



ИНСТРУКЦИЯ по организации резервного копирования информации

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая инструкция разработана в соответствии с требованиями законодательства Российской Федерации в области защиты информации (в том числе персональных данных), с целью обеспечения возможности незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней.

1.2. Порядок определяет правила и объёмы резервирования, а также порядок восстановления работоспособности информационных систем персональных данных (ИСПДн) Муниципального бюджетного учреждения дополнительного образования «Детская школа искусств №3» города Челябинска (далее - МБУДО «ДШИ №3» города Челябинска).

1.3. Носители информации, используемые для резервирования конфиденциальной информации в МБУДО «ДШИ №3» города Челябинска (в том числе и персональных данных), подлежат защите в той же степени, что и резервируемая конфиденциальная информация.

1.4. Ответственность за исполнением настоящего Порядка несет администратор безопасности ИСПДн.

1.5. Данный Порядок предназначен для администратора информационной безопасности ИСПДн.

2. ИНФОРМАЦИОННЫЕ РЕСУРСЫ, ПОДЛЕЖАЩИЕ РЕЗЕРВИРОВАНИЮ

2.1. Резервному копированию подлежат все информационные ресурсы МБУДО «ДШИ №3» города Челябинска, содержащие персональные данные субъектов.

3. ПОРЯДОК РЕЗЕРВИРОВАНИЯ

3.1. Резервирование информационных ресурсов ИСПДн МБУДО «ДШИ №3» города Челябинска, выполняется администратором информационной безопасности ИСПДн.

3.2. Определяется 2 вида резервирования информации:

- полное резервирование информации – резервное копирование всей информации, хранящейся в ИСПДн;
- неполное резервирование информации – резервное копирование части информации, хранящейся в ИСПДн.

Целью неполного резервирования является сохранение изменений в ИСПДн с момента полного резервирования информации.

3.3. Периодичность проведения работ по резервированию информации определяется ответственным за организацию обработки и обеспечение безопасности персональных данных, обрабатываемых в ИСПДн МБУДО «ДШИ №3» города Челябинска, но не менее 1 раза в месяц для полного резервирования и 1 раза в неделю для неполного резервирования.

3.4. Администратор информационной безопасности ИСПДн использует средства резервного копирования ИС для резервирования информации на отчуждаемый носитель. В случаях, когда резервирование информации средствами ИС не представляется возможным, администратор информационной безопасности ИСПДн может использовать средство резервного копирования, не входящее в состав ИСПДн.

3.5. Резервное копирование с использованием незащищённых каналов связи общего пользования не допустимо.

3.6. Резервное копирование по локальной сети на устройство, находящееся вне ИСПДн, не допустимо.

3.7. Администратор информационной безопасности ИСПДн не имеет право ознакомляться с резервируемой информацией. Факт ознакомления администратора информационной безопасности ИСПДн с резервируемой информацией может быть расценен как превышение служебных полномочий в соответствии с Трудовым Кодексом Российской Федерации и Кодексом об Административных Правонарушениях Российской Федерации.

3.8. В случае удаления информации из ИС должна быть так же удалена ее резервная копия.

4. ПОРЯДОК ХРАНЕНИЯ РЕЗЕРВНЫХ КОПИЙ

4.1. Хранение резервных копий информации должно исключать любой несанкционированный доступ посторонних лиц к носителям информации.

4.2. Хранение резервных копий необходимо осуществлять в сейфах, негорючих шкафах, металлических шкафах с устройством опечатывания. Доступ к местам хранения резервных копий должен быть предоставлен только администратору информационной безопасности ИСПДн.

4.3. На носителе информации, содержащем резервные копии защищаемой информации (в том числе персональных данных), не должна храниться посторонняя информация.

4.4. Должно быть обеспечено одновременное хранение не менее двух носителей информации, хранящих полную резервную копию защищаемой информации ИСПДн.

5. ПОРЯДОК ВОССТАНОВЛЕНИЯ ИНФОРМАЦИИ ПОСЛЕ СБОЯ

5.1. В случае сбоя в работе ИСПДн, восстановление данных из резервных копий осуществляет администратор информационной безопасности ИСПДн.

5.2. Администратор информационной безопасности ИСПДн обязан срочно уведомить ответственного за организацию обработки персональных данных о факте сбоя в работе ИСПДн, повлекшего нарушение целостности данных.