Министерство образования и науки Республик Бурятия
Государственное бюджетное профессиональное образовательное учреждение
«Бурятский республиканский информационно-экономический техникум»

Антивирусные программы

Выполнил: студентка 116 группы,
Шалданова Н. Б.
Проверил: преподаватель информатики,
Цыренова А. Н.

Содержание

- Введение
- Признаки появления вирусов
- Характеристика антивирусных программ
- Программы-детекторы
- Программы-доктора
- Программы-ревизоры. Вакцины
- Программы-фильтры
- Недостатки антивирусных программ
- Итак, что же такое антивирус?

Введение

- В настоящее время компьютер прочно вошел в повседневную жизнь. Его возможности используются на работе, при проведении досуга, в быту и других сферах жизни человека. Количество информации, которую люди доверяют своему «электронному другу», с каждым днем растет, поэтому рано или поздно каждый задается вопросом: «Как обеспечить надежную сохранность данных?»
- Сегодня невозможно встретить пользователя персонального компьютера, который не слышал бы о компьютерных вирусах. В Интернете такие вредоносные программы существуют в огромном количестве. Самое неприятное, что многие распространители вирусов успешно применяют в своей практике передовые достижения IT-индустрии. В результате то, что должно служить на благо пользователей, в конечном итоге может обернуться для них большими проблемами.
- Вирус - это вредоносная программа, проникающая на компьютер без ведома пользователя и выполняющая определенные действия деструктивной направленности. Вирусы – едва ли не главные враги компьютера. Чтобы не стать жертвой этой напасти, каждому пользователю следует хорошо знать принципы защиты от компьютерных вирусов.
- С давних времён известно, что к любому яду рано или поздно можно найти противоядие. Таким противоядием в компьютерном мире стали программы, называемые антивирусными. Поэтому на любом современном компьютере должна быть обязательно установлена антивирусная программа.

Признаки появления вирусов

Для маскировки вируса его действия по заражению других программ и нанесению вреда могут выполняться не всегда, а при выполнении каких-либо условий. После того как вирус выполнит нужные ему действия, он передает управление той программе, в которой он находится, и ее работа некоторое время не отличается от работы незараженной. Все действия вируса могут выполняться достаточно быстро и без выдачи каких-либо сообщений, поэтому пользователь часто и не замечает, что компьютер работает со "странностями". К признакам появления вируса можно отнести:

- замедление работы компьютера;
- невозможность загрузки операционной системы;
- частые «зависания» и сбои в работе компьютера;
- прекращение работы или неправильная работа ранее успешно функционировавших программ;
- увеличение количества файлов на диске;
- изменение размеров файлов;
- периодическое появление на экране монитора неуместных системных сообщений;
- уменьшение объема свободной оперативной памяти;
- заметное возрастание времени доступа к жесткому диску;
- изменение даты и времени создания файлов;
- разрушение файловой структуры (исчезновение файлов, искажение каталогов и др.);
- загорание сигнальной лампочки дисковода, когда к нему нет обращения.

Надо заметить, что названные симптомы необязательно вызываются компьютерными вирусами, они могут быть следствием других причин, поэтому компьютер следует периодически диагностировать.

Характеристика антивирусных программ

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

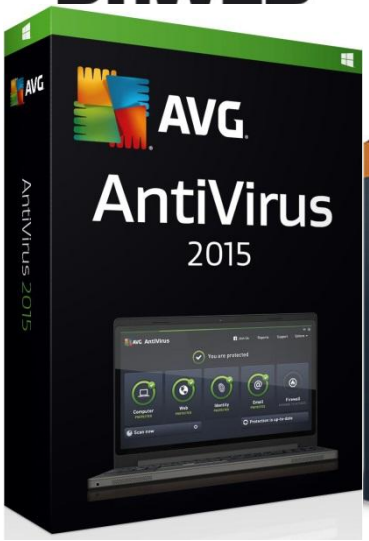
- Различают следующие виды антивирусных программ:
- программы- детекторы;
- программы-доктора или фаги;
- программы-ревизоры;
- программы-фильтры;
- программы-вакцины ли иммунизаторы.

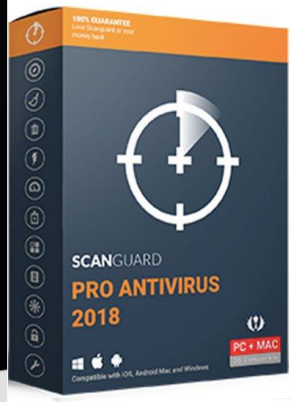
Программы-детекторы

Осуществляют поиск характерной для конкретного вируса последовательности байтов (сигнатуры вируса) в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение. Недостатком таких антивирусных программ является то, что они могут находить только те вирусы, которые известны разработчикам таких программ.

