

KASPERSKY LABS LTD.

**SECURE
YOUR
CYBERSPACE**

www.kaspersky.com



**Kaspersky Anti-Virus®
Personal / Personal Pro 4.5**

USER GUIDE

KASPERSKY ANTI-VIRUS®
PERSONAL / PERSONAL PRO 4.5

User Guide

© Kaspersky Labs Ltd.
Visit our Web Site: <http://www.kaspersky.com>

Edition date: September 2003

Contents

CHAPTER 1. KASPERSKY ANTI-VIRUS® PERSONAL.....	10
1.1. New Features of Version 4.5	11
1.2. Hardware and Software Requirements	11
1.3. Distribution kit	12
1.4. Help Desk for Registered Users	13
1.5. Conventions.....	14
CHAPTER 2. INSTALLING AND UNINSTALLING KASPERSKY ANTI-VIRUS PERSONAL	15
2.1. Installing	15
2.2. Reinstalling	18
2.3. Uninstalling	19
CHAPTER 3. KASPERSKY ANTI-VIRUS SCANNER.....	20
3.1. Starting Kaspersky Anti-Virus Scanner	20
3.2. Program Interface.....	23
3.2.1. System menu.....	23
3.2.2. Main window	24
3.2.3. Menu	24
3.2.4. Tool bar	25
3.2.5. Work area.....	26
3.2.6. Status bar	27
3.3. Changing Settings	27
3.3.1. Scanning parameters for objects. <i>Objects</i> category	28
3.3.1.1. Defining objects to be checked. Memory, sectors, and files	30
3.3.1.2. Handling infected and suspicious objects	31
3.3.1.3. Advanced scanning modes	33
3.3.2. General settings: <i>Options</i>	35
3.3.2.1. Reporting options.....	36
3.3.2.2. Renaming, copying, and deleting options.....	36
3.3.2.3. Defining priority	37
3.3.3. Advanced settings: <i>Customize</i>	37
3.3.4. Saving/loading settings.....	39

3.3.5. Previewing settings before the check	39
3.4. Checking For and Deleting Viruses	40
3.4.1. Starting and aborting the check	40
3.4.2. Changing priority of the check	42
3.4.3. Monitoring progress	42
3.4.4. Viewing statistics: <i>Statistics</i>	43
3.5. Updating Anti-Virus Databases	44
3.6. Generating a List of Currently Known Viruses	44
CHAPTER 4. KASPERSKY ANTI-VIRUS MONITOR	46
4.1. How to start, disable and enable your AV Monitor	46
4.2. Program Interface	47
4.2.1. System menu	47
4.2.2. Main window	48
4.2.3. Menu	49
4.2.4. Toolbar	50
4.2.5. Work area	51
4.3. Changing Settings	52
4.4. Loading, disabling and enabling Kaspersky AV Monitor	52
4.5. Updating Anti-Virus Databases	54
CHAPTER 5. KASPERSKY ANTI-VIRUS UPDATER	55
5.1. How to start the Kaspersky AV Updater	55
5.2. Kaspersky AV Updater Interface	55
5.2.1. Step 1. The Welcome wizard box	56
5.2.2. Step 2. The <i>Connection</i> wizard box	56
5.2.2.1. Updating via the Internet	58
5.2.2.2. Updating from a local folder	63
5.2.2.3. Choosing objects to be updated	64
5.2.3. Step 3. The <i>Options</i> wizard box	64
5.2.4. The <i>Retrieving updates</i> window	65
5.2.5. Step 5. The <i>Finishing</i> wizard box	66
CHAPTER 6. KASPERSKY ANTI-VIRUS CONTROL CENTRE	67
6.1. Launching Kaspersky AV Control Centre	67
6.2. Kaspersky AV Control Centre Interface	70
6.2.1. The <i>Tasks</i> tab	70

6.2.1.1. The <i>Property</i> window	75
6.2.2. The <i>Components</i> tab	79
6.2.3. The <i>Settings</i> tab	80
6.2.3.1. The <i>Security</i> category	82
6.2.3.2. The <i>Alerts</i> category	84
6.2.3.3. The <i>Customize</i> category	88
6.2.3.4. The <i>Quarantine</i> category	90
6.2.4. The <i>Quarantine</i> tab	91
6.3. New Task Wizard	94
6.3.1. <i>Tasks</i> window	95
6.3.2. The <i>Schedule</i> window for a Kaspersky AV Monitor task	96
6.3.3. The <i>Schedule</i> window for Kaspersky AV Scanner and Updater	96
6.3.3.1. Launching on event	98
6.3.3.2. Launching by condition	99
6.3.3.3. Launching hourly	100
6.3.3.4. Launching daily	100
6.3.3.5. Launching weekly	101
6.3.3.6. Launching monthly	102
6.3.4. The <i>Alerts</i> window	103
6.3.5. The User account window	103
6.3.6. Task settings	104
6.3.6.1. The <i>Settings</i> window for Kaspersky AV Scanner and Monitor tasks	105
CHAPTER 7. KASPERSKY REPORT VIEWER	106
CHAPTER 8. THE SETTINGS TREE	110
8.1. The Settings Tree	110
8.2. Controls	111
8.2.1. Check box	111
8.2.2. Option button	112
8.2.3. Text field	112
8.2.4. Input field defining the path to	113
8.2.5. Input field defining the number of	113
8.2.6. Drop-down list	114
8.3. Checkboxes	114
CHAPTER 9. KASPERSKY ANTI-VIRUS SCRIPT CHECKER	116

CHAPTER 10. KASPERSKY ANTI-VIRUS RESCUE DISKS	118
10.1. Creating a Fallback-Recovery Set	118
10.2. Using the Fallback-Recovery Disks	122
CHAPTER 11. KASPERSKY ANTI-VIRUS MAIL CHECKER.....	126
11.1. Configuring Kaspersky AV Mail Checker	126
11.2. Running Kaspersky Mail Checker	128
11.2.1. Incoming messages	128
11.2.2. Outgoing messages	128
11.2.3. Messages in the mailbox.....	129
CHAPTER 12. KASPERSKY ANTI-VIRUS PERSONAL PRO	130
CHAPTER 13. KASPERSKY® OFFICE GUARD.....	131
13.1. Kaspersky Office Guard – Protection from Unknown Macro Viruses	131
13.1.1. How they function	132
13.1.2. Suspicious macro instructions.....	133
13.1.3. Detecting macro viruses. Rules for suspicious macro instructions.....	134
13.2. Kaspersky Office Guard Interface.....	136
13.2.1. Launching the program	136
13.2.2. System menu.....	137
13.2.3. Main window	138
13.2.4. Closing the program	138
13.2.5. Help topics	138
13.3. Custom settings.....	138
13.3.1. Custom security level	138
13.3.2. Maximum security level	139
13.3.3. Middle security level	139
13.3.4. All ask level	140
13.3.5. Low security level	140
13.3.6. Custom level	141
13.4. Interception of suspicious macro instructions.....	143
13.5. Log.....	145
CHAPTER 14. KASPERSKY® INSPECTOR.....	146
14.1. Features of Kaspersky Inspector™ Under MS Windows NT	147
14.2. The Operating Concept of Kaspersky Inspector	147
14.2.1. Checks that Kaspersky Inspector performs.....	148

14.2.2. Analyzing changes on your disk	148
14.2.3. Searching for stealth viruses	149
14.2.4. Deleting viruses using the Kaspersky AV Cure Module™	150
14.2.4.1. The Kaspersky AV Cure Module for Windows	150
14.2.5. Checking the OS parameters during the boot (the KAVIBOOT.VXD driver).....	151
14.3. Kaspersky Inspector Interface	151
14.3.1. Main window	151
14.3.2. Menu bar	152
14.3.3. Tool bar	154
14.3.4. Icon bar	155
14.3.5. Work area	156
14.3.6. Status bar	157
14.4. Starting Kaspersky Inspector	157
14.4.1. Starting the program using the MS Windows Start menu.....	157
14.4.2. Starting Kaspersky Inspector using Control Centre	157
14.4.3. Starting the program the first time	157
14.4.4. Starting to check for changes on your disk.....	158
14.4.4.1. Checking for changes on the disk	158
14.4.4.2. Creating new tables	158
14.4.5. Starting to search for stealth viruses	159
14.5. Customizing Kaspersky Inspector	160
14.5.1. The Options work area: selecting general options	160
14.5.2. The Objects work area: selecting options for every drive to be checked	164
14.5.2.1. Defining check parameters for hard and logical drives	164
14.5.2.2. Defining how to access a drive.....	165
14.5.2.3. Items to be checked on the drive	166
14.5.2.4. Defining how to calculate CRC values.....	167
14.5.2.5. Checking for stealth viruses	167
14.5.2.6. Advanced settings	168
14.5.3. Saving and loading settings	168
14.6. Viewing Check Results	169
14.6.1. The Statistics work area: viewing Kaspersky Inspector performance statistics	169
14.6.2. The Disks work area: viewing changes detected	170
14.6.3. The Disks work area: viewing changes detected	172

14.6.4. The Disks work-area: master boot record details.....	173
14.6.5. The Disks work area: boot record details	174
14.6.6. The Registry work area: viewing modifications in registry files.....	175
14.6.7. The Disks and Registry work areas: allowing/prohibiting changes to Kaspersky Inspector tables	178
APPENDIX A. ADVANCED CHECKING TOOLS.....	179
A.1. The Heuristic Checking Tool (Code Analyzer).....	179
A.2. The Redundant Scanning Tool.....	180
APPENDIX B. GLOSSARY	182
APPENDIX C. KASPERSKY LABS LTD.....	187
C.1. Other Anti-Virus products	Ошибка! Закладка не определена.
C.2. Contact Information.....	Ошибка! Закладка не определена.
APPENDIX D. LICENSE AGREEMENT	194

CHAPTER 1. KASPERSKY ANTI-VIRUS® PERSONAL



Attention! New viruses appear every day, therefore it is important to keep this product upgraded by updating virus databases every day (see detailed information below). Please do not forget to update the anti-virus database upon product installation!

The Kaspersky Anti-Virus® Personal software package is designed to protect a computer running the **Windows** operating system against viruses.

The following software products are included in the package:

- **Kaspersky Anti-Virus® Scanner** is an anti-virus program that checks for viruses and deletes them on demand. The program searches for and removes viruses from files, boot sectors and RAM. It is able to detect (but cannot delete!) viruses in archived files and local mailboxes of the most commonly used mail systems.
- **Kaspersky Anti-Virus® Monitor** is a resident virus-detection monitor that checks files that are started and opened.



Note that Kaspersky Anti-Virus® Monitor is able to remove viruses from ZIP archives!

- **Kaspersky Anti-Virus® Updater** is a virus-definition database-updating utility. When searching for viruses, Kaspersky AV Scanner and Kaspersky AV Monitor use this anti-virus (or virus-definition) database to identify viruses detected. Kaspersky Labs updates these databases on a daily basis by adding new virus details to them; database updates are placed on Kaspersky Labs web sites and later retrieved by the updating utility.
- **Kaspersky Anti-Virus® Mail Checker** is a program that provides anti-virus security to the Microsoft Outlook 98/2000/XP users.
- **Kaspersky Anti-Virus® Script Checker** is a program that protects computers from script viruses and worms that are executed directly within computer memory. When you run the Kaspersky Anti-Virus® Personal setup utility, the program is automatically added in your operating system and later you will not have to start it manually.

- **Kaspersky Anti-Virus® Rescue Disk** is a program that allows a user to create a set of rescue disks to restore the system in the aftermath of a virus-attack
- **Kaspersky Anti-Virus® Control Centre** is a shell program for the software package components. The Kaspersky AV Control Centre allows a user to manage installation and updating of the package components, schedule required operations, launch anti-virus applications and review their performance statistics.
- **Kaspersky Anti-Virus® Report Viewer** is a program allowing a user to display reports generated by the package components.

1.1. New Features of Version 4.5

The Kaspersky Anti-Virus® Personal version described in this book has the following new features:

- Enhanced speed of program operation;
- Cleaning ZIP-archives.
- An algorithm for checking attachments in both incoming and outgoing messages has been empowered with the Kaspersky Anti-Virus® Mail Checker utility to minimize computer resources used to check your mail for viruses.

1.2. Hardware and Software Requirements

In order to run Kaspersky Anti-Virus® Personal you need a system that meets the following requirements:

Windows 95/98/Me

- Intel Pentium processor (or compatible) of **150 MHz** or higher.
- At least **32 Mb** of RAM (**64 Mb** recommended).

Windows NT Workstation 4.0 (SP6a or higher):

- Intel Pentium processor (or compatible) of **150 MHz** or higher.
- At least **48 Mb** of RAM (**64 Mb** recommended).

Windows 2000 Professional:

- Intel Pentium processor (or compatible) of **150 MHz** or higher.
- At least **64 Mb** of RAM (**96 Mb** recommended).

Windows XP Home Edition/Professional:

- Intel Pentium processor (or compatible) of **300 MHz** or higher.
- At least **128 Mb** of RAM.



When running Kaspersky Anti-Virus® under the Windows XP Home Edition or the Windows XP Professional operating system with the **Fast User Switching** option selected some features of the anti-virus program become unavailable: the user cannot change settings of Kaspersky Anti-Virus® and cannot expect the program to interactively respond to events (for example when Kaspersky Anti-Virus® will detect a virus, it will not display the appropriate dialog box asking a user how to handle the infected object).

General requirements for all operating systems:

- At least **72 Mb** space available on the hard disk to install, and **23 Mb** to run.
- Microsoft Internet Explorer of version 5.5 or higher with SP2.
- No other anti-virus programs installed on your computer, including Kaspersky Labs products.



If you have any anti-virus programs installed on your computer, we recommend that you uninstall them before installing Kaspersky Anti-Virus® Personal.

- The monitor resolution should be set to at least 800 x 600, the small font should be selected, and the system date should be set correctly.

1.3. Distribution kit

You can purchase Kaspersky Anti-Virus® Personal either from our distributors (retail box) or online at one of our Internet shops (for example, www.kaspersky.com - select the **Buy online** link).

The retail box includes:

- a sealed envelope with an installation CD containing files for the software product;
- User Guide;

- a license key written on the installation CD;
- license agreement.



Before you unseal the envelope containing the CD, be sure to thoroughly review the license agreement.

If you buy Kaspersky Anti-Virus® Personal online, you download the installation file of the product from the Kaspersky Labs website. This installation file includes this User Guide and the license key. The license key can also be sent to you by e-mail after receiving your payment.

The License Agreement (LA) is a legal agreement between you and the manufacturer (Kaspersky Labs Ltd.) describing the terms on which you may employ the anti-virus product which you have purchased.



Make sure you read the License Agreement!

If you do not agree to the terms of this LA, you can return the unused product to your Kaspersky Anti-Virus® dealer for a full refund, making sure the envelope with the CD is sealed.

If you unsealed the envelope or installed the program, you have agreed to all the terms of the LA.

1.4. Help Desk for Registered Users

Kaspersky Labs offers a large service package enabling its legal customers to enjoy all available features of Kaspersky Anti-Virus®.

If you register and purchase a subscription you will be provided with the following services for the period of your subscription:






- new versions of this anti-virus software product provided free of charge;
- phone or e-mail advising on matters related to the installation, configuration, and operation of this anti-virus product;
- information about new Kaspersky Labs products and about new computer viruses (for those who subscribe to the Kaspersky Labs newsletter).



Kaspersky Labs does not provide information related to operation and use of your operating system or various other technologies.

1.5. Conventions

In this book we use various conventions to emphasize different meaningful parts of the documentation. The Table below lists the conventions used in this User Guide.

Convention	Meaning
Bold font	Menu titles, commands, window titles, dialog elements, etc.
 Note.	Additional information, notes
 Attention!	Critical information
 <i>To do this,</i> 1. Step 1. 2. ...	Actions that must be taken
 Task or example	Formulation of the problem or an example of how to use the product.
 Solution	A solution of the problem formulated
[key] – Function of the key.	Command line keys
Text of information messages and the command line	Text of configuration files, information messages, and the command line.

CHAPTER 2. INSTALLING AND UNINSTALLING KASPERSKY ANTI-VIRUS[®] PERSONAL



Before installing Kaspersky Anti-Virus[®] Personal make sure to quit all programs running on your computer.

Launch the *setup.exe* program on the CD to start the package installation. The setup wizard operates in dialog mode. Each dialog box contains a certain set of buttons allowing management of the setup. The main buttons are:

- **OK** – accept actions
- **Cancel** – cancel actions
- **Next** – move one step forward
- **Back** – move one step backward

There are two possible variations on how to install the product: installing it for the first time and reinstalling. Below, both variants are described in detail.

2.1. Installing

Step 1. Read the license agreement

The **License Agreement** dialog box contains the agreement text. Read it carefully and press **Yes** if you agree to the license agreement terms. Otherwise, press **No** to abort the setup.

Step 2. Input user information

Enter user information in the **Customer Information** dialog box. Enter the appropriate data in the **User Name** field and the **Company Name** field. By default the information for these fields is taken from the Windows registry.

Step 3. Select the folder the program will be installed to

In the **Choose Destination Location** dialog box, select the installation folders where the Kaspersky Anti-Virus® Personal program components will be installed. **Destination Folder** indicates the folder for the components, and **Common Files Folder** indicates the path for files shared by all the components. To select folders, press **Browse** and indicate the folder path in the **Choose Folder** standard dialog box.

Step 4. Input the program group name in the Start\Programs menu

Define the folder name in the **Select Program Folder** dialog box for the Kaspersky Anti-Virus® Personal icon to appear in the standard **Program** menu. Press **Next**.

Step 5. Choose setup type

Choose one of the three setup types in the **Setup Type** dialog box:

- | | |
|----------------|---|
| Custom | You will be asked to select the required components from a list. |
| Easy | Only the most essential components of the package will be installed, namely: Kaspersky Anti-Virus® Scanner, Kaspersky Anti-Virus® Monitor, anti-virus databases and the updating program. |
| Typical | All the Kaspersky Anti-Virus® software package components will be installed. |

Step 6. Choose the Kaspersky Anti-Virus® components to be installed

If you selected the **Custom** setup, you will have to choose the required components in the **Select Components** dialog box.

To choose the components to be installed check the appropriate boxes at the left of component names.

Step 7. Copying files to the hard disk

Read the setup information in the **Start Copying Files** dialog box. Press **Next** to continue the installation. The program will start copying files to the hard disk; the process is indicated by the progress bar in the **Setup Status** dialog box.

Step 8. Choose the report storage

In the **Report Viewer Settings** dialog box, you must define the folder for the reports generated by Kaspersky Anti-Virus® Personal components to be saved to.

Step 9. Define paths to the key files

In the **Key File** dialog box, you must define the key file name and path.

If the file is located in the setup folder, its name will be displayed in the **List of key files to install** list.

If the key file is located in a different folder, press **Add** and define the key file name and path in the **Select Key File** standard dialog box. If required, the program may simultaneously use several key files.

The key file is your personal **key** that contains all the housekeeping data essential for Kaspersky Anti-Virus® to apply all its features:

- Vendor information for this version (company name, addresses, telephone numbers)
- Support information (who and where support is provided)
- Product release date
- Name and number of the license
- Functionality table for various components
- Period of validity for this license

Step 10. To complete setup

Upon completion of the Kaspersky Anti-Virus® Personal package installation the **Completing Setup Wizard** dialog box appears on the screen. Choose one of the following options:

- Yes, I want to restart my computer now**
- No, I will restart my computer later**



In this case, to correctly complete the setup of the Kaspersky Anti-Virus® Personal package and start working, it is **ESSENTIAL** to restart your computer.

Press **Finish**.



The startup of your operating system may be delayed because the program is completing installation of Kaspersky Anti-Virus® Personal on your computer. Don't worry! At this moment Kaspersky Anti-Virus® Personal is being registered with your system.

2.2. Reinstalling

If you start to reinstall the program, the **Program Maintenance** dialog box will appear on your screen. In this dialog box, you must choose one of the following options:

- **Modify** – adds new components to the existing installation
- **Repair** – reinstall all program components (damaged) installed by the previous setup.
- **Remove** – completely removes the Kaspersky Anti-Virus® Personal package from your computer (see subchapter 2.3).

Select one of the options and press **Next**.

If you selected the **Modify** option and pressed **Next**, the **Select Components** dialog box will appear on your screen. Select the required package components by checking the appropriate boxes in the dialog box and press **Next**. The **Setup Status** and the **Completing Setup Wizard** dialog boxes will consequently appear on your screen.

If you selected the **Repair** option and pressed **Next**, the **Setup Status** and the **Completing Setup Wizard** dialog boxes will appear on your screen. This mode can be used if, for example, one of the files included in the Kaspersky Anti-Virus® Personal package has been unintentionally deleted.

If Kaspersky AV Control Centre (this or a previous version) has already been installed on your computer (it could have been installed as a component of another Kaspersky Labs package), the setup wizard will display the **Component: Kaspersky Anti-Virus® Control Centre** wizard box. Use this dialog box to define installation settings of the standard settings file.

In this box, you can select one of the following options:

- **Merge** – appends a standard settings file to settings detected in the existing file;

- **Overwrite** – installs a standard settings file instead of the settings file detected on your hard drive;
- **Skip** – keeps the detected settings file unchanged.

If Kaspersky AV Updater has been already installed on your computer, a wizard box similar to the described above will appear on your screen. However, in this wizard box the **Merge** option will not be available. You can use this wizard box to overwrite or skip the detected settings file of Kaspersky AV Updater.

2.3. Uninstalling

Should you for any reason wish to uninstall the Kaspersky Anti-Virus® Personal program, select **Remove** in the **Program Maintenance** dialog box and press **Next**.

The removal confirmation dialog box will appear on your screen. Press **OK** to start the removal procedure. The program files will be removed from the computer; the process is indicated by the progress bar in the **Setup Status** dialog box.



Should the removal program detect files that may be used by other programs, the file removal confirmation dialog box will appear on your screen. Press **Yes** to remove the files.

CHAPTER 3. KASPERSKY ANTI-VIRUS[®] SCANNER


Kaspersky Anti-Virus[®] Scanner (Kaspersky AV Scanner) is an anti-virus program that checks for viruses and deletes them on demand.

The program performs the following functions:

- Detects and deletes viruses of all types in files located on user-predefined disks, in boot sectors and RAM
- Detects and deletes viruses from files that have been packed using PKLITE, LZEXE, DIET, COM2EXE and other compression utilities
- Detects viruses (but doesn't delete) in archived files that have been archived using one of the commonly used archivers, including ZIP, ARJ, LHA, RAR, etc.
- Detects viruses (but doesn't delete) in local mailboxes of the most commonly used mail systems: Microsoft Outlook, Microsoft Exchange, Microsoft Internet Mail, Eudora Pro & Lite, Pegasus Mail, Netscape Navigator Mail, JSMail SMTP/POP3 server.
- Detects and deletes viruses from the MS Outlook Express v. 5.0 (and later) mail databases.
- Utilizes an improved heuristic detection tool that is able to search for unknown viruses (up to 92% effective).

3.1. Starting Kaspersky Anti-Virus[®] Scanner

You can start Kaspersky Anti-Virus[®] Scanner from:

Option 1: The Windows main menu. To do this, press the **Start** button, point to **Programs**, point to **Kaspersky Anti-Virus[®]** and point and click **Kaspersky Anti-Virus[®] Scanner**. The program main window will appear on your screen (see subchapter □), and you will see the scanner icon  in the system tray. Right-click this icon to display the scanner system menu (see subchapter 3.2.1).

Option 2: Kaspersky AV Control Centre. To do this, you must first create the appropriate task. This task can be started manually or scheduled to start automatically.

Option 3: The command line. To do this, you must press the **Start** button in the Windows taskbar, point and click **Run**, define the full path to the file `avp32.exe` in the **Run** dialog box and press the **OK** button. For example,

```
C:\Program Files\Kaspersky Lab\Kaspersky Anti-Virus  
Personal\Avp32.exe.
```

If you decide to start your anti-virus scanner from the command line, you can use one of the following available switches:

[/?] or **[/H]** – displays the complete list of available command line switches;

[/P=filename] – starts Kaspersky AV Scanner with settings from the defined file;

[/S] – sets Kaspersky AV Scanner to check for viruses right after the program is started;

[/W] – sets Kaspersky AV Scanner to create a report file;

[/N] – minimizes the Kaspersky AV Scanner main window once the program is started;

[/Q] – sets Kaspersky AV Scanner to close the main window once the scanning operation is complete;

[/D] – does not launch Kaspersky AV Scanner from being started, if the data volumes have already been successfully checked that day (that is, if Kaspersky AV Scanner has already scanned the drives and the operation was not aborted and no viruses were detected);

[/@[!]=filename] – sets Kaspersky AV Scanner to scan for viruses in those files and/or folders listed in the defined file. The file defined by this switch must be in common text format (ASCII) and must contain a list of files and/or folders intended for scanning. Every line of the list should contain only one file or folder name (with a complete path indicated). If there is the character "!" in the switch (i.e. `/@[!]=filename`), the defined file will be deleted once the scanning operation is complete. If the character "!" is not used (i.e. `/@=filename`), this file won't be deleted;

[/redundant] – enables the redundant scan tool (for details refer to subchapter A.2). Redundant scanning is recommended if no virus was detected during an ordinary scan but the system is still behaving strangely (for example, there are frequent instances where the computer restarts by itself, unnaturally slow performance of applications, and so on). Otherwise, we do not recommend enabling the redundant scan tool as it noticeably slows down the scanning rate;

[virlist=filename] – creates a file with the defined name that will contain the list of viruses currently detectable by Kaspersky AV Scanner.

[filename and foldername] – sets Kaspersky AV Scanner to scan for viruses in those files or folders. If a file name or a folder name have spaces, they must be enclosed in quotation marks. The * or ? symbols cannot be used in file names, i. e., the *.exe or av?32.exe names cannot be written.



If a folder or a file name with a list of files (**/@=file_list.lst**) is indicated in a command line, scanning starts automatically without the **/S** key.

[/EL] excludes from the check the objects indicated in the “file_name” file of the **[/@!=filename]** parameter.

[/EF] – sets Kaspersky AV Scanner to ignore those files defined in the command line. The switch /EF can be also used in a file defined by the switch **/@=filename** (see above). In this case the object (file or folder) listed together with the switch /EF will be ignored by Kaspersky AV Scanner. If the name of the listed file contains spaces, the switch /EF must precede the filename (the switch can follow the filename, but in this case the filename must be enclosed with quotation marks). If the name of the listed file doesn't contain spaces, the switch /EF can be positioned anywhere in the line.



By using combinations of the switches **/EF**, **/EL**, **/@** and the list of files and folders in the command line you can define various locations to be checked.

Let's consider some examples of switch applications:



Example 1. Starting the program preset to check for viruses in files within the **My documents** folder.

```
C:\Program Files\Kaspersky Lab\Kaspersky Anti-Virus  
Personal\Avp32.exe" /S "C:\My documents"
```



Example 2. Starting the program preset to create a list of detectable viruses in the file **E:\virlist.txt** and to close the main window once the scanning operation is complete.

```
C:\Program Files\Kaspersky Lab\Kaspersky Anti-Virus  
Personal\Avp32.exe" /virlist=E:\virlist.txt /q
```



Example 3. Starting the program preset to check for viruses right after it is started, if Kaspersky AV Scanner has not scanned for viruses that day or if it has but the scanning operation was aborted or viruses were detected. The program is also set to close the main window once the scanning operation is complete.

```
C:\Program Files\Kaspersky Lab\Kaspersky Anti-Virus  
Personal\Avp32.exe" /s/d/q
```




Example 4. Starting the program preset to check for viruses in files in the **My documents** folder and to ignore the files listed in the file *exclude.txt*.

```
"C:\Program Files\Kaspersky Lab\Kaspersky Anti-Virus
Personal\Avp32.exe" "C:\My documents" /EL
/@=C:\exclude.txt
```

3.2. Program Interface

3.2.1. System menu

When you start the program the main window (see subchapter □) appears on the screen, and the icon  is displayed in the system tray; by clicking with your right mouse button on it you can display the system menu (Figure 1). The system menu contains the following commands:

- **Kaspersky Anti-Virus® Scanner Settings** – displays the program main window.

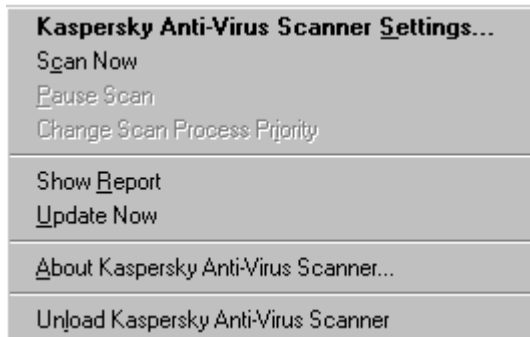


Figure 1. System menu

- **Scan now / Stop scan** – initiates/aborts scanning
- **Pause Scan / Resume Scan** – pauses/resumes scanning
- **Change Scan Process Priority** – allows you to change the check priority (this command is available during the check).
- **Show Report** – displays the report window with the program performance results.

- **Update Now** – launches Kaspersky AV Updater, the program for updating anti-virus databases.
- **About Kaspersky Anti-Virus® Scanner** – displays information about the program.
- **Unload Kaspersky Anti-Virus® Scanner** – unloads the program from memory.

3.2.2. Main window

In the Kaspersky AV Scanner main window, you can change scanning settings, start/stop scanning and review the program performance results. You can exit the main window without unloading the program from memory.

The following items are located in the Kaspersky AV Scanner main window: menu bar, tool bar, work area, and status bar. Below, these items are described in detail.

3.2.3. Menu











The menu bar is located at the top of the main window. Some menu commands can be also activated using appropriate key combinations or buttons in the tool bar (see subchapter 3.2.4). The appropriate key combinations are displayed at the left of the menu commands. For details of the matching functions of key combinations, tool bar buttons and menu commands, see subchapter 3.2.4.

Menu → commands	Function (The command allows you to...)
File → Open Profile	load settings from the current profile (see subchapter 3.3.4).
File → Save Profile	save current settings to the current profile (see subchapter 3.3.4).
File → Save Profile As	save current settings to an alternative profile (see subchapter 3.3.4).
File → Save Profile as Default	set the current settings as the default (see subchapter 3.3.4).
File → Recent Profiles	select the profile from a list of files recently used.

Menu → commands	Function (The command allows you to...)
File → Unload Kaspersky Anti-Virus® Scanner	unload the Kaspersky AV Scanner program from memory.
File → Close window	exit the program main window.
Scan → Start Now / Stop scan	start / stop scanning for viruses (see subchapter 3.4.1).
Scan → Pause Scan / Resume Scan	suspend / resume scanning for viruses (see subchapter 3.4.1).
Scan → Change Scan Process Priority	change the active scanning process priority (this item is available only during the scanning process – see subchapter 3.4.2).
Scan → View Scan Options	display the program settings in plain text form (see subchapter 3.3.5).
Tools → Update Now	update anti-virus databases (see subchapter 3.5).
Tools → Show Report	display the report window (see subchapter 3.4.3).
Tools → Make Virus List	generate a list of currently known viruses (see subchapter 3.6).
Help → Contents	display the Help topics window.
Help → Kaspersky Anti-Virus® on the Web	start your web browser and go to the Kaspersky Labs site.
Help → About Kaspersky Anti-Virus® Scanner	display information about the program.

3.2.4. Tool bar

Buttons are located in the tool bar. By pressing them you can initiate various commands.

Button	Menu → Command	Function (The button allows you to...)
	File → Open Profile	load settings from the required profile.
	File → Save Profile	save current settings to a profile.
	File → Save Profile as Default	save current settings to a file and set this file as the default profile.
	Scan → Start Now	start scanning for viruses.
	Scan → Pause Scan / Resume Scan	suspend/resume scanning.
	Scan → Stop scan	stop scanning for viruses.
	Scan → View Scan Options	display settings in plain text form.
	Tools → Show Report	display the report window
	Tools → Update Now	update Anti-Virus bases.
	File → Unload Kaspersky Anti-Virus® Scanner	unload the Kaspersky AV Scanner program from memory.

3.2.5. Work area

The main window work area is divided into two frames. The left frame contains icons with the following names: **Objects**, **Options**, **Customize** and **Statistics**. The right frame displays the settings corresponding to the left-frame icon that is currently pressed.

The **Objects** frame allows you to define a location to be checked (the list of drives and folders), objects to be checked (e.g. sectors, files, mail databases), and rules to be followed while handling infected objects (see subchapter 0). All these settings are arranged into a special control element, the *objects settings hierarchy*.

The **Options** frame allows you to define certain general settings, and you may use a *settings tree* in the **Customize** frame to define advanced settings of your Kaspersky AV Scanner (see subchapters 3.3.2, 3.3.3).

The **Statistic** frame displays a table with the scanner performance statistics (see subchapter 3.4.4).

Each item of the settings tree has a right-click menu with commands applicable to the item.



To display the right-click menu of an item in the settings tree,

1. Place your mouse cursor on the required item.
2. Click your right mouse button. The appropriate right-click menu will appear on your screen (Figure 2).

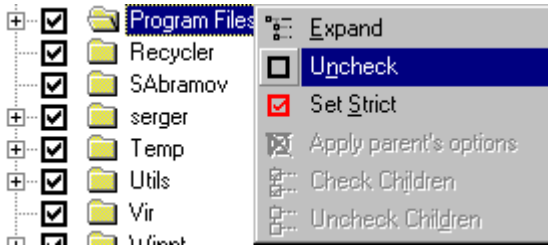


Figure 2. An example of the right-click menu

3.2.6. Status bar

At the bottom of the Kaspersky AV Scanner main window you can find a *status bar*. The status bar displays the following information:

- context-sensitive prompts / name of the examined object;
- indicator of the scanning progress.

3.3. Changing Settings

In this subchapter we describe how to customize all scanning parameters used by Kaspersky AV Scanner.

3.3.1. Scanning parameters for objects.

Objects category

The **Objects** frame (Figure 3) in the work area allows you to choose locations and objects to be checked for viruses. You may do this by selecting appropriate options in the frame hierarchies. These options may be viewed in the following two modes: **Standard** and **Expert**. To switch between these modes use the corresponding buttons in the left frame of the window work area.

