

Принято решением педагогического Совета
МКОУ «СОШ № 2 пос. Мамедкала протокол
№ 4 от 30.09.2019

Утверждено приказом директора
МКОУ «СОШ № 2 пос. Мамедкала»
протокол № 1 от 30.09.2019
Ибрагимова З.Д.



Инструкция
администратора безопасности информации МКОУ «СОШ №2 п.Мамедкала»

1. Общие положения

1.1. Настоящая Инструкция определяет обязанности должностного лица (далее – администратора безопасности), ответственного за обеспечение безопасности информационных систем (в том числе персональных данных, обрабатываемой в информационных системах – далее ИСПДн) МКОУ «СОШ №2 п.Мамедкала»

1.2. Администратор безопасности назначается приказом директора школы.

1.3. Администратор безопасности по вопросам обеспечения безопасности информации подчиняется директору, заместителю директора по учебно-воспитательной работе (школьные информационные сети) МКОУ «СОШ №2 п.Мамедкала»

1.4. Администратор безопасности отвечает за поддержание установленного уровня безопасности защищаемой информации, в том числе персональных данных, при их обработке в ИСПДн.

1.5. Администратор безопасности осуществляет методическое руководство деятельностью пользователей ИСПДн МКОУ «СОШ №2 п.Мамедкала» в вопросах обеспечения безопасности информации.

1.6. Требования администратора безопасности, связанные с выполнением им своих обязанностей, обязательны для исполнения всеми пользователями ИСПДн МКОУ «СОШ №2 п.Мамедкала»

1.7 Администратор безопасности несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИСПДн СОШ №2 п.Мамедкала», состояние и поддержание установленного уровня защиты информации, обрабатываемой в ИСПДн МКОУ «СОШ №2 п.Мамедкала»

2. Задачи администратора безопасности.

2.1. Основными задачами администратора безопасности являются:

- поддержание необходимого уровня защиты ИСПДн ГБОУ МКОУ «СОШ №2 п.Мамедкала» от несанкционированного доступа к информации;
- обеспечение конфиденциальности обрабатываемой, хранимой и передаваемой по каналам связи информации;
- установка средств защиты информации и контроль выполнения правил их эксплуатации;
- сопровождение средств защиты информации (далее - СЗИ) от несанкционированного доступа и основных технических средств и систем ИСПДн МКОУ «СОШ №2 п.Мамедкала»;
- периодическое обновление СЗИ и комплекса мероприятий по предотвращению инцидентов информационной безопасности;
- оперативное реагирование на нарушения требований по информационной безопасности в ИСПДн МКОУ «СОШ №2 п.Мамедкала» и участие в их прекращении.

2.2. В рамках выполнения основных задач администратор безопасности осуществляет:

- текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических СЗИ;
- текущий контроль технологического процесса автоматизированной обработки персональных данных;
- участие в проведении служебных расследований фактов нарушений или угрозы нарушений безопасности персональных данных;
- контроль соблюдения нормативных требований по защите информации, обеспечения комплексного использования технических средств, методов и организационных мероприятий по безопасности информации в МКОУ «СОШ №2 п.Мамедкала».
- методическую помощь всем работникам МКОУ «СОШ №2 п.Мамедкала» по вопросам обеспечения безопасности персональных данных.

3. Обязанности администратора безопасности информации.

Администратор безопасности обязан:

- 3.1. Знать и выполнять требования нормативных документов по защите информации, регламентирующих порядок защиты информации, обрабатываемой в ИСПДн МКОУ «СОШ №2 п.Мамедкала»
- 3.2. Участвовать в установке, настройке и сопровождении программных средств защиты информации.
- 3.3. Участвовать в приемке новых программных средств обработки информации.
- 3.4. Обеспечить доступ к защищаемой информации пользователям ИСПДн МКОУ «СОШ №2 п.Мамедкала» согласно их правам доступа при получении оформленного соответствующим образом разрешения (заявки).
- 3.5. Уточнять в установленном порядке обязанности пользователей ИСПДн МКОУ «СОШ №2 п.Мамедкала» при обработке персональных данных.
- 3.6. Вести контроль осуществления резервного копирования информации.
- 3.7. Анализировать состояние защиты ИСПДн МКОУ «СОШ №2 п.Мамедкала».
- 3.8. Контролировать правильность функционирования средств защиты информации и неизменность их настроек.
- 3.9. Контролировать физическую сохранность технических средств обработки информации.
- 3.10. Контролировать исполнение пользователями ИСПДн МКОУ «СОШ №2 п.Мамедкала» введенного режима безопасности, а также правильность работы с элементами ИСПДн и средствами защиты информации.
- 3.11. Контролировать исполнение пользователями правил парольной политики.
- 3.12. Периодически анализировать журнал учета событий, регистрируемых средствами защиты, с целью контроля действий пользователей и выявления возможных нарушений.
- 3.13. Не допускать установку, использование, хранение и размножение в ИСПДн МКОУ «СОШ №2 п.Мамедкала» программных средств, не связанных с выполнением функциональных задач.
- 3.14. Осуществлять периодические контрольные проверки автоматизированных рабочих мест ИСПДн МКОУ «СОШ №2 п.Мамедкала».
- 3.15. Оказывать помощь пользователям ИСПДн МКОУ «СОШ №2 п.Мамедкала» в части применения средств защиты и консультировать по вопросам введенного режима защиты.
- 3.16. Периодически представлять руководству отчет о состоянии защиты ИСПДн МКОУ «СОШ №2 п.Мамедкала» и о нештатных ситуациях и допущенных пользователями нарушениях установленных требований по защите информации.
- 3.17. В случае отказа работоспособности технических средств и программного обеспечения ИСПДн МКОУ «СОШ №2 п.Мамедкала», в том числе средств защиты, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

