Приложение № 1
к приказу МБУДО ДШИ № 28
№ 41/1-од от 25.05.2017г.

ПОРЯДОК

резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах муниципального бюджетного учреждения дополнительного образования города Новосибирска «Детская школа искусств № 28»

Глава 1. ОБЩЕЕ ПОЛОЖЕНИЕ

1. Настоящий Порядок резервирования и восстановления работоспособности технических средств (далее - ТС) и программного обеспечения (далее - ПО), баз данных и средств защиты информации (далее - СЗИ) разработан с целью обеспечения возможности незамедлительного восстановления защищаемых данных, модифицированных или уничтоженных вследствие несанкционированного доступа (далее - НСД) к ним.

2. Данный документ определяет:

а) правила и объемы резервирования, а также порядок восстановления работоспособности в информационной системе (далее - ИС) в муниципальном бюджетном учреждении дополнительного образования города Новосибирска «Детская школа искусств № 28» (далее - Учреждение);

б) предназначен для исполнения работником, в обязанности которого входит техническое обслуживание ИС (далее – администратор ИС), а также пользователями ИС, участвующими в обработке персональных данных (далее - ПДн) в ИС (далее - пользователи);

в) описывает действия администратора ИС и пользователей по обеспечению резервного копирования и восстановления ПДн, обрабатываемых в ИС.

3. Носители информации, используемые для резервирования защищаемой информации в ИС (в том числе и ПДн), подлежат защите в той же степени, что и резервируемая информация.

4. Контроль за исполнением настоящего Порядка осуществляет администратор ИС либо работник, назначенный приказом руководителя Учреждения ответственным за обеспечение безопасности ПДн в ИС.

Глава 2. НАЗНАЧЕНИЕ И ОБЛАСТЬ ДЕЙСТВИЯ

5. Резервируемой информацией следует считать любые защищаемые данные в электронном виде. Резервируемая информация разделяется по способу обработки (по способу хранения) на две категории:

а) обработка (хранение) в базе данных;

б) любом другом виде.

6. Резервному копированию подлежат все информационные ресурсы ИС, содержащие защищаемую информацию, а именно:

а) файлы баз данных;

б) электронные документы.

7. Резервному копированию могут также подвергаться:

а) системное и прикладное программное обеспечение ИС;

б) средства защиты информации.

Глава 3. ПОРЯДОК РЕЗЕРВИРОВАНИЯ

8. Резервное копирование и хранение данных должно осуществляться на периодической основе:

а) для обрабатываемых защищаемых данных - не реже одного раза в месяц;

б) для технологической информации - не реже раза в два месяца;

в) эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИС, - не реже раза в квартал и каждый раз при внесении изменений в эталонные копии (выход новых версий).

9. Резервирование защищаемых информационных ресурсов ИС, не содержащих ПДн, выполняется администратором ИС.

10. Резервирование информационных ресурсов ИС, содержащих ПДн, выполняется администратором ИС.

11. Определяется 2 вида резервирования данных:

а) полное резервирование данных - резервное копирование всех ПДн, хранящихся в ИС;

б) неполное резервирование данных - резервное копирование части ПДн, хранящихся в ИС.

12. Целью неполного резервирования является сохранение изменений в ИС с момента полного резервирования ПДн.

13. Резервирование ЗД осуществляется в автоматическом режиме на локальном дисковом массиве сервера.

14. Резервное копирование баз данных выполняется:

а) ежедневно в конце рабочего дня ответственным специалистом на учтенный съемный носитель информации;

б) ежедневно в конце рабочего дня в автоматическом режиме на локальный диск сервера.

15. Восстановление файлов ИС производится путем разархивирования файлов базы данных в исходный каталог.

16. Необходимо регулярно периодичностью один раз в квартал создавать резервные копии путем копирования информации на КОД или любой другой зарегистрированный отчуждаемый носитель информации.

17. Периодичность проведения работ по резервированию данных определяется администратором ИС либо лицом, назначенным приказом руководителя Учреждения ответственным за обеспечение безопасности ПДн в ИС с учетом специфики работы ИС, но не менее 1 раза в квартал для полного резервирования и 1 раза в месяц для неполного резервирования.

18. В случаях, когда защищаемые ресурсы хранятся на компьютерах пользователей Учреждения локально, допустимо перекладывать ответственность за проведение неполного резервирования данных на пользователей ИС.

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

20. Резервное копирование с использованием незащищенных каналов связи общего пользования недопустимо.

23. Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

24. Носители должны храниться не менее года для возможности восстановления данных.

25. В случае удаления ПДн субъекта из ИС должна быть также удалена резервная копия этих данных.

Глава 4. ПОРЯДОК ХРАНЕНИЯ РЕЗЕРВНЫХ КОПИЙ

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

27. Хранение носителей резервных копий защищаемой информации должно быть организовано в сейфе или несгораемом металлическом шкафу с устройством опечатывания.

28. Доступ к местам хранения резервных копий должен быть предоставлен только администратору ИС либо лицу, назначенному приказом руководителя Учреждения ответственным за обеспечение безопасности ПДн в ИС.

29. На носителе информации, содержащем резервные копии ПДн, не должна храниться посторонняя информация.

Глава 5. ПОРЯДОК ВОССТАНОВЛЕНИЯ ИНФОРМАЦИИ ПОСЛЕ СБОЯ

30. При искажении, модификации, блокировании, удалении ПДн необходимо руководствоваться следующим порядком восстановления:

а) в случае возникновения инцидента информационной безопасности, связанного с ПДн, следует незамедлительно сообщить об этом администратору ИС;

б) ответственным за восстановление ПДн из резервных копий является администратор ИС;

в) администратор ИС обязан срочно уведомить лицо, ответственное за организацию обработки ПДн в Учреждении о факте сбоя в работе ИС, повлекшего нарушение целостности ПДн;

г) администратор ИС должен оценить причину возникновения неисправности и принять меры по устранению технических неисправностей при неполадках программного или аппаратного обеспечения компьютера или воспользоваться резервной копией при проблемах, связанных непосредственно с ПДн.