А.М.ТЕРЕНТЬЕВ

Антивирусная защита ПК в Windows 95/98/NT

Справочное пособие
по антивирусным средствам
ЗАО "ДиалогНаука"

2-е издание

"Перспектива"
Москва 2000

ББК **32.973.26 — 018.2**
Т35
УДК **681.3.067**

Терентьев А.М.
Антивирусная защита ПК в Windows 95/98/NT: Справочное пособие по антивирусным средствам ЗАО “ДиалогНаука”. 2-е издание. — М.: Перспектива — М, 2000. — 104 с.: ил.

Книга содержит подробное описание набора основных 32-битных антивирусных средств “ДиалогНауки” (Doctor Web, ADinf и SpIDer Guard), предназначенных для использования в средах Windows. Приводятся полные схемы управления компонентами, рекомендации по их установке и настройке в соответствии с мощностью компьютера и нуждами пользователя.

Книга является справочным пособием по работе с антивирусными средствами “ДиалогНауки” для Windows и предназначена для конечных пользователей-неспециалистов, владеющих работой в среде Windows.

Текущая сопроводительная документация к версиям компонентов может иметь усовершенствования описанных возможностей.

ISBN 5-86225-490-0

При подготовке книги использована сопроводительная документация в печатном и электронном виде и другие материалы, предоставленные автору ЗАО “ДиалогНаука”.

Предисловие

Данная книга представляет собой справочное пособие по работе с антивирусными программами ЗАО "ДиалогНаука", написанное на основании опыта их использования в большом коллективе пользователей с самым различным уровнем компьютерной грамотности. Все аспекты использования программ были исследованы автором со свойственной ему дотошностью.

К сожалению, в данное издание не вошли описания программ, работающих в среде, отличной от Windows 9x/NT, – DrWeb для Novell Netware, ADinf16, ADinf Cure Module. Будем надеяться, что в дальнейшем появятся новые книги, посвященные и этим вопросам. Тем более, что и описанные программы быстро развиваются, что потребует исправлять их описания, да и новые программы на подходе.

Книга, безусловно, окажется полезной всем, кто хочет получить достаточно полную информацию о наших продуктах, и особенно об их новых "тонких" возможностях, сэкономить свое время при их установке и настройке.

Д.Н.Лозинский

СОДЕРЖАНИЕ

I. Введение

Бурное развитие программного обеспечения персональных компьютеров (ПК) неизбежно сопровождается не менее интенсивным созданием и развитием вредоносных программ, и в первую очередь компьютерных вирусов. Создание новых и совершенствование старых операционных систем (ОС), в особенности Windows-ветви (’95, ’OSR2, ’98, ’NT и ’2000), неминуемо расширяет сферу действия вирусов. Аналогично, прогресс технологий компьютерного “железа”, особенно интенсивное внедрение flash-ROM как носителей BIOS, в том числе его расширений в видеокартах, и аналогичных блоков в модемах создает особую опасность атаки вредоносных элементов в виде труднообратимой порчи оборудования компьютера.

Ситуация усугубляется тем, что ПК как современное средство вычислительной техники изначально ориентирован на эксплуатацию одним постоянным пользователем. В то же время зачастую реально один “персональный” компьютер и его “рабочий стол” использует дюжина персон... Если учесть, что квалификация “среднего” пользователя ПК далека от необходимой для выдержанности технологии исполняемых работ, станет понятно, что разрыв между все увеличивающейся сложностью и громоздкостью программных компонентов и снижающимся уровнем профессиональных знаний среднего пользователя ПК дает основу распространения вредоносных программ.

В сфере деловых приложений быстрейший рост имеют текстовые документы в форматах Word for Windows (Winword) и сообщения электронной почты (E-Mail). Понятно, что основные атаки вредоносных программ сориентированы на оба этих направления.

В описанных условиях возрастает актуальность защиты ПК от вредоносных воздействий. В этой масштабной и многоплановой задаче, среди прочего, особо важно построение эффективной защиты против компьютерных вирусов и смежных с ними вредоносных программ (“червей”, “троянцев” и др.). Динамичность задачи понятна: при десятках тысяч существующих компьютерных вирусов еженедельно добавляется около 100 новых.

Среди всех зарубежных и отечественных антивирусных средств мой интерес давно привлекает продукция “ДиалогНауки”. Именно этот творческий коллектив выделяется, на мой взгляд, целостностью подхода к решению указанных выше проблем, быстрой реакцией на изменение вирусной обстановки и, что особенно важно, акцентом на

выпуск программной продукции, предназначенной в первую очередь для решения актуальных отечественных проблем.

Отдавая себе отчет в многочисленных погрешностях и недостатках таких ОС, как Windows'95, автор в то же время вынужден констатировать, что значительный объем реальной работы пользователя в настоящее время исполняется в ОС этого клана. Подросло поколение "юных техников", которые вообще не знают о том, как работать в MS-DOS. Поэтому, при подготовке данной работы основной упор сделан на рассмотрении 32-битных антивирусных средств "ДиалогНауки", предназначенных для сред Windows '95/OSR2/98/NT. Текст рассчитан на непрофессионала, имеющего достаточные навыки работы с ПК в Windows и знание ее основных терминов и операций.

В книге применен ряд обычных соглашений. Впервые упоминаемые термины и сокращения подчеркнуты; их алфавитный список размещен со с.100. Курсив применен при переводе технических терминов и для акцентации смысла. Названия клавиш заключены в угловые скобки. Полужирным шрифтом выделены названия вирусов, дисков, процедур и иные конкретные оригинальные обозначения. Полужирным курсивом даны наименования пунктов меню или опций. Неочевидные для неспециалистов, но критически важные при практической работе сведения, акцентированы обрамлением абзацев.

По замыслу автора, материал данной работы предназначен как практическое руководство при освоении описываемых программ. Требования объема не позволили подразделить информацию соответственно разным уровням подготовки пользователей, поэтому автор предполагает максимально полное ознакомление читателя с текстом перед началом практического использования описываемых средств: многие важные детали сознательно упомянуты только один раз.

В момент подготовки книги к печати актуальны следующие версии описываемых программных средств:

* ***Doctor Web для Windows***	**4.17**
* ***ADinf-32 для Windows***	**3.00**
* ***SpIDer Guard***	**4.17**

II. Вирусы и антивирусные средства

Данная работа не претендует на полное описание всех существующих вирусных типов и их модицикаций, равно как и исчерпывающий анализ антивирусных средств различных производителей. Цель данного раздела более скромна — дать минимальный справочный материал по наиболее известным или специфическим типам вредоносных программ и напомнить читателю основные типы защитных средств против таковых.

2.1. Типы вредоносных компьютерных программ

Вирусы

Строго говоря, далеко не любая вредоносная программа является вирусом. Собственно вирус — это программный компонент, способный к самостоятельному распространению своей прямой или модифицированной копии в некоторой операционной (DOS, Windows 3.x и др.) и/или программной (например, Word-Basic) среде.

Поскольку неконтролируемое размножение само по себе уже наносит вред пользователю, отнимая время, дисковое пространство и другие ресурсы вычислительных средств (не говоря уже о психологических аспектах), вредоносность очевидна. Однако, далеко не все вирусы так безобидны — весьма часто наносится и прямой вред пользователю.

Такие программы, первоначально написанные на одном ПК, умеют самостоятельно “прикрепляться” к другим программным компонентам, доступным на том же ПК. Получая информацию о наличии потенциальных “жертв” на ПК и их уже выполненной зараженности, вирусы прикрепляются к объектам атаки с тем, чтобы при переносе зараженных программ на другой ПК первыми получить управление и продолжить свои действия на новом месте. Скорость размножения для различных типов вирусов может весьма разниться (от нескольких заражений за одно включение ПК до десятков тысяч заражений в час) и зависит от выбранного вирусописателем алгоритма заражения, действий подвергшегося вирусной атаке пользователя, типа его компьютера и многих других параметров.

Поскольку вирус является программой (точнее, программным кодом), для его распространения важна среда его предполагаемого распространения как совокупность функций, предоставляемых ею для приложений. Часто в основу классификации вирусов берется именно

среда, способ распространения или иные характеристические свойства вирусов. Основные разновидности вирусов, устоявшиеся по их названиям к настоящему моменту, перечислены ниже.

Файловые вирусы — наиболее известны, получили широкое распространение еще в DOS. Поиск объектов и большинство операций своего размножения они исполняют в основной операционной среде, пользуясь ее стандартными, недокументированными или системными функциями. Первоначальное заражение ПК происходит, когда по оплошности или незнанию на ПК устанавливается или запускается зараженная вирусом программа.

Бутовые (загрузочные) вирусы — также известны со времен DOS. Местом их укоренения является загрузочный сектор локального диска, с которого исполняется загрузка ПК. Подменяя собой стандартный загрузчик, такой вирус в силу особенностей процесса загрузки попадает в память ПК ранее, чем ОС. Многие известные вирусы комбинируют возможности распространения файловых и бутовых вирусов. Заражение чисто бутовым вирусом происходит в момент перезагрузки ПК, если в него вставлена дискета, загрузочный сектор которой содержит бутовый вирус, и ПК пытается с нее загрузиться.

Резидентные вирусы — вирусные программы, использующие один из методов оставления в памяти части своего кода после завершения программы-вирусоносителя.

Макрокомандные вирусы появились как вирусы, “живущие” в среде макрокоманд WinWord. С тех пор, как разработчики WinWord предоставили пользователю полноценную среду макрокоманд языка WordBasic с возможностями открытия/закрытия/считывания/записи файлов, естественно, появился и соответствующий класс вирусов. Эти вирусы в последнее время многочисленны и быстро развиваются. Размножение их обусловлено большим документооборотом. Следует упомянуть, что этот класс вирусов не исчерпывается средой WinWord: известны вирусы, использующие MS-макросреды: Excel, Access, PowerPoint, а в последнее время — Help и даже HTML. Ряд таких вирусов жизнеспособен и в “обычной” среде исполняемых файлов.

Пакетными можно называть вирусы, весь код которых содержится и переносится в BAT-файлах и их аналогах в других ОС (например, CMD-файлах). Хотя “чистых” BAT-вирусов весьма немного, многие вирусы других групп используют внедрение в BAT-

файлы и их аналоги (AUTOEXEC.BAT, WININIT.INI) для заражения ПК в момент старта ОС при перезагрузке.

Многоплатформенность. Ряд вирусов способен действовать в различных программных средах, распознавая их и адаптируясь. Попав, к примеру, через переданный документ WinWord, вирус **WM.MDMA** целенаправленно и различно действует в Windows 3.x, ’95, ’NT и Macintosh.

Полиморфными называют вирусы (файловые, бутовые, макро — безразлично), способные при заражении очередного объекта менять собственный код. Известно, что любая задача программирования достижима различными реализациями алгоритма. Это и используют полиморфные вирусы, имеющие встроенные кодировщики: на каждом этапе заражения такой вирус выбирает из некоторых совокупностей команд нужную группу случайным образом, обычно по содержимому таймера. Результатом этого может быть вирус, весьма значительно отличающийся своим программным кодом от оригинала, но исполняющий ту же самую задачу. Примерами таких вирусов могут являться **Phantom-1**, **Natas** или **OneHalf**, в поколениях которых может не повториться ни одна цепочка байтов.

Стелсами (stealth) называют вирусы, которые умеют скрывать свое присутствие от обычных программ, исполняемых в ОС. Эти методы также известны со времен DOS. Так, например, просматривая в Нортон-Коммандере зараженный таким вирусом файл, увидеть вирусный код невозможно: резидентный блок вируса, находящийся в памяти ПК, выявив, что поступил приказ на открытие зараженного файла, мгновенно его вылечит (либо подставит незараженную копию), а после закрытия снова заразит. Аналогичные технологии предпринимаются и в средах Windows: запуск процесса в скрытом окне, перехват системных функций и др. Прилагаемые авторами вирусов усилия могут быть весьма различными, начиная от перехвата более 20 функций операционной системы (**Frodo.4096**) и кончая маскировкой на уровне дискового драйвера (семейство **Dir-II**), на уровне прерывания Int13h (группа **ExeHeader**) или даже на уровне контроллера винчестера (**Strange**).

Троянцы

Троянцы, в отличие от собственно вирусов, самостоятельно распространяться не могут. Для своего распространения они маскируются под известные либо привлекательные программы, побуждая

пользователя их запустить. Помимо заявленной цели, такие программы выполняют скрытые функции (откуда и пошло их название), несущие вред пользователю. Дополнительной маскировкой может быть удаление (иногда переименование) старого файла и запись в тот же каталог нового с тем же именем и троянским содержанием.

Разумеется, такие программы лечению не подлежат: их следует удалить. Если при этом троянец запускался и есть опасность нарушения изначальных свойств ОС или приложений, необходимо восстановить оригинальные программные модули, которые подверглись воздействию троянца. Как видим, в дополнение к задаче обнаружения собственно вредоносной программы встает также задача поиска всех модифицированных модулей.

Вредоносность программ

Вредоносность различных программ может проявляться поразному. Помимо внедрения в тело программы и тем самым изменения ее структуры, нарушения контрольных сумм и точек входа, наиболее известны следующие проявления вирусной активности.

* Подсматривание паролей DialUp и посылка их по E-Mail нужному адресату с тем, чтобы впоследствии воспользоваться именем и паролем пользователя для доступа к Интернету, рассылки писем рекламного или иного содержания

* Пометка неиспользуемых кластеров как сбойных с тем, чтобы с течением времени свободное пространство на диске уменьшалось

* Различные видеоэффекты (осыпание букв, переворот изображения экрана, имитация перезагрузки ПК или форматирования жесткого диска (*Hard Disk Drive*, HDD), “гуляние” по экрану шарика, различных животных и т.п., нецензурные изображения, стихи, ругательства, поздравления, признания в любви и др.)

* Искажение печатаемой на принтере информации

* Постепенная шифрация HDD (при попытке просто удалить вирус информация остается нерасшифрованной необратимо)

* Стирание файлов на диске случайным образом или по какому-либо признаку

* Хаотическое или целенаправленное изменение информации на диске (разные вирусы дают весьма широкий диапазон выбора: от необратимой порчи состава избранных файлов до замены актуальной текстовой информации на матерные комментарии, — согласно интеллектуальному и культурному уровню вирусописателя)

* Порча ЭППЗУ (flash-ROM) хаотической информацией вместо BIOS так, что компьютер после этого перестает загружаться

* Посылка в регистры управления внешних устройств (HDD, видеокарта) формально возможных, но логически некорректных сигналов для выведения их из строя

* Удаление с диска компонентов антивирусных программ

Как уже было сказано, помимо этих явных вредоносных проявлений, сам факт неконтролируемого размножения наносит очевидный вред, занимая вычислительные ресурсы. Знатоки зачастую могут определить наличие вируса по дополнительным попыткам обращения к дискете при считывания с нее файла. Гораздо серьезнее многократно описанные в прессе случаи “забивания” вирусной активностью компьютерных сетей с блокированием передачи обычной информации.

Следует знать, что — по аналогии с обычной болезнью — действия вирусов могут обозначиться явным вредом не сразу, а по истечении некоторого скрытого, *латентного* периода, во время которого вирус просто размножается, не исполняя явных разрушающих действий. Наиболее известен метод таких задержек по достижении определенной даты (26 апреля у **Win.CIH**, совпадение пятницы с 13-м числом месяца у нескольких более ранних вирусов). Для бутовых вирусов стандартна инициация вредоносных действий после определенного числа перезагрузок ПК. Встречаются и более изощренные методы задержки — например, по количеству нажатий на клавиши, по номеру поколения заражения, и другие.

В общем потоке новых — больше всего сравнительно простых или даже безграмотно написанных вирусов, вызывающих локальные эпидемии. Такие вирусы обычно не получают широкого распространения, быстро обнаруживаются и уничтожаются, успев причинить вред в районе своего размножения. Встречаются, однако, резкие отклонения. Печально знаменитое детище тайваньского студента **Win.CIH**, по данным прессы, поразило миллионы компьютеров во всем мире.

Опасность вирусов известна всем пользователям ПК. Вопросы их распространения и техники обеззараживания освещены и в научной, и в популярной литературе последних лет (см. список на с.103). Однако, имеет смысл выделить ряд тенденций, акцентировавшихся в последние годы. К их числу можно отнести:

— усложнение вирусной структуры (полиморфики);

— появление вирусов под новые ОС (Windows 3.x, Windows 95/98, OS/2, Linux, а затем и под Windows NT);

— появление новых сред обитания вирусов (тексты, спредшиты, БД, а теперь еще и Help'ы и документы на HTML);

— развитие специфической направленности вирусной агрессии на системы коммуникации (в первую очередь, www-станции);

— новые каналы распространения вирусов (CD, www-сайты);

— новые объекты воздействия (атака на flash-ROM);

— новые способы распространения заразы (маскировкой под полезные программы, патчи и даже антивирусные средства, побуждающие пользователя их установить или запустить).

Упомянутые тенденции с неизбежностью смещают акценты в стратегии антивирусной защиты. Становится важным "время отклика" антивирусов (постоянное появление новых версий, еженедельные дополнения к вирусным базам — насущная необходимость каждого ПК). Невелико значение устарелых антивирусных средств или не отвечающих местной вирусной ситуации. На первый план выходят универсальные программы, обеспечивающие быструю ликвидацию локальных эпидемий, имеющие улучшенные адаптационные возможности и регулярно обновляемые базы вирусов, обеспеченные постоянной авторизованной поддержкой и эффективной "обратной связью" авторов программ с пользователями. В последние годы особо важное значение приобрели также интеллектуальные технологии выявления неизвестных вирусов, свойственные описываемым в данной работе продуктам.

Видимо, следует сказать также и о том, что нельзя любой вред однозначно относить к проявлениям неизвестных вирусов. Достаточно часто порча файлов бывает из-за отошедшего шлейфа или иной неисправности ПК. Мне известны многие случаи просто некорректно написанных программ; одним из последних примеров может служить некорректность системы защиты в ряде продуктов фирмы **1С**.

2.2. Краткий обзор антивирусных средств

Перед конкретными рекомендациями и инструкциями по применению компонентов антивирусного пакета DSAV фирмы "ДиалогНаука" представляется целесообразным указать существующие типы антивирусных средств в их краткой классификации.

Сканеры

Сканеры — самые известные антивирусные программы. У каждого сканера есть в его составе антивирусная база форматов тех вирусов, против которых он направлен. Запуская сканер в различных режимах, можно проверить все или часть файлов ПК на предмет зараженности вирусами, шаблоны которых входят в комплект сканера.

К сканерам принадлежит патриарх **Aidstest**, а также значительное число узкоцелевых сканеров, направленных на поиск и излечение конкретного вируса или группы вирусов.

В настоящее время предпочтение отдается многоцелевым сканерам, проверяющим заданную пользователем группу файлов на заражение практически всеми известными вирусами, а также тестирующим загрузочные сектора локальных дисков и оперативную память на нахождение известных вирусов.

Во всех случаях эксплуатации сканера следует отчетливо представлять себе, что:

— каждый сканер может установить зараженность лишь теми вирусами, которые "заложены" в конкретную используемую им базу форматов вирусов;

— полную гарантию отсутствия даже этого ограниченного числа вирусов большинство сканеров могут дать лишь при проверке "чистой" ОС, когда есть уверенность в том, что тот или иной вирус к моменту проверки не попал в память компьютера.

Рассматриваемые ниже в разделе 3 версии сканера ***Doctor Web-32 для Windows*** имеют и дополнительные функции, помогающие в обнаружении ряда заранее неизвестных вирусов.

Сторожа

В отличие от сканеров, которые специально запускаются на предмет выявления вирусов на ПК, сторожа присутствуют постоянно в памяти ПК и контролируют файлы, к которым имеются обращения из

других исполняемых программ, на предмет их зараженности. Разумеется, это увеличивает время исполнения всех технологических операций с файлами, зато дает возможность максимально быстрой фиксации заражения и принятия оперативных мер.

Помимо проверки файлов на соответствие шаблонам вирусов, сторожа могут исполнять и другие операции: контроль записи в критические для сохранности данных области локальных дисков, блокировку попыток форматирования дисков или дискет и др.

Сторожа известны почти так же давно, как и ревизоры. Один из первых сторожей для DOS контролировал операции форматирования дисков и дискет и попытки записи в системные области дисков, выдавая запрос оператору каждый раз при обнаружении той или иной подозрительной операции. Предполагалось, что пользователь достаточно знает о том, что делает в тот или иной момент запущенная им программа, и в состоянии осмысленно принять решение разрешить или блокировать ту или иную операцию. С усложнением ОС, когда одновременно могут протекать десятки квазипараллельных процессов (в том числе системных), часть функций пользователя неизбежно должна быть отдана встроенной в сторож интеллектуальной системе обработки информации.

Рассматриваемый в данном документе сторож ***SpIDer Guard*** — самое “молодое” 32-битное антивирусное средство для Windows. Ряд предпосылок, однако, позволяет предсказать ему значительный акцент в будущем антивирусных средств. Эта программа ведет протокол и статистику заражений, и способна анализировать “поведение” запускаемых приложений, выявляя “подозрительные” действия зараженных вирусами программ.

Ревизоры

В отличие от сканеров и сторожей, программы-ревизоры не хранят вирусных баз. Их цель — выявить изменения на дисках ПК пользователя, произошедшие с момента прошлого запуска того же ревизора. Данные обо всех или интересующих пользователя файлах сохраняются в специальных файлах-таблицах на одном из локальных дисков. Такие таблицы занимают сравнительно немного места и позволяют, сверяясь с актуальным состоянием файла, выяснить, были в нем сделаны какие-либо изменения или нет.

Целесообразность использования ревизоров становится очевидной всем, кто пробовал проводить сплошную проверку на вирусы

сканером (например, 16-битным **Doctor Web для DOS**). Для стандартного Pentium-90 при объеме HDD 2-3 Гб и числом файлов от 4000 до 8000 такая проверка может занять несколько часов непрерывной работы, причем само по себе повышение частоты процессора до 200-266 МГц это время заметно не сокращает.

Выходом из положения является задействование ревизора. Поскольку длительность ревизии зависит только от числа файлов, но не от размеров вирусной базы, да к тому же специальные способы проверки существенно сокращают время ревизий файлов, просмотр значительного числа файлов занимает считанные минуты. Одним из выходных результатов ревизии дисков является список новых/измененных файлов, который и предъявляется сканеру для тщательной проверки на вирусы. Ряд соображений позволяет в некоторых случаях существенно сократить даже эти необходимые операции, так что реальные затраты времени на противовирусные операции становятся еще меньше.

Advanced Diskinfoscope-32 для Windows, или ADinf-32, имеет солидную историю. Первые версии ADinf были сделаны еще под DOS; текущая версия для DOS поддерживается и сейчас. Есть варианты, работоспособные в среде Windows как 16-битные приложения. Описываемая в данной работе версия 3.0 **ADinf32** разработана как 32-битное приложение, работоспособное в среде Windows (в том числе NT). До версии 2.0 поддерживались файловые системы организации дисков FAT12, FAT16, VFAT и FAT32; с версии 2.0 — NTFS.

Кроме устранения последствий вирусной активности, ревизоры весьма полезны как средства отслеживания неизменности файлов (к примеру, эталонных кодификаторов в бухгалтерских системах и пр.). ADinf32 имеет развитый и полезный сервис для таких работ.

Дополнительные антивирусные средства

Помимо сканеров, ревизоров и сторожей, антивирусные средства ЗАО “ДиалогНаука” включают еще ряд компонентов, одним из которых является лечащий блок **Adinf Cure Module**.

ADinf Cure Module создан и существует как 16-битное приложение в DOS и Windows. Смысл его использования следующий.

Любое внедрение вирусов в исполняемый файл с необходимостью вызывает ограниченное число формальных операций с модулем, легко опознающихся по контрольным параметрам. Запомнив эти

параметры для некоторого файла, в дальнейшем можно проследить их сохранность и, таким образом, установить, является ли некоторый модуль измененным по сравнению с оригиналом. Далее, в ряде случаев достаточно запомнить ряд характеристик для этого файла до заражения, чтобы его можно было восстановить с полной точностью в исходное состояние.

Проверяя при ревизии дисков для некоторого файла соответствие запомненных ранее параметров текущим и обнаружив расхождение, возможно восстановить исходное состояние файла без знания каких-либо деталей о вирусе. Важно, что в данном случае достаточно просто быть уверенным в том, что изменился тот файл, который измениться не должен. **ADinf Cure Module** выполняет такое восстановление файла.

Не секрет, что сканеры при лечении пораженных вирусами файлов ради быстроты, либо вследствие некорректности работы ряда вирусов, вместо полного удаления вирусного кода из зараженного файла всего лишь блокируют исполнение вирусной ветви. Если такое лечение не удовлетворяет пользователя и требуется *точное* восстановление исходного вида модуля, необходим лечащий блок **ADinf Cure Module,** созданный как раз для таких случаев: если уж он сможет восстановить исходный вид файла, то сделает это с абсолютной точностью.

Программа **ADinf Cure Module** по ряду соображений используется для лечения в среде DOS, причем при загрузке со специальной “лечащей” дискеты. Изложение техники работы с этой программой выходит за рамки данной книги. Следует, однако, иметь в виду, что для обеспечения возможности работы этой программы под DOS ревизор ADinf32 имеет при работе в Windows режим совместимых, так называемых “16-битных”, профилей.

