**В.М.ЗИМА, А.А.МОЛДОВЯН**

# МНОГОУРОВНЕВАЯ ЗАЩИТА ОТ КОМПЬЮТЕРНЫХ ВИРУСОВ

***Утверждено в качестве учебного пособия***

***ВОЕННАЯ ИНЖЕНЕРНО-КОСМИЧЕСКАЯ АКАДЕМИЯ имени А.Ф.МОЖАЙСКОГО***
**Санкт-Петербург - 1997**

**ББК 32.973**
**З-40**
**УДК [681.324+681.3.067] (075.8)**

Зима В.М., Молдовян А.А. Многоуровневая защита от компьютерных вирусов: Учеб. пособие. - Спб, 1997. - 170 с.

Рассматриваются основы теории и практики антивирусной безопасности в вычислительных системах. Описываются основные этапы жизненного цикла вирусов, их объекты внедрения, режимы функционирования и специальные функции. Рассматриваются схемы заражения файлов и загрузчиков, а также используемые вирусами способы маскировки. Приводится классификация вирусных программ. Детально излагаются основы построения многоуровневой системы защиты от компьютерных вирусов. Описываются основные этапы восстановления компьютера после заражения вирусными программами. Рассматриваются существующие типы антивирусных средств и их принципы функционирования. Описываются способы практической реализации многоуровневой антивирусной защиты в операционных средах MS-DOS, Windows 3.11 и Windows 95.

Для курсантов и слушателей академии, специализирующихся в областях, связанных с защитой информационно-программного обеспечения, а также всех пользователей компьютерных систем, заинтересованных в безопасности хранения и обработки данных.

Рецензент: В.Н.КУСТОВ, доктор технических наук, профессор

# СОДЕРЖАНИЕ

# ПРЕДИСЛОВИЕ

Стремительное внедрение средств вычислительной техники во все сферы человеческой жизнедеятельности привело к появлению массы новых угроз безопасности людей.

Эти угрозы, с одной стороны, связаны с тем обстоятельством, что информация, как результат автоматизированной обработки, стала определять действия не только все большего числа людей, но и все большего числа технических систем, созданных человеком. Отсюда становятся понятны последствия потери информации, хранящейся в вычислительных системах, а также нарушения работоспособности самих вычислительных средств.

С другой стороны, из-за резкого возрастания объемов хранимых и обрабатываемых в вычислительных системах конфиденциальных данных увеличилось количество предпосылок к хищению этой информации, а соответственно - количество предпосылок к нанесению ущерба, так как воздействовать на любую систему (социальную, биологическую или техническую) с целью ее уничтожения, снижения эффективности функционирования или воровства ее ресурсов (денег, товара, оборудования и т.д.) возможно только в том случае, когда известна информация о ее структуре и принципах функционирования.

Одним из основных видов угроз целостности и конфиденциальности информации, а также работоспособности вычислительных систем являются преднамеренные угрозы, реализация которых заранее планируется злоумышленником для нанесения вреда. Этот вид угроз по субъекту непосредственной реализации можно разделить на две группы:

- угрозы, реализация которых выполняется при постоянном участии человека;

- ♦ угрозы, реализация которых после разработки злоумышленником соответствующих компьютерных программ выполняется этими программами без непосредственного участия человека.

Первый тип угроз называют угрозами несанкционированных действий со стороны людей, а второй - со стороны программ, созданных людьми.

Задачи по защите от реализации угроз каждого из данных типов одинаковы:

1) преградить несанкционированный доступ к ресурсам вычислительных систем;
2) сделать невозможным несанкционированное использование компьютерных ресурсов, если доступ к ним все-таки осуществлен;
3) своевременно обнаружить факт несанкционированных действий и устранить причины, а также последствия их реализации.

Способы же решения перечисленных задач по защите от несанкционированных действий со стороны людей и компьютерных программ существенно отличаются друг от друга.

Данное пособие посвящено рассмотрению основных способов защиты от компьютерных программ - программ, специально разработанных для выполнения несанкционированных действий без непосредственного участия злоумышленника. Такие программы называют компьютерными вирусами или вирусными программами.

Начало интенсивного развития вирусных программ совпадает с началом широкого распространения вычислительной техники. Появление персонального компьютера в 80-х годах и дальнейшее внедрение вычислительных систем во все сферы жизни общества привели к интенсивной разработке и распространению компьютерных вирусов. Признаками вспышки каждой очередной вирусной эпидемии в компьютерном мире были массовые потери информации и нарушения работоспособности вы-

числительных систем, ставшие причинами нанесения морального, материального, а иногда и физического ущерба людям, находящихся в зависимости от результатов автоматизированной обработки данных.

Возникает вопрос - почему же все-таки появились компьютерные вирусы? Ответ прост и вытекает из следующих особенностей нашей реальности:

- всегда найдутся люди, которые хотят нанести вред другим, забывая о том, что этим же они делают хуже себе;
- для нанесения вреда могут использоваться и средства, первоначально созданные для принесения пользы.

Таким образом, изобретая очередное средство принесения добра, человек вынужден разрабатывать способы и меры защиты от использования этого средства во имя зла. Наиболее наглядным и глобальным примером здесь может служить пример, связанный с открытием ядерной энергии, которая до сих пор успешно используется как в мирных целях, так и для создания атомного оружия, нависшего угрозой над всем человечеством.

Аналогичная картина наблюдается и по отношению к вычислительным системам. Сразу же после изобретения компьютера нашлись люди, которые открыли способ использования и этого полезного инструмента во вред другим, заключающийся в разработке и внедрении компьютерных вирусов. Этот способ вредительства обладает важным достоинством для невежественных людей - возможностью анонимного нанесения ущерба, при котором можно скрыть все улики преступления, явно не раскрывая авторство вирусов.

В настоящее время борьба против компьютерных вирусов превратилась в борьбу между их разработчиками и остальными пользователями вычислительных систем. Несмотря на то, что авторы вирусов сами страдают от своих собратьев, они прикладывают все большие усилия для об-

хода совершенствующихся уровней антивирусной безопасности. Исход такой борьбы определяет степень надежности системы антивирусной защиты.

Оптимального варианта построения системы антивирусной безопасности можно достигнуть только при изначальной антивирусной ориентации операционной системы и аппаратных средств компьютера. К сожалению, такие наиболее часто используемые в нашей стране операционные системы как MS-DOS/Windows и Windows 95 не обладают встроенными средствами защиты от вирусов. Пользователю самостоятельно необходимо устанавливать и поддерживать все требуемые уровни антивирусной безопасности с помощью специализированных программных средств. Добиться эффективности этого процесса возможно только при знании и понимании основ многоуровневой защиты от компьютерных вирусов, чему и посвящено предлагаемое пособие.

# 1. ВВЕДЕНИЕ В КОМПЬЮТЕРНУЮ ВИРУСОЛОГИЮ

## 1.1. История появления компьютерных вирусов и факторы, влияющие на их распространение

Идею разработки и создания самовоспроизводящихся программ можно отнести к концу 60-х годов, когда впервые появились публикации о возможностях программ к самовоспроизведению. На основе этих публикаций были разработаны всевозможные игровые программы, позволяющие воспроизводить себе подобных после уничтожения в оперативной памяти компьютера других программных компонентов (например, игра "Дарвин").

В 70-х годах появились научно-фантастические произведения о программах-червях, способных распространяться по сети. В конце восьмидесятых одна из таких идей была претворена в жизнь аспирантом Корнельского университета в США Р.Моррисом. Желая испытать свои силы, он разработал и ввел в компьютер сети Internet программу-вирус. Для своего распространения вирус использовал некоторые дефекты сетевого программного обеспечения. В течении нескольких часов было заражено более шести тысяч компьютеров сети. Основным признаком наличия вируса была непрерывно возрастающая загрузка компьютеров, которая привела к прекращению функционирования многих сетевых узлов. Впоследствии после долгих судебных разбирательств Р.Моррис был осужден к двум годам условно, 400 часам общественных работ и штрафу в 10 тысяч долларов. Это событие было первым из столь внушительных массовых заражений компьютерным вирусом, которое положило начало периодическим всплескам компьютерной эпидемии.

В отличие от биологических, компьютерные вирусы создаются человеком. Сейчас в мире только по статистическим данным зарегистриро-

вано более пяти тысяч компьютерных вирусов для операционных сред MS-DOS/Windows, не говоря уже о других операционных системах.

Современное состояние проблемы вирусов характеризуется большим потоком новых вирусоподобных программ, вызывающих локальные инфекции. Как правило, при соблюдении правил защиты новые вирусы быстро обнаруживаются и уничтожаются. Однако, они успевают причинить вред недостаточно бдительным пользователям в районе своего размножения. Последней глобальной эпидемией, поразившей массу компьютеров в нашей стране, пожалуй, можно назвать только эпидемию вируса "DIR" в начале девяностых. Этот вирус после заражения компьютера разрушал на его магнитных дисках файловую структуру, что вело к потери хранящейся в ней информации.

Борьба с вирусами - это борьба со злом на информационном уровне. Эта борьба требует больших затрат времени и средств, а также высокой квалификации в области вычислительных систем, так как вирусы создаются высококвалифицированными программистами, учитывающими все самые детальные нюансы в функционировании компьютерной системы. Для эффективной защиты необходимы такие своевременные действия как сбор информации о новых вирусах, разработка, поддержка и распространение программ антивирусной защиты, а также многие другие меры, затрагивающие не только технические, но также законодательные и морально-этические стороны общества.

Перечислим наиболее существенные факторы, влияющие на распространение компьютерных вирусов в вычислительной среде:

**1)** наличие и эффективность уровня защиты от несанкционированного доступа пользователей к ресурсам вычислительных систем (ВС) [3];

**2)** наличие и эффективность уровня защиты от несанкционированного использования пользователями компьютерных ресурсов [3];

**3)** наличие и эффективность функций защиты от некорректного использования ресурсов ВС [3]:

- ⇒ недоступность со стороны прикладных программ привилегированных состояний процессора, а также привилегированных функций и режимов функционирования операционной системы;
- ⇒ защищенность системных областей оперативной памяти;
- ⇒ изолирование в оперативной памяти адресных пространств прикладных программ друг от друга;
- ⇒ невозможность доступа со стороны прикладных программ к ресурсам ВС в обход программного интерфейса операционной системы;
- ⇒ постоянное поддержание и непрерывный контроль целостности и непротиворечивости хранящейся и обрабатываемой информации;

**4)** наличие и эффективность многоуровневой программно-аппаратной защиты от компьютерных вирусов;

**5)** соблюдение организационных мероприятий по защите от компьютерных вирусов;

**6)** наличие в обществе и действенность мер уголовной ответственности за нарушение безопасности информационно-программного обеспечения ВС;

**7)** принятые в обществе морально-этические нормы поведения.

Важно подчеркнуть, что только при учете всех влияющих на защиту от компьютерных вирусов факторов можно будет гарантировать антивирусную безопасность информации, а также процесса ее обработки.

## 1.2. Понятие компьютерного вируса и основные этапы его жизненного цикла

Под компьютерным вирусом будем понимать компьютерную программу, разработанную с целью нанесения ущерба пользователям вычислительной системы. Основной особенностью большинства компьютерных вирусов является способность к скрытому саморазмножению [1]. Саморазмножение или, как его еще называют, репродуцирование вируса выполняется путем включения в исполняемые или хранящиеся программы своей, возможно модифицированной копии, сохраняющей способность к дальнейшему саморазмножению.

Свойство саморазмножения вирусов само по себе представляет одну из его опасностей и может привести к снижению, вплоть до нуля, производительности вычислительной системы. Это происходит за счет повышения количества ресурсов ВС, расходуемых на выполнение программ-вирусов:

- ♦ увеличивается время процессора, расходуемое на выполнение саморазмножающихся вирусных программ;
- ♦ увеличивается задействованное пространство оперативной памяти зараженного компьютера, которое последовательно занимают получаемые в результате саморазмножения копии вируса;
- ♦ увеличиваются объемы ресурсов внешних устройств, задействованных в процессе саморазмножения.

В современной технической литературе [2, 9, 10], посвященной проблемам компьютерных вирусов, часто встречаются термины, заимствованные из других отраслей науки, в частности, медицины, а также научно-фантастических книг. К таким терминам относятся, например, следующие - троянская программа, люк, червь и другие.

Под троянской программой понимается программа, имеющая законный доступ к компьютерной системе, но выполняющая вместе с основны-

ми и скрытые (необъявленные) функции, реализуемые посредством ее вирусоподобного компонента.

Люк - это недоработка внутри операционной системы, позволяющая вирусу получить ее привилегированную функцию или запрещенный режим работы.

Червем называют вирус, обладающий способностью распространения в вычислительной сети на основе маскировки под системные средства поиска ее свободных ресурсов.

Изобилие терминов в области антивирусной безопасности порождает путаницу и создает дополнительные трудности для понимания существа вопроса, так как путь к пониманию лежит через простоту, а все лишнее приводит к сложности.

Жизненный цикл компьютерного вируса может включать следующие этапы [1, 8]:

- внедрение (инфицирование);
- латентная фаза, в течении которой вирус не выполняет никаких действий;
- инкубационный период, в процессе которого вирус осуществляет саморазмножение;
- этап выполнения специальных целевых функций;
- фаза проявления, в процессе которой компьютерный вирус явно дает понять пользователю, что его компьютер заражен.

Перечисленные этапы, кроме первого, могут выполняться в любой последовательности, повторяться, и не все являются обязательными. Особую опасность представляют стадии выполнения специальных функций и саморазмножения, которые могут иметь катастрофические последствия для компьютерной системы. По отношению к саморазмножению имеется в виду полная потеря работоспособности отдельных компьютеров или вычислительной сети в целом.

Первой и обязательной стадией жизненного цикла вируса является внедрение в компьютерную систему с целью ее заражения (инфицирования). Инфицирование компьютера возможно только при запуске на выполнение зараженной или вирусоподобной программы. После активизации вируса могут заражаться выполняемые программы, а также программы, хранящиеся на внешних запоминающих устройствах. Как правило, копия вируса вставляется в инфицируемую программу таким образом, чтобы при запуске на выполнение зараженной программы вирус получал управление первым. Признаком инфицирования компьютерной системы является заражение любой ее программы.

В процессе латентной фазы вирус не выполняет никаких действий до тех пор, пока не установятся условия его активизации. В случае наступления состояния компьютерной системы, при котором выполняются условия активизации вируса, его текущая латентная фаза заканчивается, и вирус может начать либо инкубационный период, либо стадию выполнения специальных целевых функций, либо стадию проявления. Как правило, первым после латентной фазы наступает инкубационный период. Саморазмножение в процессе инкубационного периода может осуществляться вплоть до уничтожения вирусоносителя.

Одновременно или после определенного числа внедренных копий вирус может приступить к выполнению специальных целевых функций. Активизация вирусом процесса реализации специальных функций начинается при наступления условий их активизации, запрограммированных в теле вируса.

Вирус может иметь также фазу проявления, которая сопровождается визуальными или звуковыми эффектами. Отдельные вирусы явно сообщают пользователю о себе и заражении компьютера.

## 1.3. Объекты внедрения, режимы функционирования и специальные функции вирусов

### *1.3.1. Объекты внедрения*

Так как вирус является программой, то он может активизироваться и распространяться только путем запуска зараженных или вирусоподобных программ. Соответственно, вирус может внедряться только в другие программы. При этом под программой здесь понимается любая последовательность команд, подлежащих выполнению процессором или другой программой. Например, макросы, включаемые в файлы документов редактора Word, также по сути являются программами, так как представляют собой последовательности команд, выполняемых редактором для автоматизации действий пользователя.

Программы могут содержаться в файлах или некоторых компонентах системной области диска, участвующих в процессе загрузки операционной системы. Согласно этому различают:

- ♦ файловые вирусы, инфицирующие программные файлы;
- ♦ загрузочные (бутовые) вирусы, заражающие системные программы, хранящиеся в системных областях дисков.

Следует иметь в виду, что основную свою часть, называемую еще телом, вирус может хранить не только в программах, а в любой области внешней или внутренней памяти компьютера. В программах же должна храниться та часть вируса, которая используется для его активизации. Например, существует целый класс вирусов [1, 6], использующих для хранения своих тел свободные области дисковой памяти. Для маскировки и предотвращения доступа к этим областям со стороны других программ вирусы помечают кластеры этих областей как дефектные. После своей активизации вирус такого класса сразу же загружает в оперативную па-

мять из соответствующих кластеров свое тело и передает ему управление.

Файловые вирусы могут внедряться в файлы следующих типов:

**1)** программные файлы с компонентами операционной системы, например, IO.SYS, MSDOS.SYS, COMMAND.COM, WIN.COM, WININIT.EXE;

**2)** любые исполняемые файлы с расширениями .EXE и .COM;

**3)** командные файлы и файлы конфигурирования, например, AUTOEXEC.BAT, CONFIG.SYS, SYSTEM.INI, WIN.INI;

**4)** файлы, составляемые на макроязыках программирования, или файлы, которые могут включать выполняемые макросы, например, файлы документов редактора WORD, файлы баз данных СУБД ACCESS;

**5)** файлы с внешними драйверами устройств (обычно имеют расширения .SYS и .BIN);

**6)** объектные модули и библиотеки, файлы которых, как правило, имеют расширение .OBJ;

**7)** оверлейные файлы (обычно имеют расширение .OV? и .RTL);

**8)** библиотеки динамической компоновки, файлы которых имеют расширение .DLL;

**9)** исходные тексты программ.

Загрузочные вирусы могут заражать следующие программы:

- системный загрузчик, расположенный в стартовом секторе (BR) дискет и логических дисков;
- внесистемный загрузчик, расположенный в стартовом секторе (MBR) жестких дисков.

### 1.3.2. Режимы функционирования и специальные функции вирусов

Компьютерный вирус может функционировать резидентно или транзитно.

Резидентный вирус после своей активизации запрашивает у операционной системы участок оперативной памяти, копирует себя в него и объявляет, что данный участок задействуется для резидентной программы [1]. Этот вирус перехватывает требуемые прерывания, анализирует их, и при выполнении запрограммированных в нем условий реализует запланированные действия, после чего может передать управление стандартному обработчику прерываний. Тем самым со стороны вируса обеспечивается полный контроль за вычислительным процессом.

Резидентные вирусы после активизации постоянно находятся в оперативной памяти компьютера вплоть до его полной перезагрузки, выполняемой путем нажатия кнопки Reset или отключения и последующего включения питания компьютера. При неполной перезагрузке, реализуемой посредством одновременного нажатия комбинаций клавиш Ctrl+Alt+Del или путем выполнения команды **Пуск/ Завершение работы/ Перезагрузить компьютер** для Windows 95, резидентный вирус может сохранить свое тело в оперативной памяти. Более того, существуют резидентные вирусы, которые, если им помогают конструктивные особенности компьютера, могут сохранять свое тело в оперативной памяти даже после полной перезагрузки, выполняемой путем нажатия кнопки Reset. Поэтому единственным надежным путем удаления резидентного вируса из оперативной памяти является перезагрузка компьютера, реализуемая отключением и последующим (не ранее, чем через 20-30 секунд) включением его питания.

Транзитный вирус после запуска зараженной им программы выполняется только в момент нахождения этой программы в оперативной памя-

ти компьютера. Такие вирусы сложнее обнаружить, так как оперативную память они постоянно не занимают.

К специальным функциям вирусов, которые они могут выполнять после своей активизации, можно отнести любые функции по нанесению ущерба, реализация которых возможна на зараженном компьютере. К целевым функциям, наиболее часто реализуемыми вирусами, относятся следующие:

- низкоуровневое форматирование областей жесткого диска или дискет;
- полное уничтожение файлов и каталогов, исключающее возможность их восстановления;
- разрушение файловой структуры дисковых носителей информации;
- нарушение работоспособности компьютера путем модификации или уничтожения системных данных либо исполняемых файлов операционной системы;
- снижение производительности вычислительной системы в результате выполнения ложных программ или саморазмножения вирусов в оперативной памяти компьютеров;
- подмена выполняемых функций операционной системы или системы защиты с целью хищения информации, например, перехвата паролей;
- модификация содержимого информационных файлов;
- изменение данных, передаваемых через последовательные или параллельные порты.

Можно выделить две стратегии в выполнении вирусами своих специальных функций [8, 10]:

- нанесение крупного ущерба за короткий промежуток времени, что обнаруживается сразу же;

- периодическое выполнение мелких вредных действий, которых пользователь может не замечать длительное время.

Очень опасными являются мелкие повреждения содержимого информационных файлов, например, замена отдельных байтов, которые по причине трудности мгновенного обнаружения, могут со временем привести к «порче» значительного объема информации на внешних носителях.

## 1.4. Схемы заражения компьютерными вирусами

После своей активизации компьютерные вирусы, как правило, саморазмножаются. Специальные функции, в отличие от функций саморазмножения, выполняются вирусами достаточно редко. Такая стратегия используется для того, чтобы успеть создать достаточное количество своих копий, прежде чем факт заражения будет обнаружен пользователем.

Вирус в процессе саморазмножения осуществляет поиск компонентов системы, пригодных для заражения. Обнаружив такой компонент вирус активизирует процедуру внедрения. Обычно, эта процедура проверяет, не присутствует ли уже в объекте заражения копия вируса. Если копия отсутствует, то вирус из оперативной памяти внедряет свою копию в инфицируемый объект в соответствии с используемой схемой заражения. Если же копия вируса в зараженном объекте присутствует, то заражение не выполняется.

При определении наличия копии вируса в заражаемом объекте вирусом может быть осуществлена и проверка номера версии присутствующей копии. В этом случае инфицирование производится только при обнаружении более старой версии имеющейся копии вируса.

Рассмотрим последовательно существующие схемы заражения, используемые файловыми и загрузочными вирусам.

### *1.4.1. Схемы заражения файловыми вирусами*

Основным признаком разграничения существующих схем заражения исполняемых файлов является место файла, куда внедряется компьютерный вирус [1, 2, 6].

Наиболее часто используемым способом заражения является дописывание тела вируса к концу исполняемого файла (□). В этом случае в начало инфицируемого файла включается компонент активизации вируса. Включение этого компонента осуществляется путем изменения точки входа в программу или посредством замены соответствующих команд для передачи управления телу вируса. Тело вируса по окончании своей работы должно передать управление оригинальной программе.

Более редко используются схемы заражения, при которых вирус внедряется в начало или внутрь инфицируемой программы (см. □). Такие схемы заражения требуют переразмещения части исполняемого файла, что может быть сопряжено со значительной сложностью их реализации применительно к программам типа .EXE. Для облегчения процесса внедрения некоторые вирусы переделывают программы типа .EXE в тип .COM, так как программы с расширением .COM по причине своих конструктивных особенностей сразу же готовы к запуску и не требуют никаких настроек после загрузки в оперативную память. Вирус может внедряться в любое место COM-программы, раздвигая ее и изменяя точку входа в программу для передачи управления телу вируса.

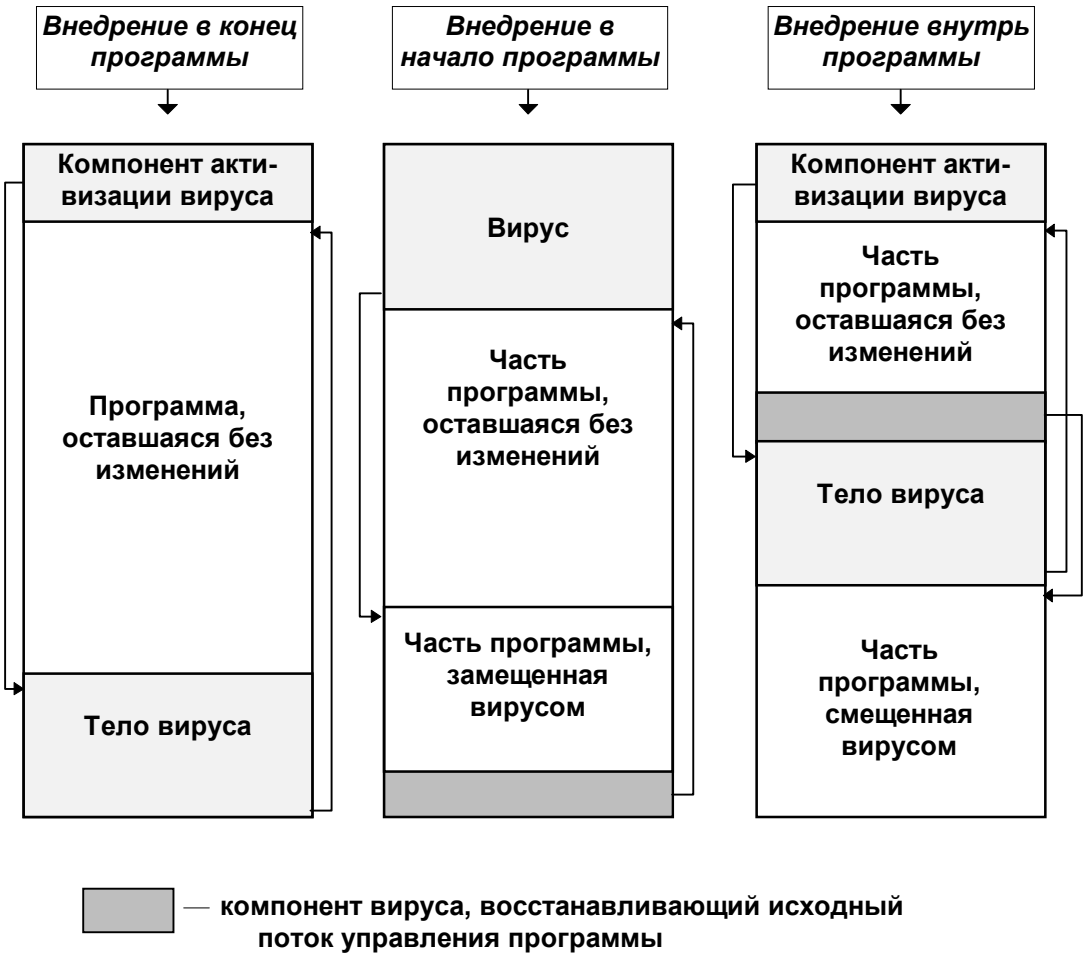


**Рис. 1.1. Схемы заражения файлов исполняемых программ**

Если основное тело вируса хранится вне файла внедрения компонента активизации вируса, например, в кластерах диска, объявленных вирусом дефектными, то в качестве тела вируса на □ будет выступать компонент вируса, предназначенный для поиска и передачи управления его основному телу, размещенному вне зараженного файла.

Следует отметить, что вирусы, тела которых хранятся вне зараженных файлов, могут использовать и более изощренные схемы заражения компьютера. Например, свое основное тело такой вирус может разместить в любом кластере диска, а все записи в каталогах, относящиеся к исполняемым файлам, изменить таким образом, чтобы в качестве первого

кластера этих файлов выступал кластер, содержащий код вируса. Таким образом, при запуске на выполнение любого исполняемого файла зараженного диска будет запускаться на выполнение сам вирус, который только по окончании своей работы загрузит в оперативную память запущенную пользователем программу и передаст ей управление. Подобная технология реализована в вирусе «DIR» [2].

При внедрении вируса в файл драйвера используется два основных способа [6]:

**1)** внедрение на основе модификации адресов процедур стратегии и прерывания;

**2)** внедрение на основе расширения драйвера до цепочки из нескольких драйверов.

В первом случае (□) вирус модифицирует заголовок драйвера, подменяя адреса процедур стратегии и прерывания [7], а также приписывает свое тело к концу файла драйвера. Встречаются вирусы, которые в заголовке драйвера изменяют адрес только одной из процедур (процедуры стратегии или процедуры прерывания).

Во втором случае (□) вирус модифицирует заголовок драйвера таким образом, что операционная система рассматривает инфицированный файл как цепочку из двух или более драйверов.

Аналогично приведенным способам вирус может записать свое тело в начало драйвера после его заголовка, а если в файле содержится несколько драйверов, то и в середину файла. Однако, эти способы реализуются труднее.

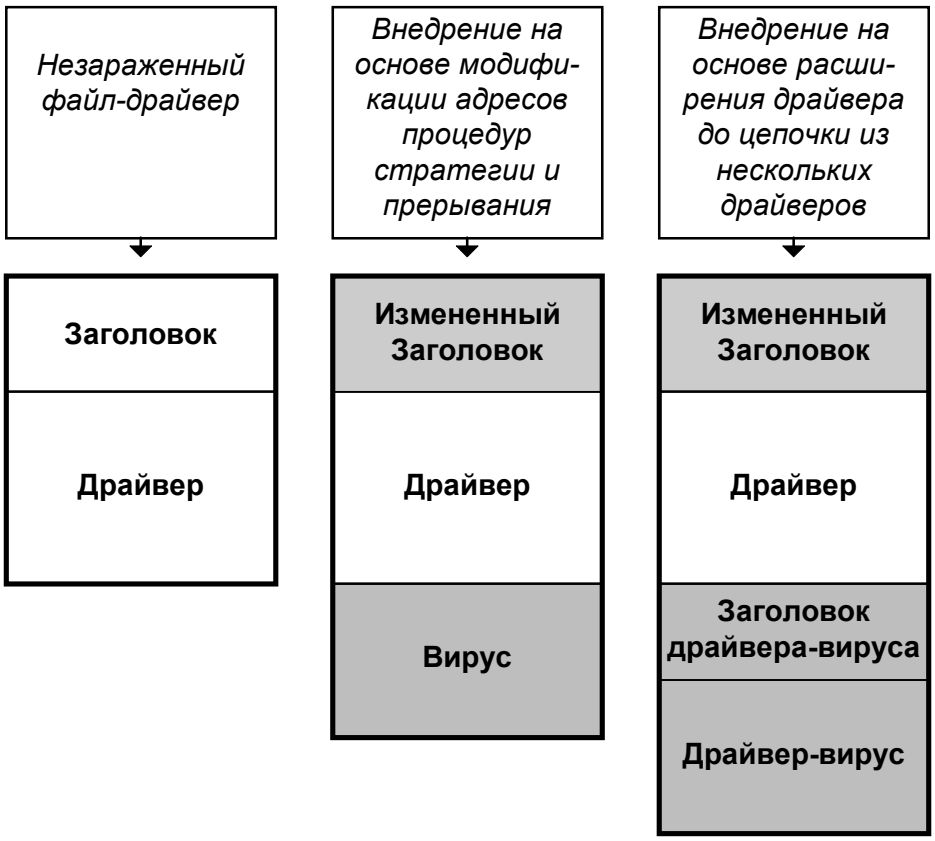


**Рис. 1.2. Схемы заражения файлов драйверов**

При внедрении вируса в файлы, которые явно не являются исполняемыми программами или драйверами, например, в объектные модули, библиотеки динамической компоновки или файлы, которые могут включать выполняемые макросы, место внедрения вируса определяется структурой и форматом файла каждого конкретного вида.

Особо опасными видами вирусов являются вирусы, прикрепляемые к объектной библиотеке какого-либо компилятора. Такие вирусы автоматически внедряются в любую программу, при компиляции которой была использована инфицированная объектная библиотека. При внедрении вируса в объектную библиотеку в нее вставляется подпрограмма с вирусом, а в начало остальных, либо отдельных подпрограмм вставляется вызов вирусной подпрограммы.

Вирус может быть внедрен и в командные файлы, а также файлы конфигурирования операционной системы, выполняемые при ее загрузке. В этом случае в такой файл помещается вызов программы, содержащей тело вируса.

В случае заражения библиотек с исходными текстами программ тело вируса в исходном виде помещается в начало какой-либо часто используемой процедуры, например, процедуры открытия диалогового окна. В результате, после компиляции и компоновки программы, использующей зараженную процедуру, вирус будет включен в состав полученной исполняемой программы.

### *1.4.2. Схема заражения загрузочными вирусами*

Загрузчик является компонентом операционной системы, продолжающим ее загрузку после аппаратной передачи ему управления процедурой начальной загрузки базовой системы ввода-вывода (BIOS).

Существует два основных загрузчика, используемых для загрузки операционной системы:

- внесистемный, расположенный в главной загрузочной записи (MBR), находящейся в начале жесткого диска;
- системный, расположенный в загрузочной записи (BR), находящейся в начале каждой дискеты и логического диска.

Внесистемный загрузчик используется в процессе загрузки операционной системы с жесткого диска и предназначен для загрузки в оперативную память системного загрузчика активного раздела винчестера и передачи ему управления.

Системный загрузчик применяется в процессе загрузки операционной системы с логического диска активного раздела винчестера или дискеты и предназначен для загрузки в оперативную память модуля расширения BIOS, а также передачи ему управления.

При заражении загрузчика [1, 2] вирус копирует исходное содержимое загрузочного сектора (BR или MBR) в свободный сектор диска, зарезервированный под нужды операционной системы, и затем внедряет свою копию на место загрузчика в загрузочный сектор (см. □). Если длина вируса больше длины загрузчика, то в загрузочный сектор помещается только компонент активизации вируса, а тело вируса размещается в других секторах, которые могут быть объявлены вирусом дефектными.

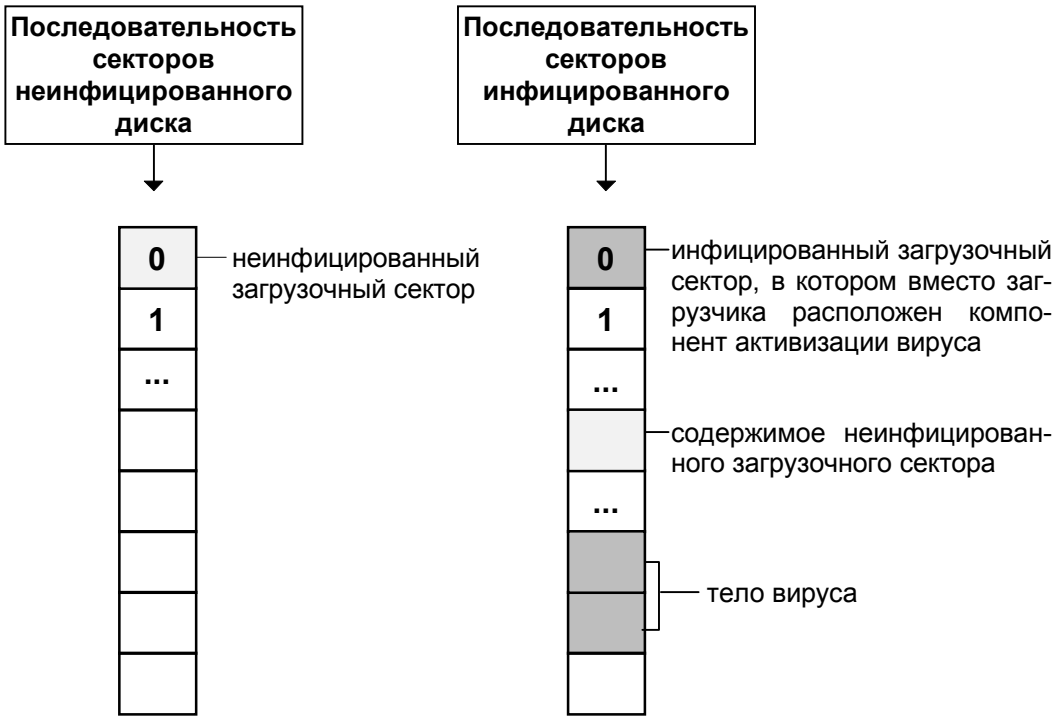


**Рис. 1.3. Схема заражения загрузочным вирусом**

Активизация загрузочного вируса осуществляется в процессе загрузки операционной системы. При этом происходит следующая последовательность действий:

**1)** после инициирования пользователем процесса загрузки операционной системы, например, включения компьютера или нажатия кнопки Reset, вместо загрузчика в оперативную память загружает-

ся вирус или компонент его активизации, и далее загруженной вирусной программе передается управление;

2) если запускается на выполнение компонент активизации вируса, то он находит тело вируса и активизирует его;
3) получив управление, вирус выполняет самоинициализацию (перенос своего тела в другую область памяти, перехват необходимых прерываний и т.д.);
4) после окончания своей инициализации вирус находит неповрежденный загрузчик в зарезервированном при заражении содержимом загрузочного сектора и загружает его в оперативную память с передачей ему управления.

После загрузки операционной системы вирус остается резидентно в оперативной памяти, выполняя запрограммированные в его теле действия.

## 1.5. Способы маскировки, используемые вирусами

Для затруднения своего обнаружения антивирусными программами компьютерные вирусы применяют множество способов маскировки, которые можно разбить на две базовые группы:

1) способы маскировки, основанные на перехвате прерываний, используемых операционной системой для доступа к компьютерным ресурсам;
2) способы маскировки, основанные на шифровании основного кода вируса.

