

image not found or type unknown



Полностью отсечь вирусы с вашего компьютера вряд ли удастся, разве что вы удалите из системы дисковод, перестанете работать в Интернете и будете пользоваться только легальным программным обеспечением. Но в наших условиях все эти советы – особенно последний – выглядят либо утопией, либо издевательством.

Остаётся один способ: снабдить вашу ОС надёжными сторожами – антивирусными программами, которые смогут вовремя распознать и обезвредить прокравшегося вируса.

Практически все программы, описанные далее, просты и удобны в пользовании, способны отлавливать практически все существующие на сегодня группы вирусов. Большинство антивирусов способны не просто проверять по запросу пользователя диск на наличие вирусов, но и вести незаметную проверку всех запускаемых на компьютере файлов. Наконец, все современные антивирусы снабжены механизмом автоматического обновления антивирусных баз данных через Интернет. Необходимо лишь остановить свой выбор на одном из них.

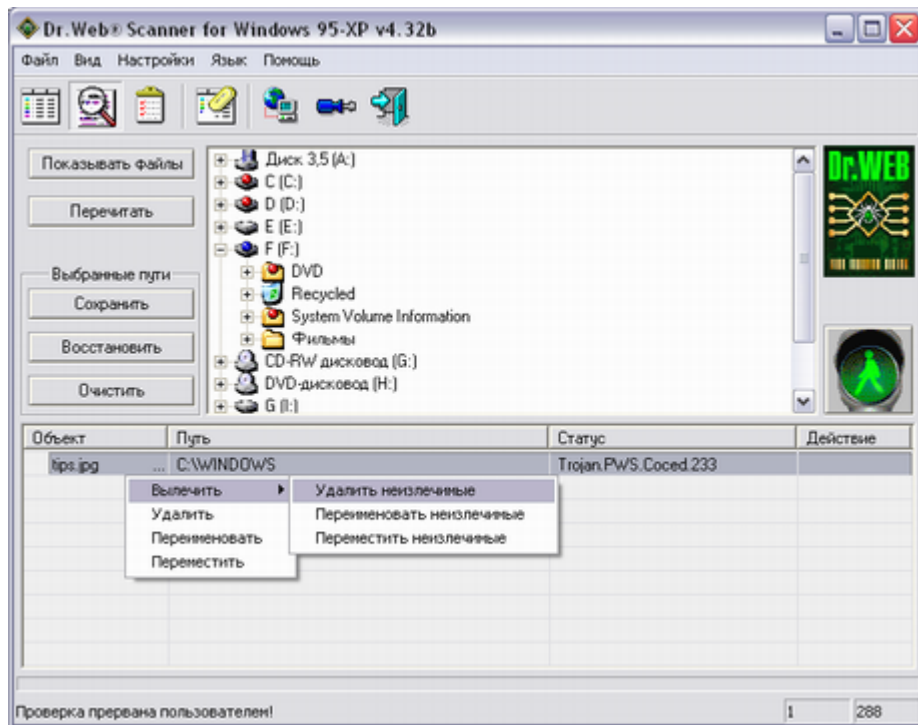
Основная часть

Антивирус Doctor Web

Программа Dr.Web является одной из первых отечественных антивирусных программ и в настоящее время относится к наиболее популярным. Немаловажным ее достоинством является относительно невысокая стоимость по сравнению с другими разработками аналогичного уровня. Разработчиком этой антивирусной программы является Игорь Данилов. Первая версия Dr.Web вышла в 1994 году.

Антивирусная база Dr.Web меньше, чем у KAV и насчитывает около 71000 записей. Однако создатели уверяют, что на результатах тестирования это не сказывается, поскольку в Dr.Web реализован принципиально иной подход, чем в его коллегам-антивирусах: в программу встроен модуль эвристического анализатора, который позволяет обезвредить не только уже известные программе, но и новые, ещё не опознанные вирусы. В любом случае, малый размер и сравнительно небольшой объём базы не мешают Dr.Web регулярно занимать призовые места в антивирусных

«чемпионатах» и сравнительных тестированиях. Кроме того, скорость пополнения баз данных у обоих антивирусов примерно одинакова. А самое главное, Dr.Web работает значительно быстрее своих громоздких конкурентов, а в некоторых случаях – ещё и корректнее. Именно Dr.Web первым из отечественных антивирусов подружился с Windows XP, что и привлекло к нему внимание пользователей.



Внешний вид Dr.Web.

При инсталляции Dr.Web пользователю предлагается выбрать требуемый вариант установки: Типичная, Минимальная и Выборочная. В большинстве случаев рекомендуется выбрать вариант Типичная, заданный по умолчанию. Следует учитывать, что после инсталляции программы необходимо перезагрузить компьютер.

Программа Dr.Web предусматривает использование двух языков интерфейса: русского и английского. Требуемый язык выбирают при инсталляции программы, однако в дальнейшем при необходимости его можно изменить.

