



Приложение №3
к приказу по учреждению
№83 от 30.03.2022 г.

ИНСТРУКЦИЯ **по организации резервного копирования информации в информационных** **системах персональных данных** **в АУК «ДК «Нефтяник» города Радужный**

1. Общие положения

1.1. Настоящая инструкция разработана в соответствии с требованиями законодательства Российской Федерации в области защиты персональных данных, с целью обеспечения возможности незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

1.2. Инструкция определяет правила и объёмы резервирования, а также порядок восстановления работоспособности информационных систем персональных данных (далее – ИСПДн) автономного учреждения культуры «Дворец культуры «Нефтяник» городского округа Радужный Ханты-Мансийского автономного округа-Югры (далее – Учреждение).

1.3. Носители информации, используемые для резервирования конфиденциальной информации Учреждения (в том числе и персональных данных), подлежат защите в той же степени, что и резервируемая конфиденциальная информация.

1.4. Контроль за исполнением настоящей инструкции осуществляет ответственный за обработку персональных данных Учреждения.

2. Назначение и область действия

2.1. Данная инструкция предназначена для администратора безопасности информационных систем (далее – администратор) Учреждения, а так же сотрудников Учреждения, участвующих в обработке персональных данных в ИСПДн (далее – пользователи).

2.2. Инструкция описывает действия Администратора и пользователей по обеспечению резервного копирования и восстановления персональных данных, обрабатываемых в информационных системах персональных данных Учреждения.

3. Информационные ресурсы, подлежащие резервированию

3.1. Резервному копированию подлежат все информационные ресурсы Учреждения, содержащие персональные данные субъектов, а именно:

- файлы баз данных;
- электронные документы;
- файлы сообщений электронной почты;
- отсканированные и хранящиеся в ИСПДн изображения документов и фотографии субъектов.

Резервному копированию могут так же подвергаться:

- системное и прикладное программное обеспечение ИСПДн;
- средства защиты информации в ИСПДн.

4. Порядок резервирования

4.1. Резервирование информационных ресурсов ИСПДн, содержащих персональные данные (далее – резервирование персональных данных), выполняется администратором безопасности информационных систем.

4.2. Определяется 2 вида резервирования персональных данных:

- полное резервирование персональных данных – резервное копирование всех персональных данных, хранящихся в ИСПДн;
- неполное резервирование персональных данных – резервное копирование части персональных данных, хранящихся в ИСПДн.

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

4.3. В случаях, когда информационные ресурсы персональных данных хранятся на компьютерах пользователей локально, допустимо перекладывать ответственность за проведение неполного резервирования персональных данных на пользователей ИСПДн.

4.4. События резервирования персональных данных фиксируются в Журнале учета резервного копирования ИСПДн, содержащих персональные данные.

4.5. Администратор безопасности информационных систем использует средства резервного копирования ИСПДн для резервирования персональных данных на отчуждаемый носитель. В случаях, когда резервирование персональных данных средствами ИСПДн не представляется возможным, администратор безопасности информационных систем по согласованию с ответственным за обработку персональных данных Учреждения может использовать средство резервного копирования, не входящее в состав ИСПДн.

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

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

4.8. Администратор безопасности информационных систем не имеет право ознакамливаться с резервируемыми персональными данными. Факт ознакомления администратора безопасности информационных систем с резервируемыми персональными данными может быть расценён как превышение служебных полномочий в соответствии с Трудовым Кодексом Российской Федерации и Кодексом об Административных правонарушениях Российской Федерации.

4.9. При резервировании персональных данных не допускается хранение на одном носителе резервных копий персональных данных, извлечённых из различных ИСПДн. Для осуществления резервирования персональных данных различных ИСПДн, для каждой ИСПДн должен быть предусмотрен отдельный носитель информации.

4.10. В случае удаления персональных данных субъекта из ИСПДн должна быть так же удалена резервная копия этих данных.

5. Порядок хранения резервных копий

5.1. Хранение резервных копий персональных данных должно исключать любой несанкционированный доступ посторонних лиц к носителям информации.

5.2. Хранение резервных копий необходимо осуществлять в сейфах, несгораемых шкафах, металлических шкафах с устройством опечатаывания. Доступ к местам хранения резервных копий должен быть предоставлен только администратору безопасности информационных систем и ответственному за обработку ПДн Учреждения.

5.3. Не допускается хранение резервных копий персональных данных совместно с другими носителями информации.

5.4. На носителе информации, содержащем резервные копии персональных данных, не должна храниться посторонняя информация.

5.5. Должно быть обеспечено одновременное хранение не менее двух носителей информации, хранящих полную резервную копию персональных данных ИСПДн.

6. Порядок восстановления информации после сбоя

6.1. В случае сбоя в работе ИСПДн, восстановление персональных данных из резервных копий осуществляет администратор безопасности информационных систем.

6.2. Администратор безопасности информационных систем обязан срочно уведомить ответственного за обработку персональных данных Учреждения о факте сбоя в работе ИСПДн, повлекшего нарушение целостности персональных данных.

6.3. Факты восстановления персональных данных должны фиксироваться в Журнале учета резервного копирования ИСПДн, содержащих персональные данные (в графе «вид резервирования» указывается «полное восстановление» либо «частичное восстановление»).

6.4. Временной норматив по восстановлению персональных данных устанавливается ответственным за обработку персональных данных Учреждения с учётом специфики работы ИСПДн.

Автономное учреждение культуры «Дворец культуры «Нефтяник»
городского округа Радужный Ханты-Мансийского автономного округа-Югры
ИНН 8609015939, КПП 860901001, ОКПО 54110251, ОГРН 1028601465837

(полное наименование организации, идентификационные коды (ИНН, КПП, ОКПО, ОГРН))

ЖУРНАЛ

**учета резервного копирования информационных систем персональных данных
АУК «ДК «Нефтяник» города Радужный**

На _____ листах

Начат «___» _____ 20__ г.

Окончен «___» _____ 20__ г.