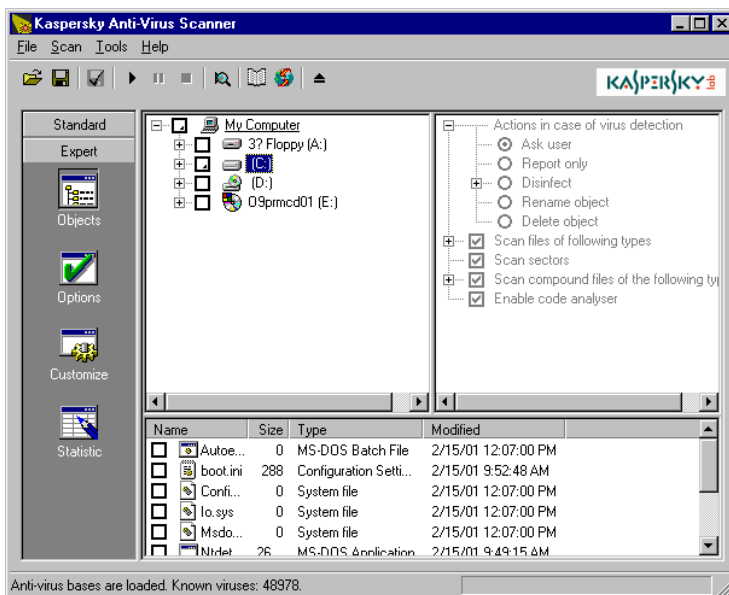


Figure 3. The **Objects** frame

With the Standard mode enabled the **Objects** frame is divided into two sub-frames: in the left sub-frame you may see the list of computer disks, and the right sub-frame displays settings for the item selected in the left sub-frame list (Figure 4).

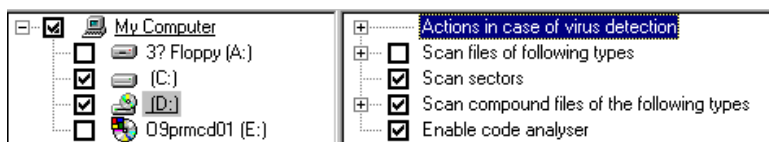


Figure 4. The Standard view mode

With the Expert mode enabled, the **Objects** frame is divided into three sub-frames: in the upper left sub-frame you can find the file system hierarchy, the upper right sub-frame displays settings for the item selected in the upper left sub-frame hierarchy, and the lower sub-frame displays the list of files located in the root of the object selected in the upper left sub-frame (Figure 5).

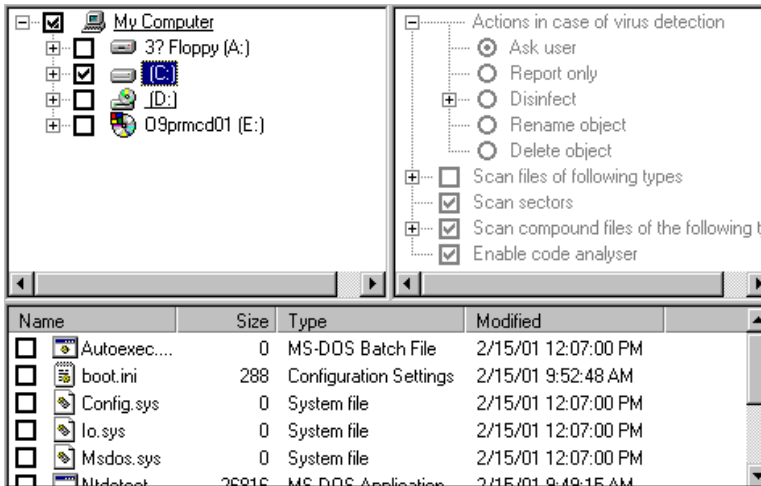


Figure 5. The Expert view mode

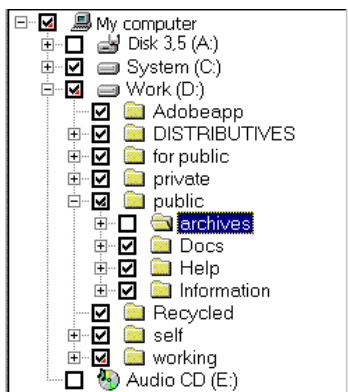
Use the upper left sub-frame to define the location that must be checked for viruses. Check a box to define the corresponding object to be checked. If you uncheck the box , the corresponding object will be skipped during the check.

To scan a certain location within the file system, check the corresponding box to the left of the location name.

To scan a group of disks, check the **My Computer** box in the upper left sub-frame and the required boxes in the upper right hierarchy:

- Scan local removable disk drives** – scans all removable disks. This check box is available only if you checked the **My Computer** box in the upper left sub-frame. If this box is checked, the program will scan all removable drives.
- Scan local hard disk drives** – scans all local hard disks. This check box is available only if you checked the **My Computer** box in the upper left sub-frame. If this box is checked, the program will scan all local hard disks.

If you select the option to scan a certain location within your file system, Kaspersky AV Scanner will automatically scan all the locations within the selected one. However, when in the Expert view mode you can mark the required sub-locations to be excluded from the check.



For example, you defined the disks **C:** and **D:** to be checked for viruses, but you do want the **D:\public\archives** directory to be excluded from the location defined to be checked. In this case you must check the **C:** and **D:** boxes, and then, in the hierarchy for the **D:** disk, uncheck the **archives** box.


If you excluded a folder from the location to be checked, a triangle will appear in the checked boxes of all the parent locations: instead of . If you excluded a certain location from the larger location that is defined to be checked for viruses, the scanner will not check it at all or will not check it using the rules defined for the parent location. You may eliminate (disable) this difference inside the larger location, or keep it for a certain period of time. For details refer to subchapter 8.3.

For every defined location within your file system you can specify separate scanning settings. For every defined location to be checked you can also specify the objects to be checked by using the settings tree in the right hand pane.


3.3.1.1. Defining objects to be checked. Memory, sectors, and files

For locations that correspond to different levels of the file-system hierarchy the upper right frame displays different groups of settings. The maximum quantity of settings is displayed for the **My Computer** location. Here you can set your scanner to check your computer memory, boot sectors, groups of disks and MS Outlook Express (v. 5.0 and later) databases. When defining settings for a disk you can enable the check of boot sectors and file systems located on this disk. For a folder you cannot disable the check of file system. You can, however, define how the scanner must process infected and suspicious objects, in what type of files it must check for viruses and enable/disable the advanced scanning modes for all the locations in the upper left frame.

- Scan files of following types** – scans files in the corresponding locations (including System, Hidden and Read Only files). This check box is available if you checked the **My Computer** or a disk box in the upper left sub-frame. You cannot uncheck it for a folder or file. If you check this box you must define file types to be checked for viruses:

- All infectable** – scans all files that are able to carry a virus.
 - All** – scans every file of every type.
 - By mask** – scans the file types defined by user in the text fields below. You can specify an unlimited quantity of file types, but make sure that one text field contains only one file type.
 - Exclude by mask** – excludes from the check the file types defined by user in the text fields below. You can specify an unlimited quantity of file types, but make sure that one text field contains only one file type.
 - Scan sectors** – scans boot sectors (master boot record and boot sectors). This check box is available only if you checked the **My Computer** or a disk box in the upper left sub-frame.
 - Scan memory** – scans RAM. This check box is available only if you checked the **My Computer** box in the upper left sub-frame.
 - Scan MS Outlook Express databases** – scans MS Outlook Express (v. 5.0 and later) databases. This check box is available only if you checked the **My Computer** box in the upper left sub-frame. For details of scanning in mail databases of the other formats see subchapter 3.3.1.3.3.
-  Kaspersky Anti-Virus® Scanner checks only in those *.dbx files that are stored within the MS Outlook Express working directory and, respectively, started every time you start MS Outlook Express. The *.dbx files in other directories are considered by the program as standard mail databases. The program is able to detect viruses in those databases but cannot delete them.
- Scan start-up objects** – scans objects started at the operating system start. This check box is available only if you checked the **My Computer** box in the upper left sub-frame.

3.3.1.2. Handling infected and suspicious objects

 **Actions in case of virus detection** – if an infected or suspicious object is detected, the program will perform one of the following actions:

- Ask user**– Kaspersky AV Scanner will open up the dialog box (Figure 6). This dialog box contains the name of the infected file, the name of the detected virus and a list of possible actions to be performed with the infected object (that is, a list of all possible actions except for Ask user). In addition, the dialog box contains the **Apply to all infected objects** check box; by checking this box, you can apply the selected action to all infected objects detected later, and which you previously predefined to be handled by opening the dialogue box. Upon detection of the next infected object, the dialog box will not appear again. The following three buttons are located at the bottom of this

dialog box: **OK** (accepts the selected action), **Cancel** (closes the dialog box and proceeds with scanning) and **Stop** (stops scanning for viruses).

- ⊙ **Report only** – the program will only report the infected and suspicious objects. The report can be viewed by starting the report viewer, Kaspersky Report Viewer (see Chapter 7).
- ⊙ **Disinfect** – the program will try to cure all infected objects without asking first. As a result, the detected viruses will be removed, and the object will be restored as an operable one.
- Make backup file before disinfection** – to create a copy of the infected object before starting a cure. A directory where the copy will be created is specified in the settings tree of the **Options** category (see subchapter 3.3.2.2). The copy will not be deleted upon completion of treatment.
- If disinfection is impossible** – not all infected objects can be cured, because some viruses damage computer data irreversibly. In this case, Kaspersky AV Scanner can operate using one of the following three methods: ⊙ **Report only** – informs you about unsuccessful attempts at treatment, ⊙ **Rename object** – renames the unrecoverable file, ⊙ **Delete object** – deletes the damaged file.
- ⊙ **Rename object** – the program will rename all infected objects. The renaming rules are specified in the settings tree of the **Options** category (see subchapter 3.3.2.2).
- **Delete object** – the program will delete all infected objects without warning.

The **Delete object** and the **Rename object** options are applied to compound infected files only if you checked the **Enable delete or rename non-disinfected compound files** box on the **Options** page. If the box is not checked the program will not delete or rename compound files.

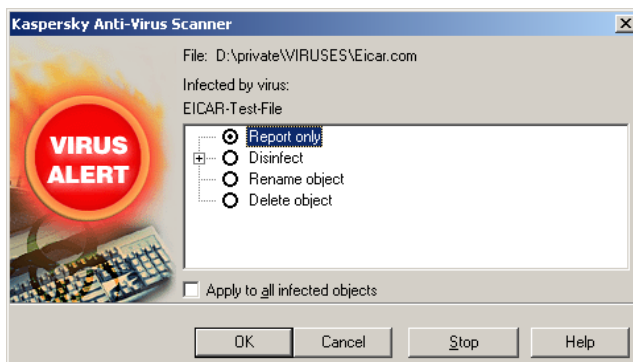


Figure 6. The **Ask user** dialog box

3.3.1.3. Advanced scanning modes

3.3.1.3.1. Scanning compound objects

You can enable advanced scanning modes to check for viruses in archives, packed files, mail databases and plain mail formats (for details see Appendix A).

- Scan compound files of the following types** – check this box to process compound objects as folders containing a set of objects.

Sometimes the program is able to detect a virus in a compound file (archive, mail database, plain mail file) but cannot remove it from the file. Therefore when you run the program with the **Delete objects** or **Rename object** option button selected it's advisable that you check the **Scan compound files of the following types** box and uncheck the **Enable delete or rename non-disinfected compound files** box on the **Options** page. In this case, if there was detected an infected compound file, the program will log this event but the file will not be deleted or renamed. Later on you will be able to extract the object, check it with your anti-virus program and delete the virus from extracted files.



If you check the **Enable delete or rename non-disinfected compound files** check box, you can lose important data.

3.3.1.3.2. Scanning archives and self-extracting files

Scanning archives for viruses is an extremely important task because a virus can be stored in an archived file for several months or even years, causing no harm to your computer. However, if activated, this virus can cause serious problems.

- Archives** – check this box to search for viruses in files archived using ZIP, ARJ, LHA, RAR, CAB and some other archiving utilities.

Kaspersky Anti-Virus® is able only to detect viruses from archives. In addition, Kaspersky Anti-Virus® does not extract password-protected archives.

- Archives with self-extractors** – check this box to search for viruses in self-extracting archives, i.e. executable files that can be started to extract the archived files. Some self-extracting archives also immediately start one of the extracted files.

The extracting tool is able to correctly extract files that have been compressed multiple times. It can also deal with some versions of immunizers, programs protecting executable files from viruses by attaching checking code blocks (CPAV and F-XLOCK) and enciphering programs (CryptCOM) to them.

3.3.1.3.3. Scanning mail databases and plain mail files

The program is able to search for viruses in mail databases and plain mail files.

- Mail databases** – check this box to search for viruses in mail databases of the following formats:
- Microsoft Outlook, Microsoft Exchange (the .pst and the .pab extension files, the MS Mail archive type);
 - Microsoft Internet Mail (the .mbx extension files, the MS Internet Mail archive type).
 - Eudora Pro & Lite;
 - Pegasus Mail;
 - Netscape Navigator Mail;
 - JSMail SMTP/POP3 server (user database).



If the mail database scan mode is enabled, the program checks every entry in mail databases and scans attached files. The following formats are supported: UUEncode; XXEncode; btoa (up to 5.0); btoa 5.*; BinHex 4.0; ship; NETRUN 3.10; NETSEND 1.0 (not packed); NETSEND 1.0C (packed); MIME base 64.

- Plain mail** – check this box to search for viruses in plain mail files of the formats Eudora Pro & Lite, Pegasus Mail, Netscape Navigator Mail, JSMail, and user databases on SMTP/POP3 servers.



If the plain mail check mode is enabled, Kaspersky Anti-Virus® checks every file for a message header. If a message header is detected, the program searches for attached data (UUEncode, XXEncode and etc.) and checks it for viruses.

The mail database and plain mail modes noticeably slow down the Kaspersky AV Scanner scanning rate. For that reason we do not recommend their use in regular virus checks.



Kaspersky AV Scanner is not able to delete viruses from mail databases and plain mail files, it is able only to detect them. However, if you check the **Scan MS Outlook Express databases** box, the program will be enabled to detect and delete viruses from MS Outlook Express (5.0 and later) databases.

3.3.1.3.4. Scanning embedded objects

The program allows you to check for viruses not only in files, but also in the objects embedded in these files using the OLE technology. Check the **Embedded objects** box to search for viruses in OLE objects embedded in the examined files.

3.3.1.3.5. Heuristic detecting module

You can enable the built-in heuristic detection module to scan for viruses that are unknown to the program (not described in current anti-virus databases). Check the **Enable Code Analyzer** box to scan for viruses using the heuristic detecting module.

3.3.2. General settings: *Options*

The **Options** frame (Figure 7) contains options allowing you to choose how the scanner should report performance statistics and rename the infected files it detected. Here you can also set the scanning priority.

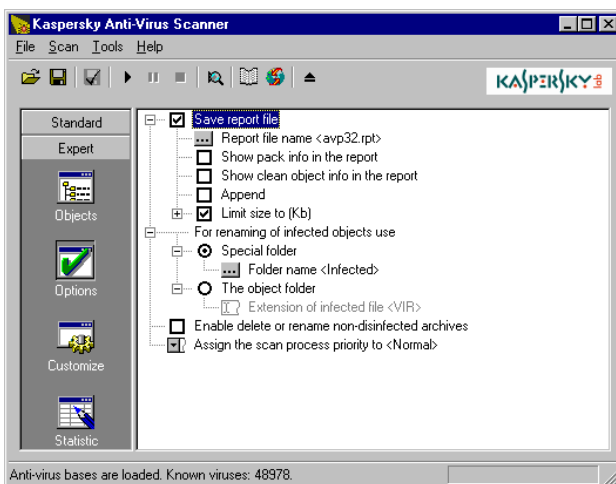



Figure 7. The **Options** frame

3.3.2.1. Reporting options

- Save report file** – check this box to save the report to a file. If you check this box, you will be able to monitor the performance of Kaspersky AV Scanner using Kaspersky® Report Viewer (see Chapter 7). When displaying the performance results, this program will use settings defined in the **Save report file** branch.

 **Report file name** – use this field to define the report file name



By default the report file is created in the directory that you specified during program installation. If the program operates independently of Kaspersky AV Control Centre, you can re-define this directory by specifying the full path to your report file. If the program is controlled by Kaspersky AV Control Centre, you cannot re-define this directory.

- Show pack info in the report**– check this box to receive reports about packed and archived objects. These messages have the following format in the Kaspersky® Report Viewer table: the **Object** column shows the object name, the **Result** column shows the **Packed** or **Archive** strings and the **Description** column shows the name of the corresponding compressing or archiving utility.
- Show clean object info in the report** – check this box receive reports about virus free objects. These messages have the following format in the Kaspersky® Report Viewer table: the **Object** column shows the object name, the **Result** column shows the **OK** string.
- Append** – check this box to append new reports to the existing report file. This is useful if you want to keep reports on several or all the previous checks. If the box is not checked, every time Kaspersky AV Scanner is started it will create a new report file.
- Limit size to (Kb)** – check this box to limit the size of the report file to the value specified in the field below. The default value is 2048 Kb.

3.3.2.2. Renaming, copying, and deleting options

- For renaming or copying of infected objects use** – these option buttons allow you to choose between moving infected objects to a special folder and renaming them. The program will apply this setting to those objects, for which you selected the **Rename object** option in the **Objects** settings tree (see subchapter 3.3.1).
- Special folder** – this option button moves infected objects to a special directory defined in the text field below. In this case, infected objects are moved to the folder with their names and extensions unchanged.

- The object folder** – this option button renames infected objects, i.e. changes their extensions to the one defined in the **Extension of infected file** field.
- Enable delete or rename non-disinfected compound files** – check this box to allow the program to delete or rename infected archives. This check box is used only for those compound objects for which you selected the **Delete object** or the **Rename object** options (respectively) in the **Objects** settings tree. It is not advisable to check this box, since you may lose the data that cannot be recovered without some type of recovery software.

3.3.2.3. Defining priority

- Assign the scan process priority to** – allows you to define the priority of the check. You can select one of the following three values: *High* – the operating system will transfer CPU control to your Kaspersky AV Scanner more frequently and for longer periods than to other applications; *Normal* – the CPU will pass control to your Kaspersky AV Scanner as frequently as to other applications; *Low* – the CPU control is transferred to your Kaspersky AV Scanner less frequently and for shorter runs than to other applications.

3.3.3. Advanced settings: *Customize*

The **Customize** frame (Figure 8) contains option allowing you to define advanced settings of the program.

- Use sound effects for the following events** – check this box to play sounds when checking for and deleting viruses.
 - Infected object found**– allows you to set the sound file that is played each time an infected object is detected. While selecting files in the corresponding window you can use the **Test** button to listen to them.
 - Scan process finished**– allows you to set the sound file that is played when the check is finished. While selecting files in the corresponding window you can use the **Test** button to listen to them.
- Pop-up Scanner window after scan finishes** – check this box to display the program main window with the Kaspersky AV Scanner performance statistics right after the check is finished. If your Kaspersky AV Scanner main window is closed and you started scanning for viruses from the system menu, the main window will appear on your screen right after the check is finished.
- Switch to "Statistic" tab after scan starts** – check this box to switch to the **Statistic** frame right after Kaspersky AV Scanner starts checking for viruses.

- Switch to "Statistic" tab after scan finishes** – check this box to switch to the **Statistic** frame right after Kaspersky AV Scanner finishes checking for viruses.

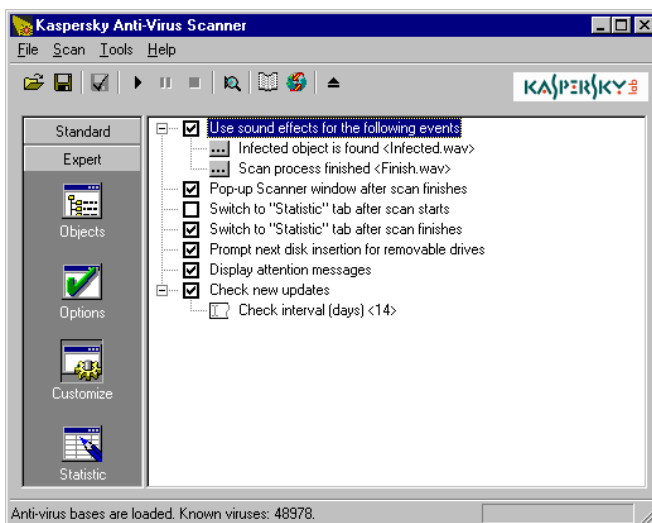


Figure 8. The **Customize** frame

- Prompt next disk insertion for removable drives** – check this box to set the program to prompt for the next removable disk. In this case Kaspersky AV Scanner will scan for viruses on the removable drive you offered and, when finished, will ask for the next removable drive. This setting is used if you preset Kaspersky AV Scanner to scan data only on the removable drive.
- Display attention messages** – check this box to display other warning messages.
- Check new updates** – check this box to automatically start the anti-virus database-updating program on a regular basis. In the **Check interval (days)** dialog box, set the required interval between two automatic starts (the dialog box is displayed right after you check this box).






If you are working with program settings from Kaspersky AV Control Centre you will not find some of the **Customize** settings listed above. These settings make no sense if you are using Kaspersky AV Control Centre.

3.3.4. Saving/loading settings

If you frequently set your Kaspersky AV Scanner a certain way, you may save these settings to a file. These settings will be stored there and if you need to set the Kaspersky AV Scanner the same way later, you can simply load them from this file. Files with Kaspersky AV Scanner settings are called scanner profiles. For example, you may want create a profile with settings allowing you to check for viruses in several diskettes one after another, or you may wish to create a separate profile with settings allowing you to thoroughly check for viruses in all the files on your computer, etc.

You can also set one profile to be loaded by default. Each time you start your Kaspersky AV Scanner it will load settings from this profile.

	Main Menu	Toolbar	Key combination
To load settings from a profile	File → Open Profile		<CTRL>+<O>
To save settings to a file	File → Save Profile, File → Save Profile As		<CTRL>+<S>
To define the profile to be loaded by default	File → Save Profile as Default		



By default, Kaspersky AV Scanner profiles have the .klr extension.

If no profile is set to be loaded by default, Kaspersky AV Scanner will use the default settings defined in the program code.

3.3.5. Previewing settings before the check

You can review your scanner settings in text form. The text describes rules specified for all the objects of your file system: from **My Computer** to separate files. For example, if the rules that your Kaspersky AV Scanner uses to check and process the autoexec.bat file differ from those used for the parent object - System disk (C:), a list of these rules will be displayed separately.

To review the text describing your Kaspersky AV Scanner settings, select the **View Scan Options** command from the **File** menu or click the toolbar button



The **Scan Options** windows containing values of the **Objects** and **Options** settings will appear on your screen (Figure 9). You can view and copy the setting values. When you finished working with this window click **OK**.



Scanner settings in text form are also written at the beginning of your report file.

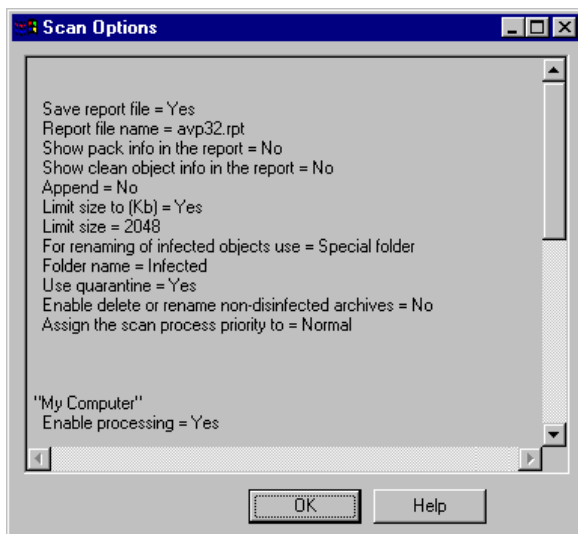






Figure 9. The **Customize** frame

3.4. Checking For and Deleting Viruses

3.4.1. Starting and aborting the check

Scanning for viruses can be initiated/terminated automatically via Kaspersky AV Control Centre, or on demand from both Kaspersky AV Control Centre, and the Kaspersky AV Scanner main window.

When Kaspersky AV Scanner starts checking for viruses, you can suspend/resume the scanning process, change the process priority or stop scanning.

	Main menu	System menu	Toolbar
Starting	Scan → Start Now	Start Now	
Aborting	Scan → Stop scan	Stop Scan	
Pausing	Scan → Pause Scan	Pause Scan	
Resuming	Scan → Resume Scan	Resume Scan	

Let's review the operations performed by Kaspersky Anti-Virus® Scanner right after it is started. First, the program loads anti-virus databases and checks itself for viruses. If the program is successfully loaded, the following string appears at the bottom of the program main window:

```
Antiviral bases were loaded. Known viruses: XXXX
```

where XXXX is the number of viruses described in the anti-virus bases. If the program is infected, it will try to disinfect itself. If the virus was successfully deleted the program will be restarted and you will see a message that all the viruses have been deleted. If the program fails to disinfect itself, it will not be started and the corresponding information window will appear on your screen. If you have the virus-free distribution copy of Kaspersky Anti-Virus®, delete the infected program and reinstall Kaspersky Anti-Virus® on your computer.



When finished checking for viruses, Kaspersky AV Scanner generates appropriate exit codes that can be used to create batch files. The program can return one of the following values:

- **0** – no viruses detected;
- **1** – scanning was interrupted;
- **2** – detected objects contain a modified or damaged virus;
- **3**—objects suspected of being viruses were detected;
- **4** – one or more viruses were detected;
- **5** – all infected objects are disinfected;
- **7** – Kaspersky AV Scanner is corrupted;
- **10**—Kaspersky AV Scanner internal error.

3.4.2. Changing priority of the check



You may change the priority of the check without aborting it. To do this, follow these steps:

1. Select the **Change Scan Process Priority** command from the **Scan** menu.
2. Select the required value (for more detail, see subchapter 3.3.2.3) from the drop-down list in the dialog box that appears on your screen (Figure 10).

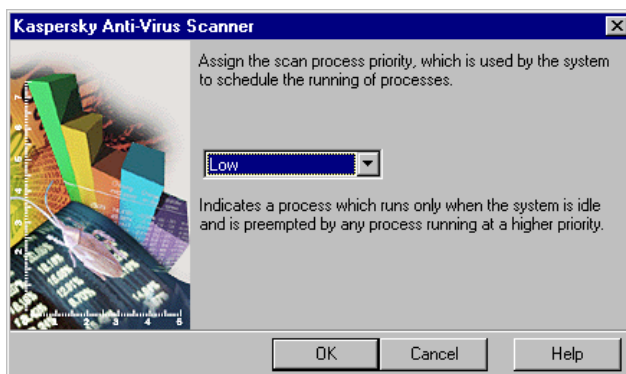



Figure 10. The scan priority dialog box



When the check is in progress you cannot change other settings! If you want to change other settings, first you must abort the check, then change settings and restart the check again.

3.4.3. Monitoring progress

If you enabled Kaspersky AV Scanner to report on its performance (see subchapter 3.3.2.1), you can use the Kaspersky® Report Viewer program to monitor the performance in progress. To start the program, select the **Show**

report command from the **Tools** menu, or click the toolbar button . The Kaspersky® Report Viewer main window allowing you to monitor your Kaspersky AV Scanner progress will appear on your screen (see Chapter 7).

3.4.4. Viewing statistics: *Statistics*

If you enabled Kaspersky AV Scanner to report on its performance you can view the performance statistics in progress in the **Statistics** frame (Figure 11).

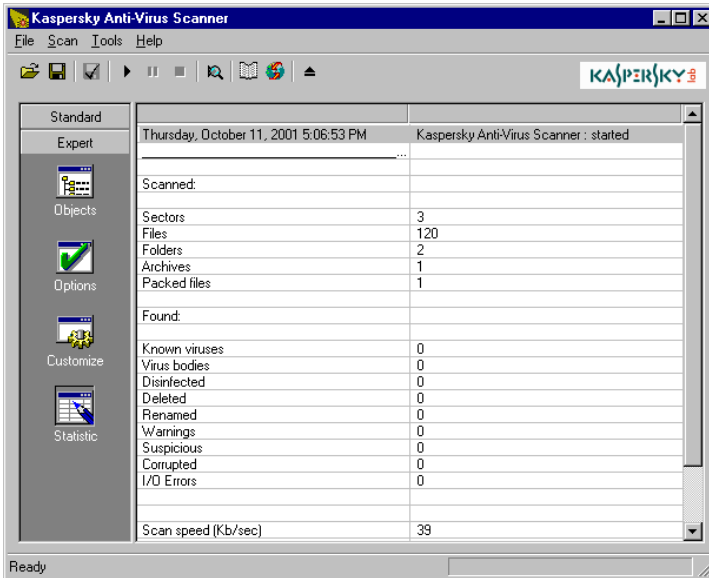


Figure 11. The **Statistics** frame


The frame table is divided into the following two sections: **Scanned** and **Found**. The **Scanned** section displays numbers of checked sectors, files, folders, archives and compressed files. The **Found** section displays the numbers of:

- viruses detected;
- virus bodies (that is, the number of files infected by a known virus);
- disinfected objects (that is, the number of objects from which viruses were correctly deleted);
- deleted objects;
- renamed objects;
- warnings, i.e. messages about objects containing codes similar to known virus modifications;
- suspicious objects (that is, Code Analyzer notifications);

- corrupted objects;
- I/O errors.

At the bottom of the frame you can see the scan speed (Kb per second) and the time that your scanner spent checking for viruses in all the objects.

3.5. Updating Anti-Virus Databases

You can start the anti-virus database-updating program from your Kaspersky AV Scanner main window. To do so, select the **Update now** command from the **Tools** menu or click the toolbar button .

3.6. Generating a List of Currently Known Viruses



You can generate and review the list of currently known computer viruses. To do this, follow these steps:

1. Select the **Make Virus List** command from the **Tools** menu. This command starts **Kaspersky® Virus List Generator**.
2. In the **Kaspersky® Virus List Generator** dialog box (Figure 12) on your screen, define the file name for the list to be saved to. To do this, use the **Browse** button.
3. Press the **Generate** button.

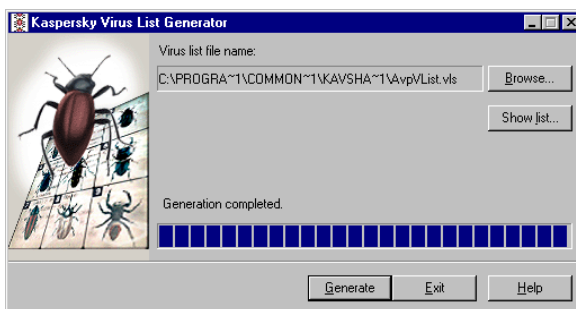


Figure 12. The **Kaspersky® Virus List Generator** dialog box

To display the list, press the **Show list** button. This button starts Report Viewer, which can be used to review the generated list of viruses.

To exit the **Kaspersky® Virus List Generator** dialog box press the **Exit** button.

You can start Kaspersky® Virus List Generator directly from the Windows main menu. To do this, press the **Start** button in the left bottom corner of your Windows screen, point to **Programs**, point to **Kaspersky Anti-Virus®** and click the **Kaspersky® Virus List Generator** command.


CHAPTER 4. KASPERSKY ANTI-VIRUS[®] MONITOR

Kaspersky Anti-Virus[®] Monitor (Kaspersky AV Monitor) is a memory-resident program that monitors files when they are accessed. Whenever somebody refers to an object, the monitor checks the object to make sure that it is free of viruses. If the object is found to be infected, the program will attempt to disinfect the object, delete it, move it to a quarantine folder or allow it to be accessed, depending on the options that were selected. In this way the anti-virus monitor allows you to detect and delete viruses before the system is actually infected.

Here we must note that there is more than one term describing programs similar to the Kaspersky Labs Anti-Virus Monitor. For example, they are sometimes called resident scanners, anti-virus filters, on-access scanners, etc.

4.1. How to start, disable and enable your AV Monitor

There are several ways to start your anti-virus monitor. Your Kaspersky AV monitor can be started:


Option 1: From the Windows **Start** menu. To do this, click the **Start** button on your Windows desktop, point to **Programs**, point to **Kaspersky Anti-Virus[®]**, then click the **Kaspersky AV Monitor** command. The monitor icon  will appear in the system tray. Click this icon with your right mouse button to display the monitor system menu (see subchapter 4.2.1).


Option 2: Automatically. The Kaspersky AV Monitor can be loaded automatically when you start your computer if you add the program to the **Startup** folder of the Windows **Start** menu.


Option 3: From Kaspersky AV Control Centre. If you install Kaspersky AV Control Centre and set your anti-virus monitor to start automatically, the program will be started right after you start Kaspersky AV Control Centre. However, in this case the monitor icon will not appear on the taskbar.


Option 4: By entering the appropriate command in the command line. To do this, go to the Kaspersky Anti-Virus[®] directory and execute the *avpm.exe* file.



If your anti-virus monitor is enabled, you can see the icon  in the system tray:

- when you place your mouse cursor on the icon , the following prompt will pop up: Kaspersky Anti-Virus® Monitor is enabled;
- the monitor system menu contains the following command: **Disable Monitoring**.

If your anti-virus monitor is disabled, you can see the icon  in the system tray:

- when you place your mouse cursor on the icon , the following prompt will pop up: Kaspersky Anti-Virus® Monitor is disabled;
- the monitor system menu contains the following command: **Enable Monitoring**.

We do not recommend that you run two anti-virus monitors from different manufacturers on the same computer. This may result in conflicts and false alarms.

If you start your anti-virus monitor from Control Centre, its options become unavailable. In this case you must use Control Centre to change your monitor settings.


4.2. Program Interface

This section describes the Kaspersky AV Monitor interface, i.e., the system menu, main window, work area, etc.



When enabled, Kaspersky Anti-Virus® Monitor can send you messages upon certain events, for example, detection of an infected object. Sometimes you have to respond to these messages. If you want to complete the current working session on your computer, close all the messages before logging off.

4.2.1. System menu

When you start your monitor the program main window will appear on your screen (see subchapter 3.2.2), and you will see the monitor icon  in the system tray. Click this icon with your right mouse button to display the monitor system menu (Figure 13). The system menu contains the following commands:

- **Kaspersky Anti-Virus® Monitor Settings** – displays the program main window.

