

_____ _____
(дата) (подпись)

ПРИЛОЖЕНИЕ № 3
к «Правилам рассмотрения
запросов субъектов ПДн»

Вх. №_____ дата _____

Администрация сельского поселения Красный Яр
Адрес организации: 446370, Самарская область,
Красноярский район, с. Красный Яр, ул. Комсомольская, д. 90
от _____
(Фамилия Имя Отчество)
адрес регистрации:_____
_____

ЗАПРОС
на уточнение персональных данных.

От _____
(фамилия, имя, отчество)

паспорт _____ выданный _____
(номер) (дата выдачи)

_____
(место выдачи паспорта)

Адрес: _____
(адрес места жительства)

Основания, по которым лицо выступает в качестве законного представителя субъекта персональных данных:
_____

Сведения, подтверждающие факт обработки персональных данных в организации «наименование»:
_____

в соответствии с положениями ст. 14 и ст. 21 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» прошу уточнить/ уничтожить мои персональные данные в связи с тем, что:
_____
_____
(указать причину: персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки; с персональными данными совершаются неправомерные действия – указать какие)

_____ _____
(подпись) (дата)

ПРИЛОЖЕНИЕ № 4
к «Правилам рассмотрения
запросов субъектов ПДн»

Вх. №_____ дата _____

Администрация сельского поселения Красный Яр
Адрес организации: 446370, Самарская область,
Красноярский район, с. Красный Яр, ул. Комсомольская, д. 90
от _____
(Фамилия Имя Отчество)
адрес регистрации:_____
_____

ВОЗРАЖЕНИЕ

против принятия решений на основании исключительно автоматизированной обработки персональных данных.

От _____
(фамилия, имя, отчество)

паспорт _____ выданный _____
(номер) (дата выдачи)

_____
(место выдачи паспорта)

Адрес: _____
(адрес места жительства)

Основания, по которым лицо выступает в качестве законного представителя субъекта персональных данных:
_____

Сведения, подтверждающие факт обработки персональных данных в организации «наименование»:
_____

Прошу исключить принятие в отношении меня юридически значимых решений на основании исключительно автоматизированной обработки моих персональных данных.

_____ _____
(дата) (подпись)

ПРИЛОЖЕНИЕ № 5
к «Правилам рассмотрения запросов
субъектов персональных данных»

ЖУРНАЛ
обращений субъектов персональных данных о выполнении ими законных прав в области защиты персональных данных.

Начат: «___» _____ 20__ г.
Окончен: «___» _____ 20__ г.

1	2	3	4	5	6	7	8
№	Сведения о запрашивающем лице (ФИО, адрес)	Краткое содержание обращения	Цель запроса	Отметка о предоставлении информации или отказе в ее предоставлении	Дата передачи / отказа в предоставлении информации	Подпись ответственного лица	Примечание
*1**	*Иванов И.И., РФ г. Иванов, ул. Иванова, д.1, кв. 1*	*перечень измененных персональных данных*	*уточнение персональных данных*	*отправлено почтовое уведомление №233 об уточнении ПДн*	*1.01.2017*	*_____ (Петров П.П.)*	*Пример заполнения*

ПРАВИЛА

по формированию и ведению журнала обращений субъектов персональных данных о выполнении ими законных прав в области защиты персональных данных.

1. ФОРМИРОВАНИЕ ЖУРНАЛА.
   1.1. Журнал формируется из стандартных листов формата А4 в альбомной ориентации
   1.2. Обложка журнала формируется на отдельном листе.
   1.3. Все листы журнала, за исключением листов обложки, нумеруются.
   1.4. Все листы журнала, вместе с обложкой сшиваются.
2. ВЕДЕНИЕ ЖУРНАЛА.
   2.1. Перед началом использования журнала на лицевой стороне обложки указывается номер журнала по номенклатуре дел (журналов) на текущий год и дата начала ведения журнала.
   2.2. Графы журнала заполняются следующим образом:
      2.2.1. Графа 1 – номер записи по порядку.
      2.2.2. Графа 2 – ФИО и адрес субъекта ПДн, обратившегося в организацию по вопросу обработки его персональных данных.
      2.2.3. Графа 3 – кратко содержание обращения (**например – перечень измененных персональных данных**).
      2.2.4. Графа 4 – кратко о цели обращения субъекта персональных данных (**например – уточнение персональных данных**).
      2.2.5. Графа 5 – запись о действии в ответ на обращение (**например – субъекту отправлено почтовое уведомление №233 об уточнении ПДн**).
      2.2.6. Графа 6 – дата отправки уведомления субъекту персональных данных.
      2.2.7. Графа 7 – подпись сотрудника отправившего уведомление субъекту персональных данных.
      2.2.8. Графа 8 – Любая информация, относящаяся к обращению субъекта персональных данных.
   2.3. Все записи в журнале делаются четко и разборчиво. В случае если вносимые данные не помещаются на одной строке (в одной ячейке), то используется необходимое количество строк.

ПРИЛОЖЕНИЕ № 6
к «Правилам рассмотрения
запросов субъектов ПДн»

Исх. №_____

Субъекту персональных данных:
_____
(ФИО)

Адрес: _____

УВЕДОМЛЕНИЕ.

Оператор персональных данных: Администрация сельского поселения Красный Яр муниципального района Красноярский Самарской области

находящийся по адресу:446370, Самарская область, село Красный Яр, ул. Комсомольская, 90

не осуществляет обработку Ваших персональных данных, начиная с:

_____
(Дата, с которой прекращена обработка ПДН)

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

« » _____ 20 г.

ПРИЛОЖЕНИЕ № 7
к «Правилам рассмотрения
запросов субъектов ПДн»

Исх. №_____

Субъекту персональных данных:
_____
(ФИО)

Адрес: _____

ОТКАЗ

в предоставлении сведений.

Оператор персональных данных: Администрация сельского поселения Красный Яр муниципального района Красноярский Самарской области

находящийся по адресу:446370, Самарская область, село Красный Яр, ул. Комсомосльская, 90

Вам отказано в предоставлении сведений по запросу от

_____
(дата запроса)

на основании _____
(ссылка на нормы ФЗ «О персональных данных» или иных федеральных законов)

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

« » _____ 20 г.

ПРИЛОЖЕНИЕ № 8
к «Правилам рассмотрения
запросов субъектов ПДн»

Исх. №_____

Субъекту персональных данных:
_____
(ФИО)

Адрес: _____

УВЕДОМЛЕНИЕ.

Оператор персональных данных: Администрация сельского поселения Красный Яр муниципального района Красноярский Самарской области

находящийся по адресу: 446370, Самарская область, село Красный Яр, ул. Комсомольская, 90

По Вашему запросу от _____
(дата запроса)

уведомляет Вас о невозможности отзыва согласия на обработку персональных данных в следующих целях:
_____

Дата начала обработки персональных данных:
_____

Срок или условие прекращения обработки персональных данных:
_____

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

« » _____ 20 г.

ПРИЛОЖЕНИЕ № 9
к «Правилам рассмотрения
запросов субъектов ПДн»

Исх. №_____

Субъекту персональных данных:
_____
(ФИО)

Адрес: _____

УВЕДОМЛЕНИЕ.

Оператор персональных данных: Администрация сельского поселения Красный Яр муниципального района Красноярский Самарской области

находящийся по адресу: 446370, Самарская область, село Красный Яр, ул. Комсомольская, 90

По Вашему запросу от _____
(дата запроса)

Было произведено уточнение Ваших персональных данных.

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

« » _____ 20 г.

ПРИЛОЖЕНИЕ № 10
к «Правилам рассмотрения
запросов субъектов ПДн»

Исх. №_____

Субъекту персональных данных:
_____
(ФИО)

Адрес: _____

ОТВЕТ

на возражение против принятия решений на основании исключительно автоматизированной обработки ПДН.

Оператор персональных данных: Администрация сельского поселения Красный Яр муниципального района Красноярский Самарской области

находящийся по адресу: 446370, Самарская область, село Красный Яр, ул. Комсомольская, 90

Рассмотрел Ваши возражения от: _____
(дата запроса)

И принял следующее решение:

_____

_____

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

« » _____ 20 г.

ПРИЛОЖЕНИЕ № 11
к «Правилам рассмотрения
запросов субъектов ПДн»

Исх. №_____

Субъекту персональных данных:
_____
(ФИО)

Адрес: _____

УВЕДОМЛЕНИЕ
о блокировании персональных данных.

Оператор персональных данных: Администрация сельского поселения Красный Яр муниципального района Красноярский Самарской области

находящийся по адресу: 446370, Самарская область, село Красный Яр, ул. Комсомольская, 90 осуществил блокирование Ваших персональных данных, включая:

_____
(перечисление блокированных персональных данных: Ф.И.О., адрес, телефон…)

которые обрабатывались в целях:

_____
(цель обработки указанных персональных данных)

Указанные персональные данные были заблокированы _____
(дата блокирования)

в связи с: _____
(причина блокирования персональных данных)

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

« » _____ 20 г.

Приложение № 11

УТВЕРЖДЕНЫ
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

ПРАВИЛА ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Статья 1. Цель внутреннего контроля.

1. Внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных осуществляется с целью проверки соответствия обработки персональных данных требованиям к защите персональных данных, установленных Федеральным законом №152-ФЗ «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области .

Статья 2. Виды и периодичность внутреннего контроля.

1. Внутренний контроль соответствия обработки персональных данных делится на текущий и периодический.
2. Текущий внутренний контроль осуществляется на постоянной основе Ответственным за обеспечение безопасности персональных данных.
3. Периодический внутренний контроль осуществляется комиссией в соответствии с поручением Главы или Администрации сельского поселения Красный Яр.

Периодичность проверки – **не реже одного раза в шесть месяцев.**

Статья 3. Порядок создания комиссии для осуществления внутреннего контроля.

1. Проверки осуществляются комиссией, созданной Распоряжением Главы сельского поселения Красный Яр муниципального района Красноярский Самарской области Глава Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области , из числа сотрудников Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области , допущенных к обработке персональных данных, так же возможно привлечение в качестве членов комиссий экспертов или сотрудников Администрации сельского поселения Красный Яр.

В проведении проверки не может участвовать лицо, прямо или косвенно заинтересованное в её результатах.

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

Статья 4. Порядок проведения внутренней проверки.

1. При проведении внутренней проверки комиссией должны быть полностью, объективно и всесторонне установлены:

- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке;
- порядок и условия применения средств защиты информации;
- эффективность принимаемых мер по обеспечению безопасности персональных данных;
- состояние учёта бумажных и машинных носителей персональных данных;
- соблюдение правил доступа к персональным данным;
- наличие (отсутствие) фактов несанкционированного доступа к персональным данным;
- мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- осуществление мероприятий по обеспечению целостности персональных данных.

2. Осуществлении внутреннего контроля мероприятий проводятся комиссией периодически в соответствии с Перечнем мероприятий для осуществления внутреннего контроля за

выполнением требований к защите персональных данных при их обработке в информационных системах персональных данных. Форма Перечня мероприятий для осуществления внутреннего контроля за выполнением требований к защите персональных данных при их обработке в информационных системах персональных данных приведена в Приложении 1 к настоящим Правилам.

Для каждой проверки составляется Протокол проведения внутренней проверки. Форма Протокола приведена в Приложении 2 к настоящим Правилам.

3. При выявлении в ходе проверки нарушений в Протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.

4. Протоколы хранятся у председателя комиссии в течение текущего года. Уничтожение Протоколов проводится комиссией самостоятельно по истечении срока хранения.

5. О результатах проверки и мерах, необходимых для устранения нарушений председатель комиссии докладывает Главе.

6. Срок проведения проверки не может составлять более 30 (тридцати) дней со дня принятия решения о её проведении.

Приложение 1

Перечень

мероприятий для осуществления внутреннего контроля за выполнением требований к защите персональных данных при их обработке в информационных системах персональных данных

№ п/п	Краткое описание мероприятий
1	Контроль технического состояния средств охранной и пожарной сигнализации и соблюдения режима охраны
2	Проверка выполнения требований по условиям размещения автоматизированных рабочих мест (далее - АРМ) в помещениях, в которых размещены средства информационных систем персональных данных (далее - ИСПДн)
3	Проверка соответствия состава и структуры программно-технических средств ИСПДн документированному составу и структуре средств, разрешенных для обработки персональных данных
4	Проверка режима допуска в помещения, где размещены средства ИСПДн и осуществляется обработка персональных данных
5	Проверка соответствия реального уровня полномочий по доступу к персональным данным различных пользователей, установленному в списке лиц, допущенных к обработке персональных данных, уровню полномочий
6	Проверка наличия и соответствия средств защиты информации в соответствии с указанными в техническом паспорте на ИСПДн
7	Проверка правильности применения средств защиты информации
8	Проверка неизменности настроенных параметров антивирусной защиты на рабочих станциях пользователей
9	Контроль за обновлениями программного обеспечения и единообразия применяемого программного обеспечения на всех элементах ИСПДн
10	Проверка соблюдения правил парольной защиты
11	Проверка работоспособности системы резервного копирования
12	Проведение мероприятий по проверке организации учета и условий хранения съемных носителей персональных данных
13	Проверка соблюдения требований по обеспечению безопасности при использовании ресурсов сети "Интернет"
14	Проверка знаний работниками руководящих документов, технологических инструкций, предписаний, актов, заключений и уровня овладения работниками технологией безопасной обработки информации, изложенных в инструкциях
15	Проверка знаний инструкций по обеспечению безопасности информации пользователями ИСПДн
16	Проверка наличия документов, подтверждающих возможность применения технических и программных средств вычислительной техники для обработки персональных данных и применения средств защиты (сертификатов соответствия и других документов)

Приложение 2

Протокол

осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

Настоящий Протокол составлен в том, что __.__.202_ комиссией по внутреннему контролю проведена проверка _____
_____.
место проверки

Проверка осуществлялась в соответствии с требованиями _____
_____
название документа

В ходе проверки проверено:_____
_____
_____

Выявленные нарушения:

_____
_____

Меры по устранению нарушений:

_____
_____

Срок устранения нарушений: ____.

Председатель комиссии _____ И.О. Фамилия

Члены комиссии:

Должность _____ И.О. Фамилия

Должность _____ И.О. Фамилия

Должность Главы
проверяемого подразделения _____ И.О. Фамилия

Приложение № 12

УТВЕРЖДЕНА
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

ИНСТРУКЦИЯ ПО ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ АДМИНИСТРАЦИИ СЕЛЬСКОГО ПОСЕЛЕНИЯ КРАСНЫЙ ЯР МУНИЦИПАЛЬНОГО РАЙОНА КРАСНОЯРСКИЙ САМАРСКОЙ ОБЛАСТИ

1. Общие положения

Данный документ определяет правила и основные требования по обеспечению антивирусной защиты в информационных системах персональных данных (далее –ИСПДн) и устанавливает ответственность за их выполнение.

2. Основные определения

Вредоносное программное обеспечение (далее ПО) - специально разработанное программное обеспечение, программный модуль, блок, группа команд, имеющая способность к самораспространению, которая может попадать в общее и специальное программное обеспечение ИСПДн и приводить к:

- дезорганизации вычислительного процесса (нарушению или существенному замедлению обработки информации);
- модификации или уничтожению программ, или данных;
- приведению в негодность носителей информации и других технических средств;
- нарушению функционирования средств защиты информации.

3. Инструкция по применению средств антивирусной защиты

Защита ПО ИСПДн от вредоносного ПО осуществляется путем применения специализированных средств антивирусной защиты.

- К использованию допускаются только лицензионные антивирусные средства, обладающие необходимой сертификацией в регулирующих органах РФ.
- Решение задач по установке и сопровождению средств антивирусной защиты возлагается на системного администратора Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области .
- Частота обновления баз данных средств антивирусной защиты устанавливается не реже 1 раза в сутки.
- Всё впервые вводимое в эксплуатацию ПО должно проходить обязательный антивирусный контроль.
- Контроль системы управления средствами антивирусной защиты осуществляется централизованно с рабочего места системного администратора Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области .
- Средства антивирусной защиты устанавливаются на всех рабочих станциях и серверах ИСПДн.
- Ежедневно в установленное время в автоматическом режиме проводится антивирусный контроль всех дисков и файлов рабочих станций и серверов ИСПДн.
- Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы, архивы), получаемая и передаваемая по телекоммуникационным каналам (включая электронную почту), а также информация на съемных носителях.
- Контроль входящей информации необходимо проводить непосредственно после ее приема.
- Контроль исходящей информации необходимо проводить непосредственно перед отправкой.
- Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

- 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.) пользователь, обнаруживший проблему, должен провести внеочередной антивирусный контроль рабочей станции либо обратиться к системному администратору Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области.
- При получении информации о возникновении вирусной эпидемии вне ИС должно быть осуществлено информирование пользователей о возможной эпидемии и рекомендуемых действиях.
- В случае обнаружения зараженных компьютерными вирусами файлов пользователи обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения вируса системного администратора Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области;
- провести лечение зараженных файлов;
- в случае невозможности лечения обратиться к администратору безопасности ИСПДн.

- По факту обнаружения зараженных вирусом файлов системный администратор Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области должен составить служебную записку, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.
- Пользователям запрещается отключать, выгружать или деинсталлировать средства антивирусной защиты на рабочих станциях.
- Настройка параметров средств антивирусной защиты осуществляется в соответствии с руководствами по применению конкретных антивирусных средств.
- Ответственный за организацию обработки ПДн должен проводить расследования случаев появления вирусов для выявления причин и принятия соответствующих действий по их предотвращению.
- С данной инструкцией Пользователи должны быть ознакомлены под подпись в листе ознакомления с данной инструкцией.
- Проводить периодическое тестирование функций средств антивирусной защиты.
- Проводить тестирование функций средств антивирусной защиты при изменениях (внедрении новых средств, их обновлении, изменениях в системе).

Приложение № 13
УТВЕРЖДЕН
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

ПОРЯДОК УЧЕТА, ХРАНЕНИЯ И УНИЧТОЖЕНИЯ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ В АДМИНИСТРАЦИИ СЕЛЬСКОГО ПОСЕЛЕНИЯ КРАСНЫЙ ЯР МУНИЦИПАЛЬНОГО РАЙОНА КРАСНОЯРСКИЙ САМАРСКОЙ ОБЛАСТИ

1. Термины и определения

В настоящем Порядке использованы следующие термины и определения:

Информация: Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Конфиденциальная информация: Информация, доступ к которой ограничивается в соответствии с действующим законодательством РФ, и иными регламентирующими документами.

Конфиденциальность персональных данных: Обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта ПДн или наличия иного законного основания.

Несанкционированный доступ (несанкционированные действия): Доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами ПДн.

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 ПДн.

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

Пользователь персональных данных: Лицо, участвующее в процессах(е) обработки ПДн или использующее результаты их функционирования.

