УДК 004.056.57

Сравнение платных и бесплатных антивирусов

Гранков Д.В. Орел УНПК, 11-ТБ.

Общепринятое определение термина антивирус звучит как «программа, которая защищает ваш компьютер от вирусов, т.е. вредоносных программ». Но прежде всего, цель антивируса – обнаружить и вылечить зараженную программу, а также предотвратить заражение файлов. Кроме того, существуют «файрволы» - приложения, осуществляющие контроль над пакетами, передаваемыми по сети. По сути файрвол – это межсетевой экран для отдельного компьютера, но также имеет некоторые дополнительные функции.

Первые самые простые антивирусные программы появились закономерно сразу после появления первых самых простых вирусов. На данном этапе развития технологий антивирусные программы ушли далеко от своих прототипов. Существует большое разнообразие программ, несколько методов обнаружения вирусов и крупные компании, занимающиеся разработкой антивирусного программного обеспечения.

Условно антивирусы можно поделить на несколько категорий в зависимости от способа пользования и частоты применения.

Комплексные антивирусные программы. Это тип антивирусов, которые осуществляют полный контроль программного обеспечения, установленного на компьютере. Самые распространенные программы такого типа – антивирусы Касперского, Dr.Web, Avira, Avast, NOD32, McAfee, Panda, Norton, AVG.

Бесплатные версии антивирусов для домашнего пользования. Эти антивирусы представляют собой урезанные аналоги комплексных программ. Пользователь устанавливает такую программу на свой компьютер, убеждается в качестве продукции, а после покупает полную, «профессиональную», версию этой же антивирусной программы. Вполне

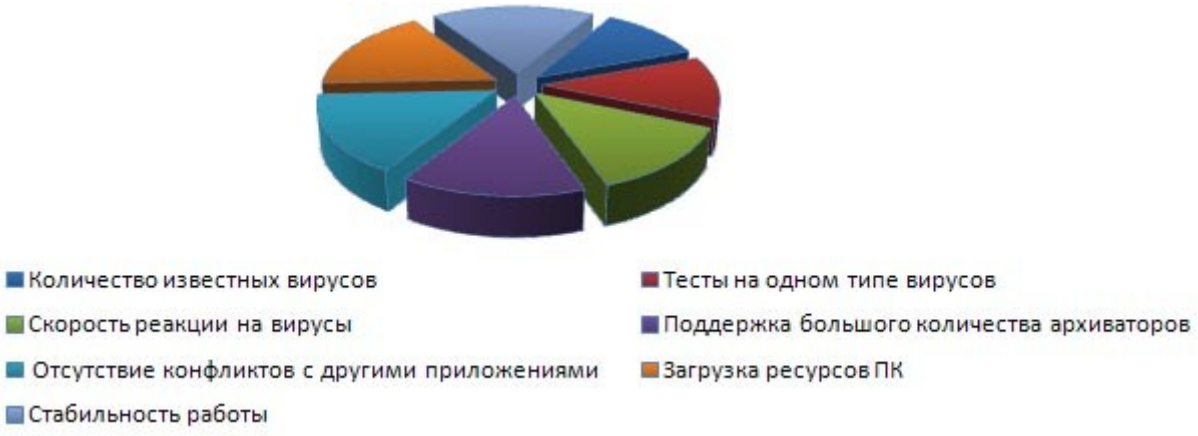
продуманный маркетинговый ход. Самые известные среди таких версий антивирусов – Avira AntiVir Personal Edition Classic и avast! 4 Home Edition.

Антивирусные программы, требующие запуска вручную. Такие программы не проводят постоянный мониторинг программного обеспечения компьютера, а запускаются при необходимости (например, перед выходом в сеть или для сканирования съемных носителей). Из такого типа программ – самые известные Dr.Web CruelIT! и утилиты Касперского.

Антивирусы, проверяющие систему при загрузки. Для использования такого типа утилит не достаточно иметь уровень пользователя – необходимы дополнительные навыки и квалификация выше средней.

Практически каждая копания производитель антивирусов выпускает демо-версию продукта (либо «trial»). Пользователь может установить антивирусную программу на определенный срок (обычно от 10 дней до месяца), после чего должен либо удалить программу с компьютера либо приобрести продукт. По истечении срока демо-версия продукта может полностью потерять функциональность либо частично выполнять какие-либо функции, но в любом случае полноценно работать не сможет.

На вопрос «Какую антивирусную программу предпочесть?» нельзя дать однозначного ответа. Многие спорят, какой из антивирусов надежнее, удобнее, по каким критериям можно их вообще оценивать. Вот примерный список параметров, по которым антивирус можно выбирать.