- **Disable monitoring / Enable monitoring** – disables/enables the program to monitor for viruses in files.
- **Show Report** – displays a window containing the program performance report.
- **Update Now** – starts the anti-virus database-updating program, Kaspersky AV Updater.
- **About Kaspersky Anti-Virus® Monitor** – displays a box containing information about the program.
- **Unload Kaspersky Anti-Virus® Monitor** – unloads the program from your computer memory.

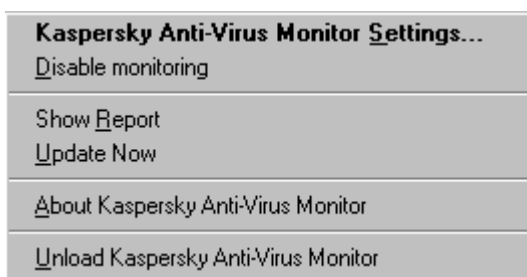


Figure 13. System menu

4.2.2. Main window

The Kaspersky AV Monitor main window allows you to change the monitor settings, to disable/enable the monitor and to view the performance statistics (Figure 14). You may close the window without unloading the program from your computer memory.

The Kaspersky AV Monitor main window contains the following items:

- menu;
- toolbar;
- work area;
- the **OK**, **Cancel**, **Apply** and **Help** buttons.

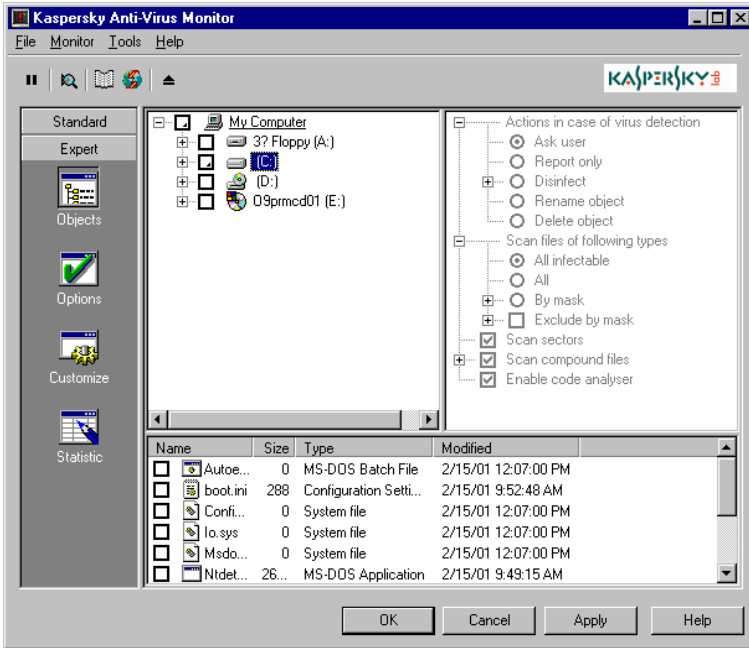


Figure 14. The Kaspersky AV Monitor main window

4.2.3. Menu



At the top of the Kaspersky AV Monitor main window you can see a *menu bar* with drop-down menus. Some commands in these menus may be substituted by appropriate key combinations or toolbar buttons. The key combination that may be used instead of a command is defined to the right of this command in the appropriate drop-down menu. For the list of key combinations and toolbar buttons that might be used instead of some menu commands refer to the table in subchapter 4.2.4.




Menu → command	Function (The menu command allows you to...)
File → Unload Kaspersky Anti-Virus® Monitor	unload Kaspersky AV Monitor from the computer memory.
File → Close window	close the Kaspersky AV Monitor main window.

Menu → command	Function (The menu command allows you to...)
Monitor → Enable monitoring / Disable monitoring	enable/disable the program to monitor for viruses (see subchapter 4.4).
Monitor → View monitoring options	display your monitor settings in text form (similar to subchapter 3.3.5).
Tools → Update Now	update your anti-virus bases (see subchapter 3.5).
Tools → Show Report	display the report window (see subchapter 3.4.3).
Tools → Make Virus List	generate a list of currently known viruses (see subchapter 3.6).
Help → Contents	display the Help topics window.
Help → Kaspersky Anti-Virus® on the Web	start your web browser and go to the Kaspersky Labs site.
Help → About Kaspersky Anti-Virus® Monitor	display information about the program.

4.2.4. Toolbar

The Kaspersky AV Monitor main window *toolbar* contains the following buttons:

Button	Menu → command	Function (The button and the menu command allow you to...)
	Monitor → Enable monitoring / Disable monitoring	enable/disable the program to monitor for viruses.
	Scan → Preview Monitoring	display your monitor settings in text form.

Button	Menu → command	Function (The button and the menu command allow you to...)
	Tools → Update Now	start the anti-virus database-updating program
	Tools → Show Report	display the report window
	File → Unload Kaspersky Anti-Virus [®] Monitor	unload Kaspersky AV Monitor from computer memory.

4.2.5. Work area

The work area of the main window is divided into two frames. The left frame contains icons with the following names: **Objects**, **Options**, **Customize** and **Statistic**. The right frame displays settings that correspond to the left frame icon that is currently pressed.

The **Objects** frame allows you to define the locations and the objects that must be checked for viruses, and to specify how the monitor must process objects that have been defined as infected. All these settings are arranged in a special control element, the *objects settings hierarchy*.

The **Options** frame allows you to define certain general settings, and you can use the *settings tree* in the **Customize** frame to define advanced settings of your Kaspersky AV Monitor (see subchapters 3.3.2 and 3.3.3).

The **Statistic** frame displays a table with the monitor performance statistics (see subchapter 3.4.4).

Each item of the settings tree has a right-click menu with commands applicable to the item.



To display the right-click menu of an item in the settings tree:

1. Place your mouse cursor on the required item.
2. Click your right mouse button. The appropriate right-click menu will appear on your screen.

4.3. Changing Settings

The options of your monitor are similar to the settings of your anti-virus scanner (see subchapter 3.3).

They differ in the following ways: in the **Objects** frame you will not find the **Scan MS Outlook Express databases** or the **Scan start-up objects** check boxes and therefore you cannot monitor the objects defined by these settings. This means that while monitoring you will not be able to disinfect mail databases. However, your Kaspersky AV Monitor will be able to detect a virus in these objects if you check the **Mail databases** and the **Plain mail** check boxes.

In the **Options** frame you will not find the **Scan process priority** option, since Kaspersky AV Monitor utilizes an operating principle that is different from that of Kaspersky AV Scanner. The **Limit size compound files to (Kb)** check box is added to the frame. This allows accelerated monitoring of large archives, etc. The numerical value for the required maximum size of a compound file to be checked must be defined in the appropriate input field near the **Limit size compound files to (Kb)** box.



Note that in this version of Kaspersky Anti-Virus® Personal, Kaspersky AV Monitor scans for viruses and disinfects ZIP archives.

In the **Customize** frame you will not find the **Pop up Scanner window after scan finishes**, **Switch to "Statistic" tab after scan starts**, **Switch to "Statistic" tab after scan finishes** and **Prompt next disk insertion for removable drives** check boxes.





If you check the **Scan sectors** and **Scan memory** boxes sectors and memory will be checked only once, when monitoring is started. In addition, if you check the **Scan memory** check box the program will monitor for viruses in the memory of launched programs. Kaspersky AV Monitor performs this check, right after it is loaded, and also every time you update your anti-virus databases. If the infected memory of a program cannot be disinfecting, the program is forced to abort.

4.4. Loading, disabling and enabling Kaspersky AV Monitor

You can manually load your anti-virus monitor from Kaspersky AV Control Centre or from the Kaspersky AV Monitor main window. You can also use Kaspersky AV Control Centre to schedule your anti-virus monitor to start automatically.

After the program has begun monitoring for viruses you can disable it, and then resume the process.

	Main menu → command	System menu	Toolbar
Disabling	Monitor → Disable monitoring	Disable monitoring	
Enabling	Monitor → Enable monitoring	Enable monitoring	

If you enabled the monitor to report on its performance you can view the statistics in progress in the **Statistics** frame (Figure 15).

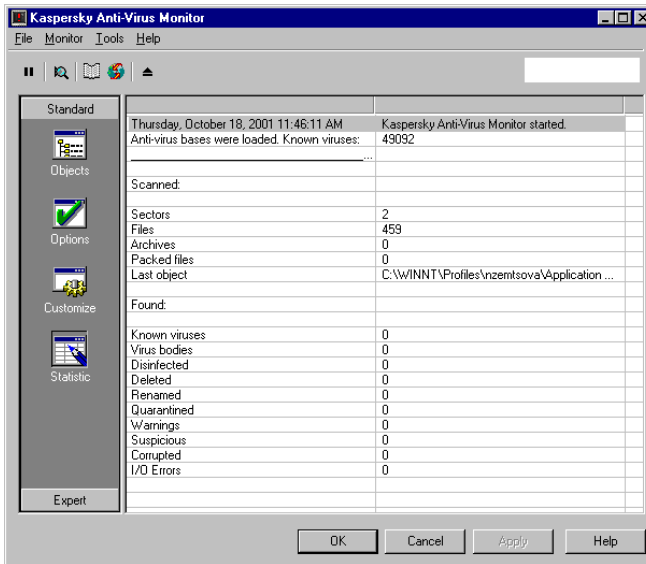


Figure 15. The **Statistic** frame

The frame table is divided into two sections: **Scanned** and **Found**. The **Scanned** section displays the numbers of checked sectors, files, folders, archives and compressed files. The **Found** section displays the numbers of:

- viruses detected;
- virus bodies (the number of files infected by a known virus);

- disinfected objects (the number of objects from which viruses were correctly deleted);
- deleted objects;
- renamed objects;
- warnings (the number of objects containing codes similar to known virus modifications);
- suspicious objects (Code Analyzer notifications);
- corrupted objects;
- I/O errors.

4.5. Updating Anti-Virus Databases

You may start the anti-virus database-updating program from your Kaspersky AV Monitor main window. To do this, select the **Update Now** command from the

Tools menu or click the toolbar button .

CHAPTER 5. KASPERSKY ANTI-VIRUS® UPDATER

The Kaspersky Anti-Virus® Updater (Kaspersky AV Updater) is used for automated updating of anti-virus databases with virus descriptions, methods of repairing infected files, and package components.

The Kaspersky AV Updater can copy anti-virus databases and executable modules from the Internet (using a network or remote connection), a Local Folder, or an anti-virus server administered by Kaspersky® Administration Kit.

5.1. How to start the Kaspersky AV Updater

There are several ways to start the Kaspersky AV Updater. You can start it:

Option 1: From the Windows Main menu. To do this, go to the **Start** menu, then to **Programs** submenu, and click on the **Kaspersky Anti-Virus® Updater** option in the **Kaspersky Anti-Virus®** group.

Option 2: From the Control Centre (automated). With Kaspersky AV Control Centre installed you can create a task to automatically start the Kaspersky AV Updater (see Control Centre chapter for detail).

Option 3: From the command line. Go to **KAV Shared Files** common folder and click on the *avpupd.exe* file. The common folder can be located at the following path: **C:\Program Files\Common Files\KAV Shared Files**.

5.2. Kaspersky AV Updater Interface

The design of the Kaspersky AV Updater interface is similar to a **Windows Wizard** and consists of a sequence of boxes (steps), which can be navigated with **Back** and **Forward** buttons. To finish updating, click on **Finish**; to close the program at any stage, click on **Cancel**.

The Tree Chart element is located in the middle of each box (see Chapter 8 for usage instructions). The control element configuration settings are grouped in a hierarchical tree.

5.2.1. Step 1. The Welcome wizard box

After the updating program has been started the Wizard will open the first wizard box – **Welcome** (Figure 16) . Checking the **Change settings** box allows you to set up the update mode, objects for updating and report options. Otherwise, the steps described below will be omitted.



Figure 16. The **Welcome** wizard box.

5.2.2. Step 2. The *Connection* wizard box

If you decide to change the default settings, you can do this in the **Connection** wizard box (Figure 17).

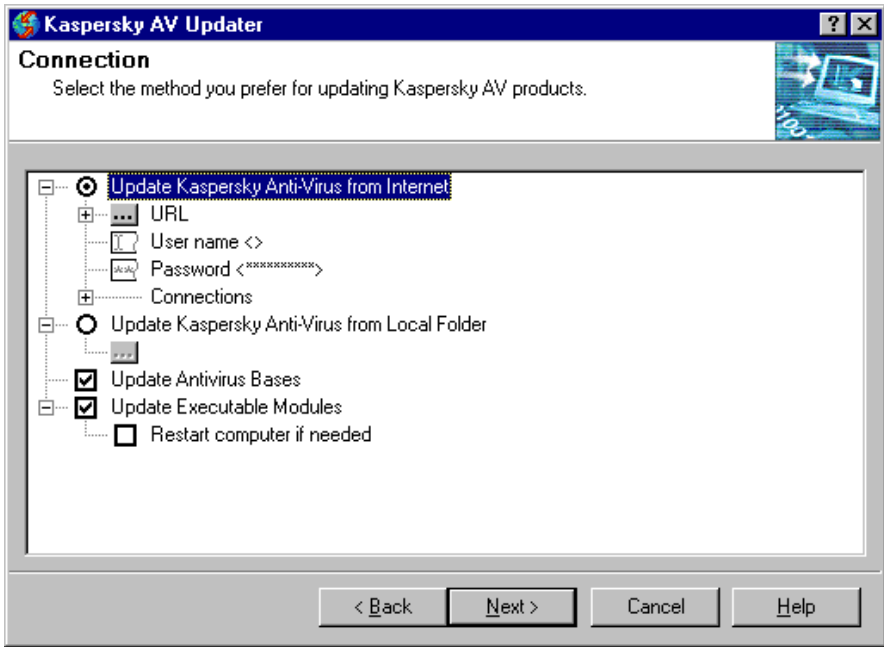


Figure 17. The **Connection** wizard box

The **Connection** wizard box allows you to define the updating mode and the object to be updated. Below we describe functions of the first-level options in the settings tree (Figure 18):

- Update Kaspersky Anti-Virus from Internet**
- Update Kaspersky Anti-Virus from Local Folder**
- Update Antivirus Bases**
- Update Executable Modules**

Figure 18. The first level of the configuration tree

- Update Kaspersky Anti-Virus® from Internet** – select this option to update via the Internet;
- Update Kaspersky Anti-Virus® from Local Folder** – select this option to update from a user-defined local folder;
- Update Antivirus Bases** – check this box to update anti-virus databases;
- Update Executable Modules** – check this box to update executable modules of the Kaspersky Anti-Virus® package.

- Restart computer if needed** – check this box to restart the computer if required after the package executable modules are updated.

When you have defined settings in this box press the **Next** button to proceed.

5.2.2.1. Updating via the Internet

If you chose to update via the Internet, expand the **Update Kaspersky Anti-Virus® from Internet** branch and define the required settings (Figure 19). Below we describe functions of the branch options.

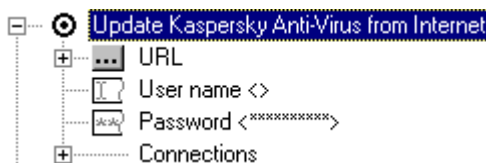






Figure 19. Options located on the Update Kaspersky Anti-Virus® from Internet branch

-  **URL** – use this button to define the source of updates (protocol, server name, etc.).
-  **User name** – use this field to define the user name allowing access to the updating server.
-  **Password** – use this field to define the password allowing access to the updating server.
-  **Connections** – use this branch to define the remote server connection settings.



If Microsoft Internet Explorer works in the Work Offline mode, the program cannot be updated via the Internet even if the connection settings have been manually adjusted.

5.2.2.1.1. Defining URL

You can download updates from one of the updating servers defined in the URL list. To view the list expand the **URL** branch of the settings tree (see Figure 20).



Figure 20. Defining the updating server address

When beginning to update, the program by default uses the first URL in the list. Other servers will be used one-by-one if the updater fails to download updates from the first URL. An error connecting to the server message will appear on your screen if the updater fails to download updates from any of the URLs in the list. If you check the **Use random URL in list as starting point** box, the program will randomly choose a URL from the list and will try to connect to this server first.

The list of URLs may be edited. To do this, press the button **...** **URL**; the **Edit URL list** dialog box will appear on your screen (see Figure 21).

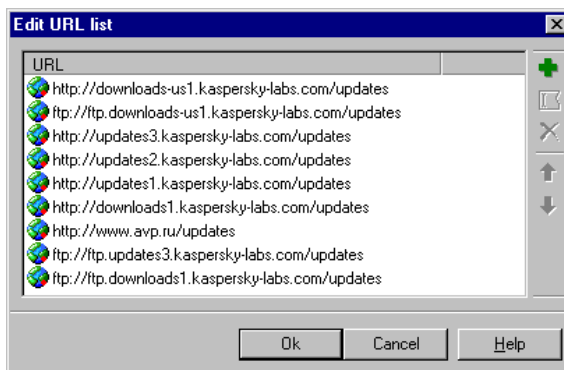





Figure 21. The **Edit URL list** dialog box

To edit the list you must use the following buttons in the dialog box (or the corresponding commands of the right-click menu):

-  – allows you to add a URL to the list;
-  – allows you to edit the URL highlighted in the list;
-  – deletes the URL highlighted in the list;



– moves the URL highlighted in the list one line up;



– moves the URL highlighted in the list one line down;

5.2.2.1.2. Defining the IP connection

Depending on the method you choose to connect to the updating server, you must define the following IP connection settings (Figure 22):

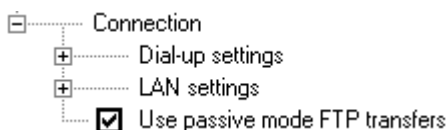


Figure 22. Defining the IP connection

- Dial-up settings – **use this branch to define the dial-up** connection to your IP;
- LAN settings **use this branch to define the** connection to your IP via the local network.
- Use passive mode FTP transfers** use passive mode when working with an FTP server (this is especially useful for those connecting to an IP via a proxy-server or a firewall).

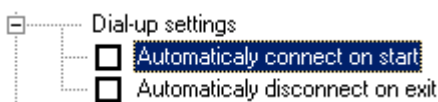


Figure 23. The dial-up options

When configuring a dial-up connection you can check the following boxes (Figure 23):

- Automatically connect on start** – dial up automatically to your IP immediately after starting the updating process;
- Automatically disconnect on exit** – disconnect automatically (switch off the modem) after the updating process is completed.

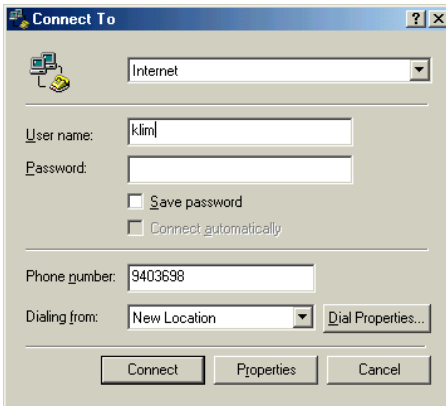


Figure 24. The **Connect To** box

If you have chosen the automated connection feature to set up a remote access to your IP, the program will enable the standard remote access utility (unless you have installed another one) after you start the updating process.

To connect to your IP fill in the **Connect To** box (Figure 24) and click on **Connect**. A remote server will be dialed and connected to. During the dial up the **Connecting to Internet** box with the **Dialing** message in the Status line will be displayed. (Figure 25).

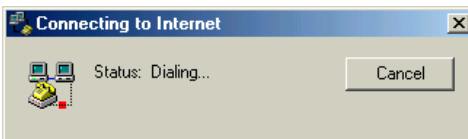


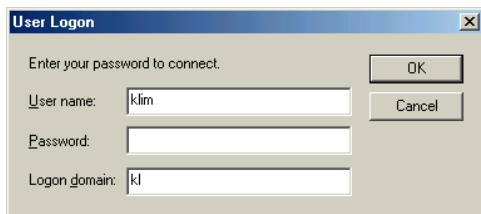
Figure 25. The **Connecting to Internet** box.
Dial-up

While dialing, the program displays the **Connecting to Internet** box with the **Dialing** message. When you have dialed in successfully, your username and password will be verified.

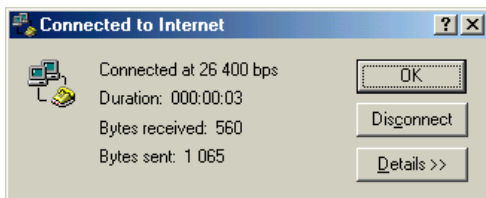


Figure 26 .The **Connected to Internet** box.
Username and password verification

In the **Status** line the message **Verifying user name and password...** will appear (Figure 26).

Figure 27. The **User Logon** box

If the user cannot be identified by his settings the **User Logon** box (Figure 27) will appear with spaces for the following connection settings to be filled in: **User name**, **Password**, **Logon domain**.

Figure 28. The **Connected to Internet** box.
Connection settings

When you have connected to the Internet, a special symbol will appear on the taskbar.

To view the connection settings double-click on the relevant icon on the taskbar (Figure 28).

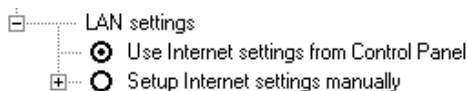


Figure 29. LAN settings

If you use a local network for your IP connection you can choose the settings from the Control Panel, or configure the connection manually (Figure 29), i.e.:

- ☉ **Use Internet settings from Control Panel** – select the connection settings defined in the Control Panel;
- ☉ **Setup Internet settings manually** – define the connection manually.



If you have chosen to define the connection manually, you must define the following settings (Figure 30):

Figure 30. The settings to be defined manually

- Use a proxy-server (Firewall)** – check this box to use a proxy-server or a firewall to connect to the IP;
 - Address** – use this field to define the required proxy-server (or firewall) address. You can define the address using the decimal notation (e.g., 125.5.29.1), or the full domain notation (e.g., test.russia.ru), or the short notation (e.g., test);
 - Port** – use this numerical field to define the proxy-server (or firewall) connection port;
- Authorization** – check this box to define the user's individual settings;
 - User name** – use this field to define the user name allowing access to the proxy (or the firewall);
 - Password** – use this field to define the password allowing access to the proxy (or the firewall);
- HTTP proxy with FTP support** – check this box to access the FTP server via the HTTP-proxy-server (CERN-proxy);

Contact your network administrator for more details about the above settings.

5.2.2.2. Updating from a local folder

If you have chosen the Local Folder as a source for updating you must give the full pathname of the folder.

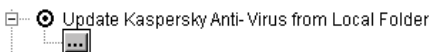


Figure 31. Update from the local folder

When you click on the button (which is outlined in Figure 31), a box will open, where you should choose the updating folder.

5.2.2.3. Choosing objects to be updated

There are the following two check boxes at the bottom of the settings tree (Figure 32):

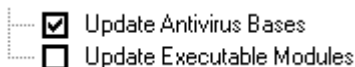


Figure 32. Choosing objects to be updated

- Update Antivirus Bases**– check this box to update anti-virus databases;
- Update Executable Modules** – check this box to update executable modules of the Kaspersky Anti-Virus® package.
 - Restart computer if needed** – check this box to restart the computer if required after the package executable modules are updated.

5.2.3. Step 3. The *Options* wizard box

In the **Options** box you can configure advanced features of the updating program (Figure 33).

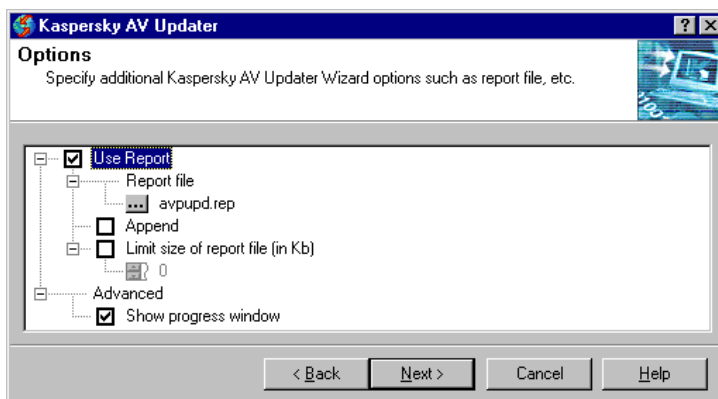


Figure 33. The **Options** dialog box

- Use Report**– check this box for the program to generate a report about the updating process.
 - Report file** – use this branch to define the report file name and the location.

- Append** – check this box to append new data to the existing report file. If you uncheck this box the program will overwrite the existing report with a new one each time the updating operation is performed.
- Limit size of report file (in Kb)** – check this box to define the maximum file size in the numerical field below. The file will be overwritten when the limit is exceeded.

Advanced – use this branch to configure the user interface;

- Show progress window** – check this box to display the updating operation progress window (see below).

Press the **Next** button to proceed with the updating operation.

5.2.4. The *Retrieving updates* window

This window (Figure 34) will appear only if you have checked the **Show progress window** box in the **Advanced** branch of the **Options** box.

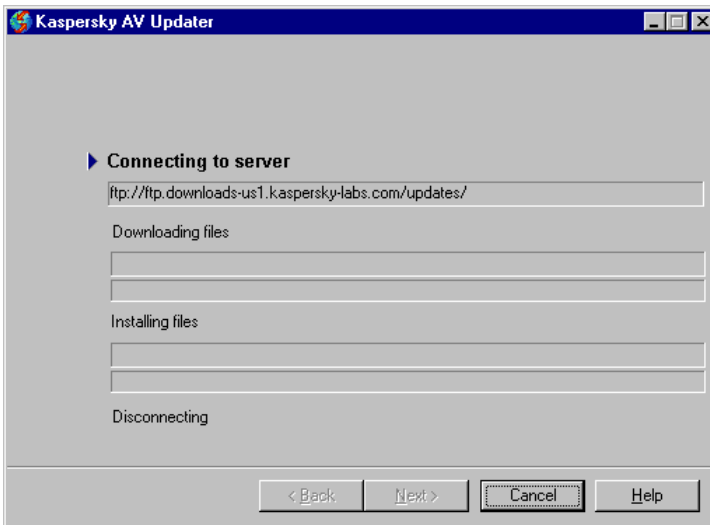




Figure 34. The **Retrieving updates** window

The window consists of four parts, showing stages of anti-virus database updating in progress:

- **Connecting to server** – connection to the source server for files to download;

- **Downloading files** – files copied from the server to the computer (the name of the copied file is displayed at the top, the percentage downloaded is displayed below);
- **Installing files...** – files are installed onto the computer (the name of the installed file is displayed on top, the scale of the updating process completion is shown below);
- **Disconnecting...** – connection session is over.

The level of completion is shown by the icon located to the left of the above messages (the icon is displayed only when the corresponding part is being updated). The  icon indicates a successful completion of this part of the updating process, while  shows that the updating program is executing this part at the moment.

5.2.5. Step 5. The *Finishing* wizard box

This is the last box (Figure 35) where you can view the updating report (click on the **Report** button) and check or uncheck the **Visit the Kaspersky Labs Web Home Page** box for the latest news about KAV products box.

Click the **Finish** button to finish a work session with the program. If you have checked the corresponding box **Internet Explorer** will automatically open the **Kaspersky Labs** web site.



Figure 35. The **Finish** box

CHAPTER 6. KASPERSKY ANTI-VIRUS® CONTROL CENTRE

The Kaspersky AV Control Centre is a component of the Kaspersky Anti-Virus® package. It performs the functions of a management shell. You can use it to install and update package components, define and schedule tasks to be started at the appropriate time, and to review the task performance results.

The program allows you to keep track of what Kaspersky Anti-Virus® components are installed on your computer, which makes it easy for you to communicate with the Kaspersky Labs technical support service, and to update your anti-virus databases and components in a timely fashion.

Using the Kaspersky AV Control Centre, you can schedule the launch of the anti-virus programs included in the package. In this way you can improve your productivity and at the same time keep your system safe from viruses.

The automated launch of the external programs allows you to use the Kaspersky AV Control Centre as a conventional task scheduler. Most commonly there is no need to use other tools of automated launch, which leads to more effective use of your computer resources. Additionally, the exact mutual synchronization of your processors is insured, provided that the processors are connected to the system's anti-virus safety system and other tasks, thus excluding the possibility of conflicts.

6.1. Launching Kaspersky AV Control Centre


There are several ways to launch your Kaspersky AV Control Centre:

Option 1: From the **Windows Main menu**: click the Start button, then go to the Programs submenu and click Kaspersky Anti-Virus® Control Centre in the Kaspersky Anti-Virus® folder.

Option 2: Automated launch at **Windows** start-up before the logon procedure (only if Kaspersky Anti-Virus® Control Centre is installed).



Figure 36. The Kaspersky AV Control Centre menu in the taskbar

When Kaspersky AV Control is successfully launched, in the taskbar notification area you will see the icon . Place your mouse cursor on it, right-click, and you will see the user menu (Figure 36), which includes the following commands:

- **Kaspersky AV Control Centre...** – displays the program main window;
- **Import settings...** – allows you to import program settings from a user-defined file (see below);
- **Export settings...** – allows you to save the current program settings to a file with the .dat extension. Later you will be able to import settings from this file (see above);
- **Help** – displays the Help topics window;
- **About ...** – displays information about the product version, the license name, the license expiration date and more (see Figure 37);
- **Exit** – exits the program.

The **Export** settings and **Import** settings commands allow you to copy Kaspersky AV Control Centre settings from one computer to another, i.e. you can set the program on a computer, then save the program settings to a file in a shared folder on the server, and later download these settings onto another computer.

At the top of the user menu above the line, you can find a list of tasks that can be started manually. To start these tasks you do not have to display the Kaspersky AV Control Centre main window; you may simply select the required command from the menu.

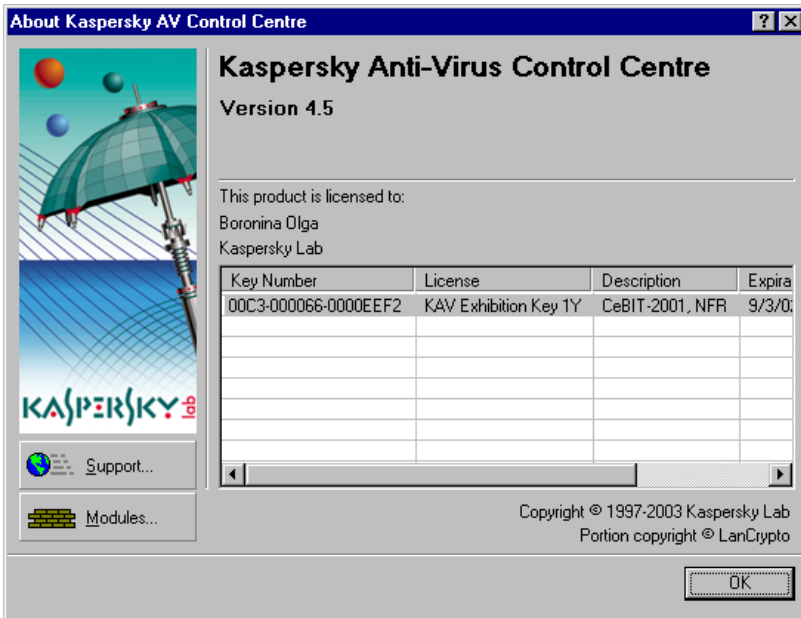


Figure 37. The **About Kaspersky AV Control Centre** box

Here we must mention some special features of the program. Kaspersky AV Control Centre is divided into the following two sub-programs: a service sub-program that is started as a system service even before the logon procedure, and an interface sub-program that provides the program's graphic interface and supports communication between a user and the program. If you unload only the interface subprogram, the tasks defined in the Kaspersky AV Control Centre settings will still be performed, but the user will not be able to edit settings and create new tasks. If you unload the service sub-program as well, Kaspersky AV Control Centre will abort the defined tasks.


Option 3: From the command line. To launch Kaspersky AV Control Centre from the command line, go to the **KAV Shared Files** folder and run **avpcc.exe**. The common folder can be located on the following path: **C:\Program Files\Common Files\KAV Shared Files**.

6.2. Kaspersky AV Control Centre Interface

The program main window contains the following four tabs: **Tasks**, **Components**, **Settings** and **Quarantine** (for details see below).

To perform various actions you can use the right-click menu or the control panel.

In the bottom of the window you can see the following buttons: **OK**, **Cancel**,

Apply and . If you press the **OK** button, the changes you made to the program settings will be saved; if you press the **Cancel** button, the changes you made will be cancelled. In both the cases the main window will be closed. If you press the **Apply** button, the changes you made will be applied and the main window will remain on your screen; in this case you can continue to change settings. For the resident tasks performed at this moment the applied settings will be immediately loaded into the executable module. To display the Help topics window press the Help button.

6.2.1. The *Tasks* tab

The **Tasks** tab (Figure 38) allows you to manage the tasks. The task is understood as a program with predefined settings that is scheduled to start at some certain time, or upon some event, or as required by the user.

The page contains three frames:

- In the left upper frame you can see each task listed with its corresponding status;
- In the right upper frame you can see the current task performance statistics¹;
- In the lower frame you can see the list of events that have occurred (errors, warnings, notifications).

Let's have a look at each frame. The task list is divided into two columns: **Name** and **Status**. In the **Name** column you will see the list of tasks, and in the **Status** column – the respective task execution status. There are several status variants:

- **Running** – the task is being executed;

¹ Program performance statistics – a short form of the report on the program performance.

- **Finished** – the task has been successfully executed;
- **Fail** – a failure occurred during execution of the task;
- **Interrupted by user** – the task was interrupted by the user;
- **Pause** – the task is suspended;
- **Start** – the task is launched;
- **Stop** – the task is stopped;
- **Start fail** – task launch error;
- **Restart** – the task is restarted.

