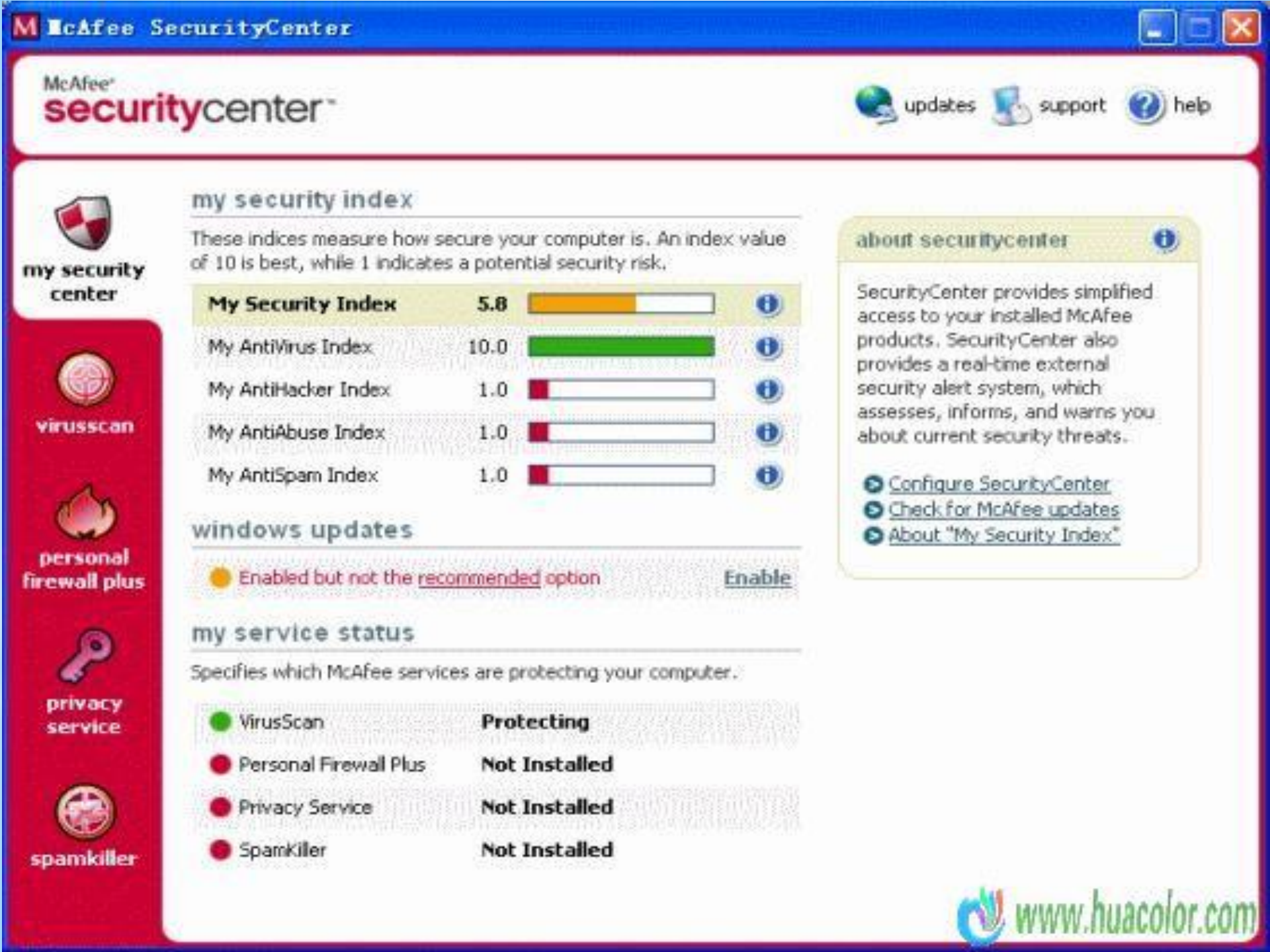
Программы-детекторы

Выполнили: Димитриев А.О.
Туракалина Т.А.
Поликарпов О.А.