Программы-доктора

- Фаги, а также программы-вакцины не только находят зараженные вирусами файлы, но и "лечат" их, т.е. удаляют из файла тело программы вируса, возвращая файлы в исходное состояние. В начале своей работы фаги ищут вирусы в оперативной памяти, уничтожая их, и только затем переходят к "лечению" файлов. Среди фагов выделяют **полифаги**, т.е. программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов. Наиболее известными полифагами являются программы Aidstest,*Scan, Norton AntiVirus*,AVT и Doctor Web.





Программы-ревизоры. Вакцины

- **Программы-ревизоры** относятся к самым надежным средствам защиты от вирусов. 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. К числу программ-ревизоров относится широко распространенная в России программа Adinf фирмы "Диалог-Наука".
- **Вакцины** или *иммунизаторы* - это резидентные программы, предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы-доктора, "лечащие" этот вирус. Вакцинация возможна только от известных вирусов. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедрится. В настоящее время программы-вакцины имеют ограниченное применение.
- Своевременное обнаружение зараженных вирусами файлов и дисков, полное уничтожение обнаруженных вирусов на каждом компьютере позволяют избежать распространения вирусной эпидемии на другие компьютеры.

Программы-фильтры

- *«Сторожа"* представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов. Такими действиями могут являться:
- попытки коррекции файлов с расширениями COM и EXE; изменение атрибутов файлов;
- прямая запись на диск по абсолютному адресу;
- запись в загрузочные сектора диска;
- загрузка резидентной программы. При попытке какой-либо программы произвести указанные действия "сторож" посылает пользователю сообщение и предлагает запретить или разрешить соответствующее действие. Программы-фильтры весьма полезны, так как способны обнаружить вирус на самой ранней стадии его существования до размножения. Однако они не "лечат" файлы и диски. Для уничтожения вирусов требуется применить другие программы, например фаги. К недостаткам программ-сторожей можно отнести их "назойливость", а также возможные конфликты с другим программным обеспечением.

Недостатки антивирусных программ

- Ни одна из существующих антивирусных технологий не может обеспечить полной защиты от вирусов
- Антивирусная программа забирает часть вычислительных ресурсов системы, нагружая центральный процессор и жёсткий диск. Особенно это может быть заметно на слабых компьютерах. Замедление в фоновом режиме работы может достигать 380 %.
- Антивирусные программы могут видеть угрозу там, где её нет (ложные срабатывания).
- Антивирусные программы загружают обновления из Интернета, тем самым расходуя трафик.
- Различные методы шифрования и упаковки вредоносных программ делают даже известные вирусы не обнаруживаемыми антивирусным программным обеспечением. Для обнаружения этих «замаскированных» вирусов требуется мощный механизм распаковки, который может дешифровать файлы перед их проверкой. Однако во многих антивирусных программах эта возможность отсутствует и, в связи с этим, часто невозможно обнаружить зашифрованные вирусы.

Итак, что же такое антивирус?

- Почему-то многие считают, что антивирус может обнаружить любой вирус, то есть, запустив антивирусную программу, можно быть абсолютно уверенным в их надежности. Такая точка зрения не совсем верна.
- Дело в том, что антивирус - это тоже программа, конечно, написанная профессионалом. Но эти программы способны распознавать и уничтожать только известные вирусы. То есть антивирус против конкретного вируса может быть написан только в том случае, когда у программиста есть в наличии хотя бы один экземпляр этого вируса. Вот и идет эта бесконечная война между авторами вирусов и антивирусов, правда, первых в нашей стране почему-то всегда больше, чем вторых.
- Но и у создателей антивирусов есть преимущество! Дело в том, что существует большое количество вирусов, алгоритм которых практически скопирован с алгоритма других вирусов. Как правило, такие вариации создают непрофессиональные программисты, которые по каким-то причинам решили написать вирус. Для борьбы с такими "копиями" придумано новое оружие - эвристические анализаторы. С их помощью антивирус способен находить подобные аналоги известных вирусов, сообщая пользователю, что у него, похоже, завелся вирус
- Таким образом, в этой информационной войне, как, впрочем, и в любой другой, остаются сильнейшие. Вирусы, которые не распознаются антивирусными детекторами, способны написать только наиболее опытные и квалифицированные программисты.