

РОССИЙСКАЯ ФЕДЕРАЦИЯ  
МУНИЦИПАЛЬНОЕ ОБРАЗОВАНИЕ ПРИОЗЕРСКИЙ МУНИЦИПАЛЬНЫЙ РАЙОН  
ЛЕНИНГРАДСКОЙ ОБЛАСТИ  
МУНИЦИПАЛЬНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
«СОСНОВСКИЙ ЦЕНТР ОБРАЗОВАНИЯ»  
ПРИКАЗ

От 21.07.2021 г.

пос. Сосново

№ 340

Об утверждении инструкции пользователя  
по компьютерной безопасности

В соответствии с Федеральным законом от 29.12.2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» в редакции Федерального закона от 28.07.2012 г. № 139-ФЗ «О внесении изменений в федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные Законодательные акты Российской Федерации», Федеральным законом от 24.07.1998 г. № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации», Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Правилами подключения общеобразовательных учреждений к единой системе контент-фильтрации доступа к сети Интернет Министерства образования и науки Российской Федерации от 11.05.2011г., Приказом Минобрнауки РФ от 02 сентября 2013 г. № 2553 «О мерах по исключению доступа к интернет-ресурсам, не совместимым с задачами образования и воспитания обучающихся», протокола педагогического совета от 06.07.2021 г. № 16,

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемую инструкцию пользователя по компьютерной безопасности в муниципальном общеобразовательном учреждении «Сосновский центр образования».
2. Контроль за исполнением настоящего приказа оставляю за собой.

Директор:



И.М. Кириллова

**ИНСТРУКЦИЯ**  
**пользователя по компьютерной безопасности**  
**в муниципальном общеобразовательном учреждении**  
**«Сосновский центр образования»**

1. Установить последние обновления операционной системы Windows.
2. Включить режим автоматической загрузки обновлений. (Пуск->Настройка->панель управления->Автоматическое обновление->Автоматически загружать и устанавливать на компьютер рекомендуемые обновления).
3. Активировать встроенный брандмауэр Windows (Пуск->Настройка->панель управления->Брандмауэр Windows->Включить).
4. Установить антивирусное программное обеспечение на каждый компьютер. Включить режим автоматического сканирования файловой системы. Включить режим ежедневной автоматической проверки всей файловой системы при включении компьютера. Активировать функцию ежедневного автоматического обновления антивирусных баз.
5. Ежедневно проверять состояние антивирусного программного обеспечения, а именно
  - a. Режим автоматической защиты должен быть включен постоянно
  - b. Дата обновления антивирусных баз не должна отличаться более чем на несколько дней от текущей даты.
  - c. Просматривать журналы ежедневных антивирусных проверок. Контролировать удаление вирусов при их появлении.
6. Не реже одного раза в месяц посещать сайт <http://windowsupdate.microsoft.com> и проверять установлены ли последние обновления операционной системы.
7. Быть крайне осторожным при работе с электронной почтой. Категорически запрещается открывать присоединенные к письмам, полученным от незнакомых лиц, файлы.
8. Контролировать посещение Интернет сайтов пользователями. Не допускать посещения т.н. «хакерских», порно и других сайтов с потенциально вредоносным содержанием.
9. В обязательном порядке проверять антивирусным программным обеспечением любые внешние носители информации перед началом работы с ними.
10. При появлении признаков нестандартной работы компьютера («тормозит», на экране появляются и исчезают окна, сообщения, изображения, самостоятельно запускаются программы и т.п.) немедленно отключить компьютер от Ethernet сети, загрузить компьютер с внешнего загрузочного диска (CD, DVD) и произвести полную антивирусную проверку всех дисков компьютера. При появлении аналогичных признаков после проделанной процедуры переустановить операционную систему с форматированием системного раздела диска.