Перехват прерываний операционной системы позволяет вирусу контролировать доступ к зараженным элементам данных. При попытке получения любой программой каких-либо характеристик зараженных файлов или загрузчиков вместо их реальных характеристик вирусом под-

ставляются фиктивные. Как правило, используются следующие приемы подстановки:

- при попытке определения длины инфицированного файла подставляется длина, которая была до его заражения;
- при попытке чтения содержимого зараженного файла вирус немедленно удаляет из файла свое тело, а при закрытии файла - заражает его опять;
- при попытке чтения зараженного системного или внесистемного загрузчика операционной системы вирус подставляет оригинальный загрузчик.

В результате выполнения перечисленных приемов вирусы могут быть невидимыми для антивирусных программ. Именно поэтому такие вирусы прозвали Stealth-вирусами (вирусами-невидимками).

В антивирусных программах после появления Stealth-вирусов проверка на наличие вирусов стала осуществляться в обход функций операционной системы на основе обращений к функциям BIOS или непосредственно к контроллерам дисководов. После обнаружения зараженных программ для определения факта наличия именно Stealth-вируса антивирусная программа может сравнить фактическую информацию о зараженных программах с информацией, полученной после запроса соответствующих функций операционной системы.

Следует отметить, что способы маскировки, основанные на перехвате прерываний, могут быть реализованы только в тех операционных системах, которые позволяют осуществить доступ к компьютерным ресурсам в обход предоставляемого ими программного интерфейса, например, в MS-DOS/Windows 3.11 (3.1) и Windows 95.

Использование вирусами способов маскировки, основанных на шифровании основного кода вируса, позволяет достичь эффекта, при котором синтезируемые в процессе саморазмножения копии вирусов отли-

чаются друг от друга. Эта особенность затрудняет процесс их обнаружения с помощью сигнатурного поиска, и из-за этой особенности такие вирусы были названы вирусами-мутантами.

Вирус-мутант состоит из двух основных частей:

**1)** расшифровщика, предназначенного для расшифровки основного кода вируса перед его исполнением;

**2)** зашифрованного основного кода вируса.

Основной код вируса, кроме компонентов, присущих обычному вирусу, содержит также шифратор, предназначенный для зашифровывания основного кода вируса при саморазмножении.

После активизации вируса первым получает управление расшифровщик, который расшифровывает основную часть вируса и передает ей управление. В процессе саморазмножения в каждую внедряемую копию вируса помещается расшифровщик, а также зашифрованный основной код. Важной особенностью является то, что для каждой новой копии основной код вируса зашифровывается по новому ключу. Ключ может зависеть от характеристик заражаемого файла. Именно за счет использования разных ключей шифрования и обеспечивается отличие между разными копиями вируса.

Для того, чтобы в различных копиях вируса-мутанта были и разные расшифровщики, авторы вирусов стали включать в основной код вируса генератор расшифровщиков. Основной и единственной функцией генератора расшифровщиков является создание для каждой новой копии вируса другого по виду, но такого же по функциям расшифровщика. Вирусы-мутанты, включающие генератор расшифровщиков называют полиморфными.

Для обнаружения вирусов-мутантов, а также полиморфных вирусов анализируются возможные места внедрения вирусных программ на нали-

чие кодовых последовательностей, характерных для программ расшифровывания.

## 1.6. Классификация компьютерных вирусов

Компьютерные вирусы можно классифицировать по следующим наиболее существенным признакам.

**1. По объекту внедрения компонента активизации вируса:**

- файловые вирусы, инфицирующие файлы с программами:
  - ⇒ вирусы, заражающие исполняемые файлы;
  - ⇒ вирусы, заражающие файлы с драйверами устройств;
  - ⇒ вирусы, заражающие командные файлы и файлы конфигурирования;
  - ⇒ вирусы, заражающие файлы, составляемые на макроязыках программирования, или файлы, которые могут включать выполняемые макросы;
  - ⇒ вирусы, заражающие файлы с различными библиотеками программ (библиотеками исходных, объектных, загрузочных и оверлейных модулей, библиотеками динамической компоновки);
- загрузочные (бутовые) вирусы, заражающие программы, хранящиеся в системных областях дисков:
  - ⇒ вирусы, заражающие системный загрузчик, расположенный в стартовом секторе дискет и логических дисков;
  - ⇒ вирусы, заражающие внесистемный загрузчик, расположенный в стартовом секторе жестких дисков.

**2. По месту размещения основного тела вируса:**

- вирусы, размещающие основное тело в одном элементе данных (файле или загрузчике) вместе с компонентом активизации вируса;

- вирусы, размещающие основное тело отдельно от элемента данных (файла или загрузчика), в котором хранится компонент активизации вируса.

**3. По режиму функционирования:**

- резидентные вирусы, которые после своей активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к требуемым им ресурсам;
- транзитные вирусы, которые выполняются только в момент запуска зараженной программы.

**4. По схеме заражения:**

- вирусы, дописывающие свое тело к концу исполняемого файла;
- вирусы, внедряющие свое тело внутрь исполняемого файла;
- вирусы, внедряющие свое тело в начало исполняемого файла;
- вирусы, вставляющие подпрограмму со своим телом и ее вызовы в различные библиотеки программ;
- вирусы, помещающие в командные файлы или файлы конфигурирования вызов программы, содержащей тело вируса;
- вирусы, замещающие системный или внесистемный загрузчик.

**5. По способам активизации функций вируса:**

- вирусы, активизирующие свои функции сразу же с момента получения управления;
- вирусы, активизирующие свои функции только при выполнении определенного условия.

**6. По характеру наносимого ущерба:**

- вирусы, наносящие ущерб низкой степени (например, выполняющие неназойливые визуальные эффекты);

- вирусы, наносящие ущерб средней степени (например, осуществляющие стирание выводимой на экран информации или подмену логического привода);
- вирусы, наносящие ущерб высокой степени (например, выполняющие уничтожение информации или значительно снижающие производительность ВС, функционирующей в режиме реального времени).

**7. По степени и способу маскировки:**

- вирусы, не использующие средств маскировки;
- stealth-вирусы, пытающиеся быть невидимыми на основе контроля доступа к зараженным элементам данных;
- вирусы-мутанты, содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса:
  - ⇒ обычные вирусы-мутанты, в разных копиях которых различаются только зашифрованные тела, а расшифровщики совпадают;
  - ⇒ полиморфные вирусы, в разных копиях которых различаются не только зашифрованные тела, но и расшифровщики.

# 2. УРОВНИ ЗАЩИТЫ ОТ КОМПЬЮТЕРНЫХ ВИРУСОВ

Подсистема защиты от компьютерных вирусов является одним из основных компонентов системы защиты информации и процесса ее обработки в вычислительных системах.

Для высокой эффективности подсистема антивирусной защиты должна иметь многоуровневую структуру. При этом можно выделить следующие уровни защиты от компьютерных вирусов:

**1)** уровень защиты от проникновения в ВС вирусов известных типов;

**2)** уровень углубленного анализа компьютерной системы на наличие вирусов как известных, так и неизвестных типов;

**3)** уровень защиты от деструктивных действий и размножения вирусов.

Каждый из данных уровней реализуется путем комплексного использования организационных и программно-аппаратных средств.

Первый уровень защиты обеспечивает препятствие доступу в ВС вирусов известных типов. Основой реализации данного уровня является поиск и обезвреживание вирусов в компьютерной системе, а также во всех программах, поступающих в компьютерную систему извне. Обнаружение и обезвреживание вирусов осуществляется на основе поиска кодовых последовательностей (сигнатур), характерных для вирусов известных типов.

Второй уровень защиты обеспечивает обнаружение в компьютерной системе вирусов, которым удалось обойти первый уровень защиты. Это в основном касается вирусов незнакомых типов, для которых неизвестны характерные им кодовые последовательности (сигнатуры). Поиск вирусов на данном уровне осуществляется путем сравнения текущих характеристик элементов компьютерной системы с эталонными характеристиками, соответствующими их незараженному состоянию.

Третий уровень защиты обеспечивает защиту от деструктивных действий и размножения вирусов, которым удалось преодолеть первые два уровня. Данный уровень реализуется на основе перехвата характерных для вирусов функций (низкоуровневое форматирование дисков, модификация программ и т.д.).

## 2.1. Защита от проникновения вирусов известных типов

### *2.1.1. Организация защиты*

Основной задачей первого уровня антивирусной защиты является предотвращение доступа в компьютерную систему вирусов, для которых известны характерные им кодовые последовательности (сигнатуры). Для выполнения этой задачи должны подвергаться тщательной проверке на наличие вирусных сигнатур следующие объекты:

- все поступающие в ВС извне носители информации и программные файлы;
- внутренняя память компьютера (постоянная и оперативная), которая должна проверяться после загрузки операционной системы;
- все носители информации (магнитные и оптические диски, магнитные ленты), предназначенные для применения в ВС, которые ранее не проверялись или после проверки использовались вне компьютерной системы.

В случае обнаружения зараженных программ эти программы должны быть либо восстановлены, либо полностью уничтожены при невозможности восстановления. Локализованные на данном уровне вирусы должны подвергаться обязательному уничтожению.

Следует учитывать, что в программах, упакованных в архивы, обнаружить вирусы без распаковки невозможно. При этом необходимо различать:

- ♦ архивы данных, не являющиеся самораспаковывающимися, например, архивы, имеющие расширения .ZIP, .RAR, .ARJ;
- ♦ самораспаковывающиеся архивы, созданные архиваторами данных и имеющие расширение .EXE, например, созданные архиваторами PKZIP, RAR или ARJ;
- ♦ исполняемые самораспаковывающиеся файлы, сжатые с помощью специальных упаковщиков программ, например, исполняемые файлы, упакованные с помощью таких программных утилит как PKLite, LZExe.

При выполнении вычислительной системой чрезвычайно важных функций полученное извне и обработанное на первом уровне защиты программное обеспечение целесообразно испытывать и первоначально использовать на специально выделенном компьютере в течении определенного промежутка времени, называемого карантином, например, в течении нескольких недель. Это поможет избежать заражения ВС неизвестным вирусом, которому удалось обойти первый уровень антивирусной защиты, так как следующий уровень (уровень углубленного анализа на наличие вирусов) не обеспечивает требуемую безопасность для новых программ по причине отсутствия для них эталонных характеристик, соответствующих их незараженному состоянию.

Перед установкой первого уровня защиты должны быть выполнены следующие действия:

**1)** тщательный анализ самой вычислительной системы на наличие вирусов;

**2)** полное обезвреживание обнаруженных вирусных программ.

В процессе анализа вычислительной системы необходимо проверить все ее компоненты, в которых могут размещаться программы: постоянное и оперативное запоминающие устройства, магнитные и оптические диски, а также кассеты с магнитными лентами.

### 2.1.2. Средства поиска и обезвреживания вирусов известных типов

Для поиска и обезвреживания вирусов перед установкой первого уровня антивирусной защиты, а также для непосредственной защиты от проникновения вирусов известных типов используют антивирусные программные средства, называемые сканерами. Их синонимы - детекторы-дезинфекторы, полидетекторы-полифаги. Программы-сканеры ориентированы на обнаружение фиксированного набора вирусов, количество которых повышается при переходе к более новым версиям этих антивирусных программ. Кроме того, сканеры позволяют восстанавливать зараженные файлы и загрузчики, а при невозможности восстановления файлов обеспечивают их уничтожение.

Существуют следующие виды программ-сканеров:

- транзитные, которые загружаются в оперативную память только для поиска и обезвреживания вирусов;
- резидентные, которые после запуска остаются в оперативной памяти резидентно и проверяют программные файлы при возникновении с ними определенных событий (запуск, копирование, создание, переименование).

Наибольшая результативность достигается при совместном использовании транзитного и резидентного сканеров, когда обеспечивается не только периодический поиск и обезвреживание вирусов на дисковом пространстве и в оперативной памяти, но и контроль на наличие вирусов в программах, к которым происходит обращение.

Должны быть предусмотрены следующие виды и периодичность использования транзитного сканера:

- первый запуск после установки сканера на компьютер для поиска и обезвреживания вирусов во всех возможных местах их внедре-

ния (в оперативной памяти, на жестких дисках, а также на всех имеющихся дискетах и оптических дисках);

- ежедневный запуск в процессе загрузки операционной системы для поиска и обезвреживания вирусов в оперативной памяти, а также во всех запускаемых в процессе загрузки программах;
- запуск несколько раз в неделю или еженедельно в заданное пользователем время для поиска и обезвреживания вирусов во всех возможных местах их внедрения (в оперативной памяти, а также на всех логических дисках);
- запуск по мере необходимости для поиска и обезвреживания вирусов в программах, а также на дискетах и оптических дисках, поступающих извне.

Для выполнения периодического запуска транзитного сканера может использоваться резидентная программа-планировщик.

Запуск резидентного сканера для его постоянного нахождения в оперативной памяти должен осуществляться в процессе загрузки операционной системы.

К недостаткам сканеров можно отнести то, что каждый из них позволяет обнаружить далеко не все известные вирусы и, как правило, отстает от появления вирусов новых типов.

Учитывая частоту появления новых вирусов и их короткий жизненный цикл, следует организовать такое использование программ-сканеров, при котором их версии будут обновляться не реже одного раза в месяц. В противном случае эффективность использования этих антивирусных программ существенно снижается.

## 2.2. Углубленный анализ на наличие вирусов

### *2.2.1. Установка и поддержание уровня углубленного анализа на наличие вирусов*

Уровень углубленного анализа компьютерной системы на наличие вирусов является вторым уровнем антивирусной защиты. Его основная задача - обнаружение вирусов, которым удалось обойти уровень защиты от проникновения известных вирусных программ. К незамеченным на первом уровне вирусам прежде всего можно отнести вирусы новых типов, для которых еще неизвестны характерные им сигнатуры. Поиск вирусов осуществляется путем сравнения текущих характеристик элементов компьютерной системы с эталонными характеристиками, соответствующими их незараженному состоянию.

Для реализации уровня углубленного анализа на наличие вирусов используют антивирусные программные средства, называемые ревизорами. При установке и поддержании данного уровня антивирусной защиты должны быть выдержаны следующие этапы.

1. Тщательный анализ вычислительной системы на наличие вирусов и полное обезвреживание обнаруженных вирусных программ с помощью обновленной версии транзитного сканера. Для большей эффективности процессов поиска и обезвреживания вирусов целесообразно независимое применение нескольких различных сканеров.
2. Формирование с помощью ревизора следующих эталонных характеристик незараженного компьютера:
   - ⇒ содержимого загрузочных секторов жестких дисков;
   - ⇒ контрольных сумм содержимого файлов конфигурирования и настройки, например, файлов AUTOEXEC.BAT, CONFIG.SYS,

*.INI для MS-DOS/Windows 3.11 (3.1), а также SYSTEM.DAT и USER.DAT для Windows 95;

⇒ контрольных сумм или описания структуры содержимого оперативной памяти компьютера;

⇒ информации о количестве и расположении сбойных кластеров жестких дисков (некоторые вирусы размещают свои тела в свободных кластерах, помечаемых затем этими вирусами как сбойные);

⇒ контрольных сумм содержимого файлов с программами, а также их системных характеристик: пути, даты и времени создания, длины, значений атрибутов, а при необходимости, и адресов физического расположения.

**3.** Периодическая проверка ревизором соответствия реальных характеристик элементов компьютерной системы их эталонным характеристикам, которые эти элементы имели при незараженном состоянии. В зависимости от возможностей ревизора могут использоваться следующие виды периодических проверок:

⇒ периодическая разовая (например, ежедневная или еженедельная), при которой после запуска ревизора проверяются все элементы компьютера, для которых созданы эталонные характеристики;

⇒ в режиме реального времени, при которой осуществляется проверка контролируемых элементов только при попытке их использования, например, при попытке запуска программ.

Процесс формирования с помощью ревизора эталонных характеристик незараженных элементов компьютера часто называют вакцинацией этих элементов. В качестве элементов компьютерной системы, для которых формируются эталонные характеристики, или, другими словами, в качестве вакцинируемых элементов должны выбираться элементы, куда

могут внедряться вирусы. При обновлении этих элементов, например, при изменении файлов конфигурирования и настройки, должны быть изменены и их эталонные характеристики (вакцины).

В случае обнаружения несоответствия реальных характеристик эталонным в начале необходимо выяснить причину этого несоответствия. Возможны три причины:

**1)** после обновления элементов, для которых формировались эталонные характеристики, не была обновлена эталонная информация;

**2)** повреждение контролируемых элементов данных по причине возникновения сбоев или отказов программно-аппаратных средств;

**3)** заражение компьютерным вирусом.

Если обновлений и повреждений не было, то произошло заражение компьютерным вирусом. В этом случае следует строго по порядку выполнить всю последовательность действий по обезвреживанию вируса и восстановлению работоспособности компьютерной системы (см. п. 2.4).

Следует отметить, что функции защиты, реализуемые на уровне углубленного анализа на наличие вирусов, обеспечивают обнаружение несанкционированных изменений в рабочей среде компьютера, вызванных действиями не только вирусов, но и злоумышленников, получивших несанкционированный доступ к компьютерным ресурсам. Кроме того, на данном уровне обеспечивается также обнаружение искажений в программах и ключевой информации, возникших в результате машинных сбоев или износа магнитного носителя.

Таким образом, функции, характерные для уровня углубленного анализа на наличие вирусов, обеспечивают своевременное обнаружение отклонений текущего состояния рабочей среды компьютера от эталонного и по этой причине должны быть реализованы не только в системе антивирусной защиты, но и в любой надежной системе защиты информации.

В качестве примера можно привести специализированная систему защиты информации «Кобра» [4, 5], обеспечивающую не только своевременное обнаружение отклонений текущего состояния рабочей среды компьютера от эталонного, но и автоматическое восстановление ее основных компонентов (содержимого CMOS-памяти, главной загрузочной записи винчестера, включая его таблицу разделов, загрузчика DOS, CONFIG.SYS, AUTOEXEC.BAT). Детальное описание возможностей данной системы по защите от компьютерных вирусов приведено в п. 3.1.4.

### *2.2.2. Особенности использования программ-ревизоров*

Как и сканеры, ревизоры можно разделить на следующие виды:

- транзитные, которые загружаются в оперативную память только для поиска и обезвреживания вирусов;
- резидентные, которые после запуска остаются в оперативной памяти резидентно и проверяют контролируемые элементы компьютера при возникновении с ними определенных событий (запуск и модификация программ, копирование, создание, переименование программных файлов);

Наибольшая результативность антивирусной защиты достигается при совместном использовании транзитного и резидентного ревизоров, когда осуществляется не только периодический разовый поиск неизвестных вирусов, но и динамический контроль на наличие неизвестных вирусов в программах, к которым происходит обращение.

Запуск транзитного ревизора, как правило, выполняется сразу после использования транзитного сканера. При этом для транзитного ревизора должны быть предусмотрены следующие виды и периодичность его использования:

- первый запуск для формирования эталонных характеристик элементов компьютера после тщательного поиска и обезвреживания вирусов в этих элементах транзитным сканером;
- ежедневный запуск в процессе загрузки операционной системы для поиска и обезвреживания вирусов в оперативной памяти, а также во всех запускаемых в процессе загрузки программах;
- запуск несколько раз в неделю или еженедельно в заданное пользователем время для поиска и обезвреживания вирусов во всех возможных местах их внедрения (в оперативной памяти, а также на всех логических дисках);
- по мере необходимости для формирования эталонных характеристик вновь поступивших программ после их тщательной проверки транзитным сканером.

Для выполнения периодического запуска может использоваться резидентная программа-планировщик.

В случае, если транзитные сканер и ревизор объединены вместе, то перед формированием или проверкой эталонных характеристик каждой программы ревизором автоматически осуществляется поиск и обезвреживание вирусов в этой программе сканером.

Запуск резидентного ревизора для его постоянного нахождения в оперативной памяти должен осуществляться в процессе загрузки операционной системы.

Недостатком ревизоров является легкая назойливость по отношению к пользователям, так как пользователями или администраторами не всегда вовремя обновляются эталонные данные. Но этот недостаток с лихвой компенсируется значительным повышением степени защищенности против вирусных программ новых типов, не обнаруживаемых сканерами.

## 2.3. Защита от деструктивных действий и размножения вирусов

Третий уровень антивирусной безопасности предназначен для защиты от деструктивных действий и размножения вирусов, которым удалось преодолеть первые два уровня. На данном уровне должно быть обеспечено блокирование всех действий вирусов, связанных с их саморазмножением и нанесением ущерба. Такое блокирование реализуется на основе перехвата выполнения функций, характерных для вирусов (модификация программ, низкоуровневое форматирование дисков и т.д.).

Уровень защиты от деструктивных действий и размножения вирусов реализуется путем использования встроенных аппаратных возможностей компьютера, а также специальных антивирусных программ, называемых фильтрами.

### *2.3.1. Использование средств аппаратного контроля*

К встроенным аппаратным возможностям по блокированию действий вирусов относится аппаратный контроль попытки модификации внесистемного загрузчика и таблицы разделов винчестера, находящихся в загрузочном секторе (MBR) каждого жесткого диска компьютера. Это позволяет блокировать действия вирусов, пытающихся заразить внесистемный загрузчик или исказить таблицу разделов винчестера. Включение и отключение функции аппаратного антивирусного контроля выполняется с помощью утилиты настроек параметров компьютера Setup, входящей в состав BIOS.

Запуск утилиты Setup выполняется нажатиями клавиши Del после активизации процесса загрузки операционной системы, т.е. после включения компьютера или нажатия кнопки Reset. После запуска утилиты необходимо войти в пункт меню **BIOS Features Setup** (**Advanced CMOS Setup**) и с помощью клавиш <PgUp> и <PgDn> установить переключа-

тель **Virus Warning** в положение **Enabled** для активизации функции антивирусного контроля или в положение **Disabled** для ее отключения. Далее следует сохранить сделанные изменения и выйти из утилиты с помощью пункта меню **Save & Exit Setup**.

Если функция аппаратного антивирусного контроля является активной, то при любой попытке изменения внесистемного загрузчика или таблицы разделов жесткого диска будет выдано предупреждающее сообщение и запрос пользователю, ответом на который пользователь может запретить или разрешить модификацию загрузочного сектора.

Перед модификацией загрузочного сектора винчестера пользователем, например, перед разбиением жесткого диска на разделы или инсталляцией операционной системы, функцию аппаратного антивирусного контроля целесообразно отключать, а после выполнения соответствующих действий активизировать снова.

### *2.3.2. Использование средств программного контроля*

В сравнении со встроенными аппаратными антивирусными возможностями компьютера применение программ-фильтров позволяет значительно расширить количество блокируемых функций вирусов для защиты от их деструктивных действий и размножения.

Фильтры являются резидентными программами и после своего запуска постоянно находятся в оперативной памяти компьютера, перехватывая все попытки выполнения контролируемых ими действий. Перехват попыток выполнения контролируемых действий реализуется фильтром за счет перехвата соответствующих прерываний процессора. К действиям, которые могут контролировать большинство фильтров, относятся следующие:

- низкоуровневое форматирование жесткого диска;
- модификация загрузочных секторов винчестера;

- ♦ модификация загрузочных секторов гибких дисков;
- ♦ изменение файлового атрибута «только чтение»;
- ♦ модификация программных файлов;
- ♦ оставление в оперативной памяти резидентной программы.

В параметрах настройки фильтров для каждого контролируемого действия, как правило, можно задать следующие способы реакции на перехват попытки его выполнения:

- ♦ полное блокирование этого действия с выдачей сообщения пользователю;
- ♦ выдача пользователю запроса, в ответе на который пользователь может разрешить или запретить выполнение действия, попытка реализации которого перехвачена фильтром.

Следует учесть, что не каждый перехват фильтром попытки выполнения контролируемого действия является признаком действия вируса. Например, запись в загрузочный сектор дискеты осуществляется и при форматировании этой дискеты, а резидентная программа может быть запущена и самим пользователем. Кроме того, многие программы хранят в своем исполняемом файле отдельные настроечные параметры, которые могут ими же изменяться после запуска. Поэтому, включение в параметрах настройки фильтра режима контроля всех возможных для него действий может привести к назойливости по отношению к пользователю. В качестве действий, режим контроля которых должен быть включен всегда, должны выступать такие, как низкоуровневое форматирование жесткого диска, а также модификация загрузочных секторов винчестера и гибких дисков.

Если модификация главной загрузочной записи винчестера (внесистемного загрузчика и таблицы разделов) контролируется на аппаратном уровне, то для снижения ресурсных затрат режим контроля этого же действия фильтром следует отключить. Можно поступить наоборот - оставить

режим контроля модификации главной загрузочной записи винчестера за фильтром, но отключить аппаратный контроль этого действия.

## 2.4. Восстановление работоспособности вычислительной системы после заражения компьютерным вирусом

### *2.4.1. Резервирование информации и подготовка средств восстановления*

Для быстрого восстановления работоспособности каждого компьютера после заражения вирусом, а также устранения всех последствий необходимо заблаговременно выполнить следующие действия:

1) зарезервировать системную информацию о параметрах настройки и функционирования компьютерной системы;
2) зарезервировать информационные файлы (файлы документов, баз данных и т.д.), хранящиеся на винчестере;
3) подготовить набор средств восстановления;
4) зарезервировать эталонную информацию о незараженном состоянии элементов компьютерной системы, сделанную ревизором.

Кроме того, должны быть всегда готовы дистрибутивные носители с инсталляционными вариантами используемых на компьютере операционной системы и программных средств.

Резервирование и подготовка средств восстановления выполняется на дискеты.

К системной информации о параметрах настройки и функционирования компьютерной системы относятся следующие элементы данных:

- параметры настройки компьютера, хранящиеся в его энергонезависимой памяти (CMOS-памяти);
- внесистемный загрузчик и таблица разделов винчестера, хранящиеся в его загрузочном секторе (MBR);

- вторичные загрузочные записи винчестера (SMBR), содержащие характеристики логических дисков в его расширенном разделе;
- файлы конфигурирования и настройки, используемые операционной системой и программными средствами:
  - ⇒для MS-DOS - AUTOEXEC.BAT, CONFIG.SYS, а также файлы настройки программных средств, находящиеся в каталогах расположения этих программ и имеющие, как правило, расширение .INI;
  - ⇒для Win3.XX - дополнительно все файлы каталога Windows, имеющие расширение .INI;
  - ⇒для Win95 - дополнительно файлы системного реестра SYSTEM.DAT и USER.DAT, находящиеся в каталоге Windows.

Резервирование системной информации о параметрах настройки и функционирования компьютерной системы выполняется с помощью специализированных утилит, например, утилиты Нортона Rescue. Эта же утилита обеспечивает восстановление системной информации в случае ее потери при наличии заблаговременно сделанного резерва. Для операционных сред MS-DOS/Win3.XX необходимо использование утилиты Rescue из седьмой или восьмой версии утилит Нортона. Для Windows 95 требуется утилита Rescue из девятой версии этого набора утилит, специально предназначенного для операционной системы Windows 95.

Обновлять резерв системной информации следует после каждого изменения параметров настройки и функционирования компьютера (переразбиения винчестера и переинсталляции операционной системы, изменения параметров ее настройки, инсталляции новых программ).

Резервирование информационных файлов на дискеты может выполняться как их обычным копированием, так и архивированием. Архивирование позволяет значительно сократить количество дискет резерва и выполняется путем применения специализированных программных

средств, осуществляющих сжатие резервируемой информации. К таким средствам относятся архиваторы, например, RAR, ARJ, WINZIP и др. Обновлять архивы с файлами данных следует после создания новых информационных фалов и модификации существующих по окончании сеанса работы пользователя.

Набор средств восстановления должен включать следующие компоненты:

- системную дискету с простой командной оболочкой, облегчающей управление компьютером, например, с оболочкой Norton Commander минимальной конфигурации (минимальную конфигурацию обеспечивают третья и четвертая версии этой оболочки);
- дискеты с набором средств восстановления, куда должны входить следующие утилиты:
  - ⇒ антивирусные средства для локализации и обезвреживания вирусов (сканер, ревизор и фильтр);
  - ⇒ утилита для восстановления зарезервированной системной информации (утилита Нортона Rescue);
  - ⇒ утилиты для подготовки дисков к работе (утилиты Fdisk, Format, Sys);
  - ⇒ утилиты для устранения логических дефектов дисковых носителей информации (утилита ScanDisk из состава MS-DOS (Windows 95) или утилиты Нортона NDD, DiskTool);
  - ⇒ архиваторы, которыми осуществлялось резервирование информационных файлов.

Версии всех программ, входящих в набор средств восстановления должны соответствовать операционной системе на системной дискете.

Каждая дискета набора средств восстановления должна быть защищена от записи (в пятидюймовых дискетах прорезь для защиты от записи должна быть заклеена специальной пленкой, а в трехдюймовых -

окошко защиты от записи должно быть открытым). Кроме того, на каждую дискету средств восстановления должен быть скопирован файл COMMAND.COM, что предотвратит необходимость вставлять системную дискету в дисковод каждый раз при запуске на выполнение какой-либо программы.

Резервирование эталонной информации о незараженном состоянии элементов компьютерной системы выполняется ее обычным копированием или архивированием.

### *2.4.2. Восстановление компьютерной системы*

Факт заражения компьютера вирусом может быть установлен после получения соответствующих сообщений на любом уровне антивирусной защиты. При получении сообщения от ревизора или фильтра следует иметь в виду, что причиной этого сообщения могут быть:

- для ревизора:
  - ⇒ искажение информации на винчестере после возникновения сбоя или отказа какого-либо программно-аппаратного средства;
  - ⇒ несвоевременное обновление пользователем эталонных данных, например, после обновления на винчестере версии программной системы;
- для фильтра - попытка выполнения контролируемого действия программой, запущенной пользователем, например, попытка записи в загрузочный сектор дискеты при ее форматировании.

При определении на любом уровне антивирусной защиты факта заражения вирусом обезвреживание компьютерного вируса в зараженной программе может быть выполнено автоматически после выдачи соответствующего запроса пользователю.

Если для защиты от вирусов используются резидентные сканер и ревизор, то после получения пользователем от любого из этих антивирусных средств сообщения об обнаружении вируса следует выдать команду на обезвреживание вируса в обнаруженной зараженной программе и далее выполнить следующие действия:

**1)** запустить транзитный сканер для поиска и обезвреживания известных вирусов:
   - ⇒ в оперативной памяти;
   - ⇒ на всех логических дисках;
   - ⇒ на всех дискетах, используемых в текущем и предыдущем сеансах работы;

**2)** запустить транзитный ревизор для поиска и обезвреживания неизвестных вирусов в оперативной памяти и на всех логических дисках;

**3)** расширить на ближайший период количество действий, контролируемых фильтром.

Если для антивирусного средства заданы соответствующие настройки, то обнаруженные в процессе поиска вирусов зараженные загрузчики и программные файлы восстанавливаются. В случае невозможности восстановления каких-либо программных файлов антивирусная программа в зависимости от настроек осуществляет их переименование или уничтожение.

При отсутствии в антивирусной защите резидентных сканера и ревизора или при полном отсутствии антивирусной защиты факт заражения может быть установлен соответственно по сообщению транзитного антивирусного средства или на основе одного из следующих признаков:

- ♦ невозможность загрузки операционной системы с винчестера;
- ♦ значительное замедление работы компьютера;

- ♦ невозможность доступа к какому-либо логическому диску или дискете - появляется сообщение об ошибке;
- ♦ невозможность запустить исполняемый файл - появляется сообщение об ошибке;
- ♦ исчезновение информационных файлов;
- ♦ искажения в информационных файлах;
- ♦ невозможность открытия информационных файлов - появляется сообщение об ошибке;
- ♦ при просмотре корневого каталога диска отображаются непонятные последовательности символов;
- ♦ на экране появляются визуальные и звуковые эффекты, которых раньше не было («падающие» буквы, «переворачивание экрана» и т.д.).

В случае обнаружения одного или нескольких перечисленных признаков вначале следует проанализировать сложившуюся ситуацию, так как причиной могут быть не только действия вирусов. Например, искажение информации может произойти и по причине некорректной работы какой-либо программы, а исчезновение информационных файлов - в результате их случайного удаления пользователем.

После установки факта заражения вирусом по сообщению транзитного антивирусного средства или на основе каких-либо из перечисленных признаков необходимо приступить к восстановлению компьютерной системы. Наиболее эффективной будет следующая последовательность восстановления.

1. Для перезагрузки компьютера с системной дискеты из состава средств восстановления отключить и спустя 20-30 секунд включить питание компьютера. Следует учесть, что текущие параметры из CMOS-памяти могут определять начальную загрузку с диска C:. Поэтому сразу же после включения питания компьютера нажатиями клавиши Del необ-

ходимо запустить утилиту BIOS Setup с целью установки порядка загрузки операционной системы «A, C».

Примечание. При неполной перезагрузке, реализуемой посредством одновременного нажатия комбинаций клавиш <Ctrl>+<Alt>+<Del> или путем выполнения команды **Пуск/ Завершение работы/ Перезагрузить компьютер** для Windows 95, резидентный вирус может сохранить свое тело в оперативной памяти. Более того, существуют резидентные вирусы, которые, если им помогают конструктивные особенности компьютера, могут сохранять свое тело в оперативной памяти даже после полной перезагрузки, выполняемой путем нажатия кнопки Reset.

2. Запустив утилиту Setup войти в пункт меню **BIOS Features Setup** (**Advanced CMOS Setup**) и с помощью клавиш <PgUp> и <PgDn> установить переключатель **Boot Sequence** (**System Boot Up Sequence**) в положение «A, C».

3. Если системная дискета из состава средств восстановления отсутствует в дисководе A:, то вставить ее в этот дисковод. Далее следует с помощью пункта меню **Save & Exit Setup** выйти из утилиты Setup с сохранением сделанных изменений.

4. Дождаться окончания загрузки операционной системы и, если загрузка выполнялась не с дискеты из набора восстановления, на которой размещены утилита Нортона Rescue и резерв системной информации (данная дискета является загрузочной), то вставить эту дискету в накопитель.

5. Восстановить системную информацию с помощью утилиты Rescue.

6. Для того, чтобы восстановленные параметры настройки компьютера (параметры из CMOS-памяти, MBR винчестера) вошли в силу, следует перезагрузить компьютер с системной дискеты из набора восстановления, нажав кнопку Reset. При этом необходимо учитывать, что исход-

ные параметры из CMOS-памяти могут определять начальную загрузку с диска C:. Поэтому сразу же после отпускания кнопки Reset нажатиями клавиши Del требуется запустить утилиту BIOS Setup и по аналогии с пунктами 2 и 3 данного алгоритма установить порядок загрузки операционной системы «A, C». Дождаться окончания загрузки операционной системы с дискеты.

7. Запустить из набора восстановления утилиту для поиска и устранения логических дефектов на всех логических дисках, а также дискетах, которые использовались на зараженном компьютере. В качестве такой утилиты могла быть зарезервирована утилита ScanDisk из состава MS-DOS (Windows 95) или утилита Нортона NDD.

8. Вставить в накопитель дискету из набора восстановления с антивирусными средствами.

9. Запустить сканер для поиска и обезвреживания вирусов на всех логических дисках, а также дискетах, которые использовались на зараженном компьютере.

10. Восстановить из резерва эталонную информацию о незараженном состоянии элементов компьютерной системы и запустить ревизор для проверки компьютерной системы на наличие неизвестных вирусов. При обнаружении неизвестного вируса зараженные файлы, которые не подлежат восстановлению, следует с помощью антивирусных средств (ревизора или сканера) удалить. В случае обнаружения неизвестного вируса требуется также удаление всех программ на дискетах, которые были использованы на зараженном компьютере, так как эти программы могут быть инфицированы. На предыдущем этапе факт заражения этих программ неизвестным вирусом сканер обнаружить не смог, так как ориентирован на поиск вирусов только по известным сигнатурам.

11. Для загрузки операционной системы с винчестера извлечь дискету из накопителя A: и перезагрузить компьютер, нажав кнопку Reset.

Если операционная система не загружается, то проанализировав сообщения об ошибках следует попытаться их устранить. Основными причинами могут быть следующие:

- ⇒ на винчестере искажены или отсутствуют компоненты операционной системы;
- ⇒ на винчестере искажены или отсутствуют программные файлы, вызываемые из файлов конфигурирования и настройки в процессе загрузки операционной системы;
- ⇒ по причине изменения файловой структуры текущее расположение программных файлов, вызываемых из файлов конфигурирования и настройки, изменено.

Понятно, что для устранения любой из первых двух причин необходима переинсталляция с дистрибутивных носителей (дискет или компакт-диска) соответствующей программной системы (операционной или прикладной). Для устранения последней причины следует изменить ссылки на вызываемые программные файлы или изменить само расположение этих файлов.

