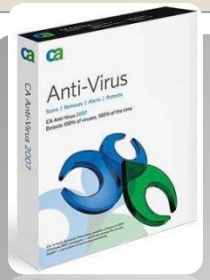
Антивирусные программы

МОУ Весьегонская СОШ



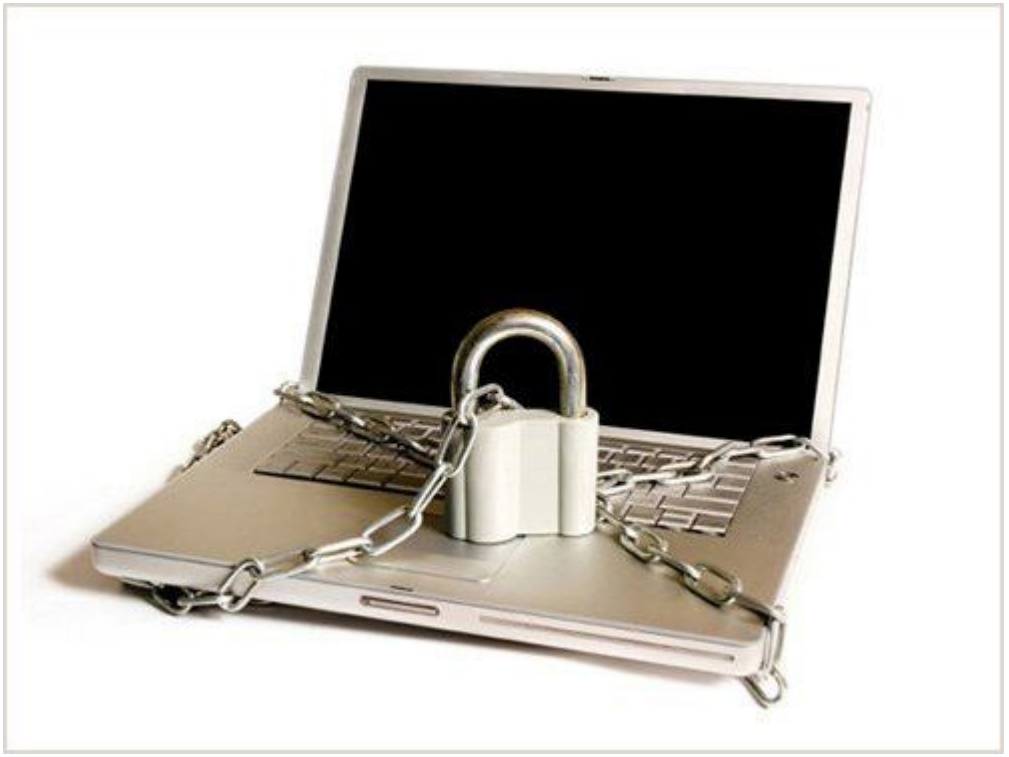
Антивирусная программа

Антивирусная программа (антивирус) — программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще, и восстановления зараженных (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом .

Антивирусное программное обеспечение

Антивирусное программное обеспечение состоит из подпрограмм, которые пытаются обнаружить, предотвратить размножение и удалить компьютерные вирусы и другое вредоносное программное обеспечение.

Методы обнаружения вирусов



Методы обнаружения вирусов

Антивирусное программное обеспечение обычно использует два отличных друг от друга метода для выполнения своих задач:

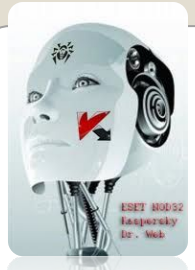
- Сканирование файлов для поиска известных вирусов, соответствующих определению в антивирусных базах.
- Обнаружение подозрительного поведения любой из программ, похожего на поведение заражённой программы.

Метод соответствия определению вирусов в словаре

Это метод, при котором антивирусная программа, анализируя файл, обращается к антивирусным базам, составленные производителем программы-антивируса. В случае соответствия какого-либо участка кода просматриваемого файла (сигнатуре) вируса в базах, программа-антивирус может по запросу выполнить одно из следующих действий:

1. Удалить инфицированный файл.
2. Заблокировать доступ к инфицированному файлу.
3. Отправить файл в карантин (то есть сделать его недоступным для выполнения с целью недопущения дальнейшего распространения вируса).
4. Попытаться «вылечить» файл, удалив тело вируса из файла.
5. В случае невозможности лечения/удаления, выполнить эту процедуру при следующей перезагрузке операционной системы.

Вирусная база регулярно обновляется производителем антивирусов, пользователем рекомендуется обновлять их как можно чаще



Метод обнаружения странного поведения программ

Антивирусы, использующие метод обнаружения подозрительного поведения программ не пытаются идентифицировать известные вирусы, вместо этого они прослеживают поведение всех программ. Если программа пытается выполнить какие-либо подозрительные с точки зрения антивирусной программы действия, то такая активность будет заблокирована, или же антивирус может предупредить пользователя о потенциально опасных действиях такой программы.

В настоящее время подобные превентивные методы обнаружения вредоносного кода, в том или ином виде, широко применяются в качестве модуля антивирусной программы, а не отдельного продукта.

