Безмалый В.Ф.
vb@upc.ua
Безмалая Е.В.
ellen@pochna.ws

Антивирусное программное обеспечение. Исследование эффективности

Проблему вирусов сложно назвать новой. Каждые 30 минут в мире появляется, по крайней мере, один новый вирус или новая разновидность существующего. К счастью, далеко не все они могут вызвать эпидемию. Пользователям компьютеров на помощь приходит специализированное программное обеспечение, призванное бороться с компьютерной инфекцией - антивирусы.

Существует огромное количество производителей такого программного обеспечения и предложений на рынке антивирусов. Зачастую пользователю не просто выбрать, что же ему действительно нужно, что отвечает всем его требованиям и не подведёт в повседневном использовании. Мы решили разобраться в эффективности такого ПО и исследовали всего лишь четыре антивирусных комплекса от различных производителей из всего многообразия (Symantec Antivirus Corporate Edition 8.1, Kaspersky Antivirus, Ukrainian National Antivirus, Dr Web).

Целью данного исследования являлось определение скорости проверки файлов на наличие вирусной инфекции (а, следовательно, и комфортности работы с ПК при использовании данного антивируса) и эффективности проверки файлов на вирусы.

Тестирование каждого из антивирусов проводилось в 4 этапа: 2 теста на быстродействие и 2 на качество детектирования вирусов.

Цель тестов по быстродействию заключалась в измерении скорости работы антивирусного ядра каждого из продуктов в двух режимах: настройки по умолчанию и максимальные настройки работы. Именно от скорости работы антивирусного ядра (а по-простому - скорости проверки одного файла) будет зависеть быстродействие каждого из модулей.

Конечно, читатель может оспорить это утверждение - мол, у какого-то из антивирусов могут быть свои Ноу-Хау в проверке файлов на лету, благодаря чему этот антивирус будет работать быстрее даже при более медленном ядре. Но практика показывает, что это связано исключительно с настройками модулей (в данном примере «Резидентных мониторов»). Если же вы зададите одинаковые параметры работы каждого из них, то разница в быстродействии будет примерно такой же, как и разница в быстродействии сканеров. А все остальные новшества, технологии проверки … сегодня они есть только у одного продукта, а завтра будут у всех, ведь разработчики антивирусов стараются не отстать друг от друга, а вот технологии работы самого антивирусного ядра, как правило, изменяются редко.

Для тестирования антивирусов на качество детектирования вирусов было собрано две группы файлов: первая группа – ITW вирусы[1], вторая группа – сборная вирусная коллекция как новых, так и старых вирусов.

[1] ITW-вирусами называются те вирусы, которые встречались в «диком виде» (то есть у реальных пользователей, а не в лабораторных условиях или в коллекциях вирусологов).

Тесты на быстродействие

Для этой цели был использован компьютер AMD K6-2/350 с установленной ОС Windows 98. Объем оперативной памяти – 128 Mb. Выбор такого слабого компьютера обусловлен следующим: как правило, в современных вычислительных системах порог быстродействия антивируса ограничивает не загрузка процессора, а скорость работы дисковой подсистемы (то есть какой объём данных система успеет предоставить антивирусу на проверку в единицу времени). Процессор же, как правило, загружен на 50-70%. Таким образом, сложно проводить сравнительный тест на быстродействие, так как разрыв будет составлять всего несколько процентов, в том время как дискомфорт работы в такой системе (во время работы антивируса) измерить цифрами практически не возможно (разве что отслеживать график загруженности процессора при работе того или иного антивируса). На медленной же системе процессор практически всегда будет загружен на 100% и разница в скорости работы антивирусов будет выражаться во времени выполнения задания. Далее дело техники: заставляем антивирусы при одинаковых настройках проверить одну и ту же папку, засекаем время и сравниваем.

