Таблица 1

N п/п	Антивирусная программа	Эффективность обнаружения вирусов, %, на тесте				Средний показатель, %
		ItW Overall	Standard	Polymorphic	Macro	
1	Sophos SWEEP	100	99,7	100	100	99,93
2	Dr Solomon's AVTK	100	100	98,4	98,9	99,33
3	DialogueScience DrWeb	97,2	97,8	100	99,5	99,63
4	ESaSS ThunderBYTE	100	97,8	93,5	97,8	97,28
5	IBM Antivirus	100	99,7	92,3	96,2	97,05
6	McAfee VirusScan	99,7	98,0	90,1	99,5	96,83
7	Alwil AVAST!	99,6	100	88,5	95,8	95,98
8	KAMI AVP	99,8	94,4	95,2	90,3	94,93
9	Norman Virus Control	100	92,2	87,4	99,1	94,68
10	EliaShim ViruSafe	97,9	100	88,5	84,7	92,78
11	Cybec VET	88,2	88,9	95,1	97,3	92,38
12	Iris AntiVirus	99,8	99,0	86,4	82,7	91,98
13	Cheyenne InnocuLAN	98,3	99,3	86,4	82,2	91,55
14	Symantec Norton AntiVirus	99,8	84,4	83,6	94,3	90,53

Категории тестов: ItW Overall - вирусы, встречающиеся в реальной жизни (In the Wild); Standard - стандартные вирусы; Polymorphic - полиморфные вирусы; Macro - макровирусы.

программа KAMI AVP обеспечивает лучшие результаты, а в общем зачете при тестировании на общей коллекции вирусов заняла первое место.

Что ж, больше антивирусов, хороших и разных!

УРОКИ ДОКТОРА ВЕБА

Итак, история антивируса Doctor Web началась на заре 90-х годов в Санкт-Петербурге, когда мало кому известный инженер И. Данилов начал трудиться на одном из предприятий ВПК. Работа была связана с компьютерами, а в них периодически появлялись вирусы. Антивирусных программ было немало и в те времена (вспомним хотя бы общеизвестный Aidstest Д. Н. Лозинского), но работали они обычно по сигнатурам, отыскивая уже известные коды известных вирусов. Антивирус всегда появлялся после вируса. Возникла идея: а почему бы не попробовать создать такой анализатор, который, наблюдая за развитием событий в компьютере, определял бы, обычные они или это проявление вирусной активности? Затем следовало установить контроль за жизненно важными объектами операционной системы и BIOS компьютера, не давая вирусам размножаться и уничтожать информацию. Разумеется, антивирус не должен чураться и традиционных методов поиска и уничтожения вирусов.

Эти в общем-то не революционные идеи и легли в основу того, что было воплощено в антивирусной системе Spider's Web. Надо сказать, что первая публикация о ней и ее авторе появилась именно в журнале "Радио". Новый антивирус ждала приятная неожиданность — с самого рождения он был очень хорошо принят на международной арене. Уже в 1993 г. Spider's Web стал финалистом конкурса Software Europe "Golden Softies" на выставке CeBIT' 1993, а в дальнейшем регулярно побеждал в различных категориях тестов. Хобби И. Данилова стало профессией. Сама система Spider's Web также из разряда любительских перешла в профессиональные. Не все ее компоненты развивались одинаково, сегодня, по существу, остался только один — Doctor Web, созданный в 1993—1994 гг. (коммерческое распространение начато летом 1994 г.).

Нынешний Doctor Web — программа нового поколения. Он способен находить как "старые", давно известные вирусы, так и появившиеся относительно недавно вирусы-мутанты. Мощный эвристический анализатор позволяет успешно обнаруживать новые, еще не известные вирусы. Программа успешно работает с большинством архивов.

Нам показалось, что именно в наступившем году можно отметить пятилетний юбилей Doctor Web. Это и послужило поводом для нашей беседы с И. Даниловым, изложение которой приводим ниже.

