

**МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ «ГОРЕЛЬСКАЯ СРЕДНЯЯ
ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА»**

Приказ

с. Горелое.

20.11.2024

№ 686

Об утверждении Положения «О порядке резервного копирования и восстановления информации»

В соответствии с требованиями Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07. 2006 № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Указом Президента РФ от 01.05.2022 №250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», нормативных и методических документов Федеральной службы по техническому и экспортному контролю Российской Федерации и Федеральной службы безопасности Российской Федерации, Уставом Организации

ПРИКАЗЫВАЮ:

1. Утвердить Положение «О порядке резервного копирования и восстановления информации в муниципальном бюджетном общеобразовательном учреждении «Горельская средняя общеобразовательная школа» (Приложение № 1).
2. Заместителю директора по ИКТ Матрохину А.А. разместить приказ на сайте образовательной организации организации.
3. Контроль за исполнением настоящего приказа оставляю за собой.

Директор школы

Е.И. Колодина

С приказом ознакомлен:

_____ Матрохин А.А.

Положение
о порядке резервного копирования и восстановления информации в
муниципальном бюджетном общеобразовательном учреждении
«Горельская средняя общеобразовательная школа»

1. Общие положения

1.1. Настоящее Положение «О порядке резервного копирования и восстановления информации в муниципальном бюджетном общеобразовательном учреждении «Горельская средняя общеобразовательная школа» (далее – Положение), хранящихся на серверах и автоматизированных рабочих местах (далее – АРМ) в муниципальном бюджетном общеобразовательном учреждении «Горельская средняя общеобразовательная школа» (далее - Организация), разработано в соответствии с требованиями Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07. 2006 № 152-ФЗ «О персональных данных», Указом Президента РФ от 01.05.2022 №250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», нормативных и методических документов Федеральной службы по техническому и экспортному контролю Российской Федерации и Федеральной службы безопасности Российской Федерации, Уставом Организации.

1.2. Настоящее Положение разработано с целью:

- определения порядка резервирования информации;
- определения порядка восстановления информации в случае ее искажения или утраты, в связи с попытками несанкционированного доступа, сбоями или отказами аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);
- упорядочения работы работников, связанной с резервным копированием и восстановлением информации.

1.3. В настоящем Положении определены действия при выполнении следующих мероприятий:

- резервное копирование;
- контроль резервного копирования; хранение резервных копий; восстановление информации.

2. Порядок резервного копирования

2.1. Резервному копированию подлежит информация следующих основных категорий:

- информация ограниченного доступа, в том числе ПДн (базы данных, файлы и каталоги), хранящаяся на АРМ Организации.

2.2. Резервное копирование/восстановление информации, хранящейся на серверах Организации, осуществляется штатными средствами операционных систем с использованием программного обеспечения Организации.

2.3. Контроль результата процедур резервного копирования, а также восстановление информации ограниченного доступа, хранящейся на АРМ Организации, осуществляет ответственный за обеспечение безопасности персональных данных в информационных системах Организации (далее – Ответственный).

2.4. Система резервного копирования должна обеспечивать возможность периодической замены (выгрузки) носителей резервных копий без потерь информации, а также обеспечивать восстановление информации в случае отказа любого из устройств резервного копирования.

2.5. В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек.

2.6. Резервное копирование/восстановление информации, хранящейся на АРМ Организации, осуществляется пользователями на учтенные съемные носители.

2.7. Необходимость и периодичность резервного копирования информации, хранящейся на АРМ Организации, а также срок хранения резервных копий такой информации на съемных носителях определяется пользователями самостоятельно.

2.8. Резервное копирование информации может осуществляться исключительно на съемные машинные носители информации, учтенные в журнале учета съемных носителей информации Организации.

2.9. Не допускается создание резервных копий на неучтенные и личные носители информации. При использовании съемных машинных носителей как носителей ПДн запись в журнале учета должна содержать отметку «Конфиденциально».

2.10. Хранение съемных машинных носителей ПДн должно осуществляться в сейфах (металлических шкафах), оборудованных внутренними замками и приспособлениями для опечатывания замочных скважин.

2.11. В случае отсутствия сейфа (металлического шкафа) у пользователя, осуществляющего хранение, допускается осуществлять хранение в сейфе Ответственного.

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

2.13. О выявленных попытках несанкционированного доступа к резервируемой информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, должно быть немедленно сообщено Ответственному.

3. Восстановление информации из резервной копии

3.1. В случае необходимости, восстановление информации, хранящейся на АРМ Организации, может производиться Ответственным на основании заявки пользователя.

3.2. В случае повреждения или утраты информации, хранящейся на АРМ Организации до начала восстановления их со съемного носителя пользователь должен определить причину утраты или повреждения файлов, содержащих ПДн.

3.3. Если повреждение или удаление информации вызвано действиями самого пользователя (непреднамеренное удаление файла), восстановление информации со съёмного носителя может осуществляться пользователем незамедлительно.

3.4. В случае повреждения файловой системы АРМ или работоспособности жесткого диска в результате системного сбоя АРМ пользователь должен обратиться к Ответственному. Перенос файлов из резервной копии может выполняться пользователем только после восстановления работоспособности АРМ.

3.5. В случае повреждения или утраты файлов, содержащих конфиденциальную информацию, в том числе ПДн, вследствие несанкционированного доступа (далее – НСД) к АРМ пользователь незамедлительно сообщает о данном факте Ответственному. Восстановление файлов из резервной копии может осуществляться только после проведения расследования инцидента безопасности НСД с соответствующим устранением угрозы дальнейших инцидентов НСД.

3.6. Если утрата файлов на АРМ произошла в результате вирусного заражения, восстановление файлов возможно только после выполнения мероприятий в соответствии с инструкцией антивирусной защиты Организации.

4. Заключительное положение

4.1. Настоящее Положение вступает в силу в силу с момента утверждения приказа руководителем Организации.

4.2. Срок действия настоящего Положения не ограничен.

4.3. По мере необходимости в настоящее Положение могут быть внесены дополнения и изменения в соответствии с законодательством РФ.