ПРИЛОЖЕНИЕ 4 к приказу
№___ от_____
об организационных мерах для
защиты персональных данных

ИНСТРУКЦИЯ ПО ОРГАНИЗАЦИИ РЕЗЕРВНОГО КОПИРОВАНИЯ

1. Общие положения

Настоящая инструкция проведения резервного копирования (восстановления) программ и данных, хранящихся на серверах и рабочих местах работников МБОУ Великооктябрьская СОШ, разработана с целью:

- определения порядка резервирования данных для последующего восстановления работоспособности автоматизированных систем 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 Учреждения, 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 подлежит информация следующих основных категорий:

- Конфигурационные файлы служб и сервисов МБОУ Великооктябрьская СОШ
- Конфигурации активного оборудования узла.
- Содержимое файловых и веб-серверов, требующее резервирования.
- Информация, необходимая для восстановления серверов и систем управления базами данных (далее – СУБД).

Ответственным сотрудником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, и за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации, является администратор локальной вычислительной сети.

2. Порядок резервного копирования

Резервное копирование автоматизированных систем производится на основании следующих данных:

- состав и объем копируемых данных, периодичность проведения резервного копирования (из Перечня резервируемых данных - по форме, приведенной в Приложении №1);
- максимальный срок хранения резервных копий - 3 года.

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

3. Методика проведения резервирования

Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха. Все критичные помещения (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации.

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания.

Способы обеспечения отказоустойчивости:

- Копирование файлов;
- Создание полные образов системы;
- Программная и программно-аппаратная кластеризация;
- Виртуализация;
- Применение технологии RAID;
- Контрольные точки восстановления.

Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель (жесткий диск и т.п.).

Для повышения отказоустойчивости сервисов может использоваться штатные механизмы резервирования, основанные на репликациях и синхронизациях данных между двумя копиями программного обеспечения, запущенными на разных физических серверах. Например, использование резервного контроллера домена, кластеризация MS SQL Server.

Для предотвращения нарушений в работе системного программного обеспечения должна

быть настроена процедура автоматического создания контрольных точек восстановления, что обеспечивает возможность отката операционной системы в рабочее состояние.

Для организации системы резервного копирования используются системные утилиты СУБД MS SQL Server, штатные функции ОС MS Windows Server 2008 R2, ОС Linux.

При создании резервных копий с конфиденциальной информацией, к ним предъявляются такие же требования по информационной безопасности как и к элементам данной ИСПДн, указанных в соответствующих инструкциях и положениях.

Хранение резервных копий данных должно соответствовать документу «Инструкция по учету и хранению машинных носителей». Съемные носители информации с резервными копиями конфиденциальных данных должны храниться в опечатываемом сейфе. Доступ лиц должен быть ограничен в соответствии с документом «Правила разграничения доступа к защищаемым информационным ресурсам ИСПДн».

Должен вестись журнал учета носителей информации, используемых для хранения конфиденциальной информации.

Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования и т.д., что в свою очередь отражается в Журнале учета носителей информации (Приложение №1 к инструкции по учету и хранению машинных носителей как носителей конфиденциальной информации).

Носители должны храниться не менее года, для возможности восстановления данных.

Для создания образов дисков рекомендуется использовать дополнительное программное обеспечение, например, Acronic True Image.

4. Контроль результатов резервного копирования

Контроль результатов всех процедур резервного копирования осуществляется ответственными должностными лицами. Обязанности по выполнению процедур резервного копирования заносятся в должностные инструкции ответственного лица.

Обязанности:

- Создание, настройка, доработка системы резервного копирования.
- Внесение существенных изменений в настройку системы резервного копирования.
- Контроль выполнения процедур резервирования, анализ логов резервного копирования, отслеживание необходимости изменений настроек резервного копирования, обеспечение ротирования носителей.
- Ротирование носителей, проверка корректности резервной копии.

Контроля автоматизированных процедур резервного выполняется еженедельно.

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.

5. 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 в случае отказа любого из устройств резервного копирования.

В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек. Конфиденциальная информация с носителей, которые перестают использоваться в системе резервного копирования, должна удаляется без возможности восстановления.

6. Восстановление информации из резервных копий

Любое восстановление информации, не вызванное необходимостью экстренного восстановления, связанной с потерей работоспособности информационной системы или ее компонент, выполняется на основании заявки.

В процессе восстановления резервной копии следует руководствоваться инструкциями по восстановлению информации из резервных копий, описанных в документации, прилагающейся к системе резервного копирования. Восстановление данных осуществляется в максимально сжатые сроки, ограниченные техническими возможностями системы, но не более одного рабочего дня.

Приложение №1
к инструкции по организации резервного копирования

Перечень резервируемой информации

№	Информационный ресурс	Объект копирования	Периодичность
1			
2			
3			
4			
5			
6			
7			
8			