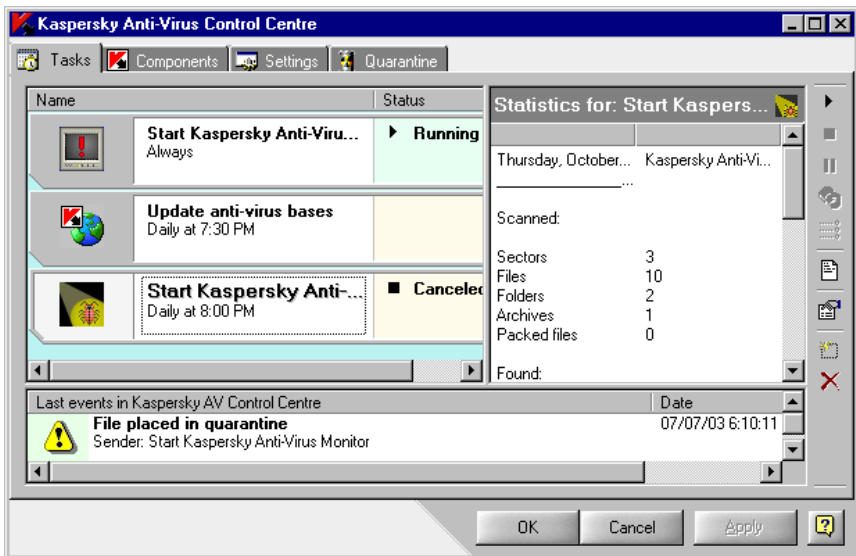


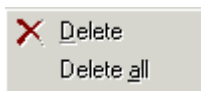
Figure 38. The **Tasks** tab

In the right part of the window you will see the statistics bar. The contents of the statistics bar depend on the task type.

Thus, for example, the automated update task has the following lines in the statistics bar: **Date**, **Time**, **Action**, **Result** and **Object**, which respectively display the date and time of the task launch, the undertaken actions and their results, and the object to which the action was applied.

At the bottom of the main window you will see a list of events with a date and a time when they occurred, and the component that generated the corresponding alert. Event alerts are delivered to Kaspersky AV Control Centre from all the

running components of the package. You may sort the list lines by any column, alphabetically or numerically, in ascending or descending order. When you select an event from the list the task that generated the corresponding alert will be highlighted.



The list has a context menu (Figure 39). The context menu items are used for the following actions:

Figure 39. Context menu in the event list

- **Delete** – deletes the selected event (with confirmation);
- **Delete all** – deletes all events from the list (with confirmation).

To carry out task management (such as creation, configuration, removal, launch, and termination) use the right-click menu, and the **Tool Panel** buttons (Figure 40).

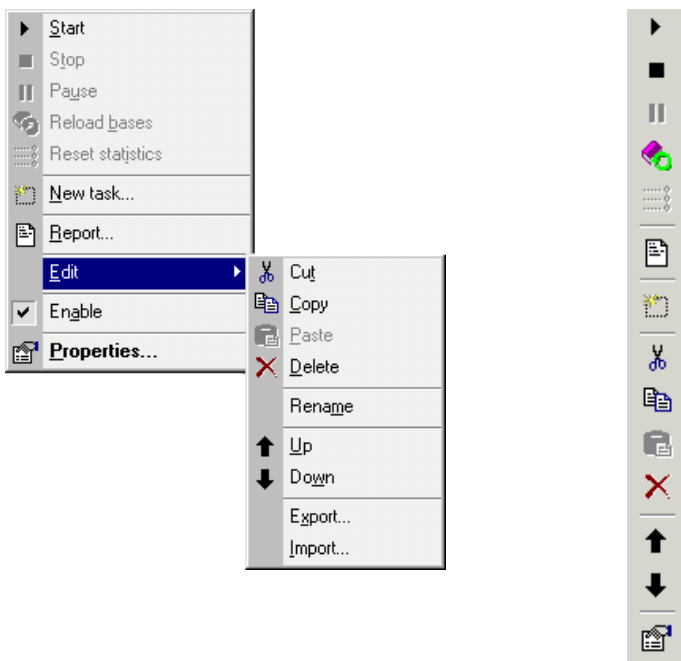


Figure 40. Right-click menu for the tasks list and the **Control Panel** on the **Tasks** tab

To open the right-click menu, click with your right mouse button in the left part of the window, where the tasks list and the status bar are located.










The right-click menu commands allows you to...

- **Start** – launch the selected task;
- **Stop** – terminate and unload the selected task that is running;
- **Pause** – pause the selected task. In this case the task is retained in memory but its performance is suspended;
- **Reload databases** – reload the anti-virus databases. This command is used when you wish to load the updated anti-virus bases into memory-resident tasks without restarting them;
- **Reset statistics** – clear the selected task performance statistics (only for memory-resident tasks);
- **New task** – create a new task. If you select this command, the New Task Wizard will be launched (see 6.3);
- **Report** – display the selected task performance report in the Kaspersky® Report Viewer window (see Chapter 7) ;
- **Enable** – enable/disable the selected task to be started as scheduled. If you disable the task, it will still be listed, but the task planner will not launch it.
- **Properties** – display the selected task settings.
- **Edit** – change the selected task settings. By pointing to this command you drop down a sub-menu with the following commands:
 - **Cut** – cut the selected task from the list and place it into the internal clipboard of Kaspersky AV Control Centre; the task name, settings, and the appropriate schedule will be saved;
 - **Copy** – copy the selected task into the internal clipboard;
 - **Paste** – paste a task from the clipboard into the program task list;
 - **Delete** – delete the selected task from the list;
 - **Rename** – rename the selected task;
 - **Up** – move the selected task one line up;
 - **Down** – move the selected task one line down;

- **Export** – save the selected task to a file. If you select this command, a window asking you to save the task settings in a file with the .tsk extension will appear on your screen;
- **Import** – download a task from a file.

The **Export** and **Import** commands allow you to copy the required task settings from one computer to another, i.e. you can create a task on a computer, then save these task settings to a file in a shared folder on the server, and later download this settings file onto another computer.

Some commands may be unavailable for some task types. The tasks are launched in the order in which they are listed. Task management, as we have mentioned above, can also be accomplished using tool bar buttons. The following buttons correspond to the right-click menu commands:


Button	Right-click menu command
	Start
	Stop
	Pause
	Reload databases
	Reset statistics
	Report
	New task
	Properties
	Delete

When you place your mouse cursor on a button, a tip describing the button function will pop up near this button.


You can use the following methods to manipulate tasks:

- *Pressing a letter key* – you can switch between the list items by pressing the key corresponding to the first letter of the target item name.
- *Using other hot keys:*

- **<INSERT>** – create a new task. If you press this key, the **New task** window will appear on your screen (for details refer to subchapter 6.3).
- **<DELETE>** – remove the task from the list (with confirmation).
- **<SPACE>** – show the selected task properties. If you press this key, the **Properties** window will appear on your screen (For details refer to subchapter 6.2.1.1).

For example, if there is a task called **Automated update** in the list, and you press the  key on the keyboard, the list pointer will move to this task.

6.2.1.1. The *Property* window

This window appears when you press the  button or select **Properties** in the context menu. The window appearance depends on the task type, which it describes.

In this product version there are the following window variants:

- The Kaspersky Anti-Virus® Scanner task property window;
- The Kaspersky Anti-Virus® Monitor task property window;
- The Kaspersky Anti-Virus® Updater window;

6.2.1.1.1. The Kaspersky Anti-Virus® Scanner task property window

The Kaspersky AV Scanner task property window (Figure 41) contains categories with a list of settings.

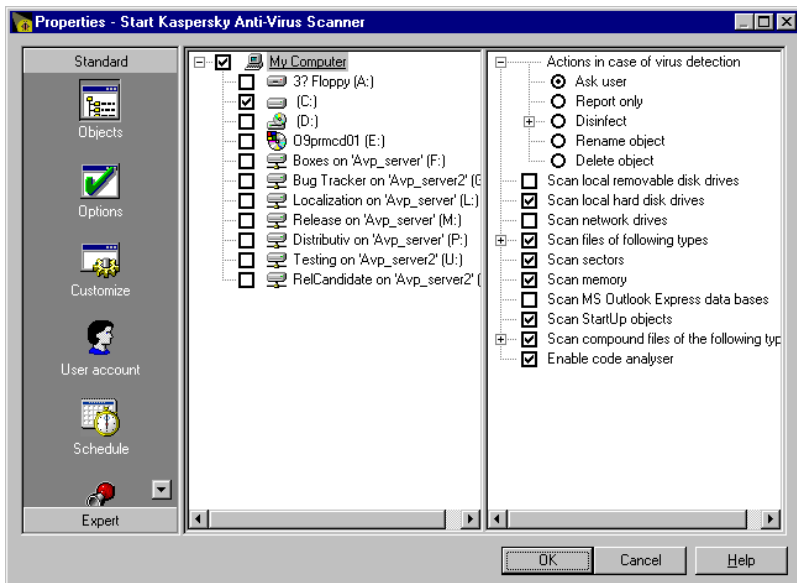


Figure 41. The Kaspersky Anti-Virus® Scanner task property window

The window contains the following categories:

Category	Reference
Objects	See subchapter 3.3.1
Options	See subchapter 3.3.2
Customize	See subchapter 3.3.3
User account	See subchapter 6.3.5
Schedule	See subchapter 6.3.3
Alerts	See subchapter 6.3.4

6.2.1.1.2. The Kaspersky Anti-Virus® Monitor task property window

The Kaspersky Anti-Virus® Monitor task property window consists of categories that contain the task settings (Figure 42). Some of the categories match those located in the corresponding component main window; other categories are specific only to Kaspersky AV Control Centre.

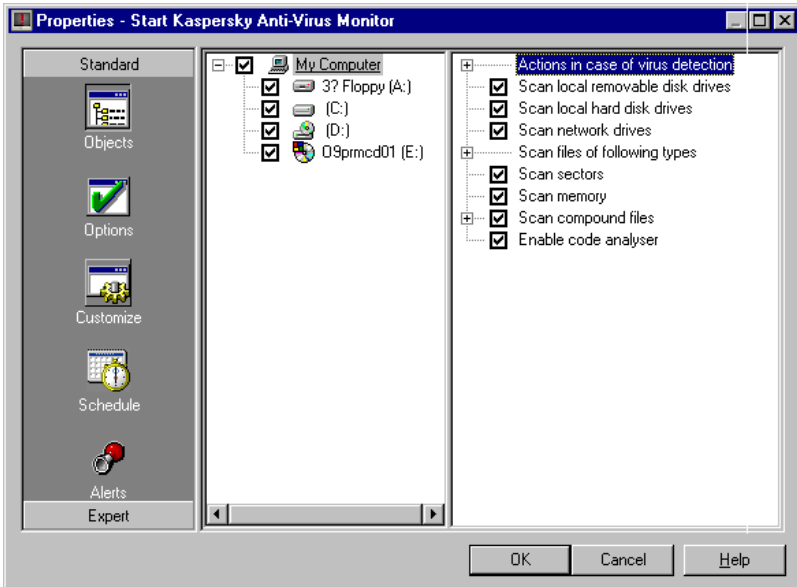


Figure 42. The Kaspersky Anti-Virus® Monitor task window

Let's explain the tab's purposes.

Category	Reference
Objects, Options, Customize	See subchapters 3.3.1, 3.3.2, 3.3.3.
Schedule	See subchapter 6.3.2.
Alerts	See subchapter 6.3.4.

6.2.1.1.3. The Kaspersky Anti-Virus® Updater task property window

The Kaspersky Anti-Virus® Updater task property window contains tabs with the task settings (Figure 43).

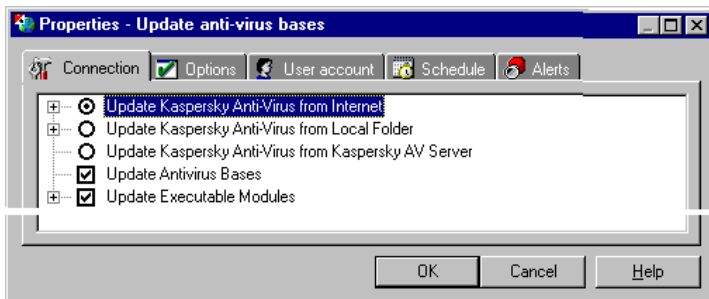


Figure 43. The Kaspersky Anti-Virus® Updater task property window

Tab	Reference
Connection	See subchapter 5.2.2
Options	See subchapter 5.2.3
User account	See subchapter 6.3.5
Schedule	See subchapter 6.3.3
Alerts	See subchapter 6.3.4



The **Connection** page in the property window contains an additional option that allows updating of your anti-virus databases and executable modules in the folder of the Kaspersky AV Server. This is the **Update Kaspersky Anti-Virus® from Kaspersky AV Server** option button.

6.2.2. The *Components* tab

The Components tab (Figure 44) contains a list of Kaspersky Anti-Virus® package components².

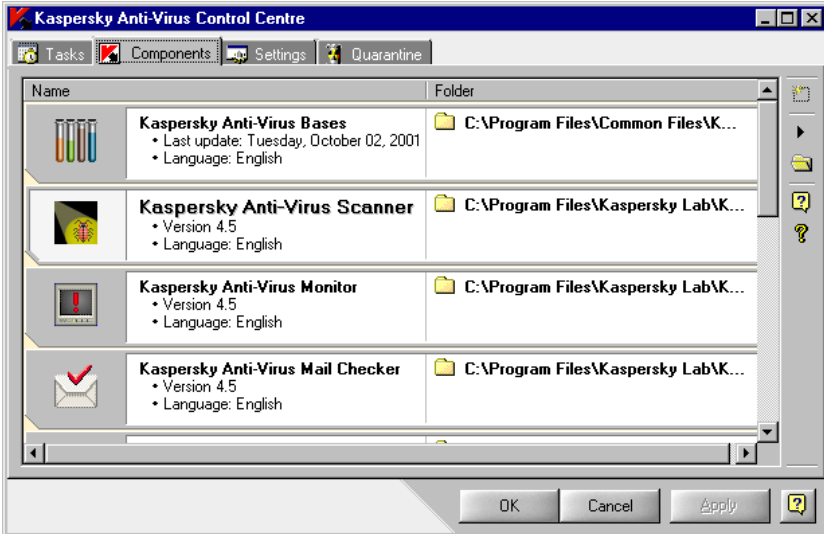


Figure 44. The **Components** tab

The tool bar is located in the right part of the tab; when you right click on it, the context menu appears (Figure 45).

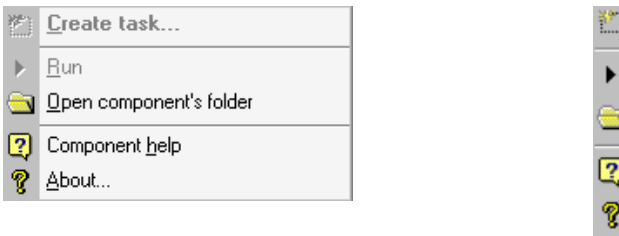







Figure 45. Context menu and the tool bar on the **Components** tab

² Component – a program, utility, library or database, included in the Kaspersky Anti-Virus package, which is responsible for a strictly limited number of tasks.

The tool bar buttons are strictly correspondent to the items of the context menu (see below).



Button	Context menu item	Description
	Create task	Creates a new task based on the selected component. If you click on this button or select this menu entry, the New task window will open (see subchapter 6.3)
	Run	Launches a task based on the selected component
	Open component's folder	Shows the component's folder in a standard window.
	Component help	Launches the help system for the selected component
	About	Displays the information about the product version, date of the last anti-virus bases update, and more. If you click on this button or select this menu entry, the About window will open.

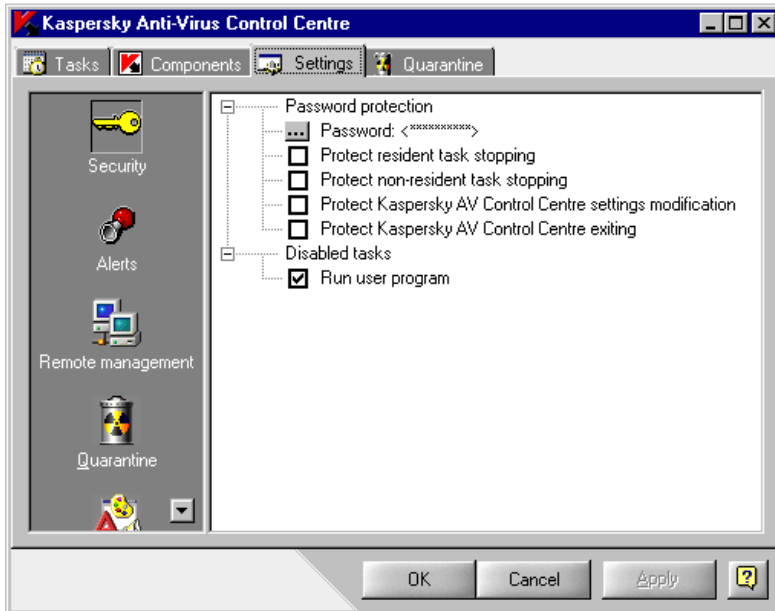
6.2.3. The *Settings* tab




The Settings tab (Figure 46) allows a user to define Kaspersky AV Control Centre settings. The settings are divided into four categories. Every category groups settings with well-defined functionality.


The list of categories (icons) is located in the left pane of the window. When you select a category, the appropriate settings tree appears in the left panel (see Chapter 8 for information about the settings tree).



If the window's size is not sufficient to display all the categories, the  and  buttons, allowing you to scroll the category list, appear at the top and the bottom of the list.

Figure 46. The **Settings** tab

Category	Function
 Security	This category contains parameters responsible for the system's safety and limiting access to Kaspersky AV Control Centre components;
 Alerts	This category contains parameters responsible for processing alerts about critical events in the Kaspersky AV Control Centre task performance;
 Quarantine	This category contains settings for the location of quarantined files on this computer or server (makes sense only if Kaspersky® Administration Kit is enabled) (see below for information about Quarantine).

Category	Function
 <p>Customize</p>	<p>This category contains user interface customization settings for Kaspersky AV Control Centre.</p>

6.2.3.1. The *Security* category



Figure 47. The **Settings** tab. The **Security** category

This category (Figure 47) is used for setup of system safety features. It is responsible for password setup and access and denial to some task types.

The Kaspersky AV Control Centre allows you to protect some running actions by a password. In that way user access to the specified commands is limited.

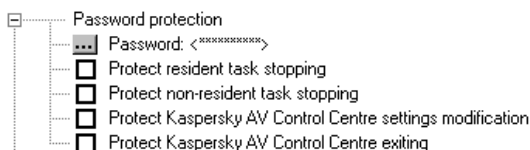


Figure 48. **Password protection** section

These features, as mentioned above, are regulated in the tree section for **Password protection** (Figure 48).

This section contains the following options:



-  **Password** – enter an administrating password for **Kaspersky Anti-Virus®** using Kaspersky Anti-Virus® Control Centre. This password will prohibit users from accessing some program functions (the list of corresponding functions is located below in the settings tree). If you press the  button, the **Change password** dialog box will appear on your screen.



Figure 49. The **Change password** dialog box

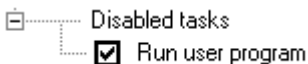
This box (see Figure 49) allows you to define and change the password. Enter your password in the **New password** text field and confirm it in the **Confirm password** text field.

- Protect resident task stopping** – If you check this box, the program will prompt for the password when somebody tries to stop resident tasks (for example, Kaspersky AV Monitor) running on the computer.
- Protect non-resident tasks stopping** – If you check this box, the program will prompt for the password when somebody tries to stop non-resident tasks (such as Anti-Virus Scanner or Kaspersky AV Updater) running on the computer.
- Protect Kaspersky AV Control Centre settings modification** – If you check this box, the program will prompt for the password when somebody tries to display the window and to change settings of Kaspersky AV Control Centre.
- Protect Kaspersky AV Control Centre exiting** – If you check this box, the program will prompt for the password when somebody tries to unload Kaspersky AV Control Centre from the memory.



When selecting a password-protected action, make sure to enter your password in the **Password** text field!

In addition, this tab allows you to disable some task types that can be dangerous, if somebody tries to remotely administer the package without any authorization (system crack).



This feature can be enabled on the **Disabled tasks** branch (see Figure 50).

Figure 50. The **Disabled tasks** branch

This product version has only one option available:

- Run user program** – If you check this box, user programs will be prohibited from starting as Kaspersky AV Control Centre tasks.

6.2.3.2. The *Alerts* category

The **Alerts** category (see Figure 51) allows you to process remotely alerts generated by the running tasks.



Figure 51 The **Settings** tab. The **Alerts** category

The settings tree contains the following options:

- Skip all alerts** – Disable the sending of alerts
- Process alerts via Kaspersky AV Server** – Send alerts using the Kaspersky AV Server, the server component of the Kaspersky Anti-Virus® remote management system
- Process alerts by Kaspersky AV Control Centre** – Send alerts using the Kaspersky AV Control Centre;

To limit the number of alerts to be generated by a single task, check the box **Maximum alerts for single task** and define the maximum value in the corresponding field.



For example, Figure 52 illustrates a situation when the maximum number of alerts is limited to 10. This means that when Kaspersky AV Control Centre receives the eleventh alert from a task, the received alert list will be automatically cleared.

If the **Process Alerts by Kaspersky AV Control Centre** option is selected, you should customize the settings for sending alerts. To enable the program to send alerts via e-mail check the **Send E-mail messages** box. Then define the following settings:

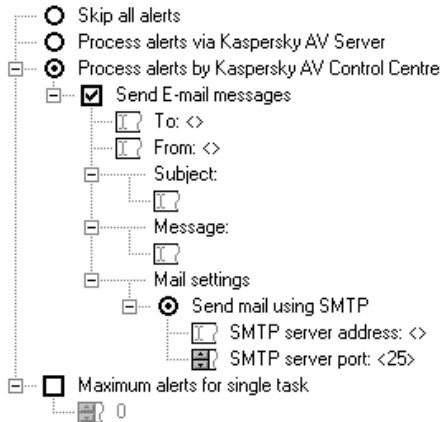


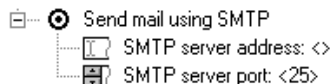
Figure 52. The **Process alerts by Kaspersky AV Control Centre** branch

- To:** Type the recipient's e-mail address in this line;
- From:** Type in the name or address to be displayed in the **From** line of an e-mail message. Any string can be the value of this line. This setting is required for work with some SMTP servers and is used for user authentication;
- Subject:** e-mail message subject;
- Message:** The message text to be sent with the e-mail;
- Mail settings** Specify the e-mail system settings for alert sending methods. There are two methods of sending:
- using MAPI;
 - using SMTP.



Contact your network system administrator for more information about SMTP and MAPI.

6.2.3.2.1. Send mail using SMTP



To send alerts using SMTP, select the **Send mail using SMTP** option (Figure 53), then select the following parameters:

Figure 53. SMTP settings

SMTP Server address

Contains the SMTP server address, which can be typed in as a decimal notation (e.g. *125.5.29.1*), or as a full domain notation (e.g. *test.mail.ru*), or a short notation (e.g. *test*);

SMTP server port

Contains the SMTP server port address. The default value is **25**.

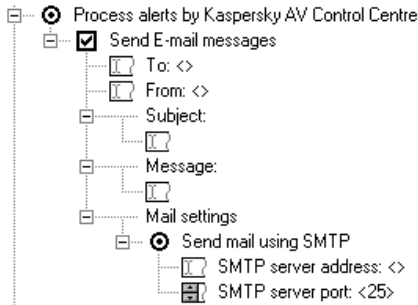
Let's study an example of tab **Alerts** settings usage. Let's say we need to set up SMS-messages sending about critical network events to the mobile phone of a system administrator via e-mail gate.

Input data:

- administrator's mobile phone number – **1234567** (direct number);
- telephone connection operator – Beeline GSM (i.e. the access code to direct phone numbers – **7 901**);
- SMTP server address – **mysmtp.home.ru**;
- SMTP server port – **25**;

Make sure that:

- The message has been sent from the Control Centre,
- The message had the Alert subject,
- The message body contained the following text: *Warning! There was a critical event!*



To do this, define the following settings (See Figure 54).

Figure 54. Settings for sending critical event SMS messages



The e-mail gate address, as well as the access code to the operator's cellular phone, can vary depending on the region.

6.2.3.2.2. Send mail using MAPI

If you have the Windows 95 OSR2/98 operating system running on your computer, the Kaspersky AV Control Centre application allows you to set up message sending through MAPI.



To set up MAPI parameters select the Send mail using MAPI option (Figure 55), then enable the following settings:

Figure 55. MAPI settings

Profile	Profile name (configuration file) of the MAPI client;
Password	Profile access password;
MAPI client	MAPI client name, which will be used for sending alerts.



Some MAPI clients do not use profiles. In that case leave the **Configuration** and **Profile** password lines empty.

6.2.3.3. The *Customize* category



The **Customize** category (Figure 56) contains the program interface settings. In this category you can set up the audio accompaniment of certain actions execution, as well as the colour mode of a program setting.

Figure 56. The **Settings** tab. The **Customize** category


The **Customize** category includes two sections: **Play sound on event** and **Appearance**. Here is their short description:

- **Play sound on event** – setting sound effect following the execution (or completion) of specified operations (see subchapter 6.2.3.3.1 for further detail);
- **Appearance** – set up the color mode of your program (see subchapter 6.2.3.3.2 for more detail).

6.2.3.3.1. Sound setup

The Kaspersky AV Control Centre application allows you to assign sound effects to specified events. This gives your program some additional service features.

The sound setup, as mentioned above, is carried out on the **Sound branch** (Figure 57).

To enable the sound, check the appropriate box and click on the corresponding  button to display the window, in which you want to select the audio file. This file should be written in the WAV format. Let's explain each sound's purpose:

- **Task start** – Play the sound immediately after the task launch (not regarding its type).
- **Task finished successfully** – Play the sound at successful task completion, i.e. in case the task hasn't been canceled by the user and hasn't terminated with errors.

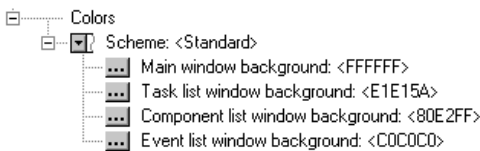
- **Task canceled by user** – Play the sound if the task was canceled by the user.
- **Task failed** – Play the sound at the emergency task close-down.



Figure 57. Sound setup

6.2.3.3.2. Color setup

The Kaspersky AV Control Centre program allows you to change the interface color setting.



Change the colors of the interface elements, as mentioned above, is carried out in the Colors section (Figure 58).

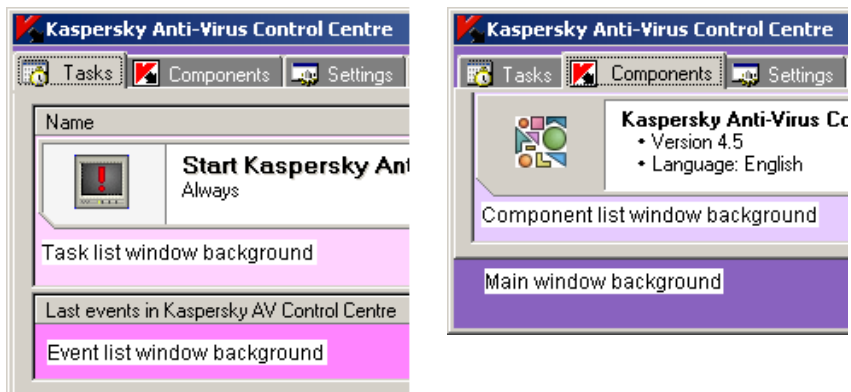
Figure 58. The Colors section

To make it easy for a user to set up the colors, the application provides a selection of standard color schemes. To choose a color scheme, go to the **Schemes** list. Each scheme is characterized by the following settings:

- **Main window background** – the application main window background color;
- **Task list window background** – the background color of the task list window of the **Tasks** tab;
- **Component window background** – the **Components** tab background color;
- **Event list window background** – the **Tasks** tab background color.



In Figure 59 below, the example of the Lilac color scheme is shown and its settings are given.

Figure 59. The **Liliac** color scheme

6.2.3.4. The **Quarantine** category

You can use the **Quarantine** settings tree to define the anti-virus quarantine settings. Quarantine is a special storage where suspicious and infected files detected by Kaspersky Anti-Virus® Scanner and Kaspersky Anti-Virus® Monitor are placed (see Figure 60).

For your Kaspersky Anti-Virus® Scanner and Kaspersky Anti-Virus® Monitor to save files to this storage, you must check the **Use quarantine** box on the **Options** page in the properties dialog window. When running in this mode the program quarantines the infected files, but does not delete them from their original location. The infected files are automatically deleted from the computer only if the **Delete** option in the Kaspersky Anti-Virus® Scanner and the Kaspersky Anti-Virus® Monitor settings is selected.

Figure 60. The **Quarantine** category

Files in quarantine are stored in encoded form. This:

- reduces the risk of infection from this virus (the executable code cannot be started without preliminary decryption);
- saves time for your anti-virus programs (files in the quarantined form are not detected as infected).

In the future you can study the quarantined files, restore them from the quarantine or delete them.

To quarantine the files locally, i.e. on your computer (*local quarantine*), select the **Quarantine files locally** option button in the settings tree. For details of how to handle quarantined files refer to the next chapter.

6.2.4. The *Quarantine* tab

On the **Quarantine** page (see Figure 61), you can see contents of the local quarantine (for details of the local quarantine see subchapter 6.2.3.4).

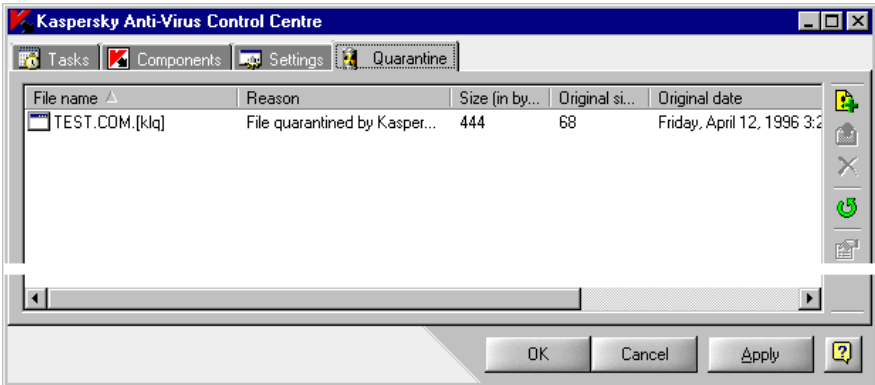


Figure 61. The **Quarantine** page

On this page you can change the display of quarantined files and handle these files as required. To do this, use the page's right-click menu (see Figure 62).

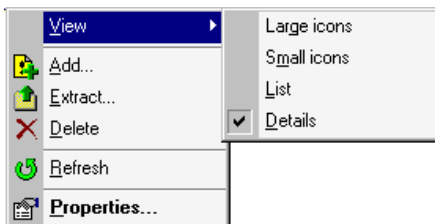



Figure 62. The **Quarantine** page right-click menu

All the commands on the menu, except for **View**, can also be activated using the appropriate tool bar buttons located at the right side of the page.

By using commands from the **View** sub-menu you can define the display of the icons and the list (in table form or just file names).



To review the file properties, follow these steps:

1. Select the required file name from the list and press the  button or select the **Properties** command from the file right-click menu.
2. The file properties box will appear on your screen (information in this box is similar to the file information displayed in the table, the difference is that it is arranged in a more friendly way, Figure 63).

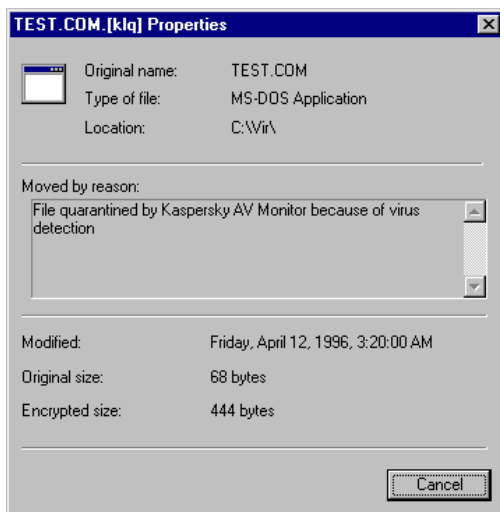





Figure 63. The file properties box

To update the list of quarantined files, select the **Refresh** command from the right-click menu or press the  button.



To restore a file from the quarantine, follow these steps:

1. Select the file from the list of quarantined files and press the  button at the right side of the frame or select the **Extract** command from the file right-click menu.
2. In the file restoration wizard box on your screen (Figure 64) press the  button to define the target folder where the restored file will be placed.
3. Check the **Decrypt** box.
4. Press the **Next** button.
5. The restoration progress box will appear on your screen. When the file is restored press the **Finish** button.

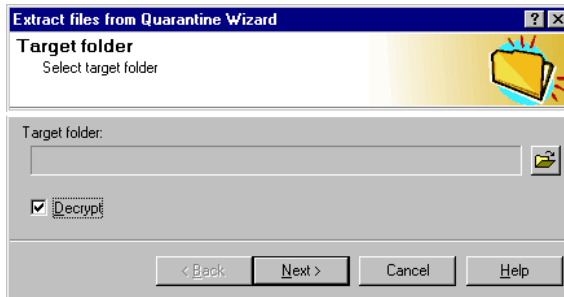



Figure 64. The file restoration wizard box



To delete a file from the quarantine, follow these steps:



1. Select it from the list of quarantined files and press the  button or select the **Delete** command from the file right-click menu.
2. The deletion confirmation box will appear on your screen. Press the **Yes** button to confirm the operation.



The program will only delete the file from the quarantine but not from its original location. The file may be automatically deleted from its original location only if you preset the anti-virus programs on the computer to delete infected files (selected the **Delete** option).



To add a file to the quarantine, follow these steps:

1. Press the button  or select the **Add** command from the right-click menu. The file quarantine wizard box will appear on your screen (Figure 65).
2. Define the file to be quarantined by pressing the  button and selecting the required file in the MS Windows standard dialog box.
3. If required, edit the text in the **Reason** field and press the **Next** button.
4. The quarantining progress box will appear on your screen. When the file is quarantined press the **Finish** button.

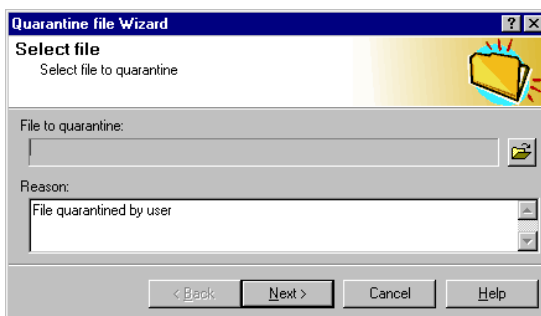



Figure 65. The file quarantine wizard box

6.3. New Task Wizard

The scheduled execution of a specified application with predefined settings can be defined as a named task of the task planner.

