В современном мире жизнь почти каждого человека неразрывно связана с компьютерами, гаджетами и сетью интернет. Но кроме информации, которая открыта абсолютно любому пользователю в сети также множество вредоносных программ, которые могут не только своровать наши данные, но и нарушить (а в некоторых случаях и полностью вывести из работоспособности) функционирование наших гаджетов.

Чтобы не допустить этого и сохранить личные данные и существуют антивирусные программы. Одной из самых простых и доступных является программа Dr.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 коллегах-антивирусах: в программу встроен модуль эвристического анализатора, который позволяет обезвредить не только уже известные программе, но и новые, ещё не опознанные вирусы. 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 начал взаимодействовать с Windows XP, что и привлекло к нему внимание пользователей.

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.

В состав приложения входит несколько самостоятельных модулей, которые, как правило, работают независимо друг от друга, хотя используют одну и ту же антивирусную базу.

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) SplDer 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 SplDer Mail. Модуль SplDer Mail представляет собой почтовый сканер и предназначен для проверки почтовых сообщений на предмет заражения их вирусами.

SplDer 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. Параметры сканирования устанавливаются в настройках программы.

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.

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.

Не смотря на то что базы и возможности программы постоянно совершенствуются, вирусы тоже не стоят на месте. Их постоянно обновляют и учат обходить системы антивирусов, поэтому так сложно постоянно обновлять базы для быстрого реагирования на обновленные вирусы. Среди множество дорогостоящих программ, всегда приято осознавать, что есть надежная доступная программа способная помочь избавиться от большинства вредоносных вирусов.

Список литературы.

1. Емельянова, Н.З. Защита информации в персональном компьютере: Учебное пособие / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. - М.: Форум, 2013. - 368 с.
2. Москвитин, Г.И. Комплексная защита информации в организации / Г.И. Москвитин. - М.: Русайнс, 2017. - 400 с.
3. Сергеева, Ю.С. Защита информации. Конспект лекций / Ю.С. Сергеева. - М.: А-Приор, 2011. - 128 с.
4. Хорев, П.Б. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - М.: Форум, 2013. - 352 с.

5. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях / В.Ф. Шаньгин. - М.: ДМК Пресс, 2012. - 592 с.
6. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: Форум, 2018. - 256 с.