12. При необходимости восстановить из резерва искаженные и уничтоженные файлы данных.

13. Для усиления антивирусной защиты установить с помощью утилиты BIOS Setup порядок загрузки операционной системы «C, A». В этом случае исключена возможность заражения компьютера при случайной загрузке с дискеты, инфицированной загрузочным вирусом.

Если системная информация заблаговременно зарезервирована не была, то пункты 4 - 6 приведенного обобщенного алгоритма восстановления следует пропустить. В этом случае процесс восстановления может быть значительно затруднен. Например, в случае разрушения вирусом

таблицы разделов жесткого диска возможны только два варианта восстановления его работоспособности:

1) восстановление таблицы разделов с помощью низкоуровневого редактора, например, утилиты Нортона DiskEdit;
2) подготовка жесткого диска к работе с «нуля» с помощью утилит Fdisk и Format.

Использование первого способа требует детального знания низкоуровневой структуры жесткого диска и больших временных затрат. При использовании второго способа информация на жестком диске будет безвозвратно потеряна.

По окончании восстановления работоспособности вычислительной системы и устранения всех последствий деструктивных действий вирусов необходимо на основе тщательного анализа установить источник и причину заражения, что поможет избежать повторного заражения компьютерными вирусами. Источником может служить, например, зараженная игровая программа, полученная у знакомого. Наиболее распространенной причиной заражения вирусами является недостаточная антивирусная защита.

Из вышесказанного становится понятным, что только комплексное использование всех уровней антивирусной защиты, а также правильные резервирование информации и подготовка средств восстановления обеспечивают своевременное обезвреживание компьютерных вирусов и эффективное восстановление работоспособности вычислительной системы.

# 3. ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ МНОГОУРОВНЕВОЙ АНТИВИРУСНОЙ ЗАЩИТЫ

## 3.1. Антивирусная защита в операционных средах MS-DOS и Windows 3.11

Особенностью организации защиты от компьютерных вирусов в операционных средах MS-DOS и Windows 3.11 (3.1) является отсутствие отдельных локализованных или отечественных полнофункциональных антивирусных пакетов, объединяющих в себе все функции по установке каждого из уровней антивирусной защиты:

**1)** уровня защиты от проникновения вирусов известных типов, требующего наличие как транзитного, так и резидентного сканера;

**2)** уровня углубленного анализа компьютерной системы на наличие вирусов, требующего наличие как транзитного, так и резидентного ревизора;

**3)** уровня защиты от деструктивных действий и размножения вирусов, требующего наличие фильтра.

Рассмотрим наиболее популярные антивирусные средства для сред MS-DOS и Windows 3.1 (3.11) по следующим направлениям:

- транзитный поиск и обезвреживание известных вирусов, где будет описан один из наиболее популярных транзитных сканеров;
- транзитный углубленный анализ на наличие вирусов, где будет описан один из наиболее популярных транзитных ревизоров;
- резидентная защита от компьютерных вирусов, где основное внимание будет уделено установке защиты с помощью резидентных средств: фильтра, а также резидентных сканера и ревизора.

### 3.1.1. Транзитный поиск и обезвреживание известных вирусов

Среди транзитных сканеров для операционных сред MS-DOS и Windows 3.xx наибольшей популярностью в нашей стране пользуются такие антивирусные программы как Aidstest Дмитрия Лозинского и DrWeb Игоря Данилова. Эти программы просты в использовании и для детального ознакомления с руководством по каждой из них следует прочитать файл с расширением .ME (AIDSREAD.ME или DRWEB.ME) поставляемый вместе с антивирусным средством.

Рассмотрим особенности использования программы-сканера DrWeb (Doctor Web) третьей версии.

Данный сканер является транзитной антивирусной программой, обеспечивающей обнаружение и обезвреживание известных ему вирусов в оперативной памяти и на дисках компьютера. Doctor Web также обладает возможностью эвристического анализа, на основе которого могут быть обнаружены новые и неизвестные вирусы. Во время такого анализа выполнимый код проверяется на наличие характерных для вирусов последовательностей команд.

Программа Doctor Web может работать как в диалоговом, так и в пакетном режимах. Пакетный режим удобен, если сканер вызывается из командного файла, например, AUTOEXEC.BAT. В этом случае в командный файл достаточно включить вызов DrWeb с указанием соответствующих параметров.

#### Диалоговый режим сканера DrWeb

Чтобы запустить программу Doctor Web в диалоговом режиме достаточно запустить на выполнение файл DrWeb.exe, находящийся в каталоге, куда был инсталлирован Doctor Web.

После запуска появляется главное окно сканера (□), активизация основного меню которого выполняется нажатием клавиши <F10>. Для вызова справки необходимо нажать клавишу <F1>. Выход из основного окна DrWeb и завершение сеанса работы со сканером выполняется по команде **Dr.Web/Выход** или путем нажатия комбинации клавиш <Alt>+<X>.

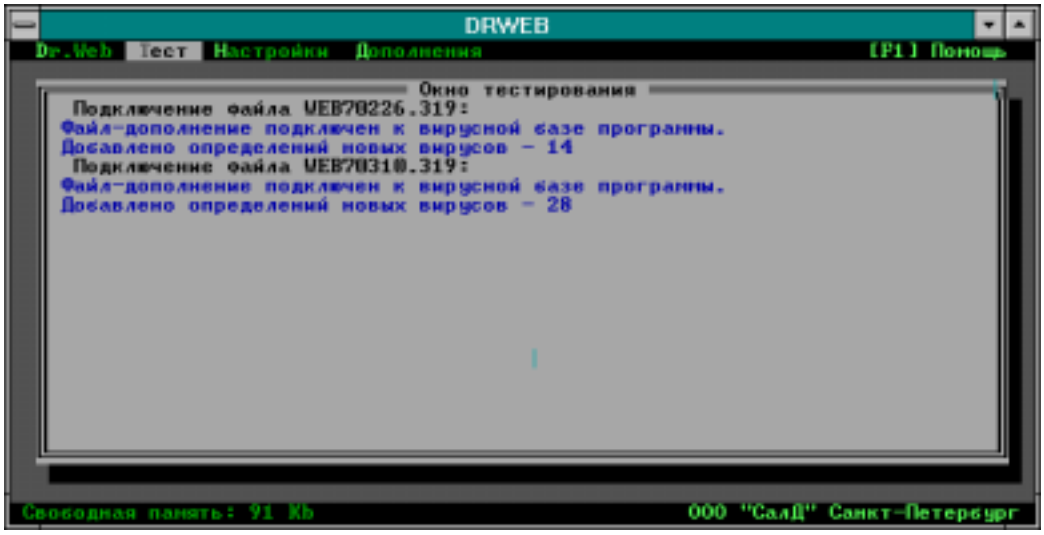


**Рис. 3.1. Главное окно программы DrWeb**

Перед поиском и обезвреживанием вирусов целесообразно настроить параметры работы сканера по команде **Настройки/ Параметры**. В результате появится диалоговое окно (□), детальное описание всех управляющих элементов которого можно получить, нажав клавишу <F1>.

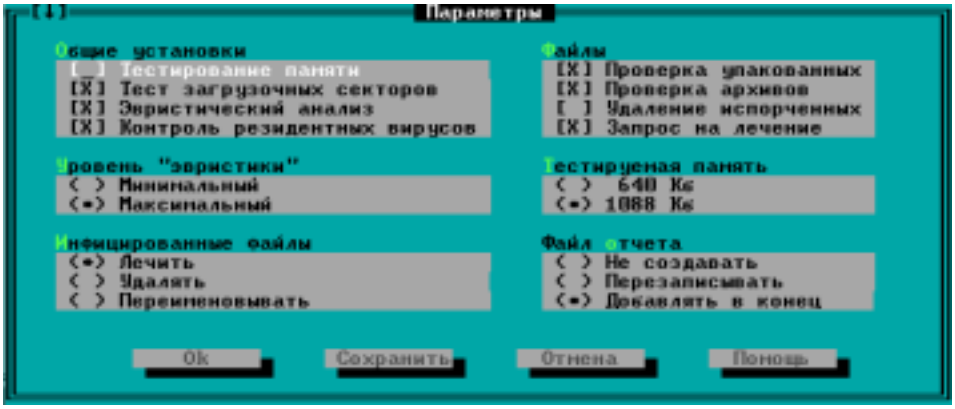


**Рис. 3.2. Диалоговое окно «Параметры»**

Флажки, расположенные в группе **Общие установки**, указывают, какие объекты будут проверяться на заражение вирусами. Для повышения надежности проверки компьютера следует установить все эти флажки.

Если установлен флажок **Тестирование памяти**, то при запуске программы Doctor Web она выполняет сканирование оперативной памяти компьютера в поиске активных вирусов. Переключатель **Тестируемая память** позволяет задать объем проверяемой памяти. Если этот переключатель установлен в положении **640 Кб**, программа проверяет только первые 640 Кбайт стандартной памяти компьютера. Если же переключатель находится в положении **1088 Кб**, проверяется вся стандартная оперативная память MS-DOS, доступная при работе процессора в реальном режиме.

Если в компьютере установлена расширенная память и она используется для загрузки резидентных программ и модулей операционной системы, рекомендуется установить переключатель **Тестируемая память** в положение **1088 Кб**.

Флажок **Тестирование загрузочных секторов** указывает программе Doctor Web выполнять проверку главной загрузочной записи (MBR) и загрузочного сектора (BR) дисков компьютера. При отключении этого переключателя сканер не сможет обнаружить загрузочные вирусы, поразившие дискеты и жесткие диски компьютера.

Одной из наиболее интересных возможностей, предоставляемых программой Doctor Web является эвристический анализ файлов и загрузочных секторов диска. Эвристический анализ позволяет обнаружить новые и неизвестные ранее вирусы. Во время такого анализа сканер проверяет исполняемый код и пытается определить, выполняет ли этот код действия, характерные для вирусов. Если будут найдены подозрительные программы, выводится предупреждение о том, что

объект, возможно, инфицирован неизвестным вирусом. В сообщениях Doctor Web приняты следующие обозначения:

- COM.Virus - вирус, заражающий COM-файлы;
- EXE.Virus - вирус, заражающий EXE-файлы;
- TSR.Virus - резидентный вирус;
- MACRO.Virus - вирус, заражающий документы Word for Windows;
- Boot.Virus - вирус, заражающий загрузочные сектора дисков;
- CRYPT.Virus - зашифрованный или полиморфный вирус.

Для управления уровнем или глубиной эвристического анализа предназначен переключатель **Уровень "эвристики"**. Возможны два уровня - **Минимальный** и **Максимальный**. Экспериментальные испытания на коллекции вирусов, состоящих из 10000 различных экземпляров, показали следующие результаты при обнаружении новых вирусов:

- **минимальный** уровень эвристического анализа обеспечивает обнаружение примерно 87% новых вирусов;
- **максимальный** - 89-91%.

Использование эвристического анализатора увеличивает время проверки компьютера. В режиме с максимальным уровнем эвристического анализа Doctor Web дополнительно проверяет файлы на подозрительное время их создания. Некоторые вирусы при заражении файлов устанавливают время создания файлов на несуществующие значения, используя их как признак или идентификатор зараженности. Например, вирусы могут увеличить дату создания файла на 100 лет или установить в поле секунд времени создания файла несуществующее значение - 62 секунды. Если Doctor Web обнаружит такие файлы, он отображает в окне тестирования соответствующее предупреждение:

*D:\DOD.COM странное время создания 2031 ??? 31 25:60:00*

В режиме эвристического анализа возможны ложные срабатывания, т.е. появление сообщений о возможном заражении, которые

еще не являются признаками реального заражения вирусами. К программным файлам, для которых получены такие сообщения следует отнестись с осторожностью, запуская их на выполнение только при активном состоянии антивирусного фильтра. Использование эвристического анализатора увеличивает время проверки компьютера. Особенно высок процент ложных срабатываний при максимальном уровне эвристического анализа. Обычно ложные срабатывания эвристического анализатора происходят при проверке файлов программ, использующих открытие файлов и запись в них, особенно если данные программы являются резидентными.

Многие резидентные вирусы заражают программы в момент, когда они открываются для чтения или записи. Это позволяет обнаружить активный вирус, так как после открытия файла его размер увеличивается (в него внедряется вирус). Флажок **Контроль резидентных вирусов** в окне «Параметры» позволяет контролировать изменение размера проверяемых файлов во время выполнения операций поиска файла и его открытия. Контроль за изменением размера файлов также позволяет обнаружить активные Stelth-вирусы, которые стремятся скрыть факт заражения ими программ. После активизации Stelth-вируса он остается резидентным в памяти и контролирует операции определения размера зараженного файла, уменьшая фактический размер зараженной программы.

Doctor Web позволяет задать различные способы удаления вирусов. Для этого в окне «Параметры» предназначен переключатель **Инфицированные файлы**. Чтобы восстановить инфицированные файлы, удалив из них код вируса, следует перевести этот переключатель в положение **Лечить**. Зараженные файлы можно также полностью удалить с диска компьютера или переименовать, установив соответственно переключатель в положение **Удалять** или **Переименовывать**. Если задан

режим **Переименовывать**, то первый символ в расширении зараженных файлов заменяется на символ 'V'. Например, инфицированный файл FIND.EXE будет переименован в FIND.VXE. Перед переименованием файла Doctor Web будет запрашивать подтверждение у пользователя.

Программа Doctor Web позволяет контролировать файлы, упакованные программами DIET, LZEXE, PKLITE, EXEPACK, PROTECT, COMPACK и CryptCOM, а также вакцинированные антивирусом CPAV. Такие файлы временно раскрываются и только затем проверяются на заражение вирусами. С помощью команды **Настройки/ Файлы** можно задать логическое имя диска компьютера, на котором будут создаваться временные файлы. Для задания режима проверки упакованных файлов, в окне «Параметры» следует установить переключатель **Проверка упакованных**.

Для сохранения свободного места на жестких и гибких дисках многие пользователи применяют программы-архиваторы. Если вирус заразил программу и затем она была записана в архив, то многие антивирусные программы, например AIDSTEST, не смогут его обнаружить. Doctor Web позволяет проверить файлы, расположенные в архивах. Для этого в окне «Параметры» следует установить флажок **Проверка архивов**. Обеспечивается проверка архивов, созданных архиваторами ARJ, PKZIP, LHA, RAR, ZOO, ICE и HA.

В некоторых случаях программные файлы, зараженные и разрушенные вирусами, не могут быть полностью восстановлены. Для задания режима полного удаления таких файлов следует установить флажок **Удаление испорченных**.

Перед лечением файлов Doctor Web может запрашивать у пользователя подтверждение на удаление обнаруженных вирусов. Для этого следует установить флажок **Запрос на лечение**. В противном

случае обезвреживание вирусов происходит автоматически и дополнительные вопросы пользователю не задаются.

Если после настройки всех параметров установленные режимы работы программы Doctor Web требуется сохранить и для последующих вызовов сканера, необходимо в диалоговом окне «Параметры» перед вводом команды **Ok** ввести команду **Сохранить**. Параметры настройки сохраняются в файле DrWeb.INI в каталоге программы Dr Web.

Поиск вирусов активизируется по команде **Тест/ Тестирование** или нажатием клавиши F5. При этом на экране появится диалоговое окно "Путь для тестирования", в котором следует указать расположение файлов, которые необходимо проверить на наличие вирусов. Можно указать не только имя диска и путь каталога, но и полные имена файлов, а также шаблоны. Для проверки всех дисков указывается символ «*». Если необходимо проверить файлы, расположенные в нескольких каталогах или на нескольких дисках, следует ввести соответственно несколько путей каталогов или несколько имен приводов, разделенных символами пробела.

Обезвреживание обнаруженных вирусов активизируется по команде **Тест/ Лечение** или нажатием комбинации клавиш <Ctrl>+<F5> . При обезвреживании вирусов Doctor Web отображает в окне тестирования список восстановленных файлов. Для прерывания процесса поиска или обезвреживания вирусов необходимо нажать клавишу <Esc>.

Просмотреть сводные результаты поиска и обезвреживания вирусов по завершении этого процесса можно по команде **Тест/Статистика**.

Имеется возможность записи протокола поиска и обезвреживания вирусов в файл отчета. Для этого необходимо в диалоговом окне «Параметры» (см. □), вызываемом по команде **Настройки/ Параметры**, установить в соответствующее положение переключатель **Файл отчета**. Впоследствии появится возможность просмотра файла отчета по команде **Тест/ Файл отчета**. Имя файла отчета определяется в диалоговом окне

"Файлы", вызываемом по команде **Настройки/ Файлы**. По умолчанию используется файл отчета REPORT.WEB в каталоге программы Dr Web.

## Пакетный режим сканера DrWeb

Для запуска сканера DrWeb из файла AUTOEXEC.BAT, а также из других командных файлов удобно использовать его пакетный режим работы. В этом случае параметры поиска и обезвреживания вирусов могут быть указаны непосредственно в командной строке вызова сканера. Отсутствующие в командной строке параметры работы извлекаются из файла настроек DrWeb.INI, расположенном в каталоге программы DrWeb. Обязательным для установки пакетного режима является параметр /CL, при котором сканер Doctor Web диалоговую оболочку не использует.

Командная строка для вызова сканера DrWeb, путь к которому указан в команде PATH файла AUTOEXEC.BAT, имеет следующий формат:

DRWEB.EXE [<диск>:[<путь>]] [<ключ>]... [<ключ>]

Здесь и далее квадратные скобки означают необязательную часть формата, которая может задаваться или нет в зависимости от конкретных требований. Сами символы квадратных скобок задавать не нужно.

Первый параметр <диск> должен содержать имя логического привода проверяемого диска. Например, в качестве параметра <диск> можно указать F: или A:. Если необходимо проверить все логические устройства жесткого диска компьютера, то в качестве параметра <диск> следует указать символ '*'. Чтобы проверить текущий каталог, можно указать в качестве параметра <диск> символ точки '.'.

Можно осуществить проверку файлов, расположенных в отдельных каталогах. Для этого в строке вызова программы Doctor Web следует добавить параметр <путь>. Этот параметр должен содержать путь к каталогу, который будет проверяться, или шаблон (маску) для имен и расширений проверяемых файлов.

Режимы работы сканера задаются параметрами <ключ>. Каждый ключ должен начинаться с символа '/' и может задаваться как маленькими, так и заглавными буквами. Ниже описаны наиболее полезные ключи запуска.

/AL - проверка всех файлов на заданном устройстве (а не только с расширениями COM, EXE, SYS, BAT, DRV, BIN, DLL, BOO, OV?, DOC и DOT).

/AR - проверка файлов, находящихся внутри архивов. Обеспечивается проверка архивов, созданных программами-архиваторами ARJ, PKZIP, LHA, RAR, ZOO, ICE и HA.

/CL - запуск программы в пакетном режиме. Диалоговая оболочка не используется.

/CU[D][R][P] - обезвреживание вирусов в файлах и системных областях дисков, удаление найденных вирусов. Могут быть указаны дополнительные параметры D, R и P.

Если указан параметр D, тогда инфицированные файлы не восстанавливаются, а просто удаляются с диска компьютера. Вместо удаления инфицированных файлов их можно переименовать. Для этого следует указать параметр R. В этом случае первый символ в расширении имени файла заменяется на символ 'V', что предотвратит случайный запуск таких файлов. Если указан дополнительный параметр P, тогда перед удалением вирусов запрашивается подтверждение у пользователя.

/DA - ежедневная проверка - тестирование дисков и(или) памяти один раз в сутки. Для данного режима необходимо наличие INI-файла - файла конфигурации DRWEB.INI, в который заносится дата последней проверки. Данный режим рекомендуется для запуска программы из пакетного файла AUTOEXEC.BAT.

/DL - удаление файлов, восстановление которых невозможно.

/FN - загрузка русских символов в знакогенератор видеоадаптера.

/GO - автоматическая проверка компьютера. Программа не ожидает подтверждения пользователя для выполнения различных операций (нехватка места на диске при распаковке, неверные параметры в командной строке, заражение программы Dr. Web неизвестным вирусом, ...). Данный режим актуален для проверки файлов в автоматическом режиме (например, при круглосуточной проверке электронной почты на станциях BBS).

/HA[<уровень>] - эвристический анализ файлов и поиск в них неизвестных вирусов. Можно выбрать уровень (глубину) эвристического анализа при помощи параметра <уровень>. Существует два возможных уровня: 0 - минимальный, 1 - максимальный. По умолчанию устанавливается минимальный уровень эвристического анализа. Следует помнить, что при максимальном уровне увеличивается количество сообщений о возможном заражении, которые еще не являются признаком реального заражения вирусами.

/HI - поиск вирусов в адресном пространстве оперативной памяти от 0 Кбайт до 1088 Кбайт.

/MT<время> - в последнее время появились сложнополиморфные вирусы, расшифровка которых занимает большое количество времени. Можно самостоятельно установить максимальное время проверки файлов с помощью параметра <время>. Время проверки указывается в секундах. Для 486 процессора или процессора Pentium целесообразно установить 30-60 секунд.

/NB - отключение проверки загрузочных секторов дисков.

/ND - тестирование файлов только в корневом или текущем каталоге без рекурсивного обхода вложенных подкаталогов.

/NI - игнорирование параметров, записанных в конфигурационном файле .INI

/NM - работа без поиска вирусов в памяти компьютера.

/NR - отмена создания файла отчета.

/NS - запретить возможность прерывания проверки компьютера. После указания параметра /NS пользователь не сможет прервать работу программы по нажатию клавиши <Esc> .

/OK - вывод сообщения "Ok" для неинфицированных файлов.

/QU - выход в командную строку DOS сразу после окончания проверки компьютера.

/RP[+][<файл>] - запись протокола работы в файл, имя которого задается параметром <файл>. По умолчанию используется файл REPORT.WEB в каталоге программы Dr. Web. "+" применяется для прибавления текущего отчета в конец уже существующего файла отчета. В противном случае файл отчета будет пересоздаваться заново.

/RV - контроль за заражением проверяемых файлов активным резидентным вирусом.

/SD - поиск и тестирование файлов во всех вложенных подкаталогах, начиная с корневого, указанного пользователем или текущего.

/SV - автоматическое сохранение по окончании работы параметров, заданных при текущем запуске программы.

/TD<диск>: - параметр <диск> определяет устройство, на котором будут создаваться временные файлы.

/UP[N][W] - проверка файлов, упакованных архиваторами LZEXE, DIET, PKLITE и т. п., а также вакцинированных антивирусом CPAV. Чтобы Doctor Web не отображал на экране названия программы архиватора, использованной для упаковки проверяемого файла, укажите дополнительный параметр N. Если задать дополнительный параметр W, выполняется восстановление файла и удаление из него кода распаковщика. Необходимо отметить, что, как правило, режим /UPW необходим только в экстренных случаях, например, при подозрении на нахождение неизвестного программе Doctor Web вируса "под упаковщиком" в определенном файле. В данном случае можно произвести восстановление данного файла в

оригинальное состояние с помощью параметра /UPW с целью дальнейшего самостоятельного изучения этого объекта на предмет инфицированности. Для обычного тестирования файлов достаточно указать просто параметр /UP. В данном режиме Dr. Web производит восстановление, или распаковывание упакованного файла во временный файл, который после этого и подвергается тестированию. После тестирования, если был установлен дополнительный параметр W, этот временный файл будет переписан, замещая исходный, и таким образом исходный упакованный файл станет распакованным.

/WA - отображение статистики после проверки каждого заданного объекта.

/? - вывод на экран краткой справки о работе с программой.

В случае запуска сканера с параметром /CL, при котором Doctor Web не использует диалоговую оболочку, появляется возможность проанализировать код завершения, возвращаемый программой. DrWeb возвращает следующие коды завершения, которые можно проверить с помощью переменной ERRORLEVEL:

- 0 - вирусы не обнаружены;
- 1 - обнаружены известные вирусы;
- 2 - обнаружены неизвестные вирусы или подозрительные файлы.

Ниже приведен пример командного файла для запуска DrWeb и последующей проверки возвращаемого сканером значения. В случае обнаружения вируса на экран в цикле выдается соответствующее сообщение.

```
drweb C: /CL /NM
echo off
if errorlevel 2 goto new_vir
if errorlevel 1 goto vir
goto end
:vir
```

```
echo Внимание! Обнаружен известный вирус!!!
pause
goto end
:new_vir
echo Внимание! Подозрение на неизвестный вирус!!!
pause
:end
```

### *3.1.2. Транзитный углубленный анализ на наличие вирусов*

Одним из наиболее популярных в нашей стране транзитных ревизоров для сред MS-DOS, а также Windows 3.1 и 3.11 является ревизор Adinf, разработанный Дмитрием Мостовым. К достоинствам ревизора Adinf (Advanced Diskinfoscope) можно отнести то, что он работает с диском непосредственно по секторам путем прямого обращения к функциям BIOS без использования функций DOS. Такой способ проверок полностью исключает маскировку Stealth-вирусов и обеспечивает весьма высокую скорость поиска вирусов.

Детальное описание ревизора Adinf приведено в текстовых файлах ADINF.TXT и ADINFFAQ.TXT, поставляемых вместе с этим антивирусным средством. Рассмотрим лишь наиболее важные особенности использования последних версий Advanced Diskinfoscope (10, 11).

Перед инсталляцией и первым запуском ревизора следует с помощью сканера DrWeb или AidsTest осуществить тщательный поиск и обезвреживание вирусов в оперативной памяти и на всех логических дисках компьютера.

В процессе инсталляции ревизора Adinf осуществляется добавление строки его вызова в файл AUTOEXEC.BAT и при первом запуске ре-

визора формируются следующие эталонные характеристики компьютерной системы:

- ♦ объем занимаемой оперативной памяти;
- ♦ адрес обработчика прерывания 13h, используемого операционной системой и программами для низкоуровневого доступа к дискам;
- ♦ код внесистемного загрузчика, таблицу разделов и вторичные загрузочные записи жестких дисков;
- ♦ количество и адреса расположения сбойных кластеров логических дисков;
- ♦ структуру системных областей логических дисков каждого винчестера;
- ♦ контрольные суммы содержимого файлов с программами, а также их системные характеристики: путь, дата и время создания, длина, значения атрибутов, адреса физического расположения.

При следующих запусках Adinf выполняет проверки на соответствие эталонным характеристикам в следующей последовательности:

**1)** проверяется объем занятой оперативной памяти и адрес обработчика прерывания 13h;

**2)** анализируются главная и вторичные загрузочные записи жестких дисков;

**3)** проверяются загрузочные сектора логических дисков каждого винчестера;

**4)** анализируется количество и адреса сбойных кластеров логических дисков;

**5)** проверяются деревья каталогов заданных логических дисков;

**6)** сверяются характеристики и контрольные суммы программных файлов.

Обнаруженные изменения анализируются и если они безобидны, например, изменения даты и времени создания, то Adinf помещает ин-

формацию об изменениях в список, который можно просмотреть и одобрить. Если же происходят подозрительные изменения, то ревизор предупредит о возможности заражения вирусом.

К подозрительным изменениям относятся следующие:

- ♦ изменение объема доступной оперативной памяти или адреса обработчика прерывания 13h;
- ♦ изменения в системных областях жестких дисков;
- ♦ появление новых сбойных кластеров;
- ♦ изменение контрольных сумм заданных файлов;
- ♦ изменение длины файлов без изменения даты и времени модификации;
- ♦ изменение файлов с появлением странных даты и времени модификации, например, 35 марта.

Новые сбойные кластеры на винчестере могут появиться после использования таких утилит проверки и восстановления дисковой памяти, как NDD, ScanDisk, Calibrat и других, которые могли сами пометить неустойчивые или дефектные кластеры как сбойные.

При обнаружении изменений в загрузочных записях жестких дисков Adinf автоматически восстанавливает их исходное содержимое по эталонной информации с выдачей сообщения пользователю.

При обнаружении этих и других изменений следует установить их причину. Если не своевременно была обновлена системная информация, то ее следует обновить. В противном случае произошло заражение компьютерным вирусом. В этой ситуации необходимо приступить к поиску и обезвреживанию вирусов, для чего можно использовать сканеры DrWeb и AidsTest или воспользоваться функциями программы ADinf Cure Module, которая за отдельную плату поставляется вместе с ревизором Adinf.

Программа ADinf Cure Module является универсальным дезинфектором (полифагом), предназначенным для удаления вирусов и восста-

новления зараженных файлов. Восстановление зараженных программ выполняется на основе эталонной информации об этих программах, созданной ревизором Adinf, а не на основе данных о принципах действия известных вирусов. Эта особенность ADinf Cure Module дает возможность полного восстановления программ, зараженных не только известным, что характерно для сканеров, но и неизвестным вирусом.

Подобно сканеру DrWeb, ревизор Adinf может работать как в диалоговом, так и в пакетном режимах. Пакетный режим удобен для ежедневного вызова ревизора из командного файла AUTOEXEC.BAT.

## Диалоговый режим ревизора Adinf

Для запуска программы Adinf в диалоговом режиме достаточно запустить на выполнение файл Adinf.exe, находящийся в каталоге, куда был инсталлирован ревизор.

После запуска программы Adinf появляется заставка ревизора. Далее нажатие любой клавиши приведет к полному отображению главного окна Adinf (□), основное меню которого всегда является активным. В левой части главного окна ревизора отображается список расширений контролируемых файлов. Для вызова краткой справки необходимо нажать клавишу <F1>. Выход из программы Adinf выполняется по команде **Выход** или путем нажатия клавиши <Esc>.


**Рис. 3.3. Главное окно ревизора Adinf**

Перед поиском и обезвреживанием вирусов следует настроить параметры работы ревизора. Для этого предназначены команды пункта меню **Параметры**. Все установленные параметры функционирования будут автоматически сохранены при выходе из программы Adinf в каталоге расположения ревизора в файле, имя которого начинается с последовательности символов **A-dinf-**.

Команда-переключатель **Параметры/ Таблицы** позволяет сделать выбор между общими и личными таблицами (файлами) для хранения эталонных характеристик элементов компьютерной системы. Общие файлы с эталонной информацией создаются в корневом каталоге каждого проверяемого диска. Личные файлы по умолчанию создаются в каталоге, в котором находится программа ADinf. Пользователь может назначить другой каталог для хранения личных файлов с помощью команды **Параметры/ Настройки/ Путь личных таблиц.** Имена для файлов с эталонными характеристиками задаются по команде **Параметры/ Настройки/ Файлы с таблицами**. По умолчанию эти имена начинаются с последовательности символов **Adinf=**.

Раздел **Режимы** пункта меню **Параметры** включает три команды-переключателя - **Звук, Режим fast, Режим INFO**. Команда **Звук** позволяет

включить и выключить звуковое сопровождение программы. Команда **Режим fast** позволяет включить и отключить режим быстрых проверок диска. В режиме быстрых проверок не анализируются контрольные суммы файлов и можно получить информацию только о новых и стертых файлах и каталогах, а также файлах, у которых изменилась длина. В этом режиме файлы с эталонными характеристиками не обновляются. При включенном режиме **INFO** полная проверка диска выполняется без обновления информации в файлах с их эталонными характеристиками.

Наибольшее количество параметров функционирования ревизора Adinf задается с помощью команд раздела **Параметры/ Настройки** (□).

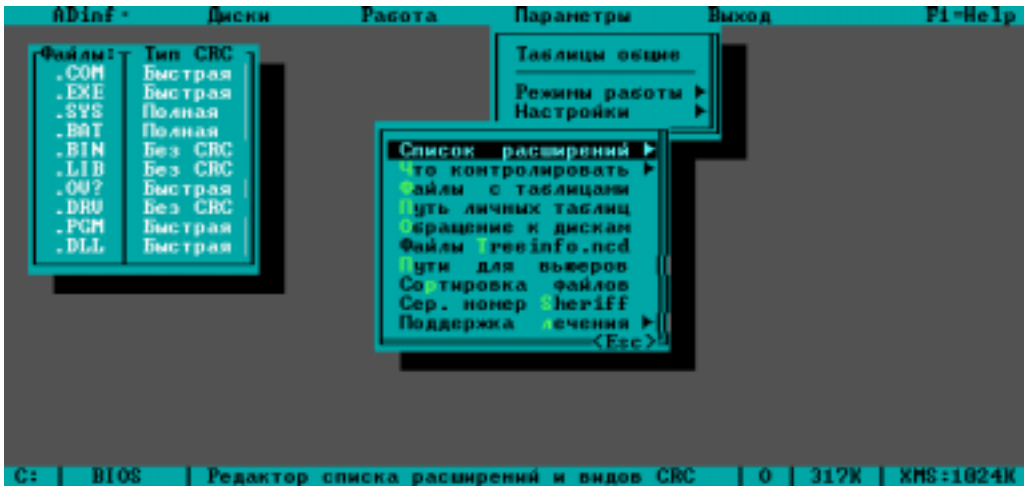


**Рис. 3.4. Команды раздела «Параметры/ Настройки»**

Команды подраздела **Параметры/ Настройки/ Список расширений** позволяют отредактировать список расширений проверяемых файлов, а также задать тип контрольного суммирования для каждого расширения:

- **Полные CRC** - полный контроль за целостностью информации, требующий больше времени для проверки диска;
- **Быстрые CRC** - контрольные суммы привязаны к внутренней структуре исполняемых файлов с расширениями COM и EXE и га-

рантируют надежную защиту от вирусов при малых затратах времени на проверку диска;

- **Без CRC** - контрольные суммы для файлов с соответствующим расширением не рассчитываются.

Команды подраздела **Параметры/ Настройки/ Что контролировать** позволяют выбрать состав проверяемой информации:

- **Расширения** - включает две альтернативы:
  - ⇒**Все файлы** - контролируются все файлы на проверяемых дисках;
  - ⇒**По списку** - контролируются только файлы, имеющие расширения, заданные по команде **Параметры/ Настройки/ Список расширений**;
- **Неизменяемые** - позволяет определить список файлов, любое изменение которых расценивается как подозрительное (файлы, определенные как неизменяемые, всегда проверяются по полной контрольной сумме).
- **Boot-Секторы** - позволяет включить или выключить контроль за загрузочными секторами дисков (отключать этот контроль бывает необходимо, например, для дисков, уплотняемых системой Stacker, поскольку эта система постоянно модифицирует содержимое BOOT-сектора);
- **Кластеры** - позволяет включить или выключить контроль за появлением новых сбойных кластеров для различных дисков;
- **Подкаталоги** - позволяет включить или выключить контроль за изменением структуры дерева каталогов диска (поиск новых и стертых каталогов);

- **Рабочие кат.** - предназначена для снижения уровня контроля за изменениями файлов в тех подкаталогах, где ведется интенсивная работа и часто изменяются файлы;
- **Таблицы HDPT** - позволяет включить/выключить контроль за таблицами Hard Disk Parameter Tables в оперативной памяти в области переменных BIOS;
- **Контр. новых** - позволяет включить/выключить режим автоматического поиска Stealth-вирусов в новых файлах;
- **Контр. изм.** - позволяет включить/выключить режим автоматического поиска Stealth-вирусов в измененных файлах.

Переключатели подраздела **Параметры/ Настройки/ Обращение к дискам** позволяют изменить способ доступа к проверяемым дискам. Диски, размеченные программой FDISK, ADinf проверяет непосредственно через BIOS, однако в некоторых нестандартных ситуациях можно указать на необходимость проверок через прерывания Int 13h или Int 25h/26h. Переключение текущего режима выполняется нажатиями клавиши Ins.

Переключатели подраздела **Параметры/ Настройки/ Файлы treeinfo.ncd** позволяют включить режим поддержки файлов с информацией о структуре диска, создаваемых пакетами Norton Commander (Nc) и Norton Change Directory (Ncd). Включив режим обновления, можно сэкономить некоторое время, избежав повторного сканирования диска этими программами, поскольку при проверках ADinf имеет полную информацию о структуре диска и может сохранить ее в виде файла treeinfo.ncd. По умолчанию обновление файлов treeinfo.ncd отключено.

Команда **Параметры/ Настройки/ Пути для вьюеров** позволяет задать пути к каталогам, в которых ADinf будет искать исполняемые модули при запуске внешних индивидуальных программ просмотра и редакторов. Можно задать несколько путей, разделенных символом ';'.

Команды-переключатели подраздела **Параметры/ Настройки/ Сортировка файлов** позволяют определить вид сортировки списка файлов при отображении новых, измененных, удаленных, перемещенных и переименованных файлов. Допускается сортировка по расширениям имен файлов или по именам каталогов.

Команда **Параметры/ Настройки/ Сер. номер Sheriff** позволяет указать серийный номер платы аппаратно-программной антивирусной системы Sheriff в случае ее установки на компьютере.