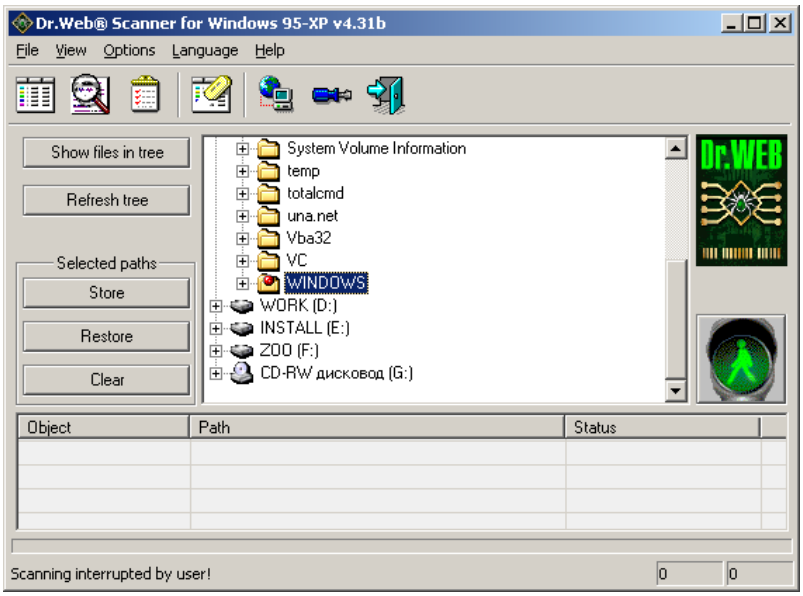
Перед началом тестирования все антивирусы были приведены в актуальное состояние (обновлены через Интернет). В ходе тестов проверялся каталог Windows операционной системы Windows 98 SE RUS. Тестирование проводилось на этой же системе.

Первый тест – проверка каталога с настройками, которые установлены в сканере по умолчанию. В ходе проверки для каждого из антивирусов получены следующие результаты.

DrWeb 4.31b

Настройки по умолчанию: сканер тестирует файлы "по формату", архивы, почтовые базы, упакованные файлы и SFX-архивы. Эвристический анализатор настроен на максимальный уровень проверки.

Результаты проверки:

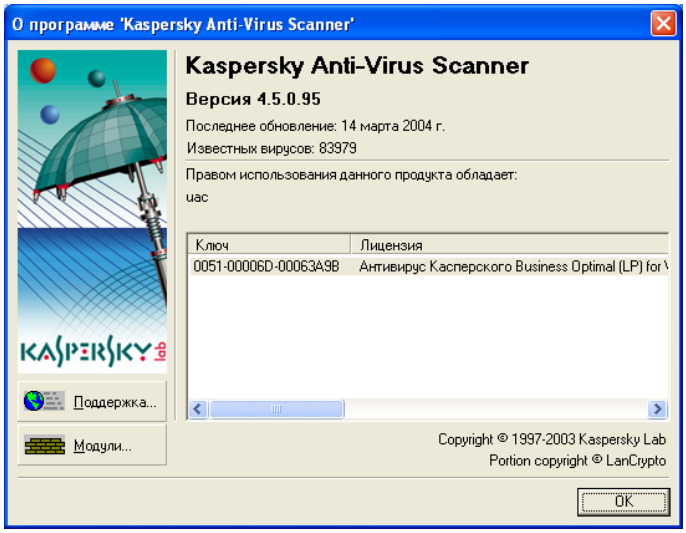


Время	06:20
Количество проверенных объектов	6607 (включая архивы, количество архивов антивирус не выдает).
Скорость тестирования	17,39 файлов в секунду

Kaspersky AntiVirus (KAV 4.5.0.95)

Настройки по умолчанию: сканер тестирует все файлы и проверяет архивы, почтовые базы, вложенные объекты и SFX.