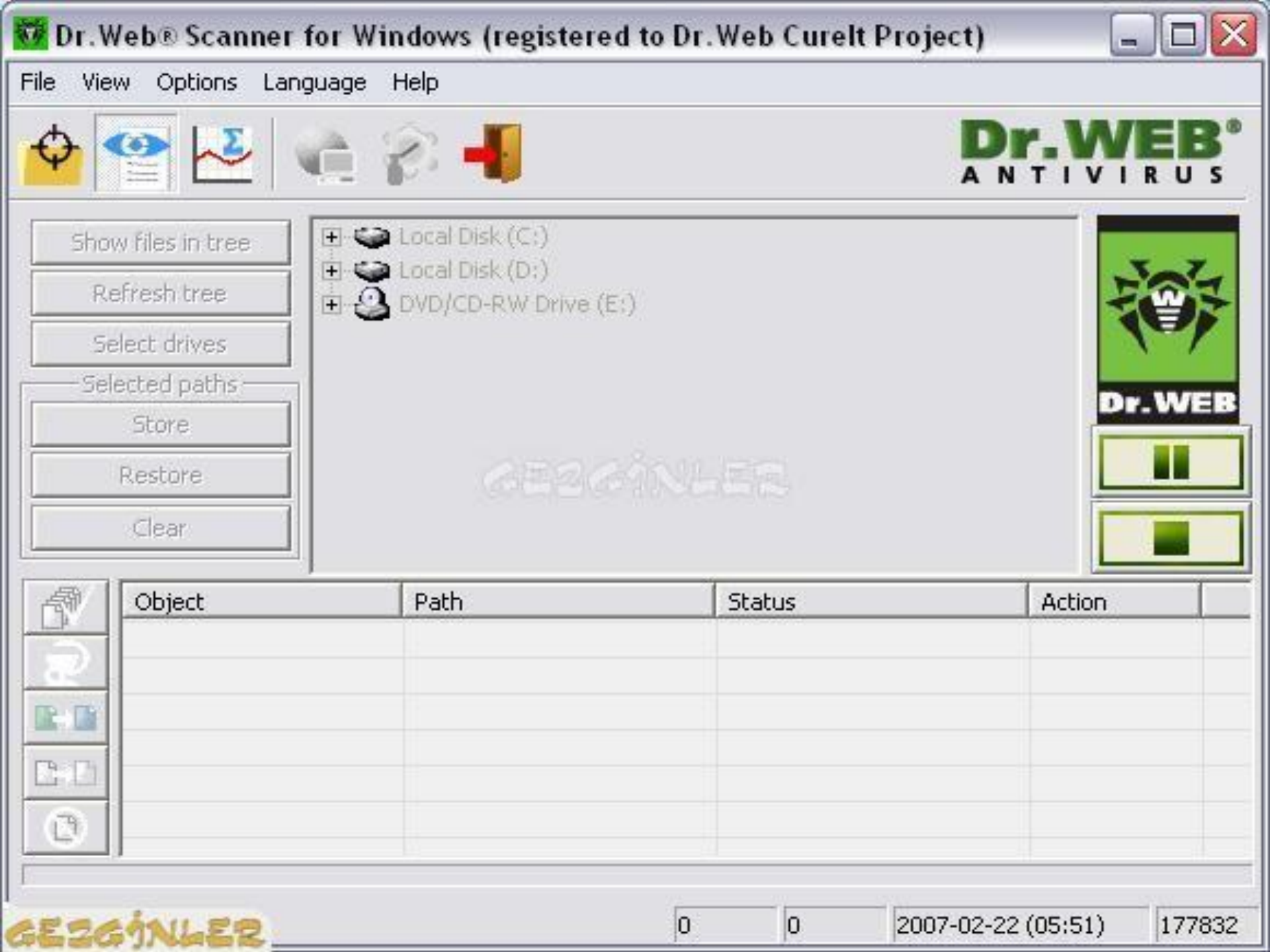
* **ПРОГРАММЫ-ДЕТЕКТОРЫ позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов. Эти программы проверяют, имеется ли в файлах на указанном пользователем диске специфическая для данного вируса комбинация байтов. При ее обнаружении в каком-либо файле на экран выводится соответствующее сообщение.**


