[start doc]

**ДЕПАРТАМЕНТ СОЦИАЛЬНОЙ ПОЛИТИКИ**

**МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ**

**«ДЕТСКИЙ САД КОМБИНИРОВАННОГО ВИДА № {number} «{name}»**

**ПРИКАЗ**

«\_\_»\_\_\_\_\_\_\_\_ 201\_\_ года № \_\_\_\_\_

г. Курган

**О назначении администратора**

**защиты персональных данных**

В целях выполнения требований Федерального закона РФ от 27.07.2006 №152-ФЗ

«О персональных данных»:

ПРИКАЗЫВАЮ:

1. Назначить администратором безопасности информационных систем персональных данных делопроизводителя {FIO1}.
2. Утвердить должностную инструкцию администратора безопасности информационных систем персональных данных Приложение №1.
3. Контроль, за исполнением приказа оставляю за собой.

Заведующий МБДОУ

«Детский сад № {number}»

{FIO2}

С приказом ознакомлена: {FIO3}

Приложение №1

к Приказу

№\_\_\_ от «\_\_» \_\_\_\_\_\_\_ 2017 г.

Должностная инструкция администратора безопасности

1. Общие положения
   1. Настоящая Инструкция определяет функции, права и обязанности Администратора безопасности информации автоматизированных систем, принадлежащих МБДОУ «Детский сад № {number}», по вопросам обеспечения информационной безопасности при обработке персональных данных в автоматизированной системе (далее АС).
   2. Администратор безопасности - субъект доступа в автоматизированную систему, владеющий паролем администратора защиты и имеющий право изменять настройки системы защиты, в том числе и системы защиты от несанкционированного доступа (далее НСД).
   3. Администратор безопасности АС назначается приказом руководителя МБДОУ «Детский сад № {number}» и в своей деятельности руководствуется данной инструкцией.
   4. Работу со средствами защиты от НСД администратор безопасности выполняет, руководствуясь инструкциями.
2. Обязанности администратора безопасности
3. Создавать/удалять новых пользователей АС.
4. Назначать/отменять пароли для пользователей АС.
5. Редактировать параметры (полномочия) пользователей АС.
6. Настраивать параметры системного журнала системы защиты от НСД.
7. Просматривать системный журнал на предмет попыток НСД к информации и анализировать случаи разрушения, уничтожения или порчи информации.
8. Проводить плановую смену паролей пользователей АС.
9. Проводить резервное копирование данных, обрабатываемых в АС.
10. Следить за исправностью средств защиты, установленных в АС.
11. Периодически контролировать наличие на системных блоках АС целостности специальных защитных знаков.
12. Периодически контролировать неизменность состава технических средств, входящих в состав АС и неизменность расположения технических средств АС в соответствии с техническим паспортом на ОИ и «Предписанием на эксплуатацию…» (при наличии).
13. Постоянно контролировать выполнение пользователями АС «Инструкции пользователя АС».
14. Контролировать доступ лиц в помещения, где установлена АС, в соответствии со списком сотрудников, допущенных в помещение и к работе на АС.
15. Осуществлять настройку системы защиты от НСД на предмет автоматического «затирания» информации, санкционировано удаленной с локальных дисков (количество проходов должно быть не менее трёх).
16. Осуществлять периодическое обновление антивирусных средств (баз данных) согласно утвержденной «Инструкции по организации антивирусной защиты в АС объекта информатизации», установленных на АС. Докладывать обо всех нарушениях порядка обработки персональных данных в АС руководителю для принятия практических мер к нарушителям безопасности информации.
17. В случае обнаружения попыток несанкционированного доступа в АС или иных воздействий с целью искажения или уничтожения информации обрабатываемой в АС, а равно попыток нарушения работоспособности технических средств, фиксировать указанные факты, немедленно докладывать руководителю организации или лицу его замещающему.
18. Работа с пользователями
19. Назначение/удаление пользователя АС осуществляется администратором защиты АС на основании «Списка должностных лиц, допущенных к обработке персональных данных в АС» и сопровождается установкой/отменой персональных паролей для пользователей АС.
20. Редактирование параметров (полномочий) пользователей АС выполняется администратором защиты АС с учетом полномочий пользователя по отношению к защищаемым информационным ресурсам в данной АС.
21. Плановая смена паролей осуществляется администратором защиты в присутствии пользователя АС с периодичностью, указанной в технической документации к средству защиты от НСД, но не реже одного раза в месяц.
22. Администратор безопасности АС обязан разрешать конфликтные ситуации пользователей при входе в систему с персональными паролями.
23. Работа с системным журналом
24. Администратор безопасности АС обязан, настраивать параметры системного журнала с целью контроля неизменности состава технических средств, входящих в состав АС, целостности служебных областей жестких дисков и целостности файлов.
25. Администратором безопасности АС ведется регулярный просмотр системного журнала системы защиты от НСД на предмет выявления попыток НСД к защищаемой информации.
26. Администратор безопасности АС при необходимости очищает системный журнал после его анализа.
27. Ремонтные и регламентные работы в АС
28. Администратор безопасности следит за исправностью средств защиты, установленных в АС. В своей деятельности руководствуется утвержденной «Инструкцией по эксплуатации средств защиты информации АС» и докладывает о неисправностях средств защиты руководству. На время ремонта технических средств АС обработка конфиденциальной информации (персональных данных) в АС запрещена.
29. Для проведения ремонтных и регламентных работ администратор безопасности привлекает сотрудников, отвечающих за ремонт и техническое обслуживание технических средств объекта информатизации. С целью недопущения просмотра информации ограниченного доступа администратор безопасности АС обязан присутствовать при проведении таких работ.
30. Резервное копирование данных
    1. Резервное копирование базы данных производится администратором безопасности АС с периодичностью, определенной в соответствии с режимом обработки конфиденциальной информации (персональных данных) в АС (по мере ее накопления, но не реже одного раза в месяц), а также по указанию руководителя.
    2. Резервные копии хранятся на учтенных в магнитных (оптических) носителях информации (дискетах, винчестерах, CD-дисках, Flesh-устройствах).
31. Права администратора безопасности АС
32. Администратор безопасности имеет право участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа.
33. Требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации.

Администратору безопасности запрещается передавать свой пароль и идентификатор (при его наличии) другим лицам. Администратор безопасности АС несет личную ответственность за их сохранность.

[end doc]