УТВЕРЖДАЮ
Директор МАОУ СОШ № 31
_____ Е.В. Иванова
«_1_» _09_____2023г.

Инструкция

Администратора информационной безопасности
муниципального автономного общеобразовательного учреждения города Калининграда
средняя общеобразовательная школа № 31
(МАОУ СОШ № 31)

1 Общие положения

1.1. Администратор информационной безопасности (далее – Администратор) назначается приказом директора муниципального автономного общеобразовательного учреждения города Калининграда средней общеобразовательной школы № 31 (далее - МАОУ СОШ № 31).

1.2. Администратор в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами ФСБ РФ и ФСТЭК РФ и регламентирующими документами МАОУ СОШ № 31.

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

1.4. Администратор является ответственным должностным лицом, уполномоченным на проведение работ по технической защите информации и поддержанию достигнутого уровня защиты информационной системы персональных данных (далее – ИСПДн) МАОУ СОШ № 31.

1.5. Рабочее место Администратора должно быть оборудовано средствами физической защиты (личный сейф, металлический шкаф, иное хранилище), а также средствами контроля над техническими средствами защиты.

1.6. Требования Администратора, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми пользователями ИСПДн.

1.7. Администратор несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИСПДн, состояние и поддержание установленного уровня защиты ИСПДн.

2 Должностные обязанности

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

2.3. Участвовать в приемке новых программных средств.

2.4. Обеспечить доступ к защищаемой информации пользователям ИСПДн, согласно их правам доступа, при получении оформленного соответствующим образом разрешения.

2.5. Вести контроль над процессом осуществления резервного копирования объектов защиты.

2.6. Осуществлять контроль над выполнением Плана мероприятий по защите персональных данных.

2.7. Анализировать состояние защиты ИСПДн и ее отдельных подсистем.

2.8. Контролировать неизменность состояния средств защиты их параметров и режимов защиты.

2.9. Контролировать физическую сохранность средств и оборудования ИСПДн.

2.10. Контролировать исполнение пользователями ИСПДн правильность работы с элементами ИСПДн и средствами защиты.

2.11. Контролировать исполнение пользователями парольной политики.

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

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

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

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

2.16. Периодически представлять ответственному за организацию обработки ПДн отчет о состоянии защиты ИСПДн и о нештатных ситуациях на объектах ИСПДн и допущенных пользователями нарушениях установленных требований по защите информации.

2.17. 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.

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