Команды **Параметры/ Настройки/ Поддержка лечения** позволяют настроить параметры использования антивирусной программы ADinf Cure Module, предназначенной для оперативного лечения зараженных файлов.

После запуска ADinf в диалоговом режиме автоматически выбирается команда **Работа/ Проверить все**. Если нажать на клавишу Enter, то ADinf начнет проверку всех дисков, для которых была созданы эталонные характеристики.

Для проверки отдельных дисков необходимо выполнить следующие действия:

**1)** с помощью пункта меню **Диски** выбрать нажатиями клавиши Enter логические приводы, диски которых должны быть проверены (повторное нажатие клавиши Enter на выбранном имени логического привода отменяет выбор);

**2)** выполнить команду **Работа/ Проверить диск**.

Принудительная остановка процесса проверки выполняется путем нажатия клавиши Esc.

Чтобы обновить или создать файлы с эталонными характеристиками, необходимо проделать следующее:

**1)** с помощью пункта меню **Диски** выбрать нажатиями клавиши Enter логические приводы, для дисков которых создаются или обновляются файлы с эталонными характеристиками;

**2)** выполнить команду **Работа/ Создать таблицы**.

Для поиска активных Stealth-вирусов необходимо с помощью команды **Диски** выбрать требуемые для проверки логические приводы и выполнить команду **Работа/ Поиск стелс**. Остановка поиска Stealth-вирусов выполняется нажатием клавиши Esc. Сканируя диск, ADinf проверяет загрузочные сектора жестких дисков, а также сравнивает длины и контрольные суммы файлов, определяемые средствами DOS, с фактическими, получаемыми путем непосредственного чтения секторов диска прямым обращением в BIOS. Если ревизор обнаруживает несовпадение, то немедленно прекращает сканирование диска, чтобы не распространить вирус по еще не зараженным каталогам, и выдает сообщение пользователю о заражении Stealth-вирусом. В этом случае следует выключить компьютер, спустя 10-15 секунд загрузиться с системной дискеты из состава средств восстановления и приступить к восстановлению нормальной работоспособности компьютера и обезвреживанию вирусов.

В ревизоре Adinf имеется возможность автоматического контроля всех новых файлов на заражение Stealth-вирусами. Этот режим устанавливается по команде **Параметры/ Настройки / Что контролировать/ Контр. новых** и позволяет обнаружить Stealth-вирусы, заражающие файлы только при их создании, например при переписи с дискеты или распаковке архивов.

Последняя строка главного окна ревизора является статусной строкой, в которой отражается следующая информация:

- ♦ имя первого из логических приводов, выбранных для обработки, или имя логического привода обрабатываемого диска;
- ♦ способ доступа к диску (через BIOS, Int 13h или Int 25h/26h);
- ♦ краткое описание выбранного пункта меню;
- ♦ тип используемых таблиц (О -общие, Л - личные);
- ♦ объем доступной оперативной памяти.

## Пакетный режим ревизора Adinf

Для запуска ревизора Adinf из файла AUTOEXEC.BAT, а также из других командных файлов удобно использовать его пакетный режим работы. В этом случае параметры поиска и обезвреживания вирусов указываются непосредственно в командной строке вызова ревизора.

Командная строка для вызова ревизора Adinf имеет следующий формат:

<путь>\Adinf[.exe] [<ключ>...<ключ>] [<диск>:] ... [<диск>:]

Здесь <путь> определяет полный путь к ревизору Adinf.exe, включая имя диска и каталог, куда он инсталлирован, например, C:\ADINF. Параметры <диск> содержат имена логических приводов проверяемых дисков. Вместо списка дисков можно задавать параметр "*". В этом случае будут проверены все диски, для которых будут найдены файлы с эталонными характеристиками, созданные ревизором. Например, для проверки всех дисков в пакетном режиме можно набрать команду

C:\ADINF\ADinf *

Режимы работы ревизора задаются параметрами <ключ>. Каждый ключ должен начинаться с символа '-' или '/' и может задаваться как маленькими, так и заглавными буквами. Ниже описаны наиболее полезные ключи запуска.

/A - устанавливает режим, в котором исключены некоторые малозначащие диалоговые остановки.

/B - отменяет закрашивание фона экрана и оставляет "прозрачный" фон. Такой режим улучшает эстетическое восприятие программы при запуске из файла AUTOEXEC.BAT.

/co[lor] - использовать цвета для цветного монитора.

/D - включает режим работы 1 раз в сутки, что экономит время при перезагрузках, если вызов программы ADinf стоит в файле AUTOEXEC.BAT.

/E - не ставить атрибут Hidden файлам с таблицами.

/F - включает режим быстрой проверки без расчета контрольных сумм файлов. В этом режиме невозможно обновление информации в файлах с эталонными характеристиками. Этот ключ аналогичен включению опции "Режим fast" в диалоговом режиме работы программы.

/force13 - заставляет ADinf переопределить адрес прерывания 13h в bios.

/I - включает "информационный" режим, при котором после проверок дисков файлы с эталонными характеристиками не обновляются. Нельзя использовать одновременно ключи /i и /d. Этот ключ аналогичен включению опции "Режим info" в диалоговом режиме работы программы.

/I+[<путь>] позволяет записать протокол проверки на диск в каталог, указанный после ключа /I+. Например, /I+C:\ADINF\. Если указать ключ /I+ без пути, то протокол будет записан в текущий каталог. Если файл с протоколом существует, то протокол дописывается в существующий файл. Протокол проверки можно также записать, не задавая ключа -I+, а выбрав вариант "Записать протокол изменений" из меню после просмотра результатов проверки диска.

/I[<путь>] позволяет записать протокол проверки на диск в каталог, указанный после ключа -I, например -IC:\ADINF\. Если указать ключ -I без пути, то протокол будет записан в текущий каталог. От ключа -I+ отличается тем, что дозапись в существующий файл не производится и файл протокола замещает существовавший.

/P[<путь>] включает режим ЛИЧНЫХ таблиц, предусмотренный специально для пользователей "персональных ЭВМ коллективного пользования". В обычном режиме программа ADinf создает свои файлы с эталонными характеристиками в корневом каталоге контролируемых дисков. Этот ключ аналогичен опции "Таблицы личные" в диалоговом режиме работы программы.

/S - отключить звуковое сопровождение программы. Этот ключ аналогичен опции "Звук выключен" в диалоговом режиме работы программы.

/Setup: <путь> - задает каталог или полную спецификацию файла для записи параметров функционирования ADinf. По умолчанию файл настроек с именем A-Dinf--.--- записывается в тот же каталог, где расположена программа Adinf.exe. Переназначить каталог для записи файла с установками бывает необходимо, если Adinf установлен на защищенный от записи раздел диска. Для этого необходимо задать путь в строке запуска ADinf в виде:

ADinf -Setup:D:\READWR\

В этом примере состояние программы будет сохраняться в файле с полным именем D:\READWR\A-Dinf--.---.

Существует возможность сохранять несколько файлов настроек программы с разными списками расширений, именами файлов эталонных характеристик, методом доступа к дискам и т.д. Для этого необходимо в строке запуска задать имя файла для записи установок, например в случае

ADinf -Setup:My_Setup

будет использован файл My_Setup.---, расположенный в том же каталоге, где расположен файл ADinf.exe, а в случае

ADinf -Setup:D:\SET\My_Setup

будет использован файл My_Setup, расположенный в каталоге D:\SET.

/Stop - при задании этого ключа в строке вызова ADinf из любое изменение, зафиксированное ревизором будет приводить к выдаче сообщения о необходимости вызвать системного программиста и продолжать работать на машине до прихода ответственного системного программиста будет нельзя.

/W - включает режим построения новых таблиц для диска.

/@<имя файла> - включает режим, при котором формируется список файлов, требующих последующей проверки полифагами. Этот список включает новые, измененные, переименованные и перемещенные из каталога в каталог файлы. Для проверки этих файлов можно использовать полифаги Aidstest и Doctor Web с ключем /@.

В процессе инсталляции ревизора Adinf в файл AUTOEXEC.BAT осуществляется добавление следующей строки его вызова

<путь>\Adinf.exe -d -a -b -l<путь> [<диск>:] ... [<диск>:]

Здесь <путь> определяет путь к ревизору Adinf.exe, а также каталог, куда будет осуществляться запись протокола проверок (ключ -l). Другие ключи (-d, -a, -b) определяют работу один раз в сутки, исключить некоторые малозначащие диалоговые остановки и не закрашивать фон экрана. Параметры <диск> содержат имена логических приводов проверяемых дисков. Например, добавляемая в файл автозапуска строка может быть следующей

C:\ANTIVIR\ADINF\ADINF.EXE -d -a -b -lC:\ANTIVIR\ADINF C: D:

Строку вызова ревизора при инсталляции необходимо вставить в файл AUTOEXEC.BAT до вызова командной оболочки, иначе в процессе загрузки операционной системы ревизор запускаться не будет.

### *3.1.3. Резидентная защита от компьютерных вирусов*

Для резидентной защиты от деструктивных действий и размножения вирусов в первую очередь целесообразно установить режим аппаратного контроля попытки модификации внесистемного загрузчика и таблицы разделов винчестера, находящихся в загрузочном секторе (MBR) каждого жесткого диска компьютера. Дальнейшего расширения количества блокируемых функций вирусов можно добиться путем использования эффективного антивирусного фильтра. Максимальная же степень безопасности будет достигнута при дополнении защиты от деструктивных действий и

размножения вирусов полным динамическим контролем на их наличие, реализуемым при совместном выполнении функций, характерных для резидентных сканеров и ревизоров.

Рассмотрим особенности использования резидентной антивирусной программы Vsafe, входящей в состав последних версий MS-DOS и являющейся наиболее популярным и функционально полным резидентным антивирусным средством для сред MS-DOS и Windows 3.11 (3.1).

Vsafe обеспечивает выполнение функций всех типов резидентных антивирусных средств - фильтра, сканера и ревизора. К этим функциям относятся следующие:

- функции, характерные для фильтра:
  - ⇒ перехват попыток выполнения вирусами деструктивных действий;
  - ⇒ перехват действий, связанных с размножением вирусов;
- функции, характерные для резидентного сканера:
  - ⇒ проверка открываемых для выполнения, копирования или переноса программных файлов на наличие известных вирусов;
  - ⇒ проверка на наличие вирусов загрузочных секторов дисков, к которым производится обращение;
- функции, характерные для резидентного ревизора:
  - ⇒ формирование эталонных характеристик открываемых незарегистрированных программных файлов и занесение полученных данных в файлы с эталонной информацией;
  - ⇒ проверка открываемых зарегистрированных программных файлов на соответствие эталонным характеристикам с возможным блокированием дальнейшего доступа при обнаружении несоответствий.

В качестве эталонных характеристик каждого программного файла используются как его контрольные суммы, так и другие системные харак-

теристики: путь, дата и время создания, длина, а также значения файловых атрибутов.

Выполнение программой Vsafe функций, характерных для резидентных ревизоров возможно только при ее совместном использовании с транзитным сканером-ревизором MSAV (MWAV). Для работы в среде MS-DOS предназначен транзитный сканер-ревизор MSAV, а для среды Windows 3.1 и 3.11 - транзитный сканер-ревизор MWAV. Обе программы, как и Vsafe входят в состав MS-DOS последних версий и отличаются лишь интерфейсом пользователя. Совместное использование данных антивирусных средств, образующих завершенный антивирусный пакет, обеспечивает эффективное дополнение антивирусной защиты, реализуемой с помощью сканера DrWeb и ревизора Adinf.

## Настройка резидента Vsafe

Программа Vsafe запускается командной строкой следующего формата:

VSAFE[.COM] [/<ключ>{+|-}] ... [(/A <клавиша>)|(/C <клавиша>)] [/N] [/D]

Как и раньше, квадратные скобки здесь определяют необязательные параметры. Параметры, разделенные символом «|», являются взаимоисключающими. Круглые и фигурные скобки приведены для указания взаимоисключающих параметров, а параметры, заключенные в треугольные скобки указывают на то, что вместо них должно подставляться конкретное значение.

Каждый из параметров /<ключ>{+|-} задает режим активизации (символ «+») или отключения (символ «-») соответствующей функции резидента. Можно активизировать или отключить следующие функции:

**1)** перехват попытки низкоуровневого форматирования жесткого диска (ключ /1+ для активизации или /1- для отключения; по умолчанию функция активизируется);

**2)** перехват попытки любой программы оставить резидентный код в оперативной памяти (ключ /2+ для активизации или /2- для отключения; по умолчанию функция не активизируется);

**3)** перехват любой попытки записи на диск (ключ /3+ для активизации или /3- для отключения; по умолчанию функция не активизируется);

**4)** проверка на наличие известных вирусов в открываемых системой программных файлах (ключ /4+ для активизации или /4- для отключения; по умолчанию функция активизируется);

**5)** проверка на наличие вирусов в системной области дисков, к которым производится доступ (ключ /5+ для активизации или /5- для отключения; по умолчанию функция активизируется);

**6)** перехват попытки записи в системную область жесткого диска (ключ /6+ для активизации или /6- для отключения; по умолчанию функция активизируется);

**7)** перехват попытки записи в системную область гибкого диска (ключ /7+ для активизации или /7- для отключения; по умолчанию функция не активизируется);

**8)** перехват попытки модификации программного файла (ключ /8+ для активизации или /8- для отключения; по умолчанию функция не активизируется).

Как видно из перечня функций по умолчанию активизируются только функции перехвата попытки низкоуровневого форматирования винчестера и записи в его системную область, а также проверки на наличие вирусов в программных файлах и загрузчиках дисков, к которым осуществляется доступ. Такой режим целесообразно задавать в качестве обычного режима работы резидента, так как активизация остальных его функций может привести к назойливости по отношению к пользователю. Например, при активизации функции перехвата любой попытки записи на диск,

придется постоянно отвечать на запросы антивирусного резидента при каждом копировании, переносе, переименовании, модификации или удалении файлов и каталогов.

При активизации функции перехвата попытки модификации исполняемого файла следует учитывать, что многие программы после своего запуска модифицируют различные параметры, расположенные в файлах их расположения.

Другие переключатели определяют следующее:

**/A <клавиша>** - использовать для активизации меню резидента комбинацию клавиш Alt+<клавиша>;

**/C <клавиша>** - использовать для активизации меню резидента комбинацию клавиш Alt+<клавиша>;

**/N** - разрешить резиденту выполнять свои функции не только для локальных, но и сетевых приводов;

**/D** - отключить функцию формирования эталонных характеристик открываемых программных файлов, для которых эти характеристики еще не сформированы.

Если не задан ни один из переключателей **/A <клавиша>** или **/C <клавиша>**, то для активизации меню резидента будет использоваться комбинация клавиш <Alt>+<V>. Активизировав меню (□) в любой момент после запуска резидента Vsafe, можно переустановить параметры его функционирования. Номера функций в меню соответствуют цифрам в ключах строки запуска резидента. Активизированные функции в меню отмечаются символом «X». Чтобы отключить или, наоборот, активизировать какую-либо функцию резидента после вызова его меню, следует нажать клавишу с номером этой функции. Для выхода из меню используется клавиша <Esc>.

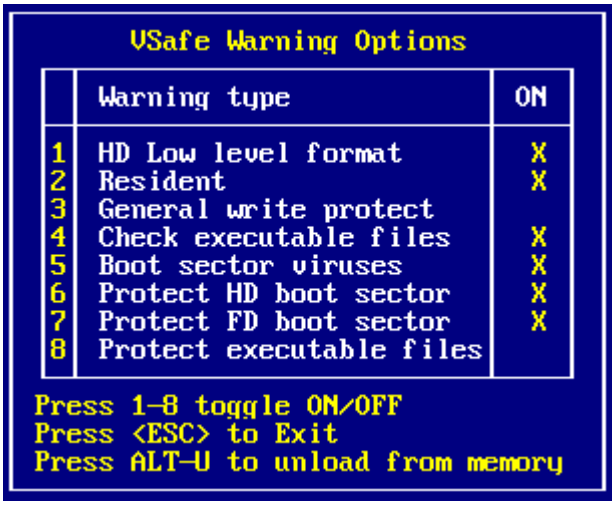


**Рис. 3.5. Меню резидента Vsafe**

Для завершения работы программы Vsafe и выгрузки ее резидентного кода из оперативной памяти можно воспользоваться одним из следующих способов:

- ♦ нажать комбинацию клавиш <Alt>+<U>;
- ♦ ввести команду: VSAFE[.COM] /U

Если резидент Vsafe необходимо использовать в среде Windows 3.1 или 3.11, то для этого нужно выполнить следующие действия:

**1)** запустить программу Vsafe в среде MS-DOS до загрузки Windows;

**2)** после загрузки Windows запустить программу MWAVTSR.EXE из каталога DOS, которая предназначена для инициализации режима работы резидента Vsafe в среде Windows 3.1 и 3.11.

После запуска программы MWAVTSR.EXE активизируется окно резидента «Vsafe Manager» (□), которое затем можно свернуть. Для изменения режима работы антивирусного резидента в среде Windows следует развернуть его окно «Vsafe Manager» и нажать кнопку **Options**. Активизация и отключение функций резидента в появившемся окне параметров (□) выполняется щелчками кнопкой мыши на соответствующих флажках. Для дезактивизации резидента Vsafe в среде Windows в его главном окне следует выполнить команду **Options/ Exit**.


**Рис. 3.6. Окно «Vsafe Manager»**

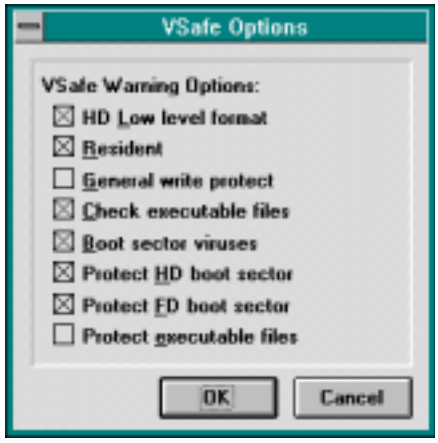


**Рис. 3.7. Окно «Vsafe Options»**

Особенностью работы резидента Vsafe в среде Windows является то, что функцию перехвата любой попытки записи на диск никогда не следует активизировать, так как по причине использования в Windows виртуальной памяти активизация этой функции приведет к отказу системы.

## Формирование и проверка эталонных характеристик программных файлов

Режим выполнения программой Vsafe функций, характерных для резидентного ревизора отключен быть не может. Однако, для эффективного выполнения этих функций необходимо перед использованием антивирусного резидента с помощью транзитного сканера-ревизора MSAV или MWAV создать эталонные характеристики существующих программных файлов.

Сформированные MSAV или MWAV эталонные характеристики программных файлов отдельного каталога записываются в файл CHKLIST.MS, размещаемый в этом же каталоге. Поэтому, если в каталоге открываемого программного файла отсутствует файл эталонных характеристик CHKLIST.MS, то для этого программного файла резидент Vsafe функции проверки эталонных характеристик не выполняет, а осуществляет формирование этих характеристик, создавая файл CHKLIST.MS.

Для формирования эталонных характеристик программных файлов в среде MS-DOS с помощью сканера-ревизора MSAV требуется выполнить следующие действия:

1) запустить программу MSAV.EXE из каталога MS-DOS, в результате чего появится главное окно этой программы (□□);

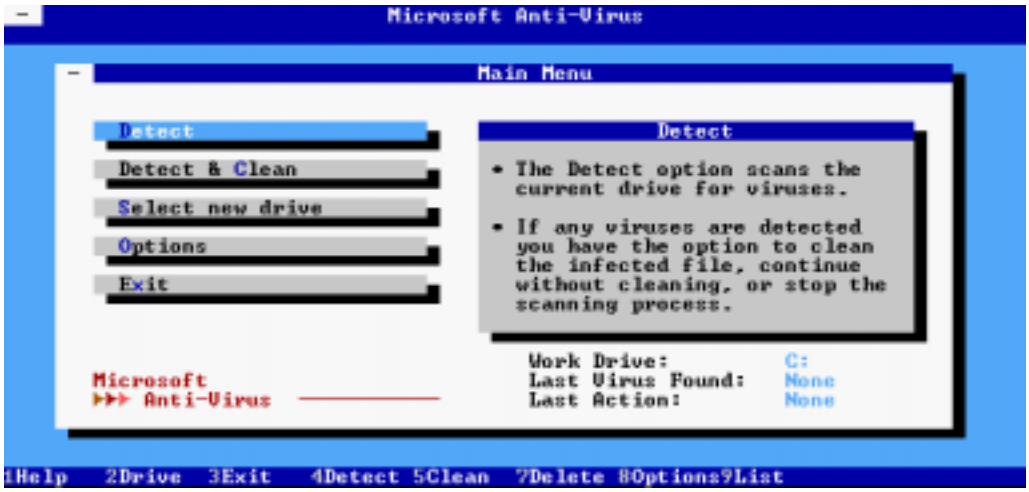


**Рис. 3.8. Главное окно программы MSAV**

2) нажать кнопку **Options** главного окна программы, в результате чего появится диалоговое окно «Options Setting» (□□);

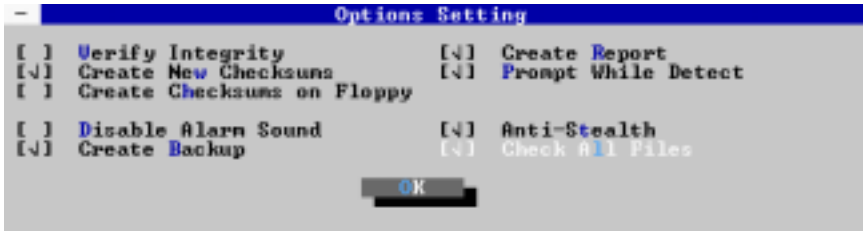


**Рис. 3.9. Окно «Options Setting»**

3) в окне «Options Setting» сделать следующие установки:

- сбросить флажок **Verify Integrity**, устанавливаемый для проверки на соответствие файлов эталонным характеристикам;
- установить флажок **Create New Checksums** для создания эталонных характеристик файлов на жестком диске;
- установить флажок **Create Checksums on Floppy**, если необходимо формирование эталонных характеристик файлов на гибком диске;
- установить флажок **Check All Files** при необходимости формирования эталонных характеристик не только для программных, но и остальных файлов; к программным файлам антивирус относит файлы, имеющие расширения .386, .APP, .BIN, .CMD, .COM, .DOM, .DLL, .DRV, .EXE, .FON, .ICO, .OV*, .PGM, .PIF, .PRG, и .SYS;
- учитывая, что эталонные характеристики создаются в процессе проверки на наличие вирусов, целесообразно также установить флажки:

⇒ **Create Report** - обеспечивается формирование отчета о работе антивирусного средства в файле MSAV.PRT, размещаемом в корневом каталоге обрабатываемого диска;

⇒ **Prompt While Detect** - при обнаружении зараженной программы пользователю будет выдан запрос, ответом на который он может активизировать процесс обезвреживания вируса;

⇒ **Anti-Stealth** - выполнение проверки на наличие Stealth-вирусов;

4) нажать кнопку Ok;

5) выбрать с помощью кнопки Select new drive требуемый диск и далее нажать кнопку Detect для активизации процесса поиска вирусов и создания эталонных характеристик.

Пятый шаг приведенной последовательности действий следует выполнить для всех логических дисков винчестера, а также для требуемых дискет.

Выход из программы MSAV выполняется нажатием кнопки **Exit** или с помощью клавиши <Esc>. Если требуется сохранить текущие настройки программы для следующих сеансов работы, то после нажатия кнопки **Exit** или клавиши <Esc> в появившемся окне «Close Microsoft Anti-Virus» перед нажатием кнопки **Ok** следует установить флажок **Save Configuration**.

При необходимости удаления эталонных характеристик, например, перед их обновлением по причине замещения старых версий программных продуктов, следует в среде программы MSAV с помощью кнопки **Select new drive** выбрать диск, на котором будут удаляться эталонные характеристики, нажать клавишу <F7> и далее кнопку **Delete**. Для удаления эталонных характеристик файлов отдельного каталога следует из этого каталога удалить файл CHKLIST.MS. При последующих проверках на наличие вирусов с помощью программы MSAV, если установлен флажок **Create New Checksums** (**Create Checksums on Floppy**), отсутствующие эталонные характеристики файлов проверяемого диска будут формироваться автоматически.

Особенности использования транзитного сканера-ревизора MWAV для Windows 3.1 или 3.11 по формированию эталонных характеристик те же, что для программы MSAV, за исключением интерфейса пользователя. В среде программы MWAV (□□) выбор дисков выполняется в окне

«Drives». Для настройки опций следует выполнить команду **Options/ Set Options** и определить требуемые параметры в окне «Options» (□□). Активизация проверки на наличие вирусов и создания эталонных характеристик выполняется нажатием кнопки **Detect** (□□). Удаление эталонных характеристик выбранного диска выполняется по команде **Scan/ Delete CHKLIST files**. При необходимости сохранения текущих настроек программы для следующих сеансов работы следует включить команду-переключатель **Options/ Save Settings on Exit**. Выход из программы MWAV выполняется обычным для Windows-программ способом или с помощью команды **Scan/ Exit Anti-Virus**.


**Рис. 3.10. Главное окно программы MWAV**

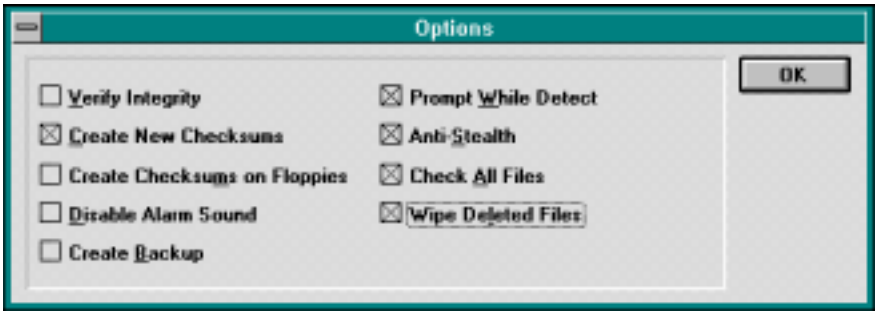


**Рис. 3.11. Окно «Options»**

## Обезвреживание вирусов, обнаруженных резидентом Vsafe

Если в процессе функционирования резидента Vsafe получено сообщение о попытке доступа к программному файлу, зараженному неизвестным вирусом, или о перехваченном действии вируса, то следует ответом на запрос резидента блокировать дальнейшие действия и выполнить все этапы по обезвреживанию вирусов и восстановлению нормального функционирования компьютера. Исключением здесь являются случаи, когда Vsafe перехватывает санкционированные действия пользователя, перед выполнением которых пользователь не отключил соответствующие функции антивирусного резидента, например, когда пользователь запускает какую-либо резидентную программу. В таких случаях следует ответом на запрос Vsafe разрешить дальнейшие действия.

Если же резидентом обнаружен факт заражения открываемого файла известным вирусом, то следует ответом на запрос резидента блокировать дальнейший доступ к этому файлу и далее осуществить поиск и обезвреживание вирусов с помощью транзитного сканера-ревизора MSAV или MWAV. Аналогичные действия следует выполнить и при перехвате попытки доступа к диску с зараженным загрузочным сектором.

Для поиска и обезвреживания вирусов с помощью программы MSAV необходимо проделать следующее:

1) запустить программу MSAV.EXE из каталога MS-DOS;
2) выбрать с помощью кнопки **Select new drive** диск, на котором Vsafe обнаружил вирус;
3) нажать кнопку **Options** главного окна программы, в результате чего появится диалоговое окно «Options Setting» (□□);
4) в окне «Options Setting» сделать следующие установки:

- ♦ установить флажки **Verify Integrity**, **Create Report**, **Prompt While Detect** и **Anti-Stealth**, назначение которых описано выше;

- при необходимости установить флажок **Create Backup**, задающий режим резервирования инфицированных файлов перед их дезинфекцией (дубликат инфицированного файла получает расширение VIR);
- для включения режима звукового оповещения при обнаружении вируса сбросить флажок **Disable Alarm Sound**;
- в случае необходимости установить флажок **Check All Files**, задающий режим проверки на наличие вирусов и на соответствие эталонным характеристикам не только программных, но и всех остальных файлов;
- сбросить флажки **Create New Checksums** и **Create Checksums on Floppy**, задающих формирование эталонных характеристик для файлов;

5) нажать кнопку **Ok**;

6) активизировать процесс поиска и обезвреживания вирусов с помощью кнопки **Detect & Clean** (□□).

Шестой шаг приведенной последовательности действий следует выполнить для всех логических дисков винчестера, а также для дискет, которые использовались на зараженном компьютере.

Особенности применения транзитного сканера-ревизора MWAV для Windows 3.XX по поиску и обезвреживанию вирусов те же, что и для программы MSAV, за исключением интерфейса пользователя. В среде программы MWAV (□□) выбор дисков выполняется в окне **Drives**. Для настройки опций следует выполнить команду **Options/ Set Options**. Активизация процесса поиска и обезвреживания вирусов выполняется нажатием кнопки **Detect and Clean**.

### 3.1.4. Использование антивирусных средств специализированных систем защиты информации

Любая надежная специализированная система защиты информации должна включать подсистему обеспечения эталонного состояния рабочей среды, предназначенную для гарантированной защиты от программных закладок. Здесь под программными закладками понимаются любые программы, с помощью которых злоумышленник может похитить секретные данные или нанести ущерб санкционированным пользователям компьютера.

Обеспечение эталонного состояния рабочей среды в специализированных системах защиты информации выполняется путем периодического контроля целостности данных и эталонного состояния программ, реализующих используемую информационную технологию. Такой периодический контроль позволяет своевременно обнаружить факт несанкционированного вторжения в компьютерную систему, а также устранить причины и последствия этого вторжения.

С точки зрения организации антивирусной защиты подсистема обеспечения эталонного состояния рабочей среды позволяет реализовать уровень углубленного анализа на наличие вирусов. Рассмотрим особенности установки данного уровня с помощью специализированной системы защиты информации «Кобра» [4, 5].

Система «Кобра» в рассматриваемой версии предназначена для обеспечения безопасности хранения и обработки информации в персональных компьютерах, функционирующих под управлением операционной системы MS-DOS/ Windows 3.11 (3.1). Подсистема обеспечения эталонного состояния рабочей среды, входящая в состав данной системы, ориентирована на выполнение следующих функций:

- обнаружение несанкционированных изменений в рабочей среде компьютера со стороны лиц, получивших доступ к ПЭВМ;

- обнаружение несанкционированных изменений, вызванных компьютерными вирусами и программами-вредителями;
- обнаружение искажений в программах и ключевой информации, возникших в результате машинных сбоев или износа магнитного носителя.

Подсистема обеспечения эталонного состояния рабочей среды реагирует на появление разных типов существующих компьютерных вирусов, а также предусматривает возможность появления их новых модификаций и типов. Кроме того, данная подсистема выполняет автоматическое восстановление основных компонентов рабочей среды компьютера, а в случае невозможности автоматического восстановления сигнализирует об этом пользователю, выдавая данные о поврежденных областях рабочей среды для проведения ручного восстановления. Подсистема контролирует состояние оперативной памяти ПЭВМ, содержание главной загрузочной записи (MBR) и загрузочного сектора (BR) диска, состояние батарейной памяти CMOS, файлы конфигурирования и автозапуска CONFIG.SYS и AUTOEXEC.BAT, системные и прикладные программы, а также заданные информационные файлы.

## Создание эталонных характеристик

Перед периодической проверкой характеристик текущей рабочей среды на соответствие эталонным необходимо эти эталонные характеристики создать. Для этого предназначена программа COBRAINS.EXE.

Функции программы COBRAINS.EXE доступны только для пользователей, имеющих статус Администратора или Суперпользователя. При попытке выполнить программу пользователем, не обладающим таким статусом, программа завершает свою работу выдачей соответствующего сообщения.

Перед непосредственным формированием эталонных характеристик рабочей среды с помощью программы COBRAINS необходимо выполнить следующие действия:

1) тщательная проверка компьютера на наличие вирусов и их обезвреживание с помощью доступных сканеров (детекторов-дезинфекторов), например, DrWeb или AidsTest;
2) тщательный анализ файлов конфигурирования и автозапуска на отсутствие вызовов программных закладок и удаление программных закладок при их обнаружении.

Если же перед формированием эталонных характеристик перечисленные действия реализованы не будут, то при создании эталонных характеристик будут сформированы характеристики зараженной среды, и в дальнейшем зараженная среда будет считаться как безопасная.

Для формирования эталонных характеристик следует запустить программу COBRAINS.EXE, задать параметры ее работы и далее нажать клавишу Enter. Формируемые эталонные характеристики программа COBRAINS зашифровывает и записывает в специальные файлы, располагаемые в каталоге, куда была инсталлирована система «Кобра». Если была задана соответствующая опция в параметрах настройки программы, то файлы с эталонными характеристиками будут записаны не только на винчестер, но и на дискету.

Параметры работы программы COBRAINS определяют режим формирования эталонных характеристик и их количество. Задание параметров выполняется с помощью окна настроек (□□), появляющегося сразу после запуска программы .

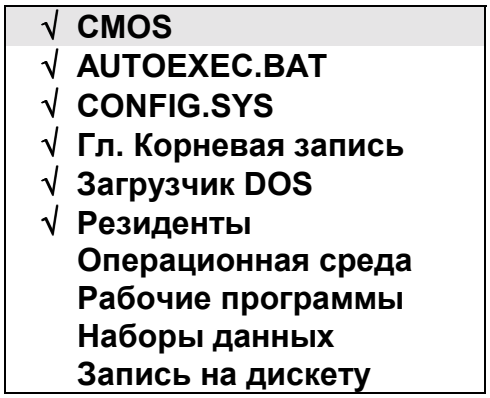


**Рис. 3.12. Окно настроек программы COBRAINS**

Каждая строка окна настроек является командой-переключателем, включенное состояние которой определяет выполнение соответствующей функции после активизации процесса формирования эталонных характеристик нажатием клавиши Enter. При выключенном состоянии команды-переключателя соответствующая ей функция выполняться не будет. Для настройки параметров в окне настроек необходимо нажатием клавиши пробела включить или отключить команды-переключатели. Выбор команды выполняется клавишами с вертикальными стрелками. Включенное состояние команды-переключателя помечается «птичкой».

Все команды, за исключением последней, задают функцию формирования соответствующих им эталонных характеристик:

1) **CMOS** - содержимого CMOS-памяти;
2) **AUTOEXEC.BAT** - содержимого файла автозапуска;
3) **CONFIG.SYS** - содержимого файла конфигурирования CONFIG.SYS;
4) **Гл. Корневая запись** - главной загрузочной записи (MBR) винчестера;
5) **Загрузчик DOS** - системного загрузчика (BR) активного раздела DOS;
6) **Резиденты** - контрольных сумм резидентных программ;

7) **Операционная среда** - контрольных сумм системных программ MS-DOS;

8) **Рабочие программы** - контрольных сумм любых программ;

9) **Наборы данных** - контрольных сумм любых файлов данных.

Если необходима запись всех сформированных эталонных характеристик не только в каталог расположения системы «Кобра», но и на дискету, то в окне настроек необходимо включить команду-переключатель **Запись на дискету**. Дискету с эталонными характеристиками следует формировать обязательно, так как эта дискета понадобиться для восстановления эталонных характеристик рабочей среды, когда автоматическое восстановление с винчестера окажется невозможным.

Формирование эталонных характеристик содержимого CMOS-памяти, файлов автозапуска и конфигурирования, главной загрузочной записи и системного загрузчика винчестера, а также резидентных программ после нажатия клавиши Enter выполняется автоматически.

Если же при активизации процесса формирования эталонных характеристик (нажатии клавиши Enter) были включены такие команды-переключатели как **Операционная среда**, **Рабочие программы** и **Наборы данных**, то для вычисления контрольных сумм по каждой из данных команд будет произведен запрос (□□).

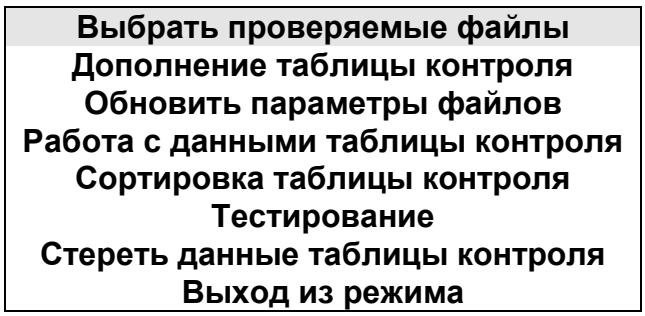


**Рис. 3.13. Запрос на выполнение действий с файлами**

Перед непосредственным вычислением контрольных сумм необходимо сформировать таблицу с обрабатываемыми файлами, называемую таблицей контроля. Для формирования или дополнения такой таблицы требуется выполнить следующие этапы:

1) с помощью команды **Выбрать проверяемые файлы** указать файлы, из которых необходимо сформировать, или которыми следует дополнить таблицу контроля;
2) выполнить команду **Дополнить таблицу контроля**, которая создаст таблицу контроля или дополнит существующую.