McAfee SecurityCenter
McAfee securitycenter
updates
support
help
my security center
virusscan
personal firewall plus
privacy service
spamkiller
my security index
These indices measure how secure your computer is. An index value of 10 is best, while 1 indicates a potential security risk.
My Security Index 5.8
My AntiVirus Index 10.0
My AntiHacker Index 1.0
My AntiAbuse Index 1.0
My AntiSpam Index 1.0
windows updates
Enabled but not the recommended option
Enable
my service status
Specifies which McAfee services are protecting your computer.
VirusScan Protecting
Personal Firewall Plus Not Installed
Privacy Service Not Installed
SpamKiller Not Installed
about securitycenter
SecurityCenter provides simplified access to your installed McAfee products. SecurityCenter also provides a real-time external security alert system, which assesses, informs, and warns you about current security threats.
Configure SecurityCenter
Check for McAfee updates
About "My Security Index"
www.huacolor.com

* Многие детекторы имеют режимы лечения или уничтожения зараженных файлов. Следует подчеркнуть, что программы-детекторы могут обнаруживать только те вирусы, которые ей "известны". Программа Scan фирмы McAfee Associates и Aidstest Д.Н.Лозинского позволяют обнаруживать около 1000 вирусов, но всего их более пяти тысяч! Некоторые программы-детекторы, например Norton AntiVirus или AVSP фирмы "Диалог-МГУ", могут настраивать на новые типы вирусов, им необходимо лишь указать комбинации байтов, присущие этим вирусам. Тем не мение невозможно разработать такую программу, которая могла бы обнаруживать любой заранее неизвестный вирус.

```
E:\ANTIVIR\AIDSTEST>aidstest.exe c:

      А О "Диалог Наука"
        Антивирус AIDSTEST
      Версия 1644 от 09.12.96
       (c) Copyright 1990-96
    Лозинский Дмитрий Николаевич
  Москва, тел./факс (095) 938-2970
         тел.  135-6253, 137-0150
    BBS  938-2856  (28800/V.34)
      E-mail loz@dials.msk.su
        FidoNet   2:5020/69

 Для НАДЕЖНОГО ЕЖЕДНЕВНОГО антивирусного
контроля рекомендую также другие продукты:
- ревизор ADinf с лечащим модулем
- полифаг Doctor Web
- аппаратно-программный комплекс Sheriff

 Информация - в документации и изданиях:
   "Человек и Компьютер", индекс 50165
   "Софт Маркет", индекс 50138

СПРАВКИ об услугах, условиях - aidstest /d
Антивирусная СКОРАЯ ПОМОЩЬ - тел.137-0150

Проверка "C:" (метка тома: SYSTEM)
c:\EXE\KIRS.COM
```

* Многие программы-детекторы (в том числе и Aidstest) не умеют обнаруживать заражение "невидимыми" вирусами, если такой вирус активен в памяти компьютера. Дело в том, что для чтения диска они используют функции DOS, а они перехватываются вирусом, который говорит, что все хорошо. Правда, Aidstest и другие детекторы пытаются выявить вирус путем просмотра оперативной памяти, но против некоторых "хитрых" вирусов это не помогает. Так что надежный диагноз программы-детекторы дают только при загрузке DOS с "чистой", защищенной от записи дискеты, при этом копия программы-детектора также должна быть запущена с этой дискеты.