Результаты проверки:

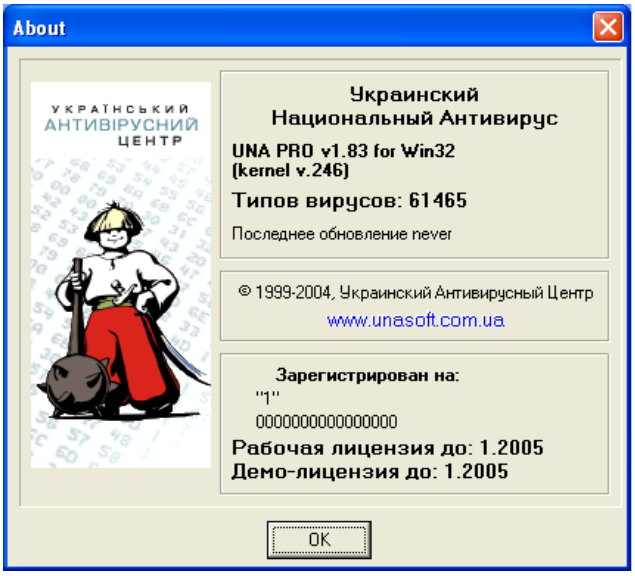


Время	11:33
Количество проверенных объектов	11962[2] (включая 218 архивов)
Скорость тестирования	17,26 файлов в секунду

Ukrainian National Antivirus (UNA 1.83 kernel 246)

Настройки по умолчанию: сканер тестирует "расширенный набор" файлов и проверяет архивы. Эвристический анализатор отключен.

Результаты проверки:



Время	04:41
Количество проверенных объектов	5729 (включая 17 архивов)
Скорость тестирования	20,61 файлов в секунду

Symantec Antivirus Corporate Edition 8.1 (SAV)

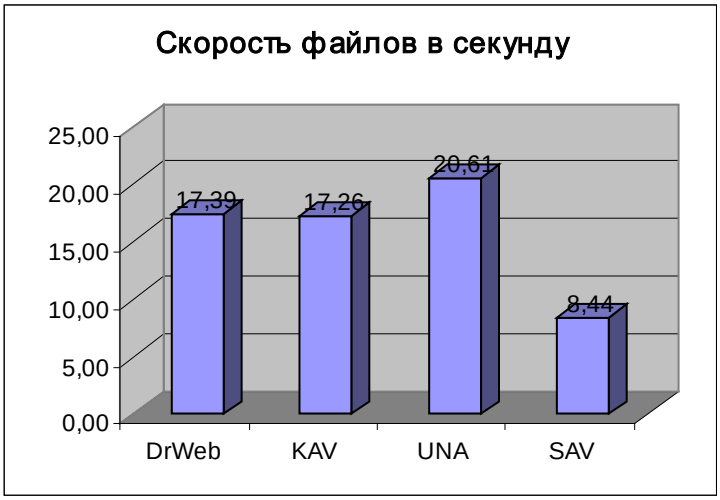
[2] Количество файлов в каталоге разное, т.к. различные антивирусы по умолчанию тестируют архивы различной вложенности.

Настройки по умолчанию: сканер тестирует все файлы и проверяет архивы вложением до 3-х.

Результаты проверки:

Время	15:07
Количество проверенных объектов	7651
Скорость тестирования	8,44 файла в секунду

Итоговая диаграмма:



Сводная таблица тестирование на быстродействие при настройках по умолчанию:

Наименование антивируса	**Скорость тестирования (файлов в секунду)**	**Всего проверено файлов**	**Затраченное время, секунд**
DrWeb	17,39	6607	380
KAV	17,26	11962	693
UNA	20,61	5792	281
SAV	8,44	7651	907

Второй тест – проверка каталога с максимальными настройками, но при отключенной проверке архивов. Для тестирования использовалась та же система, что и для предыдущего теста (K6 2 – 350, Windows98 SE).

Dr Web 4.31b

Настройки: проверяемые объекты - все файлы, тестирование архивов и почтовых баз отключено, эвристика включена на максимум.

Результаты проверки:

Время	04:24
всего объектов	3168
скорость тестирования	12,00 файлов в секунду

KASPERSKY ANTIVIRUS (KAV 4.5.0.95)

Настройки: проверяемые объекты - все файлы, тестирование архивов и почтовых баз отключено, эвристика включена на максимум.

