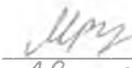


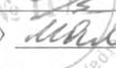
СОГЛАСОВАНО

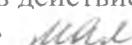
Председатель профсоюзного комитета
МОУ СШ № 117


М.Ю.Рунаева
«26»  2018 г.

УТВЕРЖДАЮ

Директор МОУ СШ № 117


Л.А.Абрамова
«26»  2018 г.

Введена в действие приказом МОУ СШ № 117
от «26»  2018 г. № 144 

ИНСТРУКЦИЯ Администратора безопасности информационных систем персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Администратор безопасности информационных систем персональных данных (ИСПДн) (далее – Администратор) назначается приказом руководителя, МОУ СШ № 117, на основании Положения о разграничении прав доступа к обрабатываемым персональным данным.

1.2. Администратор подчиняется руководителю МОУ СШ № 117.

1.3. Администратор в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами в РФ и регламентирующими документами МОУ СШ № 117

1.4. Администратор отвечает за поддержание необходимого уровня безопасности объектов защиты.

1.5. Администратор безопасности является ответственным должностным лицом, уполномоченным на проведение работ по технической защите информации и поддержанию достигнутого уровня защиты ИСПДн и ее ресурсов.

1.6. Администратор безопасности должен иметь специальное рабочее место, размещенное в здании МОУ СШ № 117 так, что бы исключить несанкционированный доступ к нему посторонних лиц и других пользователей.

1.7. 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.

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

1.9. 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.

2. ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

Администратор безопасности обязан:

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;

осуществлять установку, настройку и сопровождение технических средств защиты;

участвовать в контрольных и тестовых испытаниях и проверках элементов ИСПДн;

участвовать в приеме новых программных средств;

обеспечить доступ к защищаемой информации пользователям ИСПДн согласно их правам доступа при получении оформленного соответствующим образом разрешения;

уточнять в установленном порядке обязанности пользователей ИСПДн по обработке объектов защиты;

вести контроль над процессом осуществления резервного копирования объектов защиты;

осуществлять контроль над выполнением Плана мероприятий по защите персональных данных;

анализировать состояние защиты ИСПДн и ее отдельных подсистем;

контролировать неизменность состояния средств защиты их параметров и режимов защиты;

контролировать физическую сохранность средств и оборудования ИСПДн;

контролировать исполнение пользователями ИСПДн введенного режима безопасности, а так же правильность работы с элементами ИСПДн и средствами защиты;

контролировать исполнение пользователями парольной политики;

не допускать установку, использование, хранение и размножение в ИСПДн программных средств, не связанных с выполнением функциональных задач;

не допускать к работе на элементах ИСПДн посторонних лиц;

оказывать помощь пользователям ИСПДн в части применения средств защиты и консультировать по вопросам введенного режима защиты;

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;

принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

3. ОТВЕТСТВЕННОСТЬ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

3.1 Администратор безопасности имеет право в отведенное ему время решать поставленные задачи в соответствии с его полномочиями в отношении к ресурсам ИСПДн и вверенным ему техническим и программным средствам. В частности, Администратор безопасности имеет право:

- вносить изменения в конфигурацию аппаратно-программных средств
- проверять соблюдение условий использования средств защиты информации

- требовать прекращения обработки информации как в целом, так и отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования АРМ

3.2 Администраторы безопасности, виновные в несоблюдении Настоящей инструкции расцениваются как нарушители Федерального закона РФ 27.07.2006 г. N 152-ФЗ "О персональных данных" (в редакции от 29.07.2017 года) и несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Составитель:
Заместитель директора по УВР



Н.Ю.Бурлакова

С Инструкцией Администратора безопасности информационных систем персональных данных ознакомлена (а):

Львова Е.В.		«29»	мая	2018	г.
_____	_____	«__»	_____	20__	г.
_____	_____	«__»	_____	20__	г.
_____	_____	«__»	_____	20__	г.
_____	_____	«__»	_____	20__	г.