The **New Task Wizard** is activated when you select **New Task** in the context menu or click on the  button on the taskbar, the **Tasks** or **Components** tabs.

New task creation in the Kaspersky AV Control Centre is designed as a Windows Wizard with a sequence of windows (steps), each of which is used for execution of a specified action.

To change windows, click the **Next** (one step forward) and **Back** (one step backward) buttons. To terminate the process, click the **Finish** button. To cancel the new task creation, click **Cancel**. To get operation help on each step, click **Help**.

6.3.1. *Tasks window*

In accordance with the task type, running applications or settings features, tasks can be divided into two groups:

- tasks which launch **Kaspersky Anti-Virus®** applications during running;
- other tasks.

Type the task name and type in the **Task** window (Figure 66).

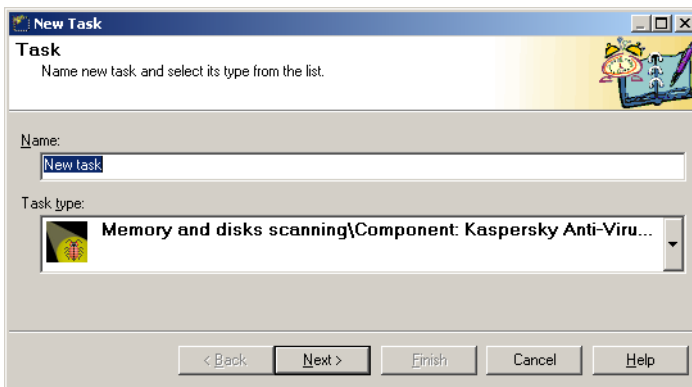


Figure 66. **Task** window

There are the following task types:

- **memory and disks scanning** – launches Kaspersky AV Scanner with the individual settings feature for different scan parameters for each task. Task launch can be scheduled to activate automatically, at a certain event occurrence, or on direct command of a user;
- **real-time scanning** – launches the Kaspersky Anti-Virus® Monitor and/or makes temporal modifications of its settings without reboot. The start-up period for each setting can be strictly specified in accordance with a schedule, determined by the occurrence of some system event, or be specified by the user during the switch to a different activity (for example,

during new software installation, importing programs and document copying, e-mail reception and so on);

- **anti-virus database update** – automated database update for new information on new viruses. You can update from the Internet, as well as from a LAN – which reduces connection expenditures, speeds up the update process and makes it easy to administer your package;
- **run user program** – any application, which can be launched from the Kaspersky AV Control Centre;
- **new product installation** – Windows Application Setup Wizard start-up.

6.3.2. The *Schedule* window for a Kaspersky AV Monitor task

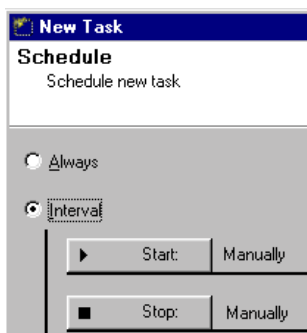


Figure 67. Schedule window for the Kaspersky Anti-Virus® Monitor task

When creating a Kaspersky Anti-Virus® Monitor task in the **Schedule** window (Figure 67) you should set the launch and pause intervals. To launch a task at the Kaspersky AV Control Centre start, select **Always**. To set a work interval, select **Interval**, then set up the launch and halt schedule. To set up the application launch, click on the **Start** button. You will see an activated window similar to the **Schedule** window for the Kaspersky Anti-Virus® Scanner task (read further for a description of this window).

Clicking on the **Pause** button will pause the task setup.

6.3.3. The *Schedule* window for Kaspersky AV Scanner and Updater

When creating a Kaspersky Anti-Virus® Scanner task in the Schedule window, you should set the conditions and frequency of the launch (Figure 68).

There are the following launch options:

- **On event** – the task launches on the occurrence of an event or by user command (See subchapter 6.3.3.1).
- **By condition** – the task launches at the occurrence of a certain task type close-down condition (See subchapter 6.3.3.2).
- **Hourly** – the task launches at a scheduled time with an hourly interval (See subchapter 6.3.3.3).
- **Daily** – the task launches every day at a scheduled time (See subchapter 6.3.3.4).
- **Weekly** – the task launches every week at a scheduled day and time (See subchapter 6.3.3.5).
- **Monthly** – the task launches on scheduled days and times (See subchapter 6.3.3.6).

Select the required start option in the left part of the window then set up the schedule according to details described in the subchapters below.

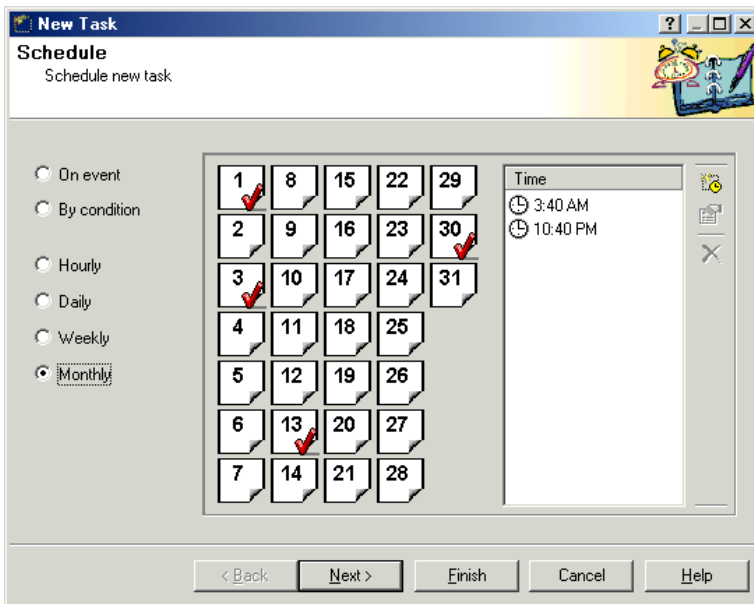


Figure 68. The **Schedule** window for Kaspersky AV Scanner and Kaspersky AV Updater

6.3.3.1. Launching on event

The Kaspersky AV Control Centre allows you to set the task launch on occurrence of a certain system event, or by user command.

To select this launch option, point to **On event**, then in the right part of the **Schedule** window you will see the condition list (Figure 69).

Select a launch condition from the list. There are several options available:

- | | |
|---|---|
| Manually | The task is launched manually from the Kaspersky AV Control Centre by user command; |
| At Control Center start | The task is launched at the Kaspersky AV Control Centre start, i.e., in fact at the user log in; |
| At Control Center system service start | The task is launched at the Kaspersky AV Control Centre System Service start-up, i.e., in fact, at system boot. |

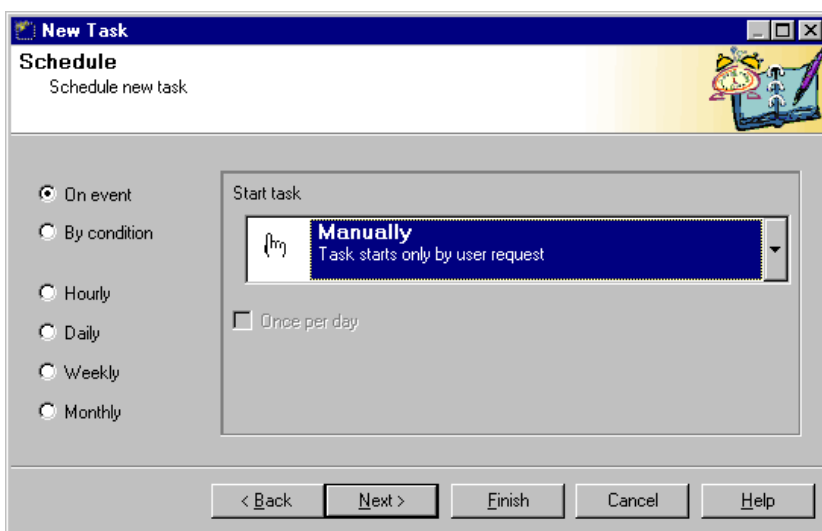


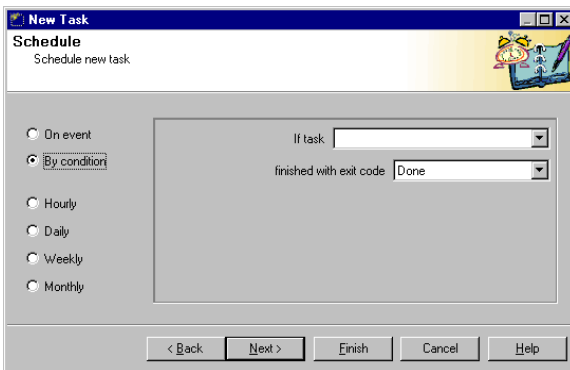
Figure 69. Start on event setup

You can schedule any of your task types to be launched once a day or on each occurrence of the event.

6.3.3.2. Launching by condition

The Kaspersky AV Control Centre allows you to set the task launch on the occurrence of specified conditions related to the results of the work of some package components.

In this product version this is realized in the following way: the user can create a task which will be launched provided that Kaspersky Anti-Virus® closes down with a certain return code.



To select this option, position the selector in the left part of the Schedule screen to By condition (Figure 70).

Figure 70. Start by condition setup

After doing so, in the If task window select the task status in respect to which the condition will be formulated, and in the finished with exit code list select the **task closedown** value.

Let's name the task status in respect to which the condition is formulated the *main task*, and the main task closedown value the *main task result*.

There are the following types of main task:

- Start Kaspersky AV Monitor;
- Update anti-virus databases;
- Start Kaspersky AV Scanner.

The program processes the following main task results:

- **Any**– the created task will run immediately after the main task execution without regard to its result;
- **Done** – the created task will run only if the main task has been successfully accomplished;

- **Failed** – the created task will run only in case of the main task failure;
- **Canceled** – the created task will run only if the user canceled the main task.

Sometimes viruses can affect the Kaspersky Anti-Virus® Monitor. In this case you should delete the viruses by other means.

By using this tab you can create, for example, a task that will automatically start your Kaspersky AV Scanner if your Kaspersky AV Monitor has generated a start error.

6.3.3.3. Launching hourly

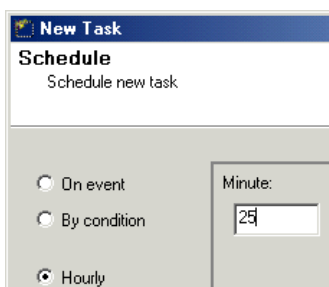


Figure 71. Start the task every hour

To launch a created task on an hourly schedule, select the **Hourly** option in the left part of the **Schedule** window (Figure 71), then specify the launch time in the right part of the window.

Figure 71 illustrates the setup of the task launch on an hourly basis within a 25 minutes period. For example, if it's 12 a.m., the task will be launched at 12:25, 13:25, 14:25 and so on.

6.3.3.4. Launching daily

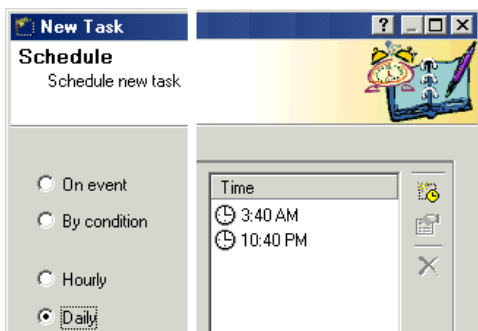





Figure 72. Start the task every day

To start the task on a daily basis at a scheduled time, select the **Daily** option in the **Schedule** window (Figure 72), then set up the launch time.

The launch time setup is done in the **Time** list. Use the Kaspersky AV Control Centre and the context menu for this purpose. You can use these as follows:

Toolbar button	Context menu option	Purpose
	Create...	Creates a new launch time record. When you select this option and the Time window is activated, you must type in the task launch time. You can display this window by double clicking with your mouse in any white place within the Time list or by pressing the <INS> key.
	Modify...	Modifies the task launch time value. When you enable this option and the Time window is activated, type in the modified time value. You can also do this by double clicking with your mouse on the line to be modified, or by pressing the <SPACE> key.
	Delete...	Deletes the task launch time record from the list. You can also do this by pressing the key when on the line to be deleted.

6.3.3.5. Launching weekly

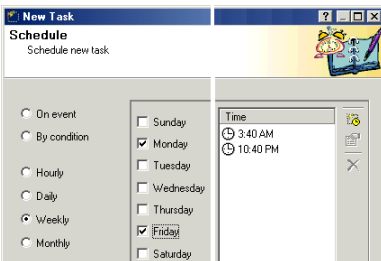


Figure 73. Start the task every week

To launch a task on a weekly basis on a scheduled day and time enable the **Weekly option** in the **Schedule window**, then specify the days and hours of the task launch in the right part of the window.

To specify the dates and hours for the task launch, checkmark the days of the week, then type in the time in the **Time window**. See subchapter 6.3.3.4 for more detail on how to specify the time.

Figure 73 illustrates the setup of a task launch on Monday (3:40 a.m. and 10:40 p.m.) and on Friday (3:40 a.m. and 10:40 p.m.).

6.3.3.6. Launching monthly

To set up the task to be started each month on scheduled days and times, select the **Monthly** option on the **Schedule** tab (Figure 74).

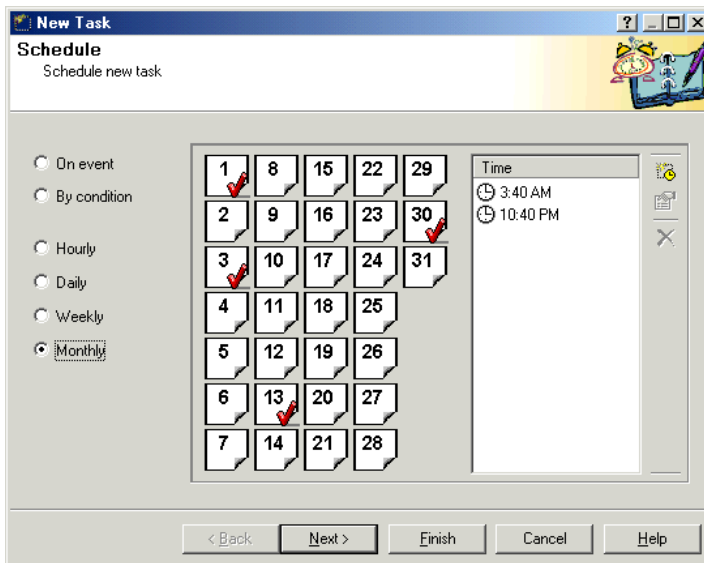



Figure 74. Start the task every month

Then, use your mouse to check the dates when the created task will be launched and specify the launch time in the **Time** tab (See subchapter 6.3.3.4 for more information on how to specify the time in the list).



The task launch days are checked . Figure 74 illustrates the settings of the created task launch on the 1st, 3rd, 13th and 30th of each month at 3:40 a.m. and 10:40 p.m.

6.3.4. The *Alerts* window

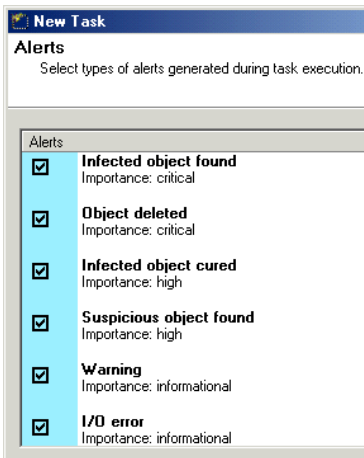


Figure 75. Alert types selection

In the **Alerts** window (Figure 75) check the alert types to be created by the task.

As has been mentioned above, alerts are messages generated by tasks.

To select an alert, check the appropriate box.

6.3.5. The *User account* window

The Kaspersky AV Control Centre can be launched as a Windows system service before login. In this case define the user account to be used by the task.

The user account contains information about the user (such as full name, password and more).

To configure the account, go to the **User account** window (Figure 76).

You can use the following accounts:

Local system account Windows account

Currently logged on user account The current user account

This account Account of the user whose settings are specified in the lines **Username**, **Password** and **Confirm password**.

If the task is to be started under an account that is different from the current one, the messages it generates will be screened only if you check the **Allow task to interact with desktop** box.

Figure 76. User account login for task start

6.3.6. Task settings

At this phase of task creation set up the task parameters specific for this type of task. As a rule, the contents of these settings are equivalent to the tabs.

Let's take a look at task types and windows that are activated during this phase:

Task type	Windows sequence	Description
Kaspersky Anti-Virus® Scanner and Kaspersky Anti-Virus® Monitor launch task	1. Objects	See subchapter 3.3.1
	2. Options	See subchapter 3.3.23.3.2
	3. Customize	See subchapter 3.3.3

Task type	Windows sequence	Description
Kaspersky Anti-Virus® Updater	1. Connecting	See description in subchapter 5.2.2. There are two additional options in this window, which allow you to enable anti-virus database and executable module installation to the specified folder on the Kaspersky AV Server.
	2. Options	See subchapter 5.2.3.

6.3.6.1. The *Settings* window for Kaspersky AV Scanner and Monitor tasks

Options in the **Settings** window for the Kaspersky AV Scanner task are similar to those in the **Settings** window of Kaspersky Anti-Virus® Scanner (for details refer to subchapter 3.3.2).

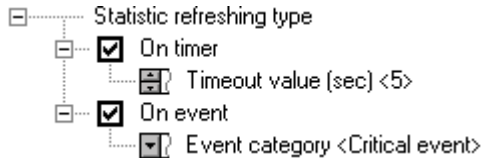


Figure 77. The **Settings** window for the Kaspersky Anti-Virus® Scanner task

The exception is the element **Statistics refreshing** (Figure 77) where the order is set for a statistics update in the Report Viewer component.

Statistics can be updated by the timer (check the **On timer** box in the **Customize** window and specify the update interval in seconds) and at the occurrence of a system event (check the **On event** box, then select the event type). In this product version you can update the statistics on critical and other events.

CHAPTER 7. KASPERSKY®

REPORT VIEWER

Kaspersky® Report Viewer is a program allowing you to display and manage reports generated by Kaspersky Anti-Virus® package components.

Kaspersky® **Report Viewer** is activated by selecting the **Show Report** option in the Kaspersky AV Scanner, AV Monitor, and Kaspersky® Inspector main windows, and by clicking the **Report** button in the **Finish** boxes of the Kaspersky AV Updater and the Kaspersky® Office Guard main window.

The Kaspersky® Report Viewer main window (Figure 78) contains the following items:

- menu;
- tool bar;
- list of sessions within the current file (you can open only one report file at a time!);
- report table;
- status bar.

To view a session report, select the required session in the left hierarchy in the window. The appropriate report will be displayed in the right frame.

The report table contains the following titles:

- **Object**– object handled;
- **Result** – performance result;
- **Description** – description of the action performed to this object.

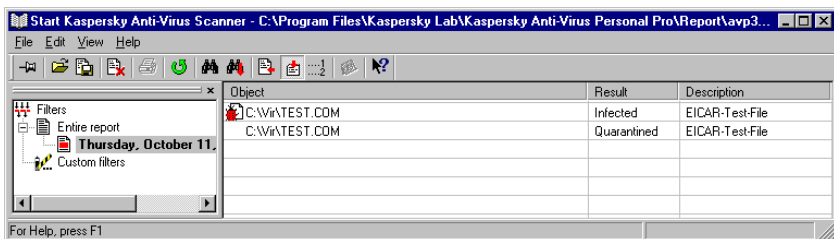














Figure 78. The report window

To the right of the report contents you can see the tool bar, which contains buttons for operation execution. The buttons have pop-up prompts. To see them, point the mouse cursor to a button; next to it you will see a small window with a short help line.

On the top you will see the main menu. We should note that taskbar buttons and some menu commands duplicate each other.

Below, there is a comparative table of buttons and menu commands. We will explain their purposes:

Toolbar button	Menu commands	Function
	View→Always on top	Sets the program main window to overlay all other windows on your Windows desktop.
	File→Open	Allows you to open a selected report file.
	File→ Save As...	Allows you to save the report into a file with a name different from the current one.
	File→ Purge	Allows you to clear a selected report file.
	File→Print	Prints
	View→Reload	Reloads the report from the corresponding file.
	Edit→Find	Allows you to search for a user-defined string or its part in the report. If you press this button, the appropriate search dialog box will appear on your screen (see below)
	Edit→Find next	Moves to the next string meeting the same search criteria (see above).

Toolbar button	Menu commands	Function
	View→Autotracking	Allows you to track the report (if you press this button (i.e. enable this mode) the report will be automatically placed on the last line, after new data is collected).
	View→View last session	Displays a report about the last session.
	View→View statistics only	Displays only statistics
	View→Comments	Displays comments

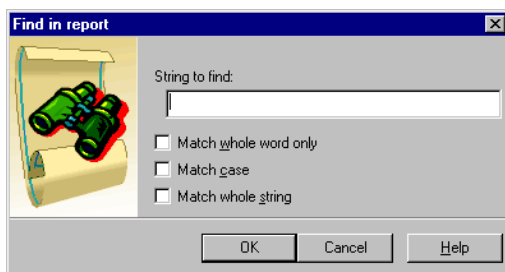



Figure 79. The **Find in report** dialog box


The **Find in report** dialog box (Figure 79) appears in the report window when you press the  toolbar button or select the **Find** command in the **Edit** menu. To search for a string (or its part), enter it in the **String to find** text field, define the required search criteria and press the **OK** button.

The dialog box contains the following check boxes:

- **Match whole word only** – check this box to search only for complete words matching the defined sample;
- **Match case** – check this box to search only for text with the specified capitalization;
- **Match whole string** – check this box to search only for complete strings matching the defined sample.

To exit the dialog box press the **Cancel** button, and to display the Help topics window press the **Help** button.



When the search function detects the first string (or the string part) matching the predefined search criteria, you can move to the next string meeting the same criteria by pressing the  toolbar button or selecting the **Find next** command from the **Edit** menu.

CHAPTER 8. THE SETTINGS TREE



The Kaspersky Anti-Virus® interface frequently uses the so-called settings tree which presents data in the form of a tree and conventional controls as joints (buttons, drop-down lists, check boxes and etc.).

This technology provides a clear and easy to understand picture of interrelations between various settings, and makes it easy to study the program.






In this book all controls are illustrated by pictures, so you can see how they look like in the program windows.




8.1. The Settings Tree

Every joint in this tree may have branches. If a branch is visible the corresponding joint looks like this: ; if the branch is hidden the corresponding joint will change to .

To change a setting you must make its branch visible.

To display and hide a branch you must use the following methods:

What to do	How it might be done (By using...)
To display a branch (the joint looks like )	the  key on your keyboard. the  command of the right-click menu. The <+> key on your keypad (all branches of the joint become visible).

What to do	How it might be done (By using...)
To hide a branch (the joint looks like )	the  key on your keyboard. the  command of the right-click menu . the <=> key on your keypad (all branches of the joint disappear from your screen).

8.2. Controls



To change settings you will use several types of controls:

8.2.1. Check box

A box may be

- All files – unchecked, meaning that this type of virus check will not be performed.
- All files – checked, meaning that the program will perform this type of virus check.

To check and uncheck a box you must use the following methods:

What to do	How it might be done (By using...)
To check the box	the <SPACE> key on your keyboard. the  command of the right-click menu . your mouse to click on it.
To uncheck the box	the <SPACE> key on your keyboard. the  command of the right-click menu . your mouse to click on it.


8.2.2. Option button

The **option buttons** are members of a group. A group of option buttons may consist of two or more buttons. You must use this group to select one of the options. The option button may be:

- Int 13h – selected (enabled);
- Int 13h – deselected (disabled);


You can select only one option button from the group.

To select and deselect an option button you must use the following methods:



What to do	How it might be done (By using...)
To select the option button	the <SPACE> key on your keyboard. the  Check command of the right-click menu . your mouse to click on it.
To deselect the option button	By selecting another option button from the group.

8.2.3. Text field

To edit value of a **text field** you must use your keyboard. You may see the text field's current value enclosed with angle brackets at the right of the field name.

 Table files base name <KAVITAB> – the text field.

To edit a text field value use the following methods:

What to do	How it might be done (By using...)
To edit the field value	your mouse to click on the field icon. the  Modify command of the right-click menu . the F2 key on your keyboard. The text field will change its appearance to  KAVITAB .


After you finish editing the text field value press the **Enter** key on your keyboard or click with your mouse outside of this text field. You can cancel changes this text field and return to the previous value by pressing the Esc key on your keyboard.

8.2.4. Input field defining the path to...

To edit value of the **path field** you must use the conventional Windows dialog to select the directory or file.


 Table files location <> – the path input field.

To edit a path field value use the following methods:


What to do	How it might be done (By using...)
To edit the field value	<p>your mouse to click on the field icon.</p> <p>the  command of the right-click menu .</p> <p>the F2 key on your keyboard.</p>

8.2.5. Input field defining the number of ...

To input a new value in the **number field** you must type it in from your keyboard or use the cursor control keys to change the current value. You may see the field's current value enclosed with angle brackets at the right of the field name.

 Dangerous number of files with similar size change <4> – the number input field.

To edit a number in the field use the following methods:

What to do	How it might be done (By using...)
To edit the field value	<p>your mouse to click on the field icon.</p> <p>the  command of the right-click menu .</p> <p>the F2 key on your keyboard.</p>



If the first character of the entered number is zero, the program interprets it as an octal notation and translates into the corresponding decimal number.

8.2.6. Drop-down list

The drop-down list allows you to select one of the items from the list (Figure 80). To browse the list you must use the \uparrow and \downarrow keys on your keyboard. To automatically scroll down/up the list you must use the **CTRL + \uparrow** and **CTRL + \downarrow** **KEY COMBINATIONS**.

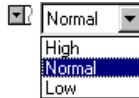


Figure 80. Drop-down list

8.3. Checkboxes

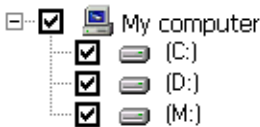


Figure 81. Disk hierarchy

When setting your anti-virus to check for viruses in the disk hierarchy (see subchapter 0) you must use the so-called Rules of Succession, i.e. if you define some settings for the **My Computer** item (Figure 81), they will be automatically assigned for all disks on your computer.

Every item of the hierarchy is associated with a *checkbox* (that can be checked or unchecked) and *rules* (applied to this item). A check box indicates whether the corresponding hierarchy item must or must not be checked for viruses, and the rules describe methods that will be applied when handling this item.

All the hierarchy items by default *inherit rules of the group* these are included in. If you change the rules to be applied to a group, the group item rules will change also.

You can assign independent rules to an item or change the status of its box. These items may have *independent rules*. If you change the rules to be applied to the group, these items will keep their processing rules. However, by changing the check box status you can restore these items as inheriting the group rules.

By selecting the **Set Strict** command from the right-click menu you can completely disable the rule-inheriting mode for the selected item. If you select this command, the corresponding box will look like a red box with a black tick inside. Items with indicators in this condition have *strictly independent rules* assigned. These items will keep their rules even after you change the group box

status. To restore these items as inheriting the group rules, you must select the **Remove Strict** command from the right-click menu.

The check box will have the following appearance:

Looks like	Description	Meaning
<input checked="" type="checkbox"/>	A square with a tick inside. The square may be red or black.	<p>The check mode is enabled.</p> <p>If the square is <i>red</i>, the inheriting mode is disabled.</p> <p>If the square is <i>black</i>, the inheriting mode is enabled.</p>
<input checked="" type="checkbox"/>	A square with the tick inside and a triangle in the right-bottom corner. The triangle may be red or black.	<p>The inheriting mode is enabled, but some objects are excluded from the group and have their own settings.</p> <p>If the triangle is <i>red</i>, the inheriting mode is disabled for one or more objects.</p> <p>If the triangle is <i>black</i>, the rule has been changed for one or more objects.</p>
<input type="checkbox"/>	A square without the tick and with the triangle in the right-bottom corner. The triangle may be red or black.	<p>The check mode is disabled, but for one or more objects this mode is enabled.</p> <p>If the triangle is <i>red</i> the inheriting mode is disabled for one or more objects.</p> <p>If the triangle is <i>black</i>, the rule is changed for one or more objects.</p>

CHAPTER 9. KASPERSKY ANTI-VIRUS® SCRIPT CHECKER

Kaspersky Anti-Virus® Script Checker (Kaspersky AV Script Checker) – is an anti-virus application that protects your computer from script viruses and worms executed directly in the memory. When you run the Kaspersky Anti-Virus® Personal setup utility, the program is automatically added in your operating system and later you will not have to start it manually.

Different programs that use Microsoft Windows Script Host (e.g., Microsoft Explorer, Microsoft Internet Explorer, Microsoft Outlook and others) send scripts (such as VB Script and Java Script) to Script Hosting for processing and further execution. Before executing these script files, Kaspersky AV Script Checker sends them to the Kaspersky Anti-Virus® Monitor for checking (provided that it is installed and launched) and, if Monitor doesn't detect viruses, carries out an heuristic analysis³ of the script file code. If a file is suspicious, Kaspersky AV Script Checker sends a message and prohibits execution of the script.



Kaspersky AV Script Checker does not use the anti-virus databases. The anti-virus databases are used by Kaspersky AV Scanner and Kaspersky AV Monitor. The advantage of the Kaspersky AV Script Checker in comparison to other anti-virus applications is that it warns the user of a possible infection by a new virus, which is not yet defined in the anti-virus databases.

Script files in Windows are executed in memory without any preliminary call to the disk. Therefore, such protection tools as Kaspersky Anti-Virus® Monitor can't check script files before their execution. Script Checker intercepts the execution of script files and sends them to Kaspersky Anti-Virus® Monitor to be checked. In that way Kaspersky AV Script Checker in combination with Kaspersky Anti-Virus® Monitor offers full protection from all virus types.

Let' study a situation in which Kaspersky AV **Script Checker** protects your computer from a virus.

³ Heuristic analysis – analysis of the succession of commands in the checked object, collection of statistics, and determination as "possibly infected" or "not infected" (See www.viruslist.com for further information).

Let's imagine that you go to a web site containing a script virus similar to **LoveLetter**⁴. If your Internet browser has low-level protection, the script virus will be immediately executed, but Kaspersky AV Script Checker will prevent the execution of the infected script and protect your computer from the virus attack. Kaspersky AV Script Checker will send a warning like that shown below (Figure 82):

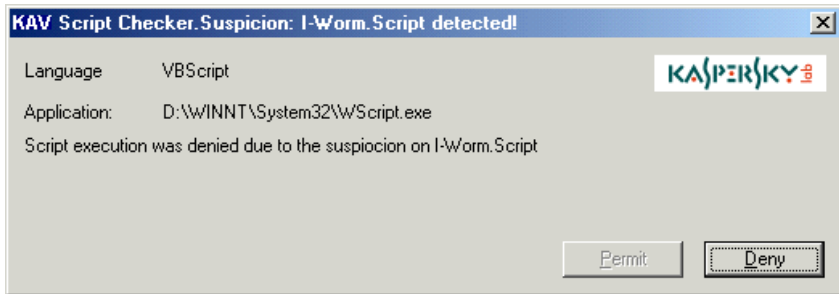


Figure 82. Warning about a possible virus

⁴ LoveLetter is a dangerous Internet worm that led to mass computer infection in May, 2000. The worm was spread by e-mail messages. When activated it would send itself to all addresses stored in the Microsoft Outlook address book (see www.viruslist.com for more detail).

CHAPTER 10. KASPERSKY ANTI-VIRUS[®] RESCUE DISKS

Kaspersky Anti-Virus[®] includes **Kaspersky Anti-Virus[®] Rescue Disk**, a special program allowing you to create a set of *fallback-recovery disks*.

The fallback-recovery (or rescue) disks are used for system recovery after a virus attack. These disks include:

- system files of the Linux operating system;
- anti-virus scanner;
- anti-virus databases.

The rescue disks work on the following principle. Let's imagine that as a result of a virus attack your computer is not capable of initial boot. In this case you have to boot your computer using a bootable disk from the fallback set. The bootable disk will load the Linux operating system, then start the anti-virus scanner. When required, the load program will prompt for disks with the anti-virus bases. If detected a virus the anti-virus scanner will ask for instructions on how to handle it: to remove the virus from the file, to delete the infected file or to log the event.

10.1. Creating a Fallback-Recovery Set

To start your rescue disk creation program, Kaspersky Anti-Virus[®] Rescue Disk, go to the Windows main menu and select **Kaspersky Anti-Virus[®] Rescue Disk** from the Kaspersky Anti-Virus[®] program group. The **Welcome** box, the first wizard box, will appear on your screen (Figure 83). To move to the next wizard box you should press the **Next** button in the current box.



Figure 83. The **Welcome to Kaspersky® Rescue Disk** wizard box

The **Configuration** wizard box (Figure 84) allows you to specify the fallback recovery disks to be created:

- Bootable disk containing executable files** – boot disk with Linux OS files and the Kaspersky Anti-Virus® executable files.
- Disks with anti-virus bases** – disks with virus definitions and methods to be used for their removal. It's advisable that you update these disks with updated anti-virus databases on the regular basis.



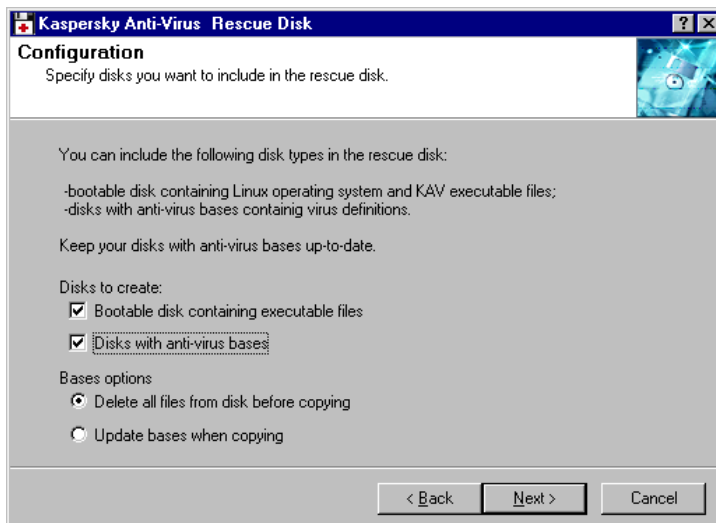
The bootable disk containing Linux operating system and the Kaspersky Anti-Virus® executable files can be created only once, and the disk with anti-virus bases must be created every time the update is released.