Антивирусные средства ЗАО “ДиалогНаука” для Windows 95/98/NT включают в себя также ряд вспомогательных утилит и программ, не отраженных в данной книге, поскольку они не являются к моменту издания книги средством конечного пользователя.

2.3. Требования к ОС и работе пользователей

Применение антивирусных средств как программ, работоспособных в некоторой среде, неминуемо налагает к этой среде ряд требований соответствия. Организация коллективной работы на ПК также накладывает свои требования при установке и эксплуатации пакетов.

Развитие операционных сред Windows по проекту разработчика предусматривало необходимость постоянной коррекции операционных компонент. С появлением Windows стало практически невозможным эксплуатировать базовую ОС годами (как ранее MS-DOS) без постоянных модификаций уже хотя бы потому, что обнаруживаемые регулярно ошибки в ОС продуцируются самой системой создания Windows[1]. Выпуск приложений, и в том числе антивирусных программ, вынужден подстраиваться под стиль работы разработчика ОС. В силу сказанного априорно ясно, что *никакой* производитель (в том числе ЗАО "ДиалогНаука") не может выпускать продукцию, одинаково работоспособную на *всех* вариантах предыдущих версий ОС. В наших условиях, когда постоянное отслеживание изменений с коррекцией базовой ОС еще не вошло в обязательность повседневной практики на всех ПК, установка серьезных антивирусных приложений, включающихся в работу ОС на системном уровне, затруднена.

В ряде случаев некорректная работа аппаратуры принималась пользователями за действие неизвестного вируса.

К этим проблемам добавляется психологическая неготовность пользователя к полной ответственности за эксплуатируемые продукты, коллективное использование персональных средств организации труда, использование нелицензированных программ и другие.

Эти теоретические рассуждения достаточно ярко проявились, в частности, когда разработчиками Windows был заменен интерфейс управления (о модуле **COMCTL32.DLL** см. ниже). Практика моей работы с пользователями также выявила такие проблемы, как наличие логических ошибок на HDD, выявляющихся непосредственно перед установкой (причем пользователи даже не представляли себе

[1] За год эксплуатации Windows'98 только официальных сообщений о найденных ошибках в ней на сайте разработчика **www.microsoft.com** превысило 6000.

необходимость подобной регулярной профилактики), использование некондиционных технических средств (в частности, видеокарт на чипе S3 с некорректными драйверами, вследствие чего попытки проверки системной памяти приводили к системной ошибке, а то и к жесткому зависанию ПК), использование различных фирменных продуктов, мешающих эксплуатации антивирусных средств.

В силу сказанного представляется уместным ставить вопрос об условиях применения антивирусных комплектов на ПК пользователей. К этим условиям представляется необходимым отнести:

— полную работоспособность технических средств ПК;

— современные версии технических устройств, поддерживаемые соблюдающими стандарты этих ОС драйверами;

— наличие последних версий базового СМО (не Windows'95, а 'OSR2; не просто Windows'NT, а установленность последнего Service Pack'а и т.п.);

— отсутствие на ПК средств, блокирующих антивирусную проверку, в том числе антивирусных комплектов альтернативных производителей;

— отсутствие ошибок логической организации диска;

— наличие *одного* лица, отвечающего полностью за эксплуатацию конкретного ПК, причем у этого лица должны быть права Администратора при эксплуатации Windows'NT.

С развитием антивирусных технологий, указанные выше проблемы ужесточатся. В недалеком будущем описываемые здесь антивирусные средства уже могут не быть работоспособными на вариантах Windows 95/OSR2 ввиду завершения поддержки этих версий производителем. Стоит подумать о своевременном переходе на Windows 98/NT/2000.

Так, начиная с некоторого момента, версия сканера DrWeb32 для работы в режиме обновления через Интернет требует модуля **WININET.DLL**, стандартного для '98, но отсутствующего в ранних комплектациях '95 и 'NT.

Другая известная проблема связана с системной библиотекой **COMCTL32.DLL**, с устаревшей версией которой работа современных версий антивирусных средств невозможна (возникает ошибка в модуле USER.EXE).

III. Сканер Doctor Web для Windows

Семейство антивирусных программ **Doctor Web-32**[1] включает в себя программы для ОС Windows, Novell NetWare, OS/2 и DOS/386. Ниже рассмотрен исключительно комплект **Doctor Web для Windows**, созданный для исполнения в 32-битной среде Windows (в комплект входит также 32-битная версия для DOS).

Doctor Web для Windows — современный антивирусный сканер. В нем впервые в мире реализована полная проверка всей памяти Windows 95/98, включая системную память (в том числе, совместно используемую), память всех виртуальных машин и прикладных процессов. Это позволяет надежно находить и обезвреживать сложные троянские программы и вирусы, использующие нетрадиционные пути внедрения в память Windows. В частности, это касается большого числа троянцев, предоставляющих несанкционированный доступ к ПК (типа **Back Orifice**) или ворующих пароли для доступа в Интернет.

Основная исполняемая сканерами функция проверки модулей на присутствие известных вирусов по шаблонам дополнена проверкой на модификации известных вирусов. Для исполняемых файлов, сжатых посредством одной из известных программ упаковки, помимо обычной проверки зараженности может быть дополнительно проведена проверка на вирусы после предварительной распаковки модуля.

В случае обнаружения вирусного кода по заявке пользователя объект может быть излечен (если он в принципе излечим), либо зараженный файл может быть удален, переименован или перемещен в специально предназначенный для таких файлов каталог.

Doctor Web умеет также проверять файлы внутри архивов самых распространенных типов: **ZIP**, **ARJ** и **RAR** (кроме файлов, разделенных по многотомным архивам). Лечение внутри архивов Doctor Web не исполняет.

Кроме проверки на шаблоны известных вирусов, хранящиеся в основной антивирусной базе и ее еженедельно выходящих дополнениях, этот сканер имеет **эвристический анализатор** — интеллектуальный аппарат оценки исполняемых файлов на соответствие их кода потенциальным вирусным технологиям. С помощью эвристического анализа возможно принципиальное выявление новых вирусов, исходя из анализа кода программных приложений.

[1] Авторы: *И. Данилов, В. Лутовинов, Д. Белоусов, А.Башаримов, С.Попов.*

Doctor Web для Windows поставляется в двух реализациях программы: с графической оболочкой (далее **DrWeb32W**) и для запуска исключительно с параметрами из командной строки (**DrWebWCL**). В тот же комплект также входит **Doctor Web-386 для DOS** (далее **DrWeb386**), предназначенный для использования под DOS на ПК класса не ниже AT-386. Все три реализации функционально схожи, задействуют одну и ту же вирусную базу, одни и те же дополнения к ней и еще часть модулей комплекта, в том числе один и тот же конфигурационный файл (но DrWeb32W и DrWebWCL — одну секцию настроек конфигурации, DrWeb386 — другую, поэтому можно попеременно использовать DrWeb32W или DrWebWCL с сохранением преемственности по настройкам, но для DrWeb386 все режимы необходимо задать отдельно от прочих программ комплекта).

Смысл подготовки в комплекте именно этих трех программ следующий. Графический интерфейс DrWeb32W включает в работу намного больше ресурсов, чем DrWebWCL. Поэтому в случаях острой нехватки памяти, а также при неработоспособности графического интерфейса на Вашем ПК (при устарелых версиях Windows или загрузки Windows в режиме работы из командной строки) Вы все же сможете использовать DrWebWCL. Пользователи, привыкшие использовать ADinf16 в DOS до загрузки Windows, могут воспользоваться DrWeb386. Остро необходим бывает именно DrWeb386 в тех случаях, когда из-за вирусных действий Windows не загружается вообще.

Для экономии места далее в этой книге программы DrWeb32W и DrWebWCL объединяет имя **DrWeb32**.

DrWeb32W поддерживает совместную работу с ADinf32. Возможна также совместная работа DrWeb32W с DOS-версией ADinf, но не с 16-битной версией ADinf для Windows.

Каждая из программ DrWeb32 может быть поставлена в одноязычном со стандартным английским языком или многоязычном варианте поставки, каждый из которых существует в двух типах поставки: как единый дистрибутивный файл большого объема и как совокупность образов дискет. К моменту подготовки этого издания комплект Doctor Web для Windows занимает три 1,44 3”-дискеты.

Ключевой файл **DrWeb32.KEY** необходим для запуска программы. Он имеет ограниченный срок действия и может иметь ограничения функциональных возможностей программы. Без ключа программа работает в ознакомительном режиме, без лечения и других функций.

3.1. Управление в основных окнах DrWeb32W

Основные окна запросов

После запуска в ручном режиме без параметров появляется одно из Основных окон программы (см.рис. 1). Если необходима проверка памяти, она начинается сразу же. При этом проверяется память всех системных процессов (внизу экрана строка показывает местонахождение соответствующего исполняемого модуля, вызвавшего процесс — не путать с проверкой конкретных файлов!).

Основное окно программы DrWeb32W

В этом окне задаются объекты проверки текущего сеанса. Отсюда возможен вход в окна Просмотра результатов и Статистики, в Панели настроек, а также возможен ряд дополнительных операций, подробно рассматриваемых ниже.

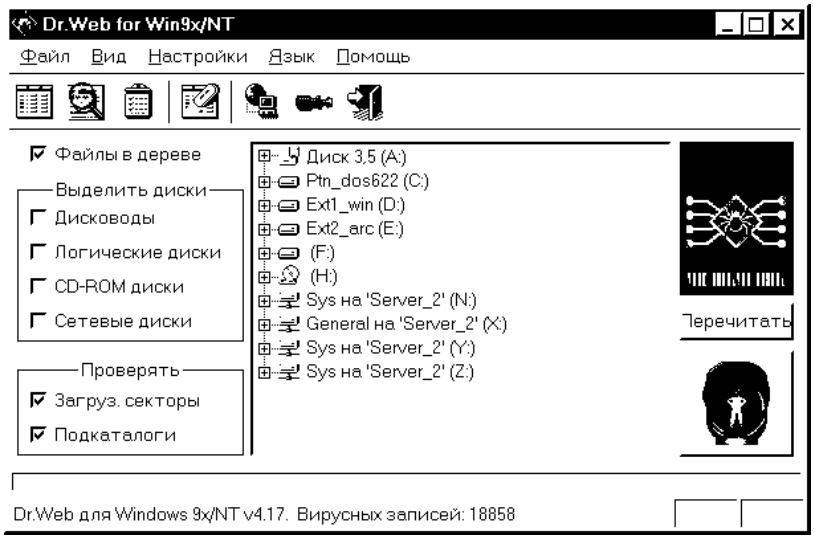


Рис. 1. Основное окно программы *DrWeb32W*

Ко многим элементам управления есть несколько альтернативных входов — например, в Панели настроек можно войти, нажав “кнопку” с изображением отвертки, либо выбрав в ниспадающем меню пункты ***Настройки — Изменить установки***, либо нажав <**F9**>**.**

Второй ряд управления образуют кнопки:

— переключения на окно Просмотра результатов;

— переключения на Основное окно;
— переключения на окно просмотра Статистики;
— очистки списка результатов;
— вызова обновления версии;
— входа в Установки;
— завершения работы программы.

В верхнем ряду находятся ниспадающие меню. Ниже приведены их пункты.

Файл — Начать проверку начинает работу по предварительно выделенным дискам, каталогам либо конкретным файлам.

Файл — Остановить проверку прерывает сканирование.

Файл — Проверить путь позволяет мышью выбрать путь проверки в специально всплывающем окне и тут же начать проверку.

Файл — Проверить память позволяет проверить память компьютера (проверка памяти при старте проводится или нет согласно INI-файлу и параметрам вызова).

Файл — Очистить список отчета очищает выходные результаты окна Просмотра.

Файл — Выход завершает работу программы.

Вид — элементами подменю переключает в нужное окно просмотра.

Настройки — меню разрешает войти в панели настроек и ***Изменить*** установки, ***Сохранить*** сделанные (к моменту нажатия!) изменения в INI-файле для использования во всех последующих сеансах работы, ***Восстановить*** установки из INI-файла. Отделенный чертой пункт меню ***Обновить*** запускает механизм обновления версии (предварительно должны быть настроены соответствующие поля панели ***Обновление***).

Язык служит для переключения языка в многоязычных версиях. После переключения все надписи в текущем окне мгновенно изменяются. Этим способом также меняется язык отчета. Сообщения в статус-строке внизу окна изменятся в последующих вызовах программы.

Помощь — содержит вход в Help-файл (***Разделы помощи***) и краткие сведения о программе и ее авторах (***О программе***), включая возможность соединения по Интернет с сайтом разработчика.

Центральная часть окна показывает общее дерево доступных логических дисков. Щелчком левой кнопки мыши на изображении

диска можно включить/выключить диск из списка проверяемых; щелчком на знаке “плюс” слева от диска можно, по традициям Windows, сойти на уровень вниз и открыть список каталогов диска; причем если включен флажок ***Файлы в дереве***, то таким образом можно добраться даже до конкретного файла. Щелчок правой кнопкой на дереве аналогичен выбору ***Файл— Проверить путь.***

Группа флагов ***Выделить диски*** позволяет задать выбираемые для следующей проверки диски в текущем сеансе. Чтобы не повторять каждый раз выбор одних и тех же дисков при вызове DrWeb32W, их можно задать постоянно в Панели настроек ***Проверка***.

> В общем случае не следует задавать проверку сетевых дисков, если Вы — не системный администратор!

Группа флагов ***Проверять*** задает необходимые действия для следующей проверки в текущем сеансе. Чтобы не повторять каждый раз установку этих опций, их можно включить постоянно в Панели настроек ***Проверка***. Галочка в поле ***Загруз.секторы*** включает в число объектов проверки не только файлы, но и загрузочные секторы (на флоппи-дисках проверяется *boot*-сектор, на HDD проверяются *MBR* и *boot*-сектор активного раздела, на сетевых дисках загрузочные сектора не проверяются). Галочка в поле ***Подкаталоги*** позволяет проверять не только выбранные каталоги, но и их подкаталоги всех уровней.

Галочка в поле ***Файлы в дереве*** разрешает показ файлов в дереве каталогов при выборе проверяемых объектов; иначе показываются только сами каталоги. Данный флаг имеет смысл использовать, если нужно проверить конкретный файл (группу файлов). При проверке всего диска/каталога эта опция не нужна: масса файлов “забивает” окно, мешая выбрать объекты проверки.

Кнопка ***Перечитать*** служит для обновления дерева каталогов и дисков. Это бывает необходимо, например, если в процессе работы программы DrWeb32W вы заменили дискету, создали каталог и пр.

Кнопка-индикатор справа внизу при выборе хотя бы одного объекта для проверки становится зеленой, и ее нужно нажать для начала сканирования. Повторное нажатие при идущем (кнопка красная) сканировании остановит его.

Строка текста внизу окна содержит информацию о версии программы. В ходе проверки памяти до версии 4.14a там может быть ин-

формация о текущих проверяемых процессах, с версии 4.15 — текст **Проверка памяти**; в ходе сканирования там стоят имена файлов.

Прогресс-индикатор над текстовой строкой показывает динамически ход проверки системной памяти или заданных объектов.

Окно просмотра результатов DrWeb32W

В этом окне (рис.2) выдаются результаты запусков с момента старта программы либо последней очистки окна. Если содержимое всех граф не умещается на экране, окно можно “растянуть” в любую сторону. Можно также передвинуть графы.

В левом столбце указываются имена файлов, на которые среагировала программа. В следующем столбце показаны полные пути к соответствующим файлам. В столбце ***Статус*** указывается причина помещения данной строки в отчет; например, здесь дается имя обнаруженного вируса.

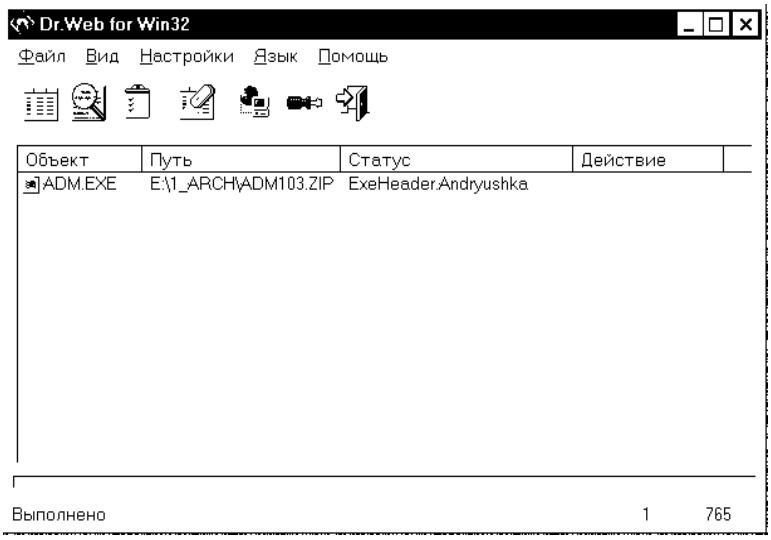


Рис. 2. Окно просмотра результатов DrWeb32W

В столбце ***Действие*** сообщена, если она последовала, реакция программы на обнаруженное явление. Это может быть пометка об излечении, переименовании, удалении, перемещении в нужный каталог и т.д., либо просто пустое место — в том случае, когда DrWeb32W ничего в обнаруженной ситуации не предпринял.

Кстати, отсутствие нормальной реакции программы Doctor Web на обнаруженный объект говорит об одной из следующих причин:

— в панели настройки ***Действие*** для вируса определено действие ***Информировать***;

— обнаружен не вирус, а троянец, которого излечить невозможно, но для ***Неизлечимых*** в панели настроек ***Действие*** поставлено ***Информировать***;

— обнаружен вирус, необратимо портящий файл, в который он внедряется, и потому неизлечимый, а для ***Неизлечимых*** поставлено ***Информировать;***

— не вирус, а лишь подозрительный файл обнаружил эвристический анализатор, и для ***Подозрительных*** в панели ***Действие*** поставлено ***Информировать***;

— вирус обнаружен не в самостоятельном файле, а в архиве (как уже было сказано, архивированные файлы **Doctor Web** не лечит);

— вирус обнаружен на дискете, защищенной от записи, на сетевом диске без прав записи на него либо на CD-ROM, так что лечение в принципе невозможно (дается сообщение об ошибке записи);

— обнаружен макрокомандный вирус в некотором документе, но в данный момент этот документ открыт каким-либо пакетом (будет выполнена попытка отложенного лечения, см.ниже);

— обнаружен вирус в файле, доступ к которому запрещает один из установленных на данном ПК пакетов, например, **Norton Unerase Wizard** (также будет попытка отложенного лечения);

— обнаружен вирус в файле, используемом одним из активных 32-битных приложений Windows (например, вирус находится в файле Internet Explorer'a, изменить который Windows не даст).

Как видим, в ряде случаев непосредственное лечение невозможно из-за особенности управления файлами в ОС. В таких случаях программа DrWeb предпринимает попытку отложенного лечения. Если обнаруженный зараженный объект недоступен по записи в момент запуска DrWeb, то в строке "Действие" по такому объекту будет дано сообщение **Будет излечен после рестарта** или **Будет удален после рестарта** в зависимости от излечимости/неизлечимости объекта. Одновременно для излечимого объекта в каталог, в котором он находится, будет дописан его аналог в виде вылеченного файла со случайным именем, и сформирован специальный приказ, по которому после рестарта Windows этот аналог заместит оригинальный зара-

женный файл. Аналогично, могут быть приказы о перемещении, удалении и переименовании файлов. Приказы на такие действия будут записаны в WININIT.INI (в Windows'95/98) или исполняемую часть реестра (в Windows'NT) для исполнения в момент ближайшего последующего рестарта системы. Этот рестарт будет предложено выполнить сразу по завершении DrWeb, если сформирован хотя бы один такой приказ.

Если проверяемый каталог закрыт по записи (Администратором Windows'98 или пользователем Windows'NT), то механизм излечения аналогичен приведенному выше.

К сожалению, если проверяемый каталог закрыт *по чтению*, либо используются какие-либо внесистемные средства разграничения доступа к файлам по чтению, то DrWeb даст ошибки чтения по каждому файлу каталога, причем прервать его весьма трудно из-за постоянной выдачи сообщений об ошибке чтения. В этих случаях рекомендуется правильно настраивать спарку ADinf32+DrWeb с исключением проверки таких каталогов у пользователей коллективно используемого ПК, которым доступ к этим каталогам закрыт.

В последней строке указывается количество обнаруженных пораженных объектов и количество проверенных объектов.

Окно просмотра статистики

В этом окне (рис. 3) демонстрируются результаты всех прогонов текущего сеанса. Верхние две строки содержат управляющие элементы, аналогичные предыдущим Окнам. Третья строка имеет кнопку ***Всего*** и остальные кнопки (по числу логических устройств), позволяющие просмотреть общую статистику либо статистику по конкретному устройству.

Кнопка внизу справа с изображением пылесоса обнуляет накопленную статистическую информацию.

Статистика, накапливаемая за все время сессии вызова DrWeb32W, содержит данные:

Проверено — общее количество проверенных объектов;

Инфицированных — число объектов, инфицированных основными разновидностями известных вирусов;

Модификаций — число объектов, инфицированных модификациями вирусов;

Подозрительных — общее число подозрительных на наличие вирусов объектов, выявленных эвристическим анализатором;

Исцелено — число вылеченных объектов;

Удалено — число удаленных объектов;

Переименовано — число переименованных объектов;

Перемещено — число объектов, перемещенных в назначенный каталог.

Операция, которая выполняется с инфицированным объектом, назначается в панели настроек ***Действие***.

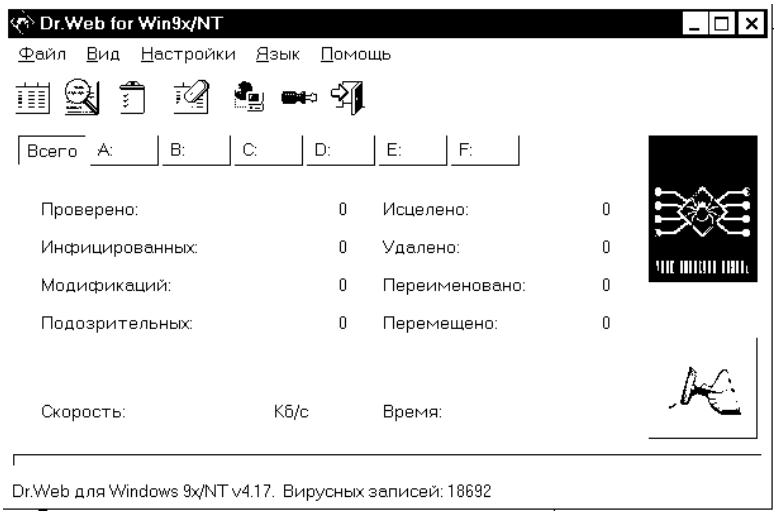


Рис. 3. Окно просмотра статистики DrWeb32W

Усредненная ***Скорость*** сканирования приведена в килобайтах в секунду, общее ***Время*** проверки включает часы, минуты и секунды, затраченные на сканирование.

Дополнительные окна запросов

Помимо основных Окон и окон Настроек (они рассмотрены в подразделе 3.2), в ряде случаев DrWeb32W выдает дополнительные окна запросов, в которых пользователь запрашивается о допустимости или необходимости тех или иных действий программы.

Запрос рис. 4 возникает при выборе ***Файл — Проверить путь*** или аналогичных действиях поль-

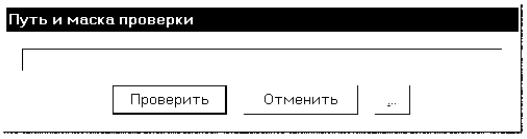


Рис. 4. Запрос выбора пути в DrWeb32W

зователя. В ответ можно в окне вручную набрать на клавиатуре требуемый путь (либо, нажав крайнюю правую кнопку, открыть окно с деревом каталогов и указать нужный путь, действуя мышью) и нажать кнопку ***Проверить***.

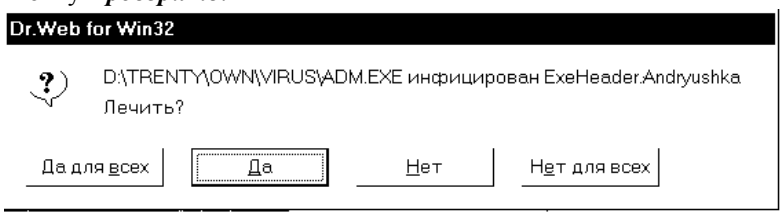


Рис. 5. Запрос подтверждения действия в DrWeb32W

Запрос рис. 5 возникает, если в панели настроек ***Действия*** установлен ***Запрос подтверждения***. Такой запрос инициируется каждым найденным инфицированным или подозрительным объектом. Ответы ***Да для всех*** и ***Нет для всех*** подразумевают как ответ на заданный запрос о конкретном проверяемом объекте, так и ответы на все последующие возможные запросы того же типа *в данном цикле проверки*. Ответы ***Да*** и ***Нет*** имеют смысл только для конкретного проверяемого объекта; о возможных остальных объектах последуют самостоятельные запросы. Аналогичные окна запросов возникают для действий ***Удалить, Переместить*** и прочих предусмотренных.

Запрос рис. 6 возникает после проверки очередной дискеты, если в панели настроек ***Действия*** стоит флаг ***Проверка нескольких дискет***. Аналогичные запросы типа ***Да*** — ***Нет*** возникают и в других случаях, например, при приказе очистить список отчета.

