Муниципальное автономное общеобразовательное учреждение
«Основная общеобразовательная школа №2»

ПРИКАЗ

16 декабря 2024 № 534

г. Верхотурье

О назначении ответственных за защиту информации и утверждении инструкций ответственных

В целях исполнения требований Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», реализации мер по защите информации, не составляющей государственную тайну, требование озащите которой, установлено законодательством Российской Федерации, нормативными правовыми актами Правительства Российской Федерации, в МАОУ «ООШ № 2»

ПРИКАЗЫВАЮ:

1. Назначить специалистом, ответственным за защиту информации в МАОУ «ООШ № 2» учителя Степанову Л.А.

2. Специалисту, ответственному за защиту информации в МАОУ «ООШ № 2», самостоятельно или с привлечением организаций-лицензиатов ФСТЭК России и/или ФСБ России обеспечить:

– определение основных технических каналов утечки информации, возможностей несанкционированного доступа к информации, ее разрушения (уничтожения) или искажения, разработку соответствующих требований и мер по защите информации;

– разработку и/или согласование технических (частных технических) заданий на проведение работ, оказание услуг по защите информации, поставку средств защиты информации;

– разработку проектов локальных нормативных актов по вопросам защиты информации;

– согласование возможности безопасной эксплуатации информационных систем (и других объектов информатизации) для обработки защищаемой информации.

3. Назначить ответственным за организацию обработки персональных данных в МАОУ «ООШ № 2» заместителя директора Мартынову И.С.

4. Утвердить инструкцию ответственного за организацию обработки персональных данных в соответствии с Приложением № 1 к настоящему приказу.

5. Назначить ответственным за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных учителя, ответственного за информационный обмен Степанову Л.А.

6. Утвердить инструкцию ответственного за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных в соответствии с Приложением № 2 к настоящему приказу.

7. Назначить администратором информационной безопасности техника Попкова А.А.

8. Утвердить инструкцию администратора информационной безопасности в соответствии с Приложением № 3 к настоящему приказу.

9. Делопроизводителю Зуевой М.Ю настоящий приказ довести до сведения сотрудников, указанных в настоящем приказе, под подпись.

10. Контроль за выполнением требований настоящего приказа оставляю за собой.

Директор  Е.А. Субботина

Приложение № 1
к приказу «О назначении
ответственных за защиту
информации»
от «16» декабря 2024 г. № 534

Инструкция

ответственного за организацию обработки персональных данных

1. Общие сведения

Настоящая инструкция разработана в соответствии с требованиями Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» с целью определения обязанностей, ответственности и прав ответственного за организацию обработки персональных данных в МАОУ «ООШ № 2».

Ответственный за организацию обработки персональных данных назначается приказом директора МАОУ «ООШ № 2».

2. Обязанности ответственного за организацию обработки персональных данных

К функциональным обязанностям ответственного за организацию обработки персональных данных относится:

– организация внутреннего контроля за соблюдением в МАОУ «ООШ № 2» и сотрудниками МАОУ «ООШ № 2» законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

– организация доведения до сведения сотрудников МАОУ «ООШ № 2» положений законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

– организация приема и обработки обращений и запросов субъектов персональных данных или их представителей, а также осуществление контроля за приемом и обработкой таких обращений и запросов.

3. Ответственность ответственного за организацию обработки персональных данных

Ответственный за организацию обработки персональных данных несет ответственность за:

– неисполнение (ненадлежащее исполнение) своих обязанностей, предусмотренных настоящей Инструкцией;

– совершенные в процессе осуществления своей деятельности правонарушения несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, предусмотренном законодательством Российской Федерации.

4. Права ответственного за организацию обработки персональных данных

Ответственный за организацию обработки персональных данных вправе:

– осуществлять внутренний контроль за соблюдением в МАОУ «ООШ № 2» и сотрудниками МАОУ «ООШ № 2» законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

– требовать прекращения обработки персональных данных в случае выявления нарушений требований по обработке и обеспечению безопасности персональных данных.

