

УТВЕРЖДАЮ

Директор школы

Л.В. Раздайбеда

»15.05.2018



ИНСТРУКЦИЯ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

МУНИЦИПАЛЬНОГО БЮДЖЕТНОГО ОБЩЕОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ УСОЛЬСКОЙ СРЕДНЕЙ ШКОЛЫ

СОДЕРЖАНИЕ

1 Общие положения	3
2 Должностные обязанности	3
2.1 Обязанности администратора безопасности:	3
2.2.Права администратора безопасности персональных данных:	4

1. Общие положения

Администратор безопасности МБОУ УСШ назначается руководителем, на основании приказа «О назначении сотрудников, ответственных за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных» из числа работников структурного подразделения, ответственного за обеспечение безопасности персональных данных (далее - ПДн) или иных сотрудников МБОУ УСШ. В своей работе Администратор информационной безопасности (далее - АИБ) руководствуется законодательством Российской Федерации в области обеспечения безопасности ПДн, руководящими и нормативными документами ФСТЭК России и ФСБ России, а так же организационно-распорядительными документам МБОУ УСШ. Администратор безопасности является ответственным должностным лицом МБОУ УСШ, уполномоченным на проведение работ по технической защите информации и поддержанию достигнутого уровня защиты информационных систем персональных данных (далее – ИСПДн) и их ресурсов на этапах промышленной эксплуатации и модернизации.

Совместно с лицом, ответственным за организацию обработки ПДн, и лицом, ответственным за обеспечение безопасности ПДн, АИБ осуществляет методическое руководство и сопровождение пользователей ИСПДн и системных администраторов ИСПДн, в вопросах обеспечения безопасности персональных данных.

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

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.

Администратор безопасности должен иметь специальное рабочее место, размещенное в здании «НО» так, чтобы исключить несанкционированный доступ к нему посторонних лиц и других пользователей.

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.

2. Должностные обязанности

2.1. Обязанности администратора безопасности:

2.1.2. Осуществлять установку, настройку и сопровождение средств защиты информации (далее - СЗИ).

2.1.3. Участвовать в контрольных и тестовых испытаниях, и проверках элементов ИСПДн.

2.1.4. Участвовать в приемке новых программных средств.

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

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

- 2.1.7. Вести контроль над процессом осуществления резервного копирования объектов защиты.
- 2.1.8. Осуществлять выполнение мероприятий по осуществлению внутреннего контроля за обеспечением уровня защищенности ПДн и соблюдением условий использования СЗИ, а также соблюдением требований законодательства Российской Федерации по обработке ПДн в ИСПДн.
- 2.1.9. Контролировать неизменность состояния средств защиты их параметров и режимов защиты.
- 2.1.10. 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.
- 2.1.11. Контролировать физическую сохранность средств и оборудования ИСПДн.
- 2.1.12. Контролировать в рамках своих полномочий исполнение пользователями ИСПДн введенного режима безопасности, а так же правильность работы с элементами ИСПДн и средствами защиты, в том числе на основании Порядка обеспечения антивирусной защиты ИСПДн и Порядка обеспечения парольной защиты ИСПДн, утвержденных регламентом обеспечения безопасности ПДн, обрабатываемых в ИСПДн.
- 2.1.13. Контролировать исполнение пользователями парольной политики.
- 2.1.14. Контролировать работу пользователей в сетях общего пользования и (или) международного обмена.
- 2.1.15. Своевременно анализировать журнал учета событий, регистрируемых средствами защиты, с целью выявления возможных нарушений.
- 2.1.16. Не допускать установку, использование, хранение и размножение в ИСПДн программных средств, не связанных с выполнением функциональных задач.
- 2.1.17. Оказывать помощь пользователям ИСПДн в части применения средств защиты и консультировать по вопросам введенного режима защиты.
- 2.1.18. Периодически представлять руководству отчет о состоянии защиты ИСПДн, о нештатных ситуациях на объектах ИСПДн и допущенных пользователями нарушениях установленных требований по защите информации.

2.2. Права администратора безопасности персональных данных:

- 2.1.1. 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.
- 2.2.1. Не допускать к работе на элементах ИСПДн лиц, не получивших в установленном порядке право доступа к персональным данным, обрабатываемым в ИСПДн.
- 2.2.2. Участвовать в периодических контрольных проверках состояния защищённости тиражируемых объектов ИСПДн, рабочих станций пользователей и тестирования правильности функционирования средств защиты ИСПДн.
- 2.2.3. Обращаться к ответственному за обеспечение безопасности или ответственному за организацию обработки персональных данных «НО» с предложениями по совершенствованию системы защиты персональных данных ИСПДн.

2.2.4.Принимать необходимые меры по оперативному реагированию, в случае возникновения внештатной ситуации, с целью ликвидации ее последствий.

Директор школы

Л.В. Раздайбеда

С инструкцией ознакомлен (а) _____

(дата)

(подпись)

(расшифровка подписи)

инструкцию получил (а): _____

(дата)

(подпись)

(расшифровка подписи)

В дело №

(личная подпись)

«_____» _____ 20__ г.