УТВЕРЖДЕНО:

Директор ЧОУ ДПО «ЦДО»

Приказ от 1.01.2023г. № 1-л

Л.А. Рец

ПРАВИЛА
резервного копирования и восстановления документов и информации Частного образовательного учреждения дополнительного профессионального образования «Центр дополнительного образования»

1. Общие положения

Настоящие Правила резервного копирования и восстановления документов и информации Частного образовательного учреждения дополнительного профессионального образования «Центр дополнительного образования» (сокращенно: ЧОУ ДПО «ЦДО»), далее – Правила, разработаны в соответствии с требованиями Федерального закона от 27 июля 2006 года № 149 ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27 июля 2006 года № 152 ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативных и методических документов Федеральной службы потехническому и экспортному контролю Российской Федерации и Федеральной службы безопасности Российской Федерации.

Настоящие правила разработаны с целью:

- определения порядка резервирования документов и информации;
- определения порядка восстановления документов и 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 сотрудников, проводящих резервное копирование и восстановлением информации;

В настоящих Правилах определены действия при выполнении следующих мероприятий:

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

2. Порядок резервного копирования

Для обеспечения резервного копирования, восстановления и архивного хранения электронных данных приказом по ЧОУ ДПО «ЦДО» назначается ответственный за резервное копирование. Ответственный за резервное копирование подчиняется директору, в своей работе руководствуются настоящими Правилами, нормативными актами по защите информации, техническими инструкциями на серверное оборудование, систему хранения данных и другими документами.

Инструктивно-методическое руководство деятельностью ответственного за резервное копирование осуществляется руководителем. *ЧОУ ДПО «ЦДО»*

Основными задачами ответственного за резервное копирование являются:

- Планирование резервного копирования и восстановления;
- Установление жизненного цикла и календаря операций;
- Защита данных резервного копирования от повреждения, модификации инесанкционированного доступа;

Резервному копированию подлежит информация следующих основных категорий:

- Персональная информация пользователей (личные каталоги на файловых серверах);
- Групповая информация пользователей (общие каталоги отделов);
- Персональные профили пользователей сети;
- Информация автоматизированных систем, в т.ч. баз данных;
- Данные с рабочих станций, содержащих критически важную информацию.

Резервное копирование/восстановление информации осуществляется штатными средствами операционных систем специалистом по обслуживанию компьютерной техники на основании заявки ответственного за обеспечение безопасности персональных данных в информационной системе (далее – ответственный).

Контроль результата процедур резервного копирования и восстановления информации ограниченного доступа осуществляет ответственный.

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.

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

Резервное копирование/восстановление информации, осуществляется на учтенные съемные носители.

Необходимость и периодичность резервного копирования информации, а также срок хранения резервных копий определяется пользователямисамостоятельно.

Не допускается создание резервных копий на неучтенные и личные носители информации.

Хранение съемных носителей должно осуществляться в сейфах (столах), оборудованных внутренними замками.

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

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

Срок хранения резервных копий определяется соглашением с лицом, ответственным за ведение соответствующего информационного ресурса.

Хранение резервных копий осуществляется в соответствии с правилами работы с документами, содержащими информацию ограниченного доступа вместе, отличном от места их изготовления.

3. Восстановление информации из резервной копии.

Восстановление информации, хранящейся на сервере производится специалистом по обслуживанию компьютерной техники (штатным или нештатным) на основании заявки ответственного.

В случае повреждения или утраты информации, до начала восстановления их со съемного носителя, следует определить причину утраты или повреждения файлов.

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

В случае повреждения файловой системы или работоспособности жесткого диска в результате системного сбоя пользователь должен обратиться к ответственному.

Перенос файлов из резервной копии может выполняться только послевосстановления работоспособности.

В случае повреждения или утраты файлов, содержащих конфиденциальную информацию, вследствие несанкционированного доступа (далее – НСД) 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.

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