The **Basis options** group allows you to specify how the anti-virus base disks should be created:

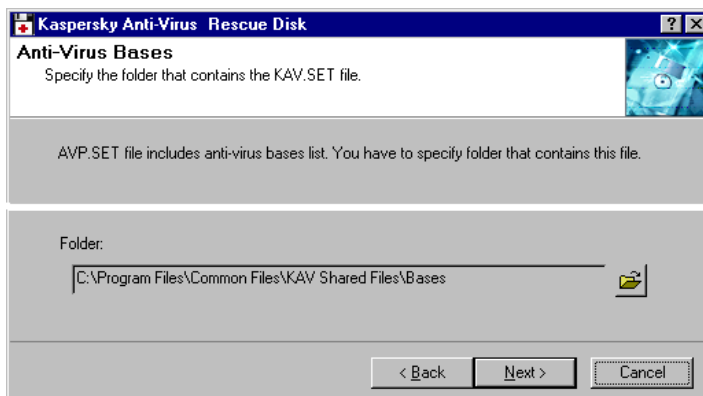
- Delete all files from disk before copying** – removes all files from the disk before copying anti-virus bases onto it.
- Update bases when copying** – copies only the updated bases onto the disk. With this option selected the program doesn't clean the disk before copying bases onto it but compares bases on the disk against those to be copied. If the bases are identical the program doesn't copy any files onto the disk.



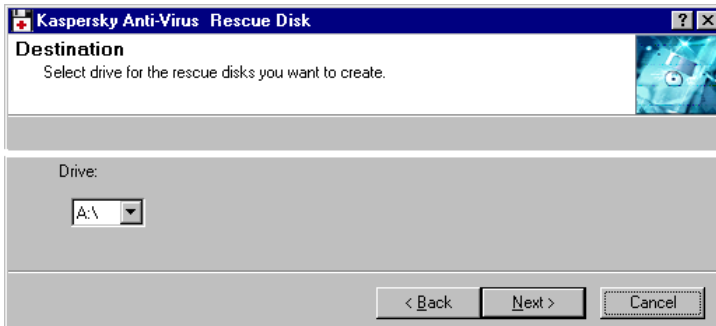
If you selected the **Update bases when copying** option, you should insert anti-virus base disks in the order, in which these were created.

Figure 84. The **Configuration** wizard box

In the next wizard box, the **Anti-Virus Bases** box (Figure 85), you must define path to the file *AVP.SET*. This file is included in the Kaspersky Anti-Virus® package and contains the list of available anti-virus databases.

Figure 85. The **Anti-Virus Bases** wizard box

In the **Destination** box (Figure 86), you must select the logical drive, where the files will be copied.

Figure 86. The **Destination** wizard box

The program will then copy the files to the defined logical drive (Figure 87). During the copying process the application may prompt for additional disks.

Figure 87. The **Copying files** wizard box

When the files are copied to the disks, you will see the **Completing** wizard box (Figure 88). This means that the rescue-disk creation program has accomplished its task.

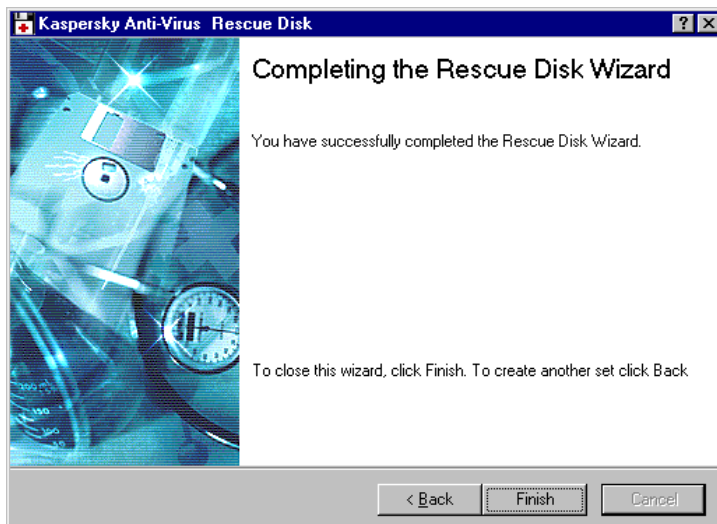


Figure 88. The **Completing the Rescue Disk Wizard** box

10.2. Using the Fallback-Recovery Disks

To use the fallback-recovery set, it is advisable that you follow these steps:

1. Insert the start-up fallback-recovery diskette into the floppy disk drive and restart your computer. When the operating system is loaded, the anti-virus scanner will start checking for viruses in boot records and the master boot record on your computer. If it detects a virus, the program will automatically delete it. Then the program will screen a prompt similar to the following:

```
Please select a device for swapping.
```

```
N ...
```

```
1. /dev/ide/host0/bus0/target0/lun0/part 1
```

```
2. /dev/ide/host0/bus0/target0/lun0/part 5
```

```
0. No swap (Recommended)
```

```
Please enter the preferred partition number and  
press ENTER.
```

```
You must select the drive where the operating system  
will create temporary files and enter its number.
```

```
File names are displayed in the Linux format. After  
that, the program will prompt for the drive where the
```

report file will be created. The prompt will look similar to the above.



Note that details of your computer disk names with the Linux OS format appear on your screen above the request for temporary data disk. You will need these disk names later, when you decide to start your anti-virus on your own. The data format is:

```
Remounting root filesystem in read-write mode.
/dev/ide/host0/bus0/target0/lun0/part1 (Vfat) has
been mounted to /mnt/disk1
```



It is not recommended to use the fallback-recovery diskettes in the NTFS file system. If the device type is defined as **ntfs**, you should not select this device or start your anti-virus scanner to check and delete viruses on it.

2. When prompted, insert the appropriate disk from the fallback-recovery set. When the anti-virus base files are copied from the diskette you should replace it and press the **<ENTER>** key three times in order to proceed with the operation. After this, the program will start scanning for viruses on your computer.
3. When detected a virus the program displays the query of the following format:

```
File <filename > Infected by virus:<virus_name>
Actions - Report only (Ok,
disInfect/Delete/Cancel/Stop)
```

where:

<filename> is the name of infected file,
 <virus_name> is the name of detected virus. By entering one of the following characters you may select how the program should handle the infected file:

- O** or nothing – log the virus details,
- I** – attempt to disinfect the file,
- D** – delete the infected file,
- C** – ignore the file,
- S** – interrupt the scanning operation.

4. After this the program will prompt you whether you want to apply the selected action to all the infected files detected later:

```
Apply to all infected objects? - Yes/No
```

To respond to this query enter one of the following characters:

- Y** – apply the selected action to all the infected files detected later,

N – display the same query as above whenever an infected file is detected

5. After the scanning operation is finished the statistics table appears on your screen. Study the statistics and press the **<ENTER>** key.

- **Sector objects** – sectors processed;
- **Files** – files processed;
- **Folders** – folders processed;
- **Archives** – archives processed;
- **Packed** – packed executable objects processed;
- **Known viruses** – known viruses detected;
- **Viruses bodies** – virus bodies detected;
- **Disinfected** – objects disinfected;
- **Deleted** – objects deleted;
- **Warnings** – warnings generated;
- **Suspicious** – suspicious objects detected;
- **Corrupted** – corrupted files detected;
- **I/O errors** – input/output errors occurred.
- **Speed (Kb/sec)** – the average speed of scanning in Kb/sec.
- **Scan time** – the total time of scanning.

6. The menu of ulterior actions will appear on your screen:

```
1: Run kavscanner
2:                               See config
3:                               See report
4: Exit
Your choice [1,2,3,4]>
```

Enter the digit that corresponds to your choice:

1 – start the anti-virus scanner again. If you enter this digit the following prompt will appear on your screen:

```
Enter directories for scanning>
```

Enter the directories to be scanned using the Linux OS format and make sure to separate them by spaces. For example, the disk C: directory called *work* may look similar to the following in the Linux OS

notation: `/mnt/disk1/work`. The disk names appear on your screen after you use the first disk from the fallback-recovery set (see above).

After you enter the directories the program will start prompting for anti-virus base disks, and after this it will start scanning in the selected location.

2 – display the anti-virus scanner profile.

3 – display results of the last scanning session.

4 – exit the program.

7. After the scanner has finished scanning and disinfecting, press the key combination **<CTRL>+<ALT>+** to reboot your computer and remove the rescue disk from the floppy disk drive.

CHAPTER 11. KASPERSKY ANTI-VIRUS[®] MAIL CHECKER

Kaspersky Anti-Virus[®] Mail Checker for Microsoft Exchange Client Compatibles (Kaspersky AV Mail Checker) is designed to protect users' computers from viruses that use Microsoft Outlook 98/2000/XP for sending and receiving mails.



The current version of Kaspersky AV Mail Checker is not compatible with Outlook Express and TheBat!

The Kaspersky AV Mail Checker program performs the following functions:

- Checks for viruses in all, the incoming and outgoing messages. The program checks messages right after these arrived or were sent and it searches for viruses in both message bodies and attached files.



Kaspersky AV Mail Checker also searches for viruses within embedded archives, packed executable files, plain mail files and mail databases.

- Checks for viruses in the messages stored in the local mailbox before the Kaspersky AV Mail Checker program was installed. These messages are checked when the user opens them.
- Allows the user to disinfect infected attached files.
- Kaspersky AV Mail Checker deletes infected objects from messages and, if all elements of the message are infected, it deletes the entire message.

The anti-virus settings are defined from the program that is used for mail processing.



While handling mounted mailboxes the program implements limited features: it doesn't check messages when these arrive to such mailboxes. The messages are checked only when the user opens these messages.

11.1. Configuring Kaspersky AV Mail Checker

The recipient protection settings can be displayed and redefined on the **Kaspersky Anti-Virus[®] MailChecker** page of the **Options** dialog window that

can be displayed from the mail-processing program Microsoft Outlook 98/2000/XP.



To display the **Options** dialog window from Microsoft Outlook:

1. Start Microsoft Outlook;
2. Select **Options** from the **Tools** menu;
3. Switch to the **Kaspersky Anti-Virus® MailChecker** tab.

On the **Kaspersky Anti-Virus® MailChecker** tab (Figure 89), you can:

- Enable or disable the anti-virus protection of your incoming or outgoing mail by checking/unchecking the **Enable Protection** box;
- Set the program to display an alert message when your mail client is trying to send an infected message by checking/unchecking the **Popup Alert Message box upon detection** box.



Kaspersky Anti-Virus® Mail Checker integrated into this version of Kaspersky Anti-Virus® Personal/Personal Pro does not allow you to employ a unified approach to handling infected messages

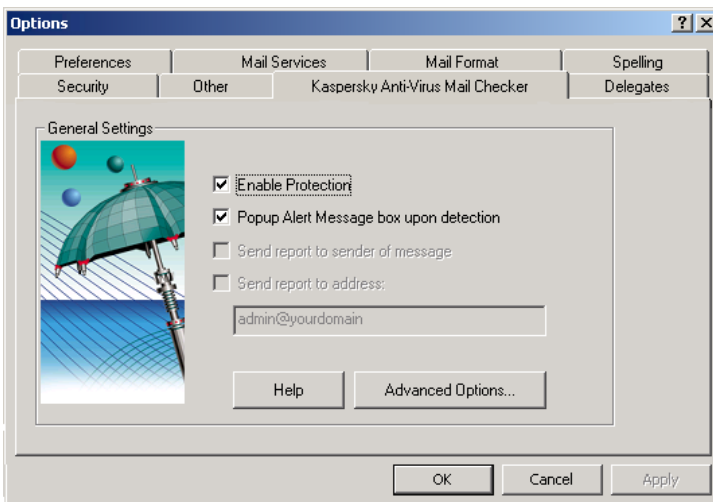


Figure 89. The **Options** dialog window with the **Kaspersky Anti-Virus® MailChecker** tab displayed

11.2. Running Kaspersky® Mail Checker

Right after installed Kaspersky AV Mail Checker will start to display alert messages. However, you will see these alerts only when the virus is detected in your outgoing message (if you have checked the **Popup Alert Message box upon detection**).

Below, we describe several differences in the ways Kaspersky AV Mail Checker treats incoming and outgoing mail traffic:

11.2.1. Incoming messages

Incoming messages are checked automatically right after these arrive to the protected mailbox. If these messages are clean, you will receive them immediately. However, if Kaspersky Anti-Virus® finds an infected object, it will try to disinfect it. If disinfection fails, the object will be deleted from the message. If disinfection is successful, the message with the disinfected object will be delivered to you immediately after treatment.



Note that the program will not notify you about disinfection / deletion of an object from your e-mail message.

If all objects in this message are infected, you will receive this letter only if at least one of these objects can be disinfected. Otherwise, the entire message will be deleted.



Note that the program will not notify you about deletion of the message.

11.2.2. Outgoing messages

Outgoing messages are checked for viruses right after the user press the **Send** button. If an outgoing message is infected the program attempts to cure it (if the appropriate option is enabled).

If the **Popup Alert Message box upon detection** box is unchecked the message will be processed in background mode, which does not require any interaction on your part. Clean messages will be sent to the recipients and infected messages will be subjected to treatment. After treatment, the messages will be:

- *sent*, if disinfection was successful;
- *sent but without infected attachments* the program failed to disinfect;
- *deleted* if disinfection of the message or ALL the attached files failed.

If the **Popup Alert Message box upon detection** box is checked, you will have to respond to the alerts:

1. If disinfection failed, the appropriate alert will appear on your screen (Figure 90).

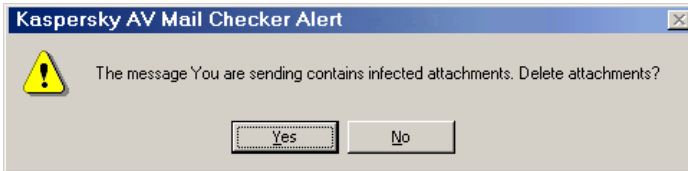


Figure 90. The alert about deleting infected attachments from an outgoing message

- Press the **Yes** button to delete the attachment and send the clean message to the recipient.
- Press the **No** button if you do not want to send this message without the attachment. After this, the infected-message-to-be-sent warning will appear on your screen (Figure 91). Cancel the sending operation by pressing the **No** button.

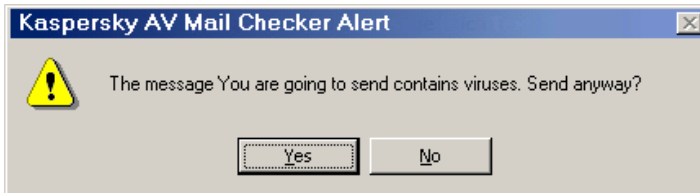


Figure 91. The outgoing message is infected!

11.2.3. Messages in the mailbox

Kaspersky AV Mail Checker checks for viruses in the messages that were stored in your mailbox before you installed this program. These messages are checked when open them. In this case the program handles these messages as if these just arrived to your mailbox.

CHAPTER 12. KASPERSKY ANTI-VIRUS[®] PERSONAL PRO

The software package Kaspersky Anti-Virus[®] Personal Pro has been developed to provide full-scale anti-virus protection for home computers running Windows 95 OSR2/98/ME, Windows 2000/NT operating systems, MS Office 2000 business applications and mail programs (Outlook and Outlook Express). Kaspersky Anti-Virus[®] Personal Pro includes the same components as Kaspersky Anti-Virus[®] Personal (see Chapter 1), plus the following two components:

- **Kaspersky[®] Office Guard.** Protects Office 2000 documents from both known and unknown macro viruses. Office Guard controls activities of macros written in Visual Basic for Applications that run within Microsoft Office 2000 applications. Upon an attempt to perform a suspicious macro command, Office Guard can perform one of the following four actions depending on the program's settings for virus protection level: forbid the command execution, permit command execution, disable macros completely, or offer the user a choice of one of these three options.
- **Kaspersky[®] Inspector.** An anti-virus disk scanner designed to work under operating systems Microsoft Windows 95 OSR2/98/ME or Microsoft Windows NT/2000. Kaspersky[®] Inspector scans disks for changes in file and folder contents. The program can be used both as an additional level of virus protection and to monitor changes on the disk.



The installation procedure of Kaspersky Anti-Virus[®] Personal Pro is completely identical to the installation of Kaspersky Anti-Virus[®] Personal.

CHAPTER 13. KASPERSKY®

OFFICE GUARD

Kaspersky® Office Guard is a tool that protects Microsoft Office 2000 documents from both known and unknown macro viruses. If a document is infected by a virus of any type, Kaspersky® Office Guard will detect the virus and disable it before it can do any harm.

Kaspersky® Office Guard...

- monitors the activity of macros written in Visual Basic for Applications (VBA) that run within Microsoft Office 2000 applications. When a macro runs, Kaspersky® Office Guard checks each program instruction that the macro wishes to execute and compares it against a list of *suspicious macro instructions*, i.e. a set of instructions that might be executed by a virus.



A list of suspicious macro instructions, their description, and the frequency of use of such instructions by viruses are given in the Help topics.

- takes actions according to the pre-set virus protection level when a macro tries to execute a suspicious instruction. Kaspersky® Office Guard can prohibit the instruction from being executed, permit it, terminate all macros or ask the user what to do.



Although Kaspersky® Office Guard will detect the activity of any macro virus infecting Microsoft Office 2000 documents, it cannot determine for sure whether a file is infected by a virus, or merely contains a harmless macro that uses instructions which are sometimes used by a virus. The final decision as to whether a macro is safe to execute rests with you or your system administrator.

13.1. Kaspersky® Office Guard – Protection from Unknown Macro Viruses

To automate repeated operations the macro programming capability was incorporated into many word-processors, spreadsheets and engineering

applications. Macros are small programs that may have a complex structure and employ a rich set of instructions.

A **macro virus** is a piece of macro code that is designed to transfer its code from the infected file (documents or spreadsheets) to others.

At the end of 2000, several systems were known to contain macro viruses. The applications that are affected most often are the principal applications of the Microsoft Office Suite that support the Visual Basic for Applications (VBA) macro programming language. These are:

- Microsoft Word – WordBasic macro language used in Microsoft Word 6/7 and VBA in Microsoft Word 8 and later;
- Microsoft Excel;
- Microsoft Access;
- Microsoft PowerPoint;
- Microsoft Project;
- Microsoft Visio.

The Lotus WordPro (AmiPro) editor is vulnerable to macro virus attacks as it also supports an embedded script language.

Currently Microsoft Office (Word, Excel and PowerPoint) macro viruses are the most widespread. Macro viruses for other Microsoft Office applications are comparatively rare, and as for AmiPro, only one macro virus affecting this application is known at this time.

13.1.1. How they function

All Microsoft Office applications support auto-macros: macros that are called automatically when a particular event occurs. Auto-macros are given specific names that determine when the macro should be called. In Microsoft Word, for example, the AutoOpen macro is called when opening a document. Before printing a document the application executes FilePrint.

Macros may also be associated with a key, or an event. They are executed when a certain key (or key-combination) is pressed or when a particular event occurs.

Macro viruses that infect Microsoft Office documents generally employ one of the methods mentioned above in order to become active without the user explicitly invoking a macro. If a document is infected by one of these macro viruses, when the user accesses one of the menus such as **File Open**, or **File Save As**, the application will run one of the auto-macros and execute the virus code.

Most macro viruses take the form of standard Microsoft Office 97 macros. However, some employ a technique to hide their code. There are three known ways of doing this and they all use the property of a macro to create, edit and execute other macros. These viruses generally contain a small (sometimes polymorphic) virus macro loader that calls the built-in macro editor, creates a new macro, fills it with virus code, executes it and then destroys it to eliminate all traces of the virus's presence. The code of such viruses is stored either in the virus itself in the form of text strings (which are sometimes encrypted) or in document variables or Autotext areas.

All Microsoft Office applications are able to encrypt macros within a document. Therefore some viruses within documents may be encrypted.

Microsoft Office viruses may infect not only PCs running Microsoft Windows, but also computers of any type that can run Microsoft Office. For example, a virus in a document created using Microsoft Word for Windows may infect a system running Microsoft Word for the Macintosh.

13.1.2. Suspicious macro instructions

Macro instructions that can be used to enable a virus to replicate itself or perform some harmful activity may be treated as *suspicious*. However, these instructions may also be used by normal, benign macros.

The tree above (Figure 92) shows macro instructions that may be considered suspicious. For convenience, suspicious macro instructions may be classified into four groups.

Macro events. Normal macros rarely change the code of other macros and hardly ever change their own code. Therefore code changes indicate with a high probability the presence of a macro virus. Macro events may be further divided into two sub-groups. The first group, module operations, enables a macro to create, add, copy, export and import modules. The second group, macro code changes, allows a macro to insert, delete and replace lines of code.

File operations. Macro instructions that can manipulate files may also be considered suspicious. For example, if the macro contains commands that can be used to delete files it may destroy your data.

Other commands. This group includes macro instructions that can change the document's anti-virus protection, instructions that can start external applications (the Shell command), working with ActiveX objects and emulating keystrokes. These macro instructions may also be employed by viruses.

API function calls. A virus may call operating system functions using the API interface in order to perform harmful actions without using Visual Basic commands.

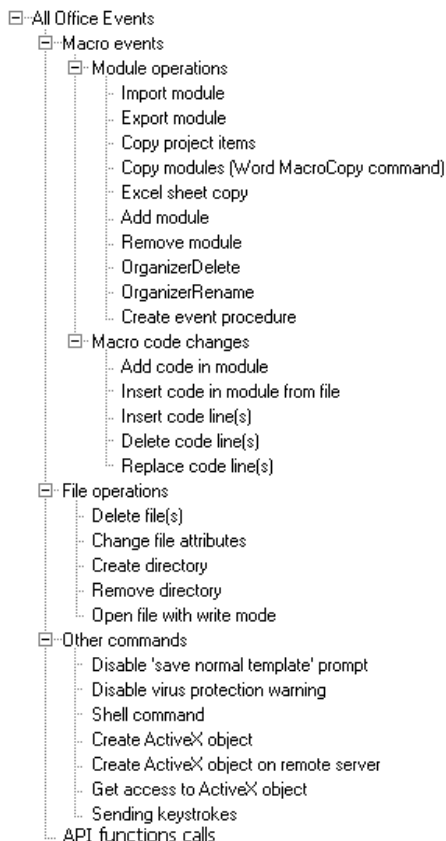




Figure 92. Suspicious Macro Instructions


13.1.3. Detecting macro viruses. Rules for suspicious macro instructions


Kaspersky® Office Guard fully controls macros execution in the Microsoft Office 2000 applications. When Kaspersky® Office Guard intercepts a macro trying to execute a suspicious instruction, it will take action depending on the rule

assigned to that particular instruction (see subchapter 13.3.1). Kaspersky® Office Guard takes one of four actions with the macro: permits it, prohibits its execution, terminates it, or asks a user about further actions. The action taken by Kaspersky® Office Guard that corresponds to a macro's instruction is called the *rule for a macro instruction*. These rules are identified by the following icons:

 **Permit** – allows the macro instruction to be executed;

 **Ask** – asks the user what to do when a macro attempts to execute this instruction;

 **Denied** – does not execute this macro instruction, but allows the macro to continue execution at the next instruction;

 **Terminate macro execution** – terminates the macro immediately.

For example, you can assign the following rules: automatically deny all macros that attempt to execute the most dangerous actions, ask for permission to run a macro instruction of copying Microsoft Excel spread sheets, permit execution of the macro instruction of creating procedures, or ignore all other suspicious macro instructions. In Figure 93, the icon displayed on the left of every instruction indicates the rule assigned to this instruction. The rule that is applied when an instruction is executed by a macro is identified by the icon displayed alongside it.

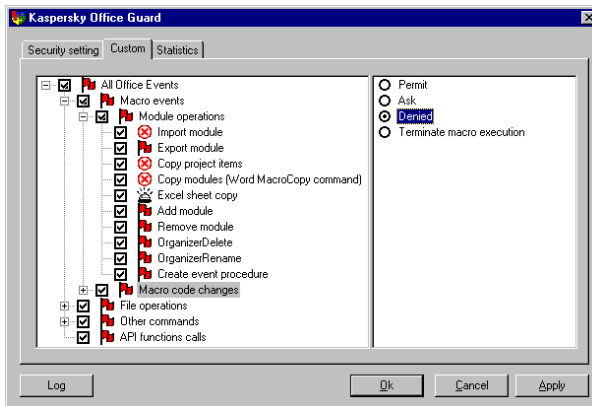


Figure 93. Example. The rules for suspicious macro instructions.

13.2. Kaspersky® Office Guard Interface


13.2.1. Launching the program

Each time you run any of the Microsoft Office 2000 applications, the *service part of Kaspersky® Office Guard* is launched on your computer. This service part acts as an anti-virus guard, which is activated when a suspicious macro instruction is trying to execute. The second, *interface part of Kaspersky® Office Guard* is launched either automatically, when the service part finds a suspicious instruction, or manually, when you want to edit the anti-virus settings.




To start the interface of Kaspersky® Office Guard on demand,

1. Click **Start**.
2. Select **Programs**.
3. In the menu, select **Kaspersky Anti-Virus®** and then **Kaspersky® Office Guard**.

After the interface part is loaded, you can see the Kaspersky® Office Guard icon  in the system tray of your Windows taskbar.



To open the Kaspersky® Office Guard main window, select the **Show settings** item in the system menu (13.2.2) or double-click the icon  in the Windows system tray (Figure 94).

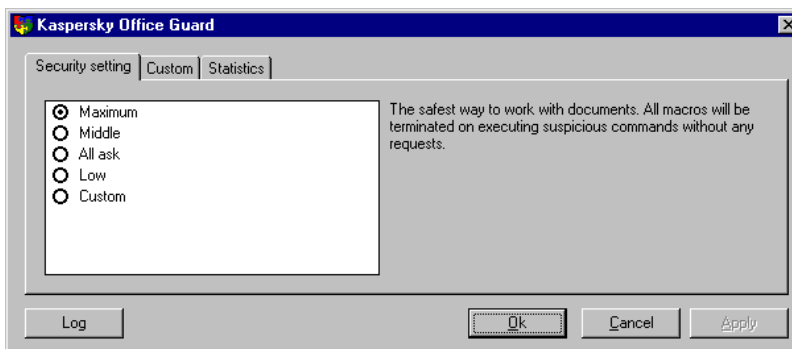


Figure 94. The Kaspersky® Office Guard user interface

13.2.2. System menu

To control the operation of the Kaspersky® Office Guard interface, use the system menu (Figure 95).




To display the system menu of the Kaspersky® Office Guard interface, right-click the icon  in the Windows system tray.



Figure 95. The Kaspersky® Office Guard system menu

The menu offers the following options:

- **Show settings** – displays the main window and allows settings to be changed;
- **Disable Kaspersky® Office Guard/Enable Kaspersky® Office Guard** – suspends/resumes the operation of Kaspersky® Office Guard. When the program is suspended the instructions executed by your macros are not monitored;
- **Close automatically** – closes the Kaspersky® Office Guard interface once all Microsoft Office 2000 applications are closed;
- **About** – displays details of the program;
- **Help** – displays the Help Topics window;
- **Close** – closes the Kaspersky® Office Guard interface immediately.



If you select **Close**, the system service that monitors macro activity will remain running.

13.2.3. Main window

The Kaspersky® Office Guard main window contains three tabs: **Security settings**, **Custom**, and **Statistics**. The **Security settings** tab allows you to set the monitoring of Kaspersky® Office Guard to a suitable level, and the **Statistics** tab allows you to view the statistics of the program performance. On the **Custom** tab, you can view the rules corresponding to the selected security level and change these rules.

To perform selected actions, the program uses dynamic menus; therefore, the main window does not have the usual standard menus.

13.2.4. Closing the program



To close the Kaspersky® Office Guard interface, select the **Close** option in the system menu.



After you close the user interface, the system service keeps on running.

13.2.5. Help topics

When working with Kaspersky® Office Guard, you can refer to the Office Guard Help.



To get help, select the **Help** option in the system menu.



To get context-sensitive help for an element of the interface, right-click the element or press <SHIFT>+<F1>.

13.3. Custom settings

13.3.1. Custom security level



To select a level of anti-virus protection,

1. Go to the **Security settings** tab (Figure 94).
2. Select the required security level:
 - **Maximum** – the level of maximum anti-virus protection (see subchapter 13.3.2).
 - **Middle** – the level of medium anti-virus protection (see subchapter 13.3.3).
 - **All ask** – at this level, Kaspersky® Office Guard will ask the user to choose what to do whenever a macro attempts to execute a suspicious instruction (see subchapter 13.3.413.3.4).
 - **Low** – the level of low anti-virus protection (see subchapter 13.3.5).
 - **Custom** – at this level, you can determine the action to be taken for each type of macro instruction. The settings are customized on the **Custom** tab (see subchapter 13.3.6).



The **Custom** tab is available only if you have the license key. The **Middle** level is most appropriate for most users. The **Low** level is not recommended.

13.3.2. Maximum security level

If the maximum security is enabled, the program will automatically terminate all macros that attempt to execute a suspicious instruction (Figure 96).

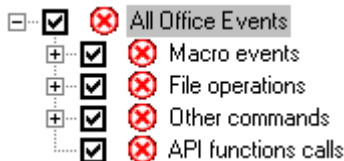


Figure 96. List of rules at the maximum security level
(the icon indicates termination of a macros)

13.3.3. Middle security level

At the middle security level, the program will prohibit execution of most suspicious macro instructions and terminate all macros that attempt to execute one of the following most dangerous instructions: **Import module**, **Copy modules**, **MacroCopy**, **Excel sheet copy**, **Delete files**, **Disable 'save normal template' prompt**, **Disable virus protection** (Figure 97).



The **Middle** level is appropriate for most users.

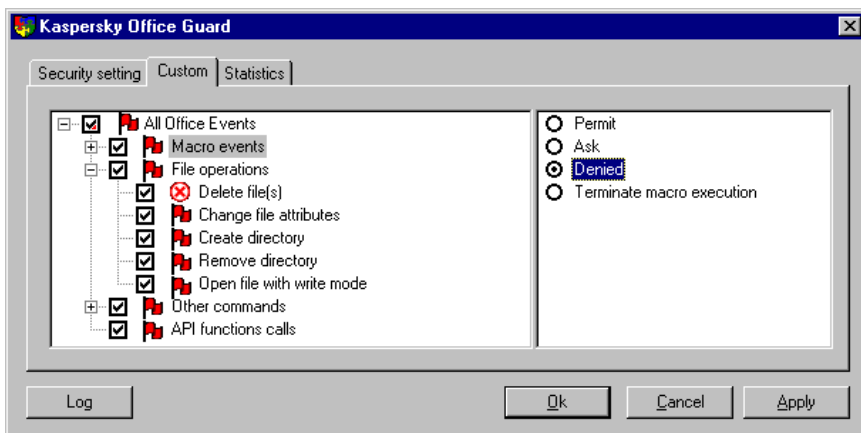


Figure 97. List of rules at the middle security level (the icon indicates termination of a macro and the icon indicates denial of a suspicious macro instruction)

13.3.4. All ask level

At the **All ask** level, Kaspersky® Office Guard will ask the user what to do each time macros attempt to execute a suspicious instruction (Figure 98).

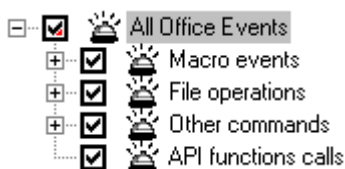


Figure 98. List of rules at the **All ask** level
(The icon indicates that the user will be asked about actions to be taken)

13.3.5. Low security level

At the low security level, the program will automatically permit all macro instructions apart from the most dangerous. The user will be asked what to do if the macro attempts to execute a dangerous instruction (Figure 99).

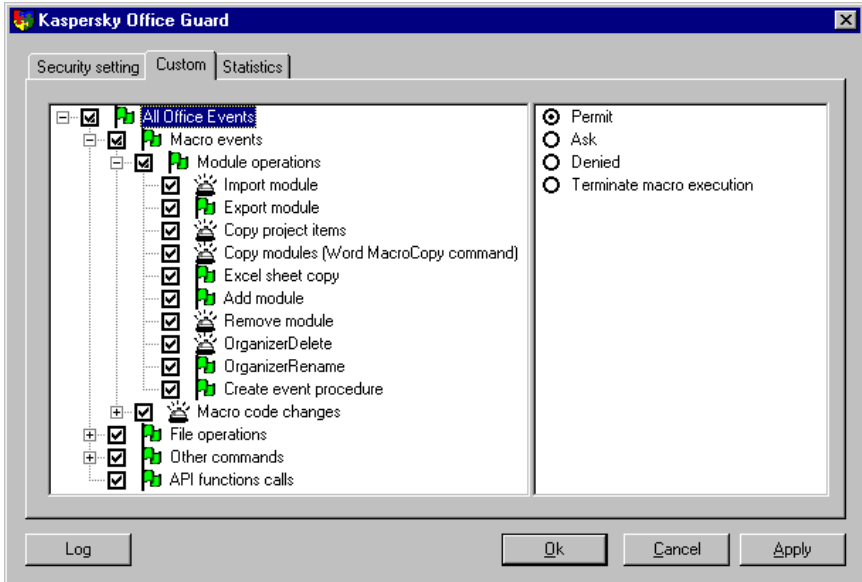




Figure 99. List of rules at the low security level (the icon  indicates that the user will be asked about actions to be taken, and the icon  indicates that a suspicious macro instruction is permitted)

13.3.6. Custom level

In some cases, you may want to assign your own settings to certain suspicious instructions.



Example. In your routine activities, you use a macro that is flagged as executing a suspicious instruction. Kaspersky® Office Guard regularly asks you if you want to permit this instruction. To avoid this, you can set your own security level, which would allow this suspicious instruction to be executed by default.



To customize the security level that is most convenient for you,

1. In the Kaspersky® Office Guard main window, go to the **Custom** tab (Figure 100).
2. On the **Custom** tab, change the rules for suspicious instructions in the *settings tree* (see below for information about the settings tree).

