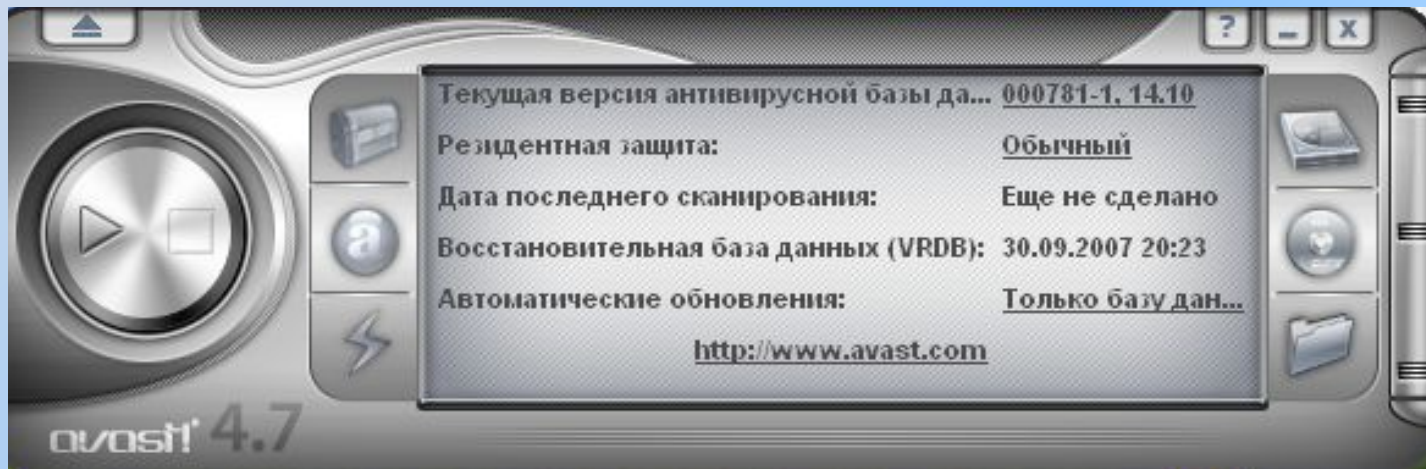


Антивирусные программы

Автор презентации:
преподаватель ГБОУ СПО ПК № 33
Зайцев О.Е.

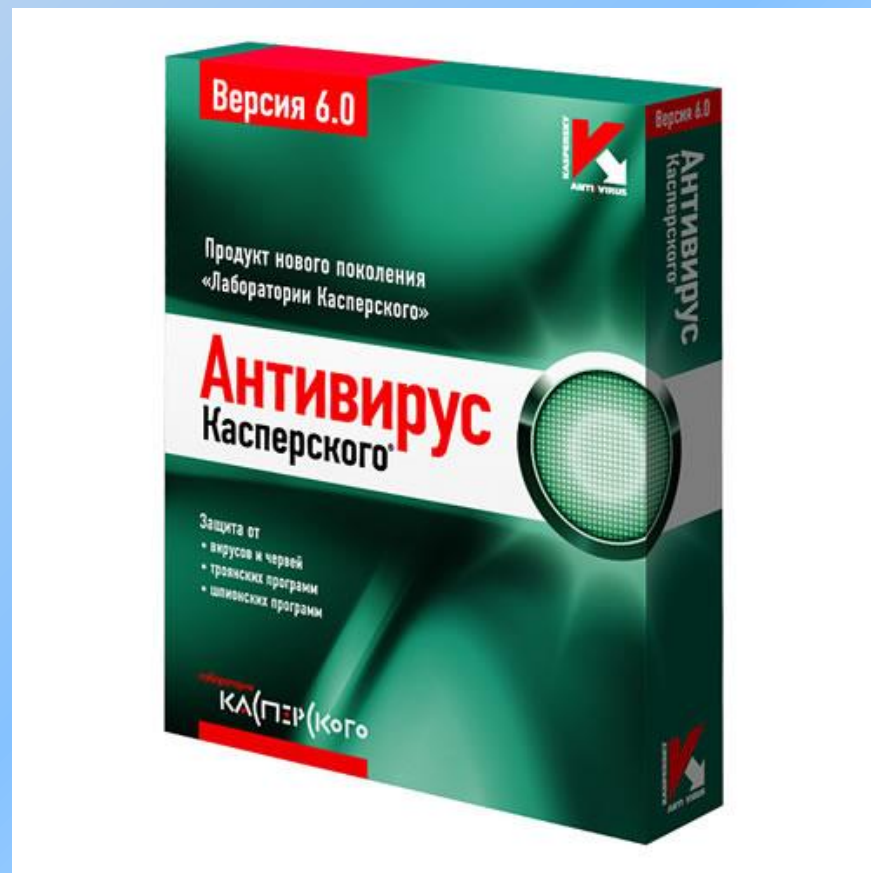
Антивирусные программы



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.

