Классификация и виды антивирусных программ. Сравнительная характеристика антивирусных программ

Для обнаружения, удаления и защиты от компьютерных вирусов разработаны специальные программы, которые позволяют обнаруживать и уничтожать вирусы.

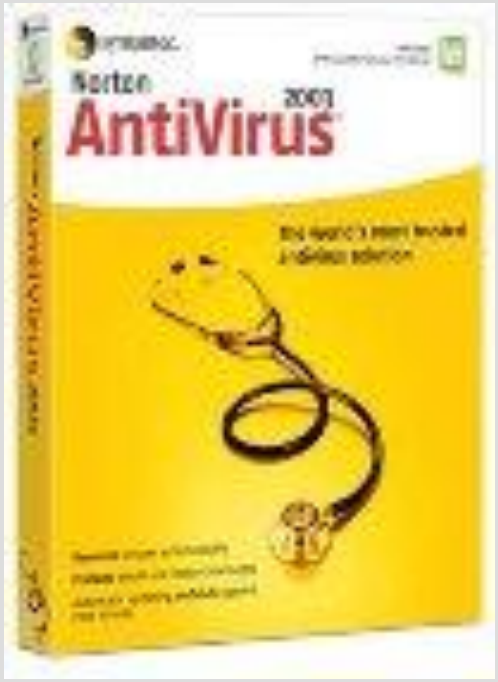
Такие программы называются антивирусными. Современные антивирусные программы представляют собой многофункциональные продукты, сочетающие в себе как превентивные, профилактические средства, так и средства лечения вирусов и восстановления данных.

Требования к антивирусным программам.

Количество и разнообразие вирусов велико, и чтобы их быстро и эффективно обнаружить, антивирусная программа должна отвечать некоторым параметрам.

Стабильность и надежность работы. Этот параметр, без сомнения, является определяющим — даже самый лучший антивирус окажется совершенно бесполезным, если он не сможет нормально функционировать на вашем компьютере, если в результате какого-либо сбоя в работе программы процесс проверки компьютера не пройдет до конца.
Тогда всегда есть вероятность того, что какие-то зараженные файлы остались незамеченными.

Размеры вирусной базы программы (количество вирусов, которые правильно определяются программой). С учетом постоянного появления новых вирусов база данных должна регулярно обновляться — что толку от программы, не видящей половину новых вирусов и, как следствие, создающей ошибочное ощущение “чистоты” компьютера. Сюда же следует отнести и возможность программы определять разнообразные типы вирусов, и умение работать с файлами различных типов (архивы, документы).

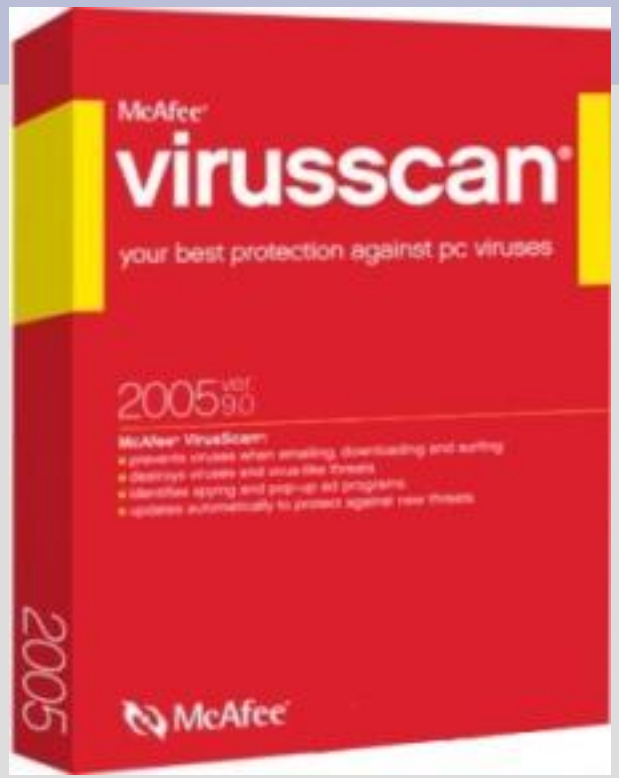


Характеристика антивирусных программ.

Антивирусные программы делятся на: программы-детекторы, программы-доктора, программы-ревизоры, программы-фильтры, программы-вакцины.

Программы-детекторы обеспечивают поиск и обнаружение вирусов в оперативной памяти и на внешних носителях, и при обнаружении выдают соответствующее сообщение. Различают детекторы универсальные и специализированные.

Универсальные детекторы в своей работе используют проверку неизменности файлов путем подсчета и сравнения с эталоном контрольной суммы. Недостаток универсальных детекторов связан с невозможностью определения причин искажения файлов. Специализированные детекторы выполняют поиск известных вирусов по их сигнатуре (повторяющемуся участку кода). Недостаток таких детекторов состоит в том, что они неспособны обнаруживать все известные вирусы. Детектор, позволяющий обнаруживать несколько вирусов, называют полидетектором.