Процесс обработки персональных данных: Процесс, в котором присутствует обработка персональных данных.

Уничтожение персональных данных: Действия, в результате которых невозможно восстановить содержание ПДн в информационной системе ПДн или в результате которых уничтожаются материальные носители ПДн.

Целостность информации: Способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Используемые сокращения

В настоящем Порядке использованы следующие сокращения, приведенные в Таблице 1:

Таблица 1. Сокращения

№ п/п	Сокращение	Описание
1.	ИСПДн	Информационная система персональных данных
2.	ОС	Операционная система
3.	ПДн	Персональные данные
4.	СВТ	Средство вычислительной техники
5.	СЗПДн	Система защиты персональных данных

3. Область применения

Настоящий Порядок учета, хранения и уничтожения носителей ПДн (далее - Порядок) предназначен для определения единого порядка обращения с машинными (электронными) и бумажными носителями персональных данных в Администрации сельского поселения Красный

Яр муниципального района Красноярский Самарской области (далее - Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области).

4. Общие положения

Настоящий Порядок устанавливает порядок учета, хранения, использования и уничтожения носителей ПДн в процессах обработки ПДн.

Настоящий Порядок разработан в соответствии с документом «Положение об обеспечении безопасности персональных данных в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области .

5. Порядок работы с бумажными носителями

5.1. Порядок учета бумажных носителей, содержащих ПДн

Любой документ, содержащий ПДн, является конфиденциальным и подлежит обязательному учету. Учет документов, содержащих ПДн, осуществляется в соответствии с положениями настоящего Порядка.

Ответственность за организацию ведения учета документов возлагается на должностное лицо ответственное за организацию работ по обработке ПДн.

5.2.Порядок хранения бумажных носителей, содержащих ПДн

С целью обеспечения физической сохранности документов, содержащих ПДн, предотвращения хищения документов, а также с целью недопущения разглашения содержащихся в них сведений документы должны храниться в местах, исключающих доступ к ним посторонних лиц.

Хранение открытых документов вместе с конфиденциальными документами разрешено только в случаях, когда они являются приложениями к конфиденциальным документам.

Рабочее место работника Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области должно быть организовано таким образом, чтобы исключить возможность просмотра документов с ПДн лицами, которые не допущены к ПДн.

Во время работы на столе должны находиться только те документы, непосредственно с которыми ведется работа, все остальные должны быть убраны в места, предназначенные для хранения.

5.3.Порядок уничтожения бумажных носителей, содержащих ПДн

Основанием для уничтожения документов, содержащих ПДн, является достижение целей обработки.

Локальные документы, содержащие ПДн, уничтожаются по мере необходимости.

Ответственность за своевременное уничтожение документов возлагается на должностное лицо ответственное за организацию работ по обработке ПДн.

Уничтожение документов производится с помощью специальных бумагорезательных технических средств (шредеров) или сжиганием.

Уничтожение массивов документов

Массивы документов (архивы, библиотеки и т.п.) уничтожаются под контролем должностного лица ответственного за защиту ПДн.

Экспертиза документа проводится раз в год. Экспертиза охватывает все документы, содержащие ПДн, за соответствующий период времени.

Экспертиза проводится путем изучения содержания документов. Цель проведения экспертизы - определить возможность уничтожения документов либо дальнейшие сроки их хранения.

После проведения экспертизы составляется Акт о выделении дел и документов, подлежащих уничтожению (Приложение А). В Акт включаются отобранные дела для уничтожения, отдельные документы из дел и документы выделенного хранения.

Уничтожение массивов документов производится с помощью бумагорезательных технических средств или сжиганием.

Если уничтожение массивов документов производит третья сторона, с которой заключен соответствующий договор, то документы, выделенные для уничтожения, помещаются в короба, после чего короба запечатываются передаются третьей стороне.

После уничтожения массива документов должностными лицами ответственными за организацию работ по обработке ПД и за защиту ПДн, а также работниками производившими уничтожение документов подписывается Акт об уничтожении документов, содержащих ПДн (Приложение Б).

6. Порядок работы с машинными носителями

Учету подлежат следующие типы машинных носителей ПДн:

- отчуждаемые носители информации (внешние жесткие магнитные диски, гибкие магнитные диски, магнитные ленты, USB флеш-накопители, карты флеш-памяти, оптические носители (CD, DVD и прочее);

- неотчуждаемые носители информации (жесткие магнитные диски).

6.1. Порядок учета машинных носителей, содержащих ПДн

Все отчуждаемые машинные носители данных, используемые при работе со средствами вычислительной техники (далее - СВТ) для обработки и хранения ПДн, обязательно регистрируются и учитываются в **Журнале учета выдачи машинных носителей ПДн (Приложение В).**

Неотчуждаемые носители информации подлежат учету в составе системных блоков СВТ, которые в свою очередь учитываются в Техническом паспорте ИСПДн.

Ответственность за ведение Журнала учеты выдачи машинных носителей ПДн и контроль учета носителей ПДн возлагается на системного администратора Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области.

Каждому машинному носителю, содержащему ПДн, присваивается учетный номер согласно Журналу.

В качестве учетного номера допускается использование серийного (заводского) номера носителя. В случае отсутствия серийного номера, учетный номер наносится на носитель информации или его корпус. Если невозможно маркировать непосредственно машинный носитель данных, то маркируется упаковка, в которой хранится носитель. В этом случае учетный номер записывается также на носитель машинным способом.

6.2. Порядок использования машинных носителей ПДн

Машинные носители ПДн выдаются пользователям или другим лицам, участвующим в обработке ПДн, для работы под подпись в Журнале. По завершении работы машинные носители ПДн сдаются обратно.

В случае повреждения машинных носителей ПДн, работник, за которым закреплен носитель, сообщает о случившемся должностному лицу ответственному за защиту ПДн.

Передача носителя, содержащего ПДн, третьим сторонам производится в соответствии с требованиями договора между Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области и третьим лицом.

Машинные носители ПДн пересылаются в том же порядке, что и документы.

При фиксации ПДн на машинных носителях не допускается фиксация на одном машинном носителе ПДн, цели обработки которых заведомо не совместимы.

Вынос машинных носителей, содержащих ПДн, за пределы контролируемой зоны Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области запрещается без соответствующего разрешения должностного лица ответственного за защиту ПДн.

6.3. Порядок хранения машинных носителей ПДн

Хранение носителей, содержащих ПДн, осуществляется в условиях, исключающих возможность хищения, нарушения целостности или уничтожения содержащейся на них информации.

Отчуждаемые съемные носители после окончания работы с ними должны убираться в сейфы или металлические шкафы, запираемые на ключ.

Не допускается оставлять без присмотра на рабочем столе или в СВТ машинные носители, содержащие ПДн.

Персональную ответственность за сохранность полученных машинных носителей и предотвращение несанкционированного доступа к записанным на них ПДн несет работник, за которым закреплен носитель.

6.4. Порядок уничтожения машинных носителей ПДн

Основанием для уничтожения машинных носителей ПДн, является повреждение машинного носителя, исключающее его дальнейшее использование, или потеря практической ценности носителя. Решение об уничтожении машинного носителя принимает должностное лицо ответственное за защиту ПДн.

Списанные машинные носители, подлежащие уничтожению, хранятся в сейфе должностного лица ответственного за защиту ПДн. Уничтожение таких носителей производится раз в год.

Уничтожение носителей производится путем их физического разрушения с предварительным затиранием (форматированием, уничтожением) содержащихся на них ПДн, если это позволяют физические принципы работы носителя.

Уничтожение машинных носителей производится Комиссией в составе не менее 3 человек. В состав Комиссии должно обязательно входить должностное лицо ответственное за защиту ПДн. После уничтожения всех машинных носителей составляется **Акт об уничтожении персональных данных (Приложение Г).**

При уничтожении, машинные носители снимаются с учета. Отметка об уничтожении носителей проставляется в Журнале.

6.5. Порядок уничтожения (стирания) ПДн с машинного носителя

Основанием для уничтожения (стирания) записей или части записей с электронного носителя являются следующие случаи:

- возврат носителя сотрудником;
- передача носителя в ремонт;
- списание носителя.

Хранящаяся на электронных носителях и потерявшая актуальность информация, содержащая ПДн, своевременно стирается (уничтожается). Работник, совместно с системным администратором Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, принимает окончательное решение о необходимости уничтожения (стирания) с него записей.

Работник осуществляет уничтожение информации с носителя самостоятельно, с использованием встроенных средств ОС.

При невозможности самостоятельного уничтожения информации с носителя, работник передает электронный носитель должностному лицу ответственному за защиту ПДн. Совместно с носителем передается служебная записка, в которой указывается причины передачи (возврата) и основание для уничтожения содержащейся на нем информации.

Должностное лицо ответственное за защиту ПДн, ответственное за уничтожение (стирание) информации с электронных носителей, при получении носителя должно обеспечить уничтожение (стирание) информации с носителя, способом, исключающим ее дальнейшее восстановление и подготовить **Акт об уничтожении персональных данных (Приложение Г).**

В Акт заносится дата, учетный номер носителя и способ уничтожения (стирания) информации, а также используемые для этого программные средства.

Носители, пригодные к повторной эксплуатации, после уничтожения записанной на них информации могут быть использованы для повторной записи информации.

7. Пересмотр и внесение изменений

Пересмотр положений настоящего документа проводится в следующих случаях:

- при появлении новых требований к обработке и обеспечению безопасности ПДн со стороны законодательства РФ и контролирующих органов исполнительной власти Российской Федерации;
- по результатам внутреннего контроля (аудита) системы защиты ПДн, в случае выявления существенных нарушений;
- по результатам расследования инцидентов информационной безопасности, связанных с обработкой и обеспечением безопасности ПДн;
- не реже одного раза в год.

Ответственным за пересмотр настоящего Порядка и составление рекомендаций по изменению является должностное лицо ответственное за защиту ПДн.

Внесение изменений производится на основании соответствующего распоряжения Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области.

_____

Приложение № 1
к порядок учета, хранения и уничтожения
носителей персональных данных
УТВЕРЖДЕН
Распоряжением Главы сельского поселения Красный Яр
муниципального района Красноярский Самарской области от г №

Приложение А

А К Т № _____
о выделении дел и документов, подлежащих уничтожению
от «_____»_____201_ г.

Комиссия в составе:
<Фамилия И.О. – должность;>
<Фамилия И.О. – должность.>
<Фамилия И.О. – должность.>
составила настоящий акт о том, что на основании проведенной экспертизы, отобрала к уничтожению, следующие документы и дела, утратившие практическую ценность:

№ п\п Заголовок документа\дела Основание для уничтожения

Члены комиссии:

_____ _____
_____ _____
_____ _____

Приложение Б

А К Т № _____
уничтожения бумажных носителей, содержащих
персональные данные
от «_____»_____20__ г.

Комиссия в составе:
<Фамилия И.О. – должность;>
<Фамилия И.О. – должность.>
<Фамилия И.О. – должность.>
составила настоящий акт о том, что произведено плановое уничтожение бумажных носителей, содержащих персональные данные, с истекшим сроком использования и/или утративших практическое значение.
«тип носителя, учётный номер носителя»
«тип носителя, учётный номер носителя»
Бумажные носители уничтожены путём сжигания/шредирования/химической обработки и т.п. *(нужное отметить)*.
Члены комиссии

_____ _____
_____ _____
_____ _____

Приложение В

Журнал учета носителей информации, содержащих персональные данные

№ п/п	Учетный № носителя	Дата	Тип носителя	Содержимое носителя	Ф.И.О. отв. лица	Подпись отв. лица	Отметка о возврате (с указанием причины)	Ф.И.О. отв. лица	Подпись отв. лица	ата уничтожения носителя	Ф.И.О. отв. за уничтожение
1	2	3	4	5	6	7	8	9	10	11	12

Приложение Г
УТВЕРЖДАЮ
_____
_____
(подпись)
«__» _____ 20__г.

Акт об уничтожении персональных данных

Комиссия в составе:
Председатель – _____
Члены комиссии – _____
провела отбор носителей персональных данных и установила, что в соответствии с требованиями руководящих документов по защите информации
_____ информация, записанная на них в процессе эксплуатации, подлежит гарантированному уничтожению:

№ п/п Дата Тип носителя Регистрационный номер носителя ПДн Примечание

Всего съемных носителей _____
(цифрами и прописью)
На указанных носителях персональные данные уничтожены путем
_____.
(стирания на устройстве гарантированного уничтожения информации и т.п.)
Перечисленные носители ПДн уничтожены путем
_____.
(разрезания, сжигания, механического уничтожения и т.п.)
Председатель комиссии: _____ /_____/
Члены комиссии: _____ /_____/
_____ /_____/

Приложение № 14

УТВЕРЖДЕН
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

ПОРЯДОК РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АДМИНИСТРАЦИИ СЕЛЬСКОГО ПОСЕЛЕНИЯ КРАСНЫЙ ЯР МУНИЦИПАЛЬНОГО РАЙОНА КРАСНОЯРСКИЙ САМАРСКОЙ ОБЛАСТИ

1. Термины и определения

В настоящем Порядке использованы следующие термины и определения:

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.

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

Вредоносное программное обеспечение: Программное обеспечение, предназначенное для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ к информации: Возможность получения информации и ее использования.

Защита информации: Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

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

Информационная система персональных данных: Информационная система, представляющая собой совокупность ПДн, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПДн с использованием средств автоматизации или без использования таковых средств**.**

Информация: Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления**.**

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

Конфиденциальность персональных данных: Обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта ПДн или наличия иного законного основания.

Несанкционированный доступ (несанкционированные действия): Доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами ПДн.

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 ПДн.

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

Пользователь персональных данных: Лицо, участвующее в процессах(е) обработки ПДн или использующее результаты их функционирования.

Процесс обработки персональных данных: Процесс, в котором присутствует обработка персональных данных.

Средство защиты информации: Техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Уничтожение персональных данных: Действия, в результате которых невозможно восстановить содержание ПДн в информационной системе ПДн или в результате которых уничтожаются материальные носители ПДн.

Целостность информации: Способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Доступность информации - Свойство информационной безопасности, состоящее в том, что информационные активы предоставляются авторизованному пользователю, причем в виде и месте, необходимых пользователю, и в то время, когда они ему необходимы.

2. Используемые сокращения

В настоящем Порядке использованы следующие сокращения, приведенные в Таблице 1:

Таблица 1. Сокращения

№ п/п	Сокращение	Описание
1.	ИБ	Информационная безопасность
2.	ИСПДн	Информационная система ПДн
3.	НСД	Несанкционированный доступ
4.	ПДн	Персональные данные

3. Область применения

Настоящий Порядок реагирования на инциденты информационной безопасности (далее - Порядок) предназначен для определения единого порядка реагирования на возникшие инциденты информационной безопасности, проведения служебных расследований, а также проведения мероприятий, нацеленных на предотвращение наступления повторных инцидентов в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области (далее по тексту - Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области).

Требования настоящего Порядка распространяются на должностных лиц Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, отвечающие за обеспечение безопасности ПДн.

4. Общие положения

Настоящий Порядок разработан в соответствии с Политикой Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области в отношении обработки персональных данных, в порядке, установленном Федеральным законом от 27 июля 2006 года № 152-фз «О персональных данных».

В соответствии с настоящим Порядком к инцидентам ИБ в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области относятся:

- нарушение конфиденциальности, целостности или доступности ПДн;
- отказ оборудования, сервисов, средств обработки и (или), входящих в состав ИСПДн;
- несоблюдение требований внутренних организационно-распорядительных документов и действующих нормативных документов РФ в области обработки и защиты ПДн (нарушение правил обработки ПДн);
- заражение программных компонентов ИСПДн вредоносным программным обеспечением.

К инцидентам ИБ в ИСПДн также относятся попытки и факты получения НСД к ИСПДн:

- сеансы работы в ИСПДн незарегистрированных пользователей;
- сеансы работы Пользователей ИСПДн, срок действия полномочий, которых истек, либо в состав полномочий, которых не входят выявленные действия с ПДн;
- действия третьего лица, пытающегося получить доступ (или получившего доступ) с использованием учетной записи другого пользователя в целях получения коммерческой или другой выгоды, методом подбора пароля или иными методами (случайного разглашения пароля и т.п.) без ведома владельца учетной записи.
- совершение попыток несанкционированного доступа к рабочей станции, сейфу, шкафу и др. (нарушение целостности пломб, наклеек с защитной и идентификационной информацией, нарушение или несоответствие номеров печатей и др.);
- несанкционированное внесение изменений в параметры конфигурации программных или аппаратных средств обработки, или защиты, входящих в состав ИСПДн.

Кроме того, к инцидентам ИБ относятся случаи создания предпосылок для возникновения описанных выше инцидентов.

5. Оповещение об инциденте информационной безопасности

В случае выявления инцидента ИБ устанавливается следующая последовательность действий сотрудников Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области :

прекратить работу с ресурсом, в котором выявлен инцидент ИБ;

оповестить своего непосредственного Главы о факте выявления инцидента ИБ;

Глава должен оповестить должностное лицо ответственное за защиту информации и обеспечение безопасности ПДн;

после извещения указанных должностных лиц по их требованию предоставить всю необходимую информацию.

Должностное лицо ответственное за защиту информации и обеспечение безопасности ПДн проводит краткий анализ произошедшего инцидента ИБ и причин, способствующих его возникновению, и составляет краткую справку, в которой описывается произошедший инцидент ИБ, его последствия и оценка необходимости проведения расследования инцидента ИБ. Справка направляется Главе Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области для принятия решения о проведении расследования инцидента ИБ.

Порядок проведения расследования инцидента ИБ описан в разделе 7 настоящего документа.

Мероприятия по устранению причин и недопущению повторного возникновения инцидента ИБ описаны в разделе 8 настоящего документа.

Мероприятия при возникновении инцидента информационной безопасности, ставшего причиной возникновения негативных последствий для субъекта ПДн

В случае если инцидент ИБ может стать (или уже стал) причиной возникновения негативных последствий для субъектов ПДн, необходимо немедленно блокировать ПДн этих субъектов до устранения причин, повлекших за собой возникновение инцидента ИБ. Решение о блокировании ПДн принимает должностное лицо ответственное за защиту информации и обеспечение безопасности ПДн.

ПДн остаются заблокированными до устранения причин, повлекших за собой возникновение инцидента ИБ.

7. Проведение расследования инцидента информационной безопасности

Внутреннее расследование и составление заключений должно в обязательном порядке проводиться в случае выявления:

- нарушения конфиденциальности, целостности или доступности ПДн;
- халатности и несоблюдения требований по обеспечению безопасности ПДн;
- несоблюдения условий хранения носителей ПДн;
- использования СЗИ, которые могут привести к нарушению заданных характеристик безопасности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн.