Формирование контрольных сумм файлов из таблицы контроля выполняется по команде **Обновить параметры файлов**. Если при следующих запусках программы COBRAINS дополнять таблицу контроля не нужно, то для обновления контрольных сумм файлов из ранее сформированной таблицы достаточно будет ввести команду **Обновить параметры файлов**.

Команда **Работа с данными таблицы контроля** предназначена для просмотра таблицы обрабатываемых файлов и удаления из нее файлов, для которых контрольные суммы проверять не нужно. С помощью команды **Сортировка таблицы контроля** можно задать критерий сортировки файлов в таблице.

По команде **Тестирование** будет выполнена проверка всех файлов из таблицы контроля на соответствие их эталонным характеристикам, если эти эталонные характеристики были созданы по команде **Обновить параметры файлов**.

Для удаления из таблицы контроля всех файлов предназначена команда **Стереть данные таблицы контроля**.

После выполнения всех необходимых действий по формированию контрольных сумм файлов следует выполнить команду **Выход из режима**.

## Поддержание эталонного состояния рабочей среды

Проверка соответствия текущих характеристик рабочей среды компьютера эталонным осуществляется запуском тестовой программы COBRATST.EXE.

Список всех ключей программа выводит на экран при ее запуске с параметром /?:

COBRATST.EXE /?

Для автоматического восстановления измененных файлов необходимо программу COBRATST запустить с параметром /A:

COBRATST.EXE /A

В процессе инсталляции системы «Кобра» вызов программы COBRATST.EXE добавляется в файл автозапуска AUTOEXEC.BAT, что обеспечивает автоматический контроль соответствия текущих характеристик рабочей среды эталонным в процессе загрузки операционной системы.

Если при проверке очередного компонента компьютерной системы устанавливается соответствие его характеристик эталонным, то на экран дисплея выводится сообщение, в котором против имени соответствующего компонента указывается «ОК». При несоответствии текущих характеристик эталонным, в сообщении указывается об обнаруженном факте несоответствия. В этом случае, если для программы COBRATST не был задан режим автоматического восстановления, то следует запустить данную программу повторно, но уже с ключом /a, устанавливающим данный режим. В результате будут автоматически восстановлены: содержимое CMOS-памяти, главная загрузочная запись, загрузчик DOS, CONFIG.SYS, AUTOEXEC.BAT. Также будет предпринята попытка восстановления взятых под контроль и измененных после этого файлов с расширением EXE, причем по каждому из таких файлов будет выведено сообщение об итогах

такой попытки (удачном восстановлении или же, напротив, о невозможности восстановления).

В случае, если в режиме автоматического восстановления появится сообщение об отсутствии или повреждении файлов с эталонными характеристиками на винчестере или загрузка с винчестера окажется невозможной, то необходимо восстановить эталонные характеристики с дискеты, на которую они должны были быть записаны при их формировании. Для этого требуется выполнить следующие действия:

**1)** загрузиться с системной дискеты;

**2)** вставить в дисковод дискету с эталонной средой, запустить с нее программу COBRATST.EXE с ключом /a, и затем ответить соответствующим образом на вопросы программы.

## 3.2. Антивирусная защита в операционной системе Windows 95

Одним из наиболее популярных антивирусных пакетов программ для Windows 95 является локализованный пакет Norton AntiVirus фирмы Symantec. К основному достоинству данного пакета относится его полнофункциональность по установке каждого из уровней антивирусной защиты:

**1)** уровня защиты от проникновения вирусов известных типов;

**2)** уровня углубленного анализа компьютерной системы на наличие вирусов как известных, так и неизвестных типов;

**3)** уровня защиты от деструктивных действий и размножения вирусов.

Для установки первого уровня защиты Norton AntiVirus располагает транзитным и резидентным сканером; второго - транзитным и резидентным ревизором; а третьего - фильтром. Организационно все функцио-

нальные компоненты антивирусного пакета распределены по следующим программам:

- транзитная программа Norton AntiVirus (файл NAVW32.EXE), объединяющая в себе функции транзитных сканера и ревизора;
- резидентная программа Norton Program Scheduler (файл NSCHED32.EXE), предназначенная для планирования и автоматизации транзитных проверок;
- резидентная программа «Автозащита» (файлы NAVAPW32.EXE, NAVAP.VXD и NAVEX.VXD), объединяющая в себе функции фильтра, а также резидентных сканера и ревизора;
- транзитная программа «Аварийный диск» (NRESQ32.EXE), предназначенная для резервирования системной информации и подготовки средств восстановления;
- транзитный сканер-ревизор NAVBOOT.EXE, предназначенный для поиска и обезвреживания вирусов в режиме MS-DOS.

Все перечисленные программы пакета Norton AntiVirus, за исключением последней, предназначены для 32-разрядного режима работы Windows 95.

В процессе инсталляции антивирусного пакета выполняются следующие действия:

- поиск и обезвреживание компьютерных вирусов в оперативной памяти компьютера;
- копирование в заданный пользователем каталог всех компонентов пакета;
- поиск и обезвреживание компьютерных вирусов на жестких дисках;
- вставка в системный реестр параметров настройки антивирусного пакета, а также параметров по загрузке виртуальных драйверов

NAVAP.VXD и NAVEX.VXD для резидентной защиты от компьютерных вирусов;

- вставка в файл автозапуска AUTOEXEC.BAT строки вызова программы NAVBOOT.EXE с параметром /STARTUP для поиска и обезвреживания вирусов в оперативной памяти компьютера и в программах, вызов которых включен в файлы CONFIG.SYS и AUTOEXEC.BAT.
- создание в меню **Пуск/ Программы** папки **Norton AntiVirus** с ярлыками программ **Norton AntiVirus**, **Norton Program Scheduler** и **Аварийный диск**.

Достижение высокого уровня антивирусной безопасности на основе любой специализированной системы защиты возможно только при детальном знании технологии ее применения. Поэтому рассмотрим детально особенности использования каждого из компонентов программного пакета Norton AntiVirus.

### *3.2.1. Транзитный контроль на наличие вирусов и формирование эталонных характеристик*

Для транзитного поиска и обезвреживания вирусов предназначена программа Norton AntiVirus, объединяющая в себе функции транзитных сканера и ревизора. Данная программа обеспечивает одновременный контроль программных файлов и загрузчиков на наличие известных вирусов, а также на соответствие ранее сформированным эталонным характеристикам. Формирование эталонных характеристик программ, для которых эти характеристики еще не были сформированы, может выполняться непосредственно в процессе поиска и обезвреживания компьютерных вирусов. В любом случае транзитный сканер-ревизор эталонные характеристики для каждой программы формирует только при условии отсутствия в ней известных вирусов, т.е. после их поиска и обезвреживания.

Для запуска программы Norton AntiVirus необходимо выполнить одноименную команду в меню **Пуск/ Программы/ Norton AntiVirus** или запустить на выполнение файл NAVW32.EXE в каталоге антивирусного пакета. В результате на экране отобразится главное окно этой программы (□□).

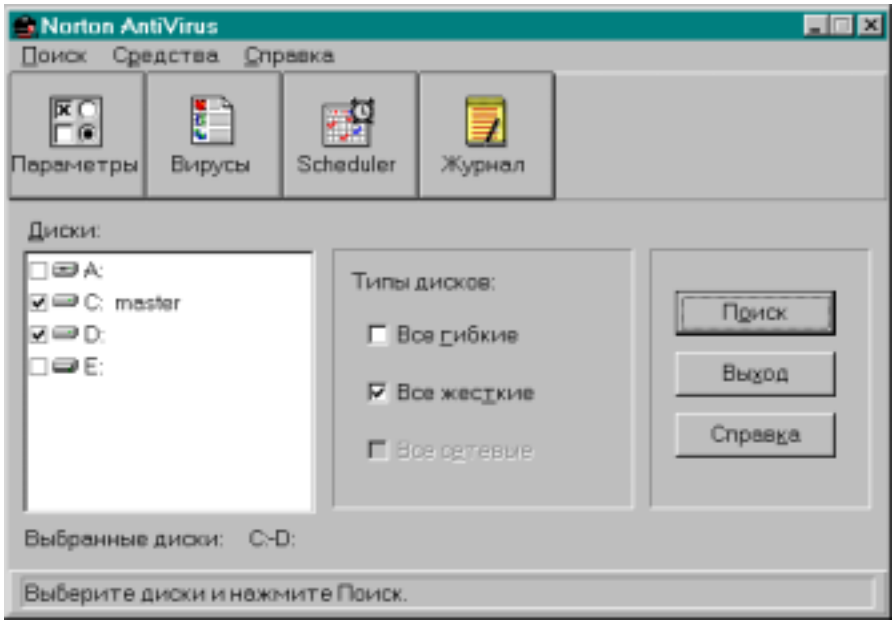


**Рис. 3.14. Главное окно программы Norton AntiVirus**

Команда **Справка/ Стол справок** позволяет осуществить доступ к стандартной справочной системе по использованию всех компонентов антивирусного пакета Norton AntiVirus. Завершение работы программы NAVW32.EXE выполняется стандартным для всех Windows-приложений способом или с помощью команды **Поиск/Выход**.

Перед активизацией процесса поиска и обезвреживания вирусов, а также формирования эталонных характеристик необходимо настроить параметры функционирования транзитного сканера-ревизора. Настройка параметров выполняется в окне «Параметры ...» (□□), появляющемся после нажатия кнопки **Параметры**. Активизацию данного окна можно выполнить также с помощью команды **Средства/ Параметры**.

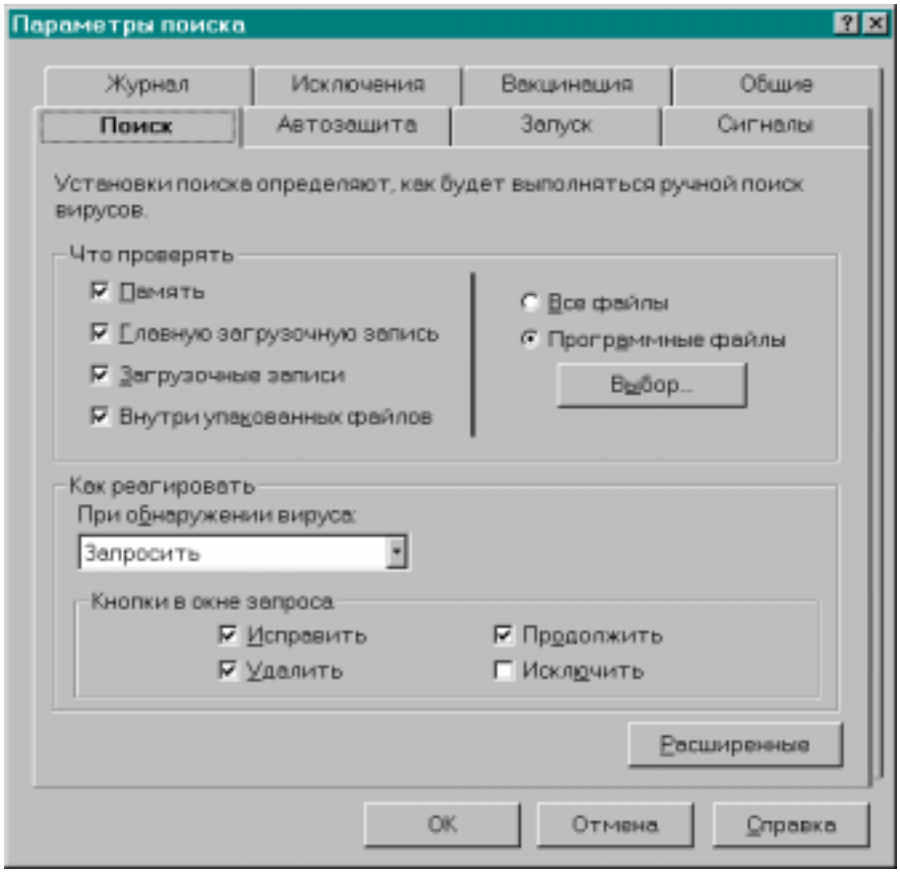


**Рис. 3.15. Лист свойств «Поиск» окна настройки параметров**

Следует отметить, что окно «Параметры ...» обеспечивает настройку параметров функционирования всех программных компонентов пакета Norton AntiVirus. К транзитному сканеру-ревизору непосредственное отношение имеют такие листы свойств как «Поиск», «Общие», «Исключения», «Сигналы», «Вакцинация» и «Журнал». Активизация требуемого листа свойств выполняется щелчком кнопкой мыши на соответствующем корешке.

### Лист свойств «Поиск»

Лист свойств «Поиск» (см. □□) позволяет настроить основные параметры поиска и обезвреживания компьютерных вирусов.

Группа элементов настройки «Что проверять» задает типы программ, подлежащих проверке. Для максимальной защиты следует установить все флажки из данной группы. Установка переключателя в положение **Все файлы** задает режим проверки на наличие вирусов для всех типов файлов, что может понадобиться только в исключительно редких случаях. При установке переключателя в положение **Программные файлы** поиск и обезвреживание вирусов будет производиться только в программных файлах. Для просмотра, дополнения или удаления расширений программных файлов, подлежащих проверке, предназначена кнопка **Выбор**.

Группа элементов настройки «Как реагировать» задает способ реакции на факт обнаружения вируса. В списке **При обнаружении вируса** могут быть определены следующие виды реакции:

- **Запросить** - пользователю будет выдан запрос для определения дальнейших действий;
- **Только известить** - пользователь будет только оповещен об обнаружении вируса без возможности восстановления или удаления инфицированного файла;
- **Сразу исправить** - при обнаружении инфицированного файла или загрузчика будет предпринята немедленная попытка их восстановления без запроса разрешения у пользователя; в конце процесса поиска и обезвреживания вирусов пользователь будет оповещен о всех выполненных транзитным сканером-ревизором действиях;
- **Сразу удалить** - инфицированные файлы по мере их обнаружения будут полностью удаляться (без возможности их дальнейшего восстановления);
- **Остановить компьютер** - при обнаружении вируса будет активизирована функция блокирования работы процессора и устройств

ввода-вывода до перезагрузки компьютера; этот вид реакции является наиболее эффективным для полного обезвреживания компьютерных вирусов путем использования средств восстановления после перезагрузки компьютера с системной дискеты.

Если выбран вид реакции «**Запросить**», то в группе флажков «Кнопки в окне запроса» можно определить кнопки, которые появятся в окне запроса при обнаружении вируса:

- **Исправить** - восстановление обнаруженного инфицированного файла или загрузчика;
- **Удалить** - удаление обнаруженного инфицированного файла без возможности его дальнейшего восстановления;
- **Продолжить** - позволяет продолжить без принятия мер; эта кнопка появляется только в том случае, если установлен флажок **Немедленное извещение** в диалоговом окне «Расширенные установки поиска» (□□), открываемом кнопкой **Расширенные** в нижней части листа свойств **Поиск**;
- **Исключить** - вносит спецификацию инфицированного файла в список файлов, исключенных из процесса проверки на наличие вирусов; этот флажок следует устанавливать только в том случае, если имеются незараженные исполняемые файлы с последовательностями команд, характерными для вирусов.

С помощью кнопки **Расширенные** в нижней части листа свойств **Поиск** устанавливаются дополнительные параметры (см. □□) по поиску и обезвреживанию компьютерных вирусов:

- группа флажков «Расширенные установки»:
  - ⇒ **Искать на сетевых дисках** - будут проверяться не только локальные жесткие диски, но и диски, подключенные через сеть (проверки сетевых дисков могут занимать достаточно много времени);

⇒**Поиск может быть прерван** - в диалоговом окне выполнения поиска устанавливается кнопка **Прервать**, дающая возможность остановки процесса поиска;

⇒**Немедленное извещение** - обеспечивает немедленное отображение окна сигнализации при обнаружении вирусов, что дает возможность сразу же вмешаться без ожидания окончания поиска;

♦ группа флажков «Выбирать при запуске»:

⇒**Все гибкие диски** - для автоматического выбора всех гибких дисков после запуска транзитного сканера-ревизора;

⇒**Все жесткие диски** - для автоматического выбора всех жестких дисков после запуска транзитного сканера-ревизора;

⇒**Все сетевые диски** - для автоматического выбора всех сетевых дисков после запуска транзитного сканера-ревизора (выбор сетевых устройств для исправления или удаления инфицированных файлов зависит от полномочий пользователя в сети); при установке данного флажка должен быть также установлен флажок **Искать на сетевых дисках**.

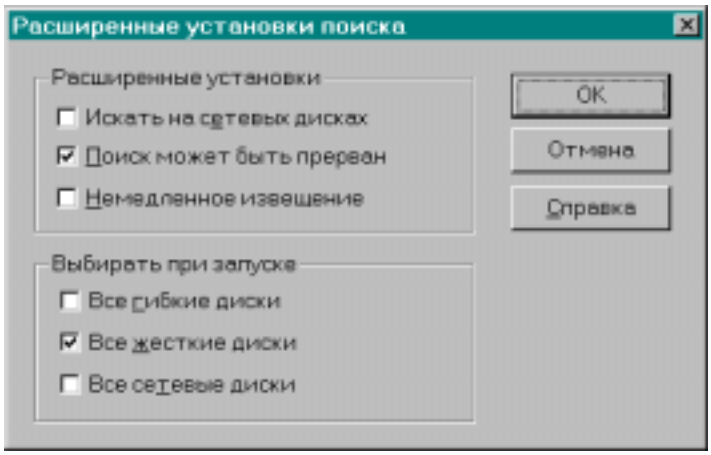


**Рис. 3.16. Диалоговое окно «Расширенные установки поиска»**

## Лист свойств «Общие»

Лист свойств «Общие» (□) позволяет настроить параметры поиска и обезвреживания компьютерных вирусов, общие для следующих программных компонентов:

- транзитного сканера-ревизора Norton AntiVirus (файл NAVW32.EXE) и резидентной программы «Автозащита» (файлы NAVAPW32.EXE, NAVAP.VXD и NAVEX.VXD), предназначенных для 32-разрядного режима работы Windows 95;
- транзитного сканера-ревизора NAVBOOT.EXE, предназначенного для режима MS-DOS.

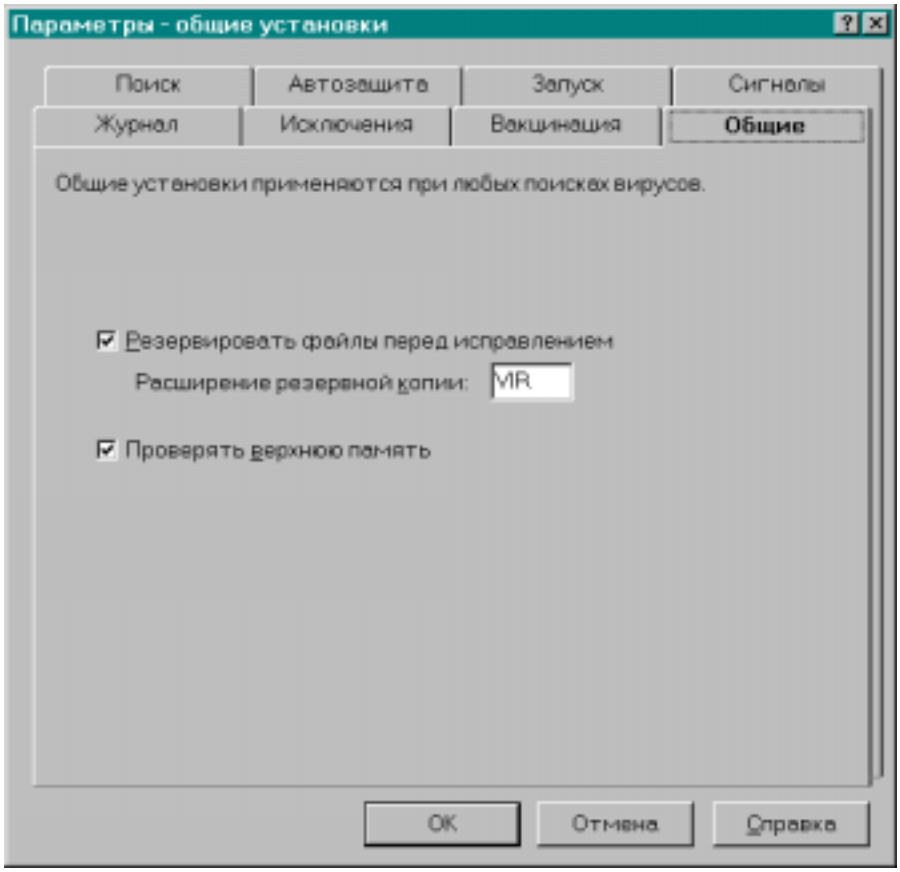


**Рис. 3.17. Лист свойств «Общие»**

Флажок **Резервировать файлы перед исправлением** задает режим работы, при котором перед исправлением зараженного файла дела-

ется его резервная копия. В текстовом поле **Расширение резервной копии** вводится нужное расширение. При просмотре списка файлов с помощью программы **Проводник** файлы резервных копий инфицированных программ, созданные компонентами пакета Norton AntiVirus, помечаются как «файлы, зараженные вирусом».

Если установлен флажок **Проверять верхнюю память**, то при проверке оперативной памяти будут также проверяться верхние участки памяти MS-DOS (UMA и HMA), которые в обычном режиме для ускорения проверки не анализируются.

## Лист свойств «Исключения»

Лист свойств «Исключения» (□□) дает возможность отредактировать или дополнить список спецификаций отдельных файлов и групп файлов, каждый из которых исключается из процесса контроля, вид которого задается с помощью этого же листа свойств. Под видом контроля при этом понимается тип действия транзитного или резидентного антивирусного компонента Norton AntiVirus, направленного на поиск и обнаружение вирусов, а также перехват попытки выполнения вирусоподобной функции. Виды контроля, которые исключены для файлов заданной спецификации, будем называть исключениями.

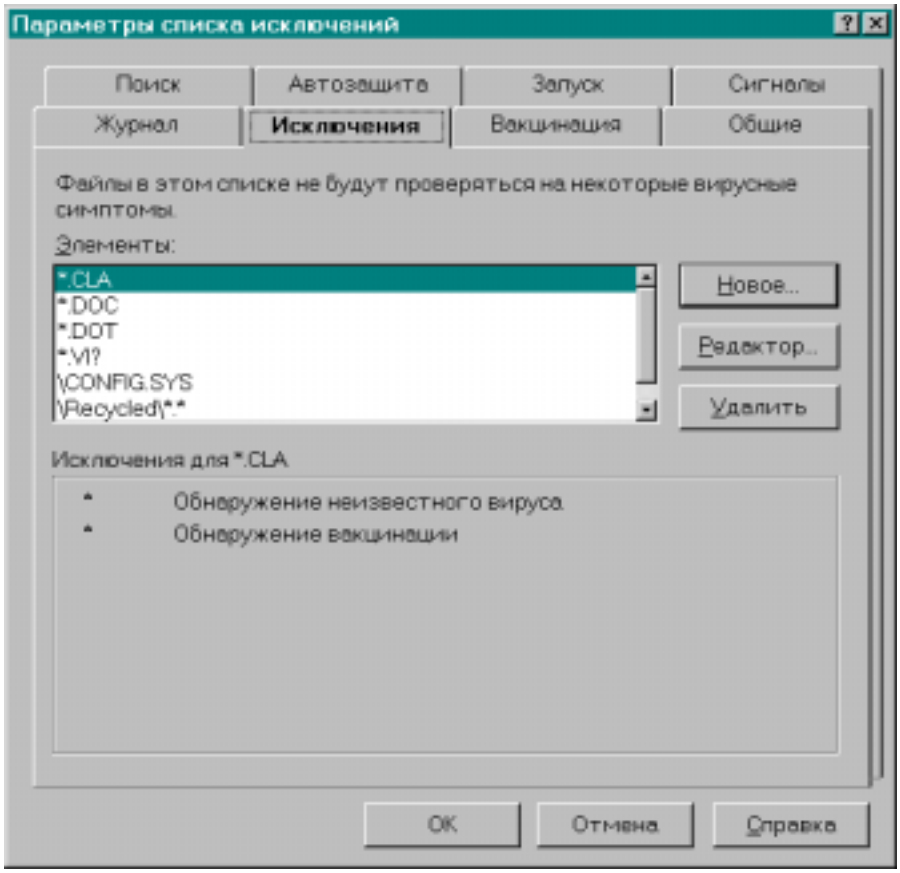


**Рис. 3.18. Лист свойств «Исключения»**

В списке «Элементы» перечисляются спецификации отдельных файлов или их групп. Исключения для текущего элемента списка отображаются в информационном поле **Исключения для #.#**, где **#.#** - спецификация файлов, задаваемая этим текущим элементом.

Для добавления спецификации файлов к списку и задания для них исключений необходимо нажать кнопку **Новое...** В результате появится диалоговое окно, представленное на □□.

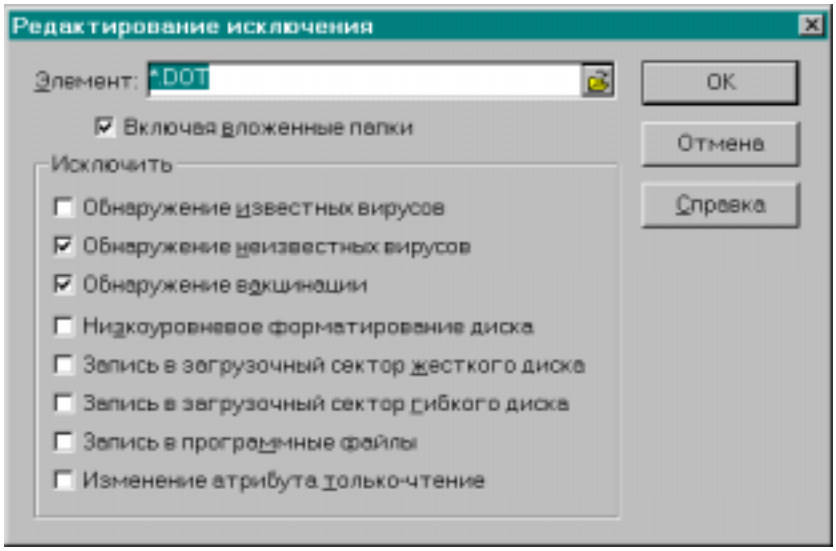


**Рис. 3.19. Диалоговое окно «Редактирование исключения»**

В текстовом поле **Элемент** необходимо ввести спецификацию группы файлов, используя символы шаблона («*» и «?»), или спецификацию отдельного файла. Для выбора каталога можно воспользоваться раскрывающимся списком, обозначенным в виде раскрытой папки. Установка флажка **Включая вложенные папки** задает режим учета исключений не только для указанных файлов каталога введенной спецификации, но и для файлов с заданным именем и расширением, находящихся во всех подкаталогах.

В группе флажков «Исключить» задаются исключения для файлов введенной спецификации:

- **Обнаружение известных вирусов** - файлы, соответствующие введенной спецификации, исключаются из процесса проверки на наличие известных вирусов (на наличие кодовых последовательностей, характерных для известных вирусов);
- **Обнаружение неизвестных вирусов** - файлы, соответствующие введенной спецификации, исключаются из процесса проверки на наличие неизвестных вирусов (на наличие кодовых последовательностей, характерных для большинства вирусов);

- **Обнаружение вакцинации** - файлы заданной спецификации исключаются из процесса проверки на наличие или изменение эталонных характеристик;
- **Низкоуровневое форматирование диска** - при выполнении программы из файла заданной спецификации не будет осуществляться перехват попытки низкоуровневого форматирования жесткого диска; данный флажок задает режим работы только программы «Автозащита»;
- **Запись в загрузочный сектор жесткого диска** - при выполнении программы из файла заданной спецификации не будет осуществляться перехват попытки записи в загрузочный сектор жесткого диска (такой режим целесообразно задать для утилиты FDISK.EXE); данный флажок влияет на параметры работы только программы «Автозащита»;
- **Запись в загрузочный сектор гибкого диска** - при выполнении программы из файла заданной спецификации не будет осуществляться перехват попытки записи в загрузочный сектор гибкого диска (такой режим целесообразно задать для утилиты FORMAT.EXE); данный флажок влияет на параметры работы только программы «Автозащита»;
- **Запись в программные файлы** - при выполнении программы из файла заданной спецификации не будет осуществляться перехват попытки записи в программные файлы (такой режим целесообразно задать только для программ, часто записывающих информацию в файлы своего размещения); данный флажок влияет на параметры работы только программы «Автозащита»;
- **Изменение атрибута только-чтение** - при выполнении программы из файла заданной спецификации не будет осуществляться перехват попытки изменения атрибута «только чтение» (такой ре-

жим целесообразно задать для файловых диспетчеров, например Norton Commander); данный флажок влияет на параметры работы только программы «Автозащита».

После задания всех требуемых исключений для файлов введенной спецификации следует нажать кнопку **Ok**.

Если в списке **Элементы** листа свойств «Исключения» необходимо отредактировать исключения для файлов какой-либо спецификации или изменить саму спецификацию, то следует воспользоваться кнопкой **Редактор...** В результате появляется то же окно, что и после нажатия кнопки **Новое...** (□□), особенности работы с которым остаются без изменений.

При необходимости отмены исключений для заданных файлов следует удалить спецификации этих файлов из списка **Элементы**. Чтобы удалить какую-либо спецификацию из списка **Элементы**, необходимо ее выделить и нажать кнопку **Удалить**.

## Лист свойств «Сигналы»

С помощью листа свойств «Сигналы» (□□) задается способ оповещения пользователя об обнаружении компьютерного вируса.

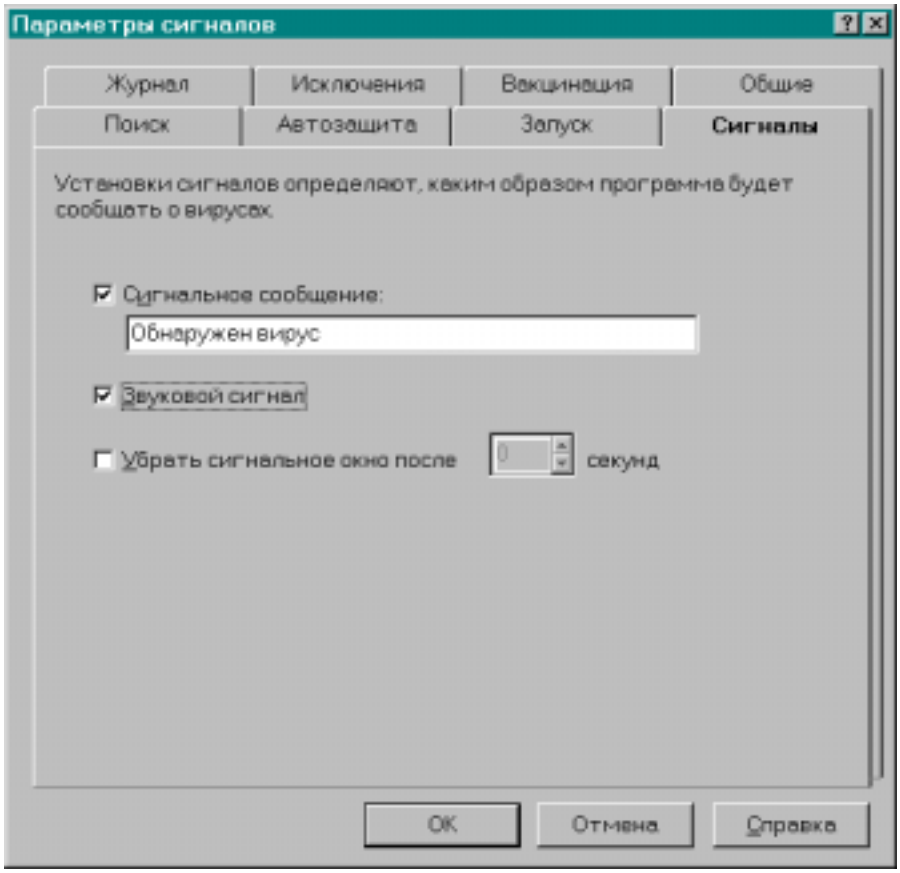


**Рис. 3.20. Лист свойств «Сигналы»**

При установке флажка **Сигнальное сообщение** в нижерасположенном текстовом поле можно задать специальные сообщения или инструкции, которые будут появляться при обнаружении вируса.

Установленный флажок **Звуковой сигнал** задает режим звукового оповещения об обнаружении вируса.

При установке флажка **Убрать сигнальное окно после** можно определить время, в течение которого диалоговое окно, сообщающее об обнаружении вируса остается на экране. Время вводится в текстовое поле секунд.

## Лист свойств «Вакцинация»

Лист свойств «Вакцинация» (□□) позволяет настроить основные параметры по формированию эталонных характеристик программ, проверке на соответствие этим характеристикам и реагированию на обнаружение несоответствий.

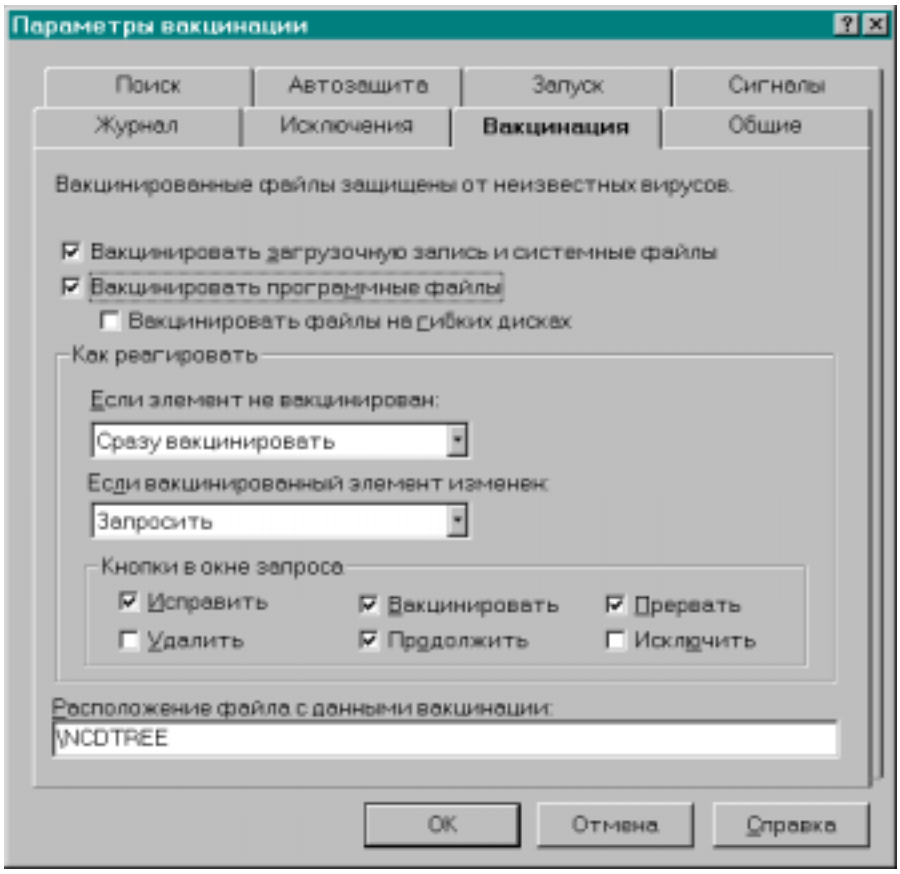


**Рис. 3.21. Лист свойств «Вакцинация»**

Первые два флажка задают режим создания эталонных характеристик для загрузочных записей, системных и программных файлов жестких дисков. При установке флажка **Вакцинировать файлы на гибких дисках** эталонные характеристики будут создаваться и для программных файлов на гибких дисках, вставленных в дисководы.

Группа элементов настройки «Как реагировать» определяют способ реакции на обнаружение отсутствия у программ эталонных характеристик, а также несоответствия текущих характеристик эталонным.