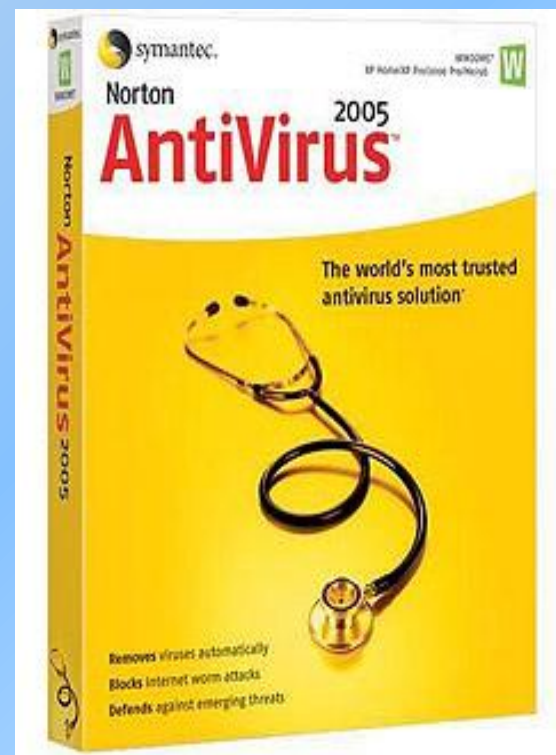
Тогда всегда есть вероятность того, что какие-то зараженные файлы остались незамеченными.



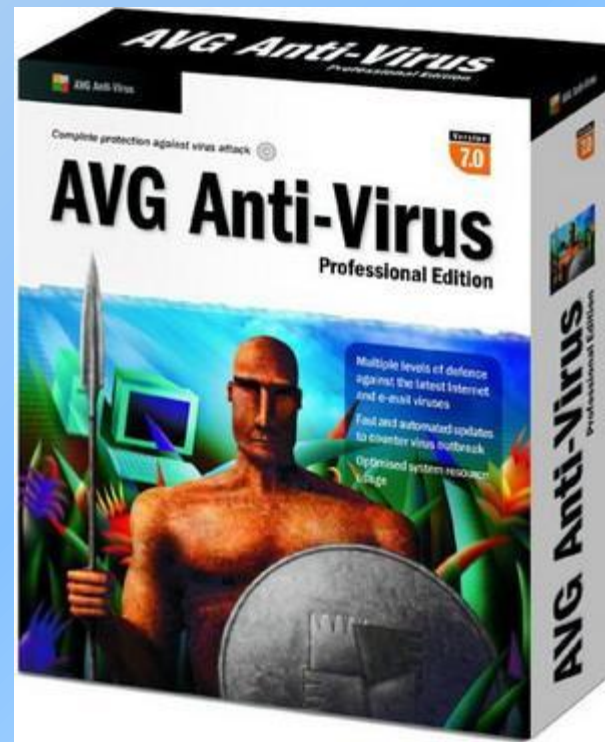
Немаловажным также является наличие резидентного монитора, осуществляющего проверку всех новых файлов “на лету” (то есть автоматически, по мере их записи на диск).



Сюда же следует отнести возможность восстанавливать зараженные файлы, не стирая их с жесткого диска, а только удалив из них вирусы. Немаловажным является также процент ложных срабатываний программы (ошибочное определение вируса в “чистом” файле).



Многоплатформенность (наличие версий программы под различные операционные системы). Конечно, если антивирус используется только дома, на одном компьютере, то этот параметр не имеет большого значения. Но вот антивирус для крупной организации просто обязан поддерживать все распространенные операционные системы.



Кроме того, при работе в сети немаловажным является наличие серверных функций, предназначенных для административной работы, а также возможность работы с различными видами серверов.



Характеристика антивирусных программ.