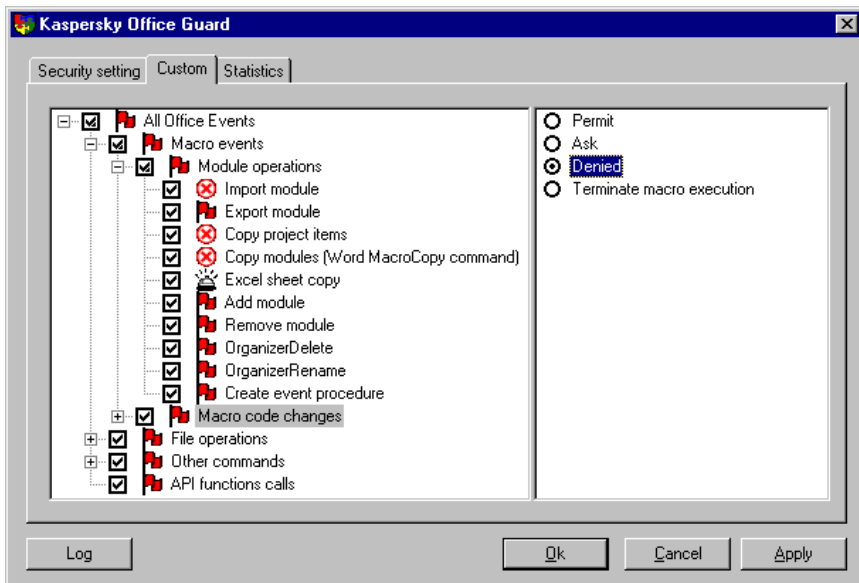


Figure 100. Customizing security settings

The **Custom** tab is divided into two frames. In the left frame there is a tree showing all suspicious macro instructions, checkboxes, and icons that indicate the rules assigned for a certain instruction. In the right frame there are option buttons indicating the name of the selected rule.

You can change the statuses of the checkboxes in the settings tree, as well as rules for certain macro instructions and groups of instructions.

Depending on user-defined settings, macro instructions can obey the rules defined for the group, have their own rules, or have rules strictly independent from those defined for the group, i. e., they can be excluded from the inheritance rules.







To change the status of the selected macro instruction or a group of macro instructions,

1. Select an appropriate line in the settings tree.
2. Check / Uncheck the corresponding box by clicking it with the mouse, or alternatively, right-click the item and select the **Check Node (Uncheck Node)** item from the pop-up menu.

The macro instruction check box can have various statuses (see subchapter 8.3).



To assign a rule for a suspicious macro instruction or a group of macro instructions,

1. Select an appropriate line in the settings tree.
2. Set a rule to be applied when an instruction is executed by a macro.
 - **Permit** – allows the suspicious macro instruction to be executed (this rule is indicated by the “green flag”  on the left of the corresponding macro in the settings tree);
 - **Ask** – asks the user what to do when a macro attempts to execute this instruction (this rule is indicated by the “ringing bell”  on the left of the corresponding macro in the settings tree);
 - **Denied** – does not execute this macro instruction, but allows the macro to continue execution at the next instruction (this rule is indicated by the “red flag”  on the left of the corresponding macro in the settings tree);
 - **Terminate macro execution** – terminates the macro immediately (this rule is indicated by the “No stop” road sign  on the left of the corresponding macro in the settings tree).

Depending on whether you change the settings for a group or a separate macro instruction, the settings tree also changes.

13.4. Interception of suspicious macro instructions

When Kaspersky[®] Office Guard intercepts a macro trying to execute a suspicious instruction, it will take action depending on the rule assigned to that particular instruction (see subchapter 13.3.1). Kaspersky[®] Office Guard takes one of four actions with the macro: permits it, prohibits its execution, terminates it, or asks a user about further actions.

If the Ask rule was assigned for a particular suspicious instruction, you will see the **Kaspersky[®] Office Guard – Permit this action?** dialog box ().

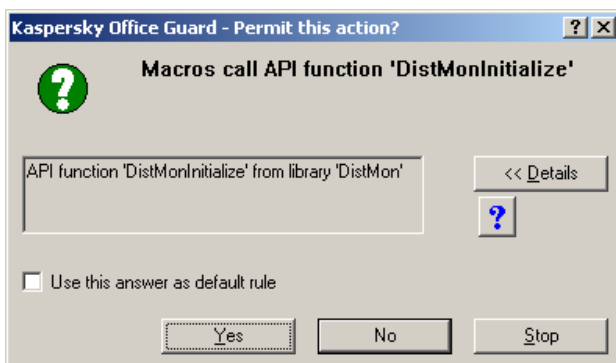



Figure 101. Asking the user about actions to be performed

In the upper part of the dialog box you can see what suspicious instruction a macro tried to execute. For more information about this instruction click the

Detail button, and to learn about its potential danger click the  button.

The lower part of the dialog box has three buttons that you should use to select an appropriate action:

- **Yes** – permits execution of the suspicious instruction.
- **No** – prohibits execution of the suspicious instruction.
- **Stop** – terminates execution of the macro.



To set a default rule for the selected action for this suspicious instruction, check the **Use this answer as default rule** box.



The **Use this answer as default rule** box is available only if you have a key file.

If you check the **Use this answer as default rule** box, the rule selected for this suspicious macro instruction will be recorded into the settings tree. You can view changes in the settings tree.

If the macro instruction was assigned the **Ask** rule and the status of “strictly independent”, the new rule will be independent.



You have to make your own decision about whether some suspicious actions are caused by a macro. After your decision, it is necessary to delete the virus code or send the infected macro to your system administrator. The Help topics have information that can help you make the right decision.

13.5. Log

The **Log** button starts Kaspersky® Report Viewer, which allows you to see a log of the actions taken by Kaspersky® Office Guard to protect your computer and your Microsoft Office 2000 documents from malicious macros.

The log contains:

- the time when a macro tried to execute a suspicious instruction;
- the suspicious instruction;
- the action performed by Kaspersky® Office Guard: **permitted** – if the suspicious instruction was permitted, **denied** – if it was prohibited, and **terminated** – if the macro was terminated.

You can view the statistics on the program performance on the **Statistics** tab of the main window (Figure 102).

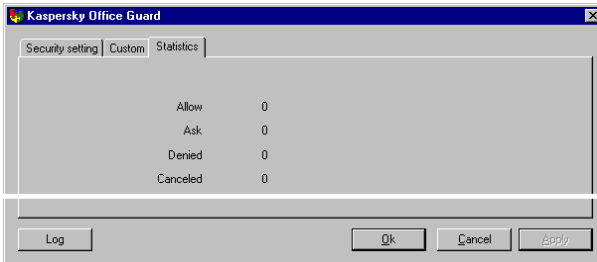


Figure 102. The **Statistics** tab

CHAPTER 14. KASPERSKY® INSPECTOR

Kaspersky® Inspector is an integrity checker running under Microsoft Windows 95 OSR298/ME® or Microsoft Windows NT/2000®.

Kaspersky® Inspector checks disks for modifications in files and directories. The program can be used as a supplementary anti-virus program to monitor changes on the disk.

The program reduces the time you need to check your computer using the Kaspersky AV Scanner, since your Kaspersky® Inspector will provide the scanner with information about the files that have been changed or created, and the scanner will check for viruses in those files only.

While checking for changes on your disk the program collects data and saves it to a table. This table contains images of your master boot and boot records, a list of bad clusters, a schema of your directory tree and information about every controlled file.

Kaspersky® Inspector accesses your disks directly via the IOS (Input-Output Supervisor) driver without using the conventional methods (the 21h and 13h interrupts). This feature allows the program to detect and kill even the most dangerous stealth viruses that settle themselves in the computer memory and process those vital interrupts.

In addition, Kaspersky® Inspector remembers and, when started again, checks the size of available DOS memory (most boot viruses change the size of random access memory), and the quantity of hard drives installed.

The main features of Kaspersky® Inspector are the following:

- it accesses the disks directly via the IOS (Input-Output Supervisor) driver, bypassing DOS resident viruses (boot viruses in particular, since they intercept the 13h interrupt when the computer is booted).
- it allows you to recover boot sectors on the disks.
- it allows you to check compressed drives.
- it reads FAT12, FAT16, VFAT32, NTFS file systems without using the corresponding OS functions.
- it analyses files while searching for changes in their sizes.
- it processes OLE2 documents (Word, Excel and Access documents).

- it allows you to recover DOS and Windows 98/NT executable files (Kaspersky AV Cure Module provides this possibility).
- it detects stealth viruses in the wild.

14.1. Features of Kaspersky[®] Inspector Under MS Windows NT

Due to architectural features of Microsoft Windows NT[®], while running in this environment Kaspersky[®] Inspector does not check:

- debug registers;
- the size of available DOS memory.

Other functions of Kaspersky[®] Inspector are performed under Microsoft Windows in corpora.

14.2. The Operating Concept of Kaspersky[®] Inspector

While searching for modifications on a hard drive all disk inspectors (also called CRC scanners or integrity checkers) utilize the same algorithm. The program performs the following tasks:

- Calculates mathematical values known as checksums or CRC values (for Cyclic Redundancy Code) for disk sectors and files.
- Stores these CRCs in a database (table).
- When started up again the disk inspector recalculates these values and checks them against the database.

The disk inspector also stores other information such as file sizes, the latest modification date and time, file attributes and other details that are required to recover modified (infected) files. The database also contains comprehensive patterns of the hard disk master boot record and boot sectors, a list of fail clusters, a subdirectory tree and other information about the objects inspected.

In addition, Kaspersky[®] Inspector remembers and, when started again, checks information about your operation system and the hardware, i.e. the RAM capacity (checking for boot viruses) and the number of your hard disks.

Kaspersky[®] Inspector accesses the disks directly via the IOS (Input-Output Supervisor) driver without using the conventional methods (the 21h and 13h

interrupts). This feature allows the program to successfully detect and kill even the most dangerous stealth viruses (see subchapter 14.2.3).

14.2.1. Checks that Kaspersky® Inspector performs

When started the first time Kaspersky® Inspector collects data about your RAM capacity in DOS and the address of your INT 13h handler. The program then saves this data in a special database (table).

When started up again Kaspersky® Inspector:

- checks your RAM capacity in DOS and the address of INT 13h handler.
- checks the master boot and boot records. The program checks the master boot record while processing all the logical drives. If the collected data doesn't match the database, the program recovers the sector. Furthermore, you can use the built-in viewer to compare the database data against the data collected by Kaspersky® Inspector during the check.
- checks numbers of bad clusters. There are viruses that mark a good cluster as the fail one and use it to place their code or data. If a new bad cluster is detected Kaspersky® Inspector informs you about this event.
- checks the directory tree on your disk. The program searches for directories that have been created or deleted.
- checks the file structure of your disks. The program searches for files that have been created, deleted, renamed or changed. While checking files Kaspersky® Inspector looks for any modifications in their size, the date and the time of creation and their CRCs.

Kaspersky® Inspector analyzes all changes detected and, if they do not indicate a virus presence (for example, changes in the file size are accompanied by the appropriate changes in the date and the time this file was saved to the disk), the program will screen the appropriate statistics window. But if Kaspersky® Inspector detects suspicious modifications that look like a virus manifestation, a warning message will appear on your screen.

14.2.2. Analyzing changes on your disk

All changes that have been detected by the program during the check are analyzed and divided into the following two groups: **harmless** and **suspicious**. For example, if the contents of a file changed, and the date and time when it was created changed also, this does not indicate a virus presence. These changes are harmless.

In any case, Kaspersky® Inspector provides you with information about all the changes detected. You can view these statistics in the dialog mode and, furthermore, you can save them to your hard drive in the form of a text file. If the program detected any suspicious changes, it informs you about the possibility that your computer is infected.

The following changes can indicate the **presence of a virus**:

- file contents changed while the date and the time of last modification remained the same (these changes can indicate the presence of a file virus on your computer);
- similar changes in the size of two or more files;
- the date and the time of last modification of a file are not valid: the date is more than 31, the month is more than 12, the year is more than the current one or the time exceeds 59 minutes, 23 hours or 59 seconds (some viruses use this method to mark infected files);
- a file registered in the list of unchangeable files is changed;
- changes indicating the presence of viruses infecting the DOS kernel (the IO.SYS, IBMBIO.BIN and... files).



Never ignore messages about changes detected on your drive by Kaspersky® Inspector (especially if the changes are suspicious). If the reason for the changes is unknown, you must investigate it.

If the program messages contain technical information that you do not understand, refer to a qualified expert or to the Kaspersky Labs Help Desk department. THESE MESSAGES MUST NOT BE IGNORED!



DISREGARD OF THESE RECOMMENDATIONS MAY RESULT IN INFECTION OF YOUR COMPUTER AND INCREASES THE PROBABILITY OF DATA LOSS.

14.2.3. Searching for stealth viruses

The term *stealth* describes viruses that use certain methods to mask their presence in the system. To hide themselves they intercept calls to infected objects and accordingly modify appropriate data blocks so that these files and sectors in infected system appear to be virus free. There are viruses using various methods to hide themselves in a system and sometimes these methods are extremely complicated. You should also know that there are stealth viruses of all types: file viruses, boot viruses and macro viruses can all possess stealth functions. For more information about stealth viruses refer to the *Virus Encyclopaedia*.

If a virus uses some methods to hide itself in a system, it cannot be detected using conventional anti-virus tools because when these tools open and read data from a file infected with a stealth virus they collect only virus-free data and the virus code remains unnoticed. To detect such a virus you must use so-called anti-stealth technology (for example, direct reading of data from the disk).

Kaspersky® Inspector uses the most reliable anti-stealth methods, which allow the program to efficiently detect both well-known and unknown stealth viruses.

You should know that the ability to hide in a system is in fact the weak point of stealth viruses. We developed a method that, though complicated, allows Kaspersky® Inspector to detect practically any stealth virus in a system. To detect a stealth virus the program checks contents of the boot sector or the suspicious file using two different methods, and then compares the results.

The first method of reading is conventional and entails reading data via the operation system.

The second method of reading entails reading data directly, i.e. bypassing the operating system.

If a stealth virus is present in the system, the results of the two checks (using two different methods) will differ, since viruses can intercept a conventional call only and cannot interfere in the direct reading operation. The comparison technique based on this method is implemented in Kaspersky® Inspector (for details about how to enable the anti-stealth mode see subchapter 14.5.2.5).

14.2.4. Deleting viruses using the Kaspersky AV Cure Module™

14.2.4.1. The Kaspersky AV Cure Module for Windows

Kaspersky AV Cure Module™ (KAVIC) is a built-in program module (*cure.dll*) that detects and deletes computer viruses without using the anti-virus bases.

The fundamental concept of KAVIC operation differs from that of anti-virus scanners. The difference is that KAVIC has some information about the protected files, but knows nothing about the virus. According to Kaspersky Labs internal tests, KAVIC completely recovered files in 96% of all cases (these statistics cannot be considered an axiom, since results of the recovery procedure depend on various external conditions). KAVIC will allow you to detect and delete most viruses whether they are known or not.

While running, Kaspersky[®] Inspector informs KAVIC about files that have been created or deleted since the last check. In its turn, KAVIC collects data that is required to recover the files.

The current KAVIC version recovers (cures) DOS and Windows files (files with the EXE, COM, SYS, PRG, DLL, SCR, OCX and etc. extensions).

14.2.5. Checking the OS parameters during the boot (the KAVIBOOT.VXD driver)

The *KAVIBOOT.VXD driver* checks some parameters of your operation system (Windows 95 OSR2/98) while it is booted. The driver checks:

- available DOS memory;
- the master boot record (MBR);
- the INT 13h handler addresses (reading/writing to the disk).

Those checks allow you to detect a boot virus in your system.

While reading from sectors, Kaspersky[®] Inspector calls your BIOS directly, bypassing the DOS handlers. In addition, the driver utilizes a special mechanism of protection from virus attempts to intercept the data read from the disk.

This system of protection from interception can result in driver hang-up. But these cases are extremely rare. To reduce such a possibility, the driver, when started the first time, automatically checks itself for hang-ups.

If, when you install Kaspersky[®] Inspector and restart your computer, the computer hangs up, you must restart it again. In this case the driver will understand that the system was restarted after an improper shutdown, and will not use these procedures again.

14.3. Kaspersky[®] Inspector Interface

14.3.1. Main window

If you start Kaspersky[®] Inspector without using any command line switch (see subchapter 14.3.6) the program main window will appear on your screen (Figure 103).

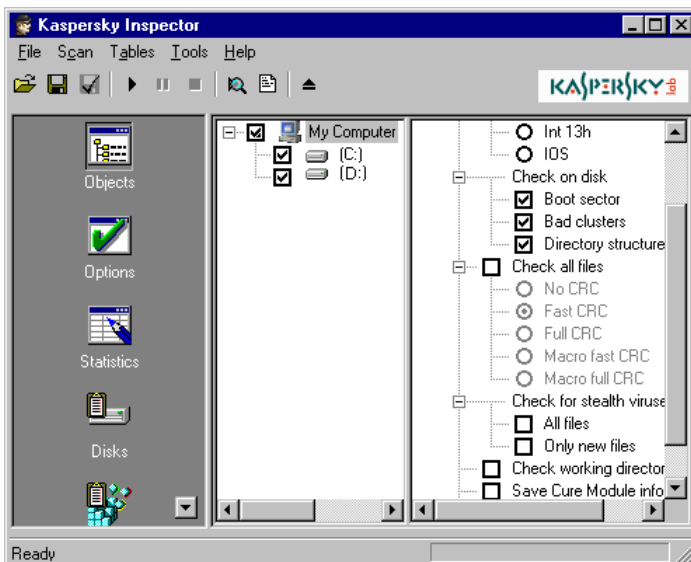


Figure 103. The Kaspersky® Inspector main window

In the program main window you will find the following items:

- menu bar (see subchapter 14.3.2);
- tool bar (see subchapter 14.3.3);
- icon bar (see subchapter 14.3.4);
- work area (see subchapter 14.3.5);
- status bar (see subchapter 15.3.6).

14.3.2. Menu bar

Right below the main window title you can find a menu bar (Figure 104).

File Scan Tables Tools Help

Figure 104. Menu bar

Use commands in these menus to initiate features that are available in your Kaspersky® Inspector. Table 1 below describes the menu commands.

Table 1. Menu commands

Menu	Command	Function
File	Save profile as default	Sets the current profile to be loaded by default
	Load profile	Allows you to load settings from one of the existing profiles (see subchapter 14.5.3)
	Save profile	Saves settings that you selected to a profile (see subchapter 14.5.3)
	Save profile as	Allows you to save your current profile under a different name
	Unload	Allows you to exit the program
Scan	Start scan	Starts the check (see subchapter 14.4.4)
	Stop scan	Aborts the check
	Pause scan	Pauses the check
Tables	Create registry table	Allows you to create a new registry table (see subchapter 14.4.4.2)
	Create disk table	Allows you to create a new disk table (see subchapter 14.4.4.2)
Tools	Show report	Loads the Report Viewer program, allowing you to view results of the last check
Help	Contents	Displays the Help topics
	About	Displays a box containing information about the program developers, this version number and your registration details

14.3.3. Tool bar

Right below the main window menu bar you can see a tool bar (Figure 105) that contains buttons allowing you to perform the most frequently used functions of the program.












Figure 105. Too bar

Most buttons perform functions that may also be initiated with the appropriate menu commands (see subchapter 14.3.2). If you place your mouse cursor on a tool bar button a tip with the name of the button will pop up.

Table 2 below describes the tool bar buttons and the corresponding menu commands.

Table 2. Tool bar buttons

Button	Command	Function
 Load profile	The Load profile command in the File menu	Allows you to load settings from one of the existing profiles (see subchapter 14.5.3)
 Save profile	The Save profile command in the File menu	Saves settings that you selected to a profile (see subchapter 14.5.3)
 Save as default	The Save profile as default command in the File menu	Sets the current profile to be loaded by default
 Start scan	The Start scan command in the Scan menu	Starts the check (see subchapter 14.4.4)
 Pause scan	The Pause scan command in the Scan menu	Pauses the check

Button	Command	Function
 Stop scan	The Stop scan command in the Scan menu	Aborts the check
 Scan preview		Allows you to preview the program's current scan settings
 Report	The Show report command in the Tools	Starts Kaspersky® Report Viewer supplied with the distribution kit.
 Exit	The Unload command in the File	Allows you to exit the program

14.3.4. Icon bar






Right below the tool bar and at the left side of the main window you can see an icon bar.

This vertical bar contains five icons describing five groups of settings (see Table 3). To switch to a certain group of settings you must press the corresponding icon.

If you click your right mouse button in any place within the icon bar the right-click menu with the following two commands will appear on your screen:

- **Small Icons** – displays small icons in the bar;
- **Large Icons** – displays large icons in the bar.

Table 3. Icons in the icon bar

Icon	Function
 <p>Objects</p>	<p>Allows you to change settings defining locations and objects to be scanned, and how your Kaspersky® Inspector must treat infected objects. This group of settings is represented by a certain type of control – the <i>settings tree of the object hierarchy</i> (see subchapter 14.5.2)</p>
 <p>Options</p>	<p>Allows you to define settings that are general for all objects to be scanned, and also the rules according to which Kaspersky® Inspector must interact with other Kaspersky AV modules (Kaspersky AV Cure Module and KAV32). Here you can also define settings of the log file.</p>
 <p>Statistics</p>	<p>Displays a table with the program performance statistics (see subchapter 14.6.1)</p>
 <p>Disks</p>	<p>Allows you to view modifications that Kaspersky® Inspector detected while checking the objects and make changes using the right-click menu (see subchapter 14.6.2– 14.6.5)</p>
 <p>Registry</p>	<p>Allows you to view the complete results of checking the registry files and make changes using the right-click menu (see subchapter 14.6.6)</p>

14.3.5. Work area

Right below the main window tool bar and at the right of the icon bar you can see the main window work area. This area occupies the major part of the main window. Depending on the icon that you selected in the icon bar the work area can show various group of settings. For more details refer to the corresponding sections in this book (see subchapters 14.5 and 14.6).

14.3.6. Status bar

At the bottom of the main window you can see a status bar.

The status bar displays information about the current status of the program, and during the check you can see there the names of files that are currently being checked.

14.4. Starting Kaspersky[®] Inspector

14.4.1. Starting the program using the MS Windows Start menu

To start Kaspersky[®] from the **Windows Start** menu, click the **Start** button, point to **Programs**, point to **Kaspersky Anti-Virus[®]**, then point and click **Kaspersky[®] Inspector**.

14.4.2. Starting Kaspersky[®] Inspector using Control Centre

Kaspersky[®] Inspector as well as all other programs included in the Kaspersky AV package can be started from Control Centre. Using your Control Centre you can schedule Kaspersky[®] Inspector to start at certain time every day or within certain periods of time.

14.4.3. Starting the program the first time

When started for the first time Kaspersky[®] Inspector suggests that you create tables (Figure 106) for every object that is checked (see subchapter 14.5.2). These tables are critical for your Kaspersky[®] Inspector operation. If the tables are not created, Kaspersky[®] Inspector cannot check for modifications on your disks.

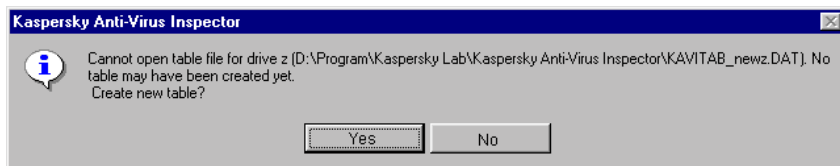


Figure 106. Suggesting creation of tables


For your Kaspersky® Inspector to create the tables automatically, click the **Yes** button. If you do this, the next time you start Kaspersky® Inspector the program will be able to detect modifications on your disks.

14.4.4. Starting to check for changes on your disk

14.4.4.1. Checking for changes on the disk

If in Control Centre you scheduled your Kaspersky® Inspector to start once a day or you started the program from the command line using the corresponding switch, then every day at the first start of your operating system Kaspersky® Inspector will be automatically launched to check for changes on your disks (see subchapter 14.2.1).

If you want to check for modifications on your disks at any other time, you must

click the  button in the main window toolbar. In this case the program will check for modifications in those objects that are defined in its settings (see subchapter 14.5.2).

14.4.4.2. Creating new tables

Sometimes (for example, when you install new drives on your computer or if the tables you had are corrupted or deleted) it is necessary to create new tables.

To create new tables for your disk, first you must mark it in the disks' tree by clicking on it with your mouse (see subchapter 14.5.2), then you must select one of the following commands from the **Tables** menu:

Create registry table – creates new registry tables. If you select this command the corresponding confirmation box will appear on your screen (Figure 107). To confirm your selection click the **Yes** button. After this, the new registry tables will be created.

Create disk table – creates new disk tables. If you select this command the corresponding confirmation box will appear on your screen (Figure 108). To confirm your selection click the **Yes** button. After this, the program will start creating new disk tables. Be patient, the procedure of creation may take some time.



Figure 107. Confirmation box to create new registry table

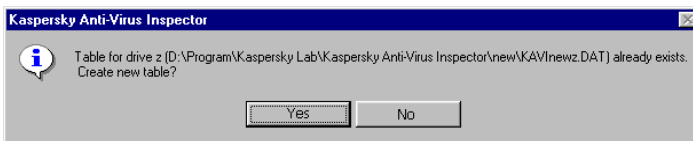



Figure 108. Confirmation box to create new disk table

14.4.5. Starting to search for stealth viruses

To start checking for stealth viruses in one or more objects (see subchapter 14.5.2), you must check the corresponding box in the **Objects** work area of the main window (see subchapter 14.5.2.5) and click the  button in the main window tool bar.

While running, Kaspersky® Inspector checks your master boot record and boot records of the logical disks, and also compares the file sizes and CRCs detected via your operation system against their actual sizes and CRCs calculated using the direct reading method. If the results differ, Kaspersky® Inspector immediately stops the check, so the virus will not have time to infect other files and sectors, and screens the corresponding alert message

14.5. Customizing Kaspersky® Inspector

14.5.1. The Options work area: selecting general options

To display general settings of your Kaspersky® Inspector, you must click the



icon in the main window icon bar (see subchapter 14.3.4). After this, the general options tree will appear in the main window work area (Figure 109).

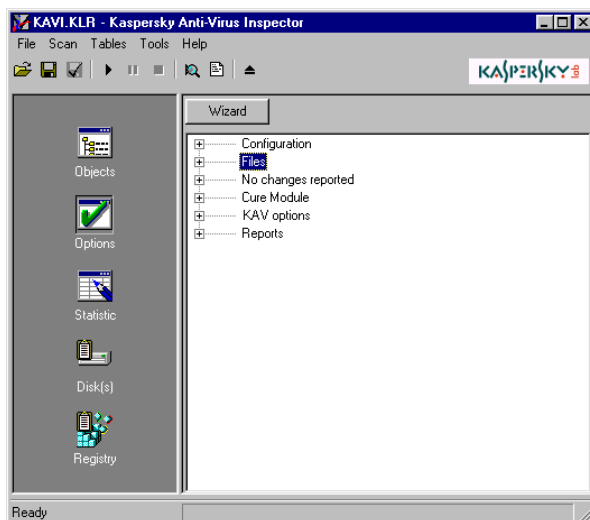


Figure 109. General options tree of the program

In the upper left corner of the options work area you can see the **Wizard** button. This is an easy-to-use tool that you can use to define general settings of the program. You can use the wizard to define and change the main settings only; other settings of the program can be changed directly in the **Options** work area



To define settings of the program using the wizard, follow the steps:

1. Click the **Wizard** button in the upper left corner of the work area.
2. The **Check Mode** wizard window (Figure 110) will appear on your screen. In this window you must select one of the available check modes. Click the **Next** button to move to the next window.

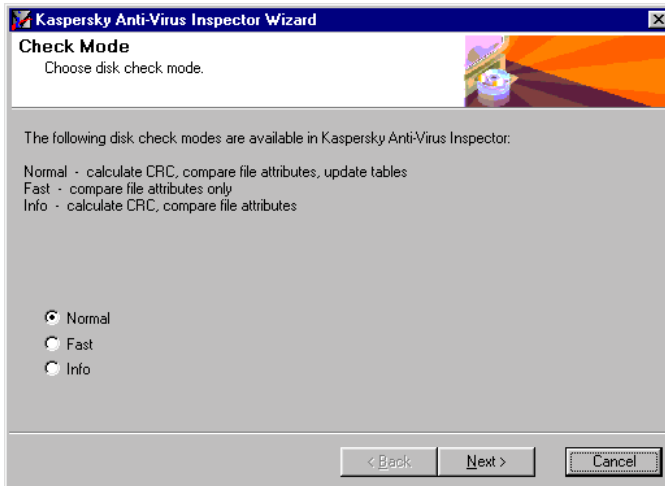


Figure 110. The **Check Mode** wizard window

3. The **File Types** wizard window (Figure 111) will appear on your screen. In this window you can see the list of file extensions that will be processed by Kaspersky[®] Inspector. You can also edit this list:

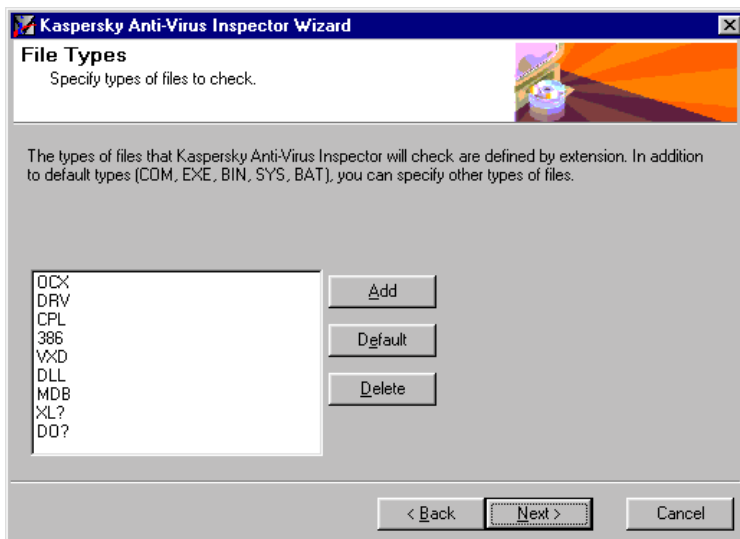


Figure 111. The **File Types** wizard window

- To add a new value to the list click the **Add** button. The **Add extension** dialog box (Figure 112) will appear on your screen. Enter the value in the **Extension** text field, and use the **CRC type** drop down list to select how you want to calculate CRC for files with this extension. Then click the **Add** button.

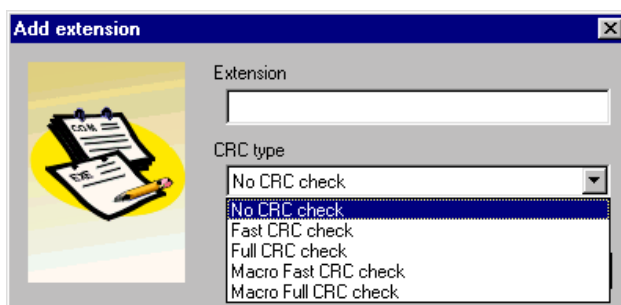


Figure 112. The **Add extension** dialog box



To define a set of extensions in the **Add extension** text field you can use the inquiry character (?) that denotes any character. For example, the value OV? in the text field denotes all files with the extension beginning with OV (OVL, OVR, ...).

- To remove a value from the list, highlight it in the list by clicking on it with your mouse and click the **Delete** button.
4. Click the **Next** button to move to the next window. The **Interaction with Kaspersky AV Scanner** wizard window (Figure 113) will appear on your screen. In this window you must specify the information that is critical for your Kaspersky® Inspector to interact with the anti-virus scanner on your computer. In this window you will find the following two input fields:

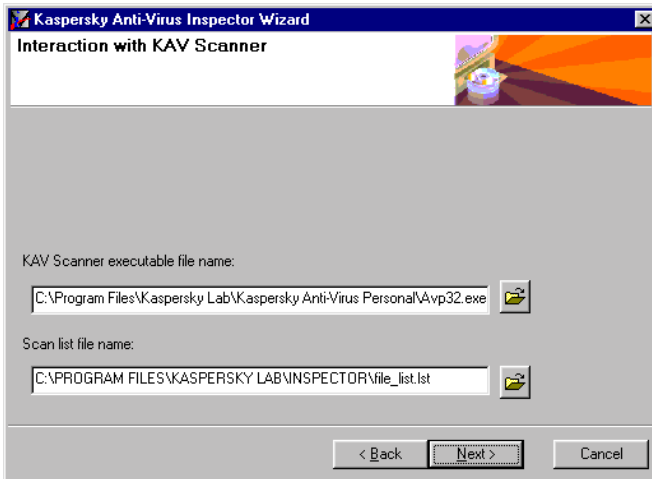


Figure 113. The **Interaction with Kaspersky AV Scanner** wizard window

- **Kaspersky AV Scanner executable file name** – in this field you must define the path to your KAV32 executable file. To do this, click the button at the right of the field and select this file in the dialog window on your screen;
 - **Scan list file name** – in this field you must define the path to a file where Kaspersky® Inspector will store the list of modifications detected in files. To do this, click the button at the right of the field and select this file in the dialog window on your screen.
5. Click the **Next** button to move to the next window. The **Report** (Figure 114) wizard window will appear on your screen. In the **Report file name** input field of this window define the path to a file where Kaspersky® Inspector will store reports describing results of the check. To do this, click the button at the right of the field and select this file in the dialog window on your screen.

6. When done, click the **Finish** button.

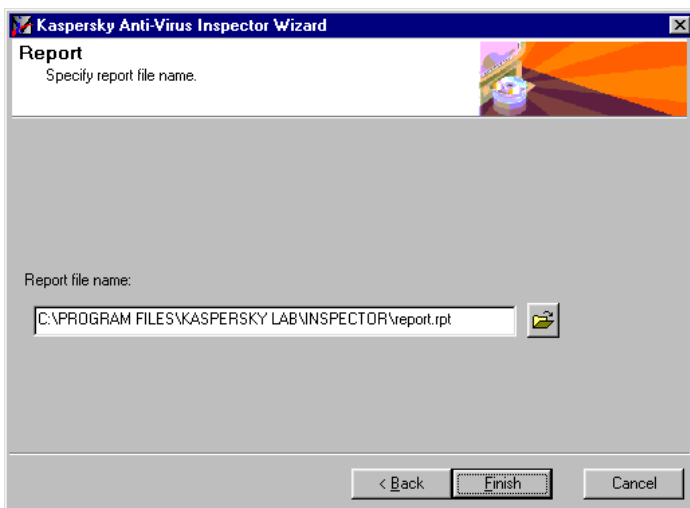



Figure 114. The **Choose Report file** wizard window

14.5.2. The Objects work area: selecting options for every drive to be checked

14.5.2.1. Defining check parameters for hard and logical drives



To define check parameters for your drives you must click the  icon in the main window icon bar (see subchapter 14.3.4). After this, the work area will split into two parts (Figure 115).