Результаты проверки:

Время	05:30
кол-во объектов	3201 (включая 4 архива)
скорость тестирования	9,70 файлов в секунду

UKRAINIAN NATIONAL ANTIVIRUS (UNA 1.83 KERNEL 246)

Настройки: проверяемые объекты - все файлы, тестирование архивов и почтовых баз отключено, эвристика включена на максимум.

Результаты проверки:

время	08:44
кол-во объектов	3126
скорость тестирования	5,97 файлов в секунду

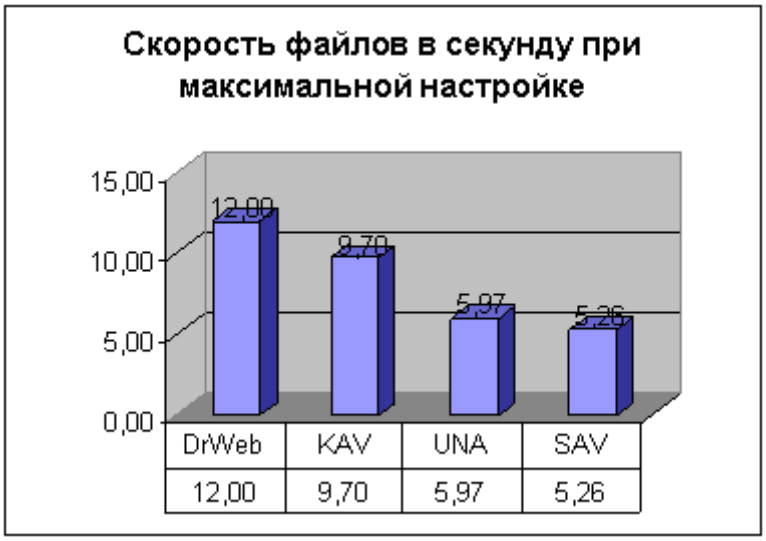
SYMANTEC ANTIVIRUS CORPORATE EDITION 8.1 (SAV)

Настройки: проверяемые объекты - все файлы, тестирование архивов и почтовых баз отключено, эвристика включена на максимум.

Результаты проверки:

время	09:55
кол-во объектов	3128
скорость тестирования	5,26 файлов в секунду

Итоговая диаграмма:



Сводная таблица тестирования антивирусов на быстродействие при максимальных настройках:

Наименование антивируса	**Скорость тестирования (файлов в**	**Всего проверено файлов**	**Затраченное время, секунд**

	секунду)		
DrWeb	12,00	3168	264
KAV	9,70	3201	330
UNA	5,97	3126	524
SAV	5,26	3128	595

Проверка на детектирование ITW вирусов.

Для проведения этого теста было отобрано 593 вируса[3], которые были зафиксированы в диком виде в течение последних 2-х месяцев.

Этот тест был проведен на компьютере Pentium IV – 1800 256 Mb RAM с установленной операционной системой Windows XP SP1 RUS. При проведении данного теста основной задачей антивирусов было детектирование максимального количества вирусов, в связи с этим все сканеры были настроены на максимальный уровень проверки.

Методика проведения теста.

Тест осуществляется следующим образом:

1. На «чистую» (настроенную систему, в которой отсутствуют антивирусные продукты) устанавливается тестируемый антивирусный продукт, антивирусные базы продукта доводятся до актуального состояния;
2. Запускается сканер с интерфейсом GUI (если есть несколько вариантов интерфейса, запускается профессиональный вариант) и его настройки устанавливаются в состояние максимального качества детектирования (на максимум включаются все модули эвристического сканирования, подключаются все базы);
3. В качестве объекта тестирования вбирается, содержащая коллекцию вирусов в виде набора инфицированных файлов, собранную для тестирования продуктов;
4. Запускается сканирование в режиме создания отчёта с записью в log-файл (без выполнения действий над инфицированными файлами);
5. По окончании выполнения тестирования полученный отчёт о тестировании сохраняется и снимаются окончательные результаты работы: количество проверенных объектов, количество обнаруженных инфицированных файлов, количество обнаруженных «подозрительных» файлов.
6. Далее система восстанавливается к состоянию до выполнения пункта 1. и начинается тестирование следующего антивирусного продукта.

