УТВЕРЖДАЮ

Директор МАОУ СОШ № 51

_____О.В.Тропина

«01» сентября 2023г.

ИНСТРУКЦИЯ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

г. Краснодар, 2023

Содержание

1. Общие положения

1.1. Администратор безопасности информационных систем персональных данных (ИСПДн) (далее – Администратор) назначается приказом руководителя МАОУ СОШ № 51, на основании Положение о разграничении прав доступа к обрабатываемым персональным данным.

1.2. Администратор подчиняется директору школы.

1.3. Администратор в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами ФСТЭК России и регламентирующими документами МАОУ СОШ № 51.

1.4. Администратор отвечает за поддержание необходимого уровня безопасности объектов защиты.

1.5. Администратор безопасности является ответственным должностным лицом МАОУ СОШ № 51, уполномоченным на проведение работ по технической защите информации и поддержанию достигнутого уровня защиты ИСПДн и ее ресурсов на этапах промышленной эксплуатации и модернизации.

1.6. Администратор безопасности должен иметь специальное рабочее место, размещенное в здании МАОУ СОШ № 51 так, чтобы исключить несанкционированный доступ к нему посторонних лиц и других пользователей.

1.7. Рабочее место администратора безопасности должно быть оборудовано средствами физической защиты (личный сейф, железный шкаф, запирающийся шкаф или другое), подключением к ИСПДн, а так же средствами контроля за техническими средствами защиты.

1.8. Администратор безопасности осуществляет методическое руководство Оператора и Администраторов ИСПДн в вопросах обеспечения безопасности персональных данных.

1.9. Требования администратора информационной безопасности, связанные с выполнением своих должностных обязанностей, обязательны для исполнения всеми пользователями ИСПДн.

1.10. Администратор безопасности несет персональную ответственность за качество проводимой им работы по контролю. Действий пользователей при работе в ИСПДн, состояние и поддержание установленного уровня защиты ИСПДн.

2. Должностные обязанности

Администратор безопасности обязан:

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

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

- программного обеспечения автоматизированных рабочих мест (АРМ) и серверов (операционные системы, прикладное и специальное программное обеспечение (ПО));
- аппаратных средств;
- аппаратных и программных средств защиты.

2.3. участвовать в контрольных и тестовых испытаниях и проверках элементов ИСПДн.

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

2.5. Участвовать в приеме новых программных средств.

2.6. 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.

2.7. Обеспечить доступ к защищаемой информации пользователями ИСПДн согласно их правам доступа при получении оформленного соответствующим образом разрешения.

2.8. Уточнять в установленном порядке обязанности пользователей ИСПДн по обработке объектов защиты.

2.9. Осуществлять постоянный контроль за выполнением пользователями Плана мероприятий по защите персональных данных.

2.10. Анализировать состояние защиты ИСПДн и ее отдельных подсистем.

2.11. Контролировать неизменность состояния средств защиты, их параметров и режимов защиты.

2.12. Контролировать физическую сохранность средств и оборудования ИСПДн.

2.13. Контролировать исполнение пользователем ИСПДн введенного режима безопасности, а так же правильность работы с элементами ИСПДн и средствами защиты.

2.14. Контролировать исполнение пользователями парольной политики.

2.15. Контролировать работу пользователей в сетях общего пользования и (или) международного обмена.

2.16. Своевременно анализировать журнал учета событий, регистрируемых средствами защиты, с целью выявления возможных нарушений.

2.17. Не допускать установку, использование, хранение и размножение в ИСПДн программных средств, не связанных с выполнением функциональных задач.

2.18.Не допускать к работе на элементах ИСПДн посторонних лиц.

2.19. Осуществлять периодические контрольные проверки рабочих станций и тестирование правильности функционирования средств защиты ИСПДн.

2.20. Оказывать помощь пользователям ИСПДн в части применения средств защиты и консультировать по вопросам введенного режима защиты.

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

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

3. Права и ответственность АДМИНИСТРАТОРА безопасности

3.1 Администратор безопасности имеет право в отведенное ему время решать поставленные задачи в соответствии с его полномочиями в отношениях к ресурсам ИСПДн, и вверенным ему техническим и программным средствам. В частности администратор безопасности имеет право:

- проверять электронный журнал обращений;
- вносить изменения в конфигурацию аппаратно – программных средств;
- проверять соблюдение условий использования средств защиты информации;
- требовать прекращения обработки информации как в целом, так и отдельных пользователей в случае выявления наркшений установленного порядка работ или нарушения функционирования АРМ.

3.2 Администраторы безопасности, виновные в несоблюдении Настоящей инструкции расцениваются как нарушители Федерального закона РФ 27.07.2006 г. N 152-ФЗ "О персональных данных" и несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.