151

Государственное учреждение культуры Тульской области
«ОБЪЕДИНЕНИЕ ЦЕНТРОВ РАЗВИТИЯ ИСКУССТВА, НАРОДНОЙ КУЛЬТУРЫ И ТУРИЗМА»

П Р И К А З № 48

г. Тула **18 марта 2019 года**

Об утверждении регламента резервного копирования и восстановления информации в государственном учреждении культуры Тульской области «Объединение центров развития искусства, народной культуры и туризма»

В соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативными и методическими документами Федеральной службы по техническому и экспортному контролю Российской Федерации и Федеральной службы безопасности Российской Федерации, на основании Устава государственного учреждения культуры Тульской области «Объединение центров развития искусства, народной культуры и туризма»,

ПРИКАЗЫВАЮ:

1. Утвердить регламент резервного копирования и восстановления информации в государственном учреждении культуры Тульской области «Объединение центров развития искусства, народной культуры и туризма» (приложение).
2. Контроль над исполнением настоящего приказа возложить на ответственного за обеспечение безопасности персональных данных в Учреждении.
3. Приказ вступает в силу со дня подписания.

Директор **Е.В. Арбекова**

Приложение к приказу
от 18 марта 2019 года № 48

РЕГЛАМЕНТ
резервного копирования и восстановления информации в государственном учреждении культуры Тульской области «Объединение центров развития искусства, народной культуры и туризма»

1. Настоящий Регламент резервного копирования и восстановления информации в государственном учреждении культуры Тульской области «Объединение центров развития искусства, народной культуры и туризма» (далее – Регламент), хранящихся на серверах и автоматизированных рабочих местах (далее – АРМ) Учреждения, разработан в соответствии с требованиями Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативных и методических документов Федеральной службы по техническому и экспортному контролю Российской Федерации и Федеральной службы безопасности Российской Федерации.

2. Настоящий регламент разработан с целью:

определения порядка резервирования информации;

определения порядка восстановления информации в случае ее искажения или утраты, в связи с попытками несанкционированного доступа, сбоями или отказами аппаратного, или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);

упорядочения работы сотрудников, связанной с резервным копированием и восстановлением информации;

3. В настоящем Регламенте определены действия при выполнении следующих мероприятий:

резервное копирование;

контроль резервного копирования;

хранение резервных копий;

восстановление информации.

II. Порядок резервного копирования

4. Резервному копированию подлежит информация следующих основных категорий:

информация ограниченного доступа, в том числе персональные данные (далее – ПДн), хранящаяся на серверах Учреждения (базы данных, файлы и каталоги);

информация ограниченного доступа, в том числе ПДн, хранящаяся на АРМ Учреждения.

5. Резервное копирование/восстановление информации, хранящейся на серверах Учреждения, осуществляется штатными средствами операционных систем.

6. Контроль результата процедур резервного копирования, а также восстановление информации ограниченного доступа, хранящейся на серверах Учреждения, осуществляет ответственный за обеспечение безопасности персональных данных в информационных системах Учреждения (далее – Ответственный).

7. Система резервного копирования должна обеспечивать возможность периодической замены (выгрузки) носителей резервных копий без потерь информации, а также обеспечивать восстановление информации в случае отказа любого из устройств резервного копирования.

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

9. Резервное копирование/восстановление информации, хранящейся на АРМ Учреждения, осуществляется пользователями на учтенные съемные носители.

10. Необходимость и периодичность резервного копирования информации, хранящейся на АРМ Учреждения, а также срок хранения резервных копий такой информации на съемных носителях определяется пользователями самостоятельно.

11. Резервное копирование информации может осуществляться исключительно на съемные машинные носители информации, учтенные в журнале учета съемных носителей информации Учреждения.

12. Не допускается создание резервных копий на неучтенные и личные носители информации. При использовании съемных машинных носителей как носителей ПДн запись в журнале учета должна содержать отметку «Конфиденциально».

13. Хранение съемных машинных носителей ПДн должно осуществляться в сейфах (металлических шкафах), оборудованных внутренними замками и приспособлениями для опечатывания замочных скважин.

14. В случае отсутствия сейфа (металлического шкафа) у пользователя, осуществляющего хранение, допускается осуществлять хранение в сейфе Ответственного.

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

16. О выявленных попытках несанкционированного доступа к резервируемой информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, должно быть немедленно сообщено Ответственному.

III. Восстановление информации из резервной копии

17. В случае необходимости, восстановление информации, хранящейся на серверах Учреждения, может производиться Ответственным на основании заявки пользователя.

18. В случае повреждения или утраты информации, хранящейся на АРМ Учреждения до начала восстановления их со съемного носителя пользователь должен определить причину утраты или повреждения файлов, содержащих ПДн.

19. Если повреждение или удаление информации вызвано действиями самого пользователя (непреднамеренное удаление файла), восстановление информации со съёмного носителя может осуществляться пользователем незамедлительно.

20. В случае повреждения файловой системы АРМ или работоспособности жесткого диска в результате системного сбоя АРМ пользователь должен обратиться к Ответственному.

Перенос файлов из резервной копии может выполняться пользователем только после восстановления работоспособности АРМ.

21. В случае повреждения или утраты файлов, содержащих конфиденциальную информацию, в том числе ПДн, вследствие несанкционированного доступа (далее – НСД) к АРМ Учреждения пользователь незамедлительно сообщает о данном факте Ответственному.

Восстановление файлов из резервной копии может осуществляться только после проведения расследования инцидента безопасности НСД с соответствующим устранением угрозы дальнейших инцидентов НСД.

22. Если утрата файлов на АРМ Учреждения произошла в результате вирусного заражения, восстановление файлов возможно только после выполнения мероприятий в соответствии с инструкцией антивирусной защиты государственного учреждения культуры Тульской области «Объединение центров развития искусства, народной культуры и туризма».