**Антивирус** – программа, ищущая [вирусы](http://security.mosmetod.ru/zashchita-ot-virusov/3-virusy), [трояны](http://security.mosmetod.ru/zashchita-ot-virusov/43-chto-eshche-nuzhno-znat-o-troyanskikh-programmakh), [червей](http://security.mosmetod.ru/zashchita-ot-virusov/41-chto-eshche-nuzhno-znat-o-kompyuternykh-virusakh-i-chervyakh), бэкдоры и прочее [нежелательное ПО](http://security.mosmetod.ru/zashchita-ot-virusov/44-klassifikatsiya-vredonosnykh-programm) на компьютере пользователя.

Как правило антивирусы разрабатываются для семейства ОС Windows, что как бы намекает на следующие особенности этой операционки: а) большую распространенность, б) большую уязвимость к атакам, в) большую перспективность рынка антивирусов из-за высокой коммерциализации (а Windows – в большинстве релизов платная ОС) и г) увы, малую компьютерную грамотность её пользователей.

Антивирусы бывают платные и [бесплатные](http://security.mosmetod.ru/zashchita-ot-virusov/besplatnye-antivirusy).

Если посмотреть со стороны на работу антивируса, его самого можно легко принять за вирус, но только со знаком плюс. Методы работы антивируса – слежение за сетевым трафиком, прослушивание портов, контроль служб, модификация и удаление файлов, сбор статистики и отправка данных разработчику ПО, изрядное потребление вычислительных мощностей… Разве что вывода из строя оборудования не хватает! Разумеется, все это направлено во благо пользователя и во имя сохранения его данных, но общая картина по меньшей мере любопытна. Кстати, именно из-за этой особенности крайне не рекомендуется устанавливать на одну машину сразу два антивируса. Мало того, что это без танцев с бубном редко кому удастся, так и последствия их совместной «работы» могут быть самыми причудливыми, вплоть до летальных для ОС.

Разные антивирусы по-разному борются с вредоносным ПО. Все антивирусы могут обнаруживать вирусы, но, к сожалению, не все эффективно лечить. В состав антивируса могут входить несколько модулей, в зависимости от релиза и того, на что способна контора-разработчик антивируса. Модули могут быть следующие: модуль поиска нежелательного ПО, модуль анализа подозрительного поведения программ (эвристический модуль), карантинный модуль для изоляции подозрительных файлов, [модуль обновлений](http://security.mosmetod.ru/zashchita-ot-virusov/53-regulyarnye-obnovleniya-antivirusnykh-programm) – для поддержания актуальности новым угрозам, модуль «исцеления» зараженных файлов, брандмауэр, он же файрвол, и некоторые другие.

Антивирус не является панацеей! Это один из множества «бойцов», брошенных в бой с угрозами безопасности в бесконечной войне за информацию, причем не самый сильный. Никакой антивирус не дает 100% защиты в силу особенностей его функционирования.

К сожалению, большая часть работы антивируса направлена на устранение последствий «негигиеничной» рискованной, а иногда, увы, попросту неграмотной работы пользователя в Интернете, с внешними носителями данных и неизвестными приложениями.

Основные методы борьбы с вирусами

Сигнатурный метод обнаружения

Наверняка вы встречались с сообщениями антивируса, например, Антивируса Касперского, о том, что антивирусные базы устарели и их необходимо обновить. О каких базах идет речь?

Антивирусная лаборатория – разработчик антивируса – выявляет вирус, анализирует его, и выявляет так называемую сигнатуру. Сигнатура вируса (сигнатура атаки) – особый цифровой признак вредоносной программы, по которому её можно «узнать» и однозначно определить. Эти сигнатуры вносятся в базу данных, чье обновление регулярно скачивает пользователь вручную или по расписанию. Сообщение от антивируса об устаревании базы вирусов сигнализирует об ослаблении защиты и повышении вероятности подхватить какой-нибудь «свежак».

Достоинства этого метода:

1. Отработанная надежность. Метод применяется давно и с успехом, можно сказать что это основной метод обнаружения вируса.
2. Высокое быстродействие.