Приложение № 2
к приказу «О назначении
ответственных за защиту
информации»
от «16» декабря 2024 г. № 534

Инструкция

ответственного за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных

1. Общие сведения

Настоящая инструкция разработана в соответствии с требованиями Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» с целью определения обязанностей, ответственности и прав ответственного за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных МАОУ «ООШ № 2».

Ответственный за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных назначается приказом директора МАОУ «ООШ № 2».

2. Обязанности ответственного за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных

К функциональным обязанностям ответственного за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных относится:

– организация работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;

– представление руководству отчетов о состоянии защиты персональных данных, обрабатываемых в информационных системах персональных данных;

– участие в составе комиссии при проведении служебных проверок по фактам нарушений требований по обеспечению безопасности персональных данных;

– оперативное принятие мер по пресечению нарушений требований по обеспечению безопасности персональных данных.

3. Ответственность ответственного за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных

Ответственный за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных несет ответственность за:

– неисполнение (ненадлежащее исполнение) своих обязанностей, предусмотренных настоящей Инструкцией;

– совершенные в процессе осуществления своей деятельности правонарушения несут

материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, предусмотренном законодательством Российской Федерации.

4. Права ответственного за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных

Ответственный за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных вправе:

– получать сведения об актуальном состоянии защиты персональных данных, обрабатываемых в информационных системах персональных данных, а также отчеты о результатах работ, направленных на обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных;

– требовать прекращения обработки персональных данных в случае выявления нарушений требований по обработке и обеспечению безопасности персональных данных.

Приложение № 3
к приказу «О назначении
ответственных за защиту
информации»
от «16» декабря 2024 г. № 534

Инструкция

администратора информационной безопасности

1. Общие сведения

Настоящая инструкция разработана в соответствии с требованиями Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» с целью определения функций, обязанностей, ответственности и прав администратора информационной безопасности в МАОУ «ООШ № 2».

Администратор информационной безопасности назначается приказом директора МАОУ «ООШ № 2».

2. Обязанности администратора информационной безопасности

Администратор информационной безопасности обязан:

– обеспечивать функционирование и поддерживать работоспособность средств защиты информации (далее – СЗИ) автоматизированных рабочих мест (далее – АРМ) пользователей информационных систем (далее – ИС), в пределах, возложенных на него функций;

– в случае отказа работоспособности технических средств и программного обеспечения, средств вычислительной техники, в том числе СЗИ, принимать меры по их своевременному восстановлению и выявлению причин, которые вызвали отказ работоспособности;

– информировать руководство о фактах нарушения установленного порядка работ, попытках и фактах несанкционированного доступа (далее – НСД) к персональным данным и информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (далее – защищаемая информация) и ИС.

Администратор информационной безопасности выполняет следующие мероприятия, направленные на обеспечение безопасности защищаемой информации.

1. Настройка и сопровождение системы защиты ИС:

– реализует полномочия доступа для каждого пользователя ИС на основе утвержденного директором МАОУ «ООШ № 2» перечня лиц, имеющих доступ к защищаемой информации;

– своевременно удаляет учетные записи пользователей ИС при увольнении или перемещении сотрудника;

– своевременно блокирует и производит разблокировку учетных записей пользователей ИС при их уходе на больничный или в отпуск и при выходе с больничного или из отпуска;

– периодически, но не реже одного раза в квартал, контролирует смену паролей пользователями для доступа в ИС;

– регистрирует новых пользователей ИС;

– регистрирует средства защиты информации;

– периодически, но не реже одного раза в месяц, выполняет мероприятия по периодическому тестированию функционирования СЗИ в соответствии с документацией разработчика данных средств, регистрируя проведение данных мероприятий.