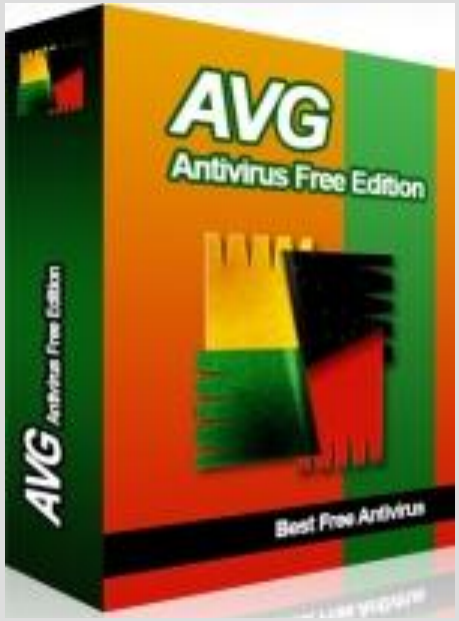


Программы-доктора (фаги), не только находят зараженные вирусами файлы, но и "лечат" их, т.е. удаляют из файла тело программы вируса, возвращая файлы в исходное состояние. В начале своей работы фаги ищут вирусы в оперативной памяти, уничтожая их, и только затем переходят к "лечению" файлов.
Среди фагов выделяют полифаги, т.е. программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов.

Учитывая, что постоянно появляются новые вирусы, программы-детекторы и программы-доктора быстро устаревают, и требуется регулярное обновление их версий.

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. Обнаруженные изменения выводятся на экран видеомонитора.

Программы-ревизоры имеют достаточно развитые алгоритмы, обнаруживают стелс-вирусы и могут даже отличить изменения версии проверяемой программы от изменений, внесенных вирусом.



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.

Для уничтожения вирусов требуется применить другие программы, например фаги. К недостаткам программ- сторожей можно отнести их "назойливость" (например, они постоянно выдают предупреждение о любой попытке копирования исполняемого файла), а также возможные конфликты с другим программным обеспечением.

Вакцины (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.

Краткий обзор антивирусных программ.

При выборе антивирусной программы необходимо учитывать не только процент обнаружения вирусов, но и способность обнаруживать новые вирусы, количество вирусов в антивирусной базе, частоту ее обновления, наличие дополнительных функций.

В настоящее время серьезный антивирус должен уметь распознавать не менее 25000 вирусов. Это не значит, что все они находятся "на воле". На самом деле большинство из них или уже прекратили свое существование или находятся в лабораториях и не распространяются. Реально можно встретить 200- 300 вирусов, а опасность представляют только несколько десятков из них.

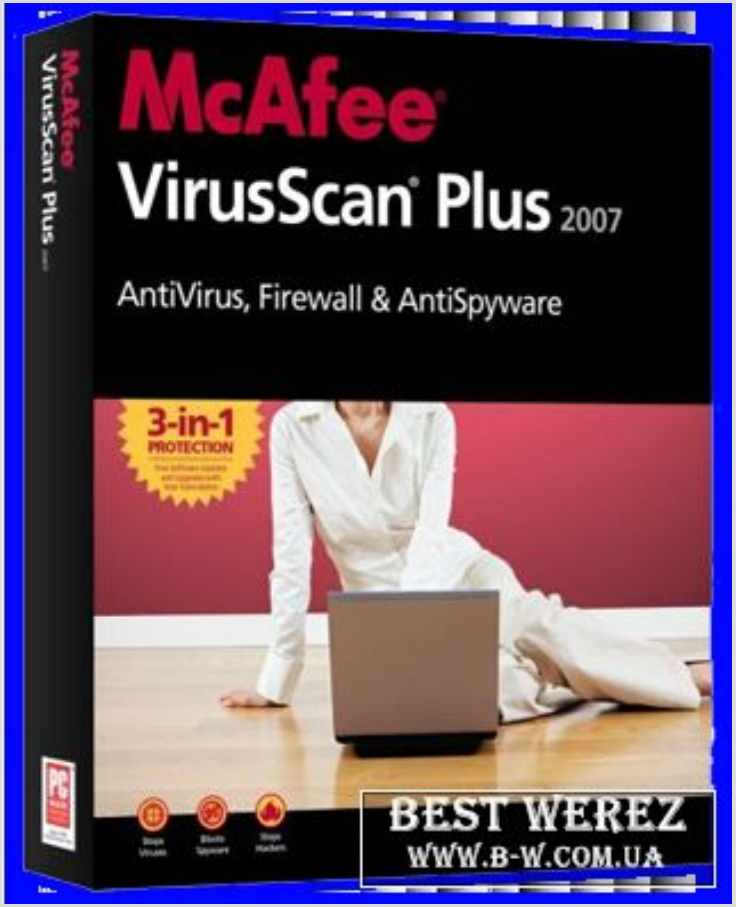
Существует множество антивирусных программ. Рассмотрим наиболее известные из них.