Список **Если элемент не вакцинирован** определяет вид реакции на обнаружение отсутствия у какой-либо программы (загрузчика или программного файла) эталонных характеристик:

- **Запросить** - пользователю будет выдан запрос для определения дальнейших действий;
- **Сразу вакцинировать** - для программы с отсутствующими эталонными характеристиками эти характеристики будут сформированы после поиска и обезвреживания в ней известных вирусов;
- **Известить - не вакцинировать** - пользователь будет только оповещен об обнаружении отсутствия эталонных характеристик;
- **Запретить доступ** - запуск программного файла, для которого обнаружено отсутствие эталонных характеристик, будет запрещен; данный режим устанавливается только для программы «Автозащита».

Список **Если вакцинированный элемент изменен** определяет вид реакции на обнаружение несоответствия текущих характеристик программы ее эталонным:

- **Запросить** - пользователю будет выдан запрос для определения дальнейших действий;
- **Известить - не ревакцинировать** - пользователь будет только оповещен об обнаружении несоответствия;
- **Запретить доступ** - запуск программного файла, для которого обнаружено несоответствие его реальных характеристик эталонным, будет запрещен; данный режим устанавливается только для программы «Автозащита».

Если в списке «Если элемент не вакцинирован» или в списке «Если вакцинированный элемент изменен» выбран вид реакции «**Запросить**», то в группе флажков «Кнопки в окне запроса» можно определить кнопки, которые появятся в окне запроса при обнаружении отсутствия эталонных характеристик или несоответствия реальных характеристик эталонным:

- **Исправить** - восстановление программного файла или загрузчика, для которого обнаружено несоответствие эталонным характеристикам; при невозможности восстановления будет выдано соответствующее сообщение;
- **Удалить** - удаление программного файла, для которого обнаружено несоответствие эталонным характеристикам;
- **Вакцинировать** - создание или обновление эталонных характеристик;
- **Продолжить** - позволяет продолжить текущую операцию (поиск или обращение к файлу) без принятия каких-либо мер;
- **Прервать** - позволяет остановить текущую операцию (поиск или обращение к файлу) без принятия каких-либо мер;
- **Исключить** - вносит спецификацию файла, для которого обнаружено несоответствие эталонным характеристикам или их отсутствие, в список файлов, исключенных из процесса проверки на наличие эталонных характеристик и соответствие этим характеристикам.

В текстовом поле **Расположение файла с данными вакцинации** вводится путь к каталогу, в котором будут формироваться эталонные характеристики. При отсутствии в этом пути имени логического привода, указанный каталог будет формироваться на каждом диске, для программ которого задан режим формирования эталонных характеристик. В этом случае в каждый каталог для формирования эталонных характеристик будут заноситься только характеристики программ соответствующего диска.

## Лист свойств «Журнал»

С помощью листа свойств «Журнал» (□□) задаются параметры регистрации всех действий, связанных с поиском и обезвреживанием вирусов, а также перехватом выполнения вирусоподобных функций.

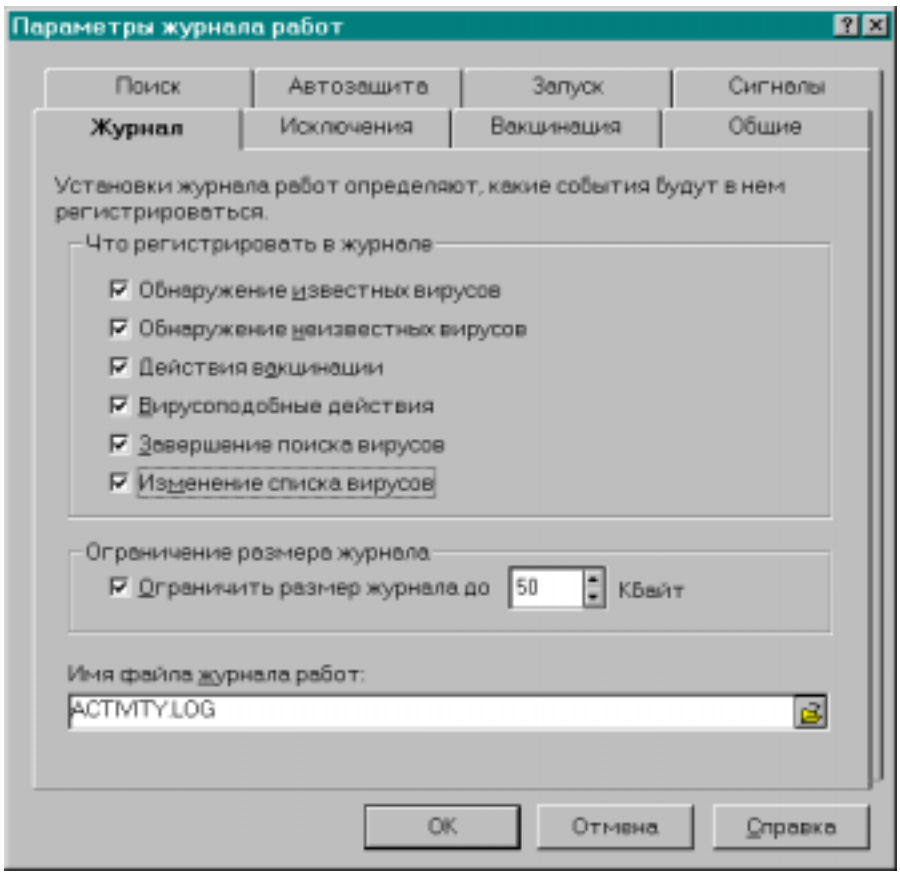


**Рис. 3.22. Лист свойств «Журнал»**

Группа флажков «Что регистрировать в журнале» определяет виды учетных записей, заносимых в журнал:

- **Обнаружение известных вирусов** - задает формирование учетных записей об обнаружении известных вирусов;
- **Обнаружение неизвестных вирусов** - задает формирование учетных записей об обнаружении неизвестных вирусов;

- **Действия вакцинации** - в журнал регистрации будут помещаться записи об обнаружении отсутствия эталонных характеристик и несоответствия текущих характеристик эталонным;
- **Вирусоподобные действия** - в журнал будут помещаться учетные записи о всех попытках вирусоподобных действий, перехваченных программой «Автозащита»;
- **Завершение поиска вирусов** - задает формирование учетных записей о завершении процесса поиска и обезвреживания вирусов с помощью транзитного сканера-ревизора;
- **Изменение списка вирусов** - будут формироваться учетные записи о модификации базы вирусных сигнатур.

Флажок **Ограничить размер журнала до** задает ограничение на размер файла журнала регистрации. Величину ограничения в килобайтах следует ввести в текстовое поле справа от флажка. По достижении указанного предела каждая новая запись журнала регистрации вытесняет самую старую.

В текстовом поле **Имя файла журнала работ** указывается спецификация файла журнала регистрации. Если введено только имя и расширение файла, то данный файл будет сформирован в каталоге размещения пакета Norton AntiVirus.

После настройки всех требуемых параметров работы транзитного сканера-ревизора в окне «Параметры ...» следует нажать кнопку **Ok**. При этом осуществляется автоматическое запоминание установленных параметров до их следующего изменения.

## Активизация процесса поиска и обезвреживания вирусов, а также формирования эталонных характеристик

Для активизации процесса поиска и обезвреживания вирусов, а также формирования эталонных характеристик для дисков целиком необходимо выполнить следующие действия:

1) в списке флажков «Диски» главного окна транзитного сканера-ревизора Norton AntiVirus (см. □□) указать диски, подлежащие обработке; для выбора всех жестких или всех гибких дисков предназначены соответствующие флажки группы элементов управления **Типы дисков**;
2) нажать кнопку **Поиск** или ввести команду **Поиск/ Диски**.

Если не будет выбрано ни одного диска, то по умолчанию будет обработан диск **C:**.

С целью активизации процесса поиска и обезвреживания вирусов, а также формирования эталонных характеристик по отношению к отдельному каталогу или файлу предназначены соответственно команды **Поиск/ Папки...** и **Поиск/ Файлы...** После ввода любой из этих команд необходимо будет указать каталог или файл, подлежащий проверке.

Создание (удаление) эталонных характеристик отдельного программного файла или программных файлов, входящих в заданные каталоги, выполняется с помощью команды **Средства/ Вакцинация**. В результате ввода данной команды появится диалоговое, представленное на □□.

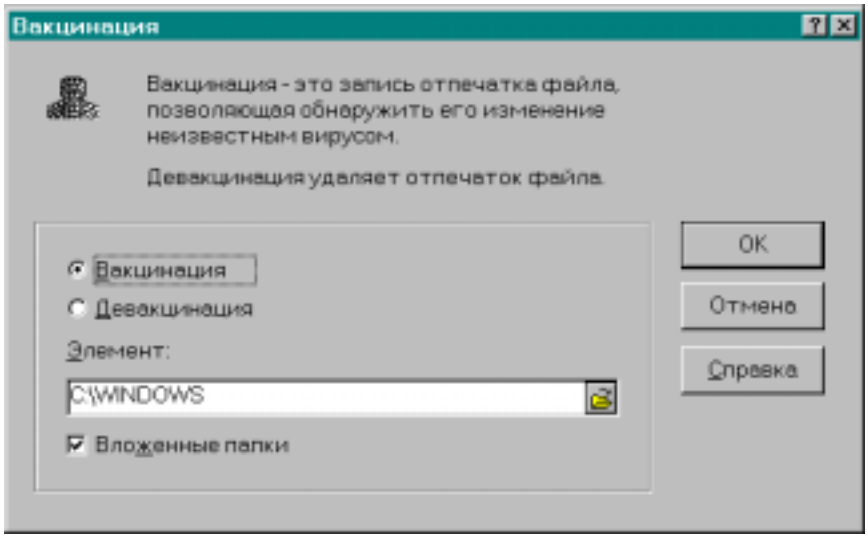


**Рис. 3.23. Диалоговое окно «Вакцинация»**

Для создания эталонных характеристик следует установить переключатель данного окна в положение **Вакцинация**, а для удаления - в положение **Девакцинация**. Далее необходимо в текстовое поле **Элемент** ввести спецификацию каталога или отдельного программного файла. При указании спецификации каталога будут обработаны все его программные файлы. Для выбора отдельного файла можно воспользоваться раскрывающимся списком выбора, обозначенным значком открытой папки. Активизация процесса создания или удаления эталонных характеристик выполняется нажатием кнопки **OK**.

## Работа с журналом регистрации

Настройка параметров регистрации выполняется с помощью рассмотренного выше листа свойств «Журнал» (см. □□). Для просмотра или распечатки журнала регистрации предназначена кнопка **Журнал** или команда **Средства/ Журнал работ** в главном окне транзитного сканера-ревизора Norton AntiVirus (см. □□). После активизации любого из этих элементов управления появляется окно журнала работ (□□).

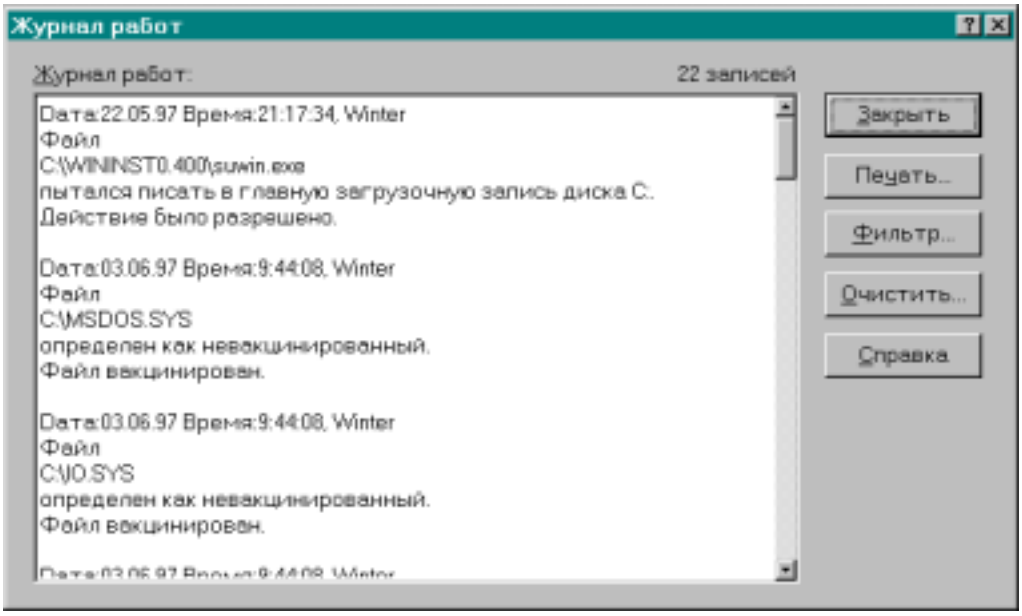


**Рис. 3.24. Диалоговое окно «Журнал работ»**

Каждая запись журнала включает:

- дату и время регистрации;
- идентификатор пользователя, работающего на компьютере;
- описание причины формирования учетной записи.

Для отбора записей из журнала регистрации по заданному признаку предназначена кнопка **Фильтр**, после нажатия которой появляется окно настройки параметров фильтрации (□□).

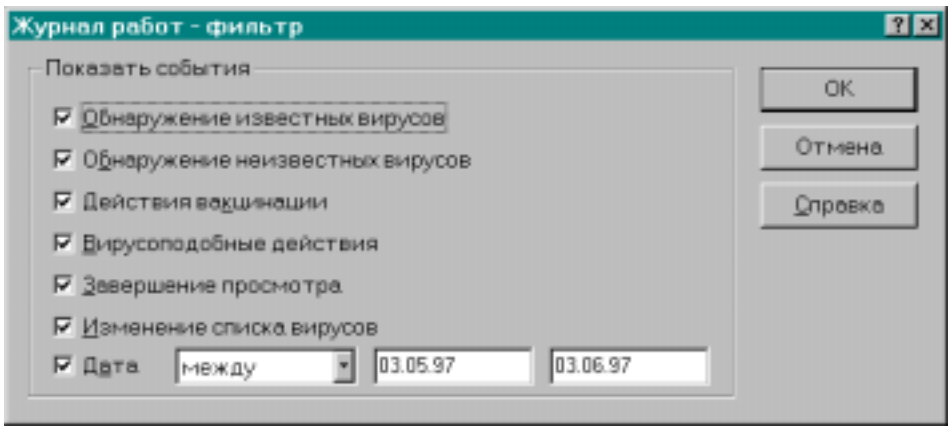


**Рис. 3.25. Диалоговое окно настройки параметров фильтрации**

В данном окне следует установить флажки с названиями требуемых учетных записей и нажать кнопку **OK**. В результате окно журнала работ будет отображать только записи указанных типов. В диалоговом окне настройки параметров фильтрации можно также, установив флажок **Дата**, указать период, для которого необходим просмотр учетных записей.

С помощью кнопки **Печать** диалогового окна «Журнал работ» можно распечатать отфильтрованные записи журнала регистрации.

Кнопка **Очистить** позволяет удалить все записи журнала регистрации.

## Просмотр и обновление сведений о вирусах

Сведения о вирусах Norton AntiVirus хранит в базе вирусных сигнатур и базе общего описания вирусов.

База вирусных сигнатур содержит вирусные сигнатуры, используемые для поиска и обезвреживания известных вирусов. Данная база размещается в файле VIRSCAN.DAT каталога расположения пакета Norton AntiVirus. В этом же каталоге находится файл VIRSCAN.INF с базой общего описания вирусов, используемой для выдачи информации о известных вирусах пользователю.

Для просмотра общих сведений о вирусах предназначена кнопка **Вирусы** или команда **Средства/ Список вирусов** в главном окне транзитного сканера-ревизора Norton AntiVirus (см. □□). После активизации любого из данных элементов управления появляется окно «Список вирусов» (□□).

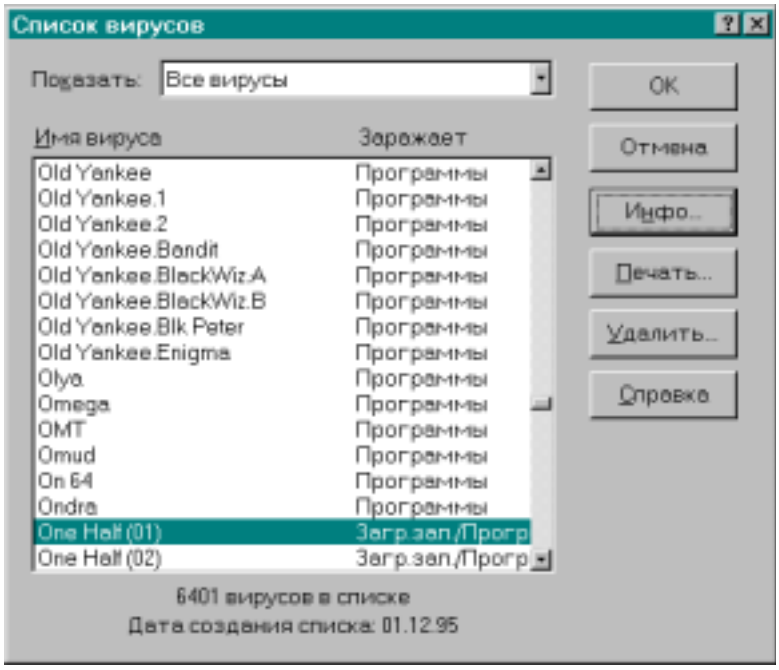


**Рис. 3.26. Диалоговое окно «Список вирусов»**

В раскрывающемся списке **Показать** можно указать тип вирусов, список которых требуется просмотреть.

Для получения более детальной информации о каком-либо вирусе из списка следует выделить имя этого вируса и нажать кнопку **Инфо...** В результате появится информационное окно с описанием выбранного вируса (□), позволяющее перейти к описанию предыдущего или следующего вируса в списке, а также распечатать отображаемую информацию.

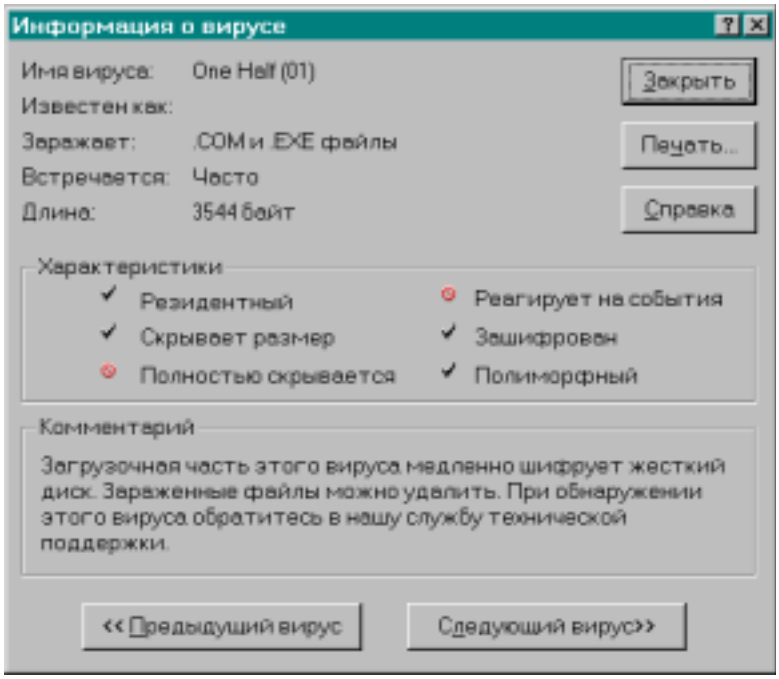


**Рис. 3.27. Окно «Информация о вирусе»**

База вирусных сигнатур используется только для поиска и обезвреживания известных вирусов. Эту базу данных следует как можно чаще обновлять, что повысит эффективность антивирусной защиты. Для обновления файла базы вирусных сигнатур необходимо получить пакет файлов обновления в сети Internet по адресу: http://sos.symantec.com/ftp/navftp.html. К этой WEB-странице, кроме непосредственного обращения, можно получить доступ, обратившись к WEB-серверу фирмы Symantec по адресу: http://www.symantec.com. В пакет файлов обновления входят следующие файлы:

APDATE.TXT - текстовый файл, содержащий общее описание процедуры обновления;

NAV950B.EXE - программа обновления до последней версии Norton AntiVirus для Windows 95;

05NAV97A.EXE - программа обновления базы вирусных сигнатур и общего описания вирусов.

Обновление базы вирусных сигнатур и общего описания вирусов следует выполнять только после обновления пакета Norton AntiVirus до его последней версии, так как отдельные компоненты пакета предыдущих версий не ориентированы на работу с обновленной базой вирусных сигнатур.

### *3.2.2. Планирование и автоматизация транзитных проверок*

Для эффективного поддержания антивирусной безопасности необходимо с помощью транзитных антивирусных средств обеспечить проверку всех программ, поступающих в компьютерную систему извне. Кроме этого, для усиления защиты требуется обязательно предусмотреть следующие мероприятия:

**1)** поиск и обезвреживание вирусов при загрузке компьютера в оперативной памяти и во всех программах, участвующих в загрузке;

**2)** периодический (например, еженедельный) поиск и обезвреживание вирусов во всех программах, хранящихся на винчестере.

#### Поиск и обезвреживание вирусов в процессе загрузки компьютера

Для решения задачи поиска и обезвреживание вирусов в процессе загрузки операционной системы следует разрешить при инсталляции пакета Norton AntiVirus вставку в начало файла Autoexec.bat последовательности строк:

```
KEYB RU,,C:\WINDOWS\COMMAND\KEYBRD3.SYS
@C:\PROGRA~1\NORTON~3\NAVBOOT.EXE /STARTUP
```

Первая команда настраивает клавиатуру на русский алфавит. Вторая вызывает транзитный сканер-ревизор NAVBOOT.EXE для поиска и обезвреживания вирусов в режиме MS-DOS перед загрузкой графической среды Windows 95. Ключ /STARTUP задает пакетный режим работы про-

граммы и режим использования параметров, установленных в листе свойств «Запуск» общих параметров настройки Norton AntiVirus.

Для настройки параметров в листе свойств «Запуск» следует в графической среде Windows 95 запустить транзитный сканер-ревизор NAVW32.EXE, выполнив команду **Norton AntiVirus** в меню **Пуск/ Программы/ Norton AntiVirus**, и далее в появившемся окне (см. □□) нажать кнопку **Параметры** или выполнить команду основного меню **Средства/ Параметры**. После отображения на экране окна параметров настройки необходимо щелчком мыши по соответствующему корешку активизировать лист свойств «Запуск» (□□).

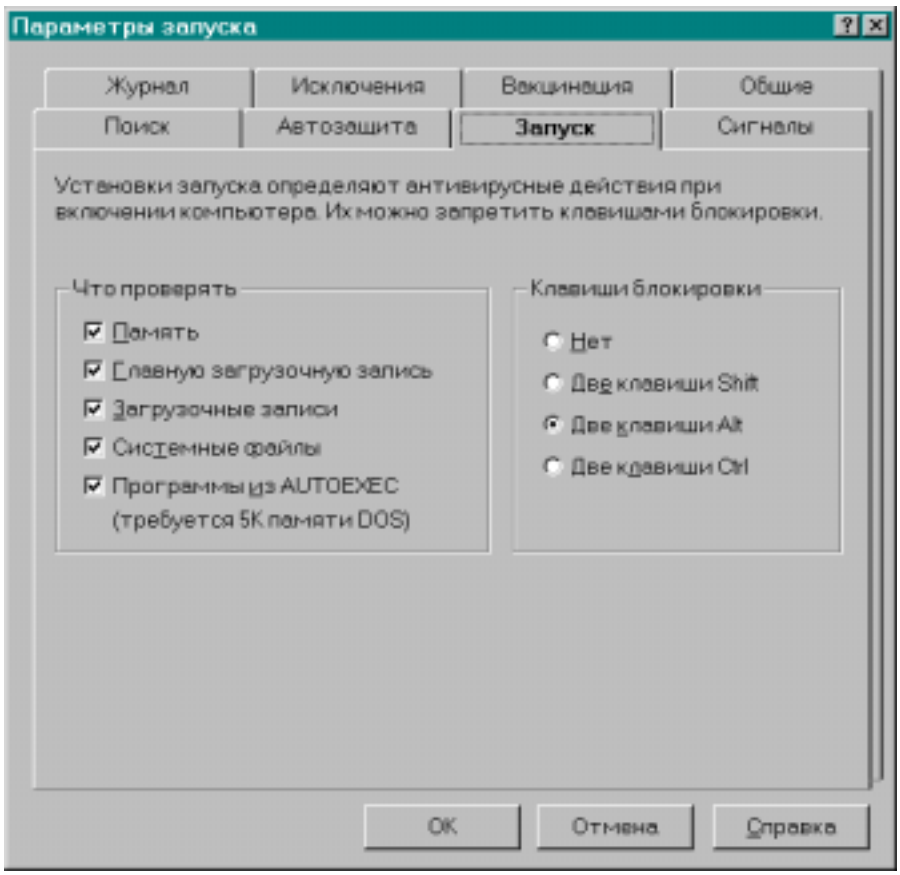


**Рис. 3.28. Лист свойств «Запуск»**

С помощью группы флажков «Что проверять» определяются объекты, в которых осуществляется поиск и обезвреживание вирусов в процес-

се загрузки операционной системы. Переключатель «Клавиши блокировки» позволяет задать комбинацию клавиш для остановки процесса проверки.

После установки требуемых параметров следует нажать кнопку **OK**. Заданные параметры вступят в силу при следующей загрузке операционной системы.

Если при инсталляции Norton Antivirus вызов программы NAVBOOT.EXE в файл AUTOEXEC.BAT вставлен не был, то этот вызов следует вставить самостоятельно, не забыв добавить в командную строку ключ /STARTUP.

Для того, чтобы при загрузке компьютера в процессе поиска и обезвреживания вирусов можно было понять выводимые на экран сообщения программы NAVBOOT.EXE, следует в файле AUTOEXEC.BAT переместить в начало файла команды, обеспечивающие подготовку и активизацию кодовой страницы кириллицы для MS-DOS. Такими командами являются следующие:

```
MODE CON CODEPAGE PREPARE=((866)C:\WINDOWS\COMMAND\EGA3.CPI)
MODE CON CODEPAGE SELECT=866
```

Эти команды помещаются в файл AUTOEXEC.BAT при инсталляции локализованной версии Windows 95.

## Периодический поиск и обезвреживание вирусов во всех программах, хранящихся на винчестере

При отсутствии повышенной степени опасности заражения вирусами, когда новые программы на винчестер поступают не слишком часто, достаточно еженедельного поиска и обезвреживания вирусов на винчестере. В противном случае это мероприятие следует проводить несколько раз в неделю или ежедневно.

Простейшим способом периодического поиска и обезвреживания вирусов на винчестере являются самостоятельные запуски транзитного сканера-ревизора Norton AntiVirus после его соответствующей настройки.

Периодические запуски транзитного сканера-ревизора можно автоматизировать с помощью резидентной программы Norton Program Scheduler (файл NSCHED32.EXE), входящей в пакет Norton AntiVirus и предназначенной для планирования и автоматизации транзитных проверок.

Программа Norton Program Scheduler, находясь резидентно в оперативной памяти, обеспечивает автоматический запуск любых программ в соответствии с определенным для нее планом событий.

В процессе инсталляции пакета Norton AntiVirus, для запуска планировщика Norton Program Scheduler при каждой загрузке операционной системы, его ярлык, если не было отмены пользователем, вставляется в папку **Автозагрузка** меню **Пуск/Программы**. При необходимости самостоятельной вставки ярлыка планировщика в папку **Автозагрузка** необходимо выполнить следующие действия:

1) запустить **Проводник** с помощью пункта меню **Пуск/Программы/Проводник** и далее открыть папку **Главное меню/ Программы/ Norton AntiVirus** в каталоге размещения Windows 95;
2) щелкнув правой кнопкой мыши на ярлыке **Norton Program Scheduler** и выбрав соответствующий пункт меню, скопировать этот ярлык в буфер обмена;
3) открыть папку **Главное меню/ Программы/ Автозагрузка** в каталоге размещения Windows 95 и, выбрав соответствующую команду в контекстном меню после щелчка правой кнопкой мыши в свободной части окна содержимого папки, вставить ярлык **Norton Program Scheduler** в папку **Автозагрузка**.

После следующей загрузки операционной системы в результате выполнения перечисленных действий планировщик **Norton Program Scheduler** будет запускаться автоматически. При активном состоянии планировщика в правой части панели задач будет расположена его пиктограмма  .

Вставка ярлыка планировщика в папку **Автозагрузка** может быть выполнена и автоматически при настройке параметров функционирования **Norton Program Scheduler**, что будет рассмотрено ниже.

Для дополнения, просмотра и редактирования плана событий **Norton Program Scheduler**, а также настройки параметров его функционирования следует открыть главное окно планировщика (□□) одним из следующих способов:

1) выполнить двойной щелчок левой кнопкой мыши по пиктограмме планировщика на панели задач;
2) выполнить щелчок правой кнопкой мыши по пиктограмме планировщика на панели задач и выбрать щелчком в появившемся контекстном меню команду **Восстановить**;
3) выполнить команду **Пуск/ Программы/ Norton AntiVirus/ Norton Program Scheduler**.

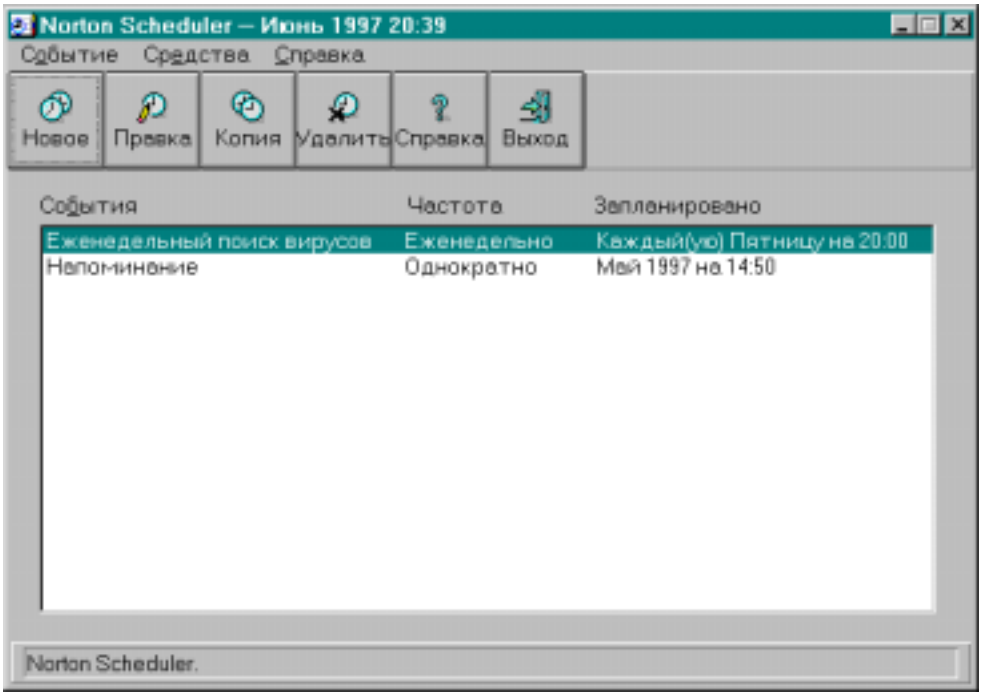


**Рис. 3.29. Главное окно Norton Program Scheduler**

Основную часть главного окна **Norton Program Scheduler** занимает поле со списком событий, для каждого из которых указывается его название, частота выполнения, а также дата и время наступления. На □□ весь план состоит только из двух событий - события по еженедельному запуску транзитного сканера-ревизора Norton AntiVirus и однократного события-сообщения.

Добавление нового события к плану событий выполняется с помощью кнопки **Новое** или команды **Событие/ Добавить**. В результате реализации любого из перечисленных способов появляется диалоговое окно, представленное на □□.

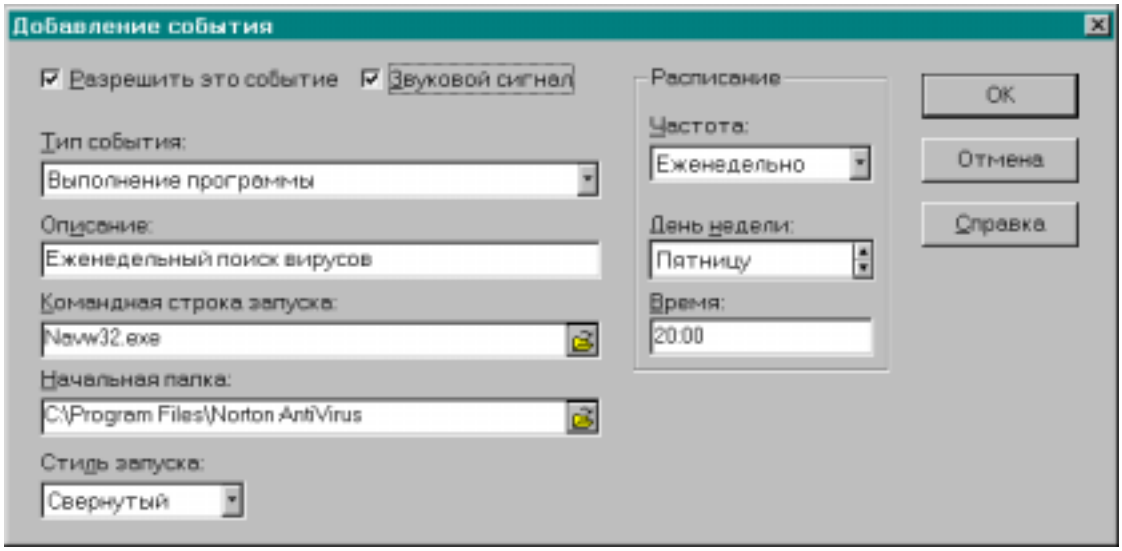


**Рис. 3.30. Добавление события по запуску программы**

Флажок **Разрешить это событие** устанавливает режим, при котором данное событие учитывается планировщиком. В противном случае событие только добавляется в список событий, отображаемых в главном окне планировщика. Этот флажок удобно использовать для событий, действие которых временно необходимо прекратить.

При установленном флажке **Звуковой сигнал** планировщик будет выдавать звуковой сигнал в начале выполнения запланированного события.

В раскрывающемся списке **Тип события** указывается вид добавляемого события:

**Выполнение программы** - для планирования запуска какой-либо программы;

**Вывод сообщения** - для планирования вывода сообщения пользователю, например, напоминания о необходимости выполнить какое-либо действие;

**Поиск вирусов** - для планирования запуска транзитного сканера-ревизора Norton AntiVirus.

В текстовом поле **Описание** необходимо ввести название, под которым событие будет внесено в список.

Если в качестве типа события выбран **Выполнение программы** (□□), то в поле **Командная строка запуска** следует ввести командную строку для планируемого запуска программы. Спецификацию программы можно выбрать с помощью раскрывающегося списка, обозначенного раскрытой папкой. Поле **Начальная папка** служит для указания каталога, в который необходимо перейти перед запуском запланированной программы. В списке **Стиль запуска** следует выбрать способ запуска (**Нормальный**, **Свернутый** или **Развернутый**), задающего требуемые размеры главного окна запускаемой программы.

Если в качестве типа события выбрана строка **Вывод сообщения** (□□), то текстовое поле **Выводимое сообщение** необходимо будет ввести текст сообщения.

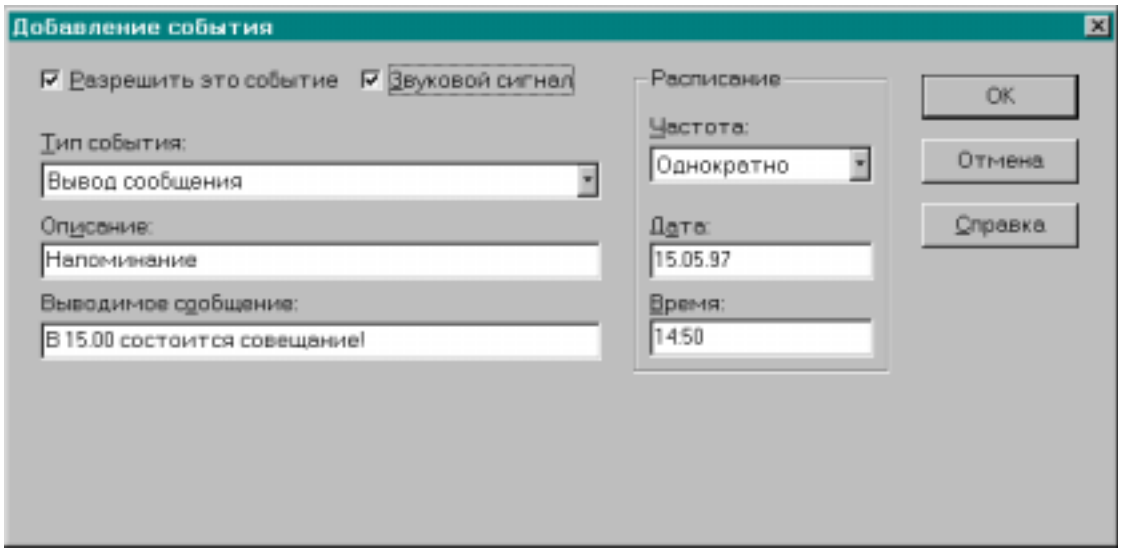


**Рис. 3.31. Добавление события-сообщения**

Если же в качестве события выбран **Поиск вирусов** (□□), то в текстовом поле **Где искать** следует через пробелы указать имена логиче-

ских дисков для поиска вирусов. Наряду с именами логических дисков могут быть указаны и спецификации каталогов для поиска.