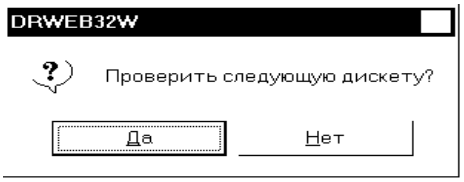


Рис.6. Запрос дискеты в DrWeb32W

Есть ряд запросов, выдающихся при некорректном использовании программы (например, некорректно заданном пути к вирусным базам). Эти запросы могут быть выданы на английском языке и здесь не рассматриваются.

Предупреждение об истечении срока действия (**expired**) ключа одновременно означает переход программы к работе в ознакомительном режиме — без лечения или каких-либо иных действий с зараженными объектами, без проверки упакованных файлов и т.д.

3.2. Настройка работы DrWeb32W

Вызвав в Основном окне ***Настройки — Изменить установки***, либо нажав <**F9**>, либо щелкнув по изображению отвертки, попадаем в первую из Панелей настроек (рис. 7) программы DrWeb32W. Щелкая по заголовкам панелей, можно выбрать любую из 8 панелей. В процессе работы с панелями можно в любой из панелей щелкнуть по одной из клавиш внизу:

— ***OK*** для фиксации сделанных изменений на текущую сессию (до выхода из программы) и выхода в Основное окно;

— ***Отмена*** для сброса всех сделанных изменений и выхода в Основное окно;

— ***Применить*** для фиксации уже сделанных изменений (если их нет, эта кнопка недоступна) и продолжения работы с настройками;

— ***Справка*** для вызова контекстной помощи из Help-файла.

Панель *Проверка*

Здесь определяются проверяемые по умолчанию[1] диски и опции

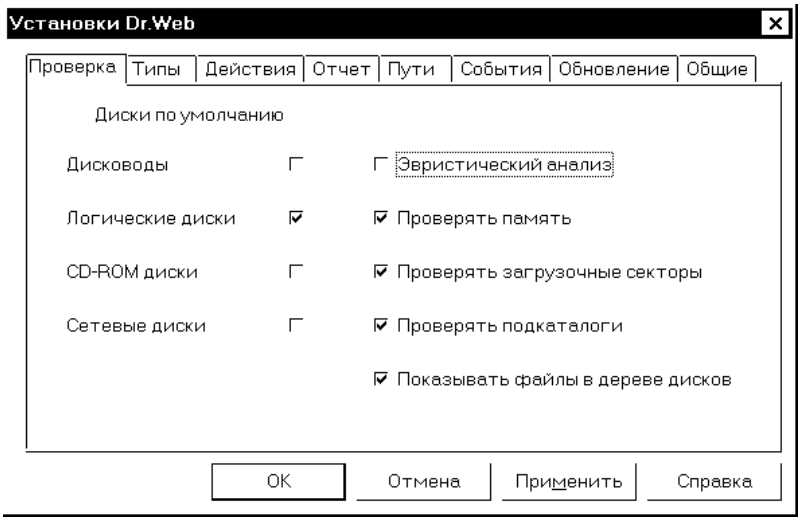


Рис. 7. Панель настроек ***Проверка*** программы DrWeb32W

проверок. В левой части панели перечислены типы проверяемых дисков, от ***Дисководов*** до ***Сетевых***. Простановка флажков в этих

[1]) Т.е. при вызове программы с параметром “*” в командной строке.

полях включает в проверку все диски соответствующих типов. Так, флажок в поле ***Логические диски*** включит при вызове с параметром "*" в командной строке все HDD-тома данного ПК.

Группа полей справа задает различные условия сканирования.

Флаг в поле ***Эвристический анализ*** заставляет DrWeb все проверяемые объекты пропускать через эвристический анализатор (см. описание в начале раздела). Естественно, достоверность такого выявления отлична от 100%, и имеет смысл вести речь о "подозрительных" файлах. На ПК со слабыми процессорами этот блок может заметно увеличить время сканирования.

Флаг в поле ***Проверить память*** заставляет программу в начале каждого очередного цикла проверки исполнять проверку памяти.

Смысл опций ***Проверять загрузочные секторы*** и ***Проверять подкаталоги*** очевиден.

Флаг в поле ***Показывать файлы в дереве дисков*** дает разрешение показа файлов в дереве дисков Основного окна.

Панель *Типы*

Здесь задается принцип отбора файлов для антивирусной проверки при сканировании. Из четырех основных режимов следует избрать один (по умолчанию избирается и рекомендуется ***По формату***), дополнив его при необходимости проверкой файлов в архивах и проверкой упакованных программ.

Вариант ***Все файлы*** задает, естественно, сплошную проверку всех файлов в области сканирования. Помимо начальной сплошной проверки ПК при установке антивирусных средств и случаев периодической профилактики, вряд ли такой выбор оправдан: на практике он приводит к чересчур большому времени проверки.

Вариант проверки ***По формату*** означает, что сканер автоматически определяет формат каждого сканируемого файла *независимо от его имени и расширения*, и далее решает самостоятельно, нужно ли проводить его проверку. Именно этот тип отбора общеупотребителен при сплошном сканировании в обычных целях.

При выборе варианта проверки ***Выбранные типы*** (кстати**,** именно этот выбор сделан на рисунке 8 в целях иллюстрации усложненных конструкций отбора) следует явно указать *расширения имен файлов*, по которым будет проверка. Как видно из рисунка, при таком выборе предлагается некоторый начальный список расширений,

который можно редактировать добавлением или исключением нужных расширений (назначение кнопок тривиально, кнопка ***Базовый*** восстанавливает базовый список при неудачных действиях пользователя). Разрешается использовать wild-символы “**?**” и “*****”.

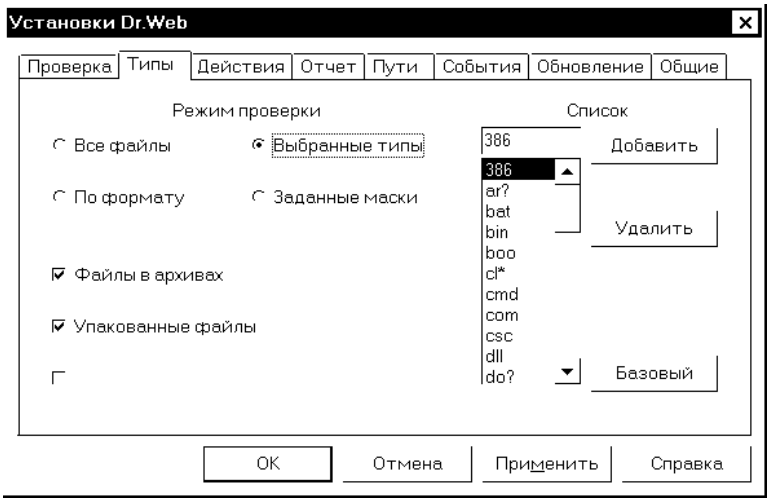


Рис. 8. Панель настройки ***Типы*** программы DrWeb32W

Вариант ***Заданные маски*** усложняет предыдущий дополнительной возможностью задания масок не только для расширений, но и для *имен* файлов списка.

Опция ***Файлы в архивах*** при включении разрешает проверять содержимое архивных файлов. Особо отметим, что при основных типах отбора по типу или маске для проверки архивов недостаточно включить комбинацию **ARJ** (или, соответственно, ***.ARJ**) в список, необходимо еще и выставить этот флаг. Разумеется, на проверку архивов тратятся дополнительные ресурсы времени и виртуальной памяти.

Опция ***Упакованные файлы*** требует, при обнаружении паковки исполняемого файла одним из известных программе DrWeb упаковщиков (полный список см. на стр.50), исполнения распаковки перед проверкой на зараженность. Такие проверки также требуют дополнительных ресурсов, но в значительно меньшем объеме, чем при проверке архивов. Рекомендуется эту опцию включать.

Опция ***Почтовые файлы*** к моменту написания данной книги пока не реализована.

Панель *Действия*

Именно здесь определяются действия DrWeb32W с обнаруженными объектами. Выше в разделе 2.1 говорилось о том, что возможность излечения вредоносных программ есть не всегда. Кроме того, наличие эвристического анализатора дает, кроме излечимых и неизлечимых, еще и класс "подозрительных" файлов. Именно в данной панели настройки задаются действия программы DrWeb32W для объектов *всех трех указанных классов,* выделяемых в процессе сканирования. Соответственно, основная часть этой панели должна быть заполнена пользователем три раза для всех трех типов файлов, указанных кнопками вверху панели. Разумеется, при выборе нужного класса набор разрешенных действий несколько меняется: вариант ***Вылечить*** для неизлечимых, скажем, файлов попросту недоступен.

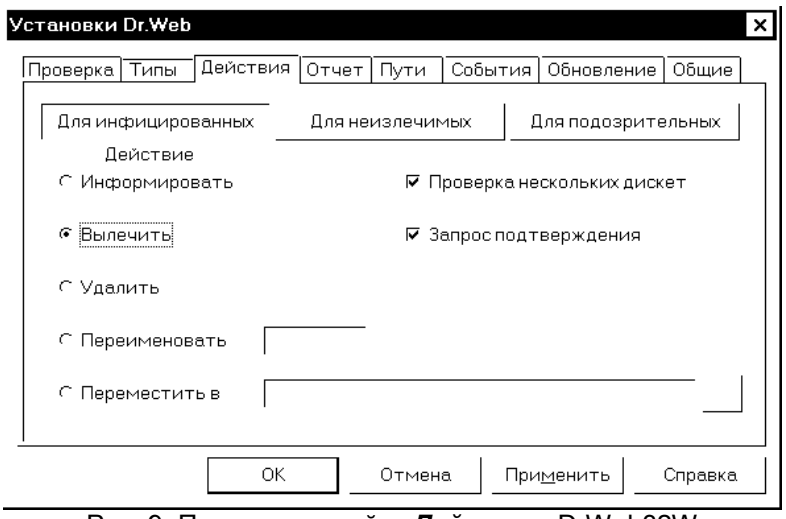


Рис. 9. Панель настройки ***Действия*** DrWeb32W

Список возможных реакций на объекты включает варианты:

Информировать — т.е. не предпринимать никаких действий, кроме фиксации в отчете и Окне результатов работы;

Вылечить — понятно, для излечимых зараженных программ;

Удалить — не действует, разумеется, для Boot-секторов;

Переименовать — при выборе этого варианта в окне правее нужно задать новое расширение имени файла, которое получит объект (по умолчанию предлагается **#??**, т.е. первый символ исходного рас-

ширения файла меняется на диез);

Переместить в — при выборе этого варианта в окне правее нужно задать имя папки, в которую перемещаются объекты (по умолчанию предлагается **Infected.!!!**, т.е. в такой подкаталог будет перемещен объект из того места, где находится — впрочем, если это не устраивает, то нажатием расположенной справа от окна имени папки browse-кнопки можно явным образом задать любую из имеющихся папок на любом диске, доступном по записи).

Следует оговориться, что в качестве альтернативного расширения имени при переименовании не стоит избирать очень уж отличающиеся от исходного значения. Безусловно не стоит избирать стандартные (EXE, COM, BAT, DOC, PAS, BAS и пр.).

Если при указании имени папки перемещения для нее не задан полный путь, начиная с имени диска, то такая папка создается в каталоге, из которого запущен DrWeb.

Две дополнительные опции в правой части панели имеют отношение ко всем типам объектов сразу, т.е. их достаточно указать один раз на этой панели. А именно,

— флаг ***Проверка нескольких дискет*** при его включении заставит по окончании проверки очередной дискеты выдать запрос, показанный на рис. 6;

— флаг ***Запрос подтверждения*** при его включении заставит DrWeb по каждому действию, которое программа собирается провести с объектом, выдать специальный запрос типа показанного на рис. 5 (см. примечание на стр. 29 по ответам на такой запрос).

Панель *Отчет*

Здесь определяются детали формируемого программой DrWeb32W отчета. Он будет вестись на диске, если в поле ***Вести файл отчета*** проставлен флаг. Отчет будет содержать информацию о зараженных, излеченных и прочих файлах, а также другую служебную информацию. Имя этого файла указывается в поле ниже, причем для гарантии места его размещения *следует указать полный путь* (иначе в версии 4.17, к примеру, отчет будет вестись в каталоге запуска программы, что в некоторых случаях может быть неприемлемым).

Режим открытия отчета позволяет указать, нужно ли при каждом новом вызове (сессии) программы формировать файл отчета заново (затирая предыдущий), либо можно пополнять существующий

файл. В случае пополнения допускается указать ***Предельный размер файла отчета*** в килобайтах. В этом случае при превышении предельного объема отчет в начале очередной сессии будет очищен.

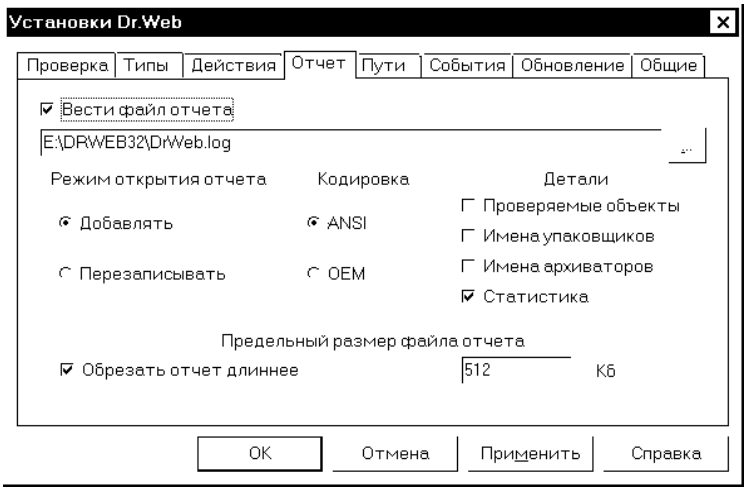


Рис. 10. Панель настройки ***Отчет*** DrWeb32W

Кодировка отчета определяет для версии с поддержкой русского языка, будет ли он писаться в кодировке 866-й страницы DOS (**OEM**) или Windows-1251 (**ANSI**).

Группа ***Детали*** задает полноту отчета как перечень включаемых в него элементов.

Флаг в поле ***Проверяемые объекты*** заставит включать в отчет все проверенные объекты, а не только зараженные и подозрительные.

Флаг в поле ***Имена упаковщиков*** включает занесение в отчет имен программ (LZEXE, PKLITE и др.), посредством которых были сжаты проверяемые исполняемые файлы.

Флаг в поле ***Имена архиваторов*** включает занесение в отчет имен программ (PKZIP, RAR и др.), посредством которых были созданы проверяемые архивы, а также тексты возможных ошибок, связанных с использованием архиваторов.

Флаг в поле ***Статистика*** заставляет DrWeb32W помещать в отчет по окончании очередного сканирования и по всему сеансу работы статистическую информацию о проверенных объектах.

Панель *Пути*

Здесь можно задать пути к исключаемым из проверки каталогам, а также вирусным базам DrWeb32W.

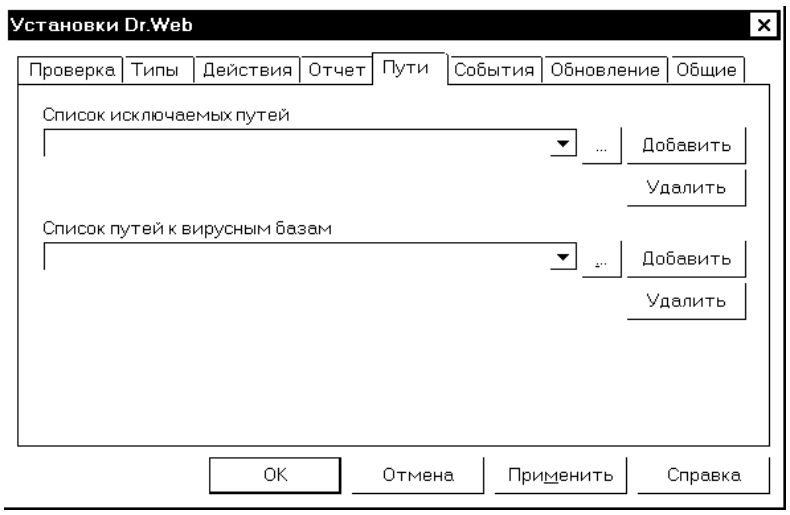


Рис. 12. Панель настройки ***Пути*** DrWeb32W

В верхней половине панели можно задать пути к каталогам, файлы в которых проверяться не будут даже в том случае, когда содержащее их устройство включено в проверку. Пути задаются их конкретным перечислением в списке. Первоначально список пуст; но введя некоторый путь вручную с клавиатуры или выбрав его мышкой с помощью browse-кнопки справа от списка, его можно включить в список нажатием на кнопку ***Добавить***. Исключить путь из списка можно, выбрав нужный в общем списке (для этого, по традициям Windows, достаточно нажать кнопку с треугольничком справа от окна пути) и нажав кнопку ***Удалить***.

В нижней части панели можно задать пути к каталогам с вирусными базами и расширение имен этих баз. Эта возможность предусмотрена, к примеру, для пользователей надежно функционирующих локальных сетей, когда часто получаемые дополнения к вирусным базам держатся на файл-сервере в специальном каталоге. Метод включения/исключения путей аналогичен описанному выше для исключаемых из проверки каталогов.

Следует с осторожностью пользоваться возможностью замены расширений вирусных баз: стандартное расширение **.VDB** вряд ли будет изменено авторами. Возможность дана на случай появления вирусов, специфически направленных против файлов с таким расширением. При замене стандартного расширения часть возможностей (например, обновление) может перестать работать.

Панель *События*

Здесь можно задать звуковые эффекты для DrWeb32W. Это имеет смысл, если ПК снабжен звуковой картой. Стандартный комп-

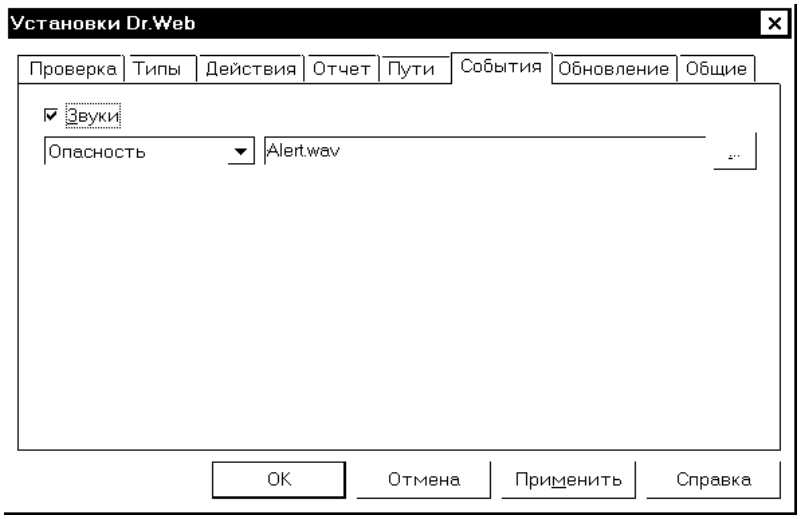


Рис. 13. Панель настройки ***События*** DrWeb32W

лект поставки предусматривает свои звуки для семи типовых ситуаций: **Опасность, Исцелен, Удален, Переименован, Перемещен, Финиш** и **Ошибка.** В комплект поставки входят 7 простых WAV-файлов под эти ситуации. Кнопка тестового прослушивания на панели почему-то не предусмотрена, но их легко воспроизвести **Универсальным проигрывателем** Windows.

Поставив общий флаг в поле ***Звуки*** и включив тем самым работу со звуковой картой, можно затем назначить стандартным ситуациям (выбираются в левом окне) выбранные Вами звуковые файлы (выбираются в правом окне).

Панель *Обновление*

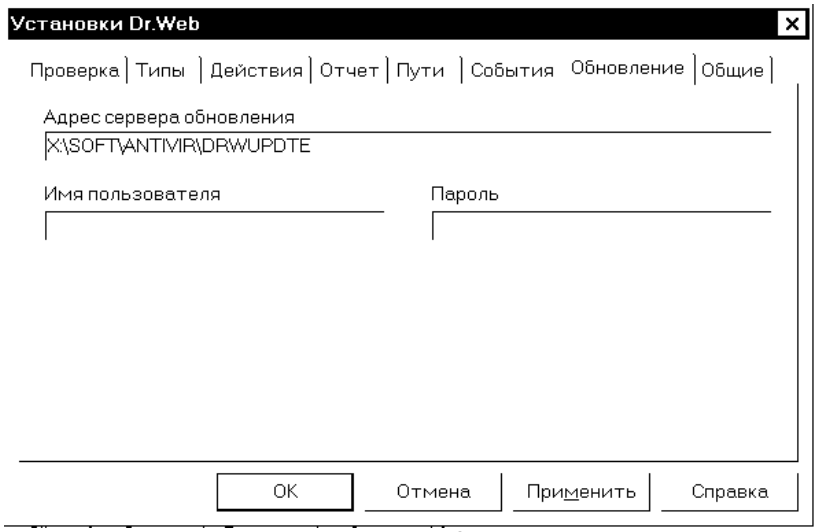


Рис. 14. Панель настройки ***Обновление*** DrWeb32W

Здесь можно задать параметры для программы DRWUPW.EXE обновления DrWeb. В общем случае, заполняются поля ***Адрес сервера, Имя пользователя*** и ***Пароль***.

Подсистема обновления обеспечивает автоматическую доставку и установку всех компонентов пакета, включая программные модули, вирусные базы, файлы помощи и документы. Подсистема работает на базе специально подготовленного текстового файла DRWEB32.LST, содержащего перечень удаляемых и новых файлов каталога. Отчет о работе подсистемы обновления накапливается в файле **DrUpdate.log**. По каждой версии список файлов с их контрольными суммами (CRC32) готовится разработчиком.

Для использования подсистемы обновления в локальной сети нужно в поле адреса сервера обновления прописать путь к файл-серверу с нужным каталогом (пример дан на рис. 14).

Вместо имени локального ресурса в этом поле можно дать адрес сетевого ресурса, напр. **\\NT_SERVER\DRWEB\UPDTE**.

Разрешается также использовать http для обновления через Интернет. По умолчанию при поставке это поле настроено на некоммерческий раздел обновления **HTTP://WWW.DIALS.RU/FREE**; для ра-

боты с коммерческими версиями необходимо указать вместо раздела **/FREE** раздел **/ENGLISH** (одноязычный вариант поставки), **/RUSSIAN** (двуязычный вариант) или **/FULL** (максимальный вариант), причем обязательно заполнить поля ***Имя пользователя*** и ***Пароль*** выданными при покупке лицензии значениями.

Ко времени подготовки данной работы к печати, LST-файлы готовятся в расчете только на полный вариант установки: DrWeb32W, DrWebWCL, DrWeb386 и SpIDER Guard, причем предусматривается обновление любой предшествующей коммерческой версии. Полагаю, в организациях с достаточным числом пользователей реальную связь с коммерческим отделом ДиалогНауки должен осуществлять один человек, системный администратор, готовящий данные в соответствующем каталоге (одном или нескольких) файл-сервера для всех остальных.

Панель *Общие*

Здесь задается ряд общих параметров работы DrWeb32W.

Флаг ***Автосохранение установок при выходе*** включает автоматическое сохранение всех настроек текущего сеанса работы DrWeb32W по окончании работы программы в INI-файле.

Следует с осторожностью пользоваться этой возможностью на ПК, где работает более одного человека: коллеги могут оказаться не готовы к тому, что после того, как Вы поменяли все установки, Windows перестал загружаться (например, если вместо лечения зараженных файлов задано перемещение их в какую-либо недоступную другим папку, и туда попал зараженный Internet Explorer по приказу на отложенное лечение после очередного рестарта...).

Флаг ***Использовать установки из реестра*** на самом деле означает фиксацию в реестре Windows местоположения окон программы DrWeb32W при ее вызове и связанные с этим параметры.

В нижней части панели можно отрегулировать приоритет исполнения сканирования программой DrWeb32W по отношению к другим приложениям Windows. Чем больше данный приоритет, тем быстрее будет работать программа (и тем значительнее будет она “притормаживать” другие программы).

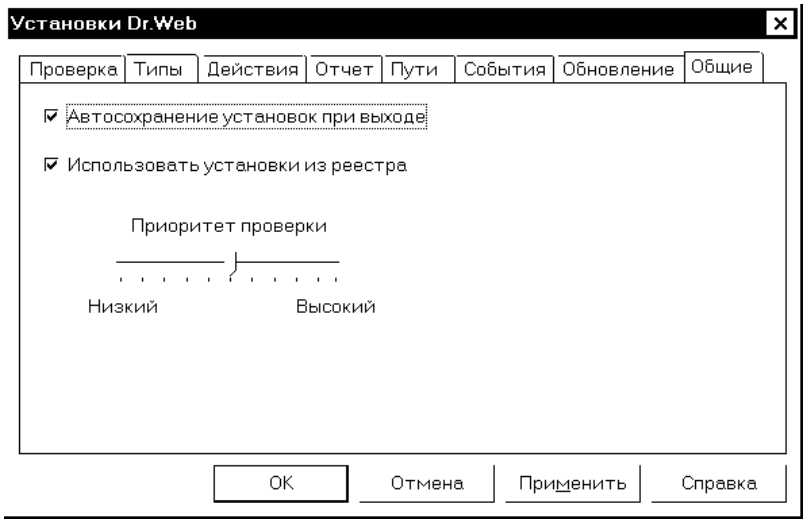


Рис. 15. Панель настройки ***Общие*** DrWeb32W

При использовании сканирования в сочетании с другими приложениями (чего, вообще-то, лучше не делать без особой нужды) возможно, придется отрегулировать приоритет так, чтобы осуществлялось желаемое соотношение скоростей работы приложений.