Задачами внутреннего расследования являются:

- установление обстоятельств нарушения, в том числе времени, места и способа его совершения;
- установление лиц, непосредственно виновных в данном нарушении;
- выявление причин и условий, способствовавших нарушению.

Проведение внутреннего расследования проводится по решению Главы. С целью проведения расследования в обязательном порядке формируется Комиссия, в состав которой входят должностное лицо ответственное за защиту информации и обеспечение безопасности ПДн, юрист и иные должностные лица Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, участие которых может потребоваться.

Комиссия должна приступить к работе по расследованию не позднее следующего рабочего дня после даты выявления инцидента ИБ.

Общая продолжительность внутреннего расследования не должна превышать одного месяца.

В рамках проведения расследования инцидента ИБ Комиссия уполномочена:

- проводить опрос сотрудников Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области , по вине которых предположительно

произошел инцидент ИБ, а также должностных лиц, которые могут оказать содействие в установлении обстоятельств возникновения инцидента ИБ;

- проводить осмотр объектов и предметов, которые могут иметь отношение к инциденту ИБ;

По решению Глава Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области на Комиссию могут быть возложены дополнительные обязанности и права.

Работник, в отношении которого проводится расследование, должен быть ознакомлен с Распоряжением Главы сельского поселения Красный Яр муниципального района Красноярский Самарской области о проведении расследования.

Все действия членов Комиссии и полученные в ходе расследования материалы подлежат письменному оформлению (акты, протоколы, справки и т.п.).

Требование от работника объяснения в письменной форме для установления причины нарушения является обязательным. В случае, когда работник отказывается дать письменные объяснения, его устные показания или отказ от них письменно фиксируются членами Комиссии в виде протокола.

В целях исключения возможности какого-либо воздействия на процесс расследования члены Комиссии обязаны соблюдать конфиденциальность расследования до принятия по нему решения Главой сельского поселения Красный Яр муниципального района Красноярский Самарской области .

Для оперативного проведения внутреннего расследования должностное лицо ответственного за защиту ПДн составляет План проведения расследования.

Одновременно с проведением внутреннего расследования, Глава Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области может поручить Комиссии определить ущерб для Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области и (или) для субъекта ПДн от произошедшего инцидента ИБ. В отдельных случаях такая оценка может быть осуществлена с привлечением специализированной организации.

По окончании внутреннего расследования Комиссия представляет Главе Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области отчет по результатам расследования, в котором излагаются:

- основания и время проведения расследования;
- проделанная работа (кратко);
- время, место и обстоятельства факта нарушения;
- причины и условия совершения нарушения;
- виновные лица и степень их вины;
- наличие умысла в действиях виновных лиц;
- предложения по возмещению ущерба;
- предлагаемые меры наказания (учитывая личные и деловые качества виновных лиц) или дальнейшие действия;
- рекомендации по исключению подобных нарушений;
- другие вопросы, поставленные перед комиссией (об актуальности конфиденциальной информации, о размерах ущерба и т. д.).

К отчету прилагаются:

- письменные объяснения лиц, которых опрашивали члены Комиссии;
- акты (справки) проверок носителей конфиденциальной информации, осмотров помещений и т. д.;
- другие документы (копии документов), относящиеся к расследованию, в том числе заключения по определению размеров ущерба.

Отчет должен быть подписан всеми членами Комиссии. При несогласии с выводами или содержанием отдельных положений член Комиссии, подписывая заключение, приобщает к нему свое особое мнение (в письменном виде).

Отчет подлежит утверждению Главой сельского поселения Красный Яр муниципального района Красноярский Самарской области.

Работник, в отношении которого проводится расследование, или его уполномоченный представитель имеют право ознакомления с материалами расследования и требовать приобщения к материалам расследования представляемых ими документов и материалов.

Работник, в отношении которого проведено расследование, должен быть ознакомлен под подпись с отчётом по результатам расследования.

Решение о привлечении к ответственности работника принимается только после завершения расследования и оформляется распоряжением.

При наличии в действиях работника признаков административного правонарушения или уголовного преступления Глава Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области обязан обратиться в правоохранительные органы для привлечения виновного к ответственности, в соответствии с положениями нормативных документов РФ.

В соответствии с Трудовым кодексом РФ, возмещение ущерба производится независимо от привлечения работника к дисциплинарной, административной или уголовной ответственности за действия или бездействие, которыми причинен ущерб работодателю.

При несогласии работника с результатами подсчета ущерба взыскание должно производиться по решению суда. В этом случае заключение по результатам внутреннего расследования становится письменным обоснованием причастности работника к действиям, повлекшим нанесение ущерба.

Первый экземпляр отчета с резолюцией Главы Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, копия распоряжения (выписка) по результатам расследования, все материалы внутреннего расследования, включая документ (копию), послуживший поводом для назначения расследования, подлежат хранению в отдельном деле. Дела о внутренних расследованиях хранятся у Главы Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области.

8. Превентивные меры по недопущению повторного возникновения инцидентов информационной безопасности

Мероприятия по устранению инцидента ИБ и предупреждающие его повторное возникновение, в зависимости от произошедшего инцидента ИБ, включают в себя:

- мониторинг событий в информационной системе ПДн;
- своевременное удаление неиспользуемых учетных записей;
- контроль и мониторинг действий пользователей в информационной системе ПДн;
- проведение обучения (повторного обучения) пользователей правилам обработки и обеспечения безопасности ПДн;
- ознакомление пользователей с мерами ответственности, установленными нормативными документами РФ, за нарушение норм и правил обработки ПДн, а также за разглашение полученных данных.

9. Пересмотр и внесение изменений

Настоящий Порядок должен пересматриваться в случаях:

- изменения требований законодательства РФ, в области обработки и обеспечения информационной безопасности ПДн;
- по результатам внутреннего контроля (аудита) системы защиты ПДн, в случае выявления существенных нарушений;
- по результатам расследования инцидентов информационной безопасности, связанных с обработкой и обеспечением безопасности ПДн;

Ответственным за пересмотр настоящего Положения и составление рекомендаций по изменению является должностное лицо ответственное за защиту информации и обеспечение безопасности ПДн в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области.

Внесение изменений производится на основании соответствующего распоряжения Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области.

Приложение № 15

УТВЕРЖДЕНА
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

ИНСТРУКЦИЯ ДОЛЖНОСТНОГО ЛИЦА, ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

1.1. Настоящий документ определяет основные обязанности, права и ответственность лица, ответственного за организацию обработки персональных данных в информационных системах персональных данных Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области (далее - ИСПДн).

1.2. Ответственный за организацию обработки персональных данных назначается из числа штатных пользователей ИСПДн, на основании распоряжения Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области «О назначении ответственного за организацию обработки персональных данных в ИСПДн».

1.3. Ответственный за организацию обработки персональных данных в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами ФСТЭК России и регламентирующими документами ИСПДн.

1.4. Ответственный за организацию обработки персональных данных является должностным лицом, уполномоченным на проведение работ по организации обработки персональных данных в ИСПДн.

2. Обязанности должностного лица, ответственного за организацию обработки персональных данных в ИСПДн

Должностное лицо ответственное за организацию работ по обработке персональных данных обязано:

- взаимодействовать с регулирующими органами по вопросам обработки и обеспечения безопасности персональных данных;
- передавать ответственному за защиту информации ИСПДн информацию по взаимодействию с регулирующими органами в рамках его компетенции;
- контролировать договоры с третьими лицами на предмет их соответствия требованиям организационно-распорядительных документов по обработке и обеспечению безопасности персональных данных, в том числе в соответствии с п. 3 статьи 18 Закона о ПД;
- предоставлять необходимую информацию при проведении проверок регулирующими органами и при проведении контрольных мероприятий по обеспечению безопасности персональных данных;
- обеспечивать выполнение требований по обработке и обеспечению безопасности персональных данных в соответствии с «Положением о порядке обработки персональных данных в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области и иными нормативными документами в области обработки и защиты персональных данных;
- осуществлять непрерывный контроль действий, пользователей при обработке персональных данных, разъяснять и требовать от пользователей выполнения требований нормативных документов в области обработки и защиты персональных данных;
- участвовать в процессе разработки организационно-распорядительных документов, регламентирующих требования по обеспечению информационной безопасности персональных данных, обрабатываемых в ИСПДн;
- определять необходимость и направлять на обучение пользователей ИСПДн;
- предоставлять консультации пользователей ИСПДн по вопросам автоматизированной и неавтоматизированной обработки персональных данных в рамках своих компетенций;
- организовывать и контролировать своевременное предоставление пользователями ИСПДн доступа к персональным данным и средствам их обработки в объеме, необходимом для выполнения ими своих трудовых обязанностей;

- определять права доступа к персональным данным и автоматизированным средствам обработки персональных данных в рамках своих компетенций;
- сообщать о выявленных нарушениях требований по обработке персональных данных должностному лицу, ответственному за защиту информации;
- обеспечивать выполнение плана периодических проверок условий обработки персональных данных в пределах своих функциональных обязанностей;
- участвовать в разработке плана периодических проверок условий обработки персональных данных.

3. Права должностного лица, ответственного за организацию обработки персональных данных в ИСПДн

Должностное лицо, ответственное за организацию работ по обработке персональных данных, имеет право:
- формировать предложения по совершенствованию системы защиты информации для должностного лица, ответственного за защиту информации, обрабатываемой в ИСПДн;
- формировать предложения о необходимости проведения контрольных мероприятий по обеспечению безопасности персональных данных для должностного лица, ответственного за защиту информации;
- формировать предложения по внесению изменений в организационно-распорядительные документы, регламентирующие требования по обеспечению информационной безопасности персональных данных, обрабатываемых в ИСПДн;
- организовывать проведение периодических проверок условий обработки персональных данных;
- осуществлять ознакомление служащих, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), локальными актами по вопросам обработки персональных данных;
- в случаях, установленных нормативными правовыми актами Российской Федерации, в соответствии с требованиями и методами, установленными уполномоченным органом по защите прав субъектов персональных данных, осуществлять обезличивание персональных данных, обрабатываемых в ИСПДн.

4. Нештатные ситуации

В случае возникновения нештатных ситуаций ответственный за организацию обработки персональных данных обязан незамедлительно принять все необходимые меры по устранению причины возникновения нештатной ситуации для минимизации ее последствий.
В случае возникновения нештатных ситуаций ответственный за организацию обработки персональных данных обязан немедленно оповестить руководство о нештатной ситуации.
В случае возникновения нештатных ситуаций ответственный руководствуется Инструкцией по порядку резервирования и восстановления работоспособности технических (аппаратных) средств, программного обеспечения, баз данных и средств защиты информации в ИСПДн.

5. Ответственность

На лицо, ответственное за организацию обработки персональных данных, возлагается персональная ответственность за организацию обработки персональных данных в ИСПДн в соответствии с функциональными обязанностями.

Лицо, ответственное за организацию обработки персональных данных, несет ответственность по действующему законодательству за разглашение информации ограниченного доступа, ставшей известной ему по роду работы.

Приложение № 16

УТВЕРЖДЕНА
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В АДМИНИСТРАЦИИ СЕЛЬСКОГО ПОСЕЛЕНИЯ КРАСНЫЙ ЯР МУНИЦИПАЛЬНОГО РАЙОНА КРАСНОЯРСКИЙ САМАРСКОЙ ОБЛАСТИ

Сокращения

Сокращение	Расшифровка
АРМ	автоматизированное рабочее место
ИСПДн	информационная система персональных данных
ПДн	персональные данные

1. Общие положения

1.1. Пользователь ИСПДн (далее – Пользователь) осуществляет обработку ПДн в ИСПДн, используемых в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области .

1.2. Пользователем является каждый сотрудник Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.3. Пользователь несет персональную ответственность согласно действующему законодательству Российской Федерации за свои действия и за разглашение сведений ограниченного распространения, ставших известными ему по роду работы.

1.4. Пользователь в своей работе руководствуется настоящей Инструкцией, Положением об обработке и защите ПДн, руководящими и нормативными документами ФСТЭК России и ФСБ России и регламентирующими документами Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области.

1.5. Методическое руководство работой пользователя осуществляется ответственным за обеспечение безопасности ПДн.

2. Должностные обязанности

Пользователь **обязан**:

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

2.2. Выполнять на АРМ только те процедуры, которые определены для него Положением о разрешительной системе допуска пользователей и обслуживающего персонала к информационным ресурсам и системе защиты персональных данных.

2.3. Знать и соблюдать установленные требования по режиму обработки ПДн, учету, хранению и пересылке носителей информации, защите ПДн, а также руководящих и организационно-распорядительных документов.

2.4. Соблюдать требования парольной политики (раздел 3).

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

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

2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, а так же для получений консультаций по вопросам информационной безопасности, необходимо обращаться к системному администратору Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области

2.8. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к системному администратору Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области.

2.9. Пользователям **запрещается**:

- - разглашать защищаемую информацию третьим лицам;
- - копировать защищаемую информацию на внешние носители без разрешения Ответственного за организацию обработки ПДн;
- - самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;
- - несанкционированно открывать общий доступ к папкам на своем АРМ;
- - 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 ИСПДн;
- - сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн;
- привлекать посторонних лиц для производства ремонта или настройки АРМ.

2.10. При отсутствии визуального контроля за АРМ доступ к нему должен быть немедленно заблокирован.

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

3. Организация парольной защиты

3.1 Личные пароли доступа к элементам ИСПДн выдаются Пользователям системным администратором Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области (Администратором ИСПДн).

3.2. Полная плановая смена паролей в ИСПДн проводится системным администратором Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области (администраторами ИСПДн).

3.3. Правила ввода пароля:

- ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан;
- во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

3.4. Правила хранение пароля:

- запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;
- запрещается сообщать другим Пользователям личный пароль и регистрировать их в системе под своим паролем.

3.5. Лица, использующие паролирование, **обязаны**:

- четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов по паролированию;
- своевременно сообщать администратору ИСПДн об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

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

4.1. Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее - Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.

4.2. При работе в Сети **запрещается**:

- осуществлять работу при отключенных средствах защиты (антивирус и др.);
- передавать по Сети защищаемую информацию без использования средств шифрования;
- посещать Интернет-ресурсы, содержащие информацию экстремистского, расистского, порнографического и криминального характера, а также загружать данные, содержащие подобную информацию;
- использовать адрес корпоративной почты при регистрации на Интернет-ресурсах, в ходе деятельности, не связанной с выполнением должностных обязанностей;

- скачивать из Сети медиа-файлы развлекательного характера, программное обеспечение и другие файлы;
- размещать в сети Интернет информацию, классифицированную как «для служебного пользования», «персональные данные», «коммерческая тайна»;

4.3. Ответственный за организацию обработки ПДн оставляет **за собой право**:

- осуществлять мониторинг использования сотрудниками Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области сети Интернет;
- определять перечень запрещенных Интернет-ресурсов и осуществлять блокировку доступа к ним;
- осуществлять мониторинг появления адресов корпоративной почты на страницах Интернет-ресурсов;
- осуществлять мониторинг появления информации конфиденциального характера о деятельности Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области в сети Интернет, в том числе и на страницах социальных сетей, таких как www.vk.com, www.odnoklassniki.ru и др;
- предоставлять информацию об использовании Интернет-ресурсов сотрудниками Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области правоохранительным органам в случаях, предусмотренных законодательством Российской Федерации;
- принимать меры дисциплинарного характера к сотрудникам, нарушающим положения настоящей инструкции.

5. Правила работы с корпоративной электронной почтой

5.1 Электронная почта является собственностью Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области и может быть использована **ТОЛЬКО** в служебных целях. Использование электронной почты в других целях категорически **ЗАПРЕЩЕНО**.

5.2 Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления по требованию Главы сельского поселения Красный Яр муниципального района Красноярский Самарской области .

5.3 При работе с корпоративной системой электронной почты сотрудникам **запрещается**:

- - использовать адрес корпоративной почты для оформления подписок, без предварительного согласования с Главой сельского поселения Красный Яр муниципального района Красноярский Самарской области;
- - публиковать свой адрес, либо адреса других сотрудников компании на общедоступных Интернет ресурсах (форумы, конференции и т.п.);
- - отправлять сообщения с вложенными файлами общий объем которых превышает 15 Мегабайт.
- - открывать вложенные файлы во входящих сообщениях без предварительной проверки антивирусными средствами, даже если отправитель письма хорошо известен;
- - осуществлять массовую рассылку почтовых сообщений внешним адресатам без их на то согласия. Данные действия квалифицируются как СПАМ и являются незаконными;
- - осуществлять массовую рассылку почтовых сообщений рекламного характера;
- рассылка через электронную почту материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете, а также ссылки на вышеуказанную информацию;
- - распространение защищаемых авторскими правами материалов, затрагивающих какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны.
- - распространять информацию содержание и направленность которой запрещены международным и Российским законодательством включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению

противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.

- - распространять информацию ограниченного доступа, представляющую коммерческую или государственную тайну;
- - предоставлять, кому быто ни было пароль доступа к своему почтовому ящику.

6.Порядок действия пользователя при возникновении инцидента информационной безопасности

- При выходе из строя СЗИ необходимо:
- - немедленно прекратить обработку информации на объекте;
- - обратиться к администратору информационной безопасности.
- При выходе из строя составных частей ИСПДн:
- - немедленно прекратить обработку информации на объекте;
- - обратиться к администратору информационной безопасности.

7.Ответственность пользователя

На пользователя возлагается персональная ответственность за соблюдение установленного режима защиты информации ограниченного распространения в соответствии с его функциональными обязанностями, определенными настоящей Инструкцией.

Пользователь несет ответственность в соответствии с действующим законодательством РФ за нарушение требований настоящей Инструкции.

Приложение № 17
УТВЕРЖДЕНА
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

ИНСТРУКЦИЯ ОТВЕТСТВЕННОГО ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения.

1.1. Настоящая инструкция разработана на основании постановления Правительства Российской Федерации от 21 марта 2012г. № 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», постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», «Положением об организации и проведении работ по обеспечению безопасности персональных данных при их автоматизированной обработке в информационных системах персональных данных и других нормативно-правовых актов регулирующих обработку персональных данных в автоматизированных системах.

1.2. Инструкция определяет функции, права и обязанности ответственного за обеспечение безопасности персональных данных в Администрации сельского поселения Красный Яр (далее — Администрация) по вопросам обеспечения информационной безопасности при обработке персональных данных.

1.3. Ответственный за обеспечение безопасности персональных данных назначается из числа сотрудников и обеспечивает правильность использования и нормальное функционирование установленных средств защиты информации (далее - СЗИ).

1.4. К СЗИ относятся средства защиты от несанкционированного доступа (далее - НСД), средства межсетевого экранирования, а также антивирусные средства.

