Подготовил студент ФУИТ С.Козлов

По материалам сайтов
http://www.lookinfo.org
http://www.anti-malware.ru
http://ru.wikipedia.org/

АНТИВИРУСНЫЕ ПРОГРАММЫ

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

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

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.

Сканирование может запускаться как и принудительно, так и по расписанию, в качестве профилактики. Обнаружение подозрительного поведения программ почти всегда производится в режиме реального времени.

Метод соответствия определению вирусов в словаре

Это метод, при котором антивирусная программа, анализируя файл, обращается к антивирусным базам, составленным 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:

- удалить инфицированный файл;
- заблокировать доступ к инфицированному файлу;
- отправить файл в карантин (то есть сделать его недоступным для выполнения с целью недопущения дальнейшего распространения вируса);

- попытаться «вылечить» файл, удалив тело вируса из файла;
- в случае невозможности лечения/удаления, выполнить эту процедуру при следующей перезагрузке операционной системы.

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

Для многих антивирусных программ с базой сигнатур характерна проверка файлов в момент, когда операционная система обращается к файлам. Таким образом, программа может обнаружить известный вирус сразу после его получения. При этом системный администратор может установить в антивирусной программе расписание для регулярной проверки (сканирования) всех файлов на жёстком диске компьютера.

Хотя антивирусные программы, созданные на основе поиска сигнатур, при обычных обстоятельствах могут достаточно эффективно препятствовать заражению компьютеров, авторы вирусов стараются обойти такие антивирусы, создавая «олигоморфические», «полиморфические» и «метаморфические» вирусы, отдельные части которых шифруются или искажаются так, чтобы было невозможно обнаружить совпадение с записью в сигнатуре.

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. Некоторые программы или модули, построенные на этом методе, могут выдавать слишком большое количество предупреждений, что может запутать пользователя.

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». Так как у

современных предприятий есть множество надежных приложений, ответственность за ограничения в использовании этой технологии возлагается на системных администраторов и соответствующим образом составленные ими «белые списки» надежных приложений.

Однако, все активно продвигающиеся на ИТ рынке антивирусы работают по принципу «черного списка», и вот почему: чтобы работать по схеме подписки, при которой есть услуга со стороны антивирусной компании по поддержанию сигнатурных баз, т.е. черного списка, в актуальном состоянии и есть регулярные отчисления за пользование этой услугой. Именно из-за несравненно большей прибыльности метода «черного списка» для антивирусных компаний метод «белого списка» остается незаслуженно незамеченным.

Недостатки антивирусов:

- 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).

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)

С 2009 года различные производители антивирусов стали сообщать о широком распространении нового типа программ — ложных или лжеантивирусов. По сути эти программы или вовсе не являются антивирусами, или даже являются вирусами.

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.

Выбор антивируса

<mad_enot> народ посоветуйте антивирус хороший
<PinDOS> каспер
<Jekel> nod32
<Distortion_Finger{Bumer}> аваст
<mad_enot> эээ
<mad_enot> так всётаки?
<Distortion_Finger{Bumer}> аваст
<Jekel> nod32
<PinDOS> каспер

Цитата из одного чатов рунета как нельзя лучше показывает, что у всех антивирусов существуют как плюсы, так и минусы. И что каждый пользователь выбирает свой антивирус, который максимально удовлетворяет его личным требованиям.

Итоги летнего голосавания пользователей одного из сайтов за лучший антивирус, посвященных антивирусам:

Антивирус	**Кол-во голосов**	**Процентное соотношение**
NOD32	452	26.1%
Kaspersky	368	21.2%
Avast	317	18.3%
Dr.Web	307	17.7%
McAfee	85	4.9%
Avira	71	4.1%
Norton	49	2.8%
Другой	29	1.7%
Не использую	24	1.4%