



УТВЕРЖДАЮ
Директор Центра

А. В. Жигайлов
«28» декабря 2018 г.

РЕГЛАМЕНТ

резервного копирования персональных данных субъектов государственного автономного образовательного учреждения дополнительного образования «Центр для одаренных детей «Поиск»

1. Общие положения

1.1. Регламент о порядке резервного копирования персональных данных субъектов государственного автономного образовательного учреждения дополнительного образования «Центр для одаренных детей «Поиск» (далее – Регламент) разработан в соответствии с Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», с Федеральным законом Российской Федерации от 27.06.2006 г. N 152-ФЗ "О персональных данных", Доктриной информационной безопасности Российской Федерации», утвержденной Президентом Российской Федерации от 09.09.2000 г. № Пр-1895.

1.2. Настоящий Регламент определяет порядок резервирования данных для последующего восстановления работоспособности автоматизированных систем Центра «Поиск» при полной или частичной потере информации, вызванной сбоями или отказами аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.); восстановления информации в случае возникновения такой

необходимости; упорядочения работы должностных лиц, связанной с резервным копированием и восстановлением информации, обрабатываемой в государственном автономном образовательном учреждении дополнительного образования «Центр для одаренных детей «Поиск» (далее – Центр «Поиск»).

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

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

1.4. Резервному копированию подлежат информация следующих основных категорий:

- персональная информация пользователей (личные каталоги на файловых серверах);
- групповая информация пользователей (общие каталоги отделов);
- информация, необходимая для восстановления серверов и систем управления базами данных (далее – СУБД);
- персональные профили пользователей сети;
- информация автоматизированных систем, в т.ч. баз данных;
- справочно-информационная информация систем общего использования;
- рабочие копии установочных компонент программного обеспечения рабочих станций;
- регистрационная информация системы информационной безопасности автоматизированных систем.

2. Порядок резервного копирования

2.1. Ответственным за организацию резервного копирования персональных данных является администратор информационной безопасности.

2.2. Резервное копирование автоматизированных систем производится на основании следующих данных:

- состав и объем копируемых данных, периодичность проведения резервного копирования (из Перечня резервируемых данных - по форме, приведенной в Приложении №1);
- максимальный срок хранения резервных копий - 1 месяц;
- хранение 3-х следующих архивов;
- архив на 1-е число текущего месяца;
- архив среда-четверг, либо пятница-суббота текущей недели;
- архив сделанный в текущую ночь.

2.3. Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации, указанной в Перечне, в установленные сроки и с заданной периодичностью. Методика проведения резервного копирования описана в Приложении 1.

2.4. О выявленных попытках несанкционированного доступа к резервируемой информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, сообщается директору Центра «Поиск» в течение рабочего дня после обнаружения указанного события.

3. Контроль результатов резервного копирования

3.1. Контроль результатов всех процедур резервного копирования осуществляется администратором информационной безопасности в срок до 17 часов рабочего дня, следующего за установленной датой выполнения этих процедур.

3.2. В случае обнаружения ошибки в резервном копировании, администратор информационно безопасности устраняет ошибку и повторяет процедуру.

3.3. 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 ее хранения.

4. Ротация носителей резервной копии

4.1. Система резервного копирования должна обеспечивать возможность периодической замены (выгрузки) резервных носителей без потерь информации на них, а также обеспечивать восстановление текущей информации автоматизированных систем в случае отказа любого из устройств резервного копирования.

4.2. В случае необходимости замены испорченных носителей информации новыми, администратор информационной безопасности заблаговременно за 10 рабочих дней согласовывает с поставщиком спецификации новых носителей информации.

4.3. Все процедуры по загрузке, выгрузке носителей из системы резервного копирования осуществляются администратором информационной безопасности по графику или по запросу других сотрудников.

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

4.5. Конфиденциальная информация с носителей, которые перестают использоваться в системе резервного копирования, должна стираться с использованием программного обеспечения PGP.

5. Восстановление информации из резервных копий

5.1. В случае необходимости восстановление данных из резервных копий производится на основании Заявки сотрудника Центра «Поиск», согласованной с Ответственным за организацию обработки персональных данных.

5.2. Процедура восстановления информации из резервной копии осуществляется в соответствии с методикой восстановления информации (Приложение 1).

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