3.3. Инсталляция DrWeb32W

Как уже говорилось, Doctor Web для Windows может поставляться в одноязычной с встроенным английским языком или двуязычной версии. Во избежание непонимания сообщений инсталлятора, следует во всех случаях инсталлировать версию на языке, совпадающим с языком выбранной версии Windows.

Как русская, так и английская версии выпускаются поставщиком в двух вариантах: одним файлом довольно значительного объема (около 4 Мб), либо подразделенным на несколько образов дискет, архивированных PKZIP. Во втором случае перед инсталляцией необходимо предварительно распаковать образы дискет и переписать каждый из них на дискету или в каталог **INSTALL.** В организациях с наличием файл-серверов создание необходимых каталогов и ведение версий в них обычно выполняет централизованная служба.

Подготовка

Поскольку операционная обстановка на каждом ПК может иметь индивидуальные особенности, перед инсталляцией необходимо найти ответ на ряд нижеследующих вопросов.

* Соответствует ли версия Windows последним рекомендациям ее разработчика? (Если нет — необходимо выполнить эти рекомендации. Так, если версия системного модуля **COMCTL32.DLL** в папке \WINDOWS\SYSTEM имеет дату образования ниже 11/1996 — нужно обновить этот модуль, причем сделать это в специальном режиме, например, загрузившись в “старой” версии MS-DOS или вообще с загрузочной дискеты, т.к. обновить этот модуль в обычном режиме Windows’95 попросту не даст!)

* Свободен ли ПК от каких-либо версий DrWeb для DOS? (Если нет — лишнее лучше удалить во избежание путаницы).

* Свободен ли ПК от ранее установленных DrWeb32 предыдущих версий? (Если нет — деинсталлировать их: освободится место. Исключением является апгрейд версий, которые его допускают, но тут и требуется не инсталляция новой, а апгрейд старой версии).

* Отсутствуют ли на Вашем ПК какие-либо программные или аппаратные средства, препятствующие нормальной работе сканера антивирусов? (Таковыми могут быть плата **Sheriff** фирмы “Диалог-Наука”, различные резидентные программы, контролирующие работу файловой системы, в особенности сторожа альтернативных фирм, перехватывающие управление при проверках файлов. Ярким при-

мером является **Norton Unerase Wizard** из Norton Utilities for Windows, который "из лучших побуждений" запретит лечение зараженных файлов в защищенной корзине). Если таковые на Вашем ПК есть — необходимо отключить соответствующие аппаратные и деинсталлировать программные средства. Между прочим, это относится и к **SpIDer Guard**, который в ряде режимов затормозит сплошную проверку диска).

* Имеется ли достаточно места на том локальном диске, куда планируется установить DrWeb? (Это должен быть локальный диск, с которым исполняется активная работа с поддержкой длинных имен в версии Windows, но в то же время диск, который доступен во всех профилях работы оборудования всем пользователям — например, у автора этих строк таковым является диск **E:**, доступный для Windows'98 и Windows'NT[1]).

* Отсутствуют ли логические ошибки на локальном диске установки и рабочем локальном диске? (Если уверенности нет, запустите ScanDisk для этих томов. Вообще-то, это надо делать регулярно...).

* Является ли комплектация Вашего ПК соответствующей требованиям DrWeb32W? (На ранних видеокартах, сделанных на чипе S3, попытка проверки памяти программой DrWeb32W приводила к жесткому "зависанию" ПК. С версии 4.12a авторы включили "обход" проверки памяти драйверов видеокарт. Однако категорического вывода о полном устранении проблемы делать нельзя: кто знает, какие драйверы и к каким устройствам появятся? Внимательно просмотрите сопроводительную документацию или сообщения на сайте!). Если тут есть сомнения, выполните принудительную дефрагментацию локального диска установки и рабочего диска, что позволит сохранить возможность "отката" при жестком повисании компьютера.

* Готов ли нужный вариант дистрибутива к установке? (Читаются ли полностью дискеты при установке с них, либо уверены ли Вы в доступности сервера при установке с сервера?)

[1]) На моем ПК установлены MS-DOS 6.22 (диск **C**:), Windows 3.11 (диск **D:**), Windows'98 (диск **E:**), UNIX и Windows'NT; имеется сменный HDD, при подключении которого в DOS и '98 меняются.имена логических дисков, а также, в некоторых вариантах загрузки MS-DOS, виртуальный диск. Через сетевую карту в '98 видно 4 тома файл-серверов, в DOS в зависимости от входа — от 0 до 4. В этом и подобных случаях правильный выбор диска установки DrWeb32W отнюдь не является тривиальной задачей.

* Готов ли Ваш ПК к неожиданным отключениям питания? (Если нет — задействуйте на время установки UPS или постарайтесь, по крайней мере, проверить, не болтается ли вилка питания в розетке и не собираются ли отключать свет / натирать полы / завершать работу и закрывать помещение в ближайшее время).

* Готовы ли Вы к требованию перезагрузить Windows? Закрыты ли все 32-битные приложения и, отдельно, документы? (Если нет — закройте, иначе это будет препятствовать лечению вирусов, если они есть, и макровирусов в открытых документах).

Представляется важным настоятельно рекомендовать следовать *всем* вышеприведенным советам. Скептикам, усматривающим мрачную юмористичность некоторых из них, я на основании собственного опыта нескольких сотен инсталляций могу сообщить, что **все** мои рекомендации следуют из повседневной практики.

При установке DrWeb на ПК совместно с ADinf32, первой из них рекомендуется устанавливать DrWeb. Этим Вы сэкономите силы на настройках их совместной работы.

Собственно инсталляция

Для последующей корректной работы всех программ комплекта Doctor Web для Windows следует соблюсти ряд правил.

* Если имеете коммерческий ключ, действующий для очередной версии — сохраните его где-нибудь, помимо папки, в которую Вы будете устанавливать Doctor Web.

* Устанавливайте программу в первый после корня каталог, т.е. в **C:\DRWEB32**, а не в рекомендуемый каталог **C:\Program Files\...** При “падении” Windows Вам может понадобиться DrWeb386, а многие DOSовские “коммандеры” не умеют спускаться в подкаталоги с длинными русскими именами. Потом, именно в этом каталоге будет формироваться отчет, и, возможно, Вам захочется посмотреть его, загрузившись в DOS, в тот момент, когда Windows уже “упадет”...

* Если у Вас недостаточно мощный ПК — не используйте входящий в комплект поставки сторож SpIDer (для его исключения нужно выполнить ряд специфических действий, описываемых ниже). Обратите внимание: SpIDer пока еще не приспособлен для NT-серверов!

* Даже среди корректно и надежно работающих опций выбирайте те, которые рекомендованы ниже, пока не освоитесь полностью с работой программ.

Инсталлятор комплекта DrWeb32 предлагает варианты установок: **Типичная**, **Минимальная** и **Выборочная**. В **Минимальной** конфигурации присутствуют: DrWeb32W (около 1 Mb), SpIDer (0.5Mb), русский язык (для двуязычной поставки). В **Типичной** конфигурации добавлен еще и DrWeb386 (0.5 Mb). Только **Выборочная** конфигурация позволяет исключить при установке SpIDer.

Ниже описаны пронумерованные этапы установки программы.

0. Имя стартовой программы зависит от выбора дистрибутива. Для многодискетного дистрибутива это **SETUP.EXE** на первой дискете. Для единого дистрибутива это — имя его файла.

1. Запустив стартовую программу, ответьте согласием на лицензионное соглашение и установите каталог **$:\DRWEB32**, где '**$**' - буква вашего *локального* диска (т.е. относящегося к винчестеру Вашего ПК и выбранного Вами в соответствии с рекомендациями выше).

2. Из возможностей инсталляции выберите ***ВЫБОРОЧНАЯ***, войдите в список инсталлируемых программ и уберите, если надо, пометки напротив DrWeb386, DrWebWCL и SpIDer'a.

3. При выборе группы для установки можете оставить ***DrWeb***, но не ставьте группу ***Стандартные*** или какую-либо иную уже существующую: могут быть сложности с исполнением **Uninstall**. Значок программы DrWeb всегда попадет на Desktop.

4. Доведите установку до последнего экрана, прочтите или откажитесь от README и согласитесь с вызовом DrWeb32W. Либо вызовите DrWeb32W щелчком по его иконке на рабочем столе.

5. Нажмите на изображение отвертки, либо в меню ***Настройки*** выберите ***Изменить установки*** и, гуляя по панелям установок, сделайте установки, как подробно пояснено ниже.

Панель ***Проверка***: в блоке ***Диски по умолчанию*** убедитесь, что галочка стоит только против ***Логические диски***; в блоке справа включите все опции (про эвристический анализатор решайте сами).

Панель ***Типы***: установите тип проверки файлов ***По формату*** или (если не жалко времени) ***Все файлы***, проверьте наличие галочек в режимах ***Файлы в архивах*** и ***Упакованные файлы***.

Панель ***Действия***: ***Для инфицированных*** установите ***Вылечить***, теперь нажмите ***Для неизлечимых*** и выберите ***Удалить***. Флаг ***Проверка нескольких дискет*** поставьте по вкусу, флаг ***Запрос подтверждения*** новичкам лучше оставить, остальным можно отключить.

Панель ***Отчет***: обязательно проставьте флаг против ***Вести файл отчета***. Нажмите browse-кнопку просмотра каталогов справа от окна с именем файла отчета и добейтесь, чтобы там был указан путь отчета (напр., **$:\WORK\DrWeb.log**) к доступной по записи папке (проще всего — к папке **DRWEB32**, если Вы следовали прошлым советам). Вникните в смысл остальных опций и поставьте то, что считаете нужным. Удобно дозаписывать отчет, ограничив его объем размером 512Кб, включая в отчет имена архивов и упаковщиков, но исключая имена проверяемых программ. Любителям NC, VC и прочих DOSовских средств просмотра файлов лучше оставить отчет в кодировке MS-DOS (**OEM**), прочим следует выбрать **ANSI**.

Панель ***Пути***: не трогайте, оставив пути пустыми.

Панель ***События***: включите ***Звуки,*** только если на Вашем ПК имеется звуковая карта, она исправна и подключен соответствующий драйвер. Критерий проверки: при старте и завершении Windows Вы слышите нормальные проигрыши.

Панель ***Обновление***: не трогайте вообще, пока не научитесь уверенно работать с программой. При наличии файл-сервера и соответствующей службы пользуйтесь ее рекомендациями.

Панель ***Общие***: галочку лучше не ставить в ***Автосохранении при выходе***, но оставьте в ***Использовать установки из реестра***.

После всех установок нажмите OK, в ниспадающем меню выберите ***Установки —> Сохранить установки***.

После выполнения инсталляции можно дополнительно сформировать ярлык Помощи на рабочем столе, например, с помощью **Проводника**, для файлов **RussianD.hlp** и **RussianS.hlp**.

Пополнение вирусных баз

При получении информации об очередном вышедшем дополнении антивирусной базы к установленной версии (имена файлов имеют вид DRWxyyzz.VDB, где **xyy** — номер версии и релиза; **zz** — порядковый номер дополнения к базе), перепишите файл в каталог с остальными файлами DrWeb32. Файл DRWxyyzz.TXT — информационный, его переписывать не обязательно.

Деинсталляция

Деинсталлировать установленную программу DrWeb32W можно двумя способами: через меню Windows ***Пуск — Настройка — Установка и удаление программ;*** либо через пункт ***Uninstall*** в груп-

пе, в которой установлен DrWeb32W, если в той же группе не было установки программ других комплектов, использующих **InstallShield**.

После исполнения, возможно, потребуется удалить элементы реестра типа **HKEY_CURRENT_USER\SOFTWARE\IDAVLab\....** или **HKEY_LOCAL_MACHINE\Software\DialogueScience\DrWeb***. Первый из списков нужно удалить *для каждого* пользователя. Проверьте также: возможно, в каталоге, где находился DrWeb, остались неудаленные старые дополнения к вирусным базам, отчет, коммерческий ключ и иные модули.

3.4. Командная строка запуска Doctor Web-32

Командная строка для запуска программ DrWeb32W, DrWebWCL и DrWeb386 имеет вид:

программа [диск:[путь]] [...] [ключи]

где

программа	– имя исполняемого модуля
диск:	– логический том жесткого диска, сетевой диск, CD-ROM, флоппи-дисковод или ***** (ряд логических устройств, см. панель ***Проверка***).
путь	– указание точного пути к файлам для проверки. В командной строке может содержаться несколько параметров **диск:[путь]**, тогда соответствующие объекты сканируются последовательно. По окончании обработки всех объектов DrWebWCL и DrWeb386 завершают свою работу, а DrWeb32W, если не задан ключ **/QU**, выходит на Основное окно, в котором можно задать новые объекты сканирования, просмотреть результаты и др. Если при запуске DrWeb32W этот параметр не указан, то программа сразу выходит на Основное окно (после проверки памяти, если это задано ключом или в INI-файле).
Ключи (дополнительные параметры) командной строки	
/@[+]<файл>	– имя файла, полученного от ревизора ADinf со списком файлов, требующих последующей проверки сканером. По окончании проверки DrWeb удаляет файл со списком. Вы можете сохранить этот файл, указав необязательный **"+"**. При взаимодействии с ADinf32, подстановка этого ключа и вызов Doctor Web производится автоматически (см. настройки в описании ADinf32).
/AL	– отбор для проверки всех файлов на заданном устройстве.
/AR[N][-]	– проверка файлов, находящихся внутри архивов. Дополнительный параметр **N** блокирует вывод имени программы-архиватора после имени

	архивного файла в отчете и на экране. Отрицательная форма запрещает проверять архивы.
/DA	– тестировать компьютер один раз в сутки. Для данного режима необходимо наличие файла конфигурации (.INI), в который записывается дата следующей проверки. Режим рекомендуется при вызове DrWeb386 из AUTOEXEC.BAT; при совместной работе с ADinf32 режим не нужен.
/EX	– проверка файлов с расширениями, стандартными для исполняемых модулей, документов и таблиц MS Office (т.е. только с расширениями **COM, EXE, SYS** и др., полный список см. в начале INI-файла или в сопровождающей документации).
/FM	– проверка файлов по внутреннему формату исполняемых модулей. Независимо от расширения проверяются файлы, имеющие внутреннюю структуру исполняемых программных модулей, а также "макросодержащих" документов MS Word и электронных таблиц MS Excel.
/FN[-]	– загружать русские буквы в знакогенератор видеоадаптера (только для DrWeb386).
/GO	– программа не ожидает подтверждения пользователя при выполнения различных операций (нехватка места на диске при распаковке, неверные параметры в командной строке, заражение программы Doctor Web неизвестным вирусом, удаление поврежденных файлов,...). Этот режим полезно использовать для проверки файлов в автоматическом режиме, например, при круглосуточной проверке электронной почты на сервере.
/HA[-]	– эвристический анализ файлов; отрицательная форма — запрет эвристического анализа.
/NI	– не использовать параметры, записанные в конфигурационном файле программы (.INI).
/LNG[:<путь>]	– использовать альтернативный файл языковых ресурсов (.DWL) с заданным именем и/или

	путем, либо использовать английский язык.
/INI:<путь>	– использовать альтернативный INI-файл с указанным именем и/или путем.
/NS	– запретить возможность прерывания проверки компьютера. После указания параметра **/NS** пользователь не сможет прервать работу программы по нажатию клавиши <Esc> (данный ключ не работает для DrWeb32W).
/OK[-]	– выводить полный список сканируемых объектов, сопровождая незараженные пометкой "**Ok**"; отрицательная форма — не выводить информацию о незараженных объектах.
/PF[-]	— запрашивать подтверждение на проверку следующей дискеты.
/PR[-]	— запрашивать подтверждение при действиях с зараженными и подозрительными файлами.
/QU	—завершить работу после исчерпания списка проверки (только для DrWeb32W).
/RP[+]<файл>	– записать отчет о работе программы в файл, имя которого задается дополнительным параметром **<файл>**. По умолчанию используется файл с именем DRWEB32W.LOG, DRWEBWCL.LOG или DRWEB386.LOG (соответственно запущенной программе). Если указан дополнительный знак "+", то отчет дописывается в конец существующего файла.
/NR	– не создавать файл отчета.
/SD[-]	– проверять/не проверять подкаталоги.
/SO[-]	– включить/выключить звуковое сопровождение.
/SS[-]	– по окончании работы сохранить режимы, заданные в текущем запуске программы, в INI-файле.
/TB[-]	– выполнять/нет проверку загрузочных секторов и главного загрузочного сектора.
/TM[-]	– выполнять/нет поиск вирусов в оперативной памяти, включая системную область Windows (для DrWeb32W и DrWebWCL).

/UP[N][-]	– проверка выполнимых файлов, упакованных программами ASPACK, COMPACK, DIET, EXEPACK, LZEXE, OPTLINK, PEPACK, PGMPAK, PKLITE, WWPACK, WWPACK32, UCEXE, UPX; файлов, преобразованных программами BJFNT, COM2EXE, CONVERT, CRYPTCOM, CRIPTEXE, PECRYPT, PESHIELD, PROTECT, TINYPROG; а также файлов, иммунизированных вакцинами CPAV, F–XLOCK, PGPROT, VACCINE. Чтобы Doctor Web не отображал на экране название программы, использованной для упаковки, преобразования или вакцинирования проверяемого файла, укажите дополнительный символ **N**. Отрицательная форма: не выполнять проверку упакованных файлов.
/CU[RDM][P] **/CU-**	– лечение файлов и системных областей дисков, удаление найденных вирусов. Можно указать дополнительные параметры: **"–"** – только выводить отчет, **R** – переименовывать (по умолчанию, первая буква расширения файла заменяется на “#”), **D** – удалять, **M** – перемещать (по умолчанию, в подкаталог **INFECTED.!!!**), **P** – перед действием выводить запрос.
/SP[RDM][P] **/SP-**	– что делать с подозрительными файлами: **"–"** – только выводить отчет, **R** – переименовывать, **D** – удалять, **M** – перемещать, **P** – перед действием выводить запрос.
/IC[RDM][P] **/IC-**	– что делать с файлами, вылечить которые невозможно: **"–"** – только выводить отчет, **R** – переименовывать, **D** – удалять, **M** – перемещать, **P** – перед действием выводить запрос.
/?	– вывод на экран краткой справки о работе с программой (DrWebWCL, DrWeb386) или запуск справочной системы (для DrWeb32W).
Из режимов **/AL**, **/EX** и **/FM** можно задать только один	
Режимы, установленные по умолчанию (при отсутствии или неиспользовании INI-файла): **/AR /FM /HA /PR /SD /TB /TM /UP**	

Режимы, установленные по умолчанию в профилях ADinf32 при вызове сканера (если не изменены при настройке ADinf32): **/AL /AR /HA /NM /SO** (параметр **/NM** эквивалентен **/TM-**)

Рис. 16. Ключи командной строки для Doctor Web-32

Реальный код завершения при завершении программ DrWeb386 и DrWebWCL может быть суммой указанных ниже кодов соответственно реально имевшей место ситуации при проверке.

0	Вирусов или подозрительных объектов не обнаружено
1	Обнаружены известные вирусы
2	Обнаружены модификации известных вирусов
4	Обнаружены подозрительные на вирус объекты
8	В архиве обнаружены известные вирусы
16	В архиве обнаружены модификации известных вирусов
32	В архиве найдены подозрительные на вирус объекты
64	Успешно выполнено лечение хотя бы одного вируса
128	Выполнено удаление/переименование/перемещение хотя бы одного зараженного файла

Рис. 17. Коды завершения у DrWeb386 и DrWebWCL

IV. Ревизор дисков ADinf32

Ревизор **Advanced Diskinfoscope**[1] предназначен для контроля изменений файловой системы на дисках. Методом ведения такого контроля являются организуемые программой справочные таблицы, в которых запоминаются данные по файлам: полное имя и местоположение, дата включения в таблицу или последнего изменения, длина и контрольная сумма.

Контрольная сумма файла — обобщенный числовой показатель, зависящий от содержимого файла. В ADinf32 используются следующие типы контрольных сумм.

Быстрые (Win32) — основаны на знании структуры исполняемых модулей (форматы **COM, MZ, NE**, **PE** и **LE**). Показатель контролирует только ту часть кода программного модуля, которая неминуемо изменится при заражении любым вирусом (при перетрансляции программы сумма этого типа может и не измениться[2]).

Макро — созданы специально для документов OLE2 (файлы типов **.DOC**, **.DOT**, **.XLS** и **.XLT**), зависят от макросредств внутри документа и некоторых формул таблиц Excel, так что при изменениях, например, основного текста документа не меняются.

CRC16, CRC32 — основаны на сплошном суммировании всего файла с длиной хэш-функции соответственно 16 и 32 бита. Большинство вирусов вызывают изменения этих сумм, хотя известны методы имитации неизменности этих показателей.

CRC48 — одновременный расчет CRC16 и CRC32.

LAN64 (доступны только в модификации ADinf-Pro) — специальный метод[3] непрямого взвешенного суммирования, гарантирующий обнаружение любых изменений в файлах.

Профиль настройки является средством организации хранения справочных таблиц и, в то же время, группы сведений об установленных режимах работы программы. Одновременно возможно (и в ряде случаев оправдано) существование нескольких различных профилей — разумеется, с разными именами. При инсталляции ADinf32 автоматически создает профиль, называемый в русской версии ***Настройки***

[1] Разработчики: *Д.Мостовой, В.Ладыгин, Д.Зуев, А.Самотохин*

[2] Например, для программ быстрая КС рассчитывается из первых 32 байт файла плюс 32 байта от точки входа.

[3] Методика —интеллектуальная собственность фирмы “ЛАН Крипто”.

по умолчанию. Версия 3.0 программы имеет возможность работы с профилями следующих типов:

— полный 32-битный, рассчитанный на максимальное управление возможностями программы по контролю файловой системы;

— упрощенный 32-битный, рассчитанный исключительно на подготовку списка файлов для проверки сканером;

— 16-битный, позволяющий готовить список файлов для проверки сканером, и в случае необходимости задействовать **ADinf Cure Module** (который до настоящего времени существует только в 16-битном варианте)[1].

При инсталляции программы профиль ***Настройки по умолчанию*** создастся в полном или упрощенном 32-битном варианте в зависимости от желания пользователя. 16-битные профили могут быть только добавлены позднее, при настройке.

Профиль работы является средством *пользователя*, т.е. два разных пользователя одного ПК могут иметь одноименные профили работы[2]. Таким образом, *каждый* пользователь при использовании ADinf32 обязан настроить свои профили сам, осуществив самостоятельный вход в Windows под своим именем.

Между прочим, из этого следует, что для автоматического запуска при загрузке создание нужного профиля и его соответствующую настройку нужно сделать *каждому* пользователю данного ПК.

Ключевой файл определяет возможности программы. С ознакомительным ключом (USEREVAL.KEY) программа работоспособна в течение ознакомительного периода (*evaluation period*) в 30 дней. Ключевой файл USERnnnn.KEY или соответствующий ему EXE-модуль должен быть получен при покупке программы. Установка ключа означает запись ключевого файла в каталог с модулями программы ADinf32, поэтому для работы нескольких пользователей с одним и тем же комплектом ADinf32 достаточно одного ключа на один ПК.

[1] Разумеется, 16- или 32-битными являются приложения, использующие профиль, но не он сам. Устоявшийся жаргон используется для краткости.

[2] Все настройки пользователя находятся в разделе HKEY_CURRENT_USER реестра, формируемого для конкретного пользователя в начале его работы и вновь запоминаемого при завершении сеанса работы.

Метод доступа (свой для каждого логического тома) определяет способ чтения диска. Поскольку ряд вирусов подменяют собой стандартные драйверы ОС или искажают результаты их работы, ADinf32 читает содержимое дисков по секторам, моделируя работу файловой службы ОС. Соответственно, метод доступа зависит от используемой ОС. ADinf32 использует следующие методы доступа.

* **BIOS** (’95, ’OSR2 , ’98) — чтение секторов осуществляется прямой передачей управления к виртуальному BIOS. Это — самый быстрый и надежный метод для большинства дисков. Он устанавливается по умолчанию для большинства дисков.

* **Int13h** (’95, ’OSR2 , ’98) — чтение секторов осуществляется передачей управления через цепочку прерывания Int13h. Этот метод используется, если для какого-либо диска метод BIOS не работает (так, для SCSI-устройств большого объема используются специальные драйверы, доступ к которым осуществляется через Int13h).

* **VWin32** (’95, ’OSR2 , ’98) — чтение секторов обращением к виртуальному драйверу соответствующей ОС, который предоставляет 32-API прямого доступа к дискам. Метод используется для доступа к уплотненным дискам и в других случаях, когда предыдущие методы почему-либо не работают.

* **Физ.диск** (’NT, ’2000) — чтение секторов обращением к драйверу физического диска. Быстрейший и надежный метод для ’NT.