1.5. К выполнению обязанностей в области организации разграничения доступа, настройке локальной вычислительной сети ответственный за обеспечение безопасности персональных данных может привлекать к работам сторонних сотрудников. Все работы должны согласовываться с Главой поселения и проводиться только в присутствии ответственного за обеспечение безопасности персональных данных при этом не должны затрагиваться средства защиты информации от несанкционированного доступа и обрабатываемые персональные данные.

1.6. К выполнению обязанностей в области сопровождения средств защиты информации от НСД и их настройки ответственный за обеспечение безопасности персональных данных выполняет только по согласованию с органом, проводившим аттестационные мероприятия.

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

2. Основные задачи и функции ответственного за обеспечение безопасности персональных данных.

2.1. Основными задачами ответственного за обеспечение безопасности персональных данных является:

2.1.1. Сопровождение средств защиты информации от несанкционированного доступа (далее - СЗИ от НСД) и основных технических средств и систем (далее - ОТСС);

2.1.2. Организация разграничения доступа;

2.1.3. Контроль эффективности защиты информации.

2.2. Для выполнения поставленных задач, на ответственного за обеспечение безопасности персональных данных возлагаются следующие функции:

2.2.1. Контроль за выполнением требований действующих нормативных документов по

вопросам обеспечения безопасности персональных данных, обрабатываемых в информационных системах персональных данных.

2.2.2. Настройка и организация сопровождения в процессе эксплуатации подсистемы управления доступом на рабочих станциях (далее - РС):

— опыт реализации полномочий доступа (чтение, запись, модификация, создание, удаление) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтерам);

— опыт ввода описаний пользователей ИСПДн в информационную базу, установленную на РС СЗИ от НСД;

— организация своевременного удаления описаний пользователей из базы данных СЗИ при изменении списка допущенных к работе на РС лиц.

2.2.3. Контроль доступа лиц в помещения, где расположены технические средства ИСПДн, в соответствии со списком сотрудников, допущенных к работе в ИСПДн.

2.2.4. Контроль проведения смены паролей для доступа к ИСПДн пользователями ИСПДн. Периодичность смены паролей – 90 дней.

2.2.5. Настройка и сопровождение подсистемы регистрации и учета действий пользователей при работе в ИСПДн:

— введение в базу данных, установленную на РС СЗИ от НСД описания событий, подлежащих регистрации в системном журнале;

— регулярное проведение анализа системного журнала для выявления попыток несанкционированного доступа к защищаемым ресурсам.

2.2.6. Сопровождение подсистемы обеспечения целостности информации в ИСПДн:

— организация периодического тестирования функций установленной на РС СЗИ от НСД, особенно при изменении программной среды и полномочий исполнителей;

— организация восстановления программной среды, программных средств и настроек СЗИ при сбоях;

— организация поддержания установленного порядка и правил антивирусной защиты информации на ПЭВМ;

— контроль за периодическим обновлением антивирусных средств (баз данных), установленных на РС, контроль соблюдения пользователями порядка и правил антивирусной защиты.

2.2.7. Контроль соблюдения требований по размещению и использованию ИСПДн, указанных в Техническом паспорте.

3. Права и обязанности администратора безопасности

3.1. Для реализации поставленных задач и возложенных функций, ответственный за обеспечение безопасности персональных данных ОБЯЗАН:

3.1.1. Сопровождать СЗИ от НСД и ОТСС:

— вести учет и знать перечень установленных в ИСПДн ОТСС, СЗИ от НСД и перечень задач, решаемых с их использованием.

— осуществлять непосредственное управление режимами работы и административную поддержку функционирования (настройку и сопровождение) применяемых на РС специальных программных и программно-аппаратных СЗИ от НСД.

— присутствовать при внесении изменений в конфигурацию (модификации) аппаратнопрограммных средств защищенных РС и серверов, осуществлять проверку работоспособности системы зашиты после установки (обновления) программных средств в ИСПДн.

— периодически проверять состояние используемых СЗИ от НСД, осуществлять проверку правильности их настройки (выборочное тестирование).

— контролировать соответствие технического паспорта объекта вычислительной техники (далее - СВТ) фактическому составу (комплектности) СВТ в ИСПДн и вести учет изменений аппаратно-программной конфигурации (архив заявок, на основании которых были произведены данные изменения в ИСПДн).

— вести учет нештатных ситуаций, выполнения профилактических работ, установки и модификации аппаратных и программных средств ИСПДн.

— проводить инструктаж (первичный, периодический, внеочередной) сотрудников больницы, допущенных к обработке персональных данных в ИСПДн по правилам работы с используемыми средствами и системами зашиты информации.

3.1.2. Организовывать разграничения доступа:

а) участвовать в разработке и знать перечень защищаемых информационных ресурсов ИСПДн.

б) разрабатывать совместно с администраторами ЛВС решения по:

— приписке пользователей с одинаковыми правами, статусом безопасности и характером решаемых задач к соответствующим группам;

— определению списка устройств, логических дисков, каталогов общего пользования на серверах, с указанием состава допущенных к ним пользователей и режимов допуска (матрица доступа);

- осуществлению контроля за наличием активных компьютеров сети, состоянием активных пользователей, использованием разделяемых ресурсов, процессом печати на общих принтерах;

— разработке порядка пользования электронной почтой (определение списка абонентов из состава пользователей сети, проектированию системы почтовых ящиков, использованию СЗИ при передаче закрытых документов);

— разработке порядка выхода пользователей в сети общего пользования (Internet) и использованию встроенных СЗИ от НСД в сервисных программах;

— определению режимов использования СЗИ от НСД: защита паролей, защита в протоколах передачи данных, кодирование файлов, в случае необходимости подключение дополнительных алгоритмов криптографической защиты и подтверждение подлинности электронных документов (электронная цифровая подпись);

— разработке политики аудита: определению состава регистрируемых событий и списка лиц, имеющих допуск к журналам аудита.

в) осуществлять учет и периодический контроль состава и полномочий пользователей различных РС в ИСПДн.

г) контролировать и требовать соблюдения установленных правил по организации парольной защиты в больнице.

д) контролировать обеспечение защиты информации, содержащей персональные данные при взаимодействии с информационными сетями общего пользования и требовать соблюдения установленных правил по использованию сетей общего пользования (Интернет) в больнице;

е) контролировать выполнение требований парольной защиты в больнице;

ж) осуществлять оперативный контроль работы пользователей защищенных РС, анализировать содержимое журналов событий операционных систем (далее - ОС), систем управления базами данных (далее - СУБД), пакетов прикладных программ и СЗИ от НСД всех РС и адекватно реагировать на возникающие нештатные ситуации. Обеспечивать своевременное архивирование журналов событий РС и надлежащий режим хранения данных архивов.

з) принимать участие в работах по внесению изменений в аппаратно-программную конфигурацию серверов и РС в ИСПДн.

и) обеспечивать строгое выполнение требований безопасности информации при организации технического обслуживания РС и отправке их в ремонт (контролировать стирание информации на магнитных носителях).

к) организовывать учет, хранение, прием и выдачу персональных идентификаторов ответственным исполнителям, осуществлять контроль правильности их использования. л) осуществлять периодический контроль порядка учета, создания, хранения и использования резервных и архивных копий массивов данных.

м) по указанию руководства своевременно и точно отражать изменения в организационнораспорядительных и нормативных документах по управлению СЗИ от НСД, установленных на РС в ИСПДн.

н) требовать от пользователей стирания остаточной информации на несъёмных носителях (жестких дисках) установленным порядком, а в оперативной памяти по окончании обработки информации путем перезагрузки РС.

б) докладывать гл. врачу больницы о выявленных угрозах безопасности информации

3.1.3. Контролировать эффективность защиты информации:

а) проводить работу по выявлению возможности вмешательства в процесс функционирования ИСПДн и осуществления НСД к информации и техническим средствам РС.

обрабатываемой в ИСПДн, об имевших место попытках НСД к информации и техническим средствам РС.

в) проводить занятия с пользователями ИСПДн по правилам работы на РС, оснащенных СЗИ от НСД, и по изучению руководящих документов по вопросам обеспечения безопасности информации с разбором недостатков, выявленных при контроле эффективности зашиты информации.

г) участвовать в расследовании причин совершения нарушений и возникновения серьезных кризисных ситуаций в АС.

3.2. Ответственному за обеспечение безопасности персональных данных запрещается:

3.2.1. Используя служебное положение, создавать ложные информационные сообщения и учетные записи пользователей в ИСПДн, получать доступ к персональным данным и предоставлять доступ другим лицам с целью ознакомления, модификации, копирования, уничтожения, блокирования доступа к информации;

3.2.2. Использовать ставшие доступными в ходе исполнения служебных обязанностей идентификационные данные пользователей (имя, пароль, ключи и т.п.) для маскирования своих действий;

3.2.4. Использовать в своих и в чьих-либо личных интересах ресурсы ИСПДн, а также предоставлять такую возможность другим лицам;

3.2.5. Выключать СЗИ от НСД, установленные в ИСПДн, без санкции гл. врача больницы;

3.2.6. Передавать третьим лицам тем или иным способом сетевые адреса, имена, пароли, информацию о привилегиях пользователей ИСПДн, конфигурационные настройки ИСПДн;

3.2.7. Производить в рабочее время действия, приводящие к сбою, остановке, замедлению работы ИСПДн, блокированию доступа, потере информации без санкции гл. врача больницы и предупреждения пользователей ИСПДн;

3.2.8. Нарушать правила эксплуатации оборудования ИСПДн;

3.2.9. Корректировать, удалять, подменять журналы аудита событий в ИСПДн.

4. Права и ответственность ответственного за обеспечение безопасности персональных данных

4.1. Ответственный за обеспечение безопасности персональных данных имеет право:

4.1.1. Получать доступ к программным и аппаратным средствам ИСПДн, средствам их защиты, а также просмотру прав доступа к ресурсам на серверах ИСПДн и РС пользователей;

4.1.2. Требовать от пользователей ИСПДн выполнения требований нормативно-методических документов в больнице по обеспечению безопасности и защите персональных данных.

4.1.3. Участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения безопасности персональных данных, НСД, утраты, порчи защищаемой информации, содержащей персональные данные и технических компонентов ИСПДн;

4.1.4. Осуществлять оперативное вмешательство в работу пользователя ИСПДн при явной угрозе безопасности персональным данным в результате несоблюдения установленной технологии обработки персональных данных и невыполнения требований по безопасности с последующим докладом ответственному за обеспечение безопасности персональных данных.

4.1.5. Производить анализ защищенности ИСПДн путем применения специального программного обеспечения, осуществления попыток взлома системы защиты ИСПДн. Такие работы должны проводиться в часы наименьшей информационной нагрузки с обязательным уведомлением гл. врача больницы.

4.1.6. Вносить свои предложения по совершенствованию мер защиты в ИСПДн.

4.2. Ответственный за обеспечение безопасности защиты персональных данных несет ответственность за:

4.2.1. Реализацию принятых в ИСПДн мероприятий по защите персональных данных;

4.2.2. Программно — технические средства защиты информации, технические средства вычислительной техники ИСПДн, закрепленные за ним, а также за качество проводимых им работ по обеспечению защиты персональных данных в соответствии с функциональными обязанностями.

4.2.3.За несоблюдение требований по защите персональных данных ответственный за обеспечение безопасности персональных данных несет ответственность в соответствии с законодательством Российской Федерации

Приложение № 18

УТВЕРЖДЕНА
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

ИНСТРУКЦИЯ ПО УЧЁТУ ЛИЦ, ДОПУЩЕННЫХ К РАБОТЕ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Настоящая инструкция разработана в соответствии с требованиями подпункта «ж» пункта 12 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781. Инструкция определяет порядок учета лиц, допущенных к работе с персональными данными в информационных системах, а также в соответствии с требованиями по ведению «Журнала учета лиц, допущенных к работе с персональными данными в информационных системах». Основанием для допуска сотрудника к работе с персональными данными является включение его в список допущенных лиц к обработке персональных данных. Включение в список лиц, допущенных к работе с персональными данными, осуществляется распоряжением Главы сельского поселения Красный Яр муниципального района Красноярский Самарской области .

2. При допуске к работе с персональными данными (далее - ПДн) определяется перечень информационных систем персональных данных, к работе в которых допущен специалист, а также перечень обрабатываемых им персональных данных и разрешенный вид процедур обработки ПДн.

3. Основанием для прекращения допуска сотрудника к работе с персональными данными или внесение изменений в его обязанности по работе в информационных системах персональных данных, внесении изменений в перечень обрабатываемых ПДн и в перечень процедур обработки ПДн является распоряжение Главы Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области .

4. В Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области ведется журнал учета лиц, допущенных к персональным данным.

Приложение № 19

УТВЕРЖДЕНА
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

ИНСТРУКЦИЯ ПО ПРОВЕДЕНИЮ ИНСТРУКТАЖА ЛИЦ, ДОПУЩЕННЫХ К РАБОТЕ С ИНФОРМАЦИОННОЙ СИСТЕМОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Настоящая инструкция разработана с целью обеспечения безопасности персональных данных, обрабатываемых в информационных системах персональных данных Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области .

2. При поступлении на работу сотрудника, которому для выполнения своих трудовых обязанностей необходим доступ к ИСПДн (далее - новый сотрудник), ответственный за организацию обработки персональных данных:

а) в соответствии с п.6 ч.1 ст.18.1 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных» проводит ознакомление нового сотрудника с положениями законодательства Российской Федерации о персональных данных и локальными актами организации в отношении обработки персональных данных, перечисленными в Приложении № 1 к данной инструкции;

б) знакомит нового сотрудника с ответственностью за неисполнение требований по обеспечению безопасности персональных данных в ИСПДн, предусмотренной действующим законодательством Российской Федерации;

в) отмечает в Журнале учета прохождения первичного инструктажа данные о проведении инструктажа.

Новый сотрудник может приступить к исполнению своих непосредственных трудовых обязанностей, связанных с обработкой персональных данных, только после успешного прохождения первичного инструктажа.

приложение к инструкции
по проведению инструктажа лиц,
допущенных к работе с ИСПД

Перечень законодательных актов Российской Федерации о персональных данных, документов, определяющих требования к защите персональных данных, внутренних локальных актов, определяющих политику организации в отношении обработки персональных данных, с которыми необходимо ознакомить нового сотрудника при проведении первичного инструктажа

Законодательные акты Российской Федерации о персональных данных:

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ);
- 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 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства Российской Федерации от 21.03.2012 № 211 «Перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствие с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

- Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (для сотрудников, обрабатывающих персональные данные в том числе без использования средств автоматизации).

Внутренние локальные акты Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области:

- Политика Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области в отношении обработки персональных данных в порядке, установленном Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных».
- Положение об обеспечении безопасности персональных данных в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области .
- Правила работы с обезличенными персональными данными в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области .
- Перечень персональных данных, обрабатываемых в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области в связи с реализацией трудовых отношений.
- Перечень должностей в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных.
- Перечень должностей в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным.
- Форма обязательства о неразглашении информации, содержащей персональные данные в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области.
- Типовая форма согласия на обработку персональных данных в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области .
- Порядок доступа в помещения, в которых ведётся обработка персональных данных, в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области.
- Правила рассмотрения запросов субъектов персональных данных или их представителей в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области.
- Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.
- Инструкция по организации антивирусной защиты в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области.
- Порядок учета, хранения и уничтожения носителей персональных данных в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области.
- Порядок реагирования на инциденты информационной безопасности в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области.
- Инструкция должностного лица, ответственного за организацию обработки персональных данных в информационных системах персональных данных.
- Инструкция пользователя информационной системы персональных данных в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области.
- Границы контролируемой зоны информационных систем персональных данных Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области.

Приложение № 20

УТВЕРЖДЕН
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

ПОРЯДОК (ИНСТРУКЦИЯ) РЕЗЕРВНОГО КОПИРОВАНИЯ И ВОССТАНОВЛЕНИЯ ДАННЫХ

Общие положения.

Настоящий документ определяет порядок осуществления резервного копирования информационных ресурсов информационных систем персональных данных (ИСПДн) Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области (далее – объект автоматизации).

Процесс резервного копирования обеспечивает сохранение информации, с целью ее восстановления при потере или порче на основном носителе, и является ключевым элементом защиты от умышленной и неумышленной потери данных.

Конкретные информационные ресурсы, подлежащие резервному копированию, порядок их копирования приводится в «Перечне ресурсов, подлежащих резервному копированию» (далее – Перечень), являющимся приложением к настоящему документу.

Перечень составляется ответственным за обеспечение безопасности защиты персональных данных объекта автоматизации в соответствии с положениями данного документа.

Перечень должен содержать перечень информационных ресурсов, подлежащих резервному копированию, составленный ответственным за обеспечение безопасности защиты персональных данных и согласованный с Главой сельского поселения Красный Яр муниципального района Красноярский Самарской области .

Форма Перечня представлена в Приложении 1.

Резервное копирование осуществляется ответственным за обеспечение безопасности защиты персональных данных (системным администратором) и контролируется Главой.

Должностные лица объекта автоматизации, задействованные в осуществлении резервного копирования информационных ресурсов ИСПДн объекта автоматизации, знакомятся с основными положениями и приложениями данного порядка в части, их касающейся, по мере необходимости.

Способ резервного копирования определяются из возможностей, имеющихся на объекте автоматизации. Конкретный способ создания резервных копий определяется ответственным за обеспечение безопасности защиты персональных данных.

Способ резервного копирования.

Для проведения резервного копирования информации могут использоваться следующие способы и средства:

создание резервных копий баз данных и копирование их на носители информации (внешний жесткий диск, CD-R\DVD-R диски);

создание резервных копий баз данных и копирование их на сетевые хранилища (файловые сервера, ленточные библиотеки);

создание резервных копий встроенными средствами СУБД;

создание резервных копий встроенными средствами операционной системы;

создание резервных копий встроенными средствами программных изделий;

создание резервных копий специализированным программным обеспечением (например, Acronis True Image). Должно использоваться только лицензионное программное обеспечение.

Периодичность и схема резервного копирования.

При осуществлении резервного копирования используется один тип копирования: полное резервное копирование.

Полное резервное копирование информационных ресурсов выполняется ежемесячно (архив хранится в течение 1 года).

Порядок резервного копирования

Ответственный за обеспечение безопасности защиты персональных данных производит резервное копирование вручную и/или настраивает задания для ПО, осуществляющего резервное копирование, на автоматическое выполнение в соответствии с перечнем информационных ресурсов, подлежащих резервному копированию, и графиком резервного копирования.

Перед выполнением задания резервного копирования ответственный за обеспечение безопасности защиты персональных данных проверяет доступность резервного носителя, а также наличие на нем свободного места для записи данных.

После завершения выполнения задачи резервного копирования ответственный за обеспечение безопасности защиты персональных данных должен извлечь резервный носитель (если используется съемный носитель), подписать его по формату «число, месяц, год, уровень №» и поместить в сейф (запираемый шкаф, ящик).

