Приложение №11
к приказу от 26 ноября 2018 г.№221

Регламент
резервного копирования и восстановления персональных данных в информационной системе персональных данных Муниципального бюджетного общеобразовательного учреждения «Средняя общеобразовательная школа № 19» города Вышний Волочек

1. Общие положения.

1.1 Настоящий Регламент разработан с целью:
определения порядка резервирования данных для последующего восстановления работоспособности информационной системы персональных данных (далее – ИСПДн) Муниципального бюджетного общеобразовательного учреждения «Средняя общеобразовательная школа № 19» города Вышний Волочек

– (далее – Учреждение) 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 сотрудников Учреждения связанной с резервным копированием и восстановлением информации.

1.2 В настоящем документе определяются действия при выполнении следующих мероприятий:

– резервное копирование;

– контроль резервного копирования;

– хранение резервных копий;

– полное или частичное восстановление данных и приложений.

1.3 Резервному копированию подлежит информация в электронном виде, согласно «Перечню информации, обрабатываемой в ИСПДн».

1.4 Настоящая инструкция определяет требования к организации учета, хранения и выдачи машинных носителей, содержащих персональные данные в ИСПДн.

1.5 Учет, хранение и выдачу машинных носителей персональных данных осуществляет ответственный за обеспечение безопасности персональных данных в ИСПДн, который несет личную ответственность за сохранность персональных данных. При увольнении сотрудника, ответственного за учет, хранение и выдачу машинных носителей персональных данных, составляется акт приема-сдачи этих документов, который утверждается директором Учрежения.

1.6 Доведение Инструкции до сотрудников Учреждения в части их касающейся осуществляется администратором безопасности информации под роспись в Листе ознакомления с данной инструкцией.

2. Порядок резервного копирования.

2.1 Резервное копирование информации производится на основании следующих данных:

– состав и объем копируемых данных, периодичность проведения резервного копирования;

– максимальный срок хранения резервных копий;

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

2.3 О выявленных попытках несанкционированного доступа к резервируемой информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, сообщается ответственному за обеспечение безопасности персональных данных.

3. Методика резервного копирования.

Резервное копирование осуществляется средствами ОС Windows путем копирования информации на несъемный жесткий диск.

4. Контроль результатов резервного копирования.

4.1 Контроль результатов всех процедур резервного копирования осуществляется ответственным за эксплуатацию ИСПДн в срок до 17 часов рабочего дня, следующего за установленной датой выполнения этих процедур.

4.2 В случае обнаружения ошибки администратор безопасности информации сообщает об этом факте ответственному за обеспечение безопасности персональных данных до 18 часов текущего рабочего дня.

4.3 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 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 автоматизированных систем в случае отказа любого из устройств резервного копирования.

5.2 Все процедуры по загрузке, выгрузке носителей из системы резервного копирования осуществляются ответственным за обеспечение безопасности персональных данных.

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

5.4 Персональные данные с носителей, которые перестают использоваться в системе резервного копирования, должны стираться.

6. Ротация носителей резервной копии.

6.1 В случае необходимости восстановление данных из резервных копий производится на основании Заявки владельца информации,

согласованной с ответственным за обеспечение безопасности персональных данных.

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