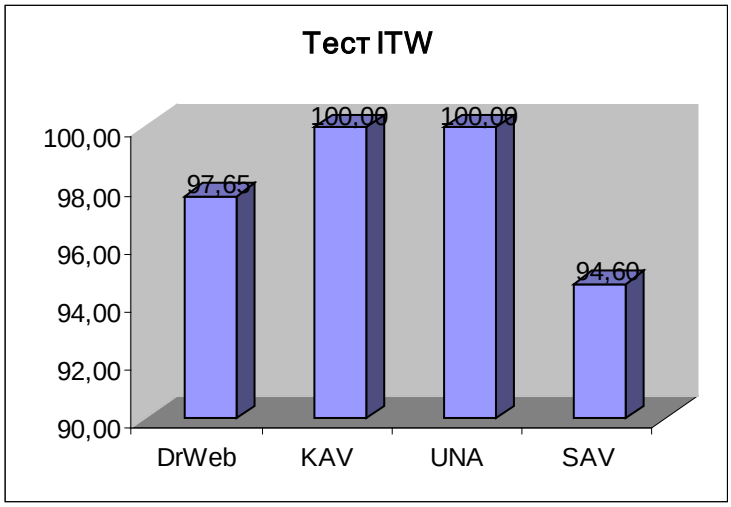
Результаты тестирования приведены в сводной таблице:

Антивирус	% обнаружения	Проверено	Тел вирусов	Подозрительных файлов

[3] за основу брался список, приведенный на сайте WildList.com и используемый при тестировании английским журналом Virus Bulletin. Из него были вычеркнуты вирусы, которые не встречались на территории СНГ за последние 2 месяца и добавлены те вирусы/трояны, которые не фигурируют в VB-списке, но тем не менее зафиксировано их неоднократное появление у конечных пользователей на территории СНГ).

DrWeb	**97,65**	596	582	1
KAV	**100,00**	593	593	
UNA	**100,00**	593	593	
SAV	**94,60**	593	561	

Итоговая диаграмма



Таким образом, антивирусные программы DrWeb 4.31b и SYMANTEC ANTIVIRUS CORPORATE EDITION 8.1 (SAV), к сожалению, показали недостаточный уровень детектирования ITW вирусов.

Тест на развернутой коллекции вирусов

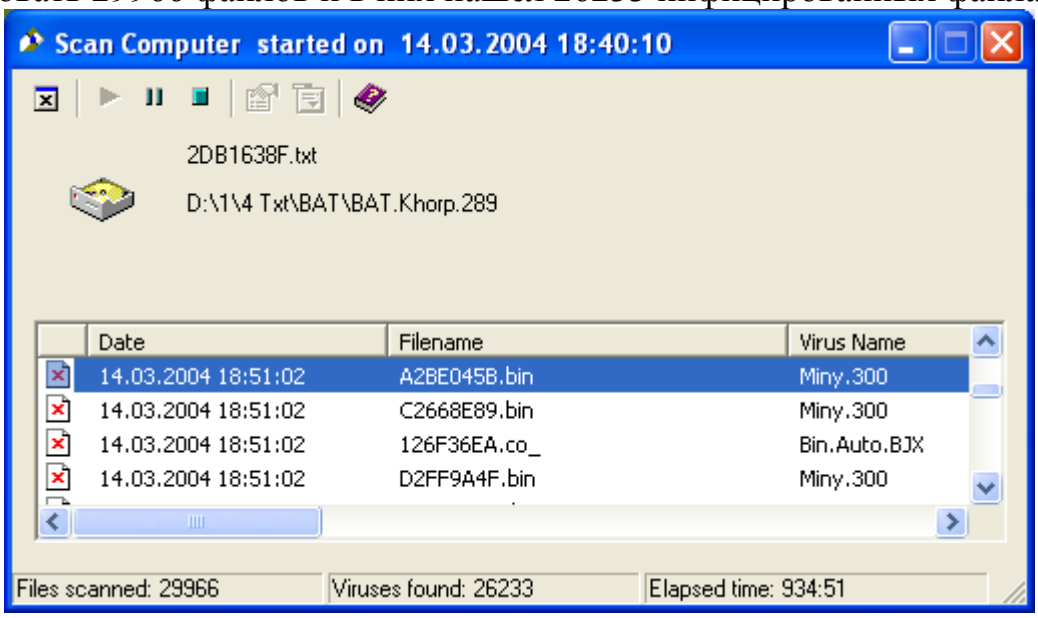
Этот тест был проведен на той же системе, что и ITW-тест (Pentium IV – 1800 256RAM ОС Windows XP). Для тестирования использовался расширенный набор вирусов. Размер коллекции составлял около 2.5 Gb и насчитывал более 30 тысяч инфицированных файлов. Как и в предыдущем тесте, главной задачей антивирусов было детектирования максимального количества инфицированных файлов.

