Приложение 17
к приказу МБОУ СОШ №3
от 07.04.2017 №181

ИНСТРУКЦИЯ
по эксплуатации средств антивирусной защиты информационных средств, производящих обработку персональных данных (конфиденциальной информации) в Муниципальном бюджетном общеобразовательном учреждении «Средняя общеобразовательная школа №3»

1. **Общие положения**

Компьютерный вирус является вредоносным программным средством и характеризуется значительным деструктивным потенциалом для программ, данных и любой информации, хранящейся на машинных носителях информации. Особую опасность представляет то обстоятельство, что компьютерные вирусы могут скрытно и постепенно уничтожать, либо мгновенно разрушать информацию, при этом также могут пострадать аппаратные средства.

Основными путями «вирусного заражения» являются неквалифицированное обращение пользователей с автоматизированным рабочим местом при использовании ими «зараженных» машинных носителей информации и программ, либо целенаправленное спланированное воздействие извне с использованием компьютерных вирусов. При любых обстоятельствах это затрагивает вопросы защиты информации и интересы собственной безопасности Учреждения.

2. **Порядок, обеспечивающий безопасную работу на автоматизированном рабочем месте и с носителями информации:**

2.1. Вновь поступающее программное обеспечение должно быть подвергнуто входному контролю – проверке на отсутствие вирусов и проверке соответствия длины и контрольных сумм, если таковые указаны в сопроводительных документах, полученным длинам и контрольным суммам.

2.2. За эксплуатацию автоматизированной системы (далее - АС) отвечает ответственный за обработку персональных данных (защиту информации) и непосредственно сотрудник, работающий на нём.

2.3. На автоматизированных рабочих местах должно использоваться программное и аппаратное обеспечение, необходимое только для выполнения служебной деятельности.

2.4. На работающем автоматизированном рабочем месте, в обязательном порядке должно быть установлено антивирусное средство защиты. Ответственность за это несет конкретный, работающий на нём сотрудник, а также Ответственный за обработку персональных данных (защиту информации). Средства антивирусной защиты информации устанавливаются при вводе в эксплуатацию автоматизированного рабочего места или при их плановой замене.

2.5. Эксплуатируемые средства антивирусной защиты информации, устанавливаемые на автоматизированное рабочее место, входящее в состав государственной (муниципальной) информационной системы должны иметь сертификат соответствия ФСТЭК России.

2.6. Периодически, не реже 1 раза в неделю, Пользователем должна быть проведена антивирусная проверка на своём автоматизированном рабочем месте на возможное наличие компьютерного вируса.

2.7. Пользователь обязан проводить антивирусный проверку любой электронной информации (текстовые файлы любых форматов, файлы данных, исполняемые файлы, архивы и т.д.), получаемой и передаваемой по телекоммуникационным каналам, а также информации на съемных носителях информации.

2.8. Порядок и правила эксплуатации средств антивирусной защиты (САВЗ) информации определяется в руководстве пользователя на средство антивирусной защиты информации поставляемой вместе с САВЗ.

2.9. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить работу;
- сообщить об обнаружении вируса Ответственному за обработку персональных данных (защиту информации);

- в дальнейшем действовать по указанию Ответственного за обработку персональных данных (защиту информации).

3. **Ответственность**

Ответственность за поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля возлагается на Пользователя, обрабатывающего персональные данные.

Пользователь и Ответственный за обработку персональных данных (защиту информации) несут ответственность за качество и своевременность выполнения задач и функций, возложенных на них в соответствии с настоящей Инструкцией.