В состав приложения входит несколько самостоятельных модулей, которые, как правило, работают независимо друг от друга, хотя используют одну и ту же антивирусную базу. На первых порах это может вызывать определенные затруднения, но уже через некоторое время неудобства исчезнут.

Как и KAV, Dr.Web устроен по модульному принципу:

- **Сканер Dr.Web**

Сканирует выбранные пользователем объекты на дисках по требованию, обнаруживает и нейтрализует вирусы в памяти, проверяет файлы автозагрузки и процессы.

- **Резидентный сторож (монитор) SpIDer Guard™**

Этот модуль предназначен для проверки файлов на наличие вирусов в тот момент, когда с ними выполняют определенное действие (запускают, записывают на диск и др.). Данная функция также отличается высокой надежностью — многие специалисты считают именно ее самым сильным местом программы. Контролирует в режиме реального времени все обращения к файлам, выявляет и блокирует подозрительные действия программ

- **Резидентный почтовый фильтр SpIDer Mail™**

Модуль SpIDer Mail представляет собой почтовый сканер и предназначен для проверки почтовых сообщений на предмет заражения их вирусами. Эту возможность настраивают отдельно: для нее предусмотрены специальные параметры. Следует отметить, что почтовый сканер SpIDer Mail отличается высокой надежностью.

SpIDer Mail контролирует в режиме реального времени все почтовые сообщения, входящие по протоколу POP3 и исходящие по протоколу SMTP

- **Сканер командной строки Dr.Web®**

Сканирует выбранные пользователем объекты на дисках по требованию, обнаруживает и нейтрализует вирусы в памяти, проверяет файлы автозагрузки и процессы.

- **Утилита автоматического обновления**

Загружает обновления вирусных баз и программных модулей, а также осуществляет процедуру регистрации и доставки лицензионного или демонстрационного ключевого файла.

- **Планировщик заданий**

Позволяет планировать регулярные действия, необходимые для обеспечения антивирусной защиты, например, обновления вирусных баз, сканирование дисков

компьютера, проверку файлов автозагрузки.

Модуль Dr.Web для Windows представляет собой инструмент для сканирования компьютера или выбранных объектов на предмет заражения вирусами. После установки программы вы сможете вызвать сканер с помощью соответствующей команды контекстного меню значка объекта в окне Проводника. При выполнении данной команды выбранный объект будет проверен на наличие вирусов.

Параметры сканирования устанавливаются в настройках программы. В частности, там указываются объекты, которые нужно проверить, определяется порядок действий в случае обнаружения вируса (переименовать зараженный объект, удалить его, вылечить или поместить в указанную папку), устанавливается количество ресурсов компьютера, выделяемых на сканирование, и др.

В процессе работы утилиты Dr.Web в области уведомлений Панели задач отображаются значки используемых в данный момент модулей.

Dr.Web проверяет все категории файлов, которые могут быть заражены: исполняемые файлы, документы Microsoft Word, архивы всех популярных форматов (ARJ, ZIP, RAR, TAR и так далее), скрипты VBS и многие другие.

Dr.Web является полифагом. Антивирусные программы полифаги являются самыми популярными и эффективными антивирусными программами. Принцип работы полифагов основан на проверке файлов, загрузочных секторов дисков и оперативной памяти и поиске в них известных и новых (неизвестных полифагу) вирусов.

Для поиска известных вирусов используются так называемые маски. Маской вируса является некоторая постоянная последовательность программного кода, специфичная для этого конкретного вируса. Если антивирусная программа обнаруживает такую последовательность в каком-либо файле, то файл считается зараженным вирусом и подлежит лечению.

Для поиска новых вирусов используются алгоритмы «эвристического сканирования», то есть анализ последовательности команд в проверяемом объекте. Если «подозрительная» последовательность команд обнаруживается, то полифаг выдает сообщение о возможном заражении объекта.

Полифаги могут обеспечивать проверку файлов в процессе и загрузки в оперативную память. Такие программы называются антивирусными мониторами.

К достоинствам полифагов относится их универсальность. К недостаткам можно отнести большие размеры используемых ими антивирусных баз данных, которые должны содержать информацию о максимально возможном количестве вирусов что, в свою очередь, приводит к относительно небольшой скорости поиска вирусов.

Заключение

В заключение хотелось бы предостеречь от слишком рьяной борьбы с компьютерными вирусами. Не стоит переоценивать возможностей этих подлых программ. Например, очень неразумным будет распоряжение начальника отформатировать все жесткие диски на компьютерах в отделе только из-за того, что на одном из них было обнаружено подозрение на такой-то вирус. Это приведет к неоправданной потере информации и сильной потере времени и сил, что, по нанесенному ущербу, будет больше, чем смог бы сделать вирус. Ежедневный запуск полного сканирования жесткого диска на наличие вирусов так же не блестящий шаг в профилактике заражений. Не превращайте компьютер в неприступную крепость, вооруженную до зубов, а то может не хватить ресурсов для выполнения необходимых задач. На мой взгляд, вам достаточно установить на компьютере программу Dr.Web. Она не требовательна к ресурсам