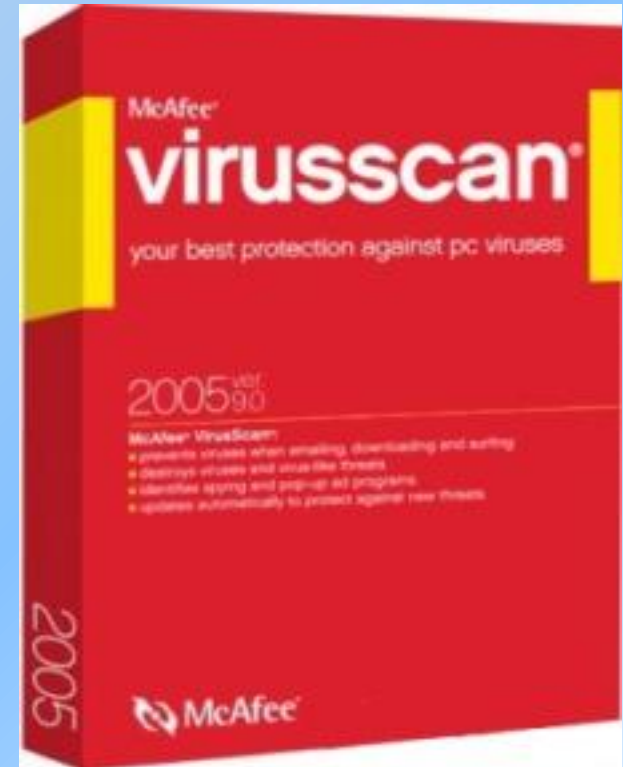
Антивирусные программы делятся на:
программы-детекторы, программы-доктора, программы-ревизоры, программы-фильтры, программы-вакцины.



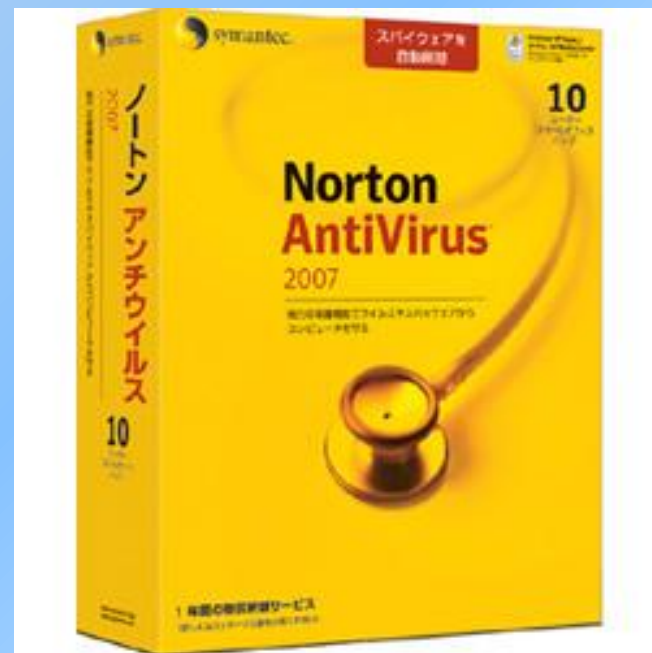
Программы-детекторы обеспечивают поиск и обнаружение вирусов в оперативной памяти и на внешних носителях, и при обнаружении выдают соответствующее сообщение. Различают детекторы универсальные и специализированные.



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.



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



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.



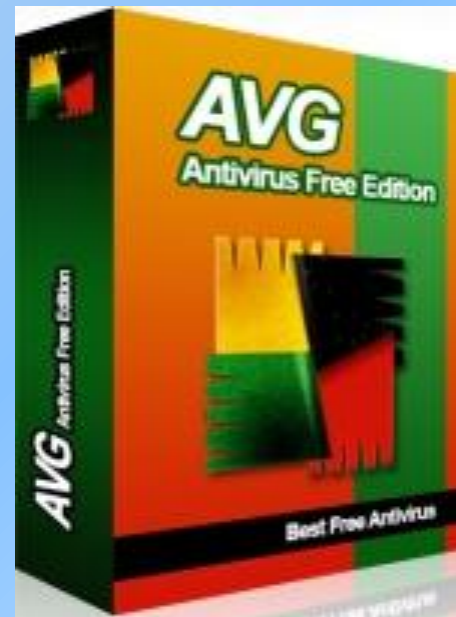
Среди фагов выделяют полифаги, т.е. программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов.