Dr Solomon's AntiVirus (производитель: «Dr Solomon's Software»).

Считается одним из самых лучших антивирусов (Евгений Касперский как- то сказал, что это единственный конкурент его AVP). Обнаруживает практически 100% известных и новых вирусов. Большое количество функций, сканер, монитор, эвристика и все что необходимо чтобы успешно противостоять вирусам.

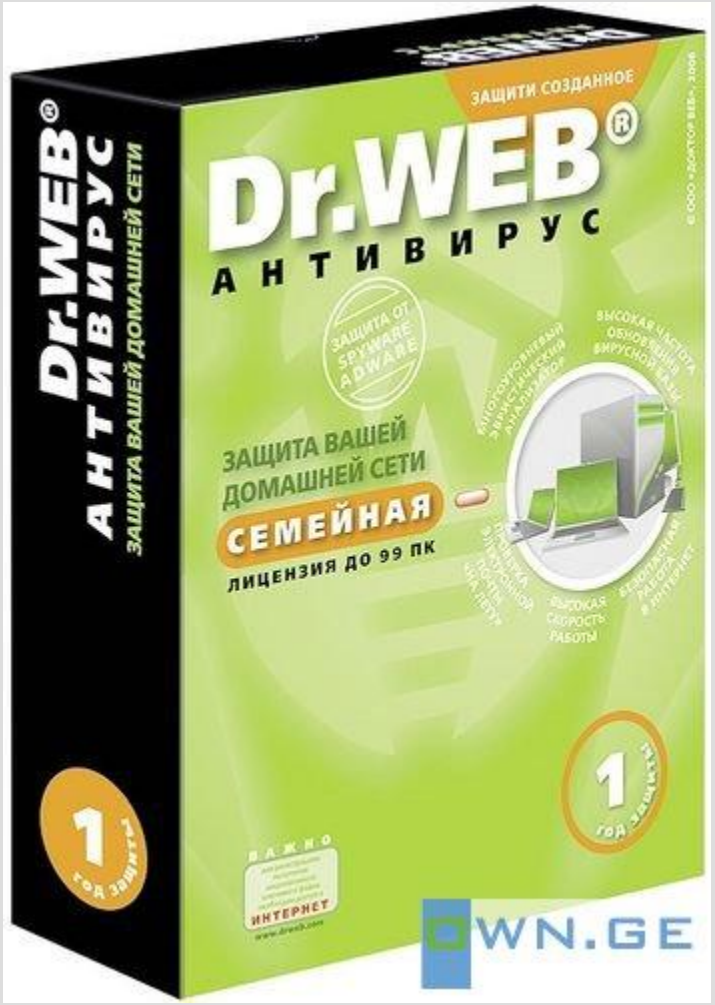
McAfee VirusScan (производитель: «McAfee Associates»).

Это один из наиболее известных антивирусных пакетов. Очень хорошо удаляет вирусы, но у VirusScan хуже, чем у других пакетов, обстоят дела с обнаружением новых разновидностей файловых вирусов. Он легко и быстро устанавливается с использованием настроек по умолчанию, но его можно настроить и по собственному усмотрению. Вы можете сканировать все файлы или только программные, распространять или не распространять процедуру сканирования на сжатые файлы. Имеет много функций для работы с сетью Интернет.



Dr.Web (производитель: «Диалог Наука»)

Популярный отечественный антивирус. Хорошо распознает вирусы, но в его базе их гораздо меньше чем у других антивирусных программ.



Antiviral Toolkit Pro (производитель: «Лаборатория Касперского»).

Это антивирус признан во всем мире как один из самых надежных. Несмотря на простоту в использовании он обладает всем необходимым арсеналом для борьбы с вирусами. Эвристический механизм, избыточное сканирование, сканирование архивов и упакованных файлов - это далеко не полный перечень его возможностей. Лаборатория Касперского внимательно следит за появлением новых вирусов и своевременно выпускает обновления антивирусных баз. Имеется резидентный монитор для контроля за исполняемыми файлами.

Заключение.

Несмотря на широкую распространенность антивирусных программ, вирусы продолжают «плодиться». Чтобы справиться с ними, необходимо создавать более универсальные и качественно-новые антивирусные программы, которые будут включать в себя все положительные качества своих предшественников. К сожалению, на данный момент нет такой антивирусной программы, которая гарантировала бы защиту от всех разновидностей вирусов на 100%, но некоторые фирмы, например «Лаборатория Касперского», на сегодняшний день достигли неплохих результатов.

Защищенность от вирусов зависит и от грамотности пользователя. Применение вкупе всех видов защит позволит достигнуть высокой безопасности компьютера, и соответственно, информации.