УТВЕРЖДАЮ
Председатель администрации
Тес-Хемского кожууна
_____ / Т.С. Самдан /
«17» февраля 2021 г.

ИНСТРУКЦИЯ
по резервному копированию защищаемой информации в информационных системах персональных данных

1. Общие положения

Настоящий документ определяет порядок осуществления резервного копирования информационных ресурсов информационных систем персональных данных (ИСПДн) Администрации Тес-Хемского кожууна Республики Тыва.

Процесс резервного копирования обеспечивает сохранение на резервных носителях информации, с целью её 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 «Инструкции по обеспечению правил информационной безопасности при работе в информационных системах» (далее – Инструкция).

Резервное копирование осуществляется системным администратором и контролируется ответственным заместителем председателя, курирующим вопросы информационной безопасности.

Должностные лица, задействованные в осуществлении резервного копирования информационных ресурсов ИСПДн, знакомятся с основными положениями Инструкции в части, их касающейся, по мере необходимости.

2. Периодичность и схема резервного копирования

При осуществлении резервного копирования используется два типа копирования: полное резервное копирование и инкрементальное резервное копирование.

Резервное копирование информационных ресурсов ИСПДн осуществляется 15-16 числа каждого месяца.

3. Порядок резервного копирования

Системный администратор 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 системный администратор проверяет доступность резервного носителя, а также наличие на нем свободного места для записи данных.

После завершения выполнения задачи резервного копирования системный администратор должен извлечь резервный носитель, подписать его по формату и поместить в сейф, расположенный в отделе правового и кадрового обеспечения.

4. Хранение резервных копий

Хранение резервных копий должно быть организовано в отдельном от копируемых информационных ресурсов помещении.

Резервные носители должны храниться в кассетах или закрытых коробках на безопасном расстоянии от источников магнитных полей: блоков питания, мониторов, телефонов и т.п.

Доступ к хранилищу резервных копий должны иметь только системный администратор, начальник отдела и ответственный заместитель председателя, курирующий вопросы информационной безопасности.

5. Восстановление после сбоя

В случае потери данных на основном носителе из хранилища извлекается накопитель с резервной копией информационных ресурсов, нуждающихся в восстановлении, от последнего произведенного резервного копирования.

В зависимости от характера и уровня повреждения информационных ресурсов, системный администратор восстанавливает либо весь массив резервных данных, либо отдельные поврежденные или уничтоженные файлы и папки.

6. Порядок пересмотра Инструкции

Инструкция подлежит полному пересмотру при изменении перечня решаемых задач, состава технических и программных средств ИСПДн, приводящих к существенным изменениям технологии обработки информации.

Инструкция подлежит частичному пересмотру в остальных случаях. Частичный пересмотр проводится ответственным за обеспечение безопасности ПДн.

Вносимые изменения не должны противоречить другим положениям Инструкции.

7. Ответственные за выполнение Инструкции

Ответственность за выполнение резервного копирования и восстановление данных из резервных копий, а также за соблюдение периодичности и порядка выполнения резервного копирования возлагается на системного администратора.

Ответственность за сохранность резервных копий возлагается на начальника отдела.

Ответственным за постоянный контроль выполнения требований данной Инструкции является ответственный заместитель председателя, курирующий вопросы информационной безопасности.