

Приложение № 6
к приказу от 31.08.2017 г. № 132 о.

Утверждаю
Директор ЛГ МАОУ «СОШ № 4»
Т.А. Панферова
2017 г.



ИНСТРУКЦИЯ

по эксплуатации средств антивирусной защиты
информационных средств,
производящих обработку конфиденциальной информации
(персональных данных)
в ЛГ МАОУ «СОШ № 4»

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 автоматизированного рабочего места

отвечает руководитель подразделения 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. Антивирусные средства устанавливаются при вводе в эксплуатацию автоматизированного рабочего места или при их плановой замене.

2.5. Периодически, не реже 1 раза в неделю, каждый сотрудник Учреждения обязан провести антивирусную проверку на своём автоматизированном рабочем месте на возможное наличие компьютерного вируса.

2.6. 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.

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

- приостановить работу;
- сообщить об обнаружении вируса Ответственному за обработку персональных данных;

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 несут ответственность за качество и своевременность выполнения задач и функций, возложенных на них в соответствии с настоящей Инструкцией.

**Ответственный за обработку
персональных данных**



И.Ш. Андреева