* **Лог.диск** (’NT, ’2000) — чтение секторов обращением к драйверу логического диска. Устанавливается, если предыдущий метод неработоспособен.

Метод доступа определяется программой автоматически при первой попытке работы с дисками, но пользователь при настройке профиля может изменить используемый метод доступа.

Отбор дисков для ревизии из числа актуальных для данного ПК также можно изменить при настройках профилей работы. Более того, в программе существуют развитые средства определения существенных, несущественных и — особо — критических изменений как на уровне каталогов, так и на уровне отдельных файлов.

По результатам каждой проведенной ревизии можно назначить сканирование вновь образованных или измененных файлов. ADinf32 умеет взаимодействовать с DrWeb32W, DrWeb32WCL, DrWeb16, двумя вариантами AVP и McAfee Virus Scan. При создании профиля или инсталляции ADinf32 автоматически проставляет взаимодействие

с имеющимся на ПК сканером, но предложенный вариант можно изменить в настройках профиля.

Основные режимы работы ревизора ADinf32 составляют:

— режим проверки и построения таблиц;

— режим ревизии дисков по существующим таблицам;

— режим просмотра результатов ревизии (проверки).

Ясно, что для исполнения второго и третьего режимов таблицы должны быть построены ранее.

Вспомогательные режимы работы ревизора ADinf32 позволяют проследить историю изменений файлов на конкретном диске и осуществить поиск активных stealth-вирусов.

Назначение программы. При исполнении ревизии дисков моделируется структура файловой системы и фиксируются произошедшие в ней изменения. Отбор интересующих изменений хранится в настраиваемом пользователем профиле. Программа способна фиксировать:

— образование новых файлов;

— изменение даты и времени файлов;

— удаление файлов;

— перемещение файлов из одного каталога в другой;

— изменение структуры контролируемых файлов (отбор контролируемых и тип контроля определяется пользователем при настройке профиля);

— перемещение исполняемого файла в другой каталог с одновременным образованием на его месте другого исполняемого файла с тем же именем, часто являющееся следствием характерной деятельности вирусов-спутников;

— появление новых и удаление старых сбойных кластеров;

— изменение объема нижней (базовой) оперативной памяти;

— изменения в загрузочных секторах диска и в MBR;

— любые изменения в неизменяемых файлах, взятых на особый контроль (список предложен программой по умолчанию, но пользователь может этот список отредактировать при настройках профиля).

ADinf32 также исполняет сравнение считанных основным методом (с разбором секторов) файлов с теми же файлами, считанными стандартными средствами, для обнаружения расхождений, характерных при заражении stealth-вирусами.

Часть указанных выше изменений, а также любые изменения неизменяемых файлов считаются подозрительными изменениями, на которые возникает особая реакция программы. Что именно из возможного списка считать подозрительными изменениями, определяет пользователь при настройке профиля. Особая реакция предусматривает специальное сообщение по завершении обработки всех дисков.

Вызовы программы возможны в ручном и автоматическом вариантах. Автоматический вариант вызова возникает при загрузке Windows, если ADinf32 настроен на автоматическую проверку при включении ПК (дополнительно можно задать, чтобы проверка исполнялась не более 1 раза в день). Поскольку любая работа ADinf32 исполняется, как уже было отмечено, в рамках некоторого профиля, по умолчанию ADinf32 при вызове запрашивает, с каким из профилей требуется исполнять работу. Этот запрос можно исключить, установив один из профилей как исполняемый по умолчанию. Разумеется, таковым можно задать любой из профилей работы, но целесообразно название профиля сделать отвечающим его смыслу.

Непосредственно после инсталляции ADinf32, если задана функция автоматического вызова, включает в нее профиль ***Настройки по умолчанию***. Вы можете сформировать другой профиль с другим именем для вызова программы из меню или по щелчку на иконке Рабочего стола.

ADinf32 позволяет создавать профили не только для томов HDD, но и для дискет или ZIP-дисков. Это бывает полезно в случаях, когда сменные носители используются для создания архивных копий: созданный на том же носителе профиль с контрольными таблицами позволит позднее убедиться в сохранности файлов.

Особое значение для системных администраторов имеет возможность использования ADinf32 для дисков на файл-серверах. Применение этой программы значительно облегчает как отслеживание изменений (с проверкой на вирусы) рабочих областей, так и проверку сохранности условно-постоянной информации.

4.1. Запуск ADinf32

Запуск программы может быть выполнен:

— автоматически после загрузки Windows, если среди профилей текущего пользователя Windows существует профиль, определенный для использования при автозагрузке;

— по непосредственной инициативе пользователя (например, по щелчку на иконке на рабочем столе).

Профиль, используемый при автозагрузке, может быть только один у каждого пользователя. Его выбор делается на вкладке ***Сканирование при загрузке*** (см. стр. 62).

Несколько иначе обстоит дело с определением профиля при старте программы по непосредственному вызову. Можно оставить выбор желаемого профиля (каждый раз при старте программы будет

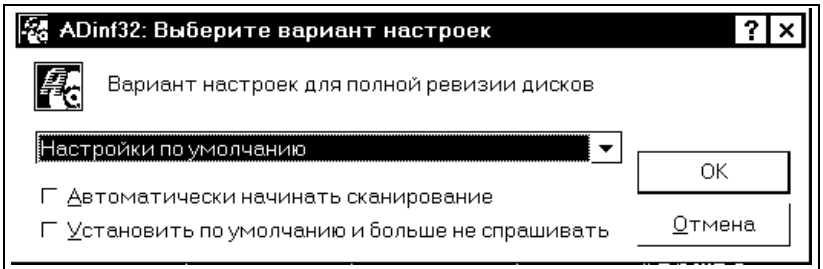


Рис. 18. Запрос профиля при загрузке ADinf32

возникать окно, показанное на рис.18, в котором достаточно выбрать из списка нужный профиль и нажать ***OK***). Можно также фиксировать нужный профиль, проставив при очередном вызове флаг в поле ***Установить по умолчанию и больше не спрашивать*** — тогда при вызове программа автоматически попадет в Главное окно, рассматриваемое в следующем разделе. Если дополнительных действий в Главном окне, как правило, предпринимать не приходится — можно выставить еще и флаг ***Автоматически начинать сканирование***.

Во всех случаях можно остановить уже начавшееся сканирование дисков, а затем изменить выбранный профиль или обрабатываемые в его рамках диски.

Показанные на рис. 18 флаги соответствуют флагу ***Автоматически начинать сканирование*** на вкладке ***Общие*** панели настроек профиля (стр. 69) и флагу ***Спрашивать вариант настроек при запуске*** на вкладке ***Варианты настроек*** панели ***Свойства*** (стр. 61).

4.2. Работа в Главном окне ADinf32

Главное окно ADinf32 может отражать различные состояния программы. На рис. 19 показано Главное окно в состоянии перед началом проверки, когда профиль уже определен как **Настройки по умол-**

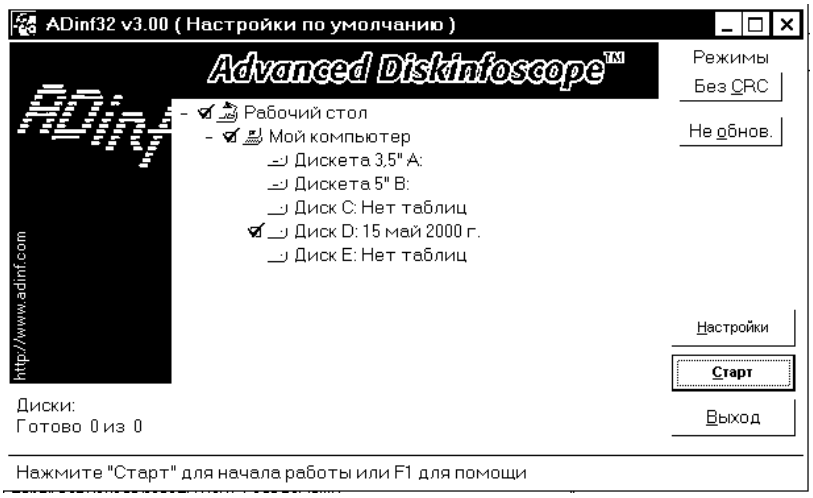


Рис. 19. Главное окно ADinf32

чанию (см. верхнюю рамку окна), соответственно, известны используемые данным профилем таблицы (в средней части окна можно видеть, что этому профилю соответствуют таблицы для диска **D:** от **15 мая 2000**). В этот момент можно:

— изменить пометки участия в профиле тех или иных дисков в дереве дисков в центральной части (при выходе из программы эти изменения будут сохранены в текущем профиле!);

— сменить состояние флагов группы ***Режимы*** (новые состояния не сохранятся в текущем профиле по выходе из программы);

— запустить сканирование по отмеченным дискам кнопкой ***Старт***, либо из контекстного меню (о контекстном меню см.ниже);

— перенастроить тот или иной профиль, “нажав” левой клавишей мыши кнопку ***Настройки***;

— завершить работу программы кнопкой ***Выход*** (автоматически запомнятся все настройки в текущем профиле);

— выполнить обработку любого видимого в окне диска *без изменения настроек текущего профиля* (в частности, без включения этого диска в число обрабатываемых в профиле), для чего выполнить двойной клик левой кнопкой мыши на изображении требуемого диска;

— “растянуть” или “сжать” изображение Главного окна в некоторых пределах, оттягивая ребристый уголок окна справа внизу;

— войти в общее контекстное меню Главного окна, щелкнув правой кнопкой мыши внутри Главного окна вне Окна дерева дисков и вне кнопок управления (рис. 20);

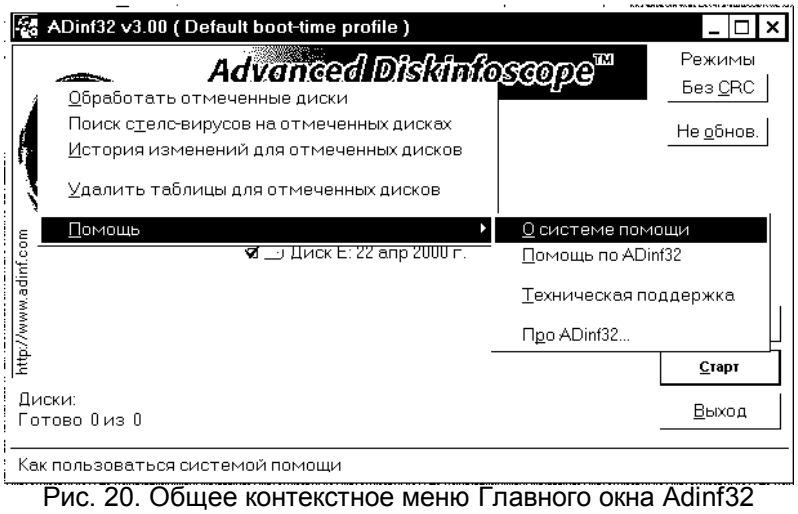


Рис. 20. Общее контекстное меню Главного окна Adinf32 перед сканированием

— войти в Контекстное меню Диска, щелкнув правой кнопкой мыши на изображении диска в дереве дисков Главного окна (рис.21).

Нажатие кнопки ***Без CRC*** (строго перед нажатием ***Старт***) позволяет задействовать сканирование диска без расчета контрольных сумм файлов и обновления таблиц. Нажатие кнопки ***Не обнов.*** блокирует обновление таблиц профиля по завершении работы. Оба этих флага *не запоминаются* в настройках по выходе из программы.

Общее контекстное меню Главного окна позволяет выполнить ряд операций (см. рис. 20) для отмеченных в дереве Главного окна дисков.

Контекстное меню Диска Главного окна (см. рис. 21) позволяет выполнить аналогичные операции для конкретного диска.

Системное меню Главного окна (рис.22) открывается при щелчке левой кнопкой мыши по логотипу в верхнем левом углу рамки.

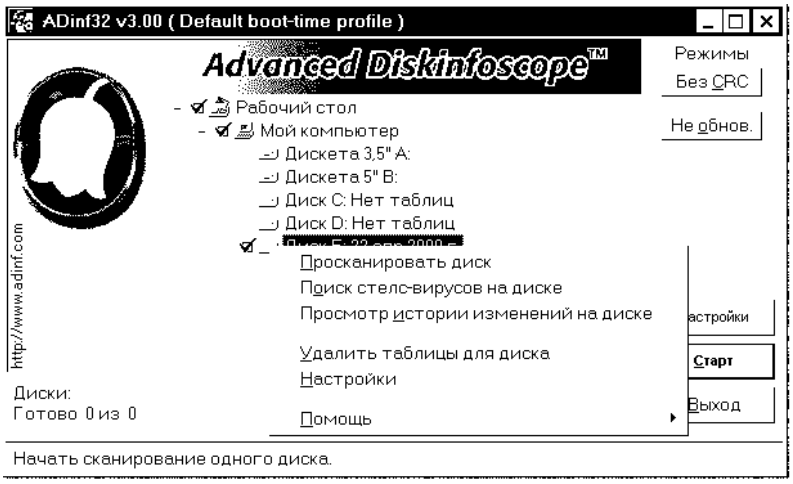


Рис. 21. Контекстное меню диска Главного окна ADinf32 перед сканированием

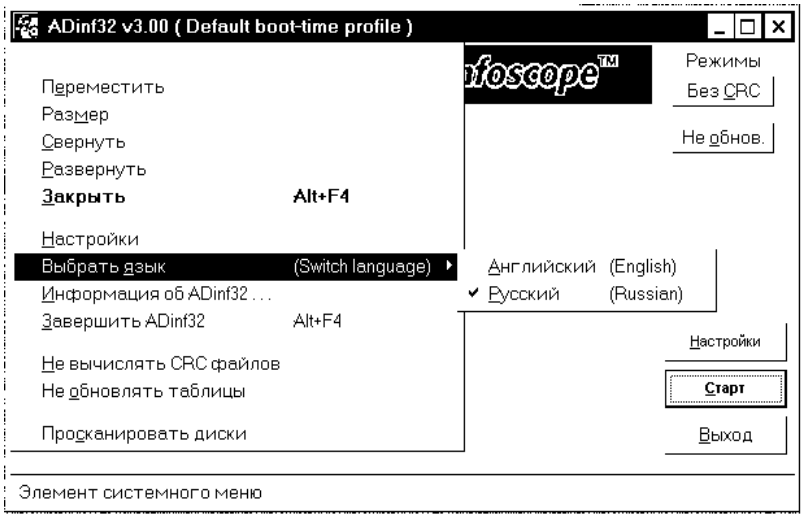


Рис. 22. Системное меню Главного окна ADinf32

4.3. Настройка работы ADinf32

При входе в настройки прежде всего следует выбрать настраиваемый профиль. Для этого служит вкладка ***Варианты настроек*** панели ***Свойства ADinf32*** (рис. 23).

Для настройки профиля следует сначала выбрать его из возможных, либо нажать кнопку ***Добавить*** (в этот момент можно выбрать нужный тип профиля и дать ему желаемое имя). Далее можно установить характеристики профиля с помощью кнопки ***Настроить***. Запомнив сделанные настройки кнопкой ***Применить***, можно настроить следующий профиль, и т.д.

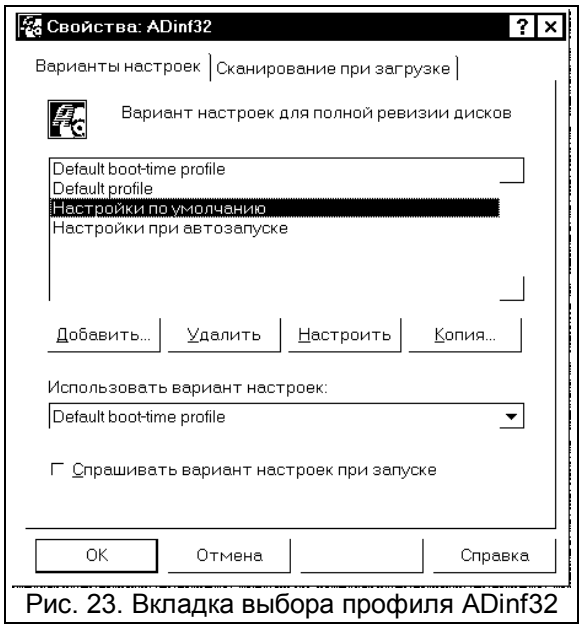


Рис. 23. Вкладка выбора профиля ADinf32

После настройки всех профилей следует установить выбранный профиль в browse-окне ***Использовать вариант настроек*** и завершить настройку нажатием кнопки ***OK***, либо переключиться на вторую вкладку для указания профиля, который будет действовать при загрузке Windows.

Флажок ***Спрашивать вариант настройки при загрузке*** заставит программу каждый раз при старте по запросу пользователя запрашивать профиль работы (см. рис. 18). Если флажок не проставлять, то по умолчанию будет использоваться профиль, заданный в окне ***Использовать вариант настроек***, а если его все же необходимо изменить— следует нажать в Главном окне кнопку ***Настройки***, выбрать в данной панели нужный профиль и, нажав ***OK***, вернуться в Главное окно. Для контроля, имя актуального профиля всегда видно на рамке Главного окна.

Вкладка ***Сканирование при загрузке*** выделяет из всех профилей тот, который автоматически устанавливается при автозапуске программы ADinf32 сразу после загрузки Windows. Делать ли такую проверку, определяет флаг ***Запускать сканирование при загрузке Windows***. При включении этого флага, актуальны остальные опции панели, позволяющие (перечень сверху вниз):

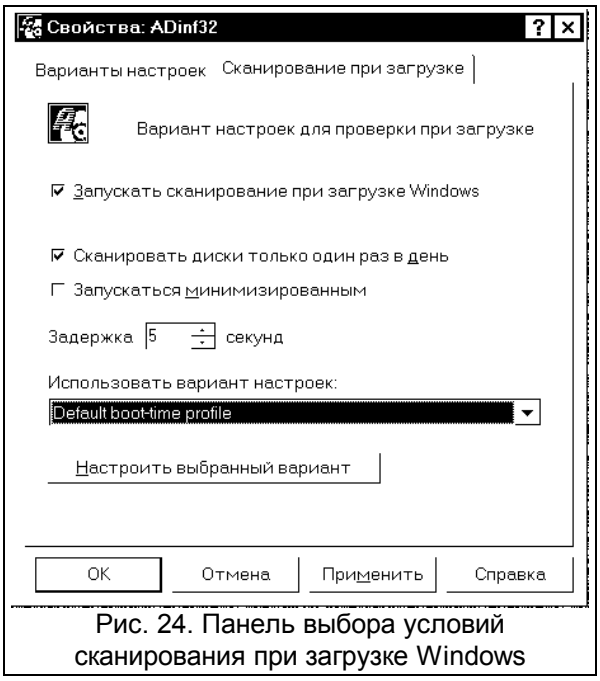


Рис. 24. Панель выбора условий сканирования при загрузке Windows

— автоматически проверять, было ли уже выполнено сканирование в текущий день, и не повторять его дважды, либо запускать ADinf32 каждый раз при загрузке Windows;

— минимизировать окно[1] ADinf32 при запуске, не отвлекаясь на его действия (не рекомендуется для неопытных пользователей);

— установить задержку в нужное число секунд перед стартом автоматического сканирования, чтобы быстрее загрузились автоматически подгружаемые модули (MS-Office и др.), а пользователь имел бы возможность при необходимости отменить сканирование;

— указать профиль для автоматического сканирования.

Для полноты на этой панели доступна кнопка настройки выбранного варианта, если он еще не настроен в панели ***Варианты настроек*** или есть необходимость что-либо изменить. Нижние кнопки

[1]) Управлять программой в это время можно через Системное меню (рис.22).

одинаковы для обеих панелей с тем же смыслом: ***OK*** завершает диалог настройки с запоминанием всех установок, ***Применить*** фиксирует сделанные изменения и продолжает диалог, ***Отмена*** завершает диалог с отменой всех изменений, ***Справка*** позволяет вызвать контекстную помощь по данной панели.

Настройка конкретного профиля содержит множество опций, распределенных по нескольким панелям (9 для полного, 7 для упрощенного, 5 для 16-битного профиля). Ниже подробно указан смысл каждой опции в каждой панели настроек для полных и упрощенных профилей (работа с профилями ADinf16 описана в [5]). Каждая панель имеет в заглавии на рамке имя настраиваемого профиля, а внизу — 4 стандартные кнопки, смысл которых аналогичен указанным в предыдущем абзаце.

Панель *Таблицы*

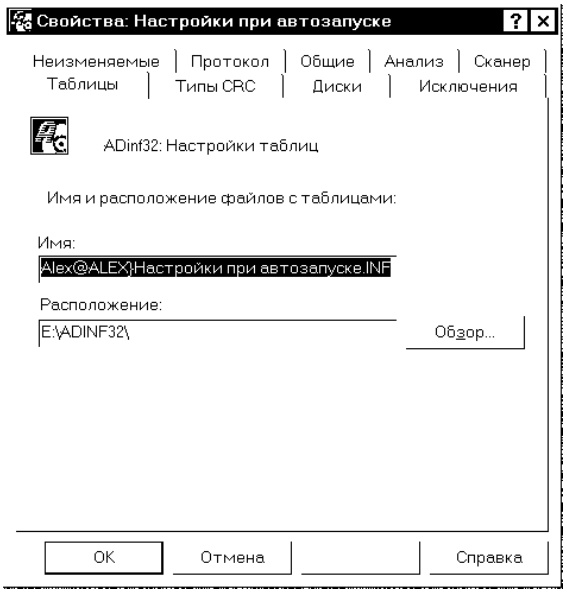


Рис. 25. Панель ***Таблицы*** настройки профиля ADinf32

Эта панель задает имя и местоположение файлов с сохраняемыми расчетными таблицами настраиваемого профиля. По умолчанию, таблицы создаются в той же папке, где установлен ADinf32. Полное имя файла каждой таблицы включает имя диска в первой позиции и имя, настраиваемое здесь (оно образуется из имени пользователя, компьютера, профиля и других компонентов). Менять без необходимости что-либо здесь нет нужды, т.к. ADinf при установке или замене версии автоматически опознает уже существующие таблицы.

Между прочим, это означает, что любой пользователь ПК вправе иметь собственные таблицы одного и того же диска в профиле с одним и тем же именем, хотя физически это будут разные файлы.

Данные в этих файлах также могут быть различны. К примеру, меня, разумеется, вряд ли заинтересуют изменения в файлах моего коллеги, а вот свои и системные файлы я постараюсь отслеживать с максимальной тщательностью.

Разумеется, при многопользовательской работе на одном ПК следует располагать таблицы профиля автозагрузки в той папке, которая доступна по записи текущему пользователю.

Панель *Типы CRC*

На этой панели (рис.26) задается список контролируемых в данном профиле файлов и состав информации, включаемой в таблицы настраиваемого профиля. Отбираемые для контроля файлы устанавливаются по списку их *расширений*, причем каждому типу файла из списка соответствует свой тип контрольной суммы. Файлы вне списка могут быть включены в контроль (с одним из допустимых типов CRC) или исключены из него.

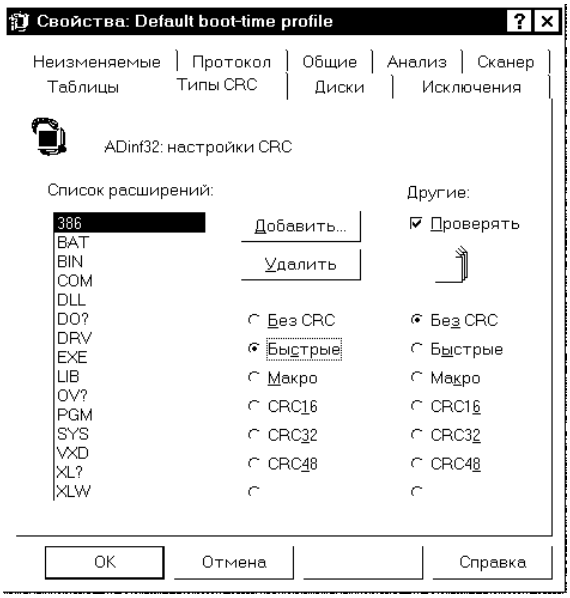


Рис. 26. Панель ***Типы CRC*** настройки профиля ADinf32

Список — редактируемый, причем для каждого типа расширений можно указать свой тип контрольной суммы. Процедура редактирования списка аналогична соответствующей процедуре, описанной для панели настроек ***Типы*** программы DrWeb32W (см.стр. 31). Отличием является отсутствие кнопки восстановления стандартного списка,

который включает расширения **386**, **BAT**, **BIN**, **COM**, **DLL**, **DO?**, **DRV**, **EXE**, **LIB**, **OV?**, **PGM**, **SYS**, **VXD,** **XL?** и **XLW** (по умолчанию, для **DO?** и **XL?** используются CRC ***Макро***, для **SYS** — ***CRC16***, для **XLW** — ***Без CRC***, для остальных — ***Быстрые***).

Не следует ради скорости менять типы CRC в сторону "ухудшения": так, установка типа ***Быстрые*** для **SYS**-файлов не даст выявить часть вирусных изменений. В подавляющем большинстве случаев установка **CRC16** достаточно для надежного контроля.

В то же время, замена всех сумм на ***CRC48***, а тем более, на ***LAN64*** сильно замедлит работу, хотя только установка ***LAN64*** позволит контролировать любые возможные изменения. В ряде случаев имеет смысл замена CRC ***Макро*** на иную (см. определение типов сумм в начале данного раздела) для изменения смысла контроля.