2. Настройка и сопровождение подсистемы регистрации и учета ИС:

– проводит регулярный анализ системного журнала ИС для выявления попыток несанкционированного доступа к защищаемым ресурсам с соответствующей регистрацией проверки;

– своевременно информирует руководство о несанкционированных действиях персонала и участвует в разбирательствах по фактам попыток НСД;

– проводит резервное копирование информационных массивов ИС.

3. Сопровождение подсистемы обеспечения целостности ИС:

– осуществляет учет возникновения нештатных ситуаций;

– осуществляет восстановление ИС при возникновении сбоев.

4. Контроль функционирования подсистемы антивирусной защиты ИС:

– обеспечивает поддержание установленного порядка и соблюдение правил антивирусной защиты;

– периодически, но не реже одного раза в месяц, проводит антивирусные проверки всех жестких дисков АРМ пользователей ИС;

– регистрирует результаты антивирусных проверок.

5. Контроль использования машинных носителей информации и ведение их учета.

6. Сопровождение подсистемы межсетевого экранирования ИС.

7. Организация обновлений программного обеспечения и СЗИ, выполнение профилактических работ, установки и модификации программных средств на АРМ пользователей ИС.

8. Проведение модернизации аппаратных компонентов.

9. Проведение инструктажа сотрудников, имеющих право доступа к защищаемой информации.

10. Осуществление контроля за соблюдением пользователями ИС требований к защите персональных данных.

11. Участие в анализе ситуаций, касающихся функционирования СЗИ и проверки фактов НСД.

12. Оказание методической помощи по вопросам обеспечения безопасности защищаемой информации пользователям ИС.

13. Разработка предложений и участие в проводимых работах по совершенствованию системы обеспечения безопасности защищаемой информации.

14. Проведение внутреннего контроля соответствия обработки персональных данных требованиям к обеспечению безопасности персональных данных в МАОУ «ООШ № 2».

15. Управление (администрирование) системой защиты информации ИС.

16. Управление конфигурацией ИС и ее системой защиты информации.

17. Реагирование на инциденты безопасности.

18. Информирование и обучение персонала по вопросам информационной безопасности в МАОУ «ООШ № 2».

19. Планирование мероприятий по обеспечению защиты информации в МАОУ «ООШ № 2».

20. Контроль за обеспечением уровня защищенности информации в ИС.

21. Анализ угроз безопасности информации в ИС:

– осуществляет выявление, анализ и устранение уязвимостей ИС;

– проводит анализ изменения угроз безопасности информации в ИС;

– проводит оценку возможных последствий реализации угроз безопасности информации в ИС.

22. Осуществление взаимодействия с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных.

3. Ответственность администратора информационной безопасности

Администратор информационной безопасности несет ответственность за:

– неисполнение (ненадлежащее исполнение) своих обязанностей, предусмотренных настоящей Инструкцией;

– совершенные в процессе осуществления своей деятельности правонарушения в пределах, определенных административным, уголовным и гражданским законодательством Российской Федерации;

– невыполнение или ненадлежащее выполнение указаний руководства;

– соблюдение требований нормативных правовых актов в сфере защиты информации и локальных актов МАОУ «ООШ № 2», определяющих порядок организации и проведения работ, направленных на обеспечение безопасности защищаемой информации при ее обработке;

– сохранность и работоспособное состояние технических средств, программного обеспечения, СЗИ, входящих в состав ИС.

4. Права администратора информационной безопасности

Администратор информационной безопасности вправе:

– контролировать работу пользователей ИС;

– требовать прекращения обработки информации, как в целом, так и отдельных пользователей ИС, в случае выявления нарушений требований по обработке и обеспечению безопасности защищаемой информации или функционирования ИС.

ЛИСТ ОЗНАКОМЛЕНИЯ

№ п/п	Ф.И.О.	Дата ознакомления	Подпись
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			
21.			
22.			
23.			
24.			
25.			
26.			
27.			
28.			
29.			
30.			
31.			
32.			
33.			
34.			