При создании резервных копий на сетевые хранилища – доступ к сетевым хранилищам должен быть ограничен. Доступ должны иметь только ответственный за обеспечение безопасности защиты персональных данных производит учет проведения полного резервного копирования данных в «Журнал учета проведения полного резервного копирования».

Инкрементальное копирование должно осуществляться в соответствии с данным порядком, но без регистрации в «Журнале учета проведения резервного копирования». Регистрация может осуществляться в журналах программного обеспечения, с помощью которого производится резервное копирование данных.

Хранение резервных копий

Хранение резервных копий (если используется съемный носитель) должно быть организовано в отдельном от копируемых информационных ресурсов помещении.

Доступ к хранилищу резервных копий должны иметь только ответственный за обеспечение безопасности защиты персональных данных.

Восстановление после сбоя

В случае потери данных, необходимо подготовить данные последнего произведенного резервного копирования.

В зависимости от характера и уровня повреждения информационных ресурсов АИБ ИСПДн восстанавливает либо весь массив резервных данных, либо отдельные поврежденные или уничтоженные файлы и папки. Все действия по восстановлению персональных данных должны быть учтены в «Журнале восстановления конфиденциальной информации».

Порядок пересмотра документа

Документ подлежит полному пересмотру при изменении перечня решаемых задач, состава технических и программных средств ИСПДн объекта автоматизации, приводящих к существенным изменениям технологии обработки информации.

Документ подлежит частичному пересмотру в остальных случаях. Частичный пересмотр проводится ответственным за обеспечение безопасности и обработку ПДн объекта автоматизации.

Полный плановый пересмотр данного документа проводится регулярно, с целью проверки соответствия положений данного документа реальным условиям применения их в ИСПДн объекта автоматизации.

Частичный пересмотр данного документа проводится по письменному предложению АИБ ИСПДн. Форма листа регистрации изменений в данном порядке представлена в Приложении 2.

Вносимые изменения не должны противоречить другим положениям данного документа.

Ответственные за выполнение порядка

Ответственность за соблюдение периодичности и порядка выполнения резервного копирования, за выполнение резервного копирования и восстановление данных из резервных копий, за сохранность резервных копий возлагается на ответственного за обеспечение безопасности защиты персональных данных.

Ответственным за постоянный контроль выполнения требований данного документа является Глава.

Приложение 1 –
Перечень ресурсов, подлежащих резервному копированию

Перечень ресурсов, подлежащих резервному копированию

Наименование ИСПДн	Тип резервного носителя	Средства копирования	Периодичность резервного копирования	Место хранения копии
1С				
УРМ				
Контур				

Приложение 2 –
Лист регистрации изменений

Лист регистрации изменений

№ п/п	Внесенное изменение	Основание (наименование, номер и дата документа)	Лицо, внесшее изменения		Дата внесения изменения
			Фамилия, инициалы	Подпись	

Приложение № 21

УТВЕРЖДЕНА
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

ИНСТРУКЦИЯ ПО ДЕЙСТВИЯМ ПЕРСОНАЛА ВО ВНЕШТАТНЫХ СИТУАЦИЯХ ПРИ ОБРАБОТКЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ И ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

Данная инструкция призвана регламентировать порядок действий пользователя информационной системы персональных данных Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области (далее - ИСПДн), при возникновении внештатных ситуаций.

Инструкция утверждается Главой сельского поселения Красный Яр муниципального района Красноярский Самарской области. Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием ИСПДн Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций.

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

Задачей данной Инструкции является определение мер защиты от прерывания и определение действий восстановления в случае прерывания.

Действие настоящей Инструкции распространяется на всех сотрудников Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области , 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.

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

2. Порядок действий при возникновении аварийной ситуации

В настоящем документе под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн.

Все действия в процессе реагирования на аварийные ситуации должны документироваться ответственным за реагирование сотрудником в «Журнал учета нештатных ситуаций, фактов вскрытия и опечатывания ПЭВМ, выполнения профилактических работ, установки и модификации аппаратных и программных средств информационной системы персональных данных».В кратчайшие сроки, не превышающие одного рабочего дня, ответственный за обеспечение информационной безопасности, администратор баз данных или другой назначенный ответственным за реагирование сотрудник предпринимает меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. При необходимости привлекаются квалифицированные сотрудники сторонних организаций с целью восстановления работоспособности в кратчайшие сроки.

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;
- других физических повреждений элементов ИСПДн, критичных для функционирования всей ИСПДн.

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.

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 сельского поселения Красный Яр муниципального района Красноярский Самарской области (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 «Порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации».

3.2. Организационные меры

Ответственные сотрудники доводят до сведения всех сотрудников Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, находящихся в их зоне ответственности, с данной инструкцией в срок, не превышающий 3х рабочих дней с момента выхода нового сотрудника на работу.

Должно быть проведено обучение сотрудников, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций.

Сотрудники, ответственные за обеспечение безопасности ИСПДн должны быть дополнительно обучены методам частичного и полного восстановления работоспособности элементов ИСПДн.

Приложение № 22

УТВЕРЖДЕНА
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ АДМИНИСТРАЦИИ СЕЛЬСКОГО ПОСЕЛЕНИЯ КРАСНЫЙ ЯР МУНИЦИПАЛЬНОГО РАЙОНА КРАСНОЯРСКИЙ САМАРСКОЙ ОБЛАСТИ

Раздел I Общие положения

1. Настоящая Модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области (далее - Модель угроз) содержит систематизированный перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Угрозы безопасности персональных данных могут быть обусловлены преднамеренными или непреднамеренными действиями физических лиц, действиями зарубежных спецслужб или организаций (в том числе террористических), а также криминальных группировок, создающих условия (предпосылки) для нарушения безопасности персональных данных, которое ведет к ущербу жизненно важных интересов личности, общества и государства.

Модель угроз содержит исходные данные по угрозам безопасности персональных данных, обрабатываемых в информационных системах персональных данных Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области (далее - ИСПДн), связанным:

с перехватом (съемом) персональных данных по техническим каналам с целью их копирования или неправомерного распространения;

с несанкционированным, в том числе случайным, доступом в ИСПДн с целью изменения, копирования, неправомерного распространения персональных данных или деструктивных воздействий на элементы ИСПДн и обрабатываемых в них персональных данных с использованием программных и программно-аппаратных средств с целью уничтожения или блокирования персональных данных.

2. Настоящая Модель угроз разработана в соответствии с:

Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных";

постановлением Правительства Российской Федерации от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";

Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной Федеральной службой по техническому и экспортному контролю 15.02.2008;

Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной Федеральной службой по техническому и экспортному контролю 15.02.2008.

3. С применением Модели угроз решаются следующие задачи:

1) разработка частных моделей угроз безопасности персональных данных в конкретных ИСПДн с учетом их назначения, условий и особенностей функционирования;

2) анализ защищенности ИСПДн от угроз безопасности персональных данных в ходе организации и выполнения работ по обеспечению безопасности персональных данных;

3) разработка системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса ИСПДн;

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

5) недопущение воздействия на технические средства ИСПДн, в результате которого может быть нарушено их функционирование;

6) контроль обеспечения уровня защищенности персональных данных.

4. В настоящей Модели угроз используются следующие понятия:

1) 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;

2) блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

3) вредоносная программа - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных;

4) 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;

5) 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;

6) доступ к информации - возможность получения информации и ее использования;

7) защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых актов или требованиями, устанавливаемыми собственником информации;

8) 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;

9) информационная система персональных данных - это 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;

10) информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

11) источник угрозы безопасности информации - субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации;

12) контролируемая зона - это пространство, в котором исключено неконтролируемое пребывание сотрудников оператора, иных лиц и посторонних транспортных, технических и иных материальных средств;

13) конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;

14) 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;

15) несанкционированный доступ (несанкционированные действия) - доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам;

16) 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;

17) перехват информации - неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов;

18) 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;

19) пользователь информационной системы персональных данных - лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования;

20) программное (программно-математическое) воздействие - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ;

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

22) технические средства информационной системы персональных данных - средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (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;

23) технический канал утечки информации - совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация;

24) 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;

25) 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;

26) утечка (защищаемой) информации по техническим каналам - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации;

27) уязвимость информационной системы персональных данных - недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которые могут быть использованы для реализации угрозы безопасности персональных данным;

28) целостность информации - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

Раздел II Классификация и исходный уровень защищенности информационных систем персональных данных

5. Состав и содержание угроз безопасности персональных данных определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным.

Совокупность таких условий и факторов формируется с учетом характеристик ИСПДн, свойств среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, и возможностей источников угрозы.

6. В зависимости от целей и содержания обработки персональных данных осуществляется их обработка в ИСПДн различных типов.

7. ИСПДн объединяют обобщенные характеристики:

по структуре ИСПДн: локальные информационные системы и распределенные информационные системы;

по наличию подключений к сетям связи общего пользования и (или) сетям международного информационного обмена: системы, имеющие подключения, и системы, не имеющие подключений;по режиму обработки персональных данных в информационной системе информационные системы: многопользовательские;

по разграничению прав доступа пользователей: системы с разграничением прав доступа.

Все технические средства ИСПДн находятся в пределах Российской Федерации.

8. В зависимости от технологий, состава и характеристик технических средств ИСПДн, а также опасности реализации угроз безопасности персональных данных и наступления последствий в результате несанкционированного или случайного доступа все ИСПДн можно классифицировать как следующие типы ИСПДн:

локальные ИСПДн, не имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;

распределенные ИСПДн, не имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена.

9. Исходный уровень защищенности ИСПДн определен как средний, так как не менее 70% характеристик ИСПДн соответствуют уровню не ниже "средний".

Показатели исходной защищенности ИСПДн определены в Приложении 1 к настоящей Модели угроз.

Раздел III Классификация актуальных угроз безопасности персональных данных

10. Возможности источников угроз безопасности персональных данных обусловлены совокупностью способов несанкционированного и (или) случайного доступа к персональным данным, в результате которого возможно нарушение конфиденциальности (копирование, неправомерное распространение), целостности (уничтожение, изменение) и доступности (блокирование) персональных данных.

Угроза безопасности персональных данных реализуется в результате образования канала реализации угрозы безопасности персональных данных между источником угрозы и носителем (источником) персональных данных, что создает условия для нарушения безопасности персональных данных (несанкционированный или случайный доступ).

11. При обработке персональных данных в локальных ИСПДн, не имеющих подключения к сетям связи общего пользования и (или) сетям международного информационного обмена, возможна реализация следующих угроз безопасности персональных данных:

1) угрозы утечки информации по техническим каналам;

2) угрозы несанкционированного доступа к персональным данным, обрабатываемым на автоматизированном рабочем месте.

12. Угрозы утечки информации по техническим каналам включают в себя:

1) угрозы утечки акустической (речевой) информации;

2) угрозы утечки видовой информации;

3) угрозы утечки информации по каналу побочных электромагнитных излучений и наводок.

13. Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПДн, возможно при наличии функций голосового ввода персональных данных в ИСПДн или функций воспроизведения персональных данных акустическими средствами ИСПДн.

14. Реализация угрозы утечки видовой информации возможна за счет просмотра информации с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средства обработки графической, видео и буквенно-цифровой информации, входящих в состав ИСПДн.

15. Угрозы утечки информации по каналу побочных электромагнитных излучений и наводок возможны из-за наличия электромагнитных излучений, в основном, монитора и системного блока компьютера. Основную опасность представляют угрозы утечки из-за наличия электромагнитных излучений монитора.

16. Угрозы несанкционированного доступа в локальных ИСПДн связаны с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн, а также нарушителей, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена.

17. Угрозы несанкционированного доступа в ИСПДн, связанные с действиями нарушителей, имеющих доступ к ИСПДн, включают в себя:

1) угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой;

2) угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текстов в текстовых файлах и т.п.)

3) угрозы внедрения вредоносных программ.

18. Угрозы несанкционированного доступа в локальных ИСПДн включают в себя:

1) угрозы "Анализа сетевого трафика" с перехватом передаваемой по локальной сети информации;

2) угрозы выявления паролей;

3) угрозы удаленного запуска приложений;

4) угрозы внедрения по сети вредоносных программ.

Раздел IV Угрозы утечки информации по техническим каналам

19. Основными элементами описания угроз утечки информации по техническим каналам являются: источник угрозы, среда (путь) распространения информативного сигнала и носитель защищаемой информации.

20. Источниками угроз утечки информации по техническим каналам являются физические лица, не имеющие доступа к ИСПДн, а также зарубежные спецслужбы или организации (в том числе конкурирующие или террористические), криминальные группировки, осуществляющие перехват (съем) информации с использованием технических средств ее регистрации, приема или фотографирования.

21. При обработке персональных данных в ИСПДн за счет реализации технических каналов утечки информации возможно возникновение следующих угроз безопасности персональных данных:

1) угрозы утечки акустической (речевой) информации;

2) угрозы утечки видовой информации;

3) угроз утечки информации по каналам побочных электромагнитных излучений и наводок.

22. Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПДн, возможно при наличии функций голосового ввода персональных данных в ИСПДн или функций воспроизведения персональных данных акустическими средствами ИСПДн.

23. Перехват акустической (речевой) информации возможен с использованием аппаратуры, регистрирующей акустические (в воздухе) и виброакустические (в упругих средах) волны, а также электромагнитные (в том числе оптические) излучения и электрические сигналы, модулированные информативным акустическим сигналом, возникающие за счет преобразований в технических средствах обработки персональных данных, вспомогательных технических средствах и системах и строительных конструкциях и инженерно-технических коммуникациях под воздействием акустических волн.

Перехват акустической (речевой) информации также возможен с использованием специальных электронных устройств съема речевой информации, внедренных в технические средства обработки персональных данных, вспомогательные технические средства и системы и помещения или подключенных к каналам связи.

24. В ИСПДн функции голосового ввода персональных данных или функции воспроизведения персональных данных акустическими средствами отсутствуют.

Вероятность реализации угрозы утечки акустической (речевой) информации определена как маловероятная, возможность реализации угрозы является низкой, показатель опасности угрозы - неактуальная.

25. Угрозы утечки видовой информации реализуются за счет просмотра персональных данных с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео - и буквенно-цифровой информации, входящих в состав ИСПДн.

Просмотр (регистрация) персональных данных также возможен с использованием специальных электронных устройств съема, внедренных в служебных помещениях или скрытно используемых физическими лицами при посещении ими служебных помещений.

Рабочие места пользователей ИСПДн организованы таким образом, чтобы был исключен случайный просмотр информации с экранов автоматизированных рабочих мест. На окнах установлены жалюзи.

26. Вероятность реализации угрозы утечки видовой информации определена как низкая, возможность реализации угрозы является средней, показатель опасности угрозы - актуальная.

27. Возникновение угрозы утечки информации по каналам побочных электромагнитных излучений и наводок возможно за счет перехвата техническими средствами побочных (не связанных с прямым функциональным значением элементов ИСПДн) информативных электромагнитных полей и электрических сигналов, возникающих при обработке персональных данных техническими средствами ИСПДн.

Все элементы ИСПДн находятся внутри контролируемой зоны на достаточном расстоянии от ее границ. Информативный сигнал в каналах побочных электромагнитных излучений и наводок современных средств вычислительной техники очень низок, и он маскируется множеством других излучений от автоматизированных рабочих мест, не состоящих в ИСПДн, а также от прочих элементов современной информационной инфраструктуры.

28. Вероятность реализации угрозы утечки информации по каналам побочных электромагнитных излучений и наводок определена как маловероятная, возможность реализации угрозы является низкой, показатель опасности угрозы - неактуальная.

29. Обобщенная информация по угрозам утечки информации по техническим каналам представлена в Приложении 2 к настоящей Модели угроз.

Раздел V Угрозы несанкционированного доступа к информации в информационных системах персональных данных Аппарата Администрации Ненецкого автономного округа

30. Угрозы несанкционированного доступа в ИСПДн с применением программных и программно-аппаратных средств реализуются при осуществлении несанкционированного, в том числе случайного, доступа, в результате которого осуществляется нарушение конфиденциальности (копирование, несанкционированное распространение), целостности (уничтожение, изменение) и доступности (блокирование) персональных данных, и включают в себя:

1) угрозы доступа (проникновения) в операционную среду компьютера с использованием штатного программного обеспечения (средств операционной системы или прикладных программ общего применения);

2) угрозы создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т.п.;

3) угрозы внедрения вредоносных программ (программно-математического воздействия);

4) комбинированные угрозы, представляющие собой сочетание угроз, указанных в подпунктах 1 - 3 настоящего пункта.

31. Источниками угроз несанкционированного доступа в ИСПДн могут быть:

1) нарушитель;

2) носитель вредоносной программы;

3) аппаратная закладка.

32. По наличию права постоянного или разового доступа в контролируемую зону ИСПДн нарушители подразделяются на два типа:

1) нарушители, не имеющие доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена, - внешние нарушители;

2) нарушители, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн, - внутренние нарушители.

33. Носителем вредоносной программы может быть аппаратный элемент компьютера или программный контейнер. Если вредоносная программа не ассоциируется с какой-либо прикладной программой, то в качестве ее носителя рассматриваются:

1) отчуждаемый носитель, то есть дискета, оптический диск (CD-R, CD-RW), флэш-память, отчуждаемый жесткий диск и т.п.;

2) встроенные носители информации (жесткие диски, микросхемы оперативной памяти, процессор, микросхемы системной платы, микросхемы устройств, встраиваемых в системный блок: видеоадаптера, сетевой платы, звуковой платы, модема, устройств ввода/вывода магнитных жестких и оптических дисков, блока питания и т.п., микросхемы прямого доступа к памяти, шин передачи данных, портов ввода/вывода);

3) микросхемы внешних устройств (монитора, клавиатуры, принтера, модема, сканера и т.п.).

34. Если вредоносная программа ассоциируется с какой-либо прикладной программой, с файлами, имеющими определенные расширения или иные атрибуты, с сообщениями, передаваемыми по сети, то ее носителями являются:

1) пакеты передаваемых по компьютерной сети сообщений;

2) файлы (текстовые, графические, исполняемые и т.д.).

35. Причинами возникновения уязвимостей ИСПДн являются:

1) ошибки при проектировании и разработке программного (программно-аппаратного) обеспечения;

2) преднамеренные действия по внесению уязвимостей в ходе проектирования и разработки программного (программно-аппаратного) обеспечения;

3) неправильные настройки программного обеспечения, неправомерное изменение режимов работы устройств и программ;

4) несанкционированное внедрение и использование неучтенных программ с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);

5) внедрение вредоносных программ, создающих уязвимости в программном и программно-аппаратном обеспечении;

6) несанкционированные неумышленные действия пользователей, приводящие к возникновению уязвимостей;

7) сбои в работе аппаратного и программного обеспечения (вызванные сбоями в электропитании, выходом из строя аппаратных элементов в результате старения и снижения надежности, внешними воздействиями электромагнитных полей технических устройств и др.).