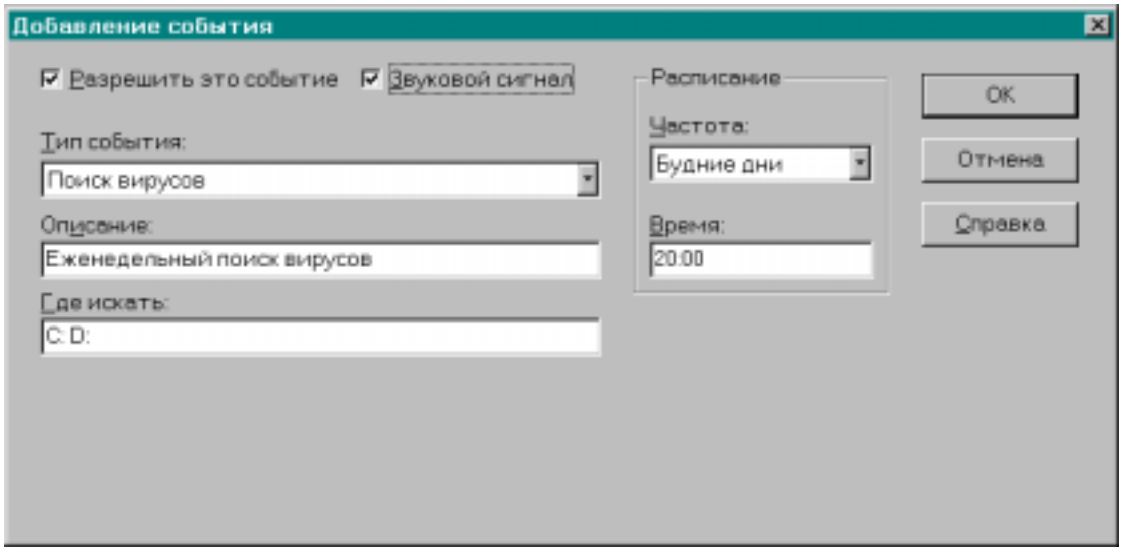


**Рис. 3.32. Добавление события по периодическому запуску транзитного сканера-ревизора Norton AntiVirus**

Независимо от типа добавляемого события, в группе параметров настройки «Расписание» необходимо указать частоту, а также время наступления события. В списке **Частота** можно выбрать следующие параметры: **Однократно**, **Ежечасно**, **Ежедневно**, **Будние дни**, **Еженедельно**, **Ежемесячно**, **Ежегодно**. Параметры настройки, находящиеся между раскрывающимся списком **Частота** и текстовым полем **Время** зависят от выбранной частоты наступления события и если они присутствуют, то определяют день или дату повторяющегося периода, когда планируемое событие должно произойти.

При добавлении события по периодическому запуску транзитного сканера-ревизора Norton AntiVirus в качестве типа события можно указать как **Выполнение программы** (см. □□), так и **Поиск вирусов** (см. □□). В процессе инсталляции пакета Norton AntiVirus в план Norton Program Scheduler включается событие, описание которого представлено на □□.

При наступлении этого события транзитным сканером-ревизором будут проверены все жесткие диски компьютера.

После установки параметров добавляемого события в диалоговом окне «Добавление события» следует нажать кнопку **OK**, в результате чего появится окно запроса подтверждения действий пользователя (□□), в котором следует нажать эту же кнопку. Если в данном окне установить имеющийся флажок, то в дальнейшем это окно при занесении события в план появляться не будет.

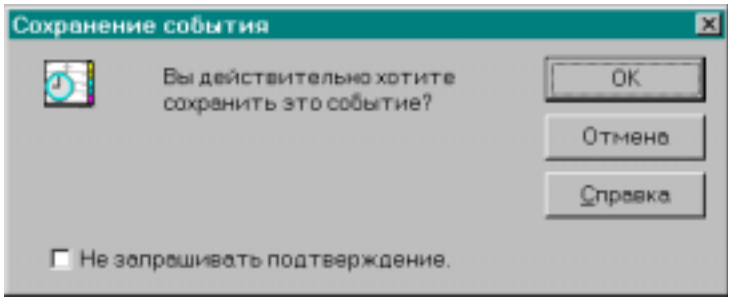


**Рис. 3.33. Диалоговое окно «Сохранение события»**

При необходимости модификации параметров события в списке событий необходимо выделить соответствующую запись события щелчком, и далее нажать кнопку **Правка** или выполнить команду **Событие/ Редактор**. В результате появится диалоговое окно «Редактирование события», аналогичное окну «Добавление события» и соответствующее типу редактируемого события (см. □□, □□ и □□). Особенности работы здесь те же, что и при добавлении нового события. Вызвать окно редактирования события можно также двойным щелчком по записи соответствующего события в списке.

Для создания события, дублирующего существующее (например, с целью его незначительной модификации) следует выделить соответствующую запись и нажать копку **Копия**. Функцию, эквивалентную данной кнопке, выполняет также команда **Событие/ Копировать**.

Кнопка **Удалить** и эквивалентная ей команда **Событие/ Удалить** позволяют удалить ненужное событие, выделенное в списке.

С помощью кнопки **Справка** или одноименного с ней пункта меню можно получить доступ к справочной информации по командам планировщика.

Для настройки параметров планировщика предназначена команда **Средства/ Параметры**. После выдачи данной команды отображается диалоговое окно с листами параметров настройки (□□).

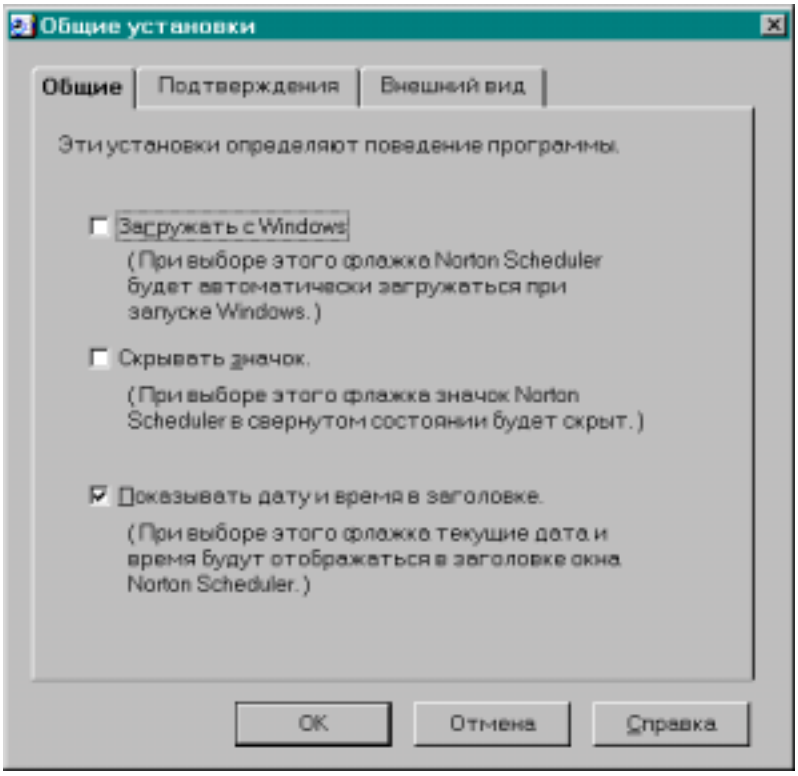


**Рис. 3.34. Лист свойств «Общие»**

Лист свойств «Общие» позволяет задать режим автоматического запуска планировщика при загрузке операционной системы, а также дополнительные настроечные параметры, описанные в окне настройки (□□). При установке флажка **Загружать с Windows** после нажатия кнопки **OK** по окончании настройки всех параметров в папку **Главное меню/**

**Программы/ Автозагрузка** каталога размещения Windows 95 будет включен ярлык Norton Program Scheduler, что обеспечит автозапуск планировщика при загрузке Windows 95.

Лист свойств «Подтверждения» (□□) включает параметры, позволяющие задать требуемые окна запроса подтверждения действий пользователя.

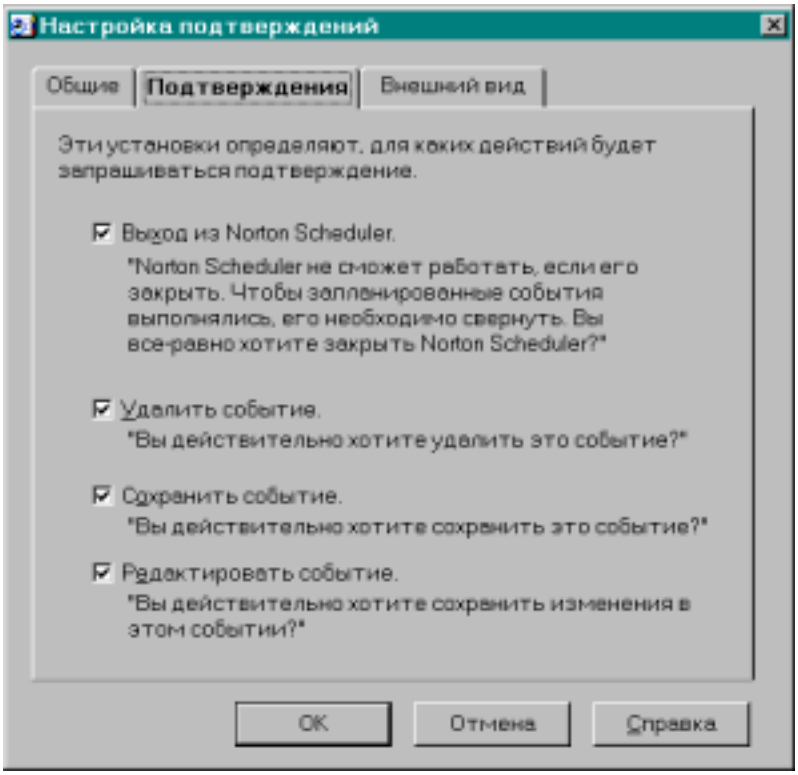


**Рис. 3.35. Лист свойств «Подтверждения»**

С помощью листа свойств «Внешний вид» (□□) определяются параметры настройки внешнего вида главного окна планировщика.

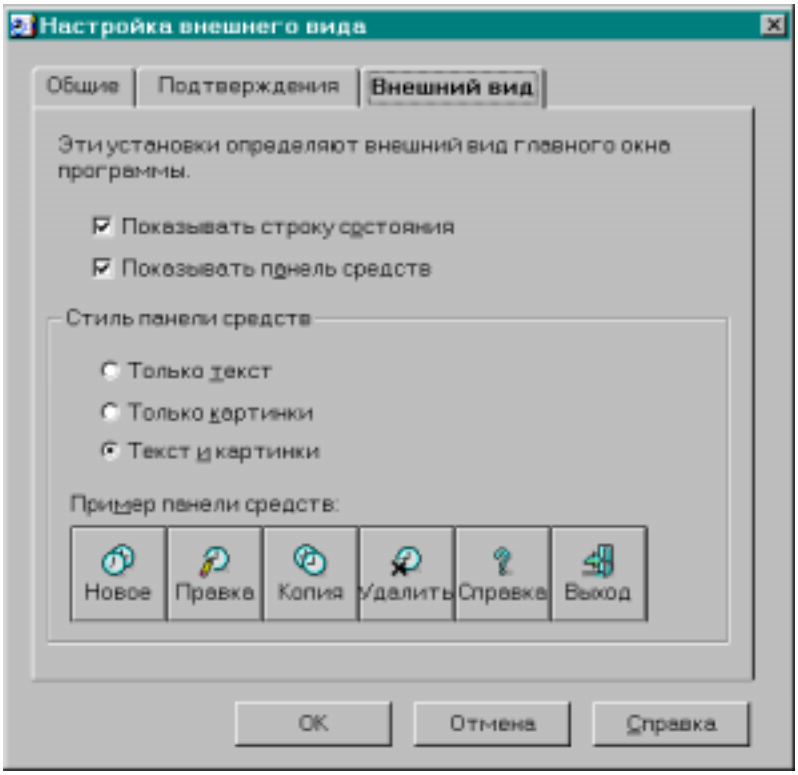


**Рис. 3.36. Лист свойств «Внешний вид»**

Установив требуемые параметры работы Norton Program Scheduler необходимо нажать кнопку **OK**.

После окончания работы с главным окном планировщика (см. □□) при необходимости оставления планировщика резидентным в оперативной памяти следует это окно свернуть.

Для завершения работы Norton Program Scheduler в текущем сеансе работы можно воспользоваться одним из следующих способов:

- если было открыто главное окно Norton Program Scheduler, то закрыть его, нажав кнопку **Выход** или выполнив команду **Событие/ Выход**, и далее в случае появления окна запроса нажать кнопку **Выход**;
- выполнить щелчок правой кнопкой мыши по пиктограмме планировщика на панели задач, выбрать щелчком в появившемся кон-

текстном меню команду **Закрыть**, и далее при появлении окна запроса нажать кнопку **Выход**.

Для того, чтобы планировщик не запускался и при следующих загрузках операционной системы, необходимо с помощью программы **Проводник** или любого другого диспетчера файлов удалить из папки **Главное меню/ Программы/ Автозагрузка** в каталоге размещения Windows 95 ярлык **Norton Program Scheduler**. Аналогичного результата можно добиться, если, не завершая работу планировщика в текущем сеансе, сбросить флажок **Загружать с Windows** в листе свойств «Общие» окна параметров настройки, появляющегося по команде **Средства/ Параметры** главного меню **Norton Program Scheduler**.

Периодический запуск транзитного сканера-ревизора Norton AntiVirus можно организовать не только с помощью **Norton Program Scheduler**, но и с помощью любого другого резидентного планировщика, способного планировать и запуск программ, например, с помощью **Norton Commander Scheduler**, входящего в пакет программ **Norton Commander** для Windows 95. В этом случае в командной строке для планируемого запуска NAVW32.EXE необходимо в качестве параметров указать через пробелы имена дисков, подлежащих проверке, например:

C:\Program Files\Norton AntiVirus\NAVW32.EXE C: D:

Наряду с именами логических дисков могут быть указаны и спецификации каталогов. Не следует забыть задать с помощью соответствующих параметров настройки свернутый режим запуска и в качестве рабочего каталога папку размещения пакета Norton AntiVirus.

### *3.2.3. Резидентная защита от компьютерных вирусов*

В пакете Norton AntiVirus для резидентной защиты от компьютерных вирусов предназначена программа «Автозащита», объединяющая в себе функции фильтра, а также резидентных сканера и ревизора. Работу дан-

ной резидентной программы обеспечивают исполняемый файл NAVAPW32.EXE, а также виртуальные драйверы устройств NAVAP.VXD и NAVEX.VXD.

При инсталляции Norton AntiVirus для запуска программы «Автозащита» в процессе загрузки операционной системы вызов виртуальных драйверов этой программы добавляется в системный реестр Windows 95. Если же данное действие при инсталляции было отменено пользователем, то для запуска программы «Автозащита» необходимо выполнить следующие действия:

**1)** запустить на выполнение транзитный сканер-ревизор Norton AntiVirus путем выполнения одноименной команды в меню **Пуск/ Программы/ Norton AntiVirus** или путем запуска на выполнение файла NAVW32.EXE в каталоге антивирусного пакета;

**2)** вызвать окно настройки параметров функционирования компонентов антивирусного пакета с помощью кнопки **Параметры** или команды **Средства/ Параметры**;

**3)** в листе свойств «Автозащита» (□□) установить флажок **Загружать Автозащиту при запуске** и нажать кнопку **OK**;

**4)** в появившемся окне запроса на подтверждение действий пользователя (□) нажать кнопку **OK**;

**5)** закрыть окно транзитного сканера-ревизора Norton AntiVirus.

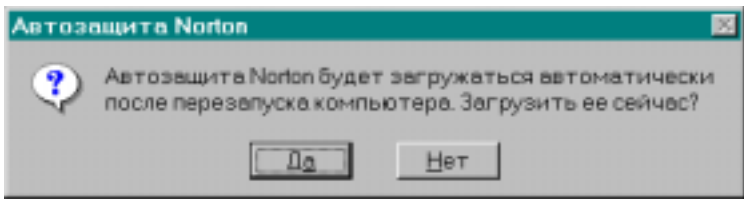


**Рис. 3.37. Окно запроса**

В активном состоянии программы «Автозащита» в левой части панели задач отображается пиктограмма этой программы .

Для настройки параметров резидентной защиты от компьютерных вирусов предназначен лист свойств «Автозащита» (□□), вызвать который можно описанным выше способом или путем выполнения одного следующих:

**1)** щелкнуть по пиктограмме программы «Автозащита» правой кнопкой мыши и в появившемся диалоговом меню выбрать щелчком пункт **Параметры**;

**2)** дважды щелкнуть левой кнопкой мыши по пиктограмме программы «Автозащита» и далее нажать кнопку **Параметры**.

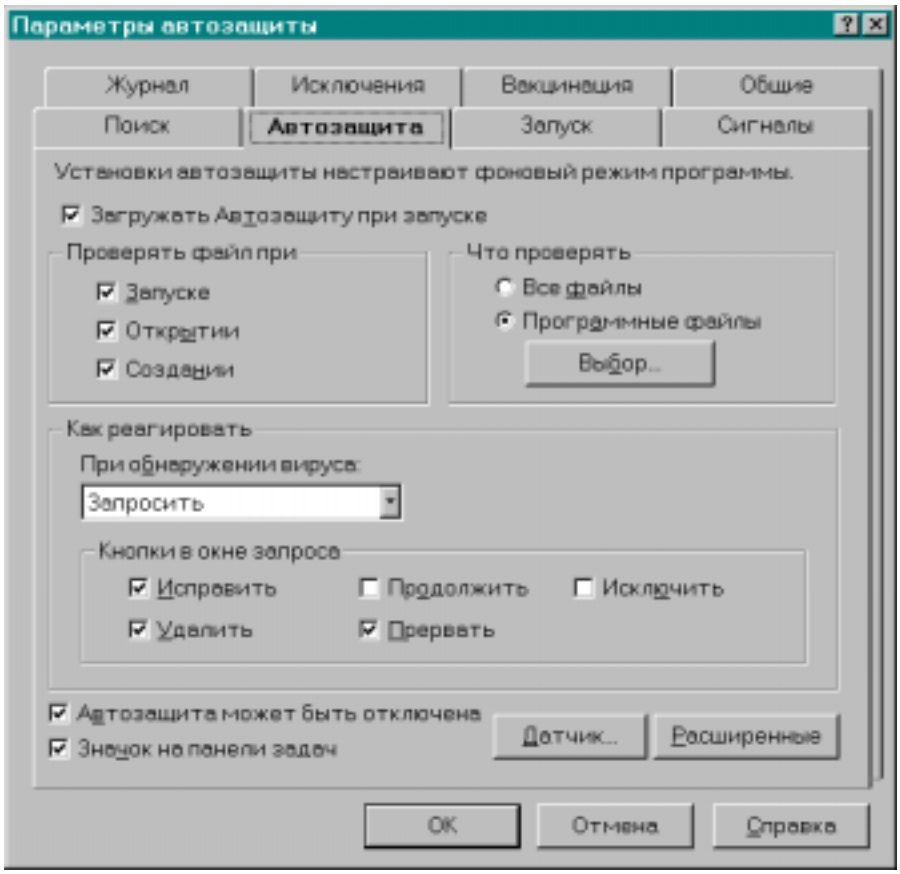


**Рис. 3.38. Лист свойств «Автозащита»**

Установка флажка **Загружать автозащиту при запуске** является единственным способом установки резидентной защиты от компьютерных вирусов с помощью пакета Norton AntiVirus и обеспечивает автоматиче-

ский запуск программы «Автозащита» при загрузке компьютера. Сброс данного флажка необходим только в случае, когда требуется выгрузить программу «Автозащита» из оперативной памяти и не нужно устанавливать резидентную защиту Norton AntiVirus при следующих загрузках операционной системы, например, для установки резидентной антивирусной защиты, реализуемой другим пакетом программ.

Группа флажков «Проверять файл при» предназначена для установки параметров, определяющих события, при наступлении которых программа «Автозащита» должна выполнять поиск и обезвреживание вирусов в файлах, связанных с этими событиями:

**При запуске** - проверка программных файлов при их запуске;

**При открытии** - проверка файлов при каждом открытии, например, при открытии для копирования;

**При создании -** проверка файлов при их создании на диске.

Динамический поиск вирусов в файлах выполняется путем проверки на наличие вирусных сигнатур и соответствие реальных характеристик файлов их эталонным. Если в листе свойств «Вакцинация» (□□) установлены флажки **Вакцинировать загрузочную запись и системные файла** и **Вакцинировать программные файлы**, а также при необходимости **Вакцинировать файлы на гибких дисках**, то при обнаружении программного файла с отсутствующими эталонными характеристиками, эти эталонные характеристики будут создаваться автоматически.

Группа параметров настройки «Что проверять» позволяет задать режим динамической проверки всех файлов (**Все файлы**) или только программных (**Программные файлы**). В случае выбора программных файлов есть возможность дополнения и редактирования списка расширений программных файлов, подлежащих динамическому контролю на наличие вирусов. Для этого предназначена кнопка **Выбор**. После нажатия данной кнопки появляется диалоговое окно, представленное на □□.

Кнопка **Новое** окна дополнения и редактирования расширений проверяемых программных файлов позволяет добавить новое расширение. Для удаления ненужного расширения из списка его следует выделить щелчком и нажать кнопку **Удалить**. С помощью кнопки **По умолчанию** можно восстановить тот список расширений, который был определен при инсталляции пакета Norton AntiVirus. По окончании работы с окном «Расширения программных файлов» для установки измененных параметров необходимо нажать кнопку **OK**.

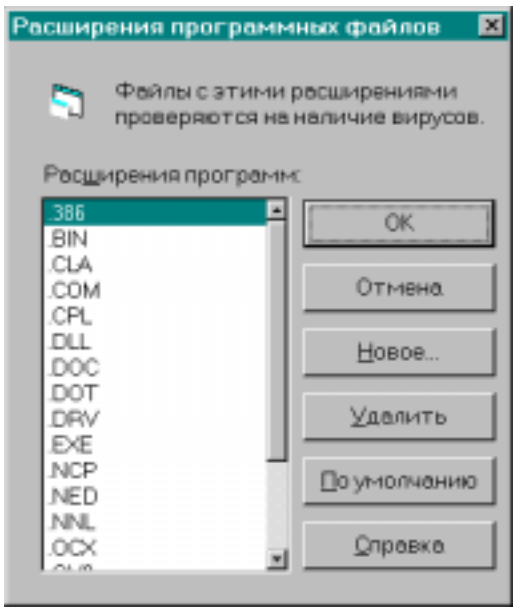


**Рис. 3.39. Диалоговое окно дополнения и редактирования расширений проверяемых программных файлов**

Группа элементов настройки «Как реагировать» задает способ реакции на факт обнаружения вируса. В списке **При обнаружении вируса** могут быть определены следующие виды реакции:

- **Запросить** - пользователю будет выдан запрос для определения дальнейших действий;
- **Запретить доступ** - при обнаружении инфицированной программы дальнейшая операция с файлом или загрузочным сектором, содержащим эту программу, будет запрещена;

- **Сразу исправить** - при обнаружении инфицированного файла или загрузчика будет предпринята немедленная попытка их восстановления без запроса разрешения у пользователя;
- **Сразу удалить** - при обнаружении инфицированного файла этот файл будет полностью удален (без возможности его дальнейшего восстановления);
- **Остановить компьютер** - при обнаружении вируса будет активизирована функция блокирования работы процессора и устройств ввода-вывода до перезагрузки компьютера; этот вид реакции является наиболее эффективным для полного обезвреживания компьютерных вирусов путем использования средств восстановления после перезагрузки компьютера с системной дискеты.

Если выбран вид реакции «**Запросить**», то в группе флажков «Кнопки в окне запроса» можно определить кнопки, которые появятся в окне запроса при обнаружении вируса:

- **Исправить** - восстановление обнаруженного инфицированного файла или загрузчика;
- **Удалить** - удаление обнаруженного инфицированного файла без возможности его дальнейшего восстановления;
- **Продолжить** - позволяет продолжить обращение к файлу или загрузчику без принятия мер; в этом случае появляется возможность активизации вируса;
- **Прервать** - позволяет прервать обращение к файлу или загрузчику, после чего вирус не активизируется, но файл или загрузчик остается инфицированным;
- **Исключить** - вносит спецификацию инфицированного файла в список файлов, исключенных из процесса проверки на наличие вирусов; этот флажок следует устанавливать только в том случае,

если имеются незараженные исполняемые файлы с последовательностями команд, характерными для вирусов.

Если установлен флажок **Автозащита может быть отключена**, то доступна функция временного блокирования резидентной защиты от компьютерных вирусов (см. ниже). В противном случае заблокировать работу программы «Автозащита» будет невозможно.

Флажок **Значок на панели задач** задает режим, когда при загруженной программе «Автозащита» на панели задач отображается ее пиктограмма  .

Кнопка **Датчик** вызывает окно параметров настройки (□□), позволяющее задать режим динамического поиска неизвестных вирусов. В этом режиме осуществляется динамический контроль на наличие кодовых последовательностей, характерных для большинства вирусов, что эффективно дополняет контроль на наличие конкретных вирусных сигнатур. Флажок **Использовать вирусный датчик** предназначен для включения режима контроля на наличие неизвестных вирусов. Настройка параметров **Когда найден неизвестный вирус** и **Кнопки в окне запроса** выполняется по аналогии с настройкой группы параметров «Как реагировать» листа свойств «Автозагрузка». После внесения всех установок следует нажать кнопку **OK**.

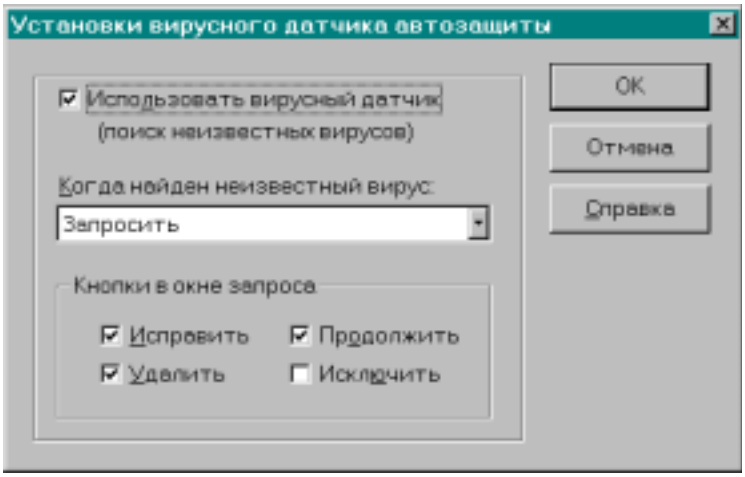


**Рис. 3.40. Окно параметров настройки режима поиска неизвестных вирусов**

Все рассмотренные в листе свойств «Автозащита» параметры настройки относились к параметрам выполнения функций, характерных для резидентных сканеров и ревизоров. Настройка функций, характерных для фильтра, выполняется с помощью кнопки **Расширенные**. После нажатия данной кнопки появляется окно параметров настройки, представленное на □□.

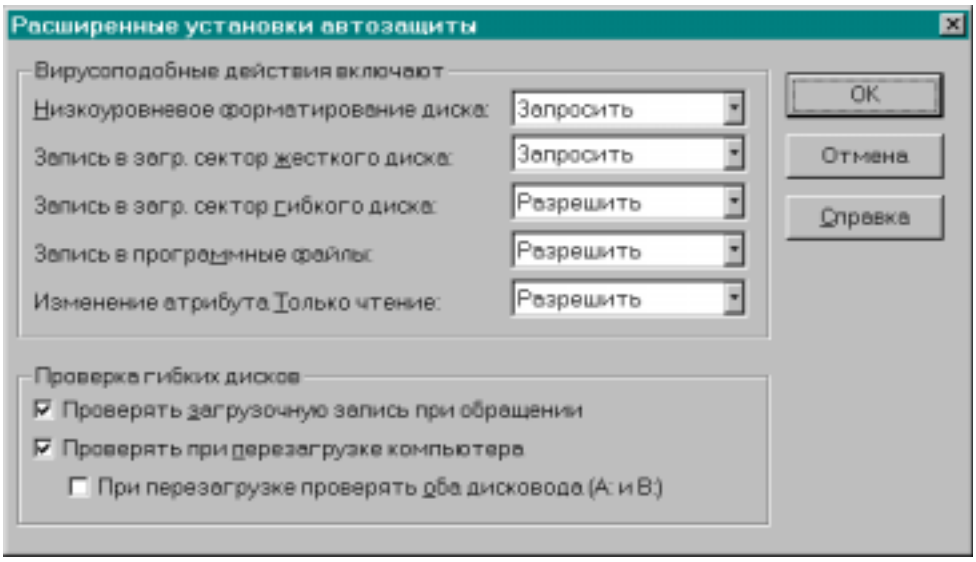


**Рис. 3.41. Диалоговое окно «Расширенные установки автозащиты»**

В группе параметров настройки «Вирусоподобные действия включают» следует указать виды реакции программы «Автозащита» на попытки выполнения функций, характерных для вирусов. При этом для каждой вирусоподобной функции может быть задан один из следующих видов реакции:

- **Запросить** - блокирование контролируемой функции при попытке ее выполнения и выдача запроса пользователю, ответом на который пользователь может:
  - ⇒ разрешить дальнейшее выполнение контролируемой функции;
  - ⇒ разрешить выполнение контролируемой функции и исключить ее из дальнейших проверок для выполняющейся программы, которая эту функцию активизировала;
  - ⇒ запретить дальнейшее выполнение контролируемой функции;
- **Запретить** - блокирование контролируемой функции при попытке ее выполнения без возможности разрешения дальнейшего выполнения;
- **Разрешить** - отсутствие контроля на выполнение вирусоподобного действия.

Наиболее гибким и в то же время безопасным видом реакции программы «Автозащита» является запрос пользователю для определения дальнейших действий.

В обычном режиме работы при отсутствии повышенной опасности заражения вирусами достаточно задать только две контролируемые функции - **Низкоуровневое форматирование диска** (имеется в виду винчестера) и **Запись в загрузочные сектора жесткого диска**.

Группа флажков **Проверка гибких дисков** определяет параметры, не относящиеся к параметрам работы антивирусного фильтра в класси-

ческом представлении. Эта группа позволяет задать параметры режима динамической проверки гибких дисков:

- **Проверять загрузочную запись при обращении** - включает режим проверки каждого гибкого диска, к которому происходит обращение, на наличие загрузочного вируса;
- **Проверять при перезагрузке компьютера** - включает режим проверки гибкого диска в дисководе A: на наличие загрузочного вируса при завершении сеанса работы с помощью команды **Пуск/Завершение работы/ Выключить компьютер**;
- **При перезагрузке проверять оба дисковода (A: и B:)** - включает режим проверки гибких дисков на наличие загрузочных вирусов в дисководах A: и B: при завершении сеанса работы с помощью команды **Пуск/Завершение работы/ Выключить компьютер**; данный флажок следует устанавливать только в случае наличия дисковода B: и при возможности загрузки с этого дисковода.

По завершении установки параметров в окне «Расширенные установки автозащиты» следует нажать кнопку **OK**.

Задать, отредактировать или дополнить список спецификаций отдельных файлов и групп файлов, каждый из которых исключается из отдельных видов динамического контроля, можно с помощью листа свойств «Исключения», который описан в п. 3.2.1.

После установки всех требуемых параметров резидентной защиты от компьютерных вирусов следует нажать кнопку **OK** и при необходимости ответить на появившиеся запросы.

Для кратковременного блокирования работы программы «Автозащита» следует выполнить щелчок правой кнопкой мыши по ее пиктограмме на панели задач и в появившемся контекстном меню щелчком выбрать пункт **Выключить**. В результате пиктограмма программы «Автозащита» примет вид  . Для возобновления резидентной защиты требуется также

выполнить щелчок правой кнопкой мыши по пиктограмме, но в появившемся меню выбрать щелчком команду **Включить**. Пиктограмма программы «Автозащита» примет исходный вид .

Для того, чтобы программу «Автозащита» полностью выгрузить из оперативной памяти и не запускать при следующих загрузках операционной системы необходимо в листе свойств «Автозащита» сбросить флажок **Загружать Автозащиту при запуске** и после нажатия кнопки **OK** ответить соответствующим образом на появившийся запрос (□□).

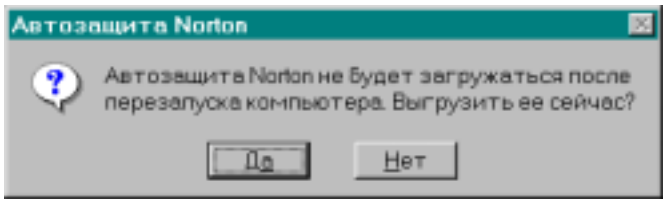


**Рис. 3.42. Окно запроса**

С помощью команды **Открыть** контекстного меню программы «Автозащита», вызываемом путем щелчка правой кнопкой мыши по ее пиктограмме на панели задач, можно открыть информационное окно «Автозащита Norton AntiVirus» (□□). Это окно открывается также при выполнении двойного щелчка левой кнопкой мыши по пиктограмме. Окно «Автозащита Norton AntiVirus» сообщает о текущей защищенности и позволяет осуществить доступ к окну параметров настройки резидентной защиты (□□), а также выполнить временное блокирование и отмену блокировки функций программы «Автозащита». Закрытие данного окна не приводит к отключению резидентной защиты от компьютерных вирусов.

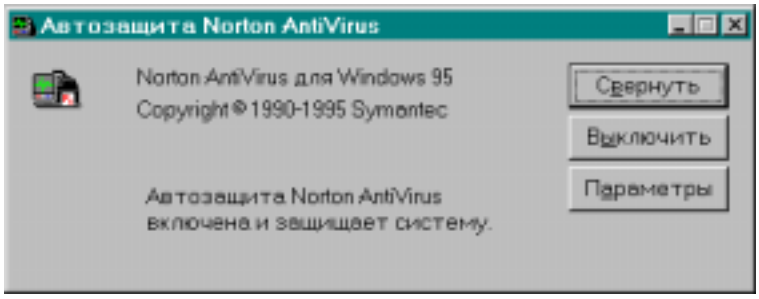


**Рис. 3.43. Информационное окно «Автозащита Norton AntiVirus»**

### *3.2.4. Подготовка и использование средств восстановления*

#### Стандартный набор восстановления Norton AntiVirus

Любой полнофункциональный пакет антивирусной защиты должен предоставлять пользователю средства автоматизированной подготовки набора дискет восстановления, обеспечивающих поиск и обезвреживание вирусов, а также устранение последствий их деструктивных действий в автономном режиме работы, не зависящем от содержимого жестких дисков компьютера. Такой автономный режим предполагает выполнение всех действий по восстановлению работоспособности компьютера только после его полной перезагрузки с системной дискеты и с помощью программ из набора восстанавливающих дискет.

Пакет программ Norton AntiVirus предоставляет пользователю возможность создания набора восстановления как в процессе инсталляции антивирусного пакета, так и в любой момент после ее проведения. Для подготовки набора восстанавливающих дискет предназначена транзитная программа «Аварийный диск» (NRESQ32.EXE).

Стандартный набор восстановления Norton AntiVirus включает две трехдюймовые дискеты по 1.44 Мбайта.

