

Приложение 6
к приказу «Об утверждении регламента по организации доступа в сеть Интернет, работы с электронной почтой, антивирусной защиты»

№326 от 31.08.2023г.



Инструкция по организации антивирусной защиты в ЧОУ «РЖД лицей №13»

1. Общие положения

1.1. Настоящая инструкция предназначена для организации порядка проведения антивирусного контроля в частном общеобразовательном учреждении «РЖД лицей №13» (далее- лицей) и предотвращения возникновения фактов заражения программного обеспечения компьютерными вирусами, а также фильтрации доступа пользователей лицея к непродуктивным Интернет-ресурсам и контроля их электронной переписки.

1.2. Директором лицея назначается лицо, ответственное за организацию антивирусной защиты в лицее.

1.3. В лицее может использоваться только лицензионное антивирусное программное обеспечение либо свободно-распространяемое программное обеспечение.

1.4. Установка, настройка и регулярное обновление антивирусных средств осуществляется только ответственным за организацию антивирусной защиты в лицее.

1.5. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы, почтовые сообщения), получаемая и передаваемая по телекоммуникационным каналам связи, а также информация на съемных носителях (магнитных лентах, дисках, CD-ROM, DVD, flash-накопителях и т.п.)

2. Регламент работы по обеспечению антивирусной безопасности компьютеров Частного общеобразовательного учреждения «РЖД лицей №13»

2.1. С целью обеспечения антивирусной безопасности компьютеров образовательной организации на них устанавливается антивирусное программное обеспечение, включается режим ежедневной автоматической проверки файловой системы при их включении, а также активируется функция автоматического обновления антивирусных баз.

2.2. Перед началом работы на компьютере проверяется не только наличие на нем антивирусного программного обеспечения, но и правильность настроек данного обеспечения.

2.3. Все внешние носители информации перед их использованием на компьютере проверяются на наличие вирусов и опасных программ.

2.4. К самостоятельной работе на компьютере допускаются лица, прошедшие инструктаж по антивирусной безопасности. Факт прохождения инструктажа фиксируется в журнале учета инструктажей по антивирусной безопасности.

2.5. 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.

2.6. Скаченная из Интернета информация (документы, программы и т. п.) должна проверяться на вирусы автоматически. В противном случае проверка всех скаченных файлов осуществляется вручную.

2.7. 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.

2.8. 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.

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