УТВЕРЖДАЮ
Директор МАОУ СОШ № 31
_____Е.В. Иванова
«_4_»_____09_____2023г.

Инструкция
по проведению антивирусного контроля
в муниципальном автономном общеобразовательном учреждении города Калининграда
средней общеобразовательной школе № 31
(МАОУ СОШ № 31)

1. Настоящая Инструкция предназначена для Администратора информационной безопасности (далее – Администратор) и пользователей, обрабатывающих информацию в информационной системы персональных данных муниципального автономного общеобразовательного учреждения города Калининграда средней общеобразовательной школы № 31 (далее - МАОУ СОШ № 31).

2. В целях обеспечения антивирусной защиты в МАОУ СОШ № 31 производится антивирусный контроль.

3. Ответственность за поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля возлагается на Администратора.

4. К применению на объекте допускаются лицензионные, сертифицированные антивирусные средства.

5. На объекте запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации на автоматизированных рабочих местах информационной системы персональных данных (далее – ИСПДн).

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

7. Ярлык для запуска антивирусной программы должен быть вынесен на «Рабочий стол» операционной системы, используемой в ИСПДн.

8. Администратор один раз в неделю осуществляет установку пакетов обновлений вирусных баз (если не предусмотрена автоматическая загрузка обновлений), осуществляет контроль их подключения к антивирусному пакету и проверку жесткого диска и съемных носителей на наличие вирусов.

9. При обнаружении компьютерного вируса пользователи обязаны немедленно поставить в известность Администратора и прекратить какие-либо действия на объекте.

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

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

12. Обо всех фактах заражения объекта, Администратор обязан ставить в известность ответственного за организацию обработки персональных данных.

13. Все факты заражения объекта, в обязательном порядке должны фиксироваться в Журнале по учету мероприятий по контролю обеспечения защиты персональных данных в ИСПДн.