

Утверждено
Приказом МБОУ «СОШ
с.Никольское» МО «Енотаевский
район» № 1/56 от 01.09.2017 года



ИНСТРУКЦИЯ

**о порядке резервирования и восстановления работоспособности
технических средств, программного обеспечения и баз данных в
муниципальном бюджетном общеобразовательном учреждении «Средняя
общеобразовательная школа с.Никольское» муниципального образования
«Енотаевский район»**

416222, Астраханская обл., Енотаевский р-н, с.Никольское, Мичурина, д. 19

1. Назначение и область действия

1.1. Данная Инструкция определяет действия, связанные с мерами и средствами поддержания непрерывной работы и восстановления работоспособности информационных систем в муниципальном бюджетном общеобразовательном учреждении «Средняя общеобразовательная школа с.Никольское» муниципального образования Енотаевский район (далее – Школа).

1.2. Настоящая Инструкция регламентирует:

- меры защиты от потери информации;
- действия по восстановлению в случае потери информации.

1.3. Действие настоящей Инструкции распространяется на Администраторов информационных систем, ответственных за резервное копирование информации.

2. Меры обеспечения надежной работы и восстановления ресурсов при возникновении инцидентов

2.1. Технические меры.

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения Инцидентов, такие как:

- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Системы жизнеобеспечения ИСПДн включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

Все критичные помещения (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, должны

подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;
- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;
- резервные линии электропитания в пределах комплекса зданий;

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

2.2. Организационные меры.

2.2.1. Резервное копирование и хранение данных должно осуществляться на периодической основе:

- для обрабатываемых персональных данных – не реже раза в неделю или по требованию пользователя ИСПДн;
- для системной информации – не реже раза в месяц;
- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элемент ИСПДн каждый раз при внесении изменений в эталонные копии (выход новых версий).

2.2.2. Данные о проведении процедуры резервного копирования должны отражаться в специально созданном Журнале учета.

2.2.3. Носители, на которые произведено резервное копирование, должны быть пронумерованы номером носителя, датой проведения резервного копирования.

2.2.4. Носители должны храниться в негорючем шкафу или помещении, оборудованном системой пожаротушения.

2.2.5. Носители и резервные копии данных должны храниться не менее года для возможности восстановления данных.

3. Порядок проведения резервирования информации

3.1. Перед проведением процедуры резервного копирования необходимо убедиться в том, что все пользователи информационной системы завершили свою работу с информационной системой.

3.2. Резервирование информации в информационных системах персональных данных проводится при помощи штатных средств, поставляемых в составе специализированного программного обеспечения для построения информационной системы, либо, в случае отсутствия таковых, штатными средствами операционной системы или системы управления базами данных (при использовании таковой).

3.3. Все файлы, входящие в состав резервной копии, должны архивироваться в один архив с присвоением имени архива в формате время_дата (например 18.00_21.11.2011).

3.4. Архивация может производиться как штатными средствами, поставляемыми в составе специализированного программного обеспечения для построения информационной системы, так и сторонним программным обеспечением (например 7zip, WinRar).

3.5. Резервные копии должны сохраняться на носители, не входящие в состав технических средств информационной системы персональных данных (внешние жесткие диски, CD/DVD диски, flash диски).

3.6. После завершения процедуры резервного копирования информации и записи резервной копии на носитель, необходимо поместить носитель с резервной копией в специально отведённое для хранения место и проставить соответствующую отметку в Журнале.

4. Порядок проведения восстановления информации

4.1. Перед проведением процедуры восстановления информации необходимо убедиться в том, что все пользователи информационной системы завершили свою работу с информационной системой.

4.2. Восстановление информации следует проводить из наиболее актуальной резервной копии.

4.3. В случае, если специализированное программное обеспечение для построения информационной системы не позволяет работать с заархивированными резервными копиями, то перед восстановлением информации необходимо разархивировать файлы резервной копии при помощи стороннего программного обеспечения (например 7zip, WinRar).

4.4. Восстановление информации в информационных системах персональных данных проводится при помощи штатных средств, поставляемых в составе специализированного программного обеспечения для построения информационной системы, либо, в случае отсутствия таковых, штатными средствами операционной системы или системы управления базами данных (при использовании таковой).

4.5. После завершения процедуры восстановления необходимо убедиться в работоспособности информационной системы персональных данных.

4.6. В случае успешного восстановления оповестить пользователей информационной системы о возможности продолжения работы. В противном случае необходимо изучить документацию, прилагаемую к программному обеспечению либо обратиться в службу технической поддержки.

5. Ответственность

5.1. Работники, нарушившие требования данной Инструкции, несут ответственность в соответствии с действующим законодательством.

С настоящей Инструкцией о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения и баз данных в муниципальном бюджетном общеобразовательном учреждении «Средняя общеобразовательная школа с.Никольское» муниципального образования «Енотаевский район» ознакомлены:

Должность	Фамилия Имя Отчество	Дата и подпись
заместитель директора школы по УВР	Мамонтова Лариса Викторовна	01.09.2017г В.Мамон
главный бухгалтер	Вешетникова Наталья Алексеевна	01.09.2017г. Вешет
директор-производитель	Петринова Лариса Владимировна	01.09.2017г. Л.П.
инженер по охране труда	Чандраев Юрий Равильевич	01.09.2017г. Ю.Ч.
педагог-организатор	Евминова Тамара Аркадьевна	01.09.2017г. Т.Е.
бухгалтер	Павлюкова Модов Михаил.ович	01.09.2017г. М.П.
социальный педагог	Кусова Елена Александровна	01.09.2017г. Е.К.
заместитель директора школы по УВР	Егорова Оксана Алексеевна	01.09.2017г. О.Е.
заместитель директора школы по ВД	Иванова Юлия Александровна	01.09.2017г. И.И.
заместитель директора школы по АХЧ	Часедаева Светлана Георгиевна	01.09.2017г. С.Ч.
педагог - психолог	Мареева Лия Викторовна	01.09.2017г. Л.М.