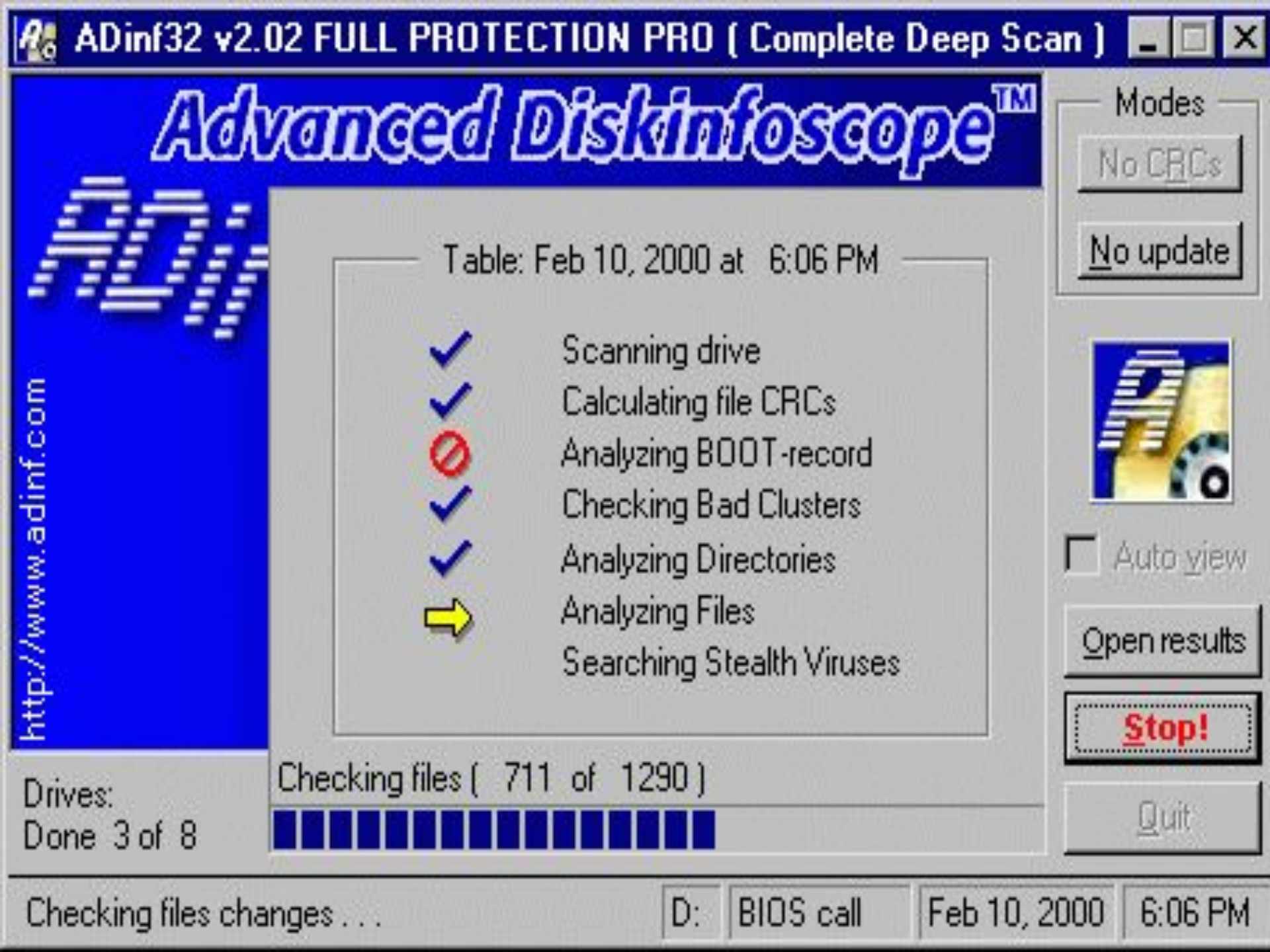

Dr.Web® Scanner for Windows (registered to Dr.Web CureIt Project)
File
View
Options
Language
Help
Dr.WEB®
ANTIVIRUS
Show files in tree
Refresh tree
Select drives
Selected paths
Store
Restore
Clear
Local Disk (C:)
Local Disk (D:)
DVD/CD-RW Drive (E:)
Dr.WEB
Object
Path
Status
Action
0
0
2007-02-22 (05:51)
177832

Некоторые детекторы, скажем, ADinf фирмы "Диалог-Наука", умеют ловить "невидимые" вирусы, даже когда они активны. Для этого они читают диск, не используя вызовы DOS. Правда, этот метод работает не на всех дисководах.