3.18. В случае выявления нарушений режима безопасности информации персональных данных, а также возникновения внештатных и аварийных ситуаций принимать необходимые меры с целью ликвидации их последствий.

3.19. Принимать участие в проведении работ по оценке соответствия ИСПДн МКОУ «СОШ №2 п.Мамедкала» требованиям безопасности информации.

4. Права администратора безопасности.

Администратор безопасности имеет право:

4.1. Отключать от ресурсов ИСПДн МКОУ «СОШ №2 п.Мамедкала» работников, осуществивших несанкционированный доступ к защищаемым ресурсам ИСПДн или нарушивших другие требования по информационной безопасности.

4.2. Давать работникам обязательные для исполнения указания и рекомендации по вопросам информационной безопасности.

4.3. Инициировать проведение служебных расследований по фактам нарушений установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических средств ИСПДн МКОУ «СОШ №2 п.Мамедкала».

4.4. Организовывать и участвовать в любых проверках по использованию пользователями ГБОУ школе № 327 телекоммуникационных ресурсов.

4.5. Осуществлять контроль информационных потоков, генерируемых пользователями ИСПДн МКОУ «СОШ №2 п.Мамедкала» при работе со съемными носителями информации, подсистемой удаленного доступа.

4.6. Запрещать устанавливать на серверах и автоматизированных рабочих местах нештатное программное и аппаратное обеспечение.

4.7. Вносить на рассмотрение директора предложения по улучшению состояния информационной безопасности персональных данных, обрабатываемых в МКОУ «СОШ №2 п.Мамедкала».

5. Ответственность администратора безопасности.

Администратор безопасности несет ответственность:

5.1. За организацию защиты информационных ресурсов и технических средств ИСПДн МКОУ «СОШ №2 п.Мамедкала».

5.2. За качество проводимых работ по контролю действий пользователей и администраторов ИСПДн, состояние и поддержание необходимого уровня защиты информационных и технических ресурсов ИСПДн МКОУ «СОШ №2 п.Мамедкала».

5.3. За разглашение сведений ограниченного доступа (персональные данные и иная защищаемая информация), ставших известными ему по роду работы.

6. Действия администратора безопасности при обнаружении попыток несанкционированного доступа

6.1. К попыткам несанкционированного доступа относятся:

- сеансы работы с телекоммуникационными ресурсами МКОУ «СОШ №2 п.Мамедкала» пользователей, нарушивших установленную периодичность доступа, либо срок действия полномочий которых истек, либо в состав полномочий которых не входят операции доступа к определенным данным или манипулирования ими;
- действия третьего лица, пытающегося получить доступ (или получившего доступ) к информационным ресурсам ИСПДн МКОУ «СОШ №2 п.Мамедкала» с использованием учетной записи администратора или другого пользователя ИСПДн, в целях получения коммерческой или другой личной выгоды, методом подбора пароля или другого метода (случайного разглашения пароля и т.п.) без ведома владельца учетной записи.

6.2. При выявлении факта/попытки несанкционированного доступа администратор безопасности обязан:

- прекратить доступ к информационным ресурсам со стороны выявленного участка несанкционированного доступа;
- проанализировать характер несанкционированного доступа;
- по решению директора осуществить действия по выяснению причин, приведших к несанкционированному доступу;
- предпринять меры по предотвращению подобных инцидентов в дальнейшем.

Лист ознакомления с настоящей инструкцией в Приложении 1.

Лист ознакомления с инструкцией.

№ п/п	Фамилия, Имя, Отчество	Ознакомлен
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		