СОГЛАСОВАНО
Протокол заседания
Педагогического совета МОУ
«Лицей № 23»
от 22.05.2018г. № 6

Утверждено
приказом директора
МОУ «Лицей № 23»
от 25.06.2018г. № 65-ОД

ПОЛОЖЕНИЕ
о регламенте работы по запуску и обновлению антивирусного программного обеспечения

Признаки заражения компьютера вирусными программами

Признаки, свидетельствующие о заражении компьютера:

- на экран выводятся непредусмотренные сообщения, изображения либо воспроизводятся непредусмотренные звуковые сигналы;
- неожиданно открывается и закрывается лоток CD/DVD-ROM-устройства;
- произвольно, без участия пользователя, на компьютере запускаются какие-либо программы;
- на экран выводятся предупреждения о попытке какой-либо из программ выйти в интернет, хотя пользователь никак не инициировали такое ее поведение
- в почтовом ящике пользователя находится большое количество сообщений без обратного адреса и заголовка;
- пользователю становится известно, что с его почтового ящика были произведены несанкционированные рассылки сообщений;

Косвенные признаки заражения компьютера (90% случаев наличие косвенных симптомов вызвано сбоем в аппаратном или программном обеспечении):

- частые зависания и сбои в работе компьютера;
- медленная работа компьютера при запуске программ;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- частое обращение к жесткому диску (часто мигает лампочка на системном блоке);
- веб-браузер (например, Microsoft Internet Explorer) "зависает" или ведет себя неожиданным образом (например, окно программы невозможно закрыть).

Действия при наличии признаков заражения

При обнаружении признаков заражения компьютера" необходимо:

1. Отключить компьютер от интернета и локальной сети, если он к ней был подключен.
2. Если симптом заражения состоит в том, что невозможно загрузить операционную систему с жесткого диска компьютера (компьютер выдает ошибку при включении), необходимо предпринять попутку загрузить компьютер в режиме защиты от сбоев или с диска аварийной загрузки Microsoft Windows.
3. Прежде чем предпринимать какие-либо действия, необходимо сохранить результаты работы на внешний носитель (дискету, CD-диск, флеш-карту и пр.).
4. Установить антивирусную программу, если это не было сделано ранее.
5. Обновите сигнатуру угроз программы. Если это возможно, для их получения необходимо выйти в интернет с незараженного компьютера, поскольку при подключении к интернету с зараженного компьютера есть вероятность отправки вирусом важной

информации злоумышленникам или распространения вируса по адресам адресной книги пользователя.
6. Запустить полную проверку компьютера.

Профилактика заражения

Компьютерная профилактика состоит из небольшого количества правил, соблюдение которых значительно снижает вероятность заражения вирусом и потери каких-либо данных.
Ниже перечислены основные правила безопасности, выполнение которых позволит избегать вирусных атак.
Правило № 1: *необходимо защитить компьютер с помощью антивирусных программ и программ безопасной работы в интернете и регулярно обновляйте сигнатуры угроз, входящие в состав программы.*

Правило № 2: необходимо соблюдать *осторожность при записи новых данных на компьютер:*

- следует проверять на присутствие вирусов все съемные диски (дискеты, CD-диски, флешкарты и пр.) перед их использованием.
- не следует запускать никаких файлов, пришедших по почте, если нет уверенности, что они действительно должны были прийти к пользователю, даже если они отправлены вашими знакомыми адресатами.
- следует внимательно относитесь к информации, получаемой из интернета. Если с какого-либо веб-сайта предлагается установить новую программу, следует обратить внимание на наличие у нее сертификата безопасности.
- при копировании файлов из интернета или локальной сети, обязательно необходимо проверить его с помощью антивирусной программы.
- следует внимательно относитесь к выбору посещаемых пользователями интернет-ресурсов. Некоторые из сайтов заражены опасными скрипт-вирусами или интернет-червями.

  Правило № 3: *необходимо пользоваться сервисом Windows Update и регулярно устанавливайте обновления операционной системы Microsoft Windows.*

  Правило №4*: следует покупать дистрибутивные копии программного обеспечения у официальных продавцов.*

  Правило №5: *следует ограничь круг людей, допущенных к работе на учебном компьютере.*

  Правило №6: *способы уменьшения риска неприятных последствий возможного заражения:*
- Своевременно делать резервное копирование данных.
- Создать диск аварийного восстановления, с которого при необходимости можно будет загрузиться, используя "чистую" операционную систему.

  Правило №7: *регулярно просматривать список установленных программ на учебном компьютере.*

  Основные антивирусные программы:
  1. Kaspersky Antivirus