Большинство программ-детекторов имеют функцию "доктора", т.е. они пытаются вернуть зараженные файлы или области диска в их исходное состояние. Те файлы, которые не удалось восстановить, как правило, делаются неработоспособными или удаляются.

Большинство программ-докторов умеют "лечить" только от некоторого фиксированного набора вирусов, поэтому они быстро устаревают. Но некоторые программы могут обучаться не только способам обнаружения, но и способам лечения новых вирусов.

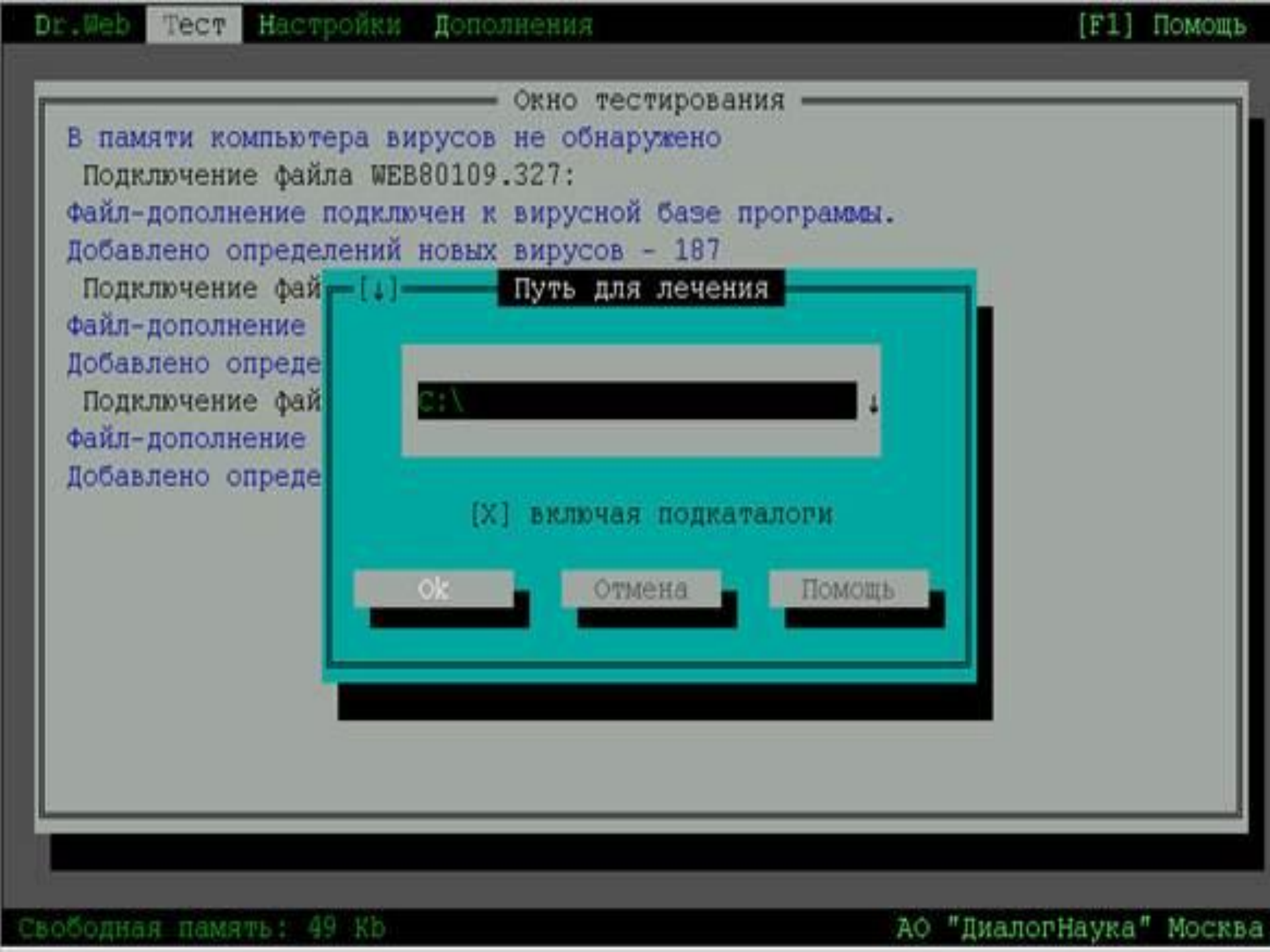
К таким программам относится AVSP фирмы "Диалог-МГУ".