36. Угрозы доступа (проникновения) в операционную среду компьютера и несанкционированного доступа к персональным данным связаны с доступом:

1) к информации и командам, хранящимся в базовой системе ввода/вывода (BIOS) ИСПДн, с возможностью перехвата управления загрузкой операционной системы и получением прав доверенного пользователя;

2) в операционную среду, то есть в среду функционирования локальной операционной системы отдельного технического средства ИСПДн с возможностью выполнения несанкционированного доступа путем вызова штатных программ операционной системы или запуска специально разработанных программ, реализующих такие действия;

3) в среду функционирования прикладных программ (например, к локальной системе управления базами данных);

4) непосредственно к информации пользователя (к файлам, текстовой, аудио- и графической информации, полям и записям в электронных базах данных) и обусловлены возможностью нарушения ее конфиденциальности, целостности и доступности.

37. В случае если ИСПДн реализована на базе локальной или распределенной информационной системы, то в ней могут быть реализованы угрозы безопасности информации путем использования протоколов межсетевого взаимодействия. При этом может обеспечиваться несанкционированный доступ к персональным данным или реализовываться угроза отказа в обслуживании. Особенно опасны угрозы, когда ИСПДн представляет собой распределенную информационную систему, подключенную к сетям общего пользования и (или) сетям международного информационного обмена.

38. Программно-математическое воздействие - это воздействие с помощью вредоносных программ.

Программой с потенциально опасными последствиями или вредоносной программой называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

скрывать признаки своего присутствия в программной среде компьютера;

обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти;

разрушать (искажать произвольным образом) код программ в оперативной памяти;

выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирование, уничтожение, блокирование и т.п.);

сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);

искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

39. Обобщенная информация по угрозам несанкционированного доступа к информации в информационной системе персональных данных представлена в Приложении 3 к настоящей Модели угроз.

Приложение 1
к Модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных

Показатели исходной защищенности информационных систем персональных данных Аппарата Администрации Ненецкого автономного округа

Технические и эксплуатационные характеристики	Уровень защищенности
1. По территориальному размещению	Средний
2. По наличию соединения с сетями общего пользования	Средний
3. По встроенным (легальным) операциям с записями баз персональных данных	Средний
4. По разграничению доступа к персональным данным	Средний
5. По наличию соединений с другими базами персональных данных иных информационных систем персональных данных	Высокий
6. По уровню обобщения (обезличивания) персональных данных	Средний
7. По объему персональных данных, которые предоставляются сторонним пользователям информационных систем персональных данных без предварительной обработки	Высокий

Приложение 2
к Модели угроз безопасности
персональных данных при их обработке
в информационных системах персональных данных

Обобщенная информация по угрозам утечки информации по техническим каналам

Наименование угрозы	Вероятность реализации угрозы	Возможность реализации угрозы	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе
Угрозы утечки информации по техническим каналам					
Угрозы утечки акустической информации	Маловероятная	Низкая	Средняя	Неактуальная	Не требуются
Угрозы утечки видовой информации	Низкая	Средняя	Средняя	Актуальная	Порядок обращения со служебной информацией ограниченного доступа
Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок	Маловероятная	Низкая	Средняя	Неактуальная	Не требуются

Приложение 3
к Модели угроз безопасности персональных данных при их

обработке в информационных системах персональных данных

Обобщенная информация по угрозам несанкционированного доступа к информации в информационной системе персональных данных

Наименование угрозы	Вероятность реализации угрозы	Возможность реализации угрозы	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе
Угрозы несанкционированного доступа к информации в информационной системе персональных данных					
Угрозы, реализуемые в ходе загрузки операционной системы	Низкая	Средняя	Средняя	Актуальная	Применение сертифицированных средств защиты информации от несанкционированного доступа
Угрозы, реализуемые после загрузки операционной системы	Низкая	Средняя	Средняя	Актуальная	Применение сертифицированных средств защиты информации от несанкционированного доступа, инструкция пользователя информационной системы персональных данных
Угрозы внедрения вредоносных программ	Низкая	Средняя	Средняя	Актуальная	Применение сертифицированных средств защиты информации от несанкционированного доступа, антивирусного программного обеспечения
Угрозы "Анализа сетевого трафика"	Маловероятная	Средняя	Средняя	Неактуальная	Не требуется
Угрозы выявления паролей	Низкая	Средняя	Средняя	Актуальная	Применение сертифицированных средств защиты информации от несанкционированного доступа, инструкция пользователя информационной системы персональных данных
Угрозы удаленного запуска приложений	Низкая	Средняя	Средняя	Актуальная	Применение сертифицированных средств защиты информации от несанкционированного доступа, инструкция пользователя информационной системы персональных данных, инструкция администратора информационной системы персональных данных
Угрозы внедрения по сети вредоносных программ	Низкая	Средняя	Средняя	Актуальная	Применение сертифицированных средств защиты информации от несанкционированного доступа, инструкция пользователя информационной системы персональных данных

Приложение № 23

УТВЕРЖДЕН
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

ДОГОВОР ПОРУЧЕНИЯ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕТЬИМ ЛИЦОМ

[с. Красный Яр] [число, месяц, год]

Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области, именуемое в дальнейшем "Доверитель", в лице Главы Ф.И.О. действующего на основании **устава,** с одной стороны, и [**наименование организации**], именуемое в дальнейшем "Поверенный", в лице [**должность, Ф. И. О.**], действующего на основании [**устава, положения, доверенности**], с другой стороны, а вместе именуемые "Стороны", заключили договор о нижеследующем:

1. Предмет договора

1.1. Поверенный обязуется по поручению, от имени и за счет Доверителя совершить действия по обработке персональных данных, которые включают следующее: [**указать перечень действий (операций) с персональными данными; такими действиями могут быть, например: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных**] (далее Поручение).
1.2. Состав персональных данных, подлежащих обработке, включает [**вписать нужное**].
1.3. Обработка персональных данных осуществляется в целях [**вписать нужное**].
1.4. Обработка персональных данных должна быть осуществлена в срок [**вписать нужное**].
1.5. Передача Доверителем персональных данных для обработки Поверенному осуществляется с согласия субъекта персональных данных по акту приема-передачи.

2. Обязанности сторон договора

2.1. Доверитель обязан:
2.1.1. В течение [**значение**] дней с даты подписания настоящего договора передать Поверенному персональные данные для обработки.
2.1.2. Возмещать Поверенному понесенные в связи с исполнением поручения издержки, подтвержденные документами, оформленными надлежащим образом.
2.1.3. Принять отчет Поверенного, все предоставленные им документы и все исполненное им в соответствии с настоящим договором.
2.1.4. Уплатить Поверенному вознаграждение в порядке, установленном разделом 3 настоящего договора.
2.2. Поверенный обязан:
2.2.1. Лично исполнять данное ему поручение.
2.2.2. Соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом от 27.07.2006 г. № 152-ФЗ "О персональных данных".
2.2.3. Осуществлять обработку персональных данных в соответствии с целями, определенными Сторонами в настоящем договоре.
2.2.4. Обеспечить при обработке персональных данных их точность, достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.
2.2.5. Осуществлять хранение персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных.
2.2.6. Соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также соблюдать требования к защите обрабатываемых персональных данных.
2.2.7. В случае выявления неправомерной обработки персональных данных прекратить неправомерную обработку персональных данных в срок, не превышающий трех рабочих дней с даты этого выявления.

2.2.8. В случае достижения цели обработки персональных данных прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных.
2.2.9. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных прекратить их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва.
2.2.10. Представлять Доверителю по его требованию информацию о ходе исполнения поручения.
2.2.11. По исполнении поручения или при прекращении настоящего договора до его исполнения без промедления возвратить Доверителю персональные данные и представить отчет о выполненном поручении с приложением документов, подтверждающих издержки Поверенного, связанные с обработкой персональных данных.
2.2.12. При сборе ПД по общему правилу использовать базы данных, находящиеся на территории РФ,
2.2.13.Соблюдать предписания ст. 18.1 Закона о ПД,
2.2.14 Предоставлять по запросу оператора ПД (в течение срока действия поручения) документы и иную информацию, подтверждающие принятие мер и соблюдение требований закона,
2.2.15.Уведомлять оператора о фактах неправомерной или случайной передачи (предоставления, распространения, доступа) ПД, повлекшей нарушение прав субъектов ПД (ч. 3 ст. 6 Закона о ПД в новой ред.), субъектом ПД наряду с оператором (ч. 6 ст. 6 Закона о ПД в новой ред.).

3. Цена договора и порядок оплаты

3.1. Размер вознаграждения Поверенного составляет [**цифрами и прописью**] рублей.
3.2. Вознаграждение по настоящему договору выплачивается Доверителем Поверенному следующим образом: [**единовременно, не позднее (значение) дней с даты предоставления отчета о выполненном поручении**].
3.3. Издержки Поверенного, понесенные в ходе исполнения настоящего договора, подлежат возмещению Доверителем в полном объеме на основании представленных Поверенным документов, подтверждающих обоснованность расходов.
Возмещение указанных расходов осуществляется Доверителем не позднее [**значение**] дней с даты предоставления отчета о выполненном поручении.
3.4. Расчеты по настоящему договору осуществляются в безналичной форме путем перечисления денежных средств на расчетный счет Поверенного, указанный в настоящем договоре.
3.5. В случае прекращения настоящего договора до того, как поручение будет исполнено, Доверитель обязан возместить Поверенному понесенные при исполнении поручения издержки и уплатить ему вознаграждение соразмерно выполненной им работе.

4. Ответственность сторон

4.1. В случае неисполнения или ненадлежащего исполнения своих обязательств по настоящему договору Стороны несут ответственность в соответствии с действующим законодательством Российской Федерации.
4.2. В случае неисполнения или ненадлежащего исполнения поручения Поверенным в сроки, предусмотренные настоящим договором, он лишается права на получение вознаграждения, предусмотренного разделом 3 настоящего договора.
4.3. В случае просрочки в уплате вознаграждения Поверенному Доверитель выплачивает последнему пени в размере [**значение**] процентов от просроченной суммы за каждый день просрочки, но не более [**значение**] процентов от суммы вознаграждения Поверенного по настоящему договору.
4.4. В случае просрочки Доверителем в возмещении расходов Поверенного в соответствии с п. 3.3. настоящего договора Доверитель выплачивает последнему пени в размере [**значение**] процентов от просроченной суммы за каждый день просрочки, но не более [**значение**] процентов от просроченной суммы.
4.5. Ответственность перед субъектом персональных данных за действия Поверенного несет Доверитель. Поверенный, осуществляющий обработку персональных данных по поручению Доверителя, несет ответственность перед Доверителем.
4.6. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, а также требований к защите персональных данных, установленных Федеральным законом от 27.07.2006 г. № 152-ФЗ "О персональных данных", подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

5. Конфиденциальность персональных данных и требования к защите обрабатываемых персональных данных

5.1. Стороны, получившие доступ к персональным данным по настоящему договору, обязуются не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных.

5.2. Стороны при обработке персональных данных обязаны принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие 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.

5.3. Обеспечение безопасности персональных данных достигается:

- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- учетом машинных носителей персональных данных;
- обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;
- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

5.4. Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы.

5.5. Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

5.6. Поверенный обеспечивает безопасность персональных данных при их обработке в информационной системе.

5.7. Поверенный осуществляет выбор средств защиты информации для системы защиты персональных данных в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю во исполнение части 4 статьи 19 Федерального закона от 27.07.2006 г. № 152-ФЗ "О персональных данных".

5.8. Поверенный производит определение типа угроз безопасности персональных данных, актуальных для информационной системы, с учетом оценки возможного вреда и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона от 27.07.2006 г. № 152-ФЗ "О персональных данных".

5.9. При обработке персональных данных в информационных системах устанавливается [значение] уровень защищенности персональных данных.

6. Основания и порядок прекращения договора

6.1. Настоящий договор подлежит прекращению вследствие:

6.1.1. Отмены поручения Доверителем.

6.1.2. Отказа Поверенного от исполнения поручения.

6.1.3. Вступления в действие решения суда о признании Доверителя несостоятельным (банкротом).

6.1.4. Вступления в действие решения суда о признании Поверенного несостоятельным (банкротом).

6.2. Доверитель вправе отменить поручение, а Поверенный отказаться от него во всякое время. Соглашение об отказе от этого права ничтожно.
6.3. В случае, если настоящий договор поручения прекращается до того, как поручение исполнено Поверенным полностью, Доверитель обязан возместить Поверенному понесенные им при исполнении поручения издержки и уплатить вознаграждение соразмерно выполненной им работе.
6.4. В случае одностороннего отказа Поверенного от исполнения поручения он обязан возместить Доверителю все причиненные этим убытки в случае, если Доверитель будет лишен возможности иначе обеспечить свои интересы.

7. Порядок разрешения споров

7.1. Споры и разногласия, которые могут возникнуть при исполнении настоящего договора, будут по возможности разрешаться путем переговоров между Сторонами.
7.2. В случае, если Стороны не придут к соглашению, споры разрешаются в судебном порядке в соответствии с действующим законодательством Российской Федерации.

8. Заключительные положения

8.1. Настоящий договор составлен в двух экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для каждой из Сторон.
8.2. Договор вступает в силу с момента подписания и действует до полного выполнения обязательств по данному договору.
8.3. Все изменения и дополнения оформляются дополнительными соглашениями Сторон в письменной форме, которые являются неотъемлемой частью настоящего договора.

9. Реквизиты и подписи сторон

Доверитель	Поверенный
[вписать нужное]	[вписать нужное]
М. П.	М. П.

Приложение № 24

УТВЕРЖДЕНЫ
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Понятие информационной системы персональных данных.

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

2. Информационные системы персональных данных:

- «Контур–Экстерн»;
- «1С: Предприятие 8.2. Зарплата и кадры бюджетного учреждения»;
- АС «Сбербанк Бизнес Онлайн» (СББОЛ);
- «УРМ»
- БАРС ЭПК Электронная похозяйственная книга.

Приложение № 25

УТВЕРЖДЕНА
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

ИНСТРУКЦИЯ ПО ПОРЯДКУ УЧЁТА, ХРАНЕНИЯ И УНИЧТОЖЕНИЯ СЪЁМНЫХ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ В АДМИНИСТРАЦИИ СЕЛЬСКОГО ПОСЕЛЕНИЯ КРАСНЫЙ ЯР МУНИЦИПАЛЬНОГО РАЙОНА КРАСНОЯРСКИЙ САМАРСКОЙ ОБЛАСТИ

1. Термины и определения

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

Съемный машинный носитель персональных данных – сменный носитель персональных данных, предназначенный для записи и считывания персональных данных, представленных в стандартных кодах;

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;

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

Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

2. Общие положения

Настоящая Инструкция по обращению со съемными машинными носителями персональных данных в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области (далее – Инструкция), разработана в соответствии с законодательством Российской Федерации о персональных данных (далее – ПДн) и нормативно-методическими документами исполнительных органов государственной власти по вопросам безопасности ПДн при их обработке в информационных системах персональных данных (далее – ИСПДн).

Настоящая Инструкция регламентирует порядок учета, хранения и регистрации выдачи съемных машинных носителей персональных данных (далее – СМНПДн).

Под СМНПДн в настоящей Инструкции понимаются следующие носители информации:

- оптические диски (CD, DVD) однократной и многократной записи;
- электронные накопители информации (флэш-память, съемные жесткие диски);
- иные носители информации.

Требования настоящей Инструкции являются обязательными для исполнения всеми работниками), использующими в своей работе СМНПДн.

Все работники, использующие СМНПДн, должны быть ознакомлены с требованиями настоящей Инструкцией под подпись.

Настоящая Инструкция является дополнением к действующим локальным нормативным актам (внутренним документам) по вопросам обеспечения безопасности сведений конфиденциального характера, в том числе и ПДн, и не исключает обязательного выполнения их требований.

3. Правила обращения со съемными машинными носителями персональных данных

Обращение со СМНПДн должно осуществляется таким образом, чтобы исключались их утрата, порча и несанкционированный доступ к ним посторонних лиц.

При обращении со СМНПДн, выполняются следующие основные правила:

- СМНПДн учитываются и выдаются под подпись;
- СМНПДн, срок эксплуатации которых истек, уничтожаются в установленном порядке;

- для выноса СМНПДн за пределы контролируемой зоны, запрашивается специальное разрешение у ответственного за обеспечение безопасности ПДн в ИСПДн (далее – Ответственный), а факт выноса фиксируется;
- право на перемещение СМНПДн за пределы контролируемой зоны, имеют только те лица, которым оно необходимо для выполнения своих должностных обязанностей (функции);
- все СМНПДн должны хранится в сейфах (металлических шкафах), оборудованных внутренними замками с двумя или более дубликатами ключей и приспособленными для опечатывания замочных скважин или кодовыми замками;
- допускается хранение СМНПДн вне сейфов (металлических шкафов) при условиях уничтожения (стирания) ПДн и остаточной информации (информации, которую можно восстановить после удаления с помощью нештатных средств и методов) с использованием средств стирания данных и остаточной информации, либо если на съемном машинном носителе ПДн хранятся только ПДн в зашифрованном виде с использованием средств криптографической защиты информации.

СМНПДн должен использоваться, не более срока эксплуатации, установленного изготовителем материального носителя.

4. **Порядок хранения и учета съемных машинных носителей персональных данных**

СМНПДн, должны иметь специальную маркировку. Тип маркировки выбирается Ответственным.

Все находящиеся на хранении и в обращении СМНПДн учитываются Ответственным в «Журнале учета съемных машинных носителей персональных данных в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области , форма которого установлена в Приложении 1 к настоящей Инструкции.

В нерабочее время и время отсутствия необходимости использования ПДн СМНПДн должны храниться в хранилищах СМНПДн.

Перечень хранилищ определяется в «Журнале учета хранилищ носителей персональных данных в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области .

Пользователи для выполнения работ получают СМНПДн у Ответственного. При получении делаются соответствующие записи в «Журнале учета съемных машинных носителей персональных данных в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области.

5. **Порядок уничтожения съемных машинных носителей персональных данных**

Уничтожение ПДн производится только в следующих случаях:

- обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом;
- ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки;
- в случае выявления неправомерной обработки ПДн, если обеспечить правомерность обработки ПДн невозможно;
- в случае достижения цели обработки ПДн;
- в случае отзыва субъектом ПДн согласия на обработку его ПДн и в случае, если сохранение ПДн более не требуется для целей обработки ПДн.