Без CRC отменяет суммирование, оставляя контроль длины файла, момента его образования и наличия подозрительных изменений.

Панель *Диски*

Эта панель (рис. 27) служит для явного указания контролируемых данным профилем логических дисков, а также — для каждого из них — метода доступа и объема контролируемой информации. Методы доступа см. в начале раздела 4.

ADinf32 самостоятельно определяет подходящий метод доступа для логических дисков. Изменять его нужно только в том случае, если диск оказывается недоступен.

Настройка панели заключается в переборе всех нужных для контроля дисков выбором их в верхнем окне панели и ус-

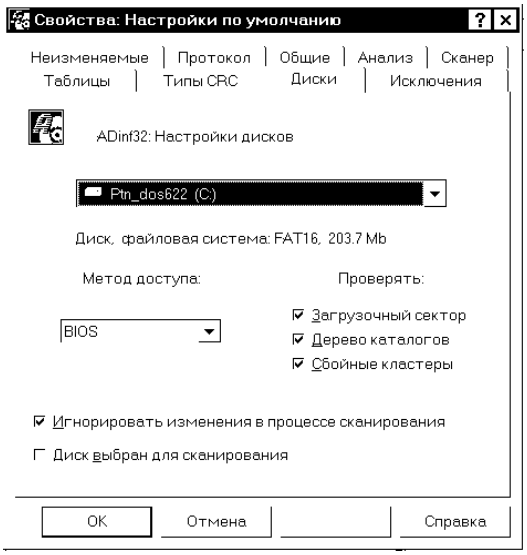


Рис. 27. Панель настройки ***Диски*** профиля ADinf32

тановкой *для каждого* выбранного диска нужных значений в средней части панели.

Флаг ***Игнорировать изменения в процессе сканирования*** отключает контроль за изменениями в файловой системе в процессе сбора информации (возможность, отсутствующая во многих утилитах — Scandisk'е, утилите дефрагментации и пр.). В подавляющем большинстве случаев отключение контроля не приводит к искажениям, однако если на ПК запущено много параллельных процессов — модемная связь, скачивание информации из Интернета, игры с видеовставками и пр., — при отсутствии флага может происходить многократное пересканирование диска с самого начала из-за постоянных изменений, что резко замедлит работу.

Флаг ***Диск выбран для сканирования*** на самом деле означает подключение выбранного логического диска к его контролю данным профилем. Простановка этого флага эквивалентна красной пометке против выбранного диска в Главном окне.

Нижеописываемые флаги имеются только в панели **полного** профиля настройки и отсутствуют для **упрощенного** профиля.

Флаг ***Проверять загрузочный сектор*** по умолчанию включается только для того диска, с которого выполнена загрузка ОС. Однако, ADinf32 сохраняет при инсталляции значения всех загрузочных секторов всех дисков, так что в любой момент можно включить эту проверку.

Флаг ***Проверять дерево каталогов*** контролирует появление новых и удаление старых каталогов на выбранном диске. Файлы в каталогах проверяются независимо от этого флага.

Флаг ***Проверять сбойные кластеры*** вызывает проверку удаления или появления новых сбойных кластеров на диске.

Панель *Исключения*

Данная панель позволяет указать список файлов, принудительно исключаемых из списка контролируемых. Файлы указываются по их маске, перечислением исключаемых масок. Совпадающие с одной из указанных масок исключены из списка контролируемых, т.е. никакая информация об этих файлах не собирается, их возможные изменения не отслеживаются и не влияют на работу ревизора.

Способ изменения элементов списка эквивалентен описанному на стр. 31. Поскольку кнопка восстановления стандартного списка от-

сутствует — укажем, что стандартный перечень исключаемых файлов включает файлы с масками: **~$*.DO?**, **~$*.RTF**, **~WRL????.TMP**, **NPS*.ICO** и **NPS*.TMP**.

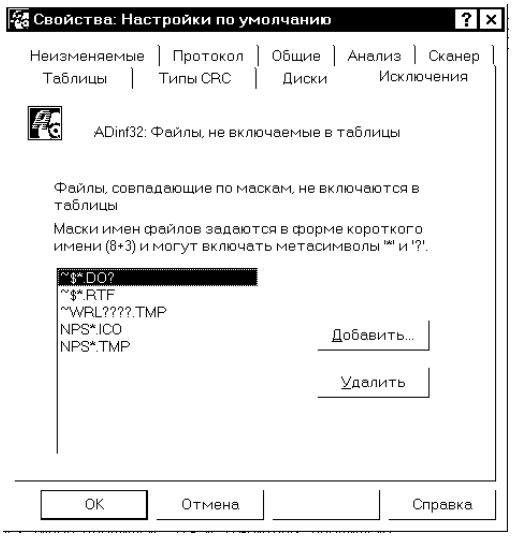


Рис. 28. Панель ***Исключения*** настройки профиля ADinf32

Помимо указанных в данной таблице, ADinf32 хранит внутренние, встроенные списки неконтролируемых файлов для всех трех типов профилей. Этими постоянно исключенными из контроля файлами для 32-битных профилей (как полных, так и упрощенных) являются, к примеру, свопы **WIN386.SWP**, **386SPART.PAR** и **PAGEFILE.SYS**, файлы **DRVSPACE.0??** и ряд других системных файлов. При желании, полный список таких файлов можно найти в файле Помощи (хелпе) к программе ADinf32.

Панель *Неизменяемые*

Среди других файлов, в каждой ОС имеются файлы, *любое* изменение которых считается подозрительным. Данная панель (рис. 28) позволяет редактировать список таких файлов. Процедура изменения списка многократно описана в данном документе и не нуждается в особых пояснениях.

Данная панель присутствует только в **полном** типе профиля настройки и отсутствует в **упрощенном**.

В рамках **полного** профиля, ревизор ADinf32 предусматривает специальные действия при изменении характеристик таких “неизменяемых” файлов. Включая интересующие Вас файлы в список данной панели, Вы тем самым автоматически предусматриваете аналогичную реакцию программы и на изменения указанных Вами файлов.

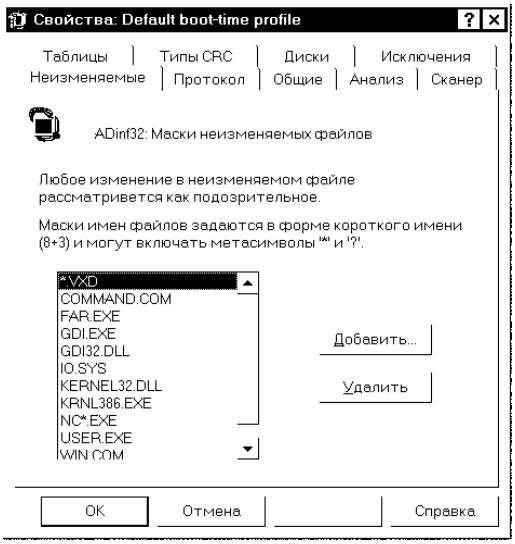


Рис. 29. Панель ***Неизменяемые*** настройки профиля ADinf32

Т.к. на данной панели отсутствует кнопка восстановления оригинального списка, приведем его состав по версии 3.0 ADinf32: ***.VXD, GDI32.DLL, FAR.EXE, GDI.EXE, COMMAND.COM, IO.SYS, NC*.EXE, WIN.COM, USER.EXE, KERNEL32.DLL, KRNL386.EXE.**

Опытный пользователь может видеть, что здесь собраны "ключевые" файлы ряда ОС, от MS-DOS до '98, а также наиболее употребительные программы (в качестве примера включены модули **FAR.EXE** и **NC*.EXE**). При необходимости можно легко изменить этот список под эксплуатируемую ОС.

Панель *Протокол*

Эта панель (см. рис. 30) служит для настройки формируемого в процессе работы программы протокола работы. Принципиальным отличием по сравнению с DrWeb32W является наличие флага ***Записывать файл протокола***, без установки которого протокол не ведется вообще.

Полное имя файла протокола должно указывать на папку (каталог), заведомо доступную по записи во время работы пользователя. Значение по умолчанию **C:\ADINF32.LOG** лучше изменить.

Как и для DrWeb32W, определена возможность дозаписи в существующий файл. В отличие от соответствующего списка возможностей DrWeb32W, помимо опций ***Замещать существующий файл*** и ***Дополнять существующий файл*** (однако, без общего ограничения длины) есть возможность ***Сохранить существующий файл и не писать протокол***.

Безусловно, для разных по характеру профилей работы пользователь должен самостоятельно установить здесь нужные значения. Например, категорически не рекомендуется отключать формирование протокола для автоматического вызова при загрузке Windows: в случае непредвиденной ситуации с нанесенными вирусом повреждениями, не отраженной документально, впоследствии трудно разобраться в причине случившегося.

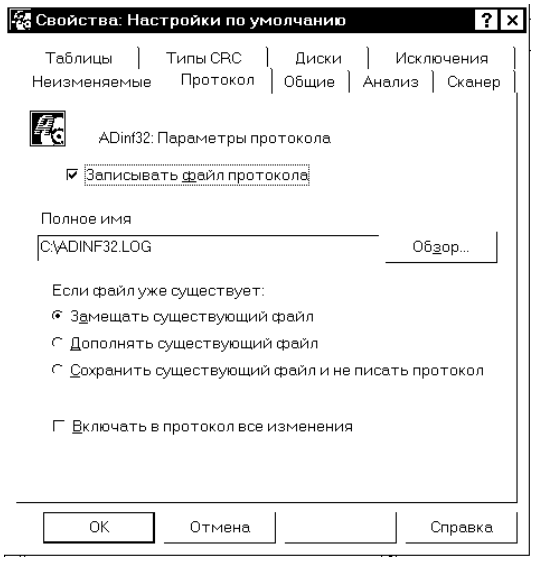


Рис. 30. Панель ***Протокол*** настройки профиля ADinf32

Флаг ***Включать в протокол все изменения*** при его установке вызывает отражение в протоколе изменений даже в тех каталогах, которые помечены флагом ***Скрыть изменения*** в контекстном меню каталога (см. подраздел 4.5).

Панель *Общие*

Эта панель настройки содержит ряд общих опций настройки профиля. Вид панели зависит от типа профиля. На рис. 30 приведена панель для **полного** профиля настройки.

Флаг ***Автоматически открывать окно результатов*** при его установке заставляет программу ADinf32 после начала сканирования немедленно открыть Окно результата. Поскольку программа ADinf32 создана с использованием многопоточной технологии, при сканировании нескольких дисков Вы можете просматривать полученные по одному из них результаты, не дожидаясь завершения просмотра остальных дисков. Это может существенно сэкономить время. Флаг присутствует только в **полном** профиле настройки.

Флаг ***Включены звуки*** включает звуковые эффекты программы. Звуки можно настроить в разделе **Звуки** (***Sounds***) Панели Управления Windows, подобрав каждой ситуации нужную мелодию.

Флаг ***Всплывающие подсказки*** при включении разрешает появление в Главном окне программы всплывающих подсказок при задержке курсора над кнопками.

Флаг ***Автоматически начинать сканирование*** позволяет при запуске программы по инициативе пользователя немедленно начать сканирование дисков, не дожидаясь нажатия клавиши ***Старт***.

Флаг ***Не предлагать создавать таблицы*** при его включении заставляет блокировать автоматическое предложение создать таблицы для всех несменных дисков, если ни на каком из этих дисков их нет. Этот флаг предназначен для специальных профилей, созданных для проверки сменных носителей, например, ZIP-дискет (разумеется, при их проверке таблицы *этого* профиля на всех остальных носителях, в том числе локальных несменных досках, будут отсутствовать!), чтобы исключить предложение создать таблицы также и для прочих дисков.

Флаг ***Запрос подтверждения перед обновлением таблиц*** при включении заставляет ADinf32 перед обновлением таблиц данного профиля обязательно запрашивать подтверждение (при появлении подозрительных изменений подтверждение будет запрошено всегда, независимо от состояния этого флага). Флаг есть только на панели **полного** профиля настроек.

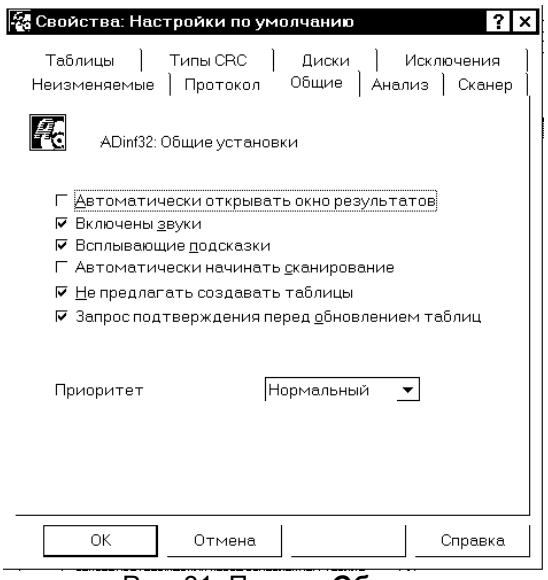


Рис. 31. Панель ***Общие*** настройки профиля ADinf32

Переключатель ***Приоритет*** позволяет уменьшить приоритет работы программы в сравнении с другими задачами. При понижении приоритета работать программа будет дольше, но ее влияние на другие задачи будет менее значительно.

Панель *Анализ*

На этой панели (рис. 32) пользователь может задать, какие ситуации относятся к группе "подозрительных изменений". При появлении таких изменений предусмотрена специальная реакция программы, требующая от пользователя принятия немедленного оперативного решения.

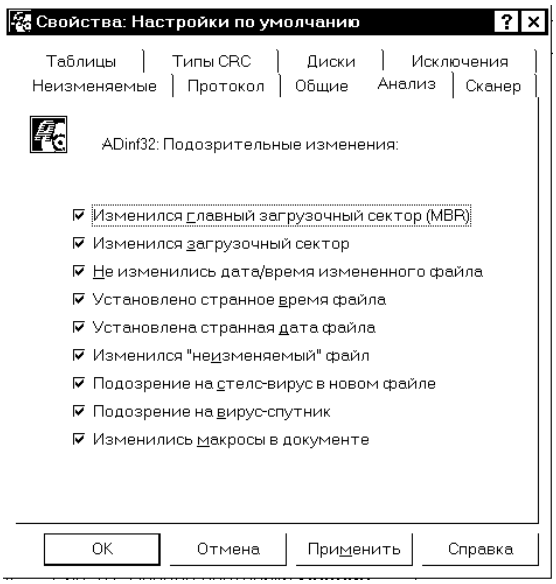


Рис. 32. Панель ***Анализ*** настройки профиля ADinf32

Панель настройки присутствует только в **полных** профилях. Смысл возможных изменений указан ниже.

Изменился главный загрузочный сектор (MBR). Изменение главного загрузочного сектора (*Master Boot Record, MBR)* не обязательно связано с действием вирусов. Пользователь может изменить таблицу разделов HDD, поставить новый вариант ОС, наконец, установить один из многочисленных пакетов выбора альтернатив загрузки (**Boot Manager, Boot Wizard** и др.). Иные программисты ряда фирм пытаются держать в MBR элементы защиты своих поделок[1]. Однако,

[1]) Пример с отечественной фирмой Инфин, писавшей систему бухучета под эгидой Минэкономики РФ, и использовавшей MBR для простановки защиты, приведен в [10].

во *всех* случаях появления таких сообщений, если нет точной информации о причине этого, лучше запретить обновление таблиц, прекратить работу на ПК и проконсультироваться со специалистом.

Изменился загрузочный сектор — вопреки расхожему мнению, ничуть не менее неприятное сообщение, чем предыдущее. Действия должны быть аналогичными.

Не изменились дата/время измененного файла — если не результат Ваших целенаправленных действий (часто вместо времени создания файла программист ставит версию программы), то, скорее всего, действительно действие вируса, т.к. многие вирусы со времени MS-DOS для сокрытия следов своего внедрения восстанавливают дату и время образования файла после заражения.

Сообщения об установке странных времени или даты в настоящее время уже не обязательно являются результатом действия вирусов, эта “мода” вирусописателей прошла. Однако, появление 13-го месяца либо 62 секунд в дате образования файла должно насторожить гораздо больше, чем 1980 год вместо 2000-го...

Среди прочих вариантов более всего должно настораживать ***Подозрение на стелс-вирус в новом файле***, поскольку в силу причины появления этого сообщения (расхождение между образом файла при чтении его разбором секторов и через файловую систему) другие объяснения здесь исключены, если не считать, конечно, возможных отказов аппаратуры.

Панель *Сканер*

В этой панели (рис. 33) пользователь настраивает взаимодействие со сканером. Автор ADinf32 предусмотрел использование различных программ в качестве сканера. В момент инсталляции избирается один из установленных на ПК сканеров, что отражается в настройках панели по умолчанию. Однако, пользователь эти настройки может изменить.

В верхней строке можно выбрать тип сканера. Следует обязательно *настроить правильный путь* в строке ***Полный путь исполняемого файла***. Параметры командной строки, предлагаемые по умолчанию, можно изменить в соответствии со схемой исполнения работ на конкретном ПК и операционной обстановкой. Полный список возможных ключей для DrWeb32 дан в 3.4, однако менять предложенные установки (они приведены в конце таблицы) следует, отдавая отчет о *всех* возможных последствиях: эти настройки вызова сканера

действуют не только при вызове сканера по завершении работы ADinf32, но и при автоматическом вызове сканера при просмотре результатов сканирования (см. подраздел 4.5) !

После флага ***Автоматически взаимодействовать со сканером***, который должен быть включен при желании автозапуска, идет важный параметр: ***Файл обмена информацией***. Не меняя имени этого файла, рекомендуется тщательно продумать путь и установить диск и каталог, доступные по записи для всех пользователей ПК.

Варианты запуска сканера ясны из контекста. Следует только пояснить, что ***Не запускать сканер*** вызывает накопление списка в файле обмена информацией без запуска сканера (предполагается, что пользователь когда-либо специально запустит сканер с приемом информации из этого файла).

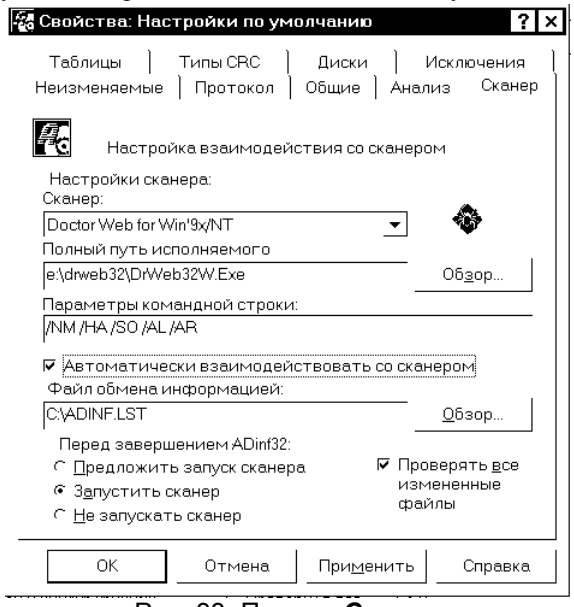


Рис. 33. Панель ***Сканер*** настройки профиля ADinf32

Флаг ***Проверять все измененные файлы*** при его установке соответствует названию. Без установки этого флага файлы в каталогах, помеченных **Скрыть изменения** (см. подраздел 4.5), файлы с индивидуальными пометками **Скрыть изменения**, а также исключенные из проверки согласно одной из масок панели ***Исключения***, в список для проверки не попадут.

4.4. Ревизия дисков программой ADinf32

Выше в подразделах 4.1- 4.2 описаны все варианты запуска сканирования как на одном избранном диске, так и на их серии.

Рис. 34. Главное окно ADinf32 в ходе сканирования

На время ревизии изменяется вид Главного окна, назначение ряда кнопок и Контекстных меню.

Главное окно выглядит аналогично рис. 34. В центральной его части теперь показан список типовых действий ревизора с отметками о ходе проверки. Анимированный рисунок справа от центра и прогресс-индикатор внизу окна отражают ход процесса.

Главная кнопка теперь имеет имя ***Стоп!*** и при ее нажатии прекращает ревизию на любой стадии. Расположенная над ней кнопка ***Результат*** открывает Окно просмотра результатов, не дожидаясь завершения процесса. Первое же обнаруженное изменение на диске вызывает появление на этой кнопке мигающей зеленой лампочки. Первое же обнаруженное подозрительное изменение на любом диске делает эту лампочку красной.

Контекстное меню Главного окна имеет пункты ***Остановить обработку дисков***, ***Открыть окно просмотра результатов*** и, как и прежде, ***Помощь***.

Открыв тем или иным способом Окно просмотра результатов, можно просматривать результаты обработки синхронно с их обна-

ружением. Работа с Окнами просмотра результатов освещена в следующем подразделе.

Если это более удобно пользователю, при настройке профиля автозапуска можно задать исполнение ревизии в минимизированном окне, не занимая места на рабочем столе. Для этого необходимо выставить флаг ***Запускаться минимизированным*** в панели ***Сканирование при загрузке***. По завершении ревизии дисков, иконка на Панели задач начнет мигать для привлечения внимания, и Главное окно можно восстановить.

Если в процессе сканирования обнаружены подозрительные изменения, появляется окно предупреждения наподобие рис. 35. С этого момента дальнейшие действия должны исполняться квалифицированным специалистом: при нажатии кнопки ***Далее*** показываются системные сведения (например, вид загрузочного сектора в шестнадцатиричном виде). После этого обязательно будет задан вопрос о необходимости фиксировать произошедшие изменения в таблицах.

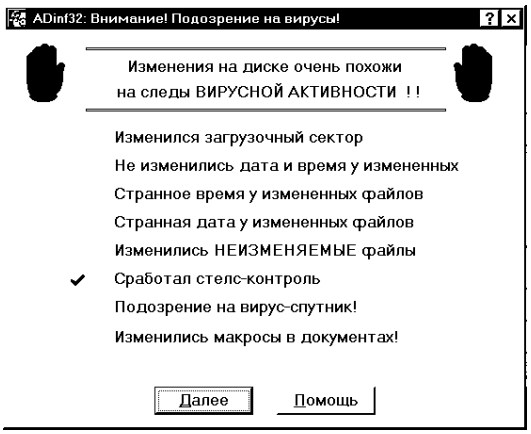


Рис. 35. Предупреждение Adinf32 после ревизии дисков

Разумеется, контроль подозрительных изменений и последующий запрос об обновлении таблиц профиля действуют только для **полного** профиля. Именно для того, чтобы исключить предынфарктное состояние у неподготовленных пользователей, начиная с версии 3.0, предложен **упрощенный** вариант профиля.

4.5. Просмотр результатов сканирования ADinf32

По завершении ревизии дисков, для полного профиля Главное окно принимает вид рис. 36 (о цвете лампочки на кнопке ***Результат*** см. в разделе 4.4). Для **упрощенного** профиля результаты не показываются и автоматически передаются на обработку сканером.

Рис. 36. Главное окно ADinf32: готовы результаты

При желании отказаться от просмотра результатов достаточно нажать кнопку ***Выход***, для просмотра результатов — нажать на кнопку ***Результат***, после чего в отдельном окне будет выведена сводка результатов сканирования (рис. 37). Это же окно может появиться и раньше, отражая результаты синхронно со сканированием, если было задано открытие этого окна без ожидания завершения сканирования или в ходе сканирования нажата кнопка **Результат**..

На этой общей сводке левую часть окна занимает дерево каталогов диска с цветными пометками, правую — перечень возможных типов изменений с указанием по каждому варианту числа обнаруженных изменений либо слова **Нет** при отсутствии изменений данного типа. Щелчком мыши на одной из кнопок **Показать** можно вывести показ каталогов и/или файлов, отфильтрованных по конкретному типу изменений. Так, на рис. 38 показан вид окна с измененными файлами, на рис. 39 — с новыми файлами. Файлы с подозрительными

изменениями будут показаны всегда, вне зависимости от примененного фильтра отбора файлов для показа.

Границу между частями окна можно передвигать вправо/влево.

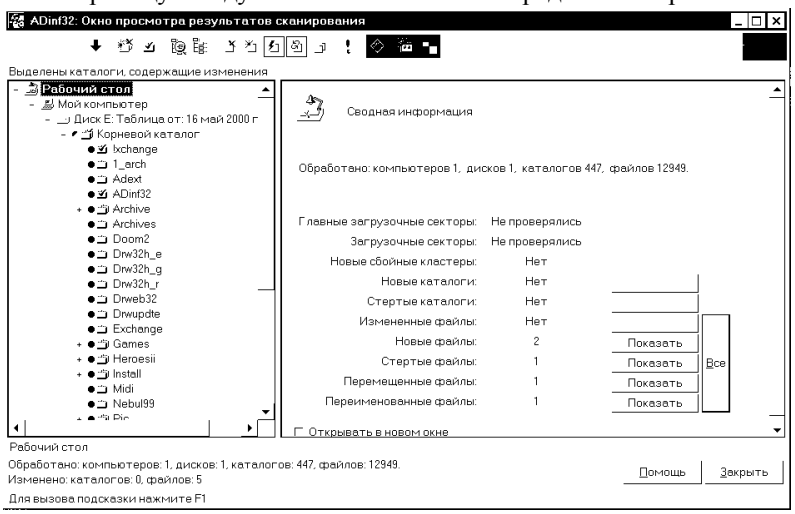


Рис. 38. Окно результатов ревизии дисков ADinf32: сводка

Флаг ***Открывать в новом окне*** заставляет при нажатии одной из кнопок ***Показать*** открыть новое окно с вариантавми просмотра.

