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	