Муниципальное бюджетное учреждение дополнительного образования
«Центр внешкольной работы»

П Р И К А З

от 11 . 02 .2019 № 26 -а

Об утверждении инструкции
по антивирусной защите
в информационных системах
муниципального бюджетного учреждения
дополнительного образования
«Центр внешкольной работы»

В соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативными и методическими документами Федеральной службы по техническому и экспортному контролю Российской Федерации и Федеральной службы безопасности Российской Федерации, на основании Устава муниципального бюджетного учреждения дополнительного образования «Центр внешкольной работы»,

ПРИКАЗЫВАЮ:

1. Утвердить инструкцию по антивирусной защите в информационных системах муниципального бюджетного учреждения дополнительного образования «Центр внешкольной работы»
2. Контроль над исполнением настоящего приказа возложить на ответственного за обеспечение безопасности персональных данных в муниципальном бюджетном учреждении дополнительного образования «Центр внешкольной работы».
3. Приказ вступает в силу со дня подписания.

Директор МБУДО «ЦВР» Н.В. Бабичева

Приложение
к Приказу муниципального
бюджетного учреждения
дополнительного образования
«Центр внешкольной работы»
от «11» 02 2019 г. № 26-02

ИНСТРУКЦИЯ
по антивирусной защите в информационных системах муниципального бюджетного учреждения дополнительного образования «Центр внешкольной работы»

1. Настоящая инструкция предназначена для ответственного за обеспечение безопасности персональных данных в информационных системах муниципального бюджетного учреждения дополнительного образования «Центр внешкольной работы» (далее – Ответственный) и пользователей, обрабатывающих персональные данные на автоматизированных рабочих местах (далее АРМ) информационных систем муниципального бюджетного учреждения дополнительного образования «Центр внешкольной работы».

2. В целях обеспечения антивирусной защиты на АРМ производится антивирусный контроль.

3. Ответственность за поддержание установленного в настоящей инструкции порядка проведения антивирусного контроля возлагается на ответственного за обеспечение безопасности персональных данных в информационных системах муниципального бюджетного учреждения дополнительного образования «Центр внешкольной работы».

4. К применению на АРМ допускаются только лицензионные и сертифицированные ФСТЭК России антивирусные средства.

5. На АРМ запрещается установка программного обеспечения, не связанного с выполнением функций муниципального бюджетного учреждения дополнительного образования «Центр внешкольной работы».

6. Пользователи АРМ при работе с носителями информации обязаны перед началом работы осуществить проверку их на предмет отсутствия компьютерных вирусов.

7. Обновление антивирусных баз осуществляется ежедневно путем настройки в антивирусном средстве доступа к серверам обновлений разработчика антивирусного средства. В случае невозможности настроить доступ к серверам обновлений разработчика антивирусного средства, Ответственный один раз в неделю осуществляет установку пакетов

обновлений антивирусных баз, осуществляет контроль их подключения к антивирусному программному обеспечению и проверку жесткого диска и съемных носителей на наличие вирусов.

8. При обнаружении компьютерного вируса пользователи обязаны немедленно поставить в известность Ответственного и прекратить какие-либо действия на АРМ.

9. Ответственный проводит расследование факта заражения АРМ компьютерным вирусом. «Лечение» зараженных файлов осуществляется путем выбора соответствующего пункта меню антивирусной программы и после этого вновь проводится антивирусный контроль.

10. В случае обнаружения вируса, не поддающегося лечению, Ответственный обязан удалить инфицированный файл в соответствующую папку антивирусного пакета, и проверить работоспособность АРМ. В случае отказа АРМ – произвести восстановление соответствующего программного обеспечения.

11. Обо всех фактах заражения АРМ, Ответственный обязан ставить в известность ответственного за организацию обработки персональных данных и своего непосредственного руководителя.