

Инструкция по резервному копированию и восстановлению данных

I. Общие положения

1. Настоящая Инструкция по резервному копированию и восстановлению данных (далее – Инструкция), хранящихся на серверах и автоматизированных рабочих местах Муниципального автономного учреждения дополнительного образования «Дворец пионеров и школьников им. Н.К. Крупской г. Челябинска» (далее – МАУДО «ДПШ») разработана в соответствии с требованиями приказа ФСТЭК России «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18.02.2013 №21.

2. Настоящая Инструкция разработана с целью:

1) определения порядка резервирования данных для последующего восстановления работоспособности информационной системы (далее ИС) МАУДО «ДПШ» при полной или частичной потере информации, вызванной попытками несанкционированного доступа, сбоями или отказами аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);

2) определения порядка восстановления информации в случае возникновения такой необходимости;

3) упорядочения работы должностных лиц, связанной с резервным копированием и восстановлением информации.

3. В настоящем документе регламентируются действия при выполнении следующих мероприятий:

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

4. Если резервирование предполагает выгрузку на съемные носители информации, то такие носители должны учитываться в порядке, установленном «Инструкцией ответственного за обеспечение безопасности персональных данных в информационных системах».

II. Термины и определения

5. **Автоматизированное рабочее место (АРМ)** – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.

Информация – сведения (сообщения, данные) независимо от формы их представления (Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»).

Информационная система (ИС) – система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию.

Носитель информации – любой материальный объект или среда, используемый для хранения или передачи информации.

Программное обеспечение – все или часть программ, процедур, правил и соответствующей документации системы обработки информации (ISO/IEC 2382-1:1993).

Резервное копирование – процесс создания копии данных на носителе (дисковом массиве, магнитной ленте и т. д.), предназначенном для восстановления данных в оригинальном месте их расположения в случае их повреждения или разрушения.

Система резервного копирования – совокупность программного и аппаратного обеспечения, выполняющая задачу резервного копирования информации.

III. Порядок резервного копирования

6. Резервному копированию подлежат информация следующих основных категорий:

- данные (файлы и каталоги) на файловых серверах;
- базы данных, содержащие защищаемую информацию.

7. Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации, в установленные сроки и с заданной периодичностью.

8. 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 обеспечение безопасности персональных данных в информационных системах, либо ответственному за организацию обработки персональных данных МАУДО «ДПШ».

9. Для организации системы резервного копирования используются стандартные средства Windows.

10. Существуют следующие наборы резервных копий:

- 1) месячный набор. Записывается информация на первое число текущего месяца. Срок хранения – 1 (один) месяц.
- 2) недельная копия. Записывается в ночь на среду и в ночь на субботу. Срок хранения – субботняя копия – до следующей среды, вторничная копия – до субботы.
- 3) суточная копия. Записывается ежедневно в 12:00. Срок хранения – сутки.
11. Копии хранятся на сервере резервного копирования.
12. Для резервирования информации, хранимой непосредственно в файловых системах, используются стандартные средства Windows.
13. Для резервирования информации, хранимой в базах данных ИС МАУДО «ДПШ», в качестве промежуточного звена автоматизации используются средства конфигурирования ИС и архиваторы. В результате работы промежуточного звена автоматизации формируется каталог с резервной копией данных ИС. Посредством стандартных средств Windows формируются задания на проведение резервного копирования этого каталога.
14. При резервировании информации следует руководствоваться инструкциями, описанными в документации на систему резервного копирования ПО.

IV. Контроль результатов резервного копирования

15. Контроль результатов всех процедур резервного копирования осуществляется ответственным за обеспечение безопасности персональных данных в информационных системах.
16. 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.

V. Ротация носителей резервной копии

17. Система резервного копирования должна обеспечивать возможность периодической замены (выгрузки) резервных носителей без потерь информации на них, а также обеспечивать восстановление текущей информации ИС 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 обеспечение безопасности персональных данных в информационных системах. В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек.

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

VI. Восстановление информации из резервной копии

19. В случае необходимости, восстановление данных из резервных копий производится на основании заявки пользователя ИС. После поступления заявки, восстановление данных осуществляется в максимально сжатые сроки, ограниченные техническими возможностями системы, но не более 1 (одного) рабочего дня.

20. Любое восстановление информации выполняется на основании заявки пользователя ответственному за обеспечение безопасности персональных данных в информационных системах или в случае необходимости восстановления утерянной или повреждённой информации, подлежащей резервированию. В процессе восстановления резервной копии следует руководствоваться инструкциями по восстановлению информации из резервных копий, описанных в документации, на систему резервного копирования ПО.