Левая часть Окна просмотра изменений может находиться в одном из двух режимов. В одном режиме на показанных каталогах цветными пометками выделены каталоги, содержащие **изменения** в файлах; в другом — **новые** и **стертые** каталоги. При выборе фильтра показа из Сводного окна автоматически формируется нужный режим пометок, а в дальнейшем этот режим (как и фильтрацию показываемых объектов) можно изменить кнопками в верхней части окна (подробно о кнопках см. ниже в данном подразделе).

Цветные пометки против каталогов в дереве дисков Окна изменений имеют форму кружка, в некоторых случаях разделенного пополам. Цветами обозначены:

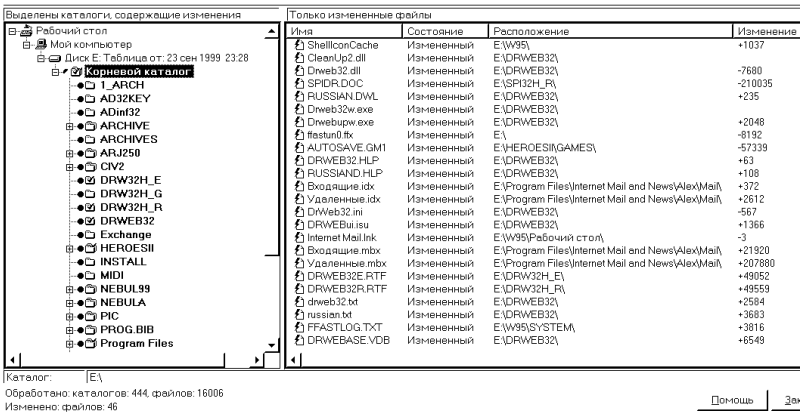


Рис. 38. Измененные файлы в Окне результатов ADinf32

зеленый — обычные каталоги;

фиолетовый — каталоги со скрытыми изменениями;

зеленый на фиолетовом — обычный каталог, в котором есть подкаталоги со скрытыми изменениями;

фиолетовый на зеленом — каталог со скрытыми измененями, под которым есть обычные каталоги.

Правая часть окна также может находиться в двух режимах показа. В одном из них там отражается подробная информация о проверенном объекте, в другом — список измененных файлов во всем поддереве *ниже* выбранного в левом окне объекта.

Выбор объекта как в левом, так и в правом окне осуществляется кликом левой кнопки мыши на этом объекте. Так, на рис. 38 в правом окне выбран файл **SPIDER.VXD**. Лампочка слева от имени файла в правом окне имеет зеленый цвет (“новый файл”). Слева от лампочки помещен замочек — признак неизменяемого файла. При желании одновременно выбрать более одного объекта, необходимо в соответствии с традициями Windows, использовать клавиши <**Shift**> и/или <**Ctrl**> при кликах.

Управление просмотром, помимо кнопок ***Показать*** Сводного окна (рис. 37), может осуществляться с помощью 17 кнопок в верхней

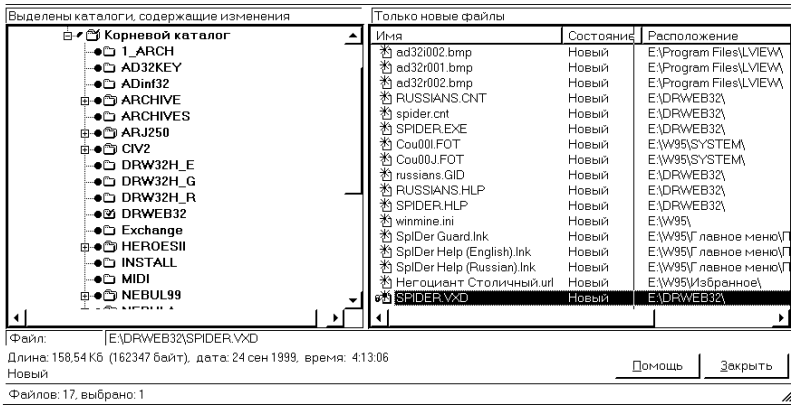
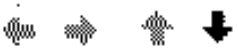


Рис.39. Новые файлы в Окне результатов ADinf32

части Окна просмотра, одинаковых во всех Окнах просмотра. Ниже описаны назначения всех кнопок, пронумерованных слева направо.

Кнопки 1 - 4. Стрелки влево/вправо позволяют перемещаться назад/вперед между состояниями просмотра результатов. Стрелки вверх/вниз позволяют переходить в дереве каталогов к следующему/предыдущему каталогу.

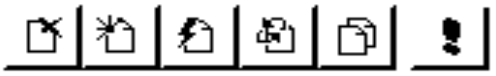


Кнопки 5 и 6 переключают режим отметок левой части Окна просмотра. Нажатие кнопки **5** включает пометки в дереве новых и стертых каталогов. Нажатие кнопки **6** включает пометки на каталогах, содержащих изменения в файлах, выбранные кнопками **9 - 13**. Кнопки взаимно исключаемы, т.е. при нажатии **5** “отжимается” **6**, и наоборот.

Кнопки 7 и 8 также взаимно исключаемы и переключают режим показа правой части Окна просмотра. При нажатии **7** в правом окне отображается подробная информация об объекте, выбранном слева (при выборе слева ***Мой компьютер*** справа показывается сводная информация). При нажатии **8** в правом окне отображается список

файлов, выбранных кнопками **9 - 13**, во всех каталогах ниже объекта, выбранного в дереве слева (при этом в дереве слева названия объектов, файлы которых попали в список, выделяются жирным шрифтом).

Кнопки 9 - 14 определяют состав файлов, отображаемых в правом окне. Кнопка **9** включает в список удаленные (стертые) файлы, кнопка **10** — новые, **11** — измененные, **12** — переименованные и перемещенные. Кнопка **13** включает в список все файлы, а файлы, выбранные кнопками **9 - 12**, выделяются яркими значками. Кнопка **14** оставляет в списке только файлы с подозрительными изменениями (эти файлы показываются всегда при любом режиме, выбранном кнопками **9 - 13)**. Все эти кнопки работают как триггеры (для отключения нужно нажать еще раз). Кнопка **14** при ее нажатии одновременно отключает кнопки **9 - 13**.



Кнопка 15 "запускает" сканер для проверки файлов, выделенных в правом окне, или каталогов, выделенных в левом окне. Сканер к этому моменту должен быть корректно сконфигурирован в Панели настроек ***Сканер.***

Кнопки 16 - 17 управляют Окнами просмотра результатов. Кнопка **16** открывает еще одно Окно просмотра. Кнопка **17** "поднимает наверх" Главное окно программы ADinf32.

Исключение из просмотра измененных каталогов или файлов бывает необходимо, когда изменения обусловлены работой самой Windows или другими программами, многочисленны или не представляют интереса. Опытные пользователи могут исключить из просмотра или даже из проверки ряд файлов или каталогов. Это может быть сделано одним из следующих способов.

* Изменение всех файлов в некоторой папке можно скрыть, выбрав пункт ***Скрыть изменения*** в контекстном меню каталога, открывающемся при клике данного каталога правой кнопки мыши (эта операция вызовет пометку каталога фиолетовым цветом в дереве слева, как отмечено выше). Снять отметку можно, выбрав в том же меню пункт ***Показывать изменения***. Такие пометки на каталогах запоминаются в таблицах текущего профиля настройки.

* Можно проставлять особые отметки для отдельных файлов, используя контекстное меню файла (рис.40), открывающееся при клике на имени файла правой кнопкой мыши. Для этого в открывшемся меню нужно выбрать пункт ***Поставить выделенным файлам отметку***[1], а в нем — одну из опций ***Обычный файл, Всегда показывать изменения*** или ***Скрывать изменения***. Таким образом можно, к примеру, в каталоге со скрываемыми изменениями иметь файлы, изменения которых показываются либо, наоборот, скрыть изменения отдельных файлов в обычном каталоге.

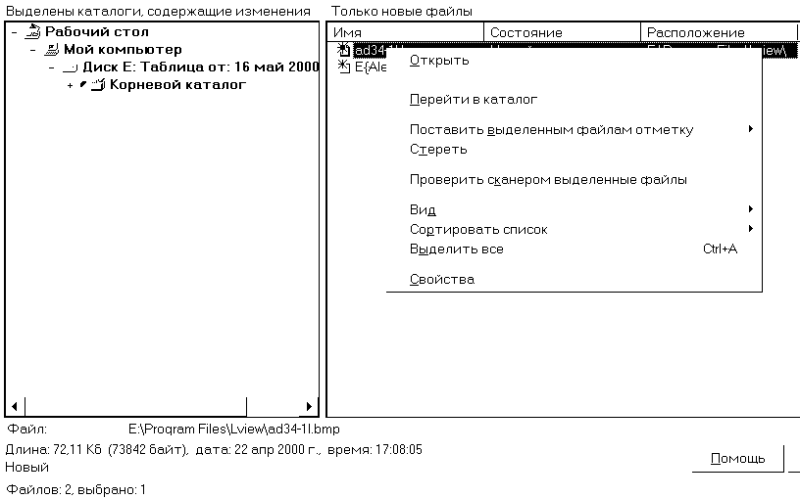


Рис.40. Контекстное меню файла в Окне результатов

Полное исключение файлов из-под контроля, в отличие от скрываемых при показе изменений, может быть сделано в Панели настройки профиля ***Исключения***.

[1] Даже если специально не выделено ни одного файла, текущий файл, атрибуты которого дополнительно показаны внизу окна, так, как это видно на рис. 39, считается выделенным.

4.6. Просмотр истории изменений в ADinf32

ADinf32 позволяет, помимо просмотра текущих изменений, анализировать историю изменений, произошедших на диске с момента создания таблиц. Запрос истории изменений осуществляется через Контекстное меню диска, вызываемое из Главного окна (см. стр. 59). Можно также запросить историю изменений для группы выделенных в Главном окне дисков через Контекстное меню Главного окна.

Сначала открывается Панель запроса истории изменений (рис. 41). В ней необходимо выбрать объект просмотра (файлы или каталоги), период просмотра и состав запрашиваемой информации.

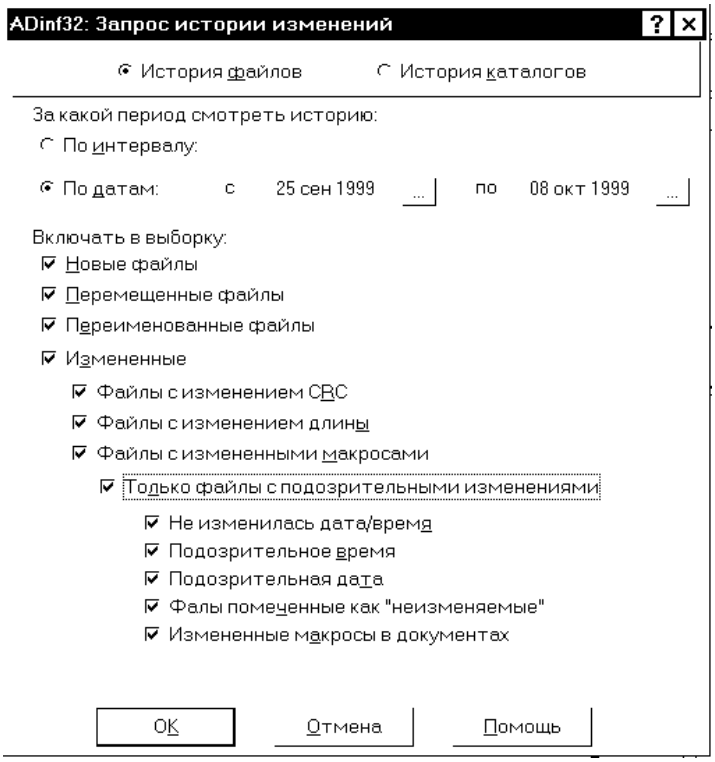


Рис. 41. Панель запроса истории изменений

Затем открывается окно Просмотра истории (рис. 42), в котором отображается список файлов или каталогов, соответствующих запросу, и информация о дате и времени произошедших изменений.

Кнопками в верхней части окна или через Контекстное меню окна Истории изменений можно выделить группу файлов, стереть их, запустить на них проверку антивирусом-сканером. Отдельные файлы можно просмотреть или запустить на исполнение.

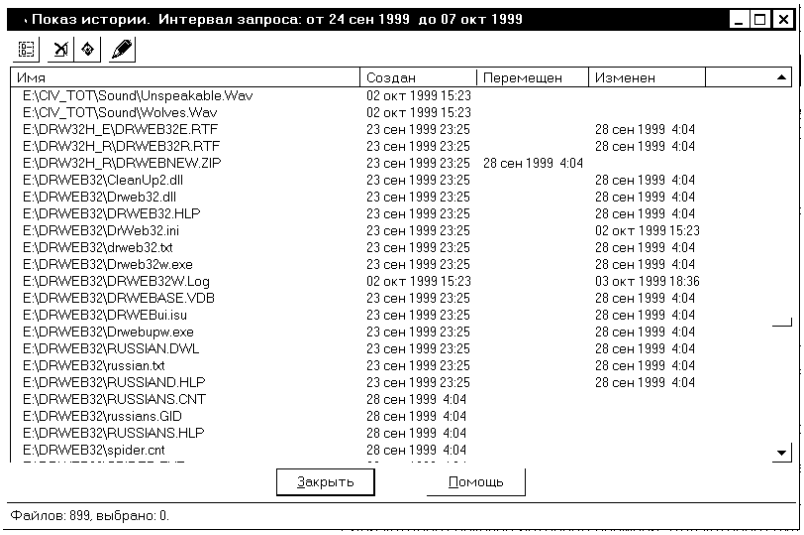


Рис. 42. Окно Истории изменений программы ADinf32

Рекомендуется ревизии дисков делать ежедневно при включении ПК. При этом в нормальном случае в конце работы обновляются таблицы профиля, сохраняя актуальные данные об изменениях.

Войдя в Контекстное меню файла окна Истории изменений (как всегда, кликом правой кнопки мыши на строке файла), можно, посмотрев характеристики файла, узнать тип последнего изменения. Сравнивая даты и осуществляя, если необходимо, запуск сканера-антивируса, можно проанализировать, что послужило источником заражения на ПК. Дополнительную информацию может дать сравнение этих данных по различным профилям различных пользователей данного ПК.

Внимание! Моменты времени, указанные в окне Истории изменений, есть моменты формирования таблиц соответствующего профиля, а не истинные моменты изменений! Чем чаще исполняется сканирование диска, тем ближе отмеченные моменты к истинным.

4.7. Инсталляция ADinf32

Подготовка

Для корректной работы ADinf32 следует соблюсти ряд правил.

* Для установки программы организуйте свой собственный каталог. Не устанавливайте программу в каталог, где находятся другие программы, кроме случая обновления предыдущей версии.

* Малейшая ошибка в процессе *обновления* приведет к УТЕРЕ таблиц от предыдущих версий. Поэтому еще до установки тщательно продумайте все её последующие этапы, проверьте наличие свободного места на диске, удалите ненужное, проверьте целостность логической структуры диска, дефрагментируйте диск, по возможности исключите все работающие приложения. Для страховки скопируйте старые таблицы (файлы с расширением **INF**) в резервные каталоги.

* Проверьте, что версия Windows достаточно новая. Файл **COMCTL32.DLL** должен иметь дату образования не менее 12.11.1996 (фирменные предупреждения ДиалогНауки требуют 1997 года, но модуль указанной даты от 'OSR2 работает с версией 3.0).

* Даже среди корректно и надежно работающих опций при первом знакомстве с программой выбирайте рекомендованные ниже. Здесь нет места объяснять все тонкости и возможные ситуации...

* Просмотрите общие соображения о готовности к установке, изложенные в аналогичном разделе для DrWeb32W на стр. 41.

* Установите и настройте DrWeb32 до установки ADinf32: при установке ADinf32 Вам все равно потребуется ссылка на DrWeb32.

Итак, Вы решили, что у Вас достаточно поздняя версия Windows, Вы получили от Вашего регионального дилера индивидуальный регистрационный ключ к ADinf32 и готовы к установке. Следуйте дальнейшим указаниям.

Собственно инсталляция

1. Прежде всего проверьте отсутствие вирусов на Вашем ПК. Это — необходимое условие установки, иначе вся работа ADinf32 может свестись на нет, более того, возможна порча файлов. Проверять следует самой последней версией DrWeb32 со всеми полагающимися к моменту установки дополнениями к вирусной базе данных, в режиме проверки *всех* фалов (а не "по формату"!).

2. Запустив SETUP.EXE из нужного каталога, ответьте **Далее** на приветствие и согласием на лицензионное соглашение. Если далее

последует окно с сообщением про библиотеку **COMCTL32.DLL** — примите во внимание сказанное об этом выше.

3. Программа предложит установить ее в некоторый каталог. Проверьте, чтобы это был каталог на локальном диске Вашего ПК с предыдущей установленной работоспособной версией (если Вы хотите сохранить преемственность работы) либо укажите нужный каталог, в котором *заведомо* нет других модулей.

4а. ЗАМЕНА ВЕРСИИ. Если инсталлятор “понял”, что Вы пытаетесь заменить существующую версию — далее последует переход к пункту 8. Если этого не произошло в данный момент — имеющаяся у Вас версия будет проигнорирована, и установка выполнена как новая.

4б. НОВАЯ УСТАНОВКА. В этот момент предлагается выбрать **Полные возможности ревизора диска** или **Упрощенный вариант функционирования**, т.е. тип стандартного профиля. Сделайте нужный выбор (впоследствии Вы сможете создать и другие профили).

5. Выберите папку запуска для ADinf32. Оставьте предлагаемую по умолчанию — так будет проще.

6. Экран **Выберите начальные значения для основных настроек**. В данной версии 3.0 этот экран содержит только одну основную настройку, уже помеченную галочкой; это ***Запускать антивирусную проверку при загрузке***. Вы можете сохранить или отказаться от этой возможности прямо сейчас или сделать это позже. Предположим, Вы оставили отметку.

7. Вам предлагается выбрать один из установленных на Вашем ПК сканеров для взаимодействия с ADinf32 (при выборе в п.4 **полных** возможностей будет присутствовать строка ***Не включать поддержку сканера***). При наличии DrWeb32W будет предложен именно он. Сделайте Ваш выбор.

8. Сообщение о том, что программа инсталляции собрала достаточно информации, дается для того, чтобы Вы могли обозреть сумму предлагаемых Вам возможностей и при необходимости сделать шаги назад, изменив какие-то этапы выбора.

Если у Вас уже была установлена предыдущая версия программы и текущий инсталлятор это "понял" — последует вопрос о том, хотите ли Вы обновить с преемственностью или заменить предыдущую версию. Наличие ответа **Обновить** является признаком того, что инсталлятор "понял" Ваше желание и сохранит преемственность в

виде уже имеющихся таблиц нужного профиля и установок по умолчанию. Если же такого сообщения нет — значит, предыдущая корректная версия не найдена. В этом случае Вы можете вернуться назад и попробовать указать на другой каталог или вообще отказаться от установки (**Отмена**), обратившись за консультацией к Вашему дилеру или в отдел технической поддержки ДиалогНауки.

Кстати. Даже если Вы устанавливаете программу в тот же каталог, Вы можете не захотеть обновить версию, а установить ее заново. В этом случае выберите пункт **Далее**.

9. Копируются файлы, обновляются системные элементы и показывается последний экран инсталляции, предлагающий прочесть ReadMe, запустить ADinf32 и побывать на сайте разработчика в Интернете. Для целей нашего изложения важен запуск ADinf32 — будем считать, что Вы оставили только его.

10. Запустившись, ADinf32 в случае, если Вы выбрали **упрощенный** тип профиля, немедленно начинает сканировать диски для составления таблиц. ПРЕРВИТЕ ЕГО, если что-либо из умалчиваемых установок (например, места хранения таблиц, корень диска **C:** для файла отчета, замещение новым отчетом старого или иное) Вас не устраивает, и переходите к пункту 11. Если устраивает все — дайте программе возможность закончить работу.

В случае выбора **полного** типа профиля последует запрос, создавать ли таблицы для всех жестких дисков ПК. Опять-таки, если Вы согласны со всеми умолчаниями (чего я рекомендую не делать), Вы можете создать таблицы. В противном случае нужно отказаться. В данном случае не важно, проставлять ли галочку на строке ***Больше не спрашивать***, она дублирует один из флагов Панели настроек.

11. Настройте программу. Войдите в ***Настройки***. Создайте все нужные профили и поочередно настройте. Ниже описана настройка типичного **полного** профиля, нацеленного на ежедневную однократную проверку при включении ПК.

В панели ***Сканирование при загрузке*** рекомендую изменить задержку с 10 секунл на 5. Этого обычно достаточно, чтобы успели стартовать все автоматически запускаемые приложения.

Нажмите **Настроить выбранный вариант**. Исполняется вход в типовые настройки ADinf32, вкладка ***Таблицы***. Настройте все значения во всех вкладках, как указано ниже.

Типы CRC — лучше всего не трогать.

Диски — выберите те диски, которые Вы желаете контролировать с помощью ADinf. У меня на ПК из полудюжины локальных дисков (ДОС, Windows 3.11, Windows'98, Windows'NT, Unix...) только один контролируется ADinf32: тот, в котором ведется работа под Windows'98; диск под ДОСом контролируется ДОСовским вариантом ADinf, еще один - 16-битной версией... Решайте сами, но не забудьте, что выбранные нужно пометить галочкой в поле ***Диск выбран для сканирования*** (свое значение этого поля соответствует каждому диску, что не очень ясно при первом взгляде на вкладку).

Для нестандартных устройств (например, SCSI) иногда приходится выбирать метод доступа, отличный от BIOS.

Исключения — оставьте, как есть. Если Вы свободно ориентируетесь в файлах Вашей ОС, можете добавить что-либо в исключаемые из проверки файлы. Пользователи '95 / 'OSR2, вероятно, захотят добавить USER.DA* и SYSTEM.DAT или что-либо в этом роде. Вызовите ***Помощь*** и проверьте, не исключены ли такие файлы автоматически данной версией ADinf32.

Протокол — обязательно измените, т.к. по умолчанию там стоит **C:\ADINF32.LOG**. Писать в корень файл протокола не всегда удобно, лучше отправьте его в каталог с таблицами. Выберите ***Дополнять существующий файл***, пометьте ***Включать в протокол все изменения***.

Общие — если в Вашем ПК установлена звуковая карта, разрешите звуки. Если ПК лучше, чем Pentium-75, разрешите всплывающие подсказки. Уберите флаг ***Запрос подтверждения перед обновлением таблиц***. Если предполагаете использовать только один профиль - включите ***Автоматически начинать сканирование***.

Сканер — с версии 3.0 путь к сканеру уже настроен, если Вы правильно делали инсталляцию. А вот кое-что из параметров, возможно, придется подстроить.

Параметры командной строки сканера установите в соответствии с инструкцией к нему (я люблю для DrWeb32W добавлять параметр **/QU**, позволяющий в любом случае завершать работу DrWeb). Если Вы по каким-либо причинам хотите добавить, к примеру, проверку памяти — добавьте параметр **/TM** (или исключите **/NM**).

Проверьте, что флаги в полях ***Автоматически взаимодействовать со сканером, Автоматически запускать сканер*** и ***Проверять все измененные файлы*** уже стоят.

Файл обмена информацией по умолчанию предлагается находящимся в корне диска **C:**. Я обычно перевожу его в каталог, где находится DrWeb32W.

12. Продолжаем инсталляцию. А Вы думали, что уже все в порядке?? ;-) Выйдите из программы ADinf32 и **установите регистрационный ключ!** Если он выдан Вам в виде EXE-модуля — запустите модуль на исполнение, если в виде KEY-файла — поместите его в каталог, в который выполнена установка.

Деинсталляция

Для деинсталляции ADinf32 Вы можете воспользоваться вызовом модуля **Uninstall** из папки, в которой установлен ADinf32, либо сервисом ***Установка и удаление программ*** в ***Панели управления***.

Не следует пользоваться возможностью **Uninstall**, если Вы вопреки рекомендациям не установили ADinf32 в отдельный каталог.

В процессе удаления могут быть заданы вопросы относительно ряда файлов, входящих в поставку, которые могут, в принципе, быть использованы и другими программами, но на данный момент не используются. Для версии 3.0 этими файлами являются **CleanUp.dll** и **CleanUp2.dll**. По каждому файлу задается отдельный вопрос, но в нем есть ответ ***Да для всех***, подтверждающий удаление всех файлов (правда, при таком ответе Вас переспросят еще раз).

После успешного исполнения деинсталляции может быть выведена рекомендация о перезагрузке ПК в целях удаления рабочих файлов, использованных самой программой удаления.

Моя практика показывает, что на самом деле из папки удаляется далеко не все: остаются LOG-файлы, остается регистрационный ключ, остаются INF-файлы с таблицами. Могут случайно или вследствие разных причин остаться и другие файлы. Их необходимо удалять вручную, если Вы не собираетесь инсталлировать ADinf32 заново.

