

Никогда не устанавливайте и не сохраняйте без предварительной проверки антивирусной программой файлы, полученные из ненадежных источников: скачанные с неизвестных web-сайтов, присланные по электронной почте, полученные в телеконференциях. Проверяйте все новые файлы, сохраняемые на компьютере. Периодически проверяйте компьютер полностью.

По возможности не сохраняйте в системе пароли (для установки соединений с Интернетом, для электронной почты и др.) и периодически меняйте их.

При получении извещений о доставке почтовых сообщений обращайте внимание на причину и, в случае автоматического оповещения о возможной отправке вируса, немедленно проверяйте компьютер антивирусной программой.

Резервное копирование – гарантия безопасности

Регулярно выполняйте резервное копирование важной информации. Подготовьте и имейте в доступном месте системный загрузочный диск.

В случае подозрения на заражение компьютера вредоносной программой загрузите систему с диска и проверьте антивирусной программой.

МЫ ЖДЕМ ВАС ПО АДРЕСУ:

ул. Щербакова,13
с 10-00 ч. до 18-00ч.
выходной – **воскресенье** тел. 3-17-40

Наш сайт : <http://ncibs.ucoz.ru/>

Информационный отдел ЦБ

Централизованная информационно-библиотечная система Нязепетровск



ВРЕДОНОСНЫЕ ПРОГРАММЫ В ИНТЕРНЕТЕ

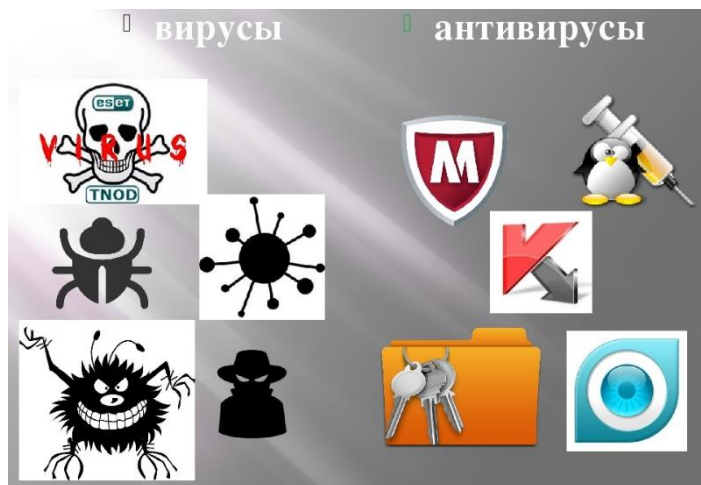
Интернет называют «миром новых возможностей». Но тем, кто только пришёл в этот мир, следует вести себя осторожно и строго следовать правилам поведения в Сети. Как и в реальном мире, в Интернете действует множество мошенников и просто хулиганов, которые создают и запускают вредоносные программы.

Вредоносные программы представляют собой файлы, которые срабатывают при активировании на компьютере. Тактика борьбы с ними достаточно проста:

а) не допускать, чтобы вредоносные программы попадали на Ваш компьютер;

б) если они к Вам все-таки попали, ни в коем случае не запускать их;

в) если они все же запустились, то принять меры, чтобы, по возможности, они не причинили ущерба.



Вредоносные программы способны самостоятельно, то есть без ведома владельца компьютера, создавать свои копии и распространять их различными способами. Подобные программы могут выполнять самые разнообразные действия: от вполне безобидных «шуток» (типа «гуляющих» по монитору картинок) до полного разрушения информации, хранящейся на дисках компьютера.

РАСШИРЕНИЕ ФАЙЛА – ЭТО ВАЖНО!

Особую опасность могут представлять файлы со следующими расширениями:

***ade, *adp, *bas, *bat; *chm, *cmd, *com, *cpl; *crt, *eml, *exe, *hlp; *hta, *inf, *ins, *isp; *jse, *lnk, *mdb, *mde; *msc, *msi, *msp, *mst; *pcd, *pif, *reg, *scr; *sct, *shs, *url, *vbs; *vbe, *wsf, *wsh, *wsc.**

1. Антивирусные программы - ваши первые защитники

Установите современное лицензионное антивирусное программное обеспечение. Регулярно обновляйте антивирусные программы либо разрешайте автоматическое обновление при запросе программы.

2. Обновления – это полезно и безопасно

Устанавливайте новые версии операционных систем и своевременно устанавливайте обновления к ним, устраняющие обнаруженные ошибки.



Регулярно обновляйте пользовательское программное обеспечение для работы в сети, такое как интернет-браузер, почтовые программы, устанавливая самые последние обновления. Помните, что обновления операционных систем разрабатываются с учётом новых вирусов. Настройте операционную систему на своём компьютере так, чтобы обеспечивались основные правила безопасности при работе в сети.

Не забудьте подкорректировать настройки почты, браузера и клиентов других используемых сервисов, чтобы уменьшить риск воздействия вредоносных программ и подверженность сетевым атакам.

Проверяйте новые файлы. Будьте очень осторожны при получении сообщений с файлами-вложениями. Обращайте внимание на расширение файла.

Вредоносные файлы часто маскируются под обычные графические, аудио и видеофайлы. *Для того, чтобы видеть настоящее расширение файла, обязательно включите в системе режим отображения расширений файлов.* Подозрительные сообщения лучше немедленно удалять.

Чтобы удалить сообщение в почтовой программе полностью нужно: удалить сообщение из папки «Входящие»; удалить сообщение из папки «Удаленные»; выполнить над папками операцию «Сжать» (Файл/Папка/Сжать все папки).