Содержание:

Антивирусные средства защиты

Количество людей, пользующихся компьютером и сотовым телефоном, имеющим выход в Интернет, постоянно растет. Значит, возрастает возможность обмена данными между ними по электронной почте и через Всемирную сеть. Это приводит к росту угрозы заражения компьютера вирусами, а также порчи или хищения информации чужими вредоносными программами, ведь основными источниками распространения вредоносных программ являются электронная почта и Интернет. Правда, заражение может также произойти через флэшку или CD-диск.

Компьютерный вирус — это целенаправленно созданная программа, автоматически приписывающая себя к другим программным продуктам, изменяющая или уничтожающая их. Компьютерные вирусы могут заразить компьютерные программы, привести к потере данных и даже вывести компьютер из строя.

Компьютерные вирусы могут распространяться и проникать в операционную и файловую систему ПК только через внешние магнитные носители (жесткий и гибкий диски, компакт-диски) и через средства межкомпьютерной коммуникации.

Вредоносные программы можно разделить на три класса: черви, вирусы и троянские программы.

Черви — это класс вредоносных программ, использующих для распространения сетевые ресурсы. Используют сети, электронную почту и другие информационные каналы для заражения компьютеров.

Вирусы — это программы, которые заражают другие программы — добавляют в них свой код, чтобы получить управление при запуске зараженных файлов.

Троянские программы — программы, которые выполняют на поражаемых компьютерах несанкционированные пользователем действия, т.е. в зависимости от каких-либо условий уничтожают информацию на дисках, приводят систему к

зависанию, воруют конфиденциальную информацию и т.д.

В зависимости от среды обитания вирусы можно разделить на сетевые, файловые, загрузочные и файлово-загрузочные.

Сетевые вирусы распространяются по различным компьютерным сетям.

Файловые вирусы внедряются главным образом в исполняемые модули, т.е. в файлы, имеющие расширения COM и EXE.

Загрузочные вирусы внедряются в загрузочный сектор диска или сектор, содержащий программу загрузки системного диска.

Файлово-загрузочные вирусы заражают файлы и загрузочные сектора дисков.

По способу заражения вирусы разделяются на резидентные и нерезидентные.

Резидентный вирус при заражении компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т.д.) и внедряется в них.

Нерезидентные вирусы не заражают память компьютера и являются активными ограниченное время.

По степени воздействия выделяют неопасные вирусы, которые не мешают работе компьютера, опасные, которые могут привести к различным нарушениям в работе компьютера, и очень опасные, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

Для обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов специальных программ, которые позволяют обнаруживать и уничтожать вирусы. Такие программы называются антивирусными.

Различают следующие виды антивирусных программ

Программы-детекторы осуществляют поиск характерной для конкретного вируса сигнатуры в оперативной памяти и файлах и при обнаружении выдают

соответствующие сообщение. Недостатком таких антивирусных программ является то, что они могут находить только те вирусы, которые известны разработчикам таких программ.

Программы-доктора или флаги не только находят зараженные вирусами файлы, но и возвращают файлы в исходное состояние. В начале своей работы флаги ищут вирусы в оперативной памяти, уничтожая их, и только затем переходят к «лечению» файлов.

Программы-ревизоры запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным. Обнаружение изменения выводится на экран монитора.

Программы-фильтры или сторожа, представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов:

попытка коррекции файлов с расширениями COM и EXE;

изменение атрибутов файла;

прямая запись на диск по абсолютному адресу;

запись в загрузочные сектора диска;

загрузка резидентной программы.

При попытке вирусной атаки сторож посылает сообщение и предлагает запретить или разрешить соответствующие действия.

Программы - вакцины или иммунизаторы — это резидентныепрограммы, предотвращающие заражение файлов.

Признаки заражения компьютера вирусом. Существует ряд признаков, свидетельствующих о заражении компьютера:

вывод на экран непредусмотренных сообщений или изображений;

подача непредусмотренных звуковых сигналов;

неожиданное открытие и закрытие лотка CD-ROM-устройства;

произвольный, без вашего участия, запуск на компьютере каких-либо программ; вывод на экран предупреждения о попытке какой-либо из программ вашего компьютера выйти в Интернет, хотя вы никак не инициировали такое ее поведение (при наличии установленной на вашем компьютере соответствующей антивирусной программы).

Однако не всегда такие признаки вызываются присутствием вирусов. Иногда они могут быть следствием других причин. Например, в случае с почтой зараженные сообщения могут рассылаться с вашим обратным адресом, но не с вашего компьютера.

Существуют и косвенные признаки заражения вашего компьютера:

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, когда часто мигает лампочка на системном блоке;

Microsoft Internet Explorer зависает или ведет себя неожиданным образом, например окно программы невозможно закрыть.

В 90 % случаев наличие косвенных симптомов вызвано сбоем в аппаратном или программном обеспечении. Несмотря на это при их появлении рекомендуем провести полную проверку компьютера на наличие вирусов.

Если вы заметили, что ваш компьютер ведет себя подозрительно, придерживайтесь следующих правил

Не паникуйте!

Отключите компьютер от Интернета.

Отключите компьютер от локальной сети, если он к ней был подключен.

Если симптом заражения заключается в том, что вы не можете загрузиться с жесткого диска компьютера, т. е. компьютер выдает ошибку, когда вы его включаете, попробуйте загрузиться в режиме защиты от сбоев или с диска аварийной загрузки Windows.

Прежде чем предпринимать какие-либо действия, сохраните результаты вашей работы, записав их на внешний носитель (CD, диск, флэш-карту, SSD).

Установите антивирусную программу, если вы этого еще не сделали.

Получите последние обновления антивирусных баз.

Установите необходимые настройки антивирусной программы и запустите полную проверку.