Утверждено
Директор МБОУ гимназии № 54
города Краснодара
_____ Н.В. Россошных
16 сентября 2015 года

Россошных Наталья Викторовна

Подписан: Россошных Наталья Викторовна
DN: C=RU, CN=Россошных Наталья Викторовна, E=yulia_03b@mail.ru
Основание: Я являюсь автором этого документа
Местоположение: место вашего подписания
Дата: 2022-04-18 03:14:57
Foxit Reader Версия: 9.5.0

ИНСТРУКЦИЯ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

Краснодар, 2015

Содержание

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Администратор безопасности информационных систем персональных данных (ИСПДн) (далее – Администратор) назначается приказом директора МБОУ Гимназии № 54, на основании Положения о разграничении прав доступа к обрабатываемым персональным данным.

1.2. Администратор подчиняется директору МБОУ Гимназии № 54

1.3. Администратор в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами ФСТЭК России и регламентирующими документами МБОУ Гимназии № 54.

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

1.5. Администратор безопасности является ответственным должностным лицом МОУ Гимназии № 54, 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 Гимназии так, что бы 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 или другое), подключением к ИСПДн, а так же средствами контроля за техническими средствами защиты.

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

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

1.10. Администратор безопасности 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 безопасности обязан:

– 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;

– осуществлять установку, настройку и сопровождение технических средств защиты;

– участвовать в контрольных и тестовых испытаниях и проверках элементов ИСПДн;

– участвовать в приеме новых программных средств;

– обеспечить доступ к защищаемой информации пользователям ИСПДн согласно их правам доступа при получении оформленного соответствующим образом разрешения;

– уточнять в установленном порядке обязанности пользователей ИСПДн по обработке объектов защиты;

– вести контроль над процессом осуществления резервного копирования объектов защиты;

– осуществлять контроль над выполнением Плана мероприятий по защите персональных данных;

– анализировать состояние защиты ИСПДн и ее отдельных подсистем;

– контролировать неизменность состояния средств защиты их параметров и режимов защиты;

– контролировать физическую сохранность средств и оборудования ИСПДн;

– контролировать исполнение пользователями ИСПДн введенного режима безопасности, а так же правильность работы с элементами ИСПДн и средствами защиты;

– контролировать исполнение пользователями парольной политики;

– контролировать работу пользователей в сетях общего пользования и (или) международного обмена;

– своевременно анализировать журнал учета событий, регистрируемых средствами защиты, с целью выявления возможных нарушений;

– не допускать установку, использование, хранение и размножение в ИСПДн программных средств, не связанных с выполнением функциональных задач;

– не допускать к работе на элементах ИСПДн посторонних лиц;

– осуществлять периодические контрольные проверки рабочих станций и тестирование правильности функционирования средств защиты ИСПДн;

– оказывать помощь пользователям ИСПДн в части применения средств защиты и консультировать по вопросам введенного режима защиты;

– периодически представлять руководству отчет о состоянии защиты ИСПДн и о нештатных ситуациях на объектах ИСПДн и допущенных пользователями нарушениях установленных требований по защите информации;

– 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;

– 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 нарушений 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.