В отличие от метода поиска соответствия определению вируса в антивирусных базах, метод обнаружения подозрительного поведения даёт защиту от новых вирусов, которых ещё нет в антивирусных базах. Но вместе с тем, такой метод даёт большое количество ложных срабатываний, выявляя подозрительную активность среди не вредоносных программ.

Метод обнаружения при помощи эмуляции

Некоторые программы-антивирусы пытаются имитировать начало выполнения кода каждой новой вызываемой на исполнение программы перед тем как передать ей управление. Если программа использует самоизменяющийся код или проявляет вирусную активность, такая программа будет считаться вредоносной, способной заразить другие файлы. Однако этот метод тоже изобилует большим количеством ошибочных предупреждений.

Метод «Белого списка»

Общая технология по борьбе с вредоносными программами — это «белый список». Вместо того, чтобы искать только известные вредоносные программы, эта технология предотвращает выполнение всех компьютерных кодов за исключением тех, которые были ранее обозначены системным администратором как безопасные. Выбрав этот параметр отказа по умолчанию, можно избежать ограничений, характерных для обновления сигнатур вирусов. К тому же, те приложения на компьютере, которые системный администратор не хочет устанавливать, не выполняются, так как их нет в «белом списке».

Эвристический анализ

В целом термином «эвристический анализ» сегодня называют совокупность функций антивируса, нацеленных на обнаружение неизвестных вирусным базам вредоносных программ, но в то же время этот же термин обозначает один из конкретных способов.

Эвристическое сканирование в целом схоже с сигнатурным, однако, в отличие от него, ищется не точное совпадение с записью в сигнатуре, а допускается расхождение. Таким образом становится возможным обнаружить разновидность ранее известного вируса без необходимости обновления сигнатур. Также антивирус может использовать универсальные эвристические сигнатуры, в которых заложен общий вид вредоносной программы. В таком случае антивирусная программа может лишь классифицировать вирус, но не дать точного названия.

HIPS

HIPS — система мониторинга всех приложений, работающих в системе, с чётким разделением прав для разных приложений. Таким образом HIPS может предотвратить деструктивную деятельность вируса, не дав ему необходимых прав. Приложения делятся на группы, начиная от «Доверенных», права которых не ограничены, заканчивая «Заблокированными», которым HIPS не даст прав даже на запуск.

Недостатки

Ни одна из существующих антивирусных технологий не может обеспечить полной защиты от вирусов

- Антивирусная программа забирает часть вычислительных ресурсов системы, нагружая центральный процессор и жёсткий диск. Особенно это может быть заметно на слабых компьютерах. Замедление в фоновом режиме работы может достигать 380 %.
- Антивирусные программы могут видеть угрозу там, где её нет (ложные срабатывания).
- Антивирусные программы загружают обновления из Интернета, тем самым расходуя трафик.
- Различные методы шифрования и упаковки вредоносных программ делают даже известные вирусы не обнаруживаемыми антивирусным программным обеспечением. Для обнаружения этих «замаскированных» вирусов требуется мощный механизм распаковки, который может дешифровать файлы перед их проверкой. Однако во многих антивирусных программах эта возможность отсутствует и, в связи с этим, часто невозможно обнаружить зашифрованные вирусы.

Классификация антивирусов

По набору функций и гибкости настроек антивирусы можно разделить на:

- ***Продукты для домашних пользователей:***
  - Собственно антивирусы;
  - Комбинированные продукты (например, к классическому антивирусу добавлен антиспам, файрвол, антируткит и т. д.);
- ***Корпоративные продукты:***
  - Серверные антивирусы;
  - Антивирусы на рабочих станциях («endpoint»);
  - Антивирусы для почтовых серверов;
  - Антивирусы для шлюзов.

Ложные антивирусы (лжеантивирусы)

В 2009 году различные производители антивирусов стали сообщать о широком распространении нового типа программ — ложных или лже-антивирусов (rogueware). По сути эти программы или вовсе не являются антивирусами (то есть не способны бороться с вредоносным ПО), или даже являются вирусами (воруют данные кредитных карт и т. п.).

Ложные антивирусы используются для вымогательства денег у пользователей путём обмана. Один из способов заражения ПК ложным антивирусом следующий. Пользователь попадает на «инфицированный» сайт, который выдаёт ему предупреждающее сообщение вроде «На вашем компьютере обнаружен вирус» и предлагает скачать бесплатную программу для удаления вируса. После установки такая программа производит сканирование компьютера и якобы обнаруживает ещё массу вирусов. Для удаления вредоносного ПО ложный антивирус предлагает купить платную версию программы. Шокированный пользователь платит (суммы колеблются от $10 до $80) и ложный антивирус очищает ПК от несуществующих вирусов.

Антивирусы, мобильные устройства и инновационные решения

Сейчас стало возможно и заражение мобильных телефонов вирусами, но только для телефонов на базе операционных систем, таких как Symbian, Windows Mobile, Blackberry, iPhone OS. Все больше разработчиков предлагают антивирусные программы для борьбы с вирусами и защиты мобильных телефонов. В мобильных устройствах есть следующие виды борьбы с вирусами:

- сигнатурный;
- защита от спама по SMS;
- шифрование данных

Антивирусные программы

- Dr.Web Space Security
- Eset Smart Security 4
- Kaspersky Internet Security
- Norton Internet Security
- Outpost Security Suite
- Panda Internet Security