Результаты тестирования приведены в сводной таблице:

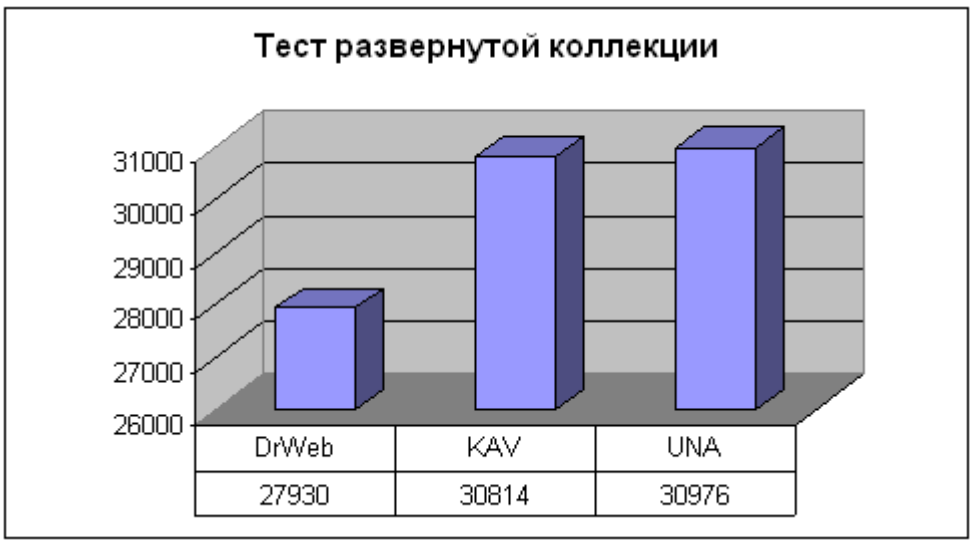
Наименование антивируса	**Обнаружено тел вирусов**	**Обнаружено модификаций вирусов**	**Обнаружено подозрительных файлов**	**Всего файлов проверено**
DrWeb	27930	472	720	31372
KAV	30814	7	18	31262
UNA	30976		62	31206
SAV	**Тест не пройден**			

С SYMANTEC ANTIVIRUS CORPORATE EDITION 8.1 (SAV) получилось следующее: антивирусу, как и всем остальным его конкурентам, было дано задание протестировать папку, содержащую файлы с вирусами, в режиме «только отчёт». В то время как остальным антивирусам для этого потребовалось около 30 минут (DrWeb - 30:05, KAV - 30:12, UNA - 25:14) Symantec Antivirus затратил на эту операцию 934 минуты (!) и при этом тестирование ещё не было завершено. У нас попросту закончилось терпение, и мы так и не дождались окончательных

результатов. К тому моменту, как Symantec Antivirus был остановлен, он успел протестировать 29966 файлов и в них нашёл 26233 инфицированных файла.



Итоговая диаграмма:



Мы предоставляем вам самим сделать вывод, о том, каким антивирусом вам будет пользоваться удобнее.