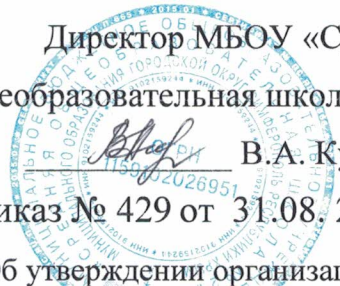


**МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 2» МУНИЦИПАЛЬНЫЙ
ОБРАЗОВАТЕЛЬНЫЙ ОКРУГ СИМФЕРОПОЛЬ РЕСПУБЛИКИ КРЫМ**

Принято на заседании
педагогического совета
Протокол № 12
От 30.08.2018 г.

УТВЕРЖДЕНО

Директор МБОУ «Средняя
общеобразовательная школа № 2»

 В.А. Кухнина

Приказ № 429 от 31.08.2018 г.

«Об утверждении организационно-
распорядительной документации по обработке
персональных данных в МБОУ «СОШ № 2» г.
Симферополя»

**Регламент
резервного копирования и восстановления данных
в МБОУ «СОШ №2» г. Симферополя**

1. Общие положения

Настоящий Регламент резервного копирования (восстановления) программ и данных в Муниципальном бюджетном общеобразовательном учреждении «Средняя общеобразовательная школа №2» (далее – МБОУ «СОШ №2» г. Симферополя, Оператор) разработан с целью:

- определения порядка резервирования данных для последующего восстановления работоспособности автоматизированных систем Оператора 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, связанной с резервным копированием и восстановлением информации.

В настоящем документе регламентируются действия при выполнении следующих мероприятий:

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

Резервному копированию подлежит информация следующих основных категорий:

- персональная информация пользователей;
- групповая информация пользователей;
- информация автоматизированных систем, в т.ч. баз данных;
- рабочие копии установочных компонент программного обеспечения рабочих станций.

2. Порядок резервного копирования

Резервное копирование информации, обрабатываемой в автоматизированных системах, производится на основании следующих данных:

- состав и объем копируемых данных, периодичность проведения резервного копирования;
- максимальный срок хранения резервных копий.

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

О выявленных попытках несанкционированного доступа к резервируемой информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, сообщается администратору информационной безопасности служебной запиской в течение рабочего дня после обнаружения указанного события. Ответственным является администратор информационной безопасности.

Резервное копирование осуществляется средствами ОС Windows путем копирования информации на учтенный съемный накопитель не реже 1 раза в 6 месяцев.

Резервному копированию подлежат базы данных, персональные данные работников МБОУ «СОШ № 2» г. Симферополя, обучающихся, их родителей или законных представителей, а также иная информация, необходимая для осуществления учебной и воспитательной деятельности.

Разные категории данных должны резервироваться на разных учтенных носителях.

Резервные копии должны храниться не менее 1 календарного года с момента создания.

3. Контроль результатов резервного копирования

Контроль результатов всех процедур резервного копирования осуществляется администратором информационной безопасности, в срок до 17

часов рабочего дня, следующего за установленной датой выполнения этих процедур.

В случае обнаружения ошибки, сбоя, или иных обстоятельств, не позволяющих осуществить резервное копирование, администратор информационной безопасности, сообщает о причинах директору до 18 часов текущего рабочего дня.

4. Ротация носителей резервной копии

Система резервного копирования должна обеспечивать возможность периодической замены (выгрузки) резервных носителей без потери информации на них, а также обеспечивать восстановление текущей информации автоматизированных систем в случае отказа любого из устройств резервного копирования. В случае необходимости замены испорченных носителей информации новыми, администратор информационной безопасности направляет служебную записку на имя директора о необходимости замены носителей, факт замены носителей учитывает в журнале учета резервного копирования. Все процедуры по загрузке, выгрузке носителей из системы резервного копирования осуществляются администратором информационной безопасности, с фиксацией действий в соответствующем журнале.

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

Информация с носителей, которые перестают использоваться в системе резервного копирования, должна стираться, путем многократного форматирования, без возможности восстановления информации.

Учтенные носители с резервными копиями должны храниться в запираемом шкафу, в помещении, исключающем несанкционированное нахождение третьих лиц.

5. Восстановление информации из резервных копий

Любое восстановление информации, не вызванное необходимостью экстренного восстановления, связанной с потерей работоспособности информационной системы или ее компонентов, выполняется на основании служебной записки на имя директора.

После поступления заявки, восстановление данных осуществляется в максимально сжатые сроки, ограниченные техническими возможностями системы, но не более одного рабочего дня.

Пронумеровано, прошито и скреплено печатью

3 (три) листа

Директор МБОУ «СОШ №2»
Г. Симферополя

В. А. Кухнина