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



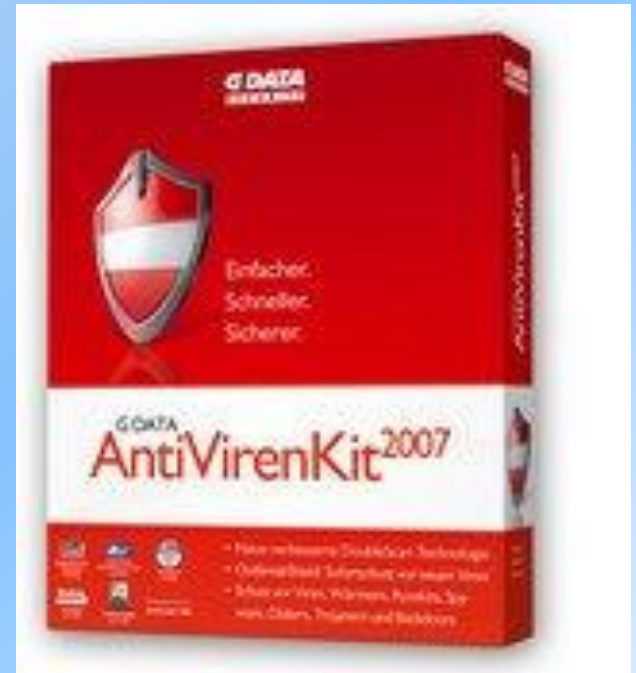
Программы-ревизоры относятся к самым надежным средствам защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на экран видеомонитора.



Как правило, сравнение состояний производят сразу после загрузки операционной системы. При сравнении проверяются длина файла, код циклического контроля (контрольная сумма файла), дата и время модификации, другие параметры.



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.

Таковыми 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" (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.



Существенным недостатком таких программ является их ограниченные возможности по предотвращению заражения от большого числа разнообразных вирусов.



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.

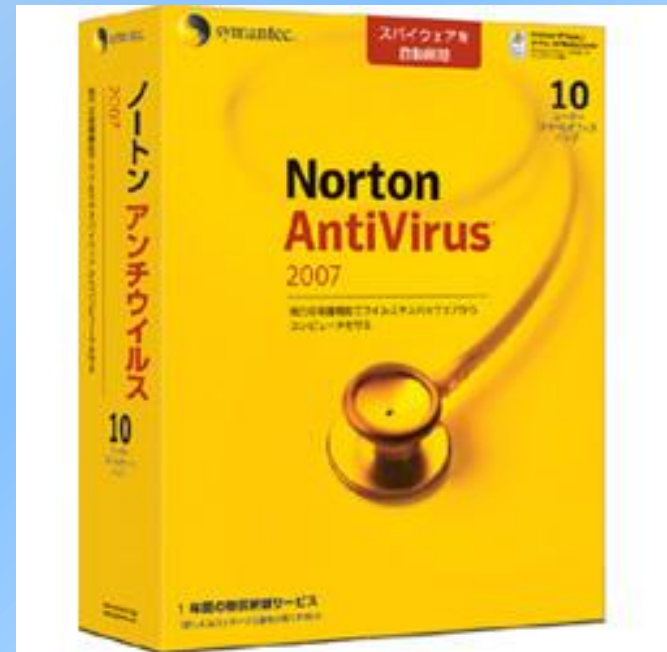


Существует множество
антивирусных программ.
Рассмотрим наиболее
известные из них.



Norton AntiVirus 4.0 и 5.0 (производитель: «Symantec»).

