

**Муниципальное бюджетное общеобразовательное учреждение
городского округа Тольятти «Школа №20»**

445017, РФ, Самарская обл., г. Тольятти, ул. Голосова, 83.
Телефон/факс (8482) 26 33 53, e-mail: school20@edu.tgl.ru

ПРИНЯТО

на заседании
педагогического совета
Протокол № 1 от 30.08.2019 г.

УТВЕРЖДЕНО

приказом директора
МБУ «Школа №20»
№ 253-од от 30.08.2019 г.
О.Н. Солодовникова



Инструкция администратора информационной безопасности

1. Общие положения

1.1. Настоящая инструкция определяет основные обязанности, права и ответственность администратора безопасности информации в информационных системах персональных данных (далее - ИСПДн).

1.2. Администратор безопасности информации назначается в соответствии с приказом директора школы.

1.3. Администратор безопасности информации осуществляет контроль выполнения требований и организационных мероприятий по обеспечению защиты информации при использовании автоматизированных рабочих мест (далее – АРМ) дополнительно к своим непосредственным обязанностям.

2. Обязанности администратора безопасности информации ИСПДн

2.1 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 Осуществлять установку, настройку и сопровождение средств защиты информации.

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

2.4 Участвовать в приемке новых программных средств.

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

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

2.7 Вести контроль над процессом осуществления резервного копирования объектов защиты.

- 2.8 Анализировать состояние защиты ИСПДн и ее отдельных подсистем.
- 2.9 Контролировать неизменность состояния средств защиты их параметров и режимов защиты.
- 2.10 Контролировать физическую сохранность средств и оборудования ИСПДн.
- 2.11 Контролировать исполнение пользователями ИСПДн введенного режима безопасности, а так же правильность работы с элементами ИСПДн и средствами защиты.
- 2.12 Контролировать исполнение пользователями парольной политики.
- 2.13 Реализовывать парольную политику.
- 2.14 Контролировать работу пользователей в сетях общего пользования и (или) международного обмена.
- 2.15 Своевременно анализировать журнал учета событий, регистрируемых средствами защиты, с целью выявления возможных нарушений.
- 2.16 Не допускать установку, использование, хранение и размножение в ИСПДн программных средств, не связанных с выполнением функциональных задач.
- 2.17 Осуществлять периодические контрольные проверки рабочих станций и тестирование правильности функционирования средств защиты ИСПДн.
- 2.18 Оказывать помощь пользователям ИСПДн в части применения средств защиты и консультировать по вопросам введенного режима защиты.
- 2.19 Периодически представлять руководству отчет о состоянии защиты ИСПДн и о нештатных ситуациях на объектах ИСПДн и допущенных пользователями нарушениях установленных требований по защите информации.
- 2.20 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.
- 2.21 Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

3. Права администратора безопасности информации ИСПДн

- 3.1. Администратор безопасности информации имеет право инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДн.
- 3.2. Администратор безопасности информации имеет право обращаться к ответственному за организацию обработки персональных данных и/или ответственному за эксплуатацию ИСПДн с требованием прекращения работы в ИСПДн при несоблюдении установленной технологии обработки информации и невыполнении требований по защите.

4. Ответственность администратора безопасности информации ИСПДн

- 4.1. На администратора безопасности информации ИСПДн возлагается персональная ответственность за качество проводимых им работ по обеспечению безопасности ПДн в ИСПДн.
- 4.2. Администратор безопасности информации ИСПДн несет ответственность по действующему законодательству за разглашение сведений ограниченного распространения, ставших известными ему по роду работы.