

Принято педагогическим советом

Утверждаю

МОУ Большесельской СОШ

Директор МОУ Большесельской СОШ

Протокол № 12 от 19.12.2014

Приказ № 540 от 19.12.2014



Дьячкова Е.Ю.

## Порядок

### **резервирования и восстановления работоспособности информационных систем персональных данных МОУ Большесельской СОШ**

#### *1. Общие положения*

1.1. Настоящий Порядок устанавливает основные требования к организации резервного копирования (восстановления) программ и данных, хранящихся в базах данных на серверах МОУ Большесельской СОШ, а также к резервированию аппаратных средств.

1.2. Настоящий Порядок разработан с целью:

- определения категории информации, подлежащей обязательному резервному копированию;
- определения процедуры резервирования данных для последующего восстановления работоспособности информационных 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 и определения ответственности должностных лиц, связанной с резервным копированием и восстановлением информации.

1.3. Под резервным копированием информации понимается создание избыточных копий защищаемой информации в электронном виде для быстрого восстановления работоспособности информационных систем персональных данных (ИСПДн) в случае возникновения аварийной ситуации, повлекшей за собой повреждение или утрату данных.

1.4. Резервному копированию подлежат информация следующих основных категорий:

- персональная информация пользователей (личные каталоги) и групповая информация на файловых серверах;
- информация, обрабатываемая пользователями в ИСПДн, а также информация, необходимая для восстановления работоспособности ИСПДн;
- рабочие копии установочных компонент программного обеспечения общего назначения и специализированного программного обеспечения ИСПДн, СУБД, серверов и рабочих станций;
- информация, необходимая для восстановления серверов и систем управления базами данных ИСПДн;
- другая информация ИСПДн, по мнению пользователей и администратора безопасности, являющаяся критичной для работоспособности ИСПДн.

1.5. К носителям информации, содержащим резервные копии, а также к резервируемым программным и аппаратным средствам допускаются только администраторы ИСПДн и администраторы безопасности ИСПДн. О выявленных попытках несанкционированного



доступа к резервируемой информации и аппаратным средствам, произошедших в процессе резервного копирования, сообщается ответственному за обработку ПДн в МОУ Большесельской СОШ служебной запиской в течение рабочего дня после обнаружения указанного события.

## **2. Общие требования к резервному копированию**

2.1. Архивное копирование резервируемой информации производится при помощи специализированных программно-аппаратных систем резервного копирования, программный и аппаратный состав которых обеспечивает выполнение требования к резервному копированию, приведенные в п. 1.4. Система резервного копирования обеспечивает производительность, достаточную для сохранения информации, указанной в п. 1.4, в установленные сроки и с заданной периодичностью.

2.2. Требования к техническому обеспечению систем резервного копирования:

- это комплекс взаимосвязанных технических средств, обеспечивающих процессы сбора, передачи, обработки и хранения информации, основывающийся на единой технологической платформе;

- имеет возможность расширения (замены) состава технических средств, входящих в комплекс, для улучшения их эксплуатационно-технических характеристик по мере возрастания объемов обрабатываемой информации.

2.3. Требования к программному обеспечению систем резервного копирования:

- программное обеспечение резервного копирования обеспечивает простоту процесса инсталляции, конфигурирования и сопровождения.

2.4. Сопровождение системы резервного копирования возлагается на уполномоченных работников, которые обязаны следить за работоспособностью программных и аппаратных средств, осуществляющих архивное копирование.

2.5. Хранение отдельных магнитных носителей архивных копий организуется в отдельном от используемых данных помещении. Физический доступ к архивным копиям строго ограничен. Контроль за физическим доступом возлагается на администратора безопасности.

2.6. Доступ к носителям архивных копий имеют только администраторы ИСПДн, которые несут персональную ответственность за сохранность архивных копий и невозможность ознакомления с ними лиц, не имеющих на то права.

2.7. Передача магнитных носителей с архивными копиями кому бы то ни было без документального оформления не допускается.

2.8. Уничтожение отделяемых магнитных носителей архивных копий производится установленным порядком в случае прихода их в негодность или замены типа носителя с обязательной записью в журнале их учета.

## **3. Ответственность за состояние резервного копирования**

3.1. Ответственность за периодичность и полноту резервного копирования, а также состояние системы резервного копирования возлагается на работников МОУ Большесельской СОШ, осуществляющих резервное копирование – администраторов ИСПДн.

3.2. Ответственность за контроль над своевременным осуществлением резервного копирования и соблюдением настоящего Порядка, а также за выполнением требований по хранению архивных копий и предотвращению несанкционированного доступа к ним возлагается на администратора безопасности.

## **4. Периодичность резервного копирования**

4.1. Резервное копирование специализированного программного обеспечения производится при его получении (если это предусмотрено инструкцией по его



применению и не противоречит условиям его распространения), а также при его обновлении и получении исправленных и обновленных версий.

4.2. Резервное копирование открытой информации делается не позднее чем через сутки после ее изменения, но не реже одного раза в месяц.

4.3. Информация (ПДн), содержащаяся в постоянно изменяемых базах данных МОУ Большесельской СОШ, сохраняется в соответствии со следующим графиком:

- ежедневно проводится копирование измененной и дополненной информации. Носители с ежедневной информацией должны храниться в течение недели;
- еженедельно проводится резервное копирование всей базы данных. Носители с еженедельными копиями хранятся в течение месяца;
- ежемесячно производится резервное копирование на специально выделенный носитель длительного хранения, информация на котором хранится постоянно.

4.4. Не реже одного раза в год на носители длительного хранения записывается информация, не относящаяся к постоянно изменяемым базам данных (приказы, распоряжения, открытые издания и т.д.).

### ***5. Контроль результатов резервного копирования***

5.1. Контроль результатов всех процедур резервного копирования осуществляется администраторами ИСПДн. В случае обнаружения ошибки лицо, ответственное за контроль результатов, сообщает администратору безопасности в течение текущего рабочего дня.

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

### ***6. Ротация носителей резервной копии***

6.1. Система резервного копирования обеспечивает возможность периодической замены (выгрузки) резервных носителей без потерь информации на них, а также обеспечивает восстановление текущей информации ИСПДн в случае отказа любого из устройств резервного копирования.

6.2. Все процедуры по загрузке, выгрузке носителей из системы резервного копирования осуществляются работником, ответственным за резервное копирование. В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек. Информация ограниченного доступа с носителей, которые перестают использоваться в системе резервного копирования, уничтожается.

### ***7. Восстановление информации из резервных копий***

7.1. В случае необходимости восстановление данных из резервных копий производится работником, ответственным за резервное копирование.

7.2. Восстановление данных из резервных копий происходит в случае ее исчезновения или нарушения вследствие несанкционированного доступа в систему, воздействия вирусов, программных ошибок, ошибок работников и аппаратных сбоев.

7.3. Восстановление системного программного обеспечения и программного обеспечения общего назначения производится с их носителей в соответствии с инструкциями производителя системным администратором.

7.4. Восстановление специализированного программного обеспечения производится с дистрибутивных носителей или их резервных копий в соответствии с инструкциями по установке или восстановлению данного программного обеспечения.

7.5. Восстановление информации, не относящейся к постоянно изменяемым базам данных, производится с резервных носителей. При этом используется последняя копия информации.

7.6. При частичном нарушении или исчезновении записей баз данных восстановление производится с последней ненарушенной ежедневной копии. Полностью информация восстанавливается с последней еженедельной копии, которая затем дополняется ежедневными частичными резервными копиями.