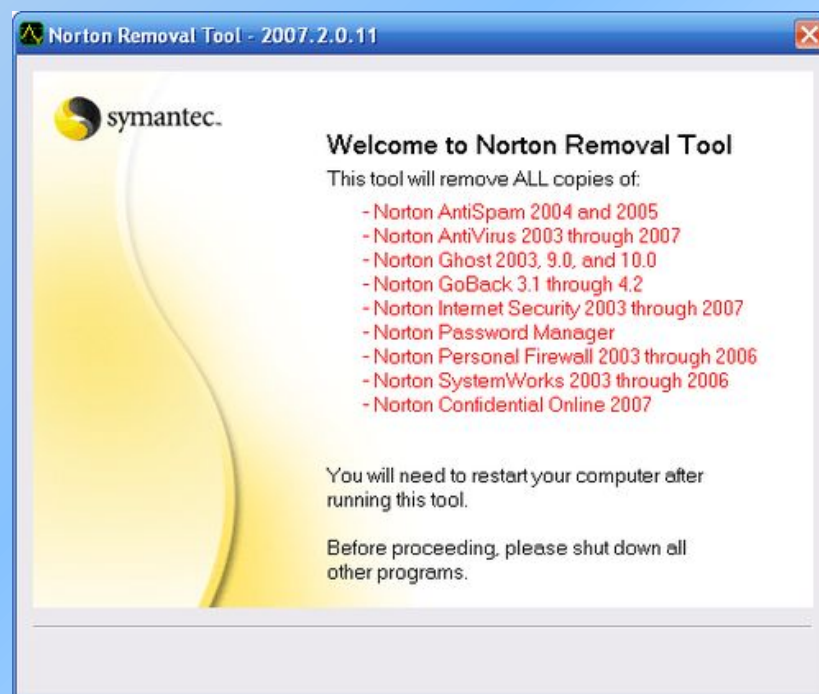
Один из наиболее известных и популярных антивирусов. Процент распознавания вирусов очень высокий (близок к 100%). В программе используется механизм, который позволяет распознавать новые неизвестные вирусы.



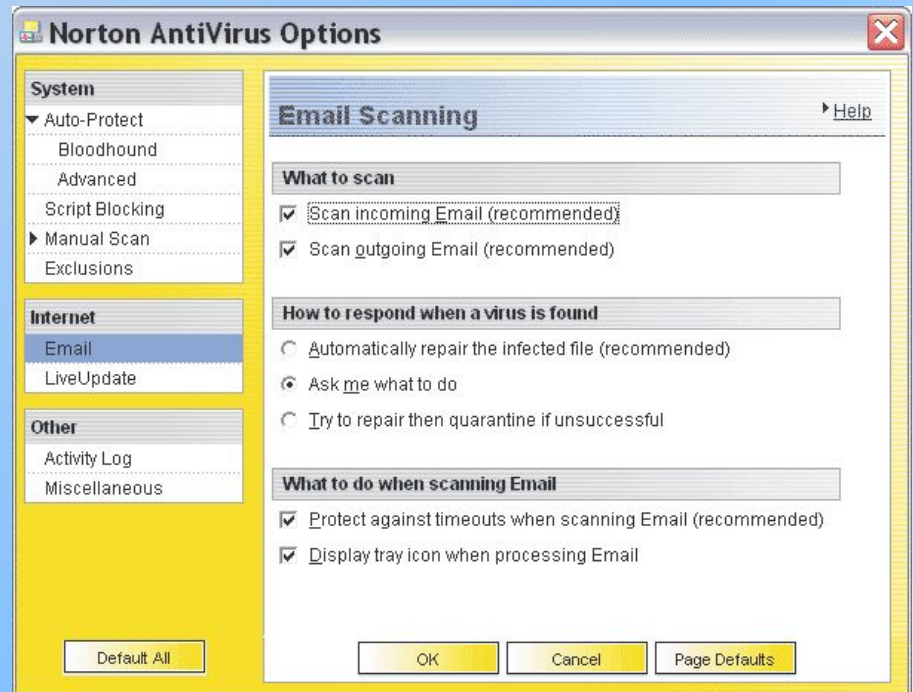
В интерфейсе программы Norton AntiVirus имеется функция LiveUpdate, позволяющая щелчком на одной-единственной кнопке обновлять через Web как программу, так и набор сигнатур вирусов.



Мастер по борьбе с вирусами выдает подробную информацию об обнаруженном вирусе, а также предоставляет вам возможность выбора: удалять вирус либо в автоматическом режиме, либо более осмотрительно, посредством пошаговой процедуры, которая позволяет увидеть каждое из выполняемых в процессе удаления действий.



Антивирусные базы обновляются очень часто (иногда обновления появляются несколько раз в неделю). Имеется резидентный монитор. Недостатком данной программы является сложность настройки (хотя базовые настройки изменять, практически не требуется).



