УТВЕРЖДЕНА
приказом МБДОУ д/с №49
от «20» июля 2017 г. № 109

Инструкция администратора информационных систем персональных данных

Обозначения и сокращения

В настоящем документе применяются следующие обозначения и сокращения:

АРМ - автоматизированное рабочее место

ИСПДн - информационная система персональных данных

ЛВС - локальная вычислительная сеть

МЭ - межсетевой экран

НСД - несанкционированный доступ

ОС - операционная система

ПДн - персональные данные

ПК - персональный компьютер

ПМВ - программно-математическое воздействие

ПО - программное обеспечение

ПЭМИН - побочные электромагнитные излучения и наводки

РД - руководящие документы

Роскомнадзор - Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций

САЗ - система анализа защищенности

СЗИ - средства защиты информации

СЗПДн - система (подсистема) защиты персональных данных

СОВ - система обнаружения вторжений

УБПДн - угрозы безопасности персональных данных

ФСТЭК - Федеральная служба по экспортному и техническому контролю

ФСБ - Федеральная служба безопасности

1. Общие положения

1.1.Администратор ИСПДн МБДОУ д/с №49 (далее - Администратор) назначается приказом руководителя МБДОУ.

1.2.Администратор в своей работе руководствуется настоящей инструкцией, требованиями законодательства РФ, руководящими и нормативными документами ФСТЭК России и ФСБ России, Роскомнадзора, а также принятыми в организации положениями, инструкциями, приказами.

1.3.Администратор отвечает за обеспечение устойчивой работоспособности элементов ИСПДн и СЗИ при обработке ПДн.

1.4.Методическое руководство работой Администратора осуществляется ответственным за организацию обработки и обеспечение безопасности ПДн.

2. Обязанности администратора ИСПДн

Администратор обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, распоряжений, регламентирующих порядок действий по защите персональных данных.

2.2. Участвовать в контрольных и тестовых испытаниях и проверках элементов ИСПДн.

2.3. Уточнять в установленном порядке обязанности пользователей и администраторов ИСПДн.

2.4. Анализировать состояние защиты ИСПДн и ее отдельных подсистем.

2.5. Контролировать неизменность состояния защищенности информационных систем обработки персональных данных.

2.6. Контролировать физическую сохранность средств и оборудования ИСПДн.

2.7. Контролировать исполнение пользователями ИСПДн введенного режима безопасности, а также правильность работы с элементами ИСПДн и средствами защиты.

2.8. Контролировать исполнение пользователями парольной политики.

2.9. Периодически представлять руководству отчет о состоянии защиты ИСПДн, о нештатных ситуациях на объектах ИСПДн и допущенных пользователями нарушениях установленных требований по защите информации.

2.10. В случае отказа работоспособности технических средств и программного обеспечения ИСПДн, в том числе средств защиты, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.11. Принимать меры по реагированию, в случае возникновения нештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

2.12. Обеспечивать установку, настройку и своевременное обновление элементов ИСПДн:

- программного обеспечения АРМ и серверов (операционные системы, прикладное и специальное ПО);
- антивирусного ПО;
- аппаратных средств;
-аппаратных и программных средств защиты.

2.13. Обеспечивать работоспособность элементов ИСПДн и локальной вычислительной сети.

2.14. Осуществлять еженедельное резервное копирование информации, содержащей ПДн.

2.15. Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.

2.16. Обеспечивать функционирование и поддержку работоспособности средств защиты информации, либо по согласованию с руководителем привлекать для этого организацию, имеющую оформленную в установленном порядке лицензию на осуществление деятельности по технической защите конфиденциальной информации.

2.17. В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.18. Проводить периодический контроль работоспособности элементов ИСПДн в пределах возложенных на него функций.

2.19. В случае необходимости хранить, осуществлять прием и выдачу персональных паролей пользователей, осуществлять контроль за правильностью использования персонального пароля пользователями ИСПДн.

2.20. Информировать ответственного за организацию обработки и обеспечение безопасности персональных данных о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

2.21. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты информации.

2.22. Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения информации.

2.23. Присутствовать при выполнении технического обслуживания элементов ИСПДн сторонними физическими лицами и организациями.

2.24. В случае возникновения нештатных и аварийных ситуаций принимать меры по реагированию с целью их предотвращения либо ликвидации их последствий.