Недостатки:

1. Проблема лавинообразного увеличения сигнатур. Виноваты и рост количества новых вирусов и способность видоизменяться у «старых». В итоге базы сигнатур вырастают до неприличных размеров, так что теряется второе достоинство метода. Ситуацию разрешают путем особых оптимизаций, когда одна сигнатура описывает сразу множество вирусов, однако при этом возникает проблема ложных срабатываний, что уменьшает первое достоинство.
2. Проблема выявления новых вирусов. Считается, что сами пользователи вносят слишком маленький вклад в увеличение базы данных вирусов. То есть обнаружение новых вирусов – это как будто бы проблема разработчиков антивируса, что с одной стороны кажется справедливым, с другой является нарушением принципа «безопасность – дело каждого». Во многих антивирусах встроена функция «отправить на проверку», которой следует невозбранно пользоваться. Основные методы решения проблемы – это взаимный обмен информацией с другими антивирусными конторами, эвристический, (то есть интеллектуальный, использующих особый алгоритм) поиск вирусов в Интернете, быстрая реакция во время эпидемий и сознательность системных инженеров, анализирующих подозрительную активность в сети.

Эвристические методы обнаружения

Многие антивирусные программы содержат в себе модуль так называемого эвристического поиска [вредоносных программ](http://security.mosmetod.ru/zashchita-ot-virusov). Суть метода в анализе поведения всех запускаемых программ. Если в процессе работы системы вдруг обнаруживается «подозрительное» поведение приложения, то есть программа вдруг начинает делать то, что раньше не делала, то срабатывает тревога и эвристический модуль сообщает пользователю о потенциальной угрозе.

Достоинства метода:

1. Весьма перспективное направление, в будущем возможности эвристического модуля возрастут и компьютер и информация будут лучше защищены от неожиданных и новейших угроз.
2. Эвристический модуль может реагировать на угрозы, информации о которых нет в базе сигнатур.

Недостатки метода:

1. Ложное срабатывание на безопасные события. В итоге пользователь может в раздражении отключить эвристический модуль, уменьшив защиту.
2. Из-за особенностей работы эвристического модуля есть проблема излишнего потребления вычислительных мощностей. Попросту говоря, антивирус сжирает всю память и процессор, в итоге не то что в игры не поиграешь, в Word`е толком не поработаешь. Итог тот же – отключение модуля и уменьшение защиты.

Брандмауэр или файрвол

Брандмауэр предназначен для защиты от сетевых угроз – из локальной сети и Интернета.

Этот модуль далеко не всегда входит в стандартный набор [антивируса](http://security.mosmetod.ru/zashchita-ot-virusov/29-printsipy-raboty-antivirusa-chast-2), зачастую брандмауэр разрабатывается, поставляется и продается как отдельная программа.

Многие программы для соединения с удаленными компьютерами или серверами могут использовать небезопасные методы, оставляя «дырки» и уязвимости для проникновения извне.



Суть работы брандмауэра в контроле как входящего, так и исходящего трафика путем ограничения возможности устанавливать соединения с определенными удаленными ресурсами. Самый наглядный метод защиты – белые и черные списки сетевых ресурсов.

«Черный» список сетевых ресурсов – это список, например, сайтов, куда заходить нельзя, а «белый» список – это список ресурсов, куда только и можно заходить. Как нетрудно заметить, метод белого списка значительно более безопасен, но и сильно ограничивает возможности пользователя и программ.

Достоинства брандмауэра:

1. Настройки брандмауэра позволяют обеспечить возможность сетевого взаимодействия только с проверенными ресурсами, отсекая все потенциально опасные и непроверенные.
2. Может быть установлен на сетевом шлюзе локальной сети, то есть на сервере, «раздающем» доступ в Интернет компьютерам, например, школы, при этом не тратя вычислительные ресурсы пользовательских машин.

Недостатки брандмауэра:

1. Недостаток брандмауэра логически вытекает из его достоинства: для качественной настройки файрвола требуются хорошие знания сетевых протоколов и особенностей работы сетевых приложений. Брандмауэр, работающий с настройками «по умолчанию» мало от чего способен защитить.

Источник информации <http://security.mosmetod.ru/zashchita-ot-virusov/29-printsipy-raboty-antivirusa-chast-2>