Приложение 16
к приказу МБОУ СОШ №3
от 07.04.2017 №181

ИНСТРУКЦИЯ
по резервному копированию и восстановлению защищаемой информации Муниципального бюджетного общеобразовательного учреждения «Средняя общеобразовательная школа №3»

3. Общие положения

1.1. Инструкция по резервному копированию и восстановлению защищаемой информации, работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации (далее – Инструкция) определяет меры и порядок действия работников Муниципального бюджетного общеобразовательного учреждения «Средняя общеобразовательная школа №3» (далее – Учреждение) по резервному копированию и восстановлению защищаемой информации в информационных системах персональных данных.

1.2. Целью настоящей Инструкции является порядок резервирования и восстановление работоспособности элементов автоматизированной системы «АРМ-К СОШ №3» и меры предотвращения потери защищаемой информации.

1.3. Для целей настоящей Инструкции защищаемой информацией признается:

- информационные ресурсы, входящие в информационные системы персональных данных;
- информационные ресурсы, хранящиеся на общих ресурсах и относящиеся к непосредственной деятельности Учреждения;
- документы электронной почты;
- дистрибутивы программного обеспечения;
- другая информация, необходимая для восстановления работоспособности технических средств и программного обеспечения.

Действие настоящей Инструкции распространяется на всех сотрудников, имеющих доступ к защищаемой информации Учреждения, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе: системы обеспечения отказоустойчивости и системы резервного копирования и хранения данных.

Задачами данной Инструкции являются определение мер защиты от потери информации и определение действий по восстановлению данных в случае потери информации.

1.4. Ответственным за резервное копирование и восстановление информации назначается администратор безопасности.

2. Меры по резервному копированию и восстановлению информации

2.1. Организационные меры

2.1.1. В Учреждении должен быть определен и документально зафиксирован порядок осуществления резервного копирования и восстановления данных, определяющий:

- ответственных лиц за выполнение работ по резервному копированию и восстановлению данных;
- перечень информационных ресурсов, подлежащих резервному копированию;
- периодичность резервного копирования, в соответствии с особенностями технологического процесса обработки информации и установленными требованиями по обеспечению безопасности;
- порядок проверки резервных копий и контроль выполнения резервного копирования;
- порядок восстановления информации из резервных копий.

2.2. Технические меры

2.2.1. Помещения Учреждения, в которых размещаются технические средства, и средства защиты информации информационных систем персональных данных в обязательном порядке должны быть оборудованы пожарной сигнализацией.

2.2.2. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы, сетевое и коммуникационное оборудование, а также

рабочие станции должны быть подключены к сети электропитания через источники бесперебойного питания.

2.2.3. В Учреждении должны быть организованы места хранения резервных копий (сейфы, металлические шкафы для съемных носителей информации, каталоги на жестких дисках для хранения информации в электронном виде), которые исключают возможность несанкционированного доступа к ним, хищения или уничтожения.

2.2.4. Для обеспечения резервного копирования и восстановления данных используются соответствующие средства операционной системы, встроенные механизмы прикладных программ, специализированного программного обеспечения или технических средств. Выбор средств, порядок их использования (автоматический или ручной режим запуска) определяется с учетом особенностей технологии обработки данных информационных ресурсов.

3. Порядок действий сотрудников при резервном копировании и восстановлении информации

3.1. **Резервное копирование**

Резервное копирование данных осуществляется администратором безопасности с использованием соответствующих средств на периодической основе.

3.1.1. Для защищаемой информации устанавливаются следующие периоды **резервного** копирования:

3.1.1.1. ежедневное резервное копирование баз данных, расположенных на сервере, администратором безопасности персональных данных. Резервные копии сохраняются на учтенный внешний жесткий диск;

3.1.1.2. дистрибутивы программного обеспечения и обновления (операционной системы, прикладное программное обеспечение, средства защиты информации), с которых осуществляется их установка:

в качестве резервной копии используется предоставленная поставщиком копия дистрибутива программного обеспечения или его обновления на оригинальном съемном носителе информации;

в случае предоставления поставщиком копии дистрибутива программного обеспечения или его обновления не на съемном носителе информации, они записываются на съемный носитель информации, который в дальнейшем используется в качестве резервной копии;

резервные копии дистрибутива программного обеспечения и их обновлений помещается в соответствующее место для хранения резервных копий.

Сроки хранения резервных копий устанавливаются, исходя из актуальности содержащих на них данных. Резервные копии сохраняют актуальность до проведения следующего резервного копирования.

3.2. **Восстановление информации**

3.2.1. Восстановление информации осуществляется администратором безопасности после устранения причин или принятия соответствующих мер по их нейтрализации, приведших к возникновению инцидента информационной безопасности, в результате которого, было осуществлено неправомерно или случайное уничтожение, изменение, блокирование защищаемой информации в следствии:

преднамеренных, непредвиденных или случайных действий сотрудников Учреждения и третьих лиц;

сбоев в работе технических средств и программного обеспечения;

возникновения нештатных ситуаций и обстоятельств непреодолимой силы.

3.2.2. Восстановление информации осуществляется с последней резервной копии, предшествующей моменту возникновения инцидента информационной безопасности.

4. Ответственность

Администратор безопасности несет персональную ответственность за:

качество проводимых им работ по обеспечению резервного копирования и восстановления информации;

выполнение мероприятий по сопровождению и поддержанию работоспособности средств системы резервного копирования и восстановления информации;

выполнение мероприятий по устранению сбоев в работе системы резервного копирования и восстановления информации;

планирование развития существующей системы резервного копирования и восстановления данных для оптимизации ее работы;

регулярный контроль результатов всех работ по резервному копированию и восстановлению информации;

периодическое выполнение проверки возможности восстановления файлов резервных копий.