

Приложение № 9
К приказу Директора МБОУ СОШ
д.Султанбеково МР Аскинский район РБ
от 21.11.2018 г. № 8800

Регламент резервного копирования данных ИСПДи

Общие положения

Настоящий Регламент проведения резервного копирования (восстановления) программ и данных, хранящихся на серверах и персональных компьютерах к приказу Директора МБОУ СОШ д.Султанбеково МР Аскинский район РБ (далее – Оператор) разработан с целью:

- определения порядка резервирования данных для последующего восстановления работоспособности информационной системы персональных данных (ИСПДн) Оператора при полной или частичной потере информации, вызванной сбоями или отказами аппаратного или
- программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);
- определения порядка восстановления информации в случае возникновения такой необходимости;
- упорядочения работы должностных лиц, связанной с резервным копированием и восстановлением информации;

В настоящем документе регламентируются действия при выполнении следующих мероприятий:

- резервное копирование;
- контроль резервного копирования;
- хранение резервных копий;
- полное или частичное восстановление данных и приложений.

Резервному копированию подлежат информация следующих основных категорий:

- персональная информация пользователей;
- групповая информация пользователей;
- информация, необходимая для восстановления серверов и систем управления базами данных (далее – СУБД);
- персональные профили пользователей сети;
- информация автоматизированных систем, в т.ч. базы данных;
- рабочие копии установочных компонент программного обеспечения рабочих станций;
- регистрационная информация системы информационной безопасности автоматизированных систем.

Машинные носители, содержащие резервные копии, маркируются и регистрируются в «Журнале учета хранилищ носителей персональных данных».

1. Порядок резервного копирования

- состав и объем копируемых данных, периодичность проведения резервного копирования (из Перечня резервируемых данных - по форме, приведенной в Приложении №1);
- минимальный срок хранения резервных копий - 3 месяца;
- резервные копии хранятся на машинных носителях, отличных от носителей, содержащих исходную информацию;
- минимальное количество резервных копий - три, сделанные последовательно, с интервалом не менее месяца.

Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации, указанной в Перечне (Приложение №1), в установленные сроки и с заданной периодичностью. Методика проведения резервного копирования описана в Приложении №2.

О выявленных попытках несанкционированного доступа к резервируемой информации, а также иных нарушениях информационной безопасности произошедших в процессе резервного копирования, должно быть немедленно сообщено ответственному за организацию обработки персональных данных Оператора.

2. Контроль результатов резервного копирования

Контроль результатов всех процедур резервного копирования осуществляется ответственным за организацию обработки персональных данных.

На протяжении периода времени, когда система резервного копирования находится в аварийном состоянии, должно осуществляться ежедневное копирование информации, подлежащей резервированию, с использованием средств файловых систем серверов, располагающих необходимыми объемами дискового пространства для её хранения.

3. Ротация носителей резервной копии

Система резервного копирования должна обеспечивать возможность периодической замены (выгрузки) резервных носителей без потерь информации на них, а также обеспечивать восстановление текущей информации ИСПДн в случае отказа любого из устройств резервного копирования. Все процедуры по загрузке, выгрузке носителей из системы резервного копирования, а также их перемещение, осуществляются ответственным за организацию обработки персональных данных. В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек.

Носители с персональными данными, которые перестали использоваться в системе резервного копирования, должны стираться (форматироваться) с использованием специального программного обеспечения, реализующим полное физическое уничтожение данных.

4. Восстановление информации из резервной копии

В случае необходимости, восстановление данных из резервных копий производится на основании Заявки пользователя ИСПДн. Процедура восстановления информации из резервной копии осуществляется в соответствии с методикой восстановления информации (Приложение №3). После поступления заявки, восстановление данных осуществляется в максимально сжатые сроки, ограниченные техническими возможностями системы, но не более одного рабочего дня.

Приложение №1

Перечень объектов ИСПДн, подлежащих резервному копированию

[illegible]

Ответственный за
организацию обработки
персональных данных

ПОДПИСЬ

/ _____ /
расшифровка подписи

Методика резервного копирования

Приложение №2

Для организации системы резервного копирования используется программное обеспечение (далее - ПО) _____ версии _____. С целью оптимизации расходов на развёртывание системы резервного копирования, запись резервной копии осуществляется на жёсткий диск. С помощью указанного ПО выполняются такие действия, как задание режимов и составление расписания резервного копирования клиентов, осуществляются операции по загрузке и выгрузке носителей информации, проводится контроль за состоянием выполнения заданий, запускаются процедуры восстановления информации. Для снижения совокупной нагрузки на информационную систему все операции по резервированию информации необходимо проводить в вечернее время.

Существуют три набора резервных копий:

1. Месячный набор. Записывается информация на первое число текущего месяца. Срок хранения – месяц. Хранится на сервере резервного копирования.
2. Недельная копия. Записывается в ночь на среду и в ночь на субботу. Срок хранения – субботняя копия – до следующей среды, вторничная копия – до субботы. Хранится на сервере.
3. Квартальный (или годовой) набор. Записывается информация в конце квартала или года, в зависимости от специфики деятельности. Максимальный срок хранения не устанавливается.

Различаются два принципиально разных источника информации, подлежащей резервированию:

1. Информация, хранящаяся непосредственно в файловой системе операционной системы.
2. Базы данных (под управлением СУБД).

Используемое для резервного копирования ПО должно быть сконфигурировано согласно настоящему Регламенту.

Для резервирования информации, хранимой в базах данных, в качестве промежуточного звена автоматизации используются средства конфигурирования СУБД и архиваторы. В результате работы промежуточного звена автоматизации формируется каталог с резервной копией данных Прикладной информационной системы. Посредством ПО резервного копирования формируются задания на проведение резервного копирования этого каталога. Данное ПО должно быть сконфигурировано согласно настоящему Регламенту.

Ответственный за
организацию обработки
персональных данных

_____ / _____
подпись

_____ / _____
расшифровка подписи

Примечание [E1]:

Методика восстановления данных

Приложение №3

Любое восстановление информации выполняется на основании заявки ответственному за организацию обработки персональных данных. В процессе восстановления резервной копии следует руководствоваться инструкциями по восстановлению информации из резервных копий, описанных в документации, прилагающейся к используемой системе резервного копирования.

Вне зависимости от требований инструкций к используемому ПО, перед каждым процессом восстановления СУБД и файлов из резервных копий, должно проводиться внеплановое резервное копирование информации, подлежащей замене из резервной копии.

Ответственный за
организацию обработки
персональных данных

подпись

расшифровка подписи

Примечание [E2]: