Антивирусные программы

Саперы ошибаются один раз...

Сфера компьютерных технологий подарила нам вместе с многочисленными благами и удобствами такую неприятную вещь как компьютерные вирусы. Порой на устранение ущерба, нанесенного вредоносными программами, тратится очень много сил и средств, и антивирусные программы тогда уже не кажутся дорогими.

Защищаться или нет?

У пожарных есть поговорка: «Пожар гораздо легче предупредить, чем потушить». Но люди, как правило, не обращают внимания на это мудрое высказывание.

Один из главных выводов, которые мы сделали, — это то, что использование любой более-менее известной антивирусной программы (надежной или не очень, дорогой или бесплатной, русской или иностранной) лучше, чем пренебрежение антивирусной защитой. Вероятность запуска вредоносного кода на компьютере с запущенным антивирусным монитором практически равна нулю.

Цели и условия тестирования

Целью данного тестирования было определение антивируса, наиболее подходящего для защиты персонального компьютера от заражения вредоносными программами.

Так как разработчики антивирусного ПО постоянно обновляют базы для своих продуктов, и количество распознаваемых известными программами вирусов стремится к 100%, мы решили не проводить тестирования по принципу «количество определяемых вирусов». Были использованы лишь несколько наиболее печально известных особей. Отталкиваясь от статистики, мы смоделировали более половины вирусных инцидентов последнего полугодия.

Антивирусы — это утилиты, которые работают с системой на низком уровне, и их надежность и быстродействие в итоге напрямую влияют на надежность и быстродействие компьютера в целом. Исходя из этой закономерности, к антивирусным сканерам и мониторам предъявлялись крайне высокие требования.

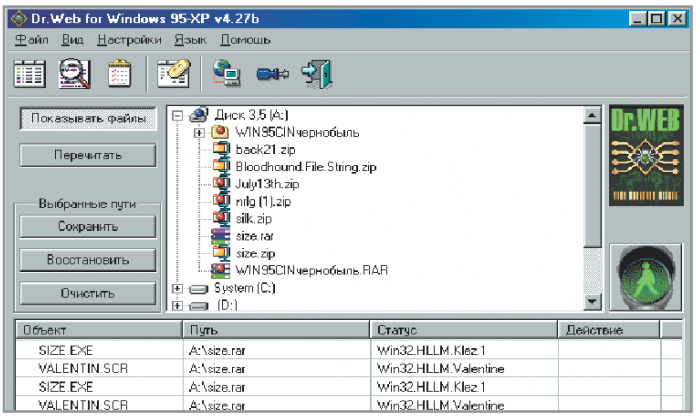
Первые тестировались по ряду параметров при отключенном эвристическом анализе, но при всех включенных опциях, отвечающих за глубину и детальность проверки объектов. Мониторы проверялись на быстродействие и надежность.

Dr.Web 4.27

Начнем обзор с русских программ. Их будет всего две: Dr.Web и «Антивирус Касперского».

Dr.Web — быстрый антивирусный пакет, обеспечивающий надежную защиту ПК. При соответствующей настройке сканер с легкостью находит вирусы в архивных файлах и файлах инсталляции, а монитор безотказно реагирует »


ILOVEYOU.TXT.VBS



◂ **Dr. Web. Комплексная и рационально организованная защита**

» на попытки любого рода работы с зараженными объектами, даже если вы просто копируете RAR-архив, в глубине которого спрятан файл с вредоносным кодом.

Отдельной похвалы достоин монитор SpIDer Guard. В Windows 9x он может реагировать на проявления вирусной активности двумя способами. Первый из них — вывод диалогового окна с описанием обнаруженного вредоносного кода и кнопками, нажимая на которые вы сможете выбрать, что с ним делать: запретить доступ, лечить, переименовать, переместить или удалить. Второй вариант срабатывания — это полная остановка системы. Она произойдет в том случае, если монитор посчитает, что ситуация крайне опасна и необходимо немедленное вмешательство. Пользователю предлагается отреагировать на ситуацию точно так же, как в первом случае, но, так как операционная система полностью обездвижена, сообщение выводится в текстовом режиме.

SpIDer Guard может быть настроен по массе параметров. «Оптимальный» режим работы монитора позволяет достичь наибольшего быстродействия, так как во время работы проверяются лишь те файлы, которые попадают на компьютер при взаимодействии с внешним миром (сетью, дискетами и т. п.). Названия режимов проверки «Запуск и открытие» и «Создание и запись» говорят сами за себя.

Еще один принципиальный момент, о котором следует упомянуть, рассказывая о Dr.Web, — это количество записей в вирусной библиотеке программы. То, что оно почти в два раза меньше, чем у других антивирусов, говорит лишь о том, что компании-разработчики по-разному подходят к учету количества вирусов.

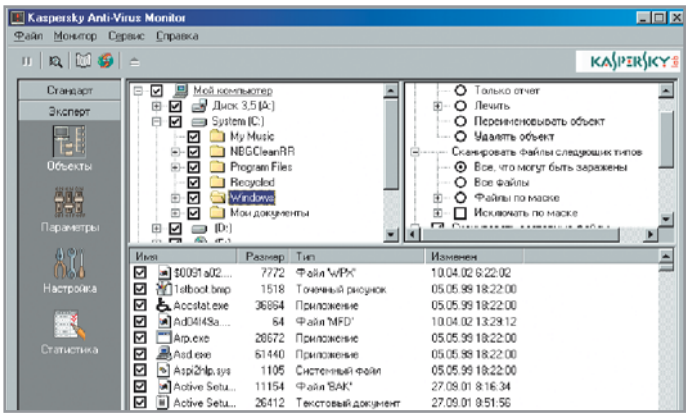
Единственный недостаток Dr.Web — это некоторая неясность в настройке. Забыв сохранить установки, можно пропустить вирус, например, в архиве.

Антивирус Касперского Personal Pro

В отличие от первого «русского», в этом нам не удалось испробовать все функции. Здесь присутствуют несколько возможностей, которые рядовому пользователю могут и не пригодиться: например, модуль Inspector позволяет отслеживать изменения на дисках компьютера и в его реестре. По сравнению с »

	Dr. Web 4.27	Kaspersky Anti-Virus Personal Pro	Panda Antivirus Titanium	McAfee VirusScan 6.0	Norton AntiVirus 2002 8.07.17	Norman Virus Control 5.3
Сайт программы	www.dials.ru	www.kaspersky.ru	www.pandasoftware.com	www.mcafee.ru	www.symantec.ru	www.dbtronix.com.hk
Цена, $	50	69	30 / 20**	49,95 (за загрузку)	49,95 (за загрузку)	60
Язык интерфейса	рус.	рус.	рус.	англ.	рус.	англ.
Условия распространения	shareware	shareware	shareware	shareware	shareware	shareware
Мониторинг						
Размер монитора в ОЗУ	697 Кбайт	6,82 Мбайт	11,08 Мбайт	2,12 Мбайт	15,8 Мбайт	4,79 Мбайт
Скорость сканирования						
HD мин:сек/кол-во файлов	7:20/31914	8:56/31582	7:15/12834*	10:56/11210*	5:26/32788	2:32/8539
CD мин:сек/кол-во файлов	7:32/7377	11:20/15775	4:16/1506*	5:50/1506*	4:42/14128	4:30/11154
Опции сканирования						
Проверка файлов инсталляции	•	•	•	•	–	не все
Проверка архивов	•	•	•	•	• но не RAR	•только ZIP
Эвристический анализ	•	•	•	•	•	•
Проверка входящей/исходящей почты на этапе трафика	–	–	–	–	•	–
Прочее						
Плюсы программы	Есть опция проверки только почтовых файлов, компактный быстрый монитор, DOS-сканер	Есть все мыслимые настройки, возможность удаления зараженных архивов	Простота в использовании, полезная, не требует перезагрузки после установки	Простота в использовании, надежность	Высокая надежность, лечение прямо в ZIP-архиве	Быстрый незаметный монитор
Минусы программы	Настройки: нужно быть внимательным, иначе можно пропустить вирусы, скажем, в архивах	Потребляет много системных ресурсов	Не вызывается из контекстного меню; может завесить машину при работе с крупным архивом	Малое количество настроек	Не находит вирусы в rar-архивах, небольшое количество настроек	Настроек мало, не получилось проверить все файлы (действует по своей маске)
Общая условная оценка	9	9	8	7	6	6

* — Реальное кол-во проверенных объектов в логе не указывается, ** — Цена для читателей CHIP



Антивирус Касперского Personal Pro. Монитор может быть и надежным, и быстрым

» облегченной версией, которую мы регулярно публикуем на Chip CD, в «Pro» просто море настроек и возможностей.

Сканер в тестах показал себя достойно и безошибочно отлавливал вирусы во вложенных архивах, не говоря уже об обычных телах вирусов. В его настройках можно разрешить переименование и удаление инфицированных архивов, этой опции безусловно недостает многим братьям по цеху «Антивируса Касперского».

Монитор может быть детально настроен. Это позволяет обеспечить необходимый уровень защиты и сохранить при этом высокое быстродействие системы. Если настроить монитор на маниакальную проверку всего подряд, то следует приготовиться к тому, что даже 500-мегабайтный архив будет протестирован при обращении к нему. Поэтому к настройкам следует относиться более чем внимательно.

Данный продукт можно порекомендовать опытным пользователям, которые готовы потратить некоторое время на настройку программы. А для тех, кого волнует не только проблема активизации вируса на компьютере, но и просто его нахождение там (например, при подготовке CD-дисков), эта программа — лучший выбор.

AntiVir® Version 6 | VirusBuster

AntiVir Personal Edition v.6	Virus Buster 3.008 bild 4
www.free-av.com	www.virusbuster.hu
free	15
англ.	англ.
freeware	shareware
3,93 Мбайт	6,8 Мбайт
3:50/31663	5:18/6438
4:11/5826	5:18/537
не все	–
•	• но не RAR
•	–
–	–
Быстрая работа, бесплатное распространение	–
Не нашел «W95/CIH.A» в rar-архиве	Неудобный интерфейс
7	5

McAfee VirusScan 6.02

Качественный, надежный и простой в использовании антивирус. При работе с ним создается впечатление, что он очень похож на Norton AntiVirus.

Опытным путем мы установили, что McAfee VirusScan успешно проверяет архивы и файлы инсталляции. Итоговое количество файлов, проверенное на каждом из тестовых носителей, нам установить не удалось, так как в логе программы указывается количество первичных проверенных файлов. Если, исходя из вышесказанного, предположить, что итоговое количество проверяемых файлов аналогично лидерам теста, то можно сказать, что McAfee VirusScan работает быстро.

Настройки в VirusScan есть только те, что являются самыми необходимыми: проверка памяти, boot-секторов, архивов. Естественно, есть файловый фильтр, эвристический анализ и настройка действия при обнаружении вредоносного кода.

Продукт можно порекомендовать не очень опытным или в меру ленивым пользователям.

Norton AntiVirus 2002

Детище корпорации Symantec порадовало нас своей надежностью и высоким уровнем интеграции в Windows. При запуске любого приложения Microsoft Office программа моментально производит проверку макросов открываемого документа. Еще одним плюсом Norton Antivirus можно назвать то, что, в отличие от многих других протестированных программ, она при проверке зараженного ZIP-архива предложила и позволила переместить зараженный файл в карантин.

Стоит отметить, что антивирусный монитор программы нам так и не удалось принудительно выгрузить из памяти компьютера, используя стандартную комбинацию «Ctrl+Alt+Delete». После нескольких попыток удалось лишь избавиться от значка в трее, сама же программа продолжала действовать.

Но все эти существенные плюсы программы уравновешиваются не менее существенными минусами. Первое, на что стоит обратить внимание, — это антивирусный монитор, занимающий в оперативной памяти компьютера более 15 Мбайт. Кроме того, было отмечено небольшое «подтормаживание» системы при открытии документов MS Office и отправке почты. »

McAfee VirusScan. Все предельно просто: нажми на кнопку — получишь результат

Проверка почтовых сообщений

Коза и баян...

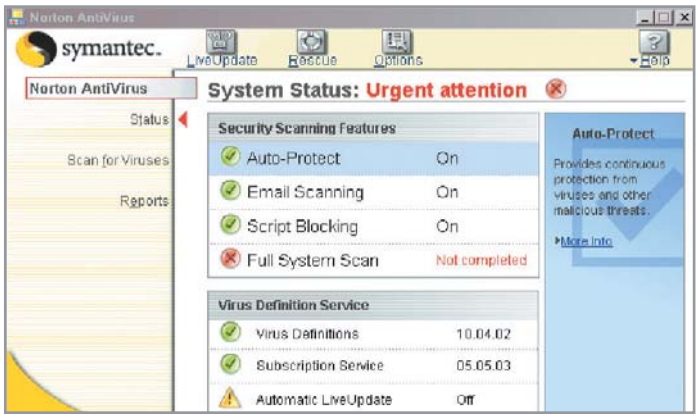
Norton AntiVirus, в отличие от своих конкурентов, может похвастаться такой возможностью, как проверка входящих и исходящих почтовых сообщений до того, как они становятся доступными в почтовом клиенте, или наоборот, перед отправкой на сервер. Но так ли это важно?

Действительно, многие компьютерные вирусы рассылают сами себя по электронной почте, используя почтовую программу, установленную на зараженном компьютере. Физически происходит отсылка писем с вложенными зараженными файлами всем пользователям, занесенным в адресную книгу. Некоторые вирусы не просто отсылают зараженный файл, но и пишут в письме текст, который направлен на то, чтобы заставить доверчивого пользователя запустить прикрепленный к письму файл.

В Symantec решили обезвреживать такие послания раньше, чем они попадут к пользователю. Разработчики наделили свою программу возможностью проверять и лечить или уничтожать подобные письма в то время, когда они представляют собой POP- или SMTP-трафик между сервером и клиентом. Однако на практике этот подход почти не дает выигрыша в безопасности.

Почти все антивирусы включают в себя монитор — резидентную программу, которая не позволит осуществлять какие-либо действия с зараженными файлами (копирование, перемещение, запуск и т. д.). Стало быть, даже если пользователь и получит письмо с приложенным к нему зараженным файлом, то дальнейшие действия с этим объектом будут невозможны, так как монитор пресечет любые попытки сохранить его на диске, скопировать и тем более запустить.

Письмо с прикрепленным к нему RAR-архивом, внутри которого находился зараженный файл, беспрепятственно миновало кордон при включенной проверке архивов и проверке почтовых сообщений. Исходя из этого, мы решили не начислять Norton AntiVirus дополнительных баллов.



Norton AntiVirus 2002. Неумение проверять rar-архивы подмочило репутацию известной программе

Более существенный минус программы мы обнаружили при проверке архивов. Антивирус наотрез отказался работать с RAR–архивами, что при его «раскрученности» выглядит как-то не серьезно. Также нами была отмечена некоторая скудность настроек сканирования.

Все это говорит о том, что Norton AntiVirus создан для не умудренных опытом пользователей: они по незнанию не смогут изменить настройки программы так, чтобы это стало для них роковой ошибкой.

AntiVir Personal Edition

Единственная бесплатная программа в тесте вопреки ожиданиям оказалась очень неплохой. При проверке на скорость сканирования она показала очень приличные результаты. Положительные результаты мы получили и при тестировании архивов: программа справилась как с архивами формата ZIP, так и RAR. AntiVir имеет антивирусный монитор, который очень легко можно выгрузить щелчком правой кнопки мыши по иконке в трее. При обнаружении деятельности известных вирусов AntiVir может как остановить работу системы в целом, так и просто предложить меню: «удалить/лечить/переместить». Кстати, не очень удобным оказалось то, что, выгрузив монитор, его можно загрузить снова только после перезагрузки компьютера.

В основном эта программа ничем не уступает своим платным собратьям и также достойно может стоять на страже компьютера. AntiVir регулярно обновляется, правда, при обновлении приходится скачивать новый файл установки (около 3,5 Мбайт), что не очень удобно для владельцев модемов. Но возмущения по этому поводу неуместны, так как программа бесплатна, и за обновления тоже платить не придется.

Несмотря на умение проверять архивные файлы, программа не смогла обнаружить в RAR-архиве вирус «W95/CIH.A» (Чернобыль). Хотя при попытке распаковать архив вирус был обнаружен, не очень приятно знать, что этот старый, но опасный вредитель может спокойно лежать в архиве на винчестере.

Несмотря на эту небольшую ложку дегтя, впечатление от программы благоприятное. Она очень быстро прошла тест на скорость проверки и обошла многих маститых конкурентов.

Virus Buster

Разработчики этой программы, по всей видимости, забыли, что одним из критериев выбора программы для пользователя является удобство ее интерфейса. Интерфейс у программы очень неудобный, и с первого раза трудно установить необходимые настройки. В минус программе можно записать и то, что при запуске зараженного файла не происходит полной остановки всей системы. Также создается впечатление, что при проверке жесткого диска программа, несмотря на установки, производит тестирование по своим критериям, так как при включенной опции «Test all files» она протестировала в три раза меньше файлов, чем остальные программы. Программа не может похвастаться наличием эвристического анализа и возможностью проверки RAR-архивов. Запуск Virus Buster недоступен из контекстного меню Windows, и проверять папки приходится из проводника программы. Virus Buster предлагает несколько опций для настройки интерфейса.

Panda Antivirus Titanium

Эта программа является, пожалуй, самым удобным антивирусным пакетом для домашнего использования. В Panda Antivirus Titanium нет никаких лишних настроек сканирова-

» ния, только самые элементарные. Пользователю остается только выбирать, что ему необходимо тестировать: жесткие диски, исключительно почтовые файлы или же произвести полную проверку системы. Panda прекрасно работает как с ZIP-, так и с RAR-архивами. Порадовало и то, что программа очень качественно переведена на русский язык, причем локализован не только интерфейс программы, но и ее справочная система.

Однако в Panda Antivirus Titanium есть и несколько недостатков. К примеру, отсутствует возможность быстрого запуска программы из контекстного меню Windows.

Как и в случае с McAfee, нам не удалось узнать точное число проверенных на тестовом носителе файлов, так как программа при проверке всех составных частей архива в своем отчете указывает, что был проверен только один файл — сам архив. Впрочем, своеобразное ведение статистики недостатком не является.

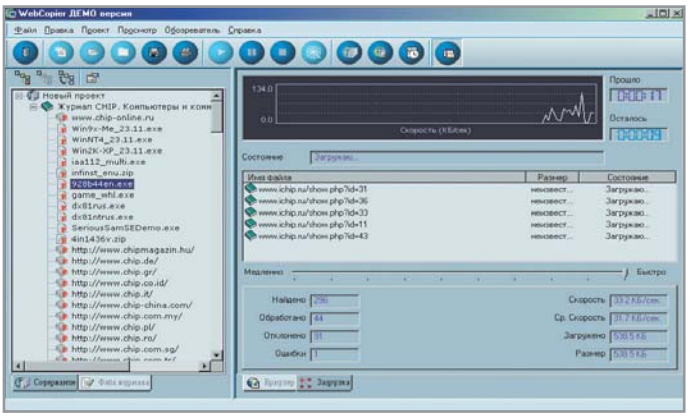
Интересная особенность программы обнаружилась при попытке произвести проверку почтовых файлов. При проверке Panda несколько раз зависала на обеих тестовых машинах. Оказалось, чтобы исправить это недоразумение, необходимо хотя бы раз после установки MS Office запустить MS Outlook и произвести его минимальную настройку. Но это вовсе не означает, что вам придется отказаться от своего почтового клиента (в нашем случае это был Outlook Express).

В целом, Panda Antivirus Titanium предоставляет высокий уровень защиты компьютера от вирусов в сочетании с простотой интерфейса и надежностью. Ее также можно порекомендовать как оптимальное сочетание цены и качества.

Norman Virus Control

При тестировании этой программы нам так и не удалось проверить все файлы тестируемого диска, так как программа даже при включенной опции «Test all files» проверила слишком мало файлов. Norman справилась с тестированием ZIP-архива, но с архивом RAR работать напрочь отказалась. В программе есть контрольный центр, наподобие «Антивируса Касперского», но, в отличие от русского конкурента, программа не предложила нам и десятой части его настроек.

Программа не обладает какими-либо уникальными возможностями и, будучи «серой мышкой», теряется среди своих коллег.



◂ **AntiVir Personal Edition.** Бесплатная программа достойно конкурирует с коммерческими

Наши рекомендации

Получилось так, что победителей нашего теста целых три, так как обделить вниманием любой из этих замечательных продуктов было бы несправедливо.

Итак, «Антивирус Касперского» с его богатыми возможностями мы рекомендуем использовать очень опытным пользователям, которые не пасуют перед многочисленными настройками и хотят сами контролировать обеспечение безопасности своей рабочей станции.

Dr.Web, оказавшийся на высшей ступени пьедестала почета, подойдет менее искушенному пользователю и может использоваться как на работе, так и дома.

И третий призер — Panda Titanium — просто идеально вписывается в рамки домашнего антивируса. Обладая минимумом настроек и мощной системой анализа и сканирования, программа подойдет для самых неискушенных пользователей.

Заключение

Подводя итоги, остается лишь добавить, что, какими бы антивирусными программами вы не пользовались, не следует пренебрегать элементарными правилами компьютерной безопасности. С подозрением стоит относиться даже к тем файлам, которые вам якобы прислали друзья. По причине того, что вирусы сами рассылают себя по почте, эта предосторожность будет отнюдь не лишней. Помните, что основной защитой вашего компьютера является ваш здравый смысл.

Более подробную информацию о тестировании и полную таблицу с результатами теста вы можете найти на нашем CD.

■ ■ ■ Дмитрий Асауленко, Павел Шошин

Проверка архивов

ZIP и RAR

Антивирусные программы могут проверять большое количество архивных файлов, то есть при сканировании происходит проверка как самого архивного файла, так и всех файлов внутри него. Некоторые программы, принявшие участие в тесте, не смогли проверить RAR-архив, внутри которого находился зараженный файл. Поскольку архиватор RAR на сегодняшний день является очень популярным, то неумение обнаруживать вредоносные программы в архивах его формата является абсолютно неприемлемой чертой для антивирусов. Да, вирус, упакованный в архив, не сможет сам активизироваться, но такой архив можно по ошибке отправить по почте или случайно попытаться распаковать при выключенном антивирусном мониторе.

Еще одна неприятная особенность заключается в том, что, проверив RAR-архив, большинство антивирусных программ просто информируют о том, что файл является инфицированным, и не предпринимают никаких действий по его излечению или удалению (исключением является «Антивирус Касперского», в нем предусмотрена возможность переименования или удаления зараженного архива).

Некоторые вирусы используют эту особенность: KLEZ, например, маскирует свои исполняемые файлы под архивы RAR, присваивая им соответствующие расширения. Для неопытного пользователя, принявшего такой файл за настоящий архив с файлами внутри, работа с ним может закончиться плачевно.