5. СМНПДн, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению.
5. Уничтожение СМНПДн осуществляется комиссией по уничтожению, назначенной распоряжением Главы Комитета.
5. При уничтожении СМНПДн необходимо:

- убедиться в необходимости уничтожения СМНПДн;
- убедиться в том, что уничтожаются только та информация, которая предназначена для уничтожения;
- уничтожить СМНПДн подходящим способом, в соответствии с настоящей Инструкцией или способом, указанным в соответствующем требовании или распорядительном документе.

5. При уничтожении СМНПДн применяются следующие способы:

- измельчение в бумагорезательной (бумагоуничтожительной) машине – для документов, исполненных на бумаге;

- тщательное вымарывание (с проверкой тщательности вымарывания) информации, подлежащей уничтожению – для сохранения возможности обработки иных данных, зафиксированных в документе;
- измельчение в специальной мультирезательной (мультиуничтожительной) машине или физическое уничтожение (разрушение) носителей информации – для СМНПДн на оптических дисках;
- физическое уничтожение частей СМНПДн – разрушение или сильная деформация – для носителей информации на жестком магнитном диске (уничтожению подлежат внутренние диски и микросхемы); SSD-дисках, USB- и Flash-носителях (уничтожению подлежат модули и микросхемы долговременной памяти);
- стирание с помощью сертифицированных средств уничтожения информации – для записей в базах данных и отдельных документов на машинном носителе.

По результатам уничтожения СМНПДн комиссией составляется «Акт уничтожения съемных машинных носителей персональных данных», форма которого установлена в Приложении 2 к настоящей Инструкции.

6. **Ответственность**

Ответственным за хранение, учет и выдачу СМНПДн, является Ответственный.

Все работники Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области , использующие СМНПДн и Ответственный несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации. За несоблюдение требований законодательства Российской Федерации предусмотрена гражданская, уголовная, административная, дисциплинарная ответственность.

7. **Срок действия и порядок внесения изменений**

Настоящая Инструкция вступает в силу с момента его утверждения и действует бессрочно.

Настоящая Инструкция подлежит пересмотру не реже одного раза в три года.

Изменения и дополнения в настоящую Инструкцию вносятся распоряжением Главы Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области.

Приложение 1 к инструкции
по обращению со съемными машинными
носителями персональных данных в
Администрации сельского поселения
Красный Яр муниципального района
Красноярский Самарской области

ФОРМА

Журнал учета съемных машинных носителей персональных данных в Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области

№ п/п	Тип носителя	Номер (серийный/ инвентарный)	Расписка в получении			Подпись ответственного лица	Место хранения	Примечание	Дата и номер акта уничтожения
			ФИО	Дата	Подпись				
1	2	3	4	5	6	7	8	9	10

Приложение 2 к инструкции
по обращению со съемными машинными
носителями персональных данных в
Администрации сельского поселения
Красный Яр муниципального района
Красноярский Самарской области

ФОРМА

АКТ
об уничтожении съемных машинных носителей персональных данных

«__»_____20__ г

Комиссия в составе:

Председатель:

_____ _____

Члены комиссии:

. _____ _____
. _____ _____
. _____ _____

составили настоящий акт о том, что в результате проведенной экспертной оценки подлежат уничтожению следующие съемные машинные носители персональных данных:

№ п/п	Дата окончания срока обработки зафиксированных на носителе персональных данных	Учетный номер съемного носителя или наименование технического средства, на котором уничтожаются файлы	Примечание
1	2	3	4

Всего съемных носителей

(цифрами и прописью)

Перечисленные съемные носители уничтожены путем

(механического уничтожения, сжигания, разрезания, деформирования и т.п.)

Председатель:

_____ _____ _____

Члены комиссии:

_____ _____ _____
_____ _____ _____
_____ _____ _____

Приложение № 26

УТВЕРЖДЕН
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

ЖУРНАЛ ПО УЧЕТУ ОБРАЩЕНИЙ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХО ВЫПОЛНЕНИИ ИХ ЗАКОННЫХ ПРАВ В ОБЛАСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ, ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, В ТОМ ЧИСЛЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ АДМИНИСТРАЦИИ СЕЛЬСКОГО ПОСЕЛЕНИЯ КРАСНЫЙ ЯР МУНИЦИПАЛЬНОГО РАЙОНА КРАСНОЯРСКИЙ САМАРСКОЙ ОБЛАСТИ

N п/п	Дата обращения	Ф. И. О. субъекта ПДн (запрашивающее лицо)	Краткое содержание обращения	Цель запроса	Отметка о предоставлении/отказе в предоставлении информации	Дата передачи/отказа в предоставлении информации	Подпись запрашивающего лица	Подпись ответственного лица	Примечание

Приложение № 27

УТВЕРЖДЕН
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

ЖУРНАЛ УЧЕТА ЛИЦ, ДОПУЩЕННЫХ К ПЕРСОНАЛЬНЫМ ДАННЫМ

№	Сведения о допуске к персональным данным			Сведения о прекращении допуска к персональным данным		
	Наименование информационной системы персональных данных	Дата утверж-дения «Списка…»	Дата и подпись допускаемого лица	Дата утверждения «Списка…» или дата распоряжения (распоряжения) об увольнении	Номер распоряжения (распоряжения) об увольнении	Дата и подпись лица об ознакомлении с документом, прекращающим допуск к ПДн

Приложение № 28

УТВЕРЖДЕН
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

ЖУРНАЛ УЧЁТА ПРОХОЖДЕНИЯ ПЕРВИЧНОГО ИНСТРУКТАЖА РАБОТНИКАМИ, ДОПУЩЕННЫМИ К РАБОТЕ С ПДН В ИСПДН

№ п/п	ФИО работника	Дата прохождения инструктажа	Подпись работника	ФИО должностного лица, проводившего инструктаж	Подпись должностного лица

Приложение № 29

УТВЕРЖДЕН
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

ЖУРНАЛ УЧЕТА НЕШТАТНЫХ СИТУАЦИЙ, ФАКТОВ ВСКРЫТИЯ И ОПЕЧАТЫВАНИЯ ПЭВМ, ВЫПОЛНЕНИЯ ПРОФИЛАКТИЧЕСКИХ РАБОТ, УСТАНОВКИ И МОДИФИКАЦИИ АППАРАТНЫХ И ПРОГРАММНЫХ СРЕДСТВ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

N п/п	Дата	Краткое описание выполненной работы (нештатной ситуации)	ФИО и подпись пользователя	ФИО и подпись ответственного за обеспечение безопасности персональных данных	Примечание (ссылка на заявку)
1	2	3	4	5	7

Приложение № 30

УТВЕРЖДЕНО
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

ПОЛОЖЕНИЕ ОБ ОРГАНИЗАЦИИ РЕЖИМА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПОМЕЩЕНИЙ, В КОТОРЫХ РАЗМЕЩЕНЫ ИНФОРМАЦИОННЫЕ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ, ПРЕПЯТСТВУЮЩЕГО ВОЗМОЖНОСТИ НЕКОНТРОЛИРУЕМОГО ПРОНИКНОВЕНИЯ ИЛИ ПРЕБЫВАНИЯ В ЭТИХ ПОМЕЩЕНИЯХ ЛИЦ, НЕ ИМЕЮЩИХ ПРАВА ДОСТУПА В ЭТИ ПОМЕЩЕНИЯ

1. Общие положения

1.1. Положение об организации режима обеспечения безопасности помещений администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области (далее – Оператор), в которых размещены информационные системы персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения (далее – Положение) разработано в соответствии с распоряжением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказом ФСБ России 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 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».

1.2. Защита от проникновения посторонних лиц в помещения Оператора обеспечивается организацией порядка доступа, а также соответствующей инженерно-технической защитой помещений, а именно охранной сигнализацией и системой контроля и управления доступом.

2. Границы контролируемой зоны

2.1. Контролируемая зона – границы пространства (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска.

2.2. План-схема контролируемых зоны помещений по адресу: Самарская область, Красноярский район, село Красный Яр, улица Комсомольская 90, , приведена в приложении 1 к настоящему Положению.

3. Порядок доступа в помещения

3.1. Перечень лиц, доступ которых в помещения, находящиеся в пределах границы контролируемой зоны, необходим для выполнения ими служебных (трудовых обязанностей) утверждается распоряжением администрации поселения.

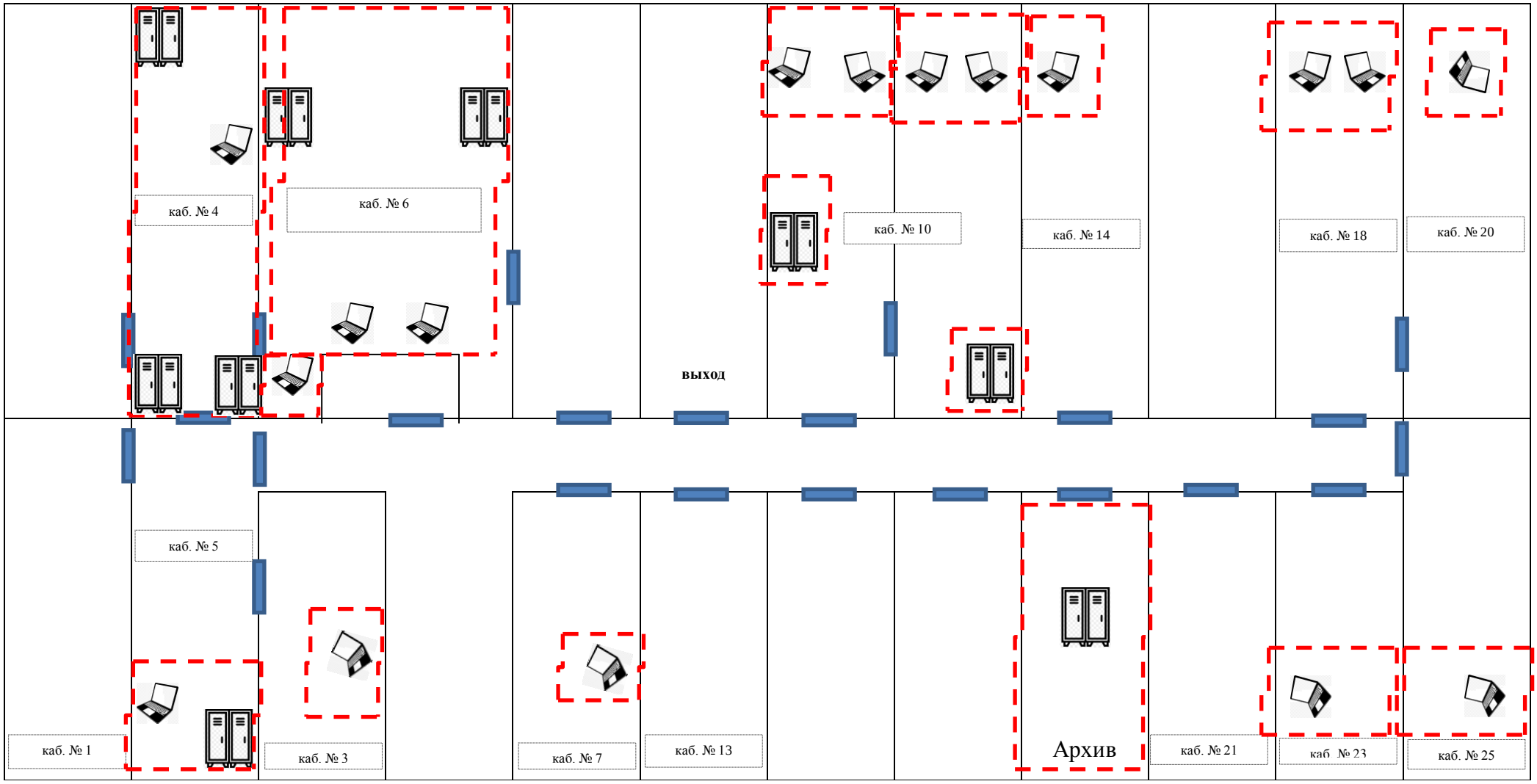
3.2. Неконтролируемое пребывание лиц в помещениях, находящихся в пределах границы контролируемой зоны, разрешено в период рабочего времени в соответствии с утверждённым графиком работы Оператора, либо вне периода рабочего времени с письменного разрешения ответственного за организацию обработки персональных данных или ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных.

3.3. Лица, не указанные в п. 3.1 настоящего Положения, допускаются в помещения в присутствии лиц, имеющих право пребывания в данных помещениях.

Приложение 1
К Положению об организации режима обеспечения безопасности помещений,
в которых размещены информационные системы персональных данных,
препятствующего возможности неконтролируемого проникновения
или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения

ПЛАН-СХЕМА КОНТРОЛИРУЕМОЙ ЗОНЫ ПОМЕЩЕНИЙ

по адресу: Самарская область, Красноярский район, село Красный Яр, улица Комсомольская, д.90 2 этаж.



- дверь, компьютер(обработка ПД) Граница контролируемой зоны - сейф для хранения ПД

Приложение № 31

УТВЕРЖДЕНА
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

ИНСТРУКЦИЯ ПО ОБРАЩЕНИЮ С КРИПТОСРЕДСТВАМИ

1. Общие положения

Настоящая инструкция регламентирует порядок обращения с шифровальными средствами (средствами криптографической защиты информации, СКЗИ), предназначенными для защиты информации, не содержащей сведений, составляющих государственную тайну, в процессе их получения, транспортировки, учета, хранения, уничтожения, встраивания в прикладные системы, тестирования, передачи клиентам, а также порядок допуска к работам с шифровальными средствами в Администрации сельского посеения Красный Яр.

Все сотрудники администрации, допущенные к работе с СКЗИ, должны ознакомиться с данной инструкцией под подпись и строго выполнять требования настоящей инструкции в части, их касающейся, а также строго выполнять требования нормативных правовых актов Российской Федерации, относящихся к деятельности с СКЗИ, нормативных и методических документов лицензирующего органа.

Разработка и проведение мероприятий по обеспечению безопасности при работе с СКЗИ осуществляется ответственным за эксплуатацию СКЗИ.

Работы с СКЗИ должны проводиться с учетом Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005).

2. Требования по размещению, оборудованию и охране помещений

Размещение, оборудование, охрана и режим в помещениях, в которых проводятся работы с СКЗИ (далее – помещения), должны обеспечивать безопасность СКЗИ, сведение к минимуму возможности неконтролируемого доступа посторонних лиц. Доступ сотрудников в эти помещения должен быть ограничен в соответствии со служебной необходимостью и определяться перечнем лиц, допущенных в кабинеты.

Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Для предотвращения просмотра извне окна помещений должны быть защищены (жалюзи, шторы и т.п.).

3. Порядок обращения с СКЗИ

Пользователи криптосредств обязаны:

- не разглашать информацию о ключевых документах;
- не допускать вывод ключевых документов на дисплей (монитор) ПЭВМ или принтер;
- не допускать установки ключевых документов в другие ПЭВМ.

Все поступающие СКЗИ, инсталлирующие СКЗИ носители, эксплуатационная и техническая документация (при наличии) к ним должны браться на поэкземплярный учет в журнале установленной формы (Приложение). Ведет журналы администратор информационной безопасности.

Единицей поэкземплярного учета СКЗИ является:

−для аппаратных и программно-аппаратных СКЗИ - конструктивно законченное техническое устройство;

−для программных СКЗИ – инсталлирующий СКЗИ носитель (дискета, компакт-диск (CD-ROM) и т.п.).

Должны быть приняты организационные меры с целью исключения возможности несанкционированного копирования СКЗИ.

Хранение инсталлирующих СКЗИ носителей допускается в одном хранилище с другими документами при условиях, исключающих непреднамеренное их уничтожение или иное, не предусмотренное правилами пользования СКЗИ применение.

В случае отсутствия у сотрудника индивидуального хранилища инсталлирующие СКЗИ носители по окончании рабочего дня должны сдаваться лицу, ответственному за их хранение.

В случае утери носителя СКЗИ или вероятном копировании сотрудник обязан немедленно сообщить об этом лицу, ответственному за обеспечение безопасности при обращении с СКЗИ.

Ответственным за эксплуатацию СКЗИ периодически должен проводиться контроль сохранности и работоспособности установленного СКЗИ, а также всего используемого совместно с СКЗИ программного обеспечения для предотвращения внесения программно-аппаратных закладок и вирусов.

4.Ответственность за нарушение требований Инструкции

За нарушение требований настоящей Инструкции виновные лица несут дисциплинарную, либо материальную ответственность в зависимости от характера нарушения и тяжести наступивших отрицательных последствий.

Приложение № 32

УТВЕРЖДЕНА
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

ИНСТРУКЦИЯ ПО ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Настоящая Инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах персональных данных (далее – ИСПДн) Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области (далее – администрации), а также контроль за действиями пользователей и обслуживающего персонала ИСПДн при работе с паролями.

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн администрации и контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями возлагается на ответственного за организацию обработки ПДн, являющегося специалистом по защите информации.

2. Личные пароли выбираются пользователями автоматизированной системы самостоятельно либо могут генерироваться и распределяться централизованно с учетом следующих требований:

- длина пароля должна быть не менее 6 символов;
- в числе символов пароля обязательно должны присутствовать буквы латинского алфавита в верхнем и нижнем регистрах и цифры, а также могут использоваться специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии пользователей, наименования АРМ, учетные записи и т.д.), а также общепринятые сокращения (USER, PASSWORD, MANAGER и т.п. и производные от них);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 3 позициях.

3. Владельцы паролей должны быть ознакомлены под роспись с настоящей инструкцией по форме согласно приложению и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

4. При наличии (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п.) технологической необходимости использования имен и паролей некоторых сотрудников в их отсутствие, такие сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте передавать на хранение ответственному за организацию обработки ПДн. Опечатанные конверты (пеналы) с паролями исполнителей должны храниться в сейфе.

5. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в месяц.

6. Внеплановая смена личного пароля или удаление учетной записи пользователя информационной системы в случае прекращения его полномочий (увольнение, переход на другую работу) должна производиться ответственным за организацию обработки ПДн, ответственным за организацию парольной защиты, немедленно после окончания последнего сеанса работы данного пользователя с системой.

7. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение и другие обстоятельства) ответственного за организацию обработки ПДн, ответственного за организацию парольной защиты, и других сотрудников, которым по роду служебной деятельности были предоставлены полномочия по управлению парольной защитой ИС.

8. В случае компрометации личного пароля пользователя информационной системы должны быть немедленно предприняты меры в соответствии с пунктом 4 или пунктом 5 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

9. Хранение сотрудником значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у Ответственного за организацию обработки ПДн, ответственного за организацию парольной защиты, или начальника отдела в опечатанном виде.

10. Каждый пользователь несет ответственность за неразглашение личного пароля третьим лицам и сохранность персонального идентификатора.