ADinf32 v2.02 FULL PROTECTION PRO (Complete Deep Scan)
Advanced Diskinfoscope™
http://www.adinf.com
Modes
No CRCs
No update
Table: Feb 10, 2000 at 6:06 PM
Scanning drive
Calculating file CRCs
Analyzing BOOT-record
Checking Bad Clusters
Analyzing Directories
Analyzing Files
Searching Stealth Viruses
Auto view
Open results
Stop!
Quit
Drives:
Done 3 of 8
Checking files (711 of 1290)
Checking files changes . . .
D:
BIOS call
Feb 10, 2000
6:06 PM

* Чрезвычайно принципиально, чтоб вирусные базы постоянно были свежайшими. Так как новейшие вирусы возникают постоянно, все главные производители антивирусных программ постоянно обновляют вирусные базы. Обычно, обновление вирусных баз реализуется постоянным, не пореже 1-го раза в день, выпуском особых дополнений к ним.

* Многие программы-детекторы (в том числе и Aidstest) не умеют обнаруживать заражение "невидимыми" вирусами, если такой вирус активен в памяти компьютера. Дело в том, что для чтения диска они используют функции DOS, перехватываются вирусом, который говорит, что все хорошо. Правда, Aidstest и др. программы могут выявить вирус путем просмотра оперативной памяти, но против некоторых "хитрых" вирусов это не помогает. Так что надежный диагноз программы-детекторы дают только при загрузке DOS с защищенной от записи дискеты, при этом копия программы-детектора также должна быть запущена с этой дискеты.

* Некоторые детекторы, скажем, ADinf "Диалог-Наука", умеют ловить "невидимые" вирусы, даже когда они активны. Для этого они читают диск, не используя вызовы DOS. Этот метод работает не на всех дисководах.
* Большинство программ-детекторов имеют функцию "доктора", т.е. пытаются вернуть зараженные файлы или области диска в их исходное состояние. Те файлы, которые не удалось восстановить, как правило, делаются неработоспособными или


Dr.Web
Тест
Настройки
Дополнения
[F1] Помощь
Окно тестирования
В памяти компьютера вирусов не обнаружено
Подключение файла WEB80109.327:
Файл-дополнение подключен к вирусной базе программы.
Добавлено определений новых вирусов - 187
Подключение фай
Файл-дополнение
Добавлено опреде
Подключение фай
Файл-дополнение
Добавлено опреде
[↓]
Путь для лечения
C:\
[X] включая подкаталоги
Ok
Отмена
Помощь
Свободная память: 49 Kb
АО "ДиалогНаука" Москва

* Многие программы-ревизоры являются довольно "интеллектуальными" - они могут отличать изменения в файлах, вызванные, например, переходом к новой версии программы, от изменений, вносимых вирусом, и не поднимают ложной тревоги. Дело в том, что вирусы обычно изменяют файлы весьма специфическим образом и производят одинаковые изменения в разных программных файлах. Понятно, что в нормальной ситуации такие изменения практически никогда не встречаются, поэтому программа-ревизор, зафиксировав факт таких изменений, может с уверенностью сообщить, что они вызваны именно вирусом.

Спасибо за внимание)))