В реестре в HKEY_CURRENT_USER\Software\ADinf могут также остаться неудаленные элементы. На ПК, который используется более чем одним пользователем, эти элементы могут остаться и в других местах.

V. Сторож SpIDer Guard

5.1. Общие сведения о SpIDer

Программа SpIDer Guard[1] предназначена для 32-битных операционных систем семейства Windows, текущая версия работоспособна в версиях Windows'95, OSR2 и '98 (для Windows'NT в комплекте поставляется специальная версия SpIDer'a, пока не работоспособная на серверах).

SpIDer в активном режиме своей работы постоянно находится в памяти ПК, обнаруживая вирусы в моменты открытия/закрытия файлов работающими приложениями, а также анализируя проявления вирусной активности. Искушенный пользователь может управлять принципом "включения в работу" антивирусной проверки, например, нацеливая сторож на запускаемые и открываемые на чтение файлы или, напротив, на вновь образуемые на данном ПК.

Сторож SpIDer, как и его собрат DrWeb32, использует эвристический анализатор, позволяющий обнаруживать не зарегистрированные в базе вирусы по особенностям кода программы. Естественно, в этом случае речь может идти только о подозрительных файлах, но не о точной диагностике. Разумеется, эта возможность сторожа отнимает дополнительные ресурсы вычислительной мощности ПК.

SpIDer использует антивирусную технологию SpIDer-Netting, нацеленную в первую очередь на противодействие неизвестным вирусам. Этот метод позволяет обнаруживать и блокировать широкий класс Windows-вирусов по их действиям в операционной среде. Благодаря этому многие новые Windows-вирусы будут обнаружены и их распространение остановлено еще до того, как их образцы попадут к разработчикам антивирусов и будут включены в антивирусные базы сканеров. Более того, как следствие, это позволит также предотвращать возможный ущерб, наносимый такими вирусами компьютерным системам. Так, например, новая технология обеспечивает перехват любых вирусов, построенных на базе алгоритмов печально известного вируса **Win95.CIH**.

В целом, работа программы выглядит следующим образом. Каждая попытка обращения (чтения, записи или исполнения — настраивается пользователем) каждого приложения к тому или иному

[1] Авторы: *И. Данилов, В. Лутовинов, Д. Белоусов, А.Башаримов, С.Попов*.

файлу перехватывается модулем SpIDer'a, и файл проверяется на зараженность. Дополнительно работает анализ вирусной активности. Получив от одного из своих блоков сигнал о вирусе, SpIDer приостанавливает работу приложения и поступает с зараженным или "подозрительным" файлом так, как предопределено в настройках SpIDer'a. Например, он может блокировать обращение приложения к файлу, может вылечить вирус, может запросить оператора, что делать.

Получив общее представление о возможностях программы, следует настроить SpIDer на необходимые режимы работы самостоятельно. Детали настроек во многом аналогичны DrWeb32W, сгруппированы по панелям программы и рассмотрены в следующем подразделе. В целом, при настройке нужно решить следующие вопросы.

* SpIDer способен отбирать файлы для проверки по их внутренней структуре или по расширению имени файла. Следует определить способ отбора.

* Поставляемая вместе с программой база известных вирусов позволяет многие пораженные вирусами файлы излечить. Ряд вирусов, однако, портят файлы необратимо. Нужно определить, что делать с излечимыми и неизлечимыми файлами.

* SpIDer имеет блоки эвристического анализа и анализа вирусной активности, позволяющие в ряде случаев заподозрить неизвестные вирусы в отдельных исполняемых модулях и других файлах. Необходимо четко определить реакцию программы на такие "подозрительные" файлы.

* В процессе работы SpIDer ведет протокол. Состав и параметры его необходимо задать.

* Можно задать ряд дополнительных возможностей — например, исключить ряд каталогов из проверки.

После своей установки программа SpIDer Guard формирует значок в правой части Панели Задач (точнее, на **System Tray**) Windows. Начиная с версии 4.13, само наличие этого значка после загрузки Windows свидетельствует об активности SpIDer'a. Для настройки программы SpIDer, в том числе его включения в активное состояние или исключения из такового, нужно щелкнуть на данном значке и изменить установки в появившихся Панелях управления. Новые значения установок вступят в действие только после перезагрузки Windows.

5.2. Настройка работы SpIDer

Настройка работы программы исполняется в Панелях настройки. Эти панели и пункты настройки во многом аналогичны панелям настройки программы DrWeb32W, рассмотренным в подразделе 3.2.

Три общих кнопки внизу панелей определяют действия программы по завершении работы с настройками. Подтверждающая кнопка ***OK*** вызывает автоматическое запоминание сделанных изменений и, поскольку любые изменения вступают в силу только после перезагрузки Windows, предлагается перезагрузиться. Кнопка ***Отмена*** означает отказ от всех сделанных изменений. ***Справка*** вызывает встроенную систему помощи.

Панель *Проверка*

На этой панели задаются общие свойства SpIDer: вариант режима проверки, подключение дополнительных блоков проверки и

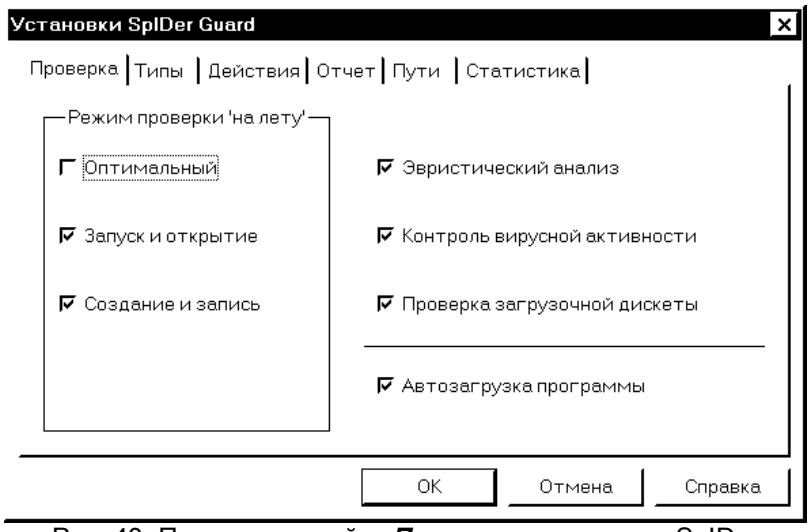


Рис. 43. Панель настройки ***Проверка*** программы SpIDer

сама необходимость наличия SpIDer'а в памяти ПК.

Т.к. загруженный в память SpIDer всегда активен, то снятие флажка ***Автозагрузка программы*** вызывает при следующей загрузке исключение программы SpIDer из загружаемых средств поддержки Windows. Для обратного включения SpIDer'а в работу нужно по меню

выполнить вызов программы, как и любой другой; однако реальное ее подключение будет только после перезагрузки Windows.

Режим проверки на лету представлен блоком настроек, определяющим режимы работы программы SpIDer, причем если включена опция ***Оптимальный***, то прочие недоступны, а если отключена — доступны порознь.

Выбор ***Оптимальный*** оставляет за авторами SpIDer определение моментов антивирусной проверки. В версии 4.17 это значит, что:

— на локальных жестких дисках проверяются только файлы, открываемые на запись (запускаемые программы не проверяются, т.к. открываются на чтение);

— на сетевых жестких дисках проверяются все открываемые файлы;

— на сменных носителях проверяются все открываемые файлы.

Выбор режима проверки ***Запуск и открытие*** заставляет SpIDer проверять все открываемые на чтение и запускаемые файлы. При использовании DrWeb32, в том числе в связке с ADinf32, этот режим вызовет ненужные двукратные проверки одних и тех же файлов с соответствующим расходом ресурсов.

Включенный режим ***Создание и запись*** заставляет SpIDer проверять все создаваемые файлы и существующие при *открытии для их изменения*[1]. Запускаемые программы не проверяются.

Флаг в поле ***Эвристический анализ*** заставляет программу SpIDer подключить эвристический анализатор, позволяющий обнаруживать новые, неизвестные заранее вирусы, анализируя код приложений перед их запуском. Точный алгоритм работы является собственностью авторов программы и не подлежит оглашению.

Флаг в поле ***Контроль вирусной активности*** заставляет программу SpIDer задействовать анализатор активности — специальный режим работы, позволяющий обнаруживать и блокировать попытки вирусов (в том числе неизвестных и даже не определяемых эвристическим анализатором) заражать файлы. Если этот режим включен, то при некоторой очередной попытке заражения файла в случае “веских подозрений” будет выдано на экран предупреждение о возможной вирусной активности с приостановкой работы подозрительного приложения. Оператор своим ответом может блокировать работу ОС,

[1] В отличие от открытия файлов исключительно для чтения

но может и просто запретить исполнение операции записи в файл (следует иметь в виду, что при некоторых типах резидентных вирусов результирующий файл к этому моменту уже может быть разрушен).

Флаг в поле ***Проверка загрузочной дискеты*** заставляет программу SpIDer при завершении работы с ПК в Windows проверять на вирусы вставленную в дисковод дискету, если таковая обнаружена. Это делается на тот случай, когда в BIOS не отключена загрузка с дискеты **A:** при ее наличии, чтобы таким образом вирус случайно не попал в ПК. Попытка проверки исполняется вне зависимости от наличия или отсутствия дискеты в дисководе. Если BIOS ПК позволяет блокировать загрузку с дискеты, рекомендуется это выполнить, а данный флаг отключить.

Панель настройки *Типы*

В этой панели задается метод отбора файлов программой SpIDer для проверки на вирусы. Устройство этой панели аналогично

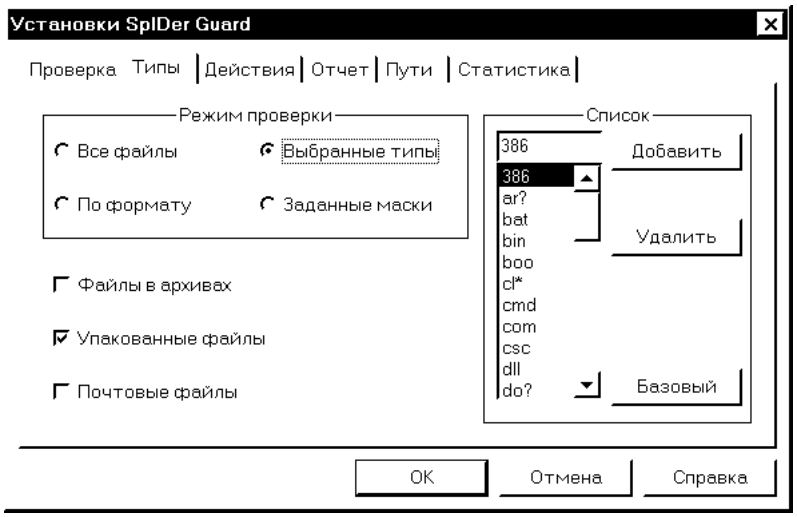


Рис. 44. Панель настройки ***Типы*** программы SpIDer

одноименной панели DrWeb32W (с.31).

В блоке ***Режим проверки*** задается отсев проверяемых файлов по их категориям. По умолчанию ставится вариант ***По формату***, означающий автоматический отбор проверяемых файлов в зависимости от их содержания, а не наименования. Именно этот

режим удобней всего в большинстве случаев. Однако, существует режим сплошной проверки ***Все файлы***, а также возможности отбора файлов по их расширению (***Выбраные типы*** с указанием в таблице исчерпывающего списка) или маске, полностью аналогичные соответствующим режимам DrWeb32W.

Действие флагов ***Файлы в архивах, Упакованные файлы*** и ***Почтовые файлы*** также полностью аналогично одноименным флагам DrWeb32W.

Панель *Действия*

Здесь задается реакция программы на каждый тип обнаруженного объекта. Эта панель также похожа на соответствующую панель

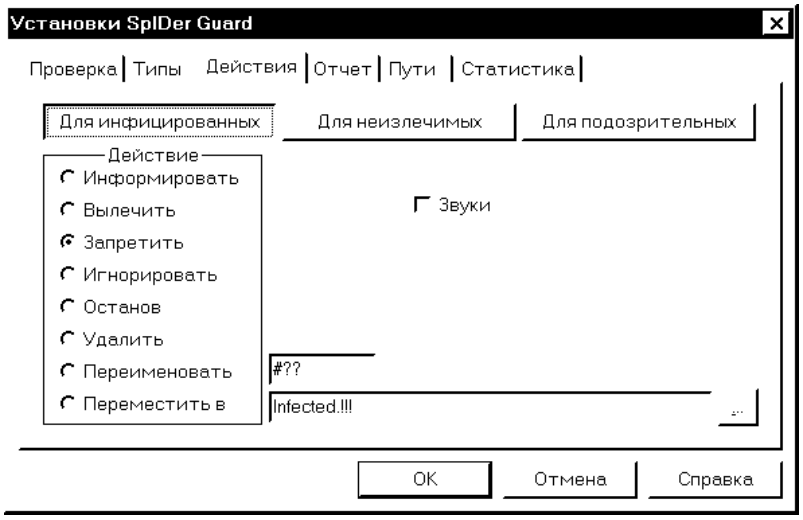


Рис. 45. Панель настройки ***Действия*** программы SpIDer

настройки программы DrWeb32W (см. стр. 33), но список вариантов каждого типа объектов несколько отличен от DrWeb32W. Дело в том, что в сканере DrWeb32W сам сканер является активно действующим приложением и “может позволить” себе игнорировать, лечить, переименовывать, перемещать или удалять объекты, зараженные или подозрительные. В случае же сторожа SpIDer, однако, изначально активной является та или иная программа, а SpIDer исполняет роль ограничителя доступа (хотя также может “на лету” излечить файл при затребовании его какой-либо программой). Поэтому, список воз-

можных действий при обнаружении зараженного или “подозрительного” объекта в данном случае включает следующие альтернативы.

Информировать — сообщить в отчет и, приостановив работу приложения, запросить, что с файлом делать.

Вылечить, Удалить, Переименовать и ***Переместить в*** — понятны по смыслу и полностью аналогичны соответствующим реакциям программы DrWeb32W. Так же, как и для DrWeb32W, ряд функций могут быть недоступными ввиду ограничений, наложенных в файле регистрационного ключа.

Игнорировать — по методике авторов программы, невозможно для однозначно инфицированных, но неизлечимых файлов.

Запретить — специфический вариант реакции сторожа, заключающийся в том, что программе, затребовавшей данный файл, будет заблокирован к нему доступ. Дальнейшее “поведение” программы зависит от качества ее написания: обрабатываются ли ею ошибки доступа.

Останов — еще более сильная по сравнению с предыдущей реакция сторожа, заключающаяся в том, что будет выполнен останов работы Windows. Предполагается, что в этом случае пользователь или системный администратор в дальнейшем сможет избавиться от зараженного объекта (например, вызвав для лечения сканер DrWeb386 из-под DOS’а или иным образом).

Разумеется, как и для DrWeb32W, не все альтернативы допустимы для всех трех типов ситуаций. Напомним, что реакцию программы следует задать для *всех* типов привлекших внимание объектов: ***Инфицированных, Неизлечимых*** и ***Подозрительных.***

На этой же панели есть флажок ***Звуки***, включение которого разрешает программе SpIDer задействовать специальные звуковые файлы из комплекта поставки для информирования пользователя о ситуации. До версии 4.17 звуки проигрываются пока что на встроенный спикер.

Панель *Отчет*

Здесь следует задать параметры отчета (протокола работы SpIDer). Панель полностью аналогична соответствующей панели DrWeb32W (см. стр. 34). Единственная разница в том, что флаг ***Статистика*** в группе ***Детали*** до версии 4.17 включительно не выводит общих данных в отчет.

Панель *Пути*

Здесь можно указать исключаемые из проверок каталоги и/или изменить умалчиваемое местонахождение вирусных баз. Эта панель структурой и содержанием также полностью аналогична соответствующей панели программы DrWeb32W (стр. 36).

Панель *Статистика*

Здесь находится сводка результатов, достигнутых с момента начала сеанса работы Windows (поскольку SpIDer активизируется все-

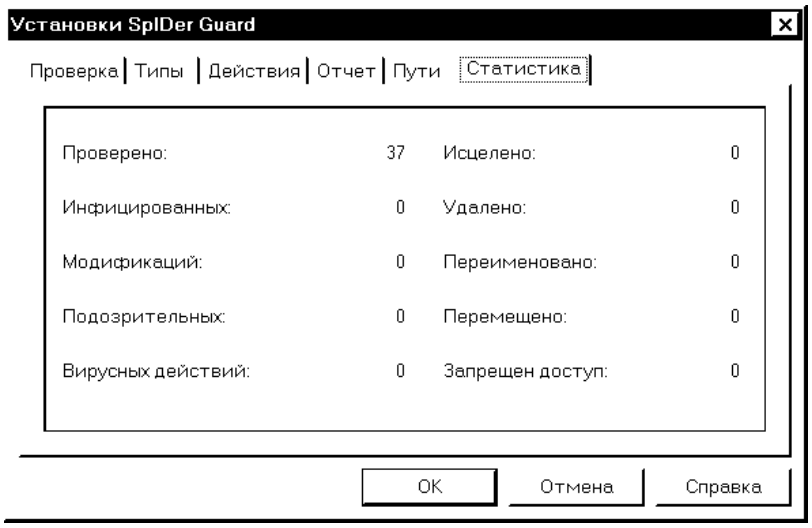


Рис. 46. Панель ***Статистика*** программы SpIDer

гда в начале работы сеанса и завершает свою работу также одновременно с Windows). Панель во многом напоминает Окно просмотра статистики DrWeb32W (см. стр. 27).

Проверено — включает общее число проверенных файлов.

Инфицированных — указывает количество объектов, инфицированных известными, “стандартными” вирусами.

Модификаций — показывает количество объектов, инфицированных модификациями “стандартных” вирусов.

Подозрительных — указывает число объектов, подозрительных на наличие вирусов как результат эвристического анализа. Это могут быть как объекты, пораженные не указанным в вирусных базах

вирусом, так и незараженные объекты, содержащие “подозрительный” код. Рекомендуется внимательно проанализировать изменения в файлах — например, с помощью программы ADinf32.

Вирусных действий — счетчик подозрительных воздействий, отмеченных анализатором вирусной активности. Ненулевые значения могут отражать как наличие на Вашем ПК неизвестных вирусов, так и “подозрительное” поведение ряда специфических программных приложений. Рекомендуется тщательный анализ изменений в файлах — например, с помощью программы ADinf32.

Исцелено, Удалено, Переименовано, Перемещено — соответственно числа успешно вылеченных файлов, удаленных, переименованных и перемещенных по вашим приказам (операции, выполняемые с инфицированными и подозрительными файлами, назначаются в панели ***Действия***).

Запрещен доступ — число запретов доступа к объектам программой SpIDer.

ЗАКЛЮЧЕНИЕ

Описанные в данной работе программные средства непрерывно совершенствуются и развиваются.

Doctor Web для Win32 позволяет теперь обнаруживать очень опасные полиморфные Win32-вирусы нового семейства **Win32.Kriz**. Подобно нашумевшим вирусам семейства **Win95.CIH** ("Чернобыль"), эти вирусы способны нанести ущерб аппаратной части компьютера.

Постоянно совершенствуются удобства пользователя. Начиная с версии 4.17, Doctor Web позволяет очень удобно “нацеливать” его на любой объект файловой структуры, имеющий отражение на Рабочем столе: достаточно на этом объекте щелкнуть правой кнопкой мыши и выбрать в полученном меню пункт проверки этого объекта сканером.

Планируется увеличить удобства пользователя, дифференцируя причину невозможности излечения излечимого в принципе вируса, планируется включить обработку почтовых файлов и многое другое.

В программе SpIDer Guard постоянно совершенствуется технология выявления подозрительных действий приложений.

Версия 3.0 программы ADinf32 успешно разбирает файловую систему NTFS для Windows/NT. Добавлена поддержка магнитооптических дисков. Учтена недокументированная особенность формирования имен файлов на FAT-разделах под Windows NT.

Описанные антивирусные средства имеют престижные международные награды. Doctor Web неоднократно награжден известным дипломом “Virus Bulletin 100%”.

Дополнительную информацию о текущих версиях программ **Doctor Web** и **SpIDer Guard** можно найти на сервере **www.drweb.ru**.

Дополнительную информацию об особенностях текущих версий **ADinf** можно получить на сервере **www.adinf.ru**.

Антивирусные средства ЗАО “ДиалогНаука” непрерывно совершенствуются, обеспечивая надежный заслон против вредоносных программ. Информацию о последних версиях всех программ, свежие новости, статьи, условия подписки и многое другое можно посмотреть на сервере **www.DialogNauka.ru**.

Координаты ЗАО "ДиалогНаука"

Адрес: **117786 Москва, ул.Вавилова, д.40, офис 103**.
Тел.: **(095)137-0150, 135-6253**
Тел./факс: **(095) 938-2970, 938-2855**
E-Mail: **Antivir@DialogNauka.ru**
Сервер WWW: **http://www.DialogNauka.ru**
BBS (круглосуточные линии):
(095) 938-2856 (28800/V.34) — линия общего доступа;
(095) 938-2867 (28800/V.34, 33600/V.34+) – подписчики;
(095) 938-2969 (28800/V.34, 33600/V.34+) – подписчики;
(095) 939-3705 (28800/V.34, 33600/V.34+) – подписчики.
Серверы FTP:
ftp://ftp.DialogNauka.ru
ftp://ftp2.DialogNauka.ru
ftp://ftp3.DialogNauka.ru
FidoNet: **2:5020/69**

Об авторе

Терентьев Александр Макарович, ведущий научный сотрудник ЦЭМИ РАН, кандидат технических наук. Автор Help'ов к программам Doctor Web для Windows и SpIDer Guard версии 4.10.
Тел.: **(095)332-4638 [среда, пятница 16.00-18.00]**
E-Mail: **tam@cemi.rssi.ru**
NickName: **Alex Trenty**
FidoNet:
2:5020/614.13
2:5020/1507.13

Список терминов и сокращений

Adinf Cure Module — лечащий модуль, дополнительная антивирусная программа, исполняющаяся в MS-DOS или как 16-битное приложение Windows **16**

ADinf32 — Advanced DiskInfoscope, ревизор дисков, один из основных компонентов антивирусного комплекта "ДиалогНаука" **16**

BIOS — Basic Input/Output System, набор программ, среди прочего, управляющих действиями ПК до загрузки операционной системы. Ранее BIOS фабричным способом прописывался в специальные микросхемы ПЗУ. Теперь часто используется flash-ROM, или ЭППЗУ, с возможностью перезаписи нового содержимого "на лету", в процессе работы ПК..... **6**

Doctor Web для Windows 9x/NT — комплект антивирусных программ, работоспособных как 32-битные приложения в Windows, плюс DrWeb386 для DOS **21**

HDD — Hard Disk Drive, накопитель на жестком магнитном диске..... **11**

MBR — Master Boot Record, заголовок HDD, содержащий начальный загрузчик и таблицу разделов тома..... **71**

SpIDer Guard — сторож, существует только в виде 32-битной компоненты, пока для сред Windows 95/98 ..... **15**

WinWord — Microsoft Word for Windows **6**

ЛИТЕРАТУРА

1. Безруков Н.Н. Компьютерные вирусы. — М.: Наука, 1991.- 160 с.
2. Безруков Н.Н. Компьютерная вирусология: справочное руководство. — Киев: Укр. сов. энцикл., 1991.- 416 с.
3. Данилов И.А. Антивирус Doctor Web для Windows 95/98/NT: Краткое руководство пользователя. — М.: ДиалогНаука, 2000 - 20с.
4. Дронов В. "Один на один с макровирусом". // "Мир ПК", N4-1998, с.66-67.
5. Лозинский Д.Н., Мостовой Д.Ю., Данилов И.А. и др. Антивирусный комплект DSAV 2.0. Руководство пользователя. — М., ДиалогНаука, 1998.
6. Ломов А. ДОС и теперь живее всех живых. — Hard'n'Soft, N2-1998, с.50.
7. Михайлов Е. Защитите ваши данные — Мир ПК, N4-1998, с.70-73.
8. Мостовой Д.Ю. Современные технологии борьбы с вирусами // Мир ПК, N 8, 1993, с.82-85.
9. Островский С. Л. Компьютерные вирусы. Выпуск 4 — М.: ДиалогНаука, 1997, - 88 с.
10. Терентьев А.М. Многопользовательский режим работы на персональных ЭВМ. Средства системной поддержки / #WP/99/071 — М.: ЦЭМИ РАН, 1999 - 79с.
11. Терентьев А.М. Формирование профессиональной рабочей среды универсального пользователя ПЭВМ в экономических ВУЗах. //Компьютерные системы в обучении экономистов. — М.: ЦЭМИ РАН, 1992, с.150-168.
12. Фролов А. В., Фролов Г. В. Осторожно: компьютерные вирусы. — М.: ДИАЛОГ-МИФИ, 1996. - 256 с. - (Персональный компьютер - шаг за шагом; Т. 5)

— Для заметок —

Терентьев Александр Макарович
Антивирусная защита ПК в Windows 95/98/NT

Издательство ОАО “Перспектива”

Формат 84x108 1/32. Печать офсетная. Объем 3,25 печ.л.
Тираж 1500 экз. Заказ N 185

Отпечатано с готового оригинал-макета в типографии ОАО “Перспектива”
107082, Москва, Переведеновский пер., д. 21