Я.А.К.

Утверждаю
Директор школы
Карницкая Л.Ю.

Приказ № 99 от 21.03.2016г.

ИНСТРУКЦИЯ
ответственного за обеспечение безопасности персональных данных информационных систем персональных данных в МБОУ «Большетроицкая СОШ»

I. Общие положения

1. Настоящая инструкция (далее – Инструкция) определяет общие функции, ответственность, права и обязанности ответственного за обеспечение безопасности персональных данных информационных систем персональных данных (далее – Ответственный) в Муниципальном бюджетном общеобразовательном учреждении «Большетроицкая средняя общеобразовательная школа Шебекинского района Белгородской области» (далее – ОУ).

2. Настоящая инструкция разработана в соответствии с руководящими и нормативными документами регуляторов Российской Федерации в области защиты персональных данных.

3. Ответственный назначается приказом по ОУ на основании «Положения о разграничении прав доступа к обрабатываемым персональным данным» в Школе из числа штатных сотрудников.

4. Ответственный подчиняется непосредственно Директору ОУ.

5. На время отсутствия Ответственного (отпуск, болезнь, пр.) его обязанности исполняет лицо, назначенное в установленном порядке, которое приобретает соответствующие права и несет ответственность за надлежащее исполнение возложенных на него обязанностей.

6. Ответственный в своей работе руководствуется настоящей Инструкцией, Политикой информационной безопасности ОУ, другими регламентирующими документами ОУ, руководящими и нормативными документами регуляторов Российской Федерации в области обеспечения безопасности персональных данных.

7. Методическое руководство работой Ответственного осуществляется ответственным за организацию обработки персональных данных в ОУ.

8. Ответственный является ответственным лицом, уполномоченным на проведение работ по технической защите информации и поддержанию необходимого уровня защищенности ИСПДн ОУ и их ресурсов на этапах эксплуатации и модернизации.

II. Организация работы

1. Ответственный должен иметь специальное рабочее место, размещённое на территории контролируемой зоны, установленной приказом директора ОУ, чтобы исключить несанкционированный доступ к нему посторонних лиц и других сотрудников ОУ.

2. Рабочее место Ответственного должно быть оборудовано средствами физической защиты (личный сейф, железный шкаф или другое), подключением к ИСПДн, а так же средствами контроля технических средств защиты информации (далее – СЗИ).

III. Обязанности

Ответственный должен:

1. Соблюдать требования законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, «Правил обработки персональных данных» и других нормативных документов ОУ в области обработки и защиты персональных данных.

2. Поддерживать необходимый уровень защищенности (режим безопасности) персональных данных при их обработке в ИСПДн согласно «Инструкции по обеспечению безопасности персональных данных».

3. Наделять и изменять права доступа всех групп пользователей ИСПДн к персональным данным и защищаемым программным ресурсам и портам ввода-вывода ИСПДн.

4. Осуществлять установку, настройку и сопровождение программных и технических СЗИ.

5. Осуществлять методическое руководство всех групп пользователей ОУ в вопросах функционирования СЗИ и введенного режима защиты.

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

7. Участвовать в приемке новых программных и технических средств, в том числе СЗИ.

8. Участвовать в проведении расследований случаев несанкционированного доступа к персональным данным и других нарушений «Правил обработки персональных данных».

9. Обеспечить доступ к защищаемой информации всем группам пользователей ИСПДн согласно их правам доступа при получении оформленного соответствующим образом разрешения.

10. Уточнять в установленном порядке обязанности всех групп пользователей ИСПДн по обеспечению безопасности персональных данных.

11. Вести контроль над процессом осуществления резервного копирования баз данных и настроек комплекса средств автоматизации ИСПДн согласно «Инструкции по порядку резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и СЗИ».

12. Осуществлять контроль порядка учёта, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.

13. Осуществлять контроль выполнения «Плана мероприятий по обеспечению защиты персональных данных в ОУ.

14. Анализировать состояние защиты ИСПДн и их отдельных подсистем.

15. Контролировать неизменность состояния СЗИ, их параметров и режимов защиты.

16. Контролировать физическую сохранность СЗИ и оборудования ИСПДн.

17. Контролировать исполнение всеми группами пользователей ИСПДн введённого режима защищенности, а так же правильность работы с элементами ИСПДн и СЗИ.

18. Контролировать исполнение всем группами пользователей ИСПДн парольной политики согласно «Инструкции по организации парольной защиты»

19. Организовывать антивирусную защиту всех элементов ИСПДн согласно «Инструкции по организации антивирусной защиты».

20. Своевременно анализировать журнал учёта событий, регистрируемых СЗИ, с целью выявления возможных нарушений.

21. Недопускать установку, использование, хранение и размножение в ИСПДн ПО, не связанных с выполнением функциональных задач.

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

23. Регистрировать факты выдачи внешних носителей в «Журнале учета мобильных технических средств».

24. Осуществлять периодические контрольные проверки рабочих станций и тестирование правильности функционирования СЗИ ИСПДн.

25. Периодически представлять руководству отчёт о состоянии и о нештатных ситуациях на объектах ИСПДн и допущенных всеми группами пользователей нарушениях и установленных требований по защите информации.

26. В случае отказа работоспособности СЗИ ИСПДн, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

27. Принимать меры по реагированию в случае возникновения нештатных или аварийных ситуаций с целью ликвидации их последствий.

28. Предлагать руководству мероприятия по совершенствованию работы по защите персональных данных.

IV. Права

Ответственный имеет право

1. Требовать от всех групп пользователей ИСПДн соблюдения законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, «Правил обработки персональных данных» и других нормативных документов Школы в области обработки и защиты персональных данных.

2. Запрещать всем группам пользователей ИСПДн доступ к персональным данным при нарушении «Правил обработки персональных данных», при неисправностях в работе СЗИ и с целью предотвращения несанкционированного доступа к охраняемой информации.

3. Участвовать в анализе ситуаций, касающихся функционирования СЗИ, и в расследованиях по случаям несанкционированного доступа к персональным данным и другим случаям нарушения режима обработки персональных данных.

4. Вносить предложения руководству по совершенствованию работы, связанной с предусмотренными настоящей инструкцией обязанностями.

5. В пределах своей компетенции сообщать руководству о недостатках, выявленных в процессе исполнения должностных обязанностей, и вносить предложения по их устранению.

6. Требовать от руководства оказания содействия в исполнении своих должностных обязанностей и прав.

7. Привлекать с разрешения руководства сотрудников всех структурных подразделений к решению задач, возложенных на него.

8. Запрашивать лично или через директора Школы информацию и документы, необходимые для выполнения своих должностных обязанностей.

V. Ответственность

Ответственный несет ответственность:

1. За качество проводимых работ по контролю всех групп пользователей ИСПДн в вопросах обеспечения безопасности персональных данных.

2. За обеспечение устойчивой работоспособности СЗИ ИСПДн.

3. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим трудовым законодательством Российской Федерации.

4. За правонарушения, совершенные в процессе осуществления своей деятельности, в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

5. За причинение материального ущерба – в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.

VI. Порядок пересмотра инструкции

1. Настоящая Инструкция пересматривается, изменяется и дополняется по мере необходимости, но не реже одного раза в три года.

2. С приказом о внесении изменений (дополнений) в настоящую Инструкцию знакомятся под расписку все сотрудники ОУ, на которых распространяется действие этой инструкции.