1. Количество вредителей, с которым знаком антивирус. Многие считают программу Kaspersky более эффективной защитой, чем DrWeb,

поскольку первая знает более сотни тысяч различных вирусов, а вторая – только шестьдесят тысяч. Однако нужно знать о том, что количество, которое указывают производители антивирусов как количество вредоносных программ, на самом деле означает число записей в антивирусных базах. А это совсем разные вещи. Одной записью может определяться несколько разных вирусов, а поэтому прямой связи между этими цифрами не существует. Иногда сами производители антивирусного программного обеспечения точно не могут сказать, какое количество вирусов может преодолеть их продукт. Поэтому количество записей в базах нельзя назвать объективным критерием выбора антивируса.

2. Тесты с одним типом вирусов. На зараженный компьютер устанавливают по очереди несколько антивирусов и сравнивают результаты поиска. Этот метод является самым популярным на данный момент.

3. Как быстро антивирус реагирует на появление новых вирусов. Пока вирус не попадет в базу антивируса, программа его не видит. Именно поэтому колоссальное значение имеет регулярность, с которой вы обновляете базы. Чем чаще базы обновляются, тем более надежным можно считать антивирус. Системные администраторы и опытные пользователи сами находят новые вирусы и присылают их на анализ. Именно поэтому базы известного антивируса всегда обновляются оперативнее, чем менее популярного.

4. Поддержка паковщиков и крипторов. Паковщики – это элемент каждого антивируса. Главная его задача – кодировать файлы. Для этого паковщик работает с исходным файлом, кодируя его и вставляя в начало процедуру декодирования. Файл при этом внешне никак не меняется. После того, как его запускаешь, вначале идет декодирование, после чего управление переходит к исходному коду. Пользователи не ощутят никакой разницы между кодированными и не кодированными файлами, значение они имеют лишь для самого антивируса. Он имеет дело с сигнатурой файла, а поэтому результат исполнения для него не важен. Сигнатура в шифрованном файле совсем другая, чем в исходном.

Возьмем, например, вирус, который известен антивирусной программе, запакуем его. Функциональность вируса при этом останется прежней, однако во время сканирования, если у антивируса нет соответствующего пакера, распознать файл, содержащий вирус, будет невозможно. Шифрование вирусов – это самый популярный прием, который применяется для того, чтобы его не распознали. Поэтому чем больше паковщиков и дешифровщиков содержит антивирус, тем лучше.

5. Соответствие антивируса другим приложениям и стабильность его работы. Качественная антивирусная программа глубоко проникает в систему, а поэтому очень важно, насколько хорошо её воспримут другие приложения, поскольку несоответствие может спровоцировать аварийную ситуацию в оперативной системе. Программ, которые бы вообще не содержали ошибок, не существует. Именно поэтому эффективно работающий антивирус может вызвать наибольшее количество конфликтов, поскольку хорошо проникает в систему. Но если антивирус является вообще «неконфликтным», скорее всего, он работает поверхностно, и не может считаться хорошей защитой вашего компьютера.

6. Загрузка ресурсов компьютера антивирусом. Если ПК работает в реальном времени, антивирус отбирает значительное количество его ресурсов. Многие оценивают антивирус именно по этому параметру: влияет ли он на скорость работы компьютера. При этом стоит учитывать, что самые эффективные программы требуют намного больше ресурсов, чем посредственные. Поэтому нужно быть готовым к каким-то жертвам ради высшей цели – обеспечения полной безопасности своему компьютеру.

Сравнение антивирусов (см. табл. 1).

Функции	Avast		AVG		Kaspersky		Dr. Web		Comodo Antivirus	Nano AntiVirus
	Коммерческий	Свободный	Коммерческий	Свободный	Коммерческий	Пробная версия	Коммерческий	Пробная версия	Свободный	Свободный
Модуль поиска и устранения угроз	+	+	+	+	+	+	+	+	+	+
Проверка исходящего трафика	+	+	+	+	+	+	+	+	+	-
Модуль антиспам	+	+	+	+	+	-	+	+	+	+
Модуль родительского контроля	-	-	-	-	+	-	+	+	+	-
Модуль самозащиты	+	+	+	+	+	+	+	+	+	+
Защита от SpyWare	+	+	+	-	+	-	+	+	+	+
Проверка сайтов в режиме реального времени	+	+	+	+	+	+	+	+	-	-

Табл.1. Сравнение платных и бесплатных антивирусов.