11. Повседневный контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на начальников отделов, периодический контроль возлагается на ответственного за организацию обработки ПДн, ответственного за организацию парольной защиты.

Приложение № 33

УТВЕРЖДЕНЫ
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

ПРАВИЛА ОЦЕНКИ ВРЕДА, КОТОРЫЙ МОЖЕТ БЫТЬ ПРИЧИНЕН СУБЪЕКТАМ ПЕРСОНАЛЬНЫХ ДАННЫХ В СЛУЧАЕ НАРУШЕНИЯ ТРЕБОВАНИЙ ПО ОБРАБОТКЕ И ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

1.1. Настоящие правила оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в администрации сельского поселения Красный Яр, (далее - Правила) определяют порядок оценки вреда, который может быть причинён субъектам персональных в случае нарушения Федерального закона N 152-ФЗ "О персональных данных" (далее - Закон N 152-ФЗ), и отражают соотношение указанного возможного вреда и принимаемых администрацией поселения (далее - Оператор) мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом N 152-ФЗ.

1.2. Настоящие Правила разработаны в соответствии с действующим законодательством Российской Федерации в области обработки и защиты персональных данных.

2. Основные понятия

В настоящих Правилах используются основные понятия приведенные в Гражданском кодексе Российской Федерации, в Федеральном законе от 27.07.2006 1149-ФЗ "Об информации, информационных технологиях и о защите информации" и в Федеральном законе от 27.07.2006 152-ФЗ "О персональных данных".

3. Методика оценки возможного вреда субъектам персональных данных

3.1. Вред субъекту персональных данных возникает в результате неправомерного или случайного доступа к персональным данным, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

3.2. Перечисленные неправомерные действия определяются как следующие нарушения безопасности информации:

нарушение конфиденциальности персональных данных:

неправомерное предоставление, распространение и копирование персональных данных;

обработка персональных данных, выходящая за рамки установленных целей обработки, в объеме больше необходимого;

неправомерное получение персональных данных от лица, не являющегося субъектом персональных данных;

принятие решения, порождающего юридические последствия в отношении субъекта персональных данных или иным образом затрагивающего права и законные интересы, на основании исключительно автоматизированной обработки его персональных данных без согласия на то в письменной форме субъекта персональных данных или не предусмотренного федеральными законами;

нарушение доступности персональных данных:

нарушение права субъекта на получение информации, касающейся обработки его персональных данных;

неправомерное уничтожение и блокирование персональных данных;

нарушение целостности персональных данных:

неправомерное изменение персональных данных;

нарушение права субъекта требовать от Оператора уточнения его персональных данных, их блокирования или уничтожения.

3.4. Вред, который может быть причинен субъекту персональных данных, определяется в виде:

убытков - расходов, которые субъект персональных данных, чье право нарушено, понесло или должно будет понести для восстановления нарушенного права, утраты или повреждения его имущества (реальный ущерб);
недополученного дохода, который этот субъект персональных данных получил бы при обычных условиях гражданского оборота, если бы его право не было нарушено;

морального вреда - физических или нравственных страданий, причиняемых действиями, нарушающими личные неимущественные права субъекта персональных либо посягающими на принадлежащие субъекту персональных данных другие нематериальные блага, а также в других случаях, предусмотренных законом.

3.4. В оценке возможного вреда необходимо исходить из следующего способа учета последствий допущенного нарушения принципов обработки персональных данных:

низкий уровень возможного вреда - последствия нарушения принципов обработки персональных данных включают только нарушение целостности персональных данных, либо только нарушение доступности персональных данных;

средний уровень возможного вреда - последствия нарушения принципов обработки персональных данных включают только нарушение целостности персональных данных, повлекшее убытки и моральный вред, либо только нарушение доступности персональных данных, повлекшее убытки и моральный вред, либо только нарушение конфиденциальности персональных данных;

высокий уровень возможного вреда - во всех остальных случаях.

4. Порядок проведения оценки возможного вреда, а также соотнесения возможного вреда и реализуемых Оператором мер

Оценка возможного вреда проводится для исполнения требований к защите персональных данных при их обработке в информационной системе персональных данных (далее - ИСПДн), в частности, при определение типа актуальных угроз безопасности персональных данных при их обработке в ИСПДн во исполнение п. 5 ч. 1 ст. 18.1 Закона N 152-ФЗ.

Оценка возможного вреда субъектам персональных данных и состав реализуемых Оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом N 152-ФЗ, осуществляется должностными лицами управления информационных технологий, связи и документооборота администрации области в соответствии с методикой оценки возможного вреда субъектам персональных данных, определенной в разделе 3 настоящих Правил, и на основании оценки вреда, который может быть причинен субъектам персональных данных, а также соотнесения возможного вреда и реализуемых Оператором мер, приведенных в приложении к Правилам, исходя из правомерности и разумной достаточности указанных мер. При необходимости допускается привлечение сторонних экспертов в области защиты информации.

Приложение
к правилам оценки вреда, который может
быть причинён субъектам персональных данных
в случае нарушения требований по обработке и
обеспечению безопасности персональных данных
в администрации поселения.

ОЦЕНКА ВРЕДА, КОТОРЫЙ МОЖЕТ БЫТЬ ПРИЧИНЕН СУБЪЕКТАМ ПЕРСОНАЛЬНЫХ ДАННЫХ, А ТАКЖЕ СООТНЕСЕНИЕ ВОЗМОЖНОГО ВРЕДА И РЕАЛИЗУЕМЫХ ОПЕРАТОРОМ МЕР

При определении уровня возможного вреда необходимо учитывать, что сами по себе нарушения целостности и доступности могут принести наименьший вред субъекту персональных данных, так как субъект персональных данных может и имеет право требовать восстановления целостности и доступности.

Если такое правомочие субъекта персональных данных затруднено, считается, что имеется основание для судебного иска, поэтому нарушение целостности или доступности, повлекшие моральный вред или ущерб, отнесены к среднему уровню вреда.

Если нарушение конфиденциальности потенциально необратимо (ставшие публичными данные невозможно снова сделать конфиденциальными), то даже в случае, если оно не повлекло причинение морального вреда субъекту персональных данных, такое нарушение относится к среднему уровню возможного вреда.

Если нарушения конфиденциальности повлекли за собой моральный ущерб и убытки, то такие нарушения относятся к наивысшему уровню возможного вреда.

Таблица

Оценка уровня возможного вреда

Требования Федерального закона от 27.07.2006 152-ФЗ "О персональных данных", которые могут быть нарушены	Возможные нарушения безопасности информации и причиненный субъекту вред		Уровень возможного вреда	Принимаемые меры по обеспечению выполнения обязанностей Оператора персональных данных
1	2		3	4
1. Порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых	Убытки и моральный вред	+	высокий	В соответствии с законодательством в области защиты информации и Положением по обеспечением безопасности персональных данных

обеспечивает установленные уровни защищенности персональных данных				
	Целостность			
	Доступность			
	Конфиденциальность	+		
2. Порядок и условия применения средств защиты информации	Убытки и моральный вред	+	средний	В соответствии с технической документацией на систему защиты информационной системы персональных данных
	Целостность	+		
	Доступность			
	Конфиденциальность			
3. Эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных	Убытки и моральный вред	+	высокий	Программа и методика испытаний систем защиты
	Целостность	+		
	Доступность	+		
	Конфиденциальность	+		
4. Состояние учета машинных носителей персональных данных	Убытки и моральный вред			Инструкция по учету машинных носителей информации
	Целостность			
	Доступность			
	Конфиденциальность			
5. Соблюдение правил доступа к персональным данным	Убытки и моральный вред	+	высокий	В соответствии с принятыми организационными мерами и в соответствии с системой разграничения доступа
	Целостность	+		
	Доступность			
	Конфиденциальность	+		
6. Наличие (отсутствие) фактов несанкционированного	Убытки и моральный вред	+	высокий	Мониторинг средств защиты информации на

доступа к персональным данным и принятие необходимых мер				наличие фактов доступа к персональным данным
	Целостность			
	Доступность			
	Конфиденциальность	+		
7. Мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним	Убытки и моральный вред		средний	Применение резервного копирования
	Целостность	+		
	Доступность	+		
	Конфиденциальность			
8. Осуществление мероприятий по обеспечению целостности персональных данных	Убытки и моральный вред		низкий	Организация режима доступа к техническим и программным средствам
	Целостность	+		
	Доступность			
	Конфиденциальность			

Приложение № 34

УТВЕРЖДЕНА
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

ТИПОВАЯ ФОРМА РАЗЪЯСНЕНИЯ СУБЪЕКТУ ПЕРСОНАЛЬНЫХ ДАННЫХ ЮРИДИЧЕСКИХ ПОСЛЕДСТВИЙ ОТКАЗА ПРЕДОСТАВИТЬ СВОИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

В соответствии с требованиями Федерального закона Российской Федерации от 27.06.2006 №152-ФЗ «О персональных данных» уведомляем Вас, что обязанность предоставления Вами персональных данных администрации установлена статьями 16, 29, 30 Федерального закона от 02.03.2007 № 25-ФЗ «О муниципальной службе в Российской Федерации», Законом Самарской области от 09.10.2007 № 96-ГД «О муниципальной службе в Самарской области» в связи с поступлением или прохождением муниципальной службы (работы).

Без представления Вами обязательных для заключения трудового договора (контракта) сведений, трудовой договор (контракт) не может быть заключен.

На основании пункта 11 части 1 статьи 77 Трудового кодекса Российской Федерации от 30.12.2001 № 197-ФЗ трудовой договор (контракт) прекращается вследствие нарушения установленных обязательных правил его заключения, если это нарушение исключает возможность замещения должности муниципальной службы (работы).

«___» _____ 20__ г. _____ _____ _____
подпись проводившего разъяснение ФИО

Мне, _____,
(указываются полностью фамилия, имя, отчество (при его наличии); сотрудника) наименование и реквизиты
_____
документа, удостоверяющего личность; серия, номер, дата выдачи, наименование органа и код подразделения органа(при его наличии), выдавшего документ)

зарегистрированному(ой) по месту жительства по адресу:_____
_____
разъяснены юридические последствия отказа предоставить свои персональные данные (далее – персональные данные) Администрации сельского поселения Красный Яр , а равно подписать согласие на обработку персональных данных по типовой форме такого согласия, предусмотренного для сотрудников, а также иных субъектов персональных данных, или отзыва указанного согласия.

2. Я предупрежден(а) о том, что в случае моего отказа предоставить персональные данные Администрация сельского поселения Красный Яр не сможет осуществлять их обработку.

3. Мне также известно, что Администрация сельского поселения Красный Яр, в целях реализации функций, полномочий и обязанностей в установленной сфере деятельности в соответствии с законодательством Российской Федерации, имеет право запрашивать мои персональные данные у третьих лиц, а также осуществлять их обработку без моего согласия при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

4. Настоящее разъяснение заполнено и подписано мною собственноручно.

«___» _____ 20__ г. _____ _____ _____
подпись ФИО

Приложение № 35

УТВЕРЖДЕНО
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПОСЕТИТЕЛЕЙ ВЕБ-САЙТА АДМИНИСТРАЦИИ СЕЛЬСКОГО ПОСЕЛЕНИЯ КРАСНЫЙ ЯР МУНИЦИПАЛЬНОГО РАЙОНА КРАСНОЯРСКИЙ САМАРСКОЙ ОБЛАСТИ

Настоящее Положение об обработке и защите персональных данных посетителей веб-сайта Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области (далее – Администрация) действует в отношении всех информационных данных, которые расположены на доменном имени https://kryarposelenie.ru , и которые сайт Администрации может получить о Пользователе во время использования им веб-сайта.

Отношения, связанные со сбором, хранением, распространением и защитой информации о посетителях веб-сайта https://kryarposelenie.ru, регулируются настоящим Положением, иными официальными документами Администрации веб-сайта и действующим законодательством Российской Федерации.

Общие положения

1.1. Использование веб-сайта Клиники https://kryarposelenie.ru (далее – сайт) Посетителем (регистрируясь, отправляя сообщения, заявки, иные послания (действия) с помощью средств и форм связи на сайте, Посетитель выражает свое согласие с условиями настоящего Положения об обработке и защите персональных данных посетителей веб-сайта Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области (далее — Положение).

1.2. В случае несогласия Посетителя с условиями настоящего Положения использование Сайта и его сервисов должно быть немедленно прекращено Посетителем. Ответственность за это несёт сам Посетитель.

1.3. Данное Положение применяется исключительно к сайту Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области . Клиника не несёт ответственность за сайты третьих лиц, на которые Посетитель может перейти по ссылкам, расположенным на сайте Администрации.

1.4. Администрация сайта не проверяет достоверность получаемой (собираемой) информации о Посетителях, за исключением случаев, когда такая проверка необходима в целях исполнения Администрацией сайта обязательств перед Посетителем.

1.5. Обработка персональных данных осуществляется на основе следующих принципов:

1.5.1. Законности целей и способов обработки персональных данных.

1.5.2. Добросовестности.

1.5.3. Соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Администрации.

1.5.4. Соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных.

2. Состав персональных данных, предоставляемых Посетителем, при посещении веб-сайта Администрации

2.1. Персональные данные — идентификационная информация, которая относится к Посетителю:

2.1.1. По форме «Отправка обращения»: фамилия, имя, отчество, телефон, адрес электронной почты, адрес регистрации, адрес проживания.

2.1.2. Администрация сайта обрабатывает также иную информацию о Посетителях, которая включает в себя:

2.1.2.1. Стандартные данные, автоматически получаемые сервером при доступе к сайту и последующих действиях Посетителя (IP-адрес хоста, вид операционной системы пользователя, страницы сайта, посещаемые пользователем).

2.1.2.2. Информация, автоматически получаемая при доступе к сайту с использованием закладок (cookies).

2.1.2.3. Информация, полученная в результате действий Посетителя на сайте.

2.1.2.4. Информация, полученная в результате действий других посетителей на сайте.

2.1.3. Остальные персональные данные, предоставляются Посетителем дополнительно по собственной инициативе с использованием соответствующих разделов и ресурсов сайта.
2.2. Предоставляя свои персональные данные на сайте, Посетитель дает согласие на их обработку Администрацией в течение неограниченного срока, до письменного отзыва посетителем.
2.3. Обработка персональных данных Посетителя подразумевает использование данных в целях исполнения Администрацией своих обязательств перед Посетителем, указанных в настоящем Положении.

3. Цели обработки персональных данных

3.1. Администрация использует персональные данные, предоставленные Посетителем на сайте, строго в ряде целей:
- установление обратной связи с Посетителем и обработка его заявок и запросов;
- уведомление Посетителя о статусе обработки заявок, запросов, обращений;
- предоставление Посетителю персональной технической поддержки в случае возникновения вопросов, связанных с использованием сайта;

4. Правила использования персональных данных

4.1. Администрация гарантирует использование предоставленной/размещенной Посетителем персональной информации при использовании сайта строго в целях, указанных в настоящем Положении. Администрация обязуется не передавать полученные данные третьим лицам без согласия Посетителя.
4.2. Дополнительно с персональными данными Администрация сайта (узнает IP-адрес Посетителя и получает информацию, с какого Интернет-ресурса он перешел на сайт. Данная информация не используется для установления личности посетителя сайта.

5. Защита персональных данных

5.1. Администрация сайта принимает необходимые и достаточные меры для защиты персональной информации Посетителя от случайного или умышленного неправомерного доступа, распространения и иных незаконных действий посторонних лиц.
5.2. Администрация обеспечивает надежное хранение персональной информации Посетителя, не разглашает данные без его предварительного разрешения и не осуществляет опубликование данных за исключением случаев, указанных в пункте 7.2 настоящего Положения.
5.3. В случае утраты или разглашения персональных данных Администрация совместно с Посетителем принимает все необходимые меры по предотвращению убытков и других отрицательных последствий.

6. Хранение, передача и использование персональных данных

6.1. Персональные данные Пользователей хранятся исключительно на электронных носителях и обрабатываются с использованием автоматизированных систем, за исключением случаев, когда неавтоматизированная обработка персональных данных необходима в связи с исполнением требований законодательства и ответа на обращение Посетителя.
6.2. Персональные данные Пользователей не передаются каким-либо лицам, за исключением случаев, прямо предусмотренных настоящим Положением.
6.3. Приложения, используемые Посетителями на Сайте, размещаются и поддерживаются третьими лицами (разработчиками), которые действуют независимо от Администрации сайта и не выступают от имени или по поручению Администрации. Пользователи обязаны самостоятельно ознакомиться с правилами оказания услуг и политикой защиты персональных данных таких третьих лиц (разработчиков) до начала использования соответствующих приложений.
6.4. Предоставление персональных данных Пользователей по запросу государственных органов (органов местного самоуправления) осуществляется в порядке, предусмотренном действующим законодательством Российской Федерации.

7. Ответственность

7.1. В случае невыполнения обязательств Администрация несёт ответственность за убытки, понесённые Посетителем в связи с неправомерным использованием персональных данных последнего в соответствии с законодательством РФ за исключением случаев, предусмотренных пунктом 7.2 настоящего Положения.
7.2. Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области не несёт ответственности за информацию, предоставленную Посетителем на сайте в общедоступной форме и данные, разглашённые с согласия Посетителя.

8. Иные положения

8.1. Администрация вправе вносить изменения в настоящее Положение без уведомления Посетителя и без его согласия. Изменения вносятся на основании Распоряжения Главы поселения.
8.2. Настоящее Положение, является публичным документом, доступно любому Посетителю сети Интернет, и размещено на официальном веб-сайте Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области по адрес: https://kryarposelenie.ru

8.3. Предложения или вопросы связанные с настоящим Положением можно сообщить любым удобным способом на сайте: https://kryarposelenie.ru
8.4. Настоящее Положение вступает в силу с момента его утверждения и вводится в действие распоряжение Главы сельского поселения Красный Яр.
8.5. Действие настоящего Положения не распространяется на действия и Интернет-ресурсы третьих лиц.
8.6. Администрация не несет ответственности за действия третьих лиц, получивших в результате использования Интернета или услуг сайта доступ к информации о Пользователе и за последствия использования информации, которая, в силу природы сайта, доступна любому посетителю сети Интернет.
8.7. Администрация рекомендует Посетителям ответственно подходить к решению вопроса об объеме информации о себе, передаваемой с сайта.

9. Уничтожение персональных данных

9.1. Персональные данные Посетителя уничтожаются по письменной просьбе Посетителя. Просьба должна содержат идентификационные данные, которые прямо указывает на принадлежность информации данному Посетителю.

ЛИСТ ОЗНАКОМЛЕНИЯ С ДОКУМЕНТАМИ ПО ЗАЩИТЕ И ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В АДМИНИСТРАЦИИ СЕЛЬСКОГО ПОСЕЛЕНИЯ КРАСНЫЙ ЯР
