**Инструкция по предотвращению вирусных атак**

**на компьютерах в МОУ ДО Центр детского творчества**

1. При открытии письма проверьте - точно ли Вы ждёте письмо такого

содержания и от такого адресата?

2. В адресной строке отправителя должен быть адрес вида

(ivanova @ zavod . ru , ivanova @ yandex . ru , ivanova @ mail . ru ...).

Названия почтового ящика и почтовой службы должны иметь понятное

прочтение (имя ящика допускается: ivanov @ yandex . ru ,

zavodigrushek 777@ mail . ru , не допускается : fsdfsdf 3434@ mail . ru ,

sadasdasd @ sdfsdf . cn)

3. Вложения в письме которые можно скачивать должны иметь

формат: \*.rar,\*.zip, \*.doc, \*.xls, \*.pdf, \*. Jpeg . названия файлов

должны заканчиваться именно такими расширениями.

Не допускается: фото.jpeg.exe, архив.rar.exe!!! не открывать вложения

формата \*.exe, \*.bat!!!!!!

4. Все без исключения вложения сначала скачать, потом проверить

антивирусом Касперский, и только в случае отсутствия угрозы

безопасности допускается открытие вложения!

5. Если есть хоть малейшее сомнение по поводу наличия письма на

наличие угрозы безопасности ПК, переслать это письмо на адрес

a . alpatov @ corp . yarcdu . ru для получения точного подтверждения

безопасности этого письма.

6. Если всё же Вы допустили открытие письма с вирусным вложением,

то ни в коем случае не предпринимать никаких самостоятельных

действий по уничтожению угрозы!!!! Не выключать компьютер!

Оставить в рабочем состоянии и сообщить об этом системному

администратору.