Антивирусные компании в последние месяцы все чаще сообщают о появлении поддельного программного обеспечения, которое маскируется под те или иные разработки. По словам экспертов, подобные "болванки" в лучшем случае просто ничего не делают, похитив у покупателя деньги за покупку этой программы, а в худшем, еще и заражают компьютер пользователя набором злонамеренных программ. В большинстве случае для распространения подделок злоумышленники используют такие же поддельные фишинговые сайты, которые по названию и внешнему виду похожи на легальные сайты производителей.

Первое и самое главное, что все должны знать: настоящий антивирус никогда не попросит денег за лечение вирусов. Если же закончилась лицензия - он просто либо перестанет искать вирусы, либо перестанет защищать от новых вирусов, но по прежнему будет находить и лечить старые. Так что, если “антивирус” просит деньги, чтобы вылечить вирус - это поддельный антивирус.

Эти поддельные антивирусы выглядят очень похоже на настоящие антивирусы и их сообщения очень назойливы и пугающи. Раз в 5-10 минут они всплывают, сообщают вам о том, что вы заражены и нужно срочно вылечиться, а для этого заплатить.

Естественно, этих вирусов, которыми поддельный антивирус пугает, на компьютере нет. Они просто выбирают случайные незараженные файлы на компьютере и говорят, что они заражены вирусом, а имя подбирают случайно из списка “страшных” имен.

В итоге люди пугаются и платят. Вы теряете 50 долларов, ничего не исправляете и, внимание, данные вашей кредитной карты остаются у пиратов.

Здесь невольную помощь злоумышленникам оказывают поисковики, говорят в консалтинговой компании Finjan. По расчетам этой компании, в наиболее удачные для себя дни мошенники при грамотном подходе могут заработать около 10 000 долларов на продаже "болванок". "Они (мошенники)

делают ставку на обман пользователей - сообщают, что пользовательские компьютеры якобы заражены троянами, что на компьютере нет того или иного платного кодека и принуждают купить "необходимое" программное обеспечение. В лучшем для пользователя случае, купленный софт просто ничего не будет делать", - говорит Юваль Бен-Ицхак, технический директор Finjan.

По его словам, чаще всего в подобных схемах пользователям предлагают купить поддельные антивирусы. Согласно данным отчета Anti-Phishing Working Group, за последние 4 месяца в интернете было выявлено 9 287 образцов поддельного программного обеспечения, что по сравнению с данными 12-месячной давности дает прирост в 225%. "Для продвижения своих продуктов злоумышленники также зачастую используют поисковую оптимизацию, чтобы ввести в заблуждение интернет-поисковики", - говорит он. По данным Finjan, в большинстве случае после установки на компьютеры пользователей поддельного софта, система начинает обрастать различными порно-модулями, десятками всплывающих окон при открытии браузера и предложениями принять участие в разнообразных онлайн-лотереях и т. п.

Оценки специалистов показали, то за две недели (среднее время распространения конкретного образца поддельного софта), до 1,8 млн человек успевают скачать дистрибутив программы. От 7 до 12% поддельных программ еще и требуют с пользователя деньги за покупку и около 2% пользователей готовы этот софт купить, говорят в Finjan. Средняя стоимость поддельного антивируса составляет 50 долларов.

Подведя итог, можно сказать, что смысл тратить некоторую сумму на платные антивирусы есть. Можно и даже нужно задаваться вопросом «сколько стоит тот или иной антивирус» перед его покупкой. Чтобы наверняка не ошибиться в выборе, можно воспользоваться тестовой версией — то есть, скачав программу, 30 дней с момента установки пользователь может пользоваться всеми ее функциями абсолютно бесплатно. По

истечению этого срока, для продолжения пользования необходимо приобрести лицензию.

Список литературы:

1. Что такое антивирус? [Электронный ресурс] : (с изм. и доп.) http://ru-best.ru/antivirus.htm (дата обращения 12.11.2012)

2. Какой антивирус лучше? [Электронный ресурс] : (с изм. и доп.) http://www.novogimn-virus.narod.ru/srvnenie.htm (дата обращения 12.11.2012)

3. Антивирусы: как их выбирать? [Электронный ресурс] : (с изм. и доп.) http://virkey.ru/articles/74-selectantivir (дата обращения 12.11.2012)

4. Сравнительный обзор антивирусов. [Электронный ресурс] : (с изм. и доп.) http://habrahabr.ru/post/100763/ (дата обращения 14.11.2012)

5. Осторожно - Поддельные антивирусы - новый тренд мошенников [Электронный ресурс] : (с изм. и доп.) http://forum.mozilla-russia.org/viewtopic.php?id=43821 (дата обращения 14.11.2012)