

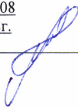
**Муниципальное автономное общеобразовательное учреждение –
средняя общеобразовательная школа № 168**

620102 г. Екатеринбург, ул. Серафимы Дерябиной 27а, телефон - факс (343) 233-40-81 e-mail: school168@bk.ru
ИНН/КПП 6658066139/665801001 ОКПО 41746036

ПРИНЯТО

Педагогическим советом
Протокол № 08
от 25.05.2018г.

Секретарь _____ О.В. Бажова



УТВЕРЖДЕНО

Директором MAOY - СОШ № 168

Т.О. Вяткиной

Приказом № 01-01-11/44

от 28.05.2018г.



**Регламент работы по обеспечению антивирусной безопасности
компьютеров**

Настоящий регламент работы по обеспечению антивирусной безопасности компьютеров в Муниципальном автономном общеобразовательном учреждении – средняя общеобразовательная школа № 168 (далее – Учреждение) разработан в соответствии с Письмом Министерства образования и науки Российской Федерации от 14.05.2018 № 08-1184 "О направлении информации" (вместе с "Методическими рекомендациями о размещении на информационных стендах, официальных интернет-сайтах и других информационных ресурсах общеобразовательных организаций и органов, осуществляющих управление в сфере образования, информации о безопасном поведении и использовании сети "Интернет").

1. С целью обеспечения антивирусной безопасности компьютеров Учреждения на них устанавливается антивирусное программное обеспечение, включается режим ежедневной автоматической проверки файловой системы при их включении, а также активируется функция автоматического обновления антивирусных баз.
2. Перед началом работы на компьютере проверяется не только наличие на нем антивирусного программного обеспечения, но и правильность настроек данного обеспечения.
3. Все внешние носители информации перед их использованием на компьютере проверяются на наличие вирусов и опасных программ.
4. К самостоятельной работе на компьютере допускаются лица, прошедшие инструктаж по антивирусной безопасности. Факт прохождения инструктажа фиксируется в журнале

учета инструктажей по антивирусной безопасности.

5. Пользователям компьютеров запрещается:

- использовать компьютер без установленного антивирусного программного обеспечения с регулярно обновляемой антивирусной базой;
- использовать любые внешние носители информации, не проверенные антивирусным программным обеспечением;
- при работе с электронной почтой открывать файлы, присоединенные к письмам, полученным от незнакомых лиц.

6. В случае корректной работы "программы-сторожа" скаченная из Интернета информация (документы, программы и т. п.) должна проверяться на вирусы автоматически. В противном случае проверка всех скаченных файлов осуществляется вручную.

7. При обнаружении антивирусной защитой вируса или вредоносной программы необходимо выполнить следующие действия:

- лечение зараженного файла;
- удаление зараженного файла, если лечение невозможно;
- блокирование зараженного файла, если его невозможно удалить.

8. При появлении признаков нестандартной работы компьютера (на экране появляются и исчезают окна, сообщения, изображения, самостоятельно запускаются программы и т. п.) необходимо выполнить следующие действия:

- отключение компьютера от интернет-сети;
- загрузка компьютера с внешнего загрузочного диска (CD, DVD);
- проведение полной антивирусной проверки компьютера.

При появлении аналогичных признаков после совершения данных действий рекомендуется переустановить операционную систему с форматированием системного раздела диска.

9. С целью сохранения важной информации, которая находится на компьютерах, проводится ее резервное копирование на внешние носители памяти не реже 1 раза в месяц.

10. Регламент вступает в силу с момента его утверждения.

11. Один экземпляр настоящего Регламента хранится в библиотеке Учреждения.

12. Регламент размещается на официальном сайте Учреждения в сети Интернет.

13. Срок действия настоящего Регламента неограничен, действует до принятия новой редакции.