Приложение № 18
к приказу №___ от «____»_____ 20___ г.

РЕГЛАМЕНТ

резервного копирования и восстановления данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Регламент резервного копирования и восстановления данных, хранящихся на серверах и рабочих станциях МБОУ «Гимназия №1» разработан 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 г. № 21.

1.2. Настоящий Регламент разработан с целью:

1.2.1. Определения порядка резервирования данных для последующего восстановления работоспособности информационной системы персональных данных (далее ИСПДн) 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.);

1.2.2. Определения порядка восстановления информации в случае возникновения такой необходимости;

1.2.3. Упорядочения работы должностных лиц, связанной с резервным копированием и восстановлением информации;

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

1.3.1. Резервное копирование;

1.3.2. Контроль резервного копирования;

1.3.3. Хранение резервных копий;

1.3.4. Полное или частичное восстановление данных и приложений.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»).

2.2. Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (ст. 3 ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»).

2.3. 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.

2.4. Система резервного копирования - совокупность программного и

аппаратного обеспечения, выполняющая задачу резервного копирования информации.

3. ПОРЯДОК РЕЗЕРВНОГО КОПИРОВАНИЯ

3.1. Резервному копированию подлежит информация следующих основных категорий:

3.1.1. данные (файлы и каталоги) на файловых серверах;

3.1.2. базы данных, содержащие персональные данные субъектов;

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

3.3. О выявленных попытках несанкционированного доступа к резервируемой информации, а также иных нарушениях информационной безопасности произошедших в процессе резервного копирования, должно быть немедленно сообщено администратору безопасности ИСПДн, либо ответственному за обеспечение безопасности персональных данных МБОУ «Гимназия №1».

3.4. Для организации системы резервного копирования используется программное обеспечение (далее - ПО) 7-Zip.

3.5. Копии хранятся на сетевом хранилище.

3.6. Для резервирования информации, хранимой непосредственно в файловых системах, используется ПО 7-Zip.

4. КОНТРОЛЬ РЕЗУЛЬТАТОВ РЕЗЕРВНОГО КОПИРОВАНИЯ

4.1. Контроль результатов всех процедур резервного копирования осуществляется администратором безопасности ИСПДн.

4.2. На протяжении периода времени, когда система резервного копирования находится в аварийном состоянии, должно осуществляться ежедневное копирование информации, подлежащей резервированию, с использованием носителей располагающих необходимыми объемами дискового пространства для её хранения.

5. РОТАЦИЯ НОСИТЕЛЕЙ РЕЗЕРВНОЙ КОПИИ

5.1. Система резервного копирования должна обеспечивать возможность периодической замены (выгрузки) резервных носителей без потерь информации на них, а также обеспечивать восстановление текущей информации ИСПДн в случае отказа любого из устройств резервного копирования. Все процедуры по загрузке, выгрузке носителей из системы резервного копирования, а также их перемещение, осуществляются администратором безопасности ИСПДн. В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек.

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

6. ВОССТАНОВЛЕНИЕ ИНФОРМАЦИИ ИЗ РЕЗЕРВНОЙ КОПИИ

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

6.2. Любое восстановление информации выполняется на основании заявки пользователя администратору безопасности ИСПДн 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, прилагающейся к системе резервного копирования.