Первая дискета формируется как системная и на нее помещаются следующие компоненты:

- файлы из состава Windows 95, необходимые для загрузки базовой MS-DOS (IO.SYS, MSDOS.SYS, COMMAND.COM, DRVSPACE.BIN, AUTOEXEC.BAT, CONFIG.SYS, HIMEM.SYS, DISPLAY.SYS, COUNTRY.SYS, MODE.COM, EGA3.CPI, KEYB.COM, KEYBRD3.SYS);
- зарезервированные файлы автозапуска и конфигурирования (C:\AUTOEXEC.BAT и C:\CONFIG.SYS), имеющие соответственно спецификации AUTOEXEC.SAV и CONFIG.SAV;
- зарезервированное содержимое загрузочных записей жесткого диска (MBR, SMBR и BR), включая таблицу разделов, а также CMOS-памяти, хранящееся в файлах BOOTINFO.DAT, PARTINFO.DAT и CMOSINFO.DAT;
- программа Rescue (RESCUE.EXE и RESCUED.HLP), для восстановления нефайловых системных данных (содержимого MBR, SMBR и BR винчестера, включая таблицу разделов, а также CMOS-памяти) на основе файлов BOOTINFO.DAT, PARTINFO.DAT и CMOSINFO.DAT;
- утилиты для подготовки к работе жесткого диска FDISK.EXE, FORMAT.COM и SYS.COM, которые могут понадобиться в случае его разрушения.

На вторую дискету помещаются такие файлы как:

- файлы транзитного сканера-ревизора Navboot, предназначенного для режима MS-DOS: NAVBOOT.EXE, NAVBOOT.OVL, NAVBOOT.HLP;
- файлы базы данных о вирусах, предназначенные для транзитного сканера-ревизора Navboot и имеющие расширение .DAT;
- текстовый файл VIRSPEC.TXT, содержащий сведения о специфических вирусах;

- файл COMMAND.COM, необходимый для того, чтобы после загрузки с системной дискеты при запуске программы Navboot со второй дискеты набора восстановления не нужно было вставлять в дисковод системную дискету.

Для создания набора восстановления в процессе инсталляции пакета Norton AntiVirus необходимо лишь иметь в наличии две свободные дискеты и следовать инструкциям инсталлирующей программы.

Для создания набора восстановления в любой момент после инсталляции антивирусного пакета при наличии двух свободных дискет требуется запустить программу NRESQ32.EXE с помощью команды панели задач **Пуск/ Программы/ Norton AntiVirus/ Аварийный диск** или двойным щелчком по ее имени в среде любого диспетчера файлов. В результате появится окно запроса, представленное на □□.

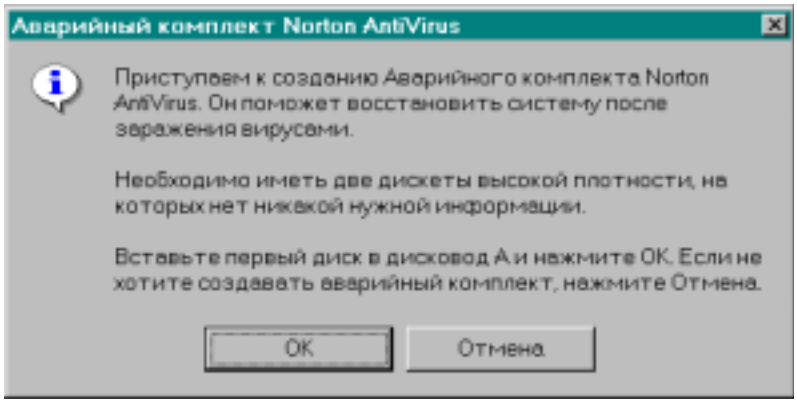


**Рис. 3.44. Окно запроса на создание первой дискеты набора восстановления**

После появления данного окна необходимо вставить первую дискету в дисковод и нажать кнопку **OK**.

Если на дискете, вставленной в дисковод, программа NRESQ32.EXE обнаружит какие-либо файлы, то перед ее форматированием будет выдано предупреждающее сообщение-запрос о том, что в процессе форматирования данные на дискете будут потеряны. Нажав

кнопку **Отмена** пользователь может отменить дальнейший процесс создания набора восстановления. При нажатии **OK** процесс создания набора восстановления будет продолжен.

После форматирования первой дискеты и копирования на нее требуемых файлов, пользователю будет выдан следующий запрос (□□).

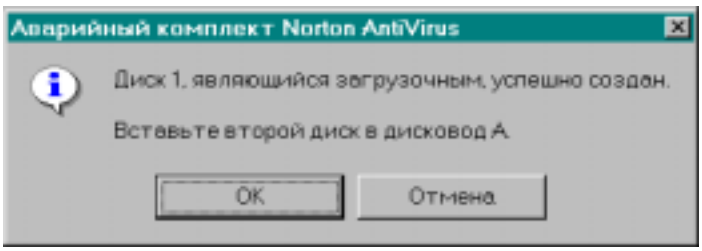


**Рис. 3.45. Окно запроса на создание второй дискеты набора восстановления**

Вставив вторую дискету в дисковод, следует нажать кнопку **OK**. Особенности создания второй дискеты те же, что и первой. После окончания формирования второй дискеты пользователю будет выдано итоговое сообщение (□□), внимательно прочитав которое, необходимо нажать **OK** и выполнить все указанные в нем действия.

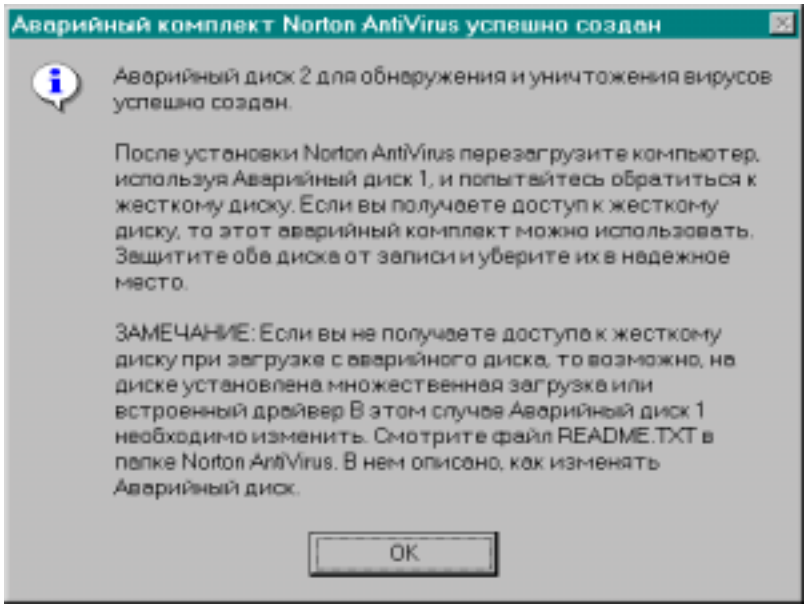


**Рис. 3.46. Итоговое сообщение по окончании создания второй дискеты набора восстановления**

Если по окончании создания набора восстановления при проверке видимости жесткого диска после загрузки с первой дискеты этого набора жесткий диск будет доступным, то обе восстанавливающие дискеты следует защитить от записи, открыв на каждой из них задвижку с окошка защиты от записи, подписать и убрать в надежное место.

Ввиду того, что некоторые производители жестких дисков используют специфичные технологии настройки и инициализации жестких дисков, то после загрузки с первой дискеты набора восстановления может оказаться, что жесткий диск будет невидим. В этом случае загрузочную дискету набора восстановления следует доработать.

При использовании дисковой системы OnTrack для доработки загрузочной дискеты необходимо выполнить следующие действия:

1) выбрать из меню **Пуск** панели задач пункт **Завершение работы** и выполнить **Перезапуск компьютера в режиме MS-DOS**;

2) после загрузки компьютера вставить в дисковод A: дискету с Ontrack Disk Manager;

3) набрать в командной строке команду **A:\DM** и нажать <Enter> для запуска программы Disk Manager;

4) выбрать в главном окне из меню **Select an Installation** пункт **Maintenance Menu/ Create Ontrack Boot Diskette**;

5) выбрать **Make this diskette an Ontrack Boot Diskette**;

6) вынуть из дисковода A: дискету Ontrack Disk Manager и вставить первый диск набора восстановления Norton AntiVirus;

7) нажать клавишу <Enter> для принятия ключей по умолчанию;

8) по завершении операции следует защитить сформированный загрузочный диск от записи и перезагрузить с него компьютер для проверки доступности жесткого диска.

При использовании дисковой системы со встроенным драйвером следует иметь в виду, что такие системы тесно привязаны к особенностям жесткого диска. Для доработки загрузочной дискеты в этом случае необходимо следовать инструкциям документации по жесткому диску. В некоторых случаях могут потребоваться консультации фирмы-изготовителя.

Если на компьютере были установлены вместе система Windows 95 и Windows NT с двойной загрузкой, то для доработки загрузочного диска набора восстановления необходимо загрузить Windows NT, вставить загрузочный диск в дисковод A: и ввести следующую команду DOS для переноса операционной системы на аварийный диск:

SYS A:

## Поиск и обезвреживание вирусов с помощью транзитного сканера-ревизора NAVBOOT

Наиболее правильным, хотя, и не самым удобным способом реакции на обнаружение вирусов является блокирование работы компьютера, его полная перезагрузка с системной дискеты из состава средств восста-

новления и далее поиск и обезвреживание вирусов с помощью транзитного антивирусного средства, запущенного с дискеты.

К необходимости полной перезагрузки с системной дискеты и использованию транзитного антивирусного средства из состава средств восстановления может привести и безвыходная ситуация, когда по причине деструктивных действий вирусов нарушена работоспособность компьютера и загрузка с винчестера стала невозможной.

Для установки режима блокировки компьютера (до его перезагрузки) при обнаружении вируса следует при настройке компонентов пакета Norton AntiVirus во всех параметрах задания способа реакции на обнаружение вируса (см. параметры «**При обнаружении вируса**» и «**Когда найден неизвестный вирус**» на □□, □□ и □□) определить значение «**Остановить компьютер**».

Для поиска и обезвреживания вирусов после загрузки компьютера с системной дискеты предназначен транзитный сканер-ревизор NAVBOOT.EXE, включаемый в состав средств восстановления программой «Аварийный диск» (NRESQ32.EXE). Данный транзитный сканер-ревизор специально разработан для режима MS-DOS и, кроме применения в экстренных ситуациях после загрузки с системной дискеты, используется также для поиска и обезвреживания вирусов в процессе обычной загрузки компьютера с винчестера (см. п. 3.2.2).

Для запуска транзитного сканера-ревизора NAVBOOT.EXE после загрузки компьютера с первой дискеты набора восстановления требуется выполнить следующую последовательность действий:

**1)** вставить в дисковод вторую дискету набора восстановления Norton AntiVirus;

**2)** набрать в командной строке команду **NAVBOOT**;

**3)** нажать клавишу <Enter>.

В результате на экране появится главное окно транзитного сканера-ревизора, представленное на □.

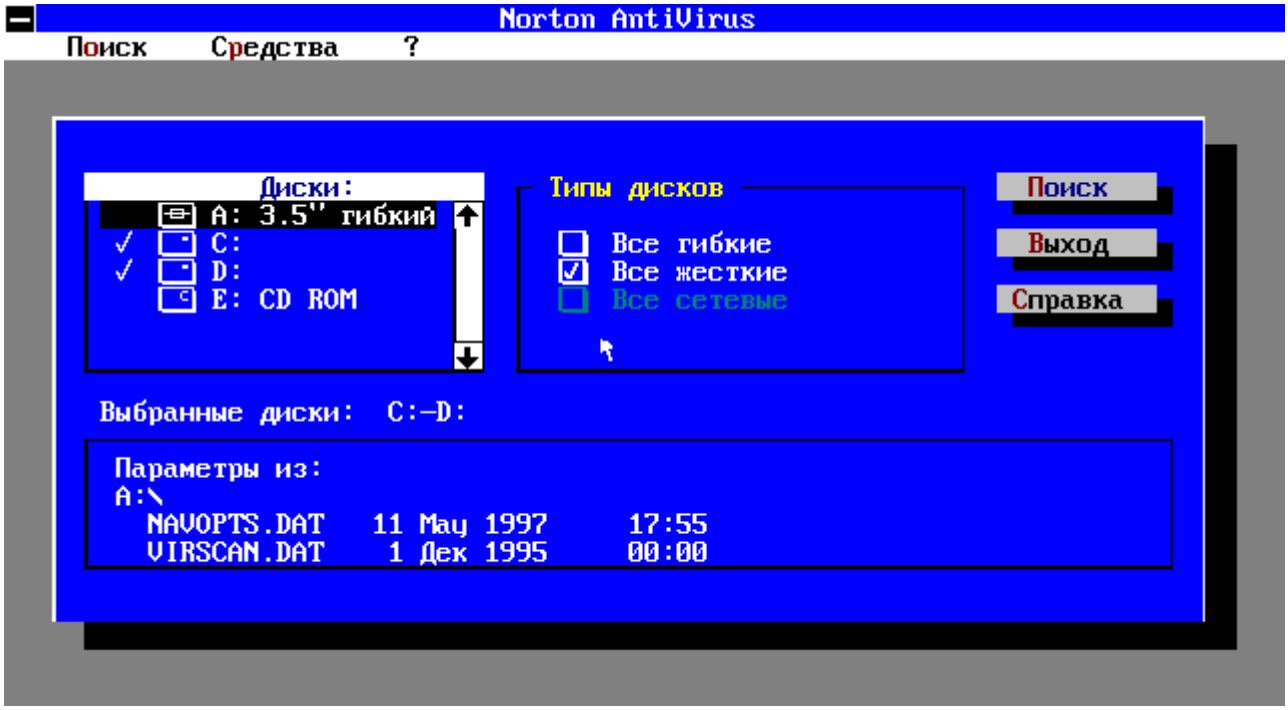


**Рис. 3.47. Главное окно транзитного сканера-ревизора NAVBOOT**

Особенности использования транзитного сканера-ревизора NAVBOOT.EXE те же, что и транзитного сканера-ревизора Norton AntiVirus (NAVW32.EXE), предназначенного для 32-разрядного режима работы Windows 95. Отличительными чертами являются только внешний вид окон интерфейса, так как интерфейс NAVBOOT.EXE является текстовым, и, соответственно, связанные с этим видом интерфейса способы управления.

Активизация главного меню, как и в среде Windows выполняется с помощью клавиши <F10> или <Alt>. Для перемещения между управляющими элементами окна в прямом направлении (сверху вниз и слева направо) предназначена клавиша <Tab>, а в обратном - комбинация клавиш <Shift>+<Tab>. Изменение состояния текущего флажка или переключате-

ля выполняется с помощью клавиши пробела, а раскрытие списка - с помощью комбинации клавиш <Ctrl>+<↓>.

Перед активизацией процесса поиска и обезвреживания вирусов, как и при работе с транзитным сканером-ревизором NAVW32.EXE, необходимо настроить параметры функционирования программы NAVBOOT. Настройка параметров выполняется в окне «Параметры ...» (□□), появляющемся после выполнения команды **Средства/ Параметры**.

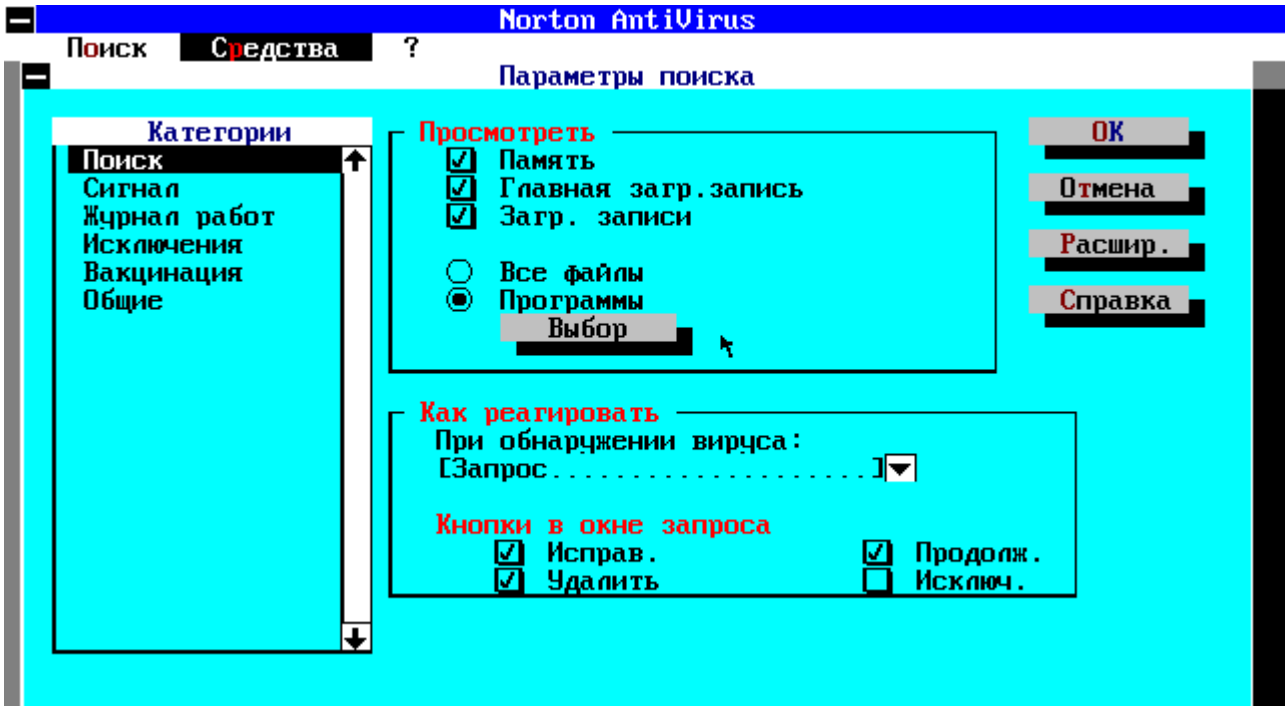


**Рис. 3.48. Диалоговое окно настройки параметров работы транзитного сканера-ревизора NAVBOOT**

Выбор листов свойств в данном окне выполняется путем выбора соответствующего элемента в списке «Категории». Как видно из этого списка, окно настройки параметров функционирования транзитного сканера-ревизора NAVBOOT включает те же листы свойств, что и окно параметров настройки транзитного сканера-ревизора NAVW32.EXE (□□), за исключением листов свойств «Запуск» и «Автозащита», которые для программы NAVBOOT не нужны. Управляющие элементы каждого из листов

свойств окна настройки параметров программы NAVBOOT те же, что и управляющие элементы одноименного листа свойств окна настройки транзитного сканера-ревизора NAVW32.EXE (см. п. 3.1.1).

После настройки всех требуемых параметров работы транзитного сканера-ревизора в окне «Параметры ...» следует нажать кнопку **Ok**.

Для активизации процесса поиска и обезвреживания вирусов, а также формирования эталонных характеристик необходимо выполнить следующие действия:

**1)** в списке флажков «Диски» главного окна транзитного сканера-ревизора NAVBOOT (см. □) указать диски, подлежащие обработке; для выбора всех жестких или всех гибких дисков предназначены соответствующие флажки группы элементов управления **Типы дисков**;

**2)** нажать кнопку **Поиск** или ввести команду **Поиск/ Диски**.

С целью активизации процесса поиска и обезвреживания вирусов, а также формирования эталонных характеристик по отношению к отдельному каталогу или файлу предназначены соответственно команды **Поиск/ Папки...** и **Поиск/ Файлы...** После ввода любой из этих команд необходимо будет указать каталог или файл, подлежащий проверке.

Создание (удаление) эталонных характеристик отдельного программного файла или программных файлов, входящих в заданные каталоги, выполняется с помощью команды **Средства/ Вакцинация**.

Для создания эталонных характеристик следует установить переключатель данного окна в положение **Вакцинация**, а для удаления - в положение **Девакцинация**. Далее необходимо в текстовое поле **Элемент** ввести спецификацию каталога или отдельного программного файла. При указании спецификации каталога будут обработаны все его программные файлы. В случае необходимости следует установить флажок **Включая подпапки**, задающий режим обработки и подкаталогов указан-

ного каталога. Активизация процесса создания или удаления эталонных характеристик выполняется нажатием кнопки **OK**.

Для просмотра или распечатки журнала регистрации предназначена команда **Средства/ Журнал работ**.

При необходимости получения детальной справочной информации следует воспользоваться командами пункта меню **?** (Справка). Команда **?/ Содержание** открывает доступ к полному списку тем справочной системы. С помощью пункта меню **?/ Команды** можно получить описание всех команд главного меню транзитного сканера-ревизора NAVBOOT. Команда **?/ Процедуры** предоставляет возможность (□□) получения пошаговых инструкций по поиску и обезвреживанию вирусов в памяти и на дисках компьютера, а также настройке параметров функционирования программы NAVBOOT.

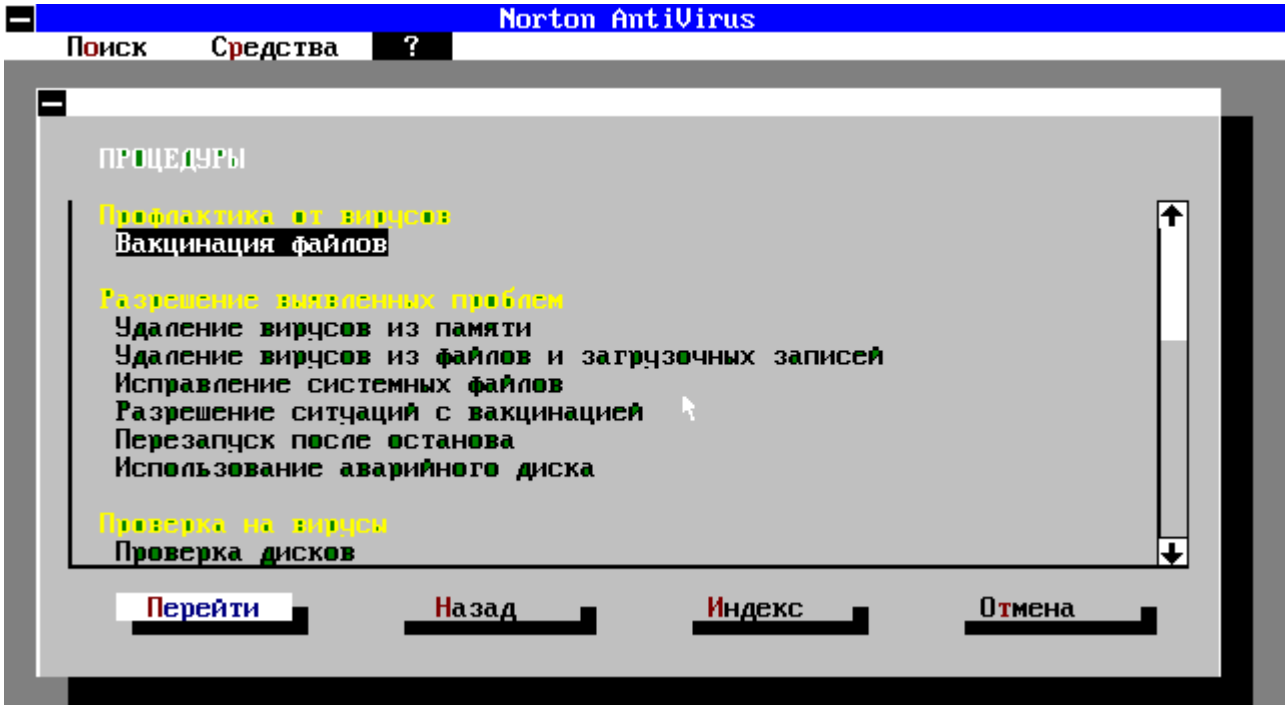


**Рис. 3.49. Справочное окно «Процедуры»**

Завершение работы программы NAVBOOT выполняется с помощью команды **Поиск/ Выход**.

Для транзитного сканера-ревизора NAVBOOT предусмотрен и пакетный режим работы. Формат командной строки для запуска программы NAVBOOT в пакетном режиме следующий:

NAVBOOT <путь> <путь> ... [<ключ>]... [<ключ>]

Здесь <путь> - спецификация проверяемого каталога. Параметры <путь> должны быть отделены друг от друга пробелами.

Основные ключи:

/L или /A - поиск только на жестких или на всех дисках;

/B[+|-] - разрешить/запретить поиск в загрузочных записях (по умолчанию поиск вирусов в загрузочных записях производится);

/BOOT - поиск только в загрузочных записях указанных дисков;

/M[+|-] - разрешить/запретить поиск в оперативной памяти (по умолчанию поиск вирусов в оперативной памяти производится);

/MEM - поиск вирусов только в оперативной памяти компьютера;

/S[+|-] - разрешить/запретить просмотр подкаталогов (по умолчанию предполагается /S- и подкаталоги указанного каталога не проверяются);

/PROMPT - запрос у пользователя требуемого действия при обнаружении вируса;

/REPAIR - установка режима автоматического восстановления зараженных файлов;

/DELETE - установка режима автоматического удаления зараженных файлов;

/REPORT - выдача сообщения при обнаружении вируса;

/HALT - блокировать работу процессора до полной перезагрузки при обнаружении вируса;

/CLEAR - очистить журнал регистрации;

/EXPORT:<спецификация файла> - экспорт журнала регистрации в формате ASCII в указанный файл.

## Восстановление нефайловой системной информации с помощью утилиты Rescue

В случае, если возникает ситуация, когда вследствие деструктивных действий вирусов невозможно загрузиться с жесткого диска, невидимы какие-либо логические диски или в работе программно-аппаратных средств компьютера возникают сбои и отказы, которых раньше не было, то после полной перезагрузки с первой дискеты набора восстановления перед поиском и обезвреживанием вирусов необходимо восстановить нефайловую системную информацию (содержимое MBR, SMBR и BR винчестера, включая таблицу разделов, а также CMOS-памяти) с помощью утилиты Rescue и резервных данных, находящихся на этой же дискете. Для этого требуется выполнить следующие действия:

1) загрузить компьютер с первой дискеты из набора восстановления Norton AntiVirus;

2) набрать в командной строке команду **Rescue** и нажать клавишу <Enter> для запуска с дискеты утилиты Rescue;

3) установить в нижней части появившегося диалогового окна все флажки (см. □□); передвижение между управляющими элементами окна выполняется с помощью клавиши <TAB>, а изменение состояния флажка - клавишей пробела;

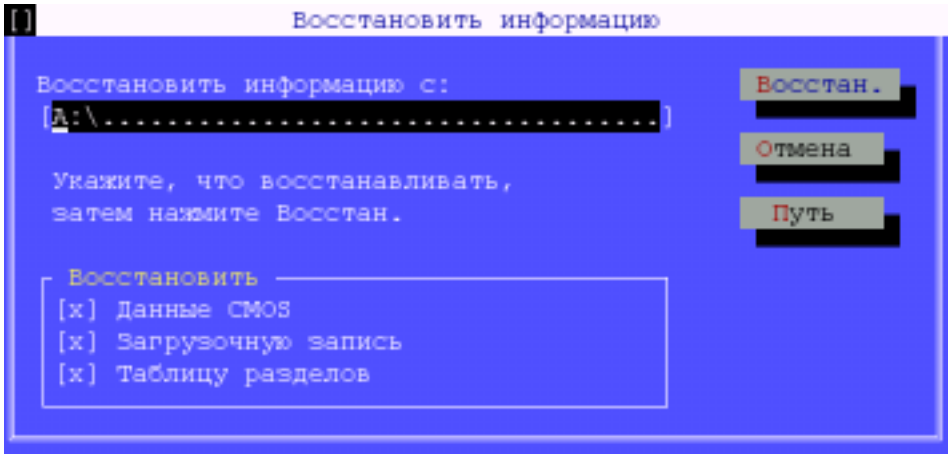


**Рис. 3.50. Диалоговое окно «Восстановить информацию»**

4) нажать кнопку **Восстановить** и далее следовать инструкциям программы.

### Дополнение стандартного набора восстановления

В стандартный набор восстановления Norton AntiVirus, создаваемый программой «Аварийный диск» (NRESQ32.EXE), не включаются следующие необходимые компоненты:

**1)** средство устранения логических и физических дефектов жестких дисков для режима MS-DOS, например, утилита Scandisk, входящая в состав Windows 95;

**2)** копии файлов системного реестра (SYSTEM.DAT, USER.DAT) и файлов инициализации (*.INI), расположенных в каталоге размещения Windows 95 и содержащих основные настроечные параметры для операционной системы, а также системных и прикладных программ, установленных на компьютере;

**3)** программа изменения атрибутов файлов ATTRIB.EXE, а также доступный архиватор, предположим, ARJ, которые понадобятся для восстановления файлов системного реестра и файлов инициализации.

Сразу же после создания программой «Аварийный диск» набора восстанавливающих дискет целесообразно на первую (загрузочную) дискету скопировать утилиту ScanDisk (файлы SCANDISK.EXE, SCANDISK.INI) и программу ATTRIB.EXE, расположенные в каталоге COMMAND каталога размещения Windows 95.

Остальные перечисленные компоненты целесообразно зарезервировать на отдельную чистую дискету. Для этого необходимо выполнить следующие действия.

1. Создать на рабочем диске, имеющем не менее 2-3 Мбайт свободной памяти, временный каталог, предположим, D:\WORK.

2. Скопировать, например, с помощью программы **Проводник**, файлы SYSTEM.DAT, USER.DAT и *.INI из каталога размещения Windows 95 в созданный каталог D:\WORK. При этом следует иметь в виду, что файлы SYSTEM.DAT и USER.DAT имеют атрибуты «только чтение», «скрытый» и «системный».

3. Отменить для файлов SYSTEM.DAT и USER.DAT каталога D:\WORK атрибуты «только чтение», «скрытый» и «системный», введя с помощью пункта меню **Пуск/ Выполнить** следующие командные строки:

```
ATTRIB -R -H -S  D:\WORK\SYSTEM.DAT
ATTRIB -R -H -S  D:\WORK \USER.DAT
```

4. Вставить в дисковод A: отформатированную чистую дискету и заархивировать на нее содержимое каталога D:\WORK, введя с помощью пункта меню **Пуск/ Выполнить** следующую командную строку:

```
ARJ  a  A:\SYS_REZ  D:\WORK\*.*
```

Здесь предполагается, что путь к каталогу размещения архиватора ARJ указан в команде PATH файла AUTOEXEC.BAT. В результате ввода данной команды резервируемые системные файлы будут занесены на дискету A: в архив SYS_REZ.ARJ.

5. Скопировать на дискету архиватор ARJ.EXE, а также файл COMMAND.COM, расположенный в корневом каталоге диска размещения Windows 95. Файл COMMAND.COM необходим для того, чтобы после загрузки с системной дискеты при запуске архиватора с дискеты не нужно было вставлять в дисковод системную дискету.

6. Также скопировать на дискету файлы C:\AUTOEXEC.BAT и C:\CONFIG.SYS несмотря на то, что эти файлы зарезервированы стандартными средствами Norton AntiVirus. Будет намного удобнее, если резерв всей файловой системной информации хранится на одной дискете.

7. Вынуть диск из дисковода, подписать и сохранить вместе с набором восстановления, подготовленном программой «Аварийный диск».

8. Удалить каталог D:\WORK вместе с его содержимым.

Резервирование файловой системной информации подобным способом или с помощью других специализированных средств, например, утилиты Remove-IT, необходимо выполнять после каждых изменений параметров настройки операционной системы, которые происходят, как правило, при инсталляции программ. Такое резервирование, помимо возможности восстановления системных данных после деструктивных действий вирусов, позволит отменить результаты последней инсталляции при отсутствии деинсталляционной программы в установленной программной системе.

Признаками повреждения системной информации является невозможность загрузки операционной системы с винчестера, недоступность каких-либо логических дисков или возникновение сбоев и отказов в работе программно-аппаратных средств компьютера. В этом случае к восстановлению системных файлов (AUTOEXEC.BAT, CONFIG.SYS, файлов системного реестра и файлов инициализации) можно перейти только после восстановления утилитой Rescue нефайловых системных данных (MBR, SMBR и BR винчестера, содержимого CMOS-памяти), устранения с

помощью утилиты ScanDisk логических дефектов файловой структуры жестких дисков, а также поиска и обезвреживания вирусов в на жестких дисках компьютера. Понятно, что все эти действия необходимо выполнять после полной перезагрузки с первой дискеты набора восстановления и с помощью программ, входящих в этот набор.

Для устранения логических дефектов файловой структуры жестких дисков следует после восстановления нефайловых системных данных утилитой Rescue и перезагрузки компьютера с первого диска набора восстановления набрать в командной строке команду **SCANDISK**, перечислить в качестве параметров через пробелы имена всех жестких дисков компьютера, например,

SCANDISK C: D: E:

и далее нажать клавишу <ENTER>. В процессе проверки и восстановления требуется следовать инструкциям программы. По окончании проверки и восстановления каждого диска, за исключением последнего, необходимо в окне запроса нажать кнопку **<Следующий диск>**. По завершении обработки всех логических дисков можно с помощью команды **<Протокол>** просмотреть протокол проверки и восстановления. Для выхода из среды утилиты следует нажать кнопку **<Выход>**.

Затем можно перейти к поиску и обезвреживанию вирусов на логических дисках с помощью транзитного сканера-ревизора NAVBOOT.

По окончании поиска и обезвреживания вирусов для восстановления системных файлов необходимо выполнить следующие действия.

1. Вставить в дисковод дискету с зарезервированными системными файлами, подготовленную описанным выше способом.

2. Выдать команды для переименования поврежденных файлов системного реестра и файлов инициализации:

A:\ATTRIB -R -H -S C:\WINDOWS\SYSTEM.DAT

A:\ATTRIB -R -H -S C:\WINDOWS\USER.DAT

REN  C:\WINDOWS\SYSTEM.DAT SYSTEM.OLD

REN  C:\WINDOWS\USER.DAT USER.OLD

REN C:\WINDOWS*.INI *.BAD

REN C:\AUTOEXEC.BAT  AUTOEXEC.BAD

REN C:\CONFIG.SYS  CONFIG.BAD

Здесь предполагается, что файлы операционной системы размещаются в каталоге C:\WINDOWS. Следует учесть, что переименовать или заменить файлы SYSTEM.DAT и USER.DAT при разархивировании без отмены их атрибутов «только чтение», «скрытый» и «системный» будет невозможно. Различные расширения для переименования файлов системного реестра и файлов инициализации выбраны для избежания конфликта, так как файлы SYSTEM.DAT и SYSTEM.INI имеют одинаковые имена. Если при выдаче перечисленных команд будут появляться сообщения, что данные файлы не обнаружены, следует эти сообщения просто принять во внимание.

3. Ввести команду для восстановления системного реестра и файлов инициализации:

A:\ARJ  E  A:\SYS_REZ  C:\WINDOWS

4. Ввести команды для восстановления файлов AUTOEXEC.BAT и CONFIG.SYS:

COPY A:\AUTOEXEC.BAT C:\

COPY A:\CONFIG.SYS C:\

5. После выяснения причин неработоспособности компьютера старые системные файлы можно удалить.

Ни в коем случае не следует забывать, что кроме подготовки набора восстановления, необходимо заархивировать на дискеты и периодически обновлять по мере модификации и создания всю ценную информацию  с жестких дисков компьютера. Только в этом случае будет обеспечена надежная защита информации от потери.

## Литература


**1.** Безруков Н.Н. Компьютерная вирусология: Справ. руководство. - Киев: издательство УРЕ. - 1991.

**2.** Зегжда Д.П., Мешков А.В., Семьянов П.В., Шведов Д.В. Как противостоять вирусной атаке. - Спб: BHV. - 1995.

**3.** Зима В.М., Молдовян А.А. Многоуровневая защита информационно-программного обеспечения вычислительных систем: Учеб. пособие. - Спб: издательско-полиграфический центр ГЭТУ. - 1997.

**4.** Зима В.М., Молдовян А.А. Схемы защиты информации на основе системы «Кобра»: Учеб. пособие. - Спб: издательско-полиграфический центр ГЭТУ. - 1997.

**5.** Зима В.М., Молдовян А.А. Технология практического обеспечения информационной безопасности: Учеб. пособие. - Спб: издательско-полиграфический центр ГЭТУ. - 1997.

**6.** Касперский Е. Компьютерные вирусы в MS-DOS. - М.: издательство «Эдэль». - 1992.

**7.** Лей Р. Написание драйверов для MS-DOS: Пер. с англ. - М.: издательство «Мир». - 1995.

**8.** Платонов В.В. Компьютерные вирусы и защита от них: Учеб. пособие. - СПб: ВИККА им. А.Ф.Можайского. - 1994.

**9.** Расторгуев С.П. Инфицирование как способ защиты жизни. Вирусы: биологические, социальные, психические, компьютерные. - М.: издательство «Яхтсмен». - 1996.

**10.** Файтс Ф., Джонсон П., Кратц М. Компьютерный вирус: проблемы и прогноз. - М.: издательство «Мир». - 1994.