Прежде всего о юбилее. Действительно, первый вариант программы Doctor Web появился в 1993 г. Однако это был не тот антивирус, который сегодня знают во всем мире. Нынешняя версия радикально отличается от первой и по алгоритмам, и по режимам работы, и по способам нахождения вирусов. Название было сохранено, так как оно уже было известно, а вот программа обновилась очень сильно. Поэтому официальной датой рождения пакета Doctor Web следует считать 18 марта 1994 г., стало быть, пятилетний юбилей коммерческого продукта отпразднуем в следующем году.

Быстрый рост популярности антивируса Doctor Web в нашей стране и за рубежом объясняется тем, что он одним из первых стал бороться с полиморфными зашифрованными вирусами, в коде которых нет ни одного постоянного участка. Кроме того, у этой программы имеется эффективный эвристический анализатор, который позволяет искать не только уже известные, но и неизвестные вирусы (он анализирует код программы на наличие характерных для них последовательностей команд). Эффективность определения новых вирусов составляет примерно 80 %. Этот режим работы программы Doctor Web является новаторским и мало у кого он есть. Громадное число антивирусных программ, использующих эвристический подход и разработанных значительно позже, вторично — в их основе лежит именно этот режим Doctor Web.

К сожалению, и сама программа Doctor Web, и алгоритмы ее работы до сих пор не запатентованы. По действующему законодательству в области авторского права программирование почему-то приравнено к писательскому труду, что отнюдь не облегчает патентование. А пока что находятся фирмы, которые расшифровывают алгоритмы работы, заимствуют их и даже готовые подпрограммы. Такие "последователи" есть и у нас в стране, и за рубежом.

Doctor Web постоянно развивается, "обзаводится" новыми режимами работы. Например, когда появились полиморфные вирусы, Doctor Web "научился" распознавать и удалять их в файлах, а на нашествие макровирусов отреагировал введением режима обнаружения и удаления их в документах. Уже создана сетевая бета-версия Dr. Web for Novell Netware. Сейчас большие усилия направлены на разработку 32-разрядных версий антивируса для Windows 95, Windows NT, OS/2, к лету текущего года они должны появиться на рынке.

Сегодня главная задача — как можно полнее и лучше удовлетворять запросы пользователей Doctor Web, число которых непрерывно растет, стараться в своих разработках предугадать появление новых, пока неизвестных вирусов, предусмотреть средства их обезвреживания.

Таблица 2

Антивирусная программа	Эффективность обнаружения вирусов, %, на тесте					
	ItW Boot	ItW File	ItW Overall	Standard	Polymorphic	Macro
Alwil AVAST!	100	95,9	97,3	98,8	100	97,7
Command F-PROT PRO	100	88,6	92,5	92,2	50,8	95,9
Cybec VET	100	66,1	77,6	98,4	99,0	98,5
Data Fellows FSAV	100	100	100	100	97,6	100
DialogueScience DrWeb	97,8	99,2	98,8	98,1	100	100
Dr Solomon's AVTK	100	100	100	100	100	100
Eliashim ViruSafe	96,7	98,9	98,1	99,4	97,9	97,9
ESET NOD-iCE	100	98,5	99,0	99,7	100	98,3
Grisoft AVG	94,5	86,2	89,0	78,4	81,0	88,2
IBM AntiVirus	100	100	100	100	96,2	100
iRiS AntiVirus	98,9	98,8	98,8	99,3	91,9	94,5
KAMI AVP	100	100	100	100	97,6	100
McAfee VirusScan	100	100	100	98,8	93,1	100
Norman ThunderByte	100	100	100	98,5	100	99,6
Norman Virus Control	100	100	100	99,4	100	99,5
Sophos SWEEP	100	100	100	99,7	100	100
Symantec Norton AntiVirus	100	99,4	99,6	97,0	87,5	99,9
Trend Micro PC-cillin	92,3	97,6	95,8	97,4	93,6	91,3

Категории тестов: ItW Overall - вирусы, встречающиеся в жизни (In the Wild); ItW Boot - загрузочные; ItW File - файловые; Standard - стандартные вирусы; Polymorphic - полиморфные вирусы; Macro - макровирусы.