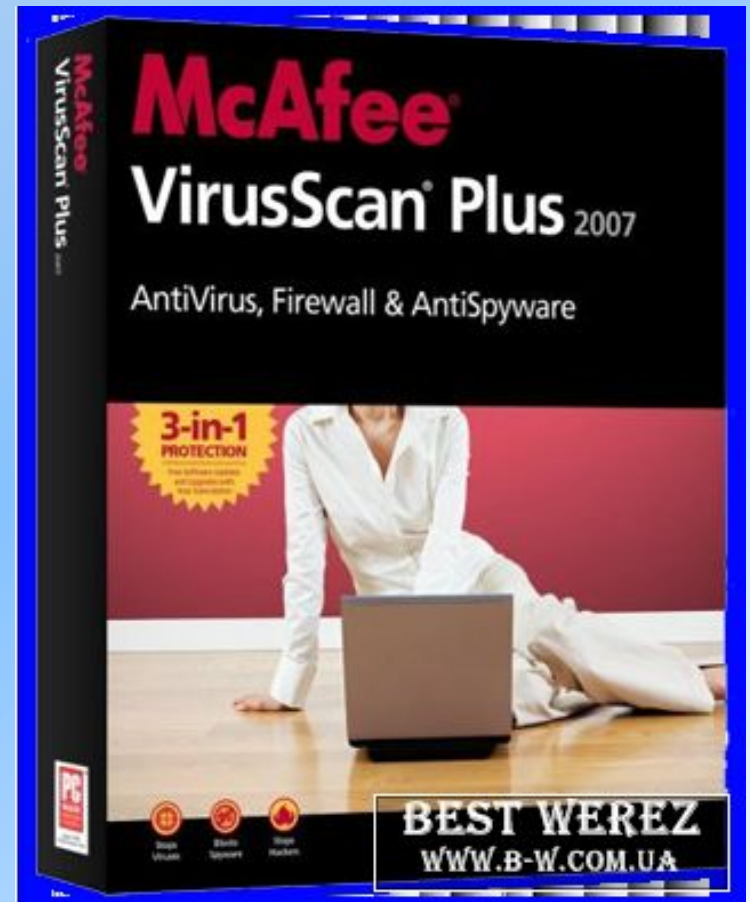
Dr Solomon's AntiVirus (производитель: «Dr Solomon's Software»).

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.



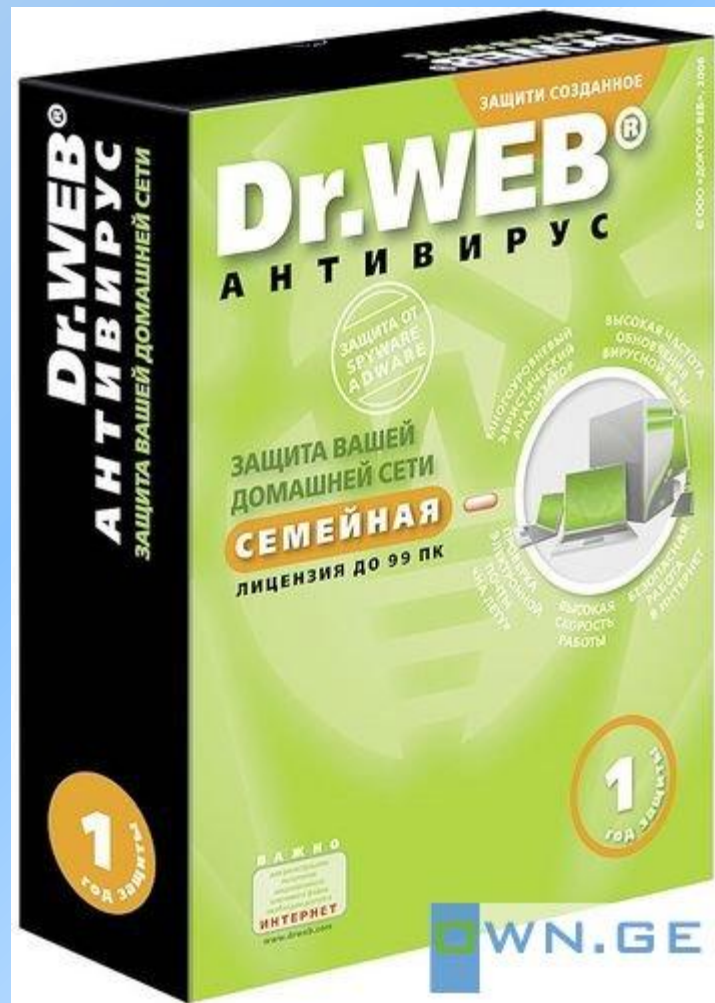
McAfee VirusScan (производитель: «McAfee Associates»).

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.



Конец

ПОВТО