In the left part of the work area you will see a list of drives that can be checked, while in the right part you will see a settings tree.

By checking a box () in the drives list you will set the corresponding drive to be checked by your Kaspersky® Inspector.

You can define separate check parameters for each drive in the list.

The set of options that are available for an object in the list completely depends on the object type. Objects located on different levels of the drive hierarchy use different sets of options.

The maximum quantity of options is available for the **My Computer** object (see subchapter 14.5.2.2 – 14.5.2.6).

For local hard drives of your computer you cannot enable Kaspersky® Inspector to check registry files (see subchapter 14.5.2.6).

You cannot define how your Kaspersky® Inspector will access objects of logical drives (see subchapter 14.5.2.2); you also cannot define which elements of the drive must be checked by Kaspersky® Inspector (on these disks the program is able to check for modifications in the directory structure only) (see subchapter 14.5.2.3).

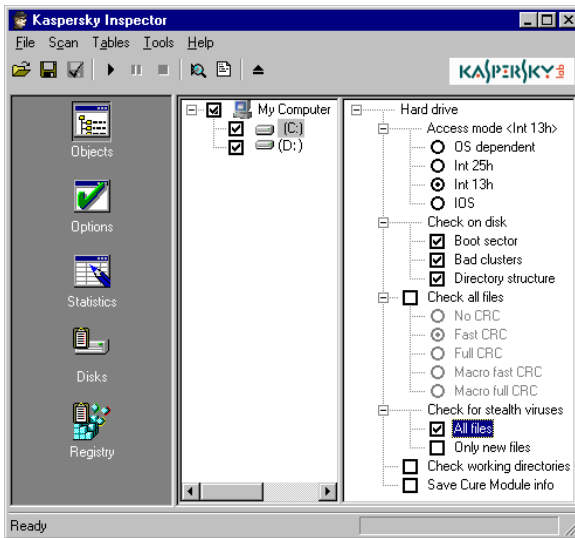




Figure 115. Parameters of drive checks

14.5.2.2. Defining how to access a drive


 **Access mode** – use this list of option buttons to define how your Kaspersky® Inspector must access the drive:

-  **OS-dependent** – enables Kaspersky® Inspector to access the drive using your operating system. In this case you can check for modifications on your network drives. If you defined this type of access

for a drive, your Kaspersky® Inspector will be not able to check for stealth viruses or check boot sectors and bad clusters on this drive.


- ⊙ **Int 25h** – enables Kaspersky® Inspector to access objects using the disk drivers (INT 25h). In this case the program bypasses DOS and reads the disk sectors directly, i.e. via the 25h interrupt (disk absolute reading). This mode can be used when checking for modifications on drives compressed using such programs as Stacker ver. 4.x or DriveSpace. The compression programs described above are supported by Kaspersky® Inspector. Such disks are displayed using special icons. If you use other compression programs that are not supported by Kaspersky® Inspector, you must define the access mode to the compressed disk as INT 25h.
- ⊙ **Int 13h** – enables Kaspersky® Inspector to access objects using INT 13h. In this case the program reads the disk directly via BIOS (the 13h interrupt). You can use this mode when checking for modifications on the physical drives **only**, i.e. in partitions of a fixed disk.
- ⊙ **IOS** – enables Kaspersky® Inspector to access objects using IOS (IO Supervisor). In this case the access type is determined by the following rules: if the 32-bit access to the disk (VFAT ("Dragon") drives) is used, protected-mode disk compression software is running (DriveSpace), or access to the disk is implemented via Real Mode Mapper, the program calls the 32-bit disk access driver (IOS) directly. Otherwise, the program accesses the disk via INT 13h or the disk driver. In other words, in almost all the cases Kaspersky® Inspector will access the drive via IO Supervisor. This option is available in Windows 9x only.

14.5.2.3. Items to be checked on the drive

 **Check on disk** – here you can define items that must be checked on the drive:

- Boot sector** – allows you to disable the check of boot records on the drive. This is useful, for example, for drives that have been created using the Stacker program (drive compacting system), since this program constantly modifies contents of the boot record.
- Bad clusters** – allows you to enable/disable the check for new fail clusters on the drive.
- Directory structure** – allows you to enable/disable the check for modifications in directory structure on the drive (detection directories that have been created or deleted).

14.5.2.4. Defining how to calculate CRC values

 **Check all files** – if checked, enables your Kaspersky® Inspector to check every file on the drive. This branch options are independent from those in the general settings tree (the **Options** icon).


The list of option buttons allows you to select how to calculate CRC values for the files:

- No CRC** – while checking files in this mode Kaspersky® Inspector will not calculate the files' CRC values. In this case the table describes only the size and the creation date and time for a file.
- Fast CRC** – this type of CRC value depends on the internal structure of DOS and Windows executable files, and while taking insignificant time allows you to reliably control the integrity of those files. It's strongly advised that you enable this mode for the COM, EXE, VXD, DLL, 386, CPL, SCR and other extensions of executable files.
- Full CRC** – CRC is calculated along the entire file contents. This type of check allows total control over the integrity of files, but it takes much more time than the previous check types. This check is advisable for files with the BAT and SYS extensions.
- Macro fast CRC** – this type of CRC value depends on the internal structure of macro documents (Microsoft Word®, Microsoft Excel® and Microsoft Access® documents) and allows reliable control over the integrity of OLE2 documents. This check is advisable for files with the DOC, DOT (DO?), XLS, XLA, (XL?) and MDB extensions.
- Macro full CRC** – this type of check allows the calculation of CRC along all the macros at large. It allows the most complete control over the integrity of OLE2 documents.



Macro CRC checks are advisable only for files that contain OLE2 macros. Currently, this check mode supports the following applications: Microsoft Word®, Microsoft Excel® and Microsoft Access®.

14.5.2.5. Checking for stealth viruses

 **Check for stealth viruses** – this joint allows you to check for stealth viruses on the drive:

- All files** – if checked, Kaspersky® Inspector checks for stealth viruses in every file on the drive.

- Only new files** – if checked, Kaspersky® Inspector checks for stealth viruses in new files only.



When checking on computer with the **All files** box checked the program searches only for stealth viruses.

Kaspersky® Inspector **does not check** for stealth viruses on drives that are accessed via the operating system (the **OS-dependent** access mode).

14.5.2.6. Advanced settings

- Check working directories** – if checked, the program checks working directories on this drive.
- Save Cure Module Info** – if checked, supports Cure Module performance for this drive.
- Check Registry** – if checked, the program checks registry files on this drive.

14.5.3. Saving and loading settings

You can save all settings to a special file with the *.klr extension.



To save all current settings to the hard drive of your computer, follow these steps:

1. Select the **Save profile as** command from the **File** menu.
2. In the Windows dialog box on your screen define the name and the location of a file where you want to save the settings.
3. Click the **Save** button.



To load settings from a file, follow these steps:

1. Select the **Load profile** command from the **File** menu.
2. In the Windows dialog box on your screen define the name and the location of a file that contains the required settings.
3. Click the **Open** button.


14.6. Viewing Check Results

14.6.1. The Statistics work area: viewing Kaspersky® Inspector performance statistics



To view your Kaspersky® Inspector performance statistics, follow these steps:



1. After a check procedure is launched, click the  icon in the main window icon bar.
2. The statistics window (Figure 116) allowing you to monitor the check will appear in the main window work area.

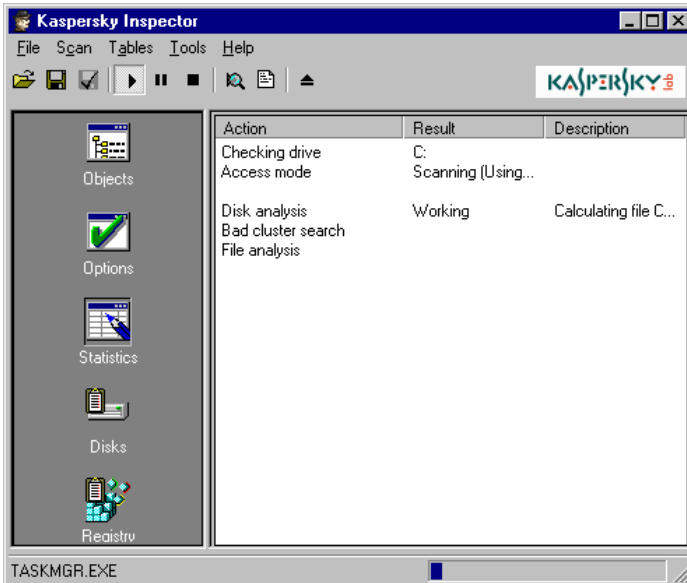


Figure 116. The performance statistics window

14.6.2. The Disks work area: viewing changes detected

After a check is completed the program will inform you and will offer to display the statistics of modifications detected (Figure 117).

To display a window containing the statistics of modifications detected during the check, click the **Yes** button in the confirmation dialog box.

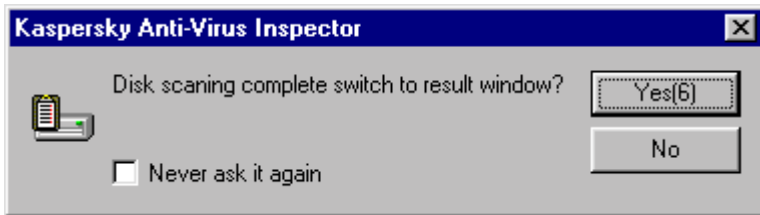


Figure 117. The confirmation dialog box to display statistics for changes detected

After this, the statistics will appear in the main window work area, indicating the number of modifications of all types (Figure 118).



If, while checking your disks, the Kaspersky® Inspector detected modifications that may indicate a virus manifestation, before displaying a list of all modifications on your disks the program will screen a warning message and a list of suspicious modifications

The modifications statistics window displays the following information about modifications detected: the quantity of files modified, deleted, renamed, moved and created; the quantity of directories created and deleted; and information about modifications in your master boot and boot records. To see more details about a certain type of modification, click the **Details** button at the right of the required list entry.

If necessary, you can view all the modifications detected in the form of a tree. To do this, switch to the **Tree view** tab (Figure 119).

On this tab page you can use right-click menu commands to work with files and folders in the tree (see subchapter 14.6.3).

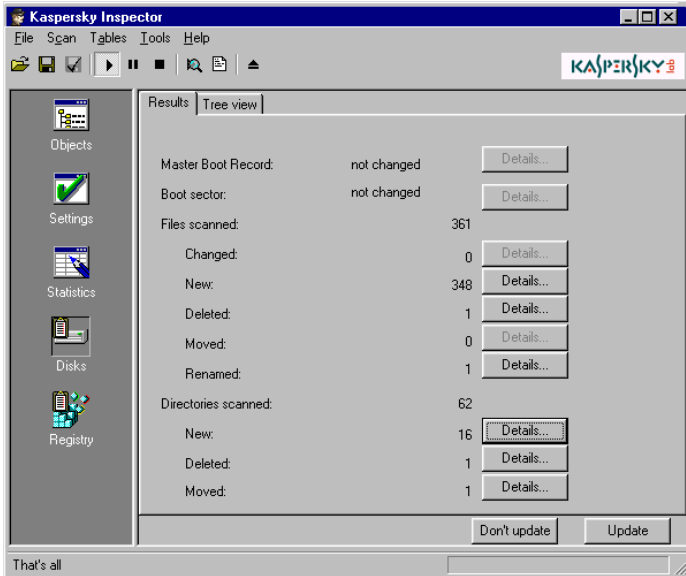


Figure 118. Statistics of modifications detected

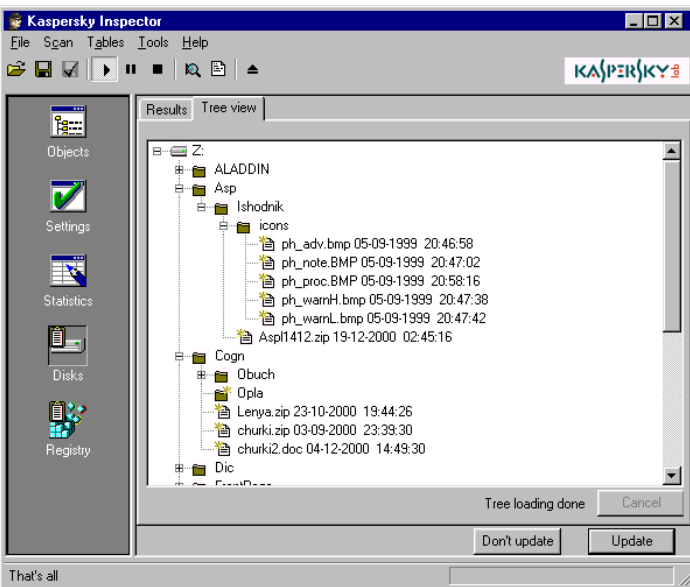
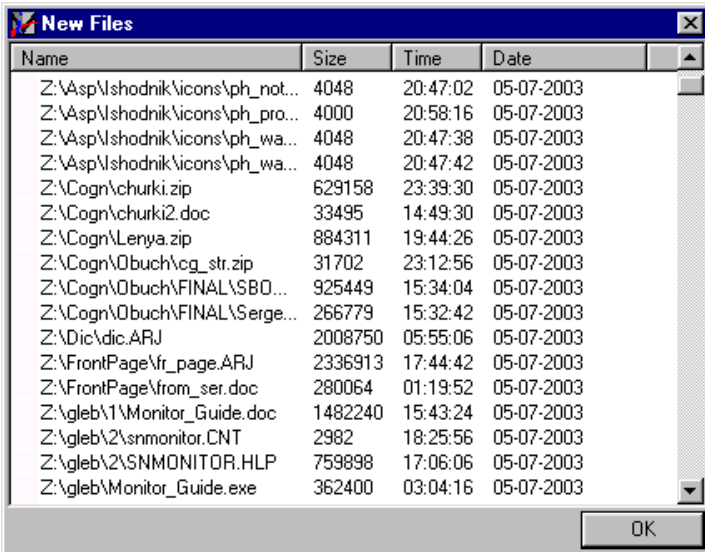


Figure 119. The modifications detected tree

14.6.3. The Disks work area: viewing changes detected

To see more details about a certain type of modification detected, display the modifications statistics window and click the **Details** button at the right of the required list entry.

After this, a window containing the list of modifications will appear on your screen (Figure 120).



Name	Size	Time	Date
Z:\Asp\shodnik\icons\ph_not...	4048	20:47:02	05-07-2003
Z:\Asp\shodnik\icons\ph_pro...	4000	20:58:16	05-07-2003
Z:\Asp\shodnik\icons\ph_wa...	4048	20:47:38	05-07-2003
Z:\Asp\shodnik\icons\ph_wa...	4048	20:47:42	05-07-2003
Z:\Cogn\churki.zip	629158	23:39:30	05-07-2003
Z:\Cogn\churki2.doc	33495	14:49:30	05-07-2003
Z:\Cogn\Lenya.zip	884311	19:44:26	05-07-2003
Z:\Cogn\Obuch\cg_str.zip	31702	23:12:56	05-07-2003
Z:\Cogn\Obuch\FINAL\SBDO...	925449	15:34:04	05-07-2003
Z:\Cogn\Obuch\FINAL\Serge...	266779	15:32:42	05-07-2003
Z:\Dic\dic.ARJ	2008750	05:55:06	05-07-2003
Z:\FrontPage\fr_page.ARJ	2336913	17:44:42	05-07-2003
Z:\FrontPage\from_ser.doc	280064	01:19:52	05-07-2003
Z:\gleb\1\Monitor_Guide.doc	1482240	15:43:24	05-07-2003
Z:\gleb\2\snmonitor.CNT	2982	18:25:56	05-07-2003
Z:\gleb\2\SNMONITOR.HLP	759898	17:06:06	05-07-2003
Z:\gleb\Monitor_Guide.exe	362400	03:04:16	05-07-2003

Figure 120. The list of new files detected

Kaspersky® Inspector allows you to work with the following types of modifications in the statistics window:

- files changed – the **Change** entry in the **Files scanned** section;
- files created – the **New** entry in the **Files scanned** section;
- files moved – the **Moved** entry in the **Files scanned** section;
- files renamed – the **Renamed** entry in the **Files scanned** section;
- directories created – the **New** entry in the **Directories scanned** section.

No other types of modification can be edited.



To edit the modifications described above you must use commands in the right-click menu.

While working with **files** that have been **modified** or **created** you can use the following commands:

- **Delete** – deletes the file.
- **Add to exclude list** – adds the file to the list files excluded from the check
- **Add to stable list** – adds the file to the list of files whose contents must not contain any modifications.
- **Check with KAV** – checks the file using your Kaspersky AV scanner
- **Check all with KAV** – checks all files in the list using your Kaspersky AV scanner.

Renamed or **moved files** can only be deleted. To do this, select the **Delete** command from the right-click menu.

While working with directories that have been created you can use the following commands:

- **Check with KAV** – checks the directory using your Kaspersky AV scanner
- **Check all with KAV** – checks all directories in the list using your Kaspersky AV scanner

14.6.4. The Disks work-area: master boot record details

If your Kaspersky® Inspector detected modifications in the master boot record of your computer a virus warning box with corresponding information will appear on your screen

To see the details of modifications detected in the master boot record, click the **Details** button at the right of the **Master Boot Record** entry in the statistics window.

The **Master Boot Record** details box (Figure 121) will appear on your screen.

In this box you can see which fields of the partition table have been modified. Usually viruses do not change the partition table, they change the loader. But there are some computer viruses that change the initial address of the active partition, leaving the loader unchanged. In addition, when you change your

operating system (or the version of your operating system) the loader also changes.



Attention! If your Kaspersky® Inspector detected modifications in the master boot record, we strongly advise that you investigate the cause!

F...	Start	End	FileSystemType	Size	Shift
80h	1/1/0	254/63/4	6	80262	63
0h	0/1/5	254/63/1023	15	59938515	80325
0h	0/0/0	0/0/0	0	0	0
0h	0/0/0	0/0/0	0	0	0

F...	Start	End	FileSystemType	Size	Shift
80h	1/1/0	254/63/4	6	80262	63
0h	0/1/5	254/63/1023	15	59938515	80325
0h	0/0/0	0/0/0	0	0	0
0h	0/0/0	0/0/0	0	0	0

DOS loader state: changed

OK

Figure 121. The **Master Boot Record** details box

14.6.5. The Disks work area: boot record details

If your Kaspersky® Inspector detected modifications in the boot record of your computer a virus warning box with corresponding information will appear on your screen.

To see the details of modifications detected in boot record, click the **Details** button at the right of the **Boot sector** entry in the statistics window.

The **Boot Record** details box (Figure 122) will appear on your screen.

In this box you can see which fields of the BIOS Parameter Block (BPB) have been modified. Usually viruses do not change BPB, they change the loader (frequently they change the JMP to loader and the OS manufacturer name). In addition, when you change your operating system (or the version of your operating system) the loader also changes.



Attention! If your Kaspersky® Inspector detected modifications in the boot record, we strongly advise that you investigate the cause!

Boot Record		
Property	Previous state	Current state
JMP to loader	EB 58 90	EB 58 90
DOS vendor label	MSDOS5.0	MSDOS8.0
Sector size	512	512
FAT count	2	2
Root entries count	0	0
Total sectors	0	0
Byte media descriptor	F8h	F8h
sectors count in FAT	4197	4197
Sectors per track	63	63
Heads count	255	255
Hidden sectors count	63	63
Total sectors	4305357	4305357
Physical media number	80h	80h
Extended BPB	29h	29h
Media serial number	-453373691	-453373691
Volume label	NO NAME	VIRUS__
File system type	FAT32	FAT32
DOS loader		CHANGED

Figure 122. The **Boot Record** details box

14.6.6. The Registry work area: viewing modifications in registry files

If you pre-set the program to check the computer registry files (see subchapter 14.5.2.6), you can view the list of modifications detected by clicking



the **Registry** icon in the main window icon bar. Statistics of the modifications detected in your system registry will appear in the main window work area (Figure 123).

If necessary, you can view all the modifications detected in the form of a tree. To do this, switch to the **Tree view** tab (Figure 124).

To view the list of registry keys that have been modified, created or deleted, click the **Details** button at the right of the list entry which details you would like to see. The information box listing corresponding modifications will appear on your screen (Figure 125).

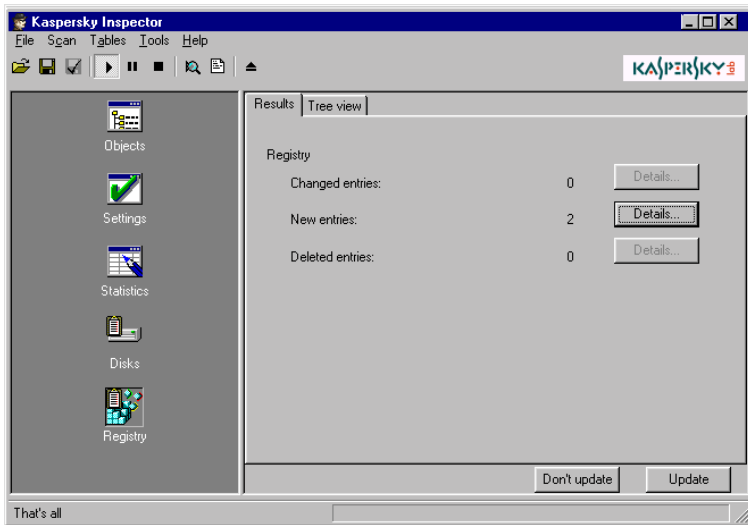


Figure 123. Statistics of modifications detected in the registry

Kaspersky® Inspector checks for modifications in those keys of your computer registry whose function is to automatically launch programs. Below, you can see a list of main program-launching keys:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones

HKEY_CURRENT_USER\Software\Microsoft\Office\8.0

HKEY_CURRENT_USER\Software\Microsoft\Office\9.0

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Runonce

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Runonce
ex

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Runservi
ces

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Runservi
cesonce

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runonce

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runonce
ex

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runservices

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runservicesonce

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion

HKEY_CURRENT_USER\Software\Mirabilis\ICQ\Agent\Apps

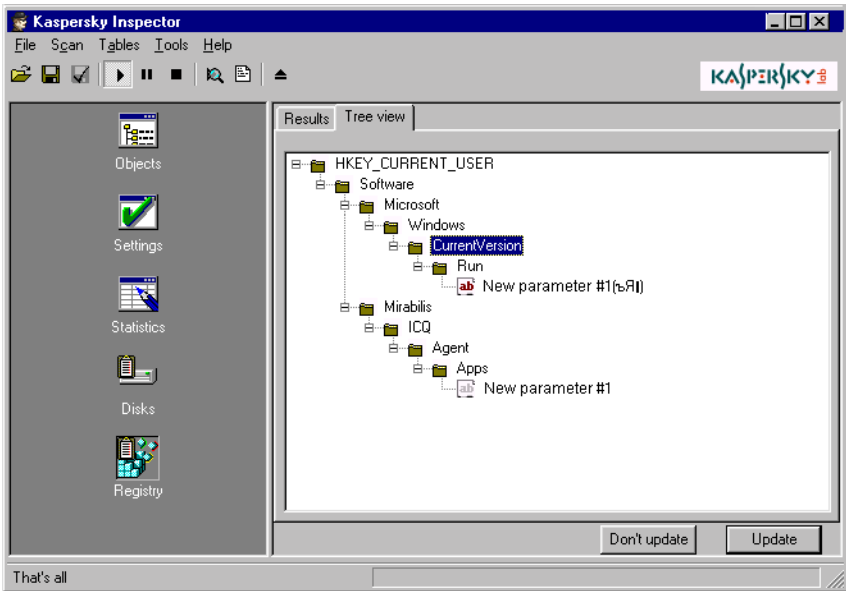


Figure 124. The registry modifications tree

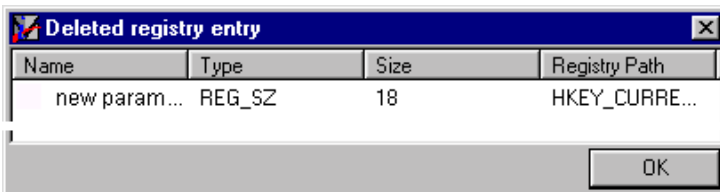


Figure 125. A list of registry keys that have been deleted

14.6.7. The Disks and Registry work areas: allowing/prohibiting changes to Kaspersky[®] Inspector tables

While checking your computer Kaspersky[®] Inspector detects modifications in files, directories, and the system registry. If you want to apply these modifications to the Kaspersky[®] Inspector tables, use the **Update** buttons in the corresponding statistics windows (see Figure 118 and 123). After this, all the modifications detected during the check will be saved to the tables and, when launched the next time, your Kaspersky[®] Inspector will compare check results against the updated data.

If for some reason you want to keep the Kaspersky[®] Inspector tables unchanged, use the **Don't update** button in the corresponding statistics windows. In this case, when started next time your Kaspersky[®] Inspector will detect those modifications again.

APPENDIX A.

ADVANCED CHECKING TOOLS

A.1. The Heuristic Checking Tool (Code Analyzer)

Code Analyzer, a heuristic checking tool, checks file and sector codes down the various Kaspersky Anti-Virus® algorithmic legs as it searches for virus-similar instructions. If the heuristic tool detects certain instructions (such as open a file, write to it, intercept the interrupt vectors, etc.), the file is *suspicious* and the program generates the appropriate message:

Suspicion: <TYPE>,

where <TYPE> is replaced by one of the following strings:

- **Com** – the file seems to be infected by a virus that infects .COM files;
- **Exe** – the file seems to be infected by a virus that infects .EXE files;
- **ComExe** – the file seems to be infected by a virus that infects both .COM and .EXE files;
- **ComTSR, ExeTSR, SysTSR, ComExeTSR** – the file seems to be infected by a virus that infects .COM, .EXE and .SYS files;
- **Boot** – the file/sector seems to be infected by a boot virus or a boot virus installer;
- **Trojan** – the file looks like a Trojan;
- **Trivial** – the file seems to be infected by an unknown virus replacing executable files in a current directory by its own codes (usually the virus size doesn't exceed 300 bytes);
- **HLL** – the file seems to be infected by an unknown virus infecting executable files. The virus is written in a high-level language (C, Pascal);
- **Win32** – the file seems to be infected by an unknown Windows virus;
- **Formula** – an Excel file contains suspicious instructions.

- **Macro.Word97.Fs** – the file seems to be infected with a Macro.Word97.Fs family virus.
- **RemoteTemplate** – the document contains a link to a template which is automatically loaded when the file is opened;
- **HTML.SecurityBreach.2** – the HTML file or the HTML message is linked to a suspicious object;
- **IRC-Worm.generic** – the file seems to be infected by an unknown worm transmitting itself via the IRC channels;
- **BAT** – the file seems to be infected with an unknown virus infecting BAT files;
- **VBS.I-Worm** – the file seems to be infected by an unknown worm transmitting itself via e-mail.

Of course, as with any other heuristic algorithm you may occasionally receive false alarms. However, Code Analyzer has been tested many times and has checked a large number of files, and so far has not been deceived. If you do encounter a false alarm while checking files using Code Analyzer, please let us know and send us copies of the virus-free files that were identified as infected so that we may study them at Kaspersky Labs.

When scanning code the heuristic detecting tool examines the structure of a program down to several sub-levels. This device detects 92 % of the viruses (including many encrypted ones) in the Kaspersky Lab's database, and we believe that newfound viruses that aren't yet in the database will be detected with the same degree of probability.

A.2. The Redundant Scanning Tool

In most cases a virus registers itself in the entry point of a file with a reference to its body, which is usually appended to the file contents. To delete such viruses you only need to run an ordinary scanning operation that will remove the virus code located in the file entry point and the virus body pointed to by the initial address.

However, sometimes the virus divides its body into several parts and places them into clean areas of the file. In this case an ordinary scanning operation will neutralize the virus (i.e. the virus code in the entry point and main part of the virus body will be deleted) but some of its parts will remain in the file.

In this case you need to run a *redundant scan operation* that will check not only the file entry points but also the entire contents of your file.

The redundant scanning tool is recommended if no virus was detected in a normal scan but the system is still behaving strangely (for example, there are

frequent instances when the computer restarts by itself, unnaturally slow performance from applications, etc.) Otherwise, we do not recommend enabling the redundant scanning tool as it noticeably slows down the scanning rate and increases the probability of false alarms.

APPENDIX B. GLOSSARY

alert (notification)

An e-mail message that is automatically transmitted by a Kaspersky Anti-Virus® package component to a predefined address at the occurrence of a predefined event (when a virus is detected, a component fails to perform its functions, etc.)

anti-virus

Computer software that is designed to protect a computer from penetration/replication of computer viruses.

anti-virus databases

A set of files that contains descriptions of viruses and methods to remove them. Kaspersky Labs updates these files on a daily basis by adding details of new viruses to them; the updates are placed on the Kaspersky Labs web sites and can be later retrieved by the updating utility.

anti-virus scanner

A computer program that allows scanning for suspicious objects on a computer (see also ***Kaspersky Anti-Virus® Scanner***).

boot virus

A virus that occupies a boot sector of the infected diskette or a boot sector or the master boot record of the infected hard drive. This virus forces the system (when it is started) to read into the memory and to transfer control to the virus code instead of the original loader. I.e. this virus infects this system every time it is loaded using an infected source.

Code Analyzer

See ***heuristic checking tool***

disk table

A file created by Kaspersky® Inspector that contains details of the computer's logical disks (CRC of files, a directory structure).

false alarm

A false claim that a file is infected by a virus is known as a "false alarm."

heuristic checking tool (Code Analyzer)

A tool that verifies an instruction sequence in the examined object, collects certain statistics and decides whether the object is "probably infected" or "not infected". This tool makes it possible to search for unknown viruses.

integrity checker

A computer program that checks disks for modifications (see also **Kaspersky® Inspector**).

interface subprogram of a Kaspersky Anti-Virus® package component

A sub-program that supports communication between a user and the service sub-program.

Kaspersky Anti-Virus® Control Centre

A computer program that performs the functions of a control shell. This program allows creation and scheduling of task performance, and also control of performance results.

Kaspersky Anti-Virus® Mail Checker

A computer program that provides protection from viruses in the incoming and outgoing messages that are processed using a Microsoft Exchange Client compatible software.

Kaspersky Anti-Virus® Monitor (monitor)

A resident anti-virus monitor. When it detects a virus in an object the monitor disables reference to the object and notifies the user.

Kaspersky Anti-Virus® Rescue Disk

A computer program that allows the user to create rescue disks. These disks allow a user to recover a system after it has been corrupted by a virus.

Kaspersky Anti-Virus® Scanner (scanner)

A computer program that detects and deletes viruses on a computer on user demand.

Kaspersky Anti-Virus® Script Checker

A computer program that protects your computer from script-viruses and worms that are executed directly in the computer memory.

Kaspersky Anti-Virus® Updater

A computer program that allows automatic updating of anti-virus bases and package components.

Kaspersky® Inspector (inspector)

An integrity checker. Kaspersky® Inspector checks disks for modifications in files and directories and, if it detects suspicious modifications, notifies the user. The program can be used as a supplementary anti-virus program or to monitor changes on disks. The program reduces the time you need to check your computer using Kaspersky AV Scanner by supplying the scanner with

information about the files that have been changed or created. The scanner will then check for viruses in those files only.

Kaspersky® Office Guard

A computer program that protects Microsoft Office 2000 documents from both known and unknown macro viruses.

Kaspersky® Report Viewer

A computer program that allows you to view and manage reports generated by Kaspersky Anti-Virus® package components.

macro virus

A virus that has been created using the macro language provided with some software applications (word processors, spreadsheets, etc.) This type of virus replicates by copying itself to documents created with the application whose macro language has been used.

notification

See **alert**

polymorphic virus

A virus which has been written in such a way as to make it harder for an anti-virus program to recognize it. These viruses contain no constant code blocks at all.

profile

See **settings file**

quarantine

A directory containing infected and suspicious files in coded form. These files can later be restored using Kaspersky Anti-Virus® Control Centre, if they were deleted by mistake, or in order to archive and e-mail to Kaspersky Labs where they can be studied.

registry table

A file created by Kaspersky® Inspector that contains details of the critical registry keys (bootstrap loading, key files).

rescue disks

A set of diskettes that allows you to boot the system and check it for viruses. They can be used to restore your system in case it has been completely disabled as the result of a virus attack. These diskettes contain an operating system, an anti-virus program and the anti-virus bases. They can be created using Kaspersky Anti-Virus® Rescue Disk.

resident anti-virus monitor

A memory-resident computer program that checks for viruses in the used objects (documents to be opened, files to be saved, etc.).

scanning

A process that is performed by an anti-virus scanner when it checks for viruses in a predefined location or by an inspector when it checks suspicious modifications in the system. A user may set the computer memory, disks, folders, etc. as locations to be checked for viruses.

script virus

A virus which has been written in a script language. This virus usually embeds itself in a web page and is started when this page is viewed. A message in HTML format may also carry such viruses.

settings file (profile)

A file that contains the main settings of a program. These settings can be exported (saved) to a file and imported (loaded) from this file. When started, the program adopts settings from the default profile.

settings tree

A graphic interface item that presents data in the form of a tree with conventional controls as joints (buttons, drop-down lists, check boxes, etc.).

service sub-program of a Kaspersky Anti-Virus® package component

A sub-program that constantly resides in the computer memory. This sub-program performs user-defined actions (scanning, monitoring, etc.).

stealth virus

A virus that utilizes various methods to conceal its presence in a system. Nowadays, any class of virus can utilize stealth features.

suspicious macro instruction

A macro instruction that can be used to enable a virus to replicate itself or perform some harmful activity may be treated as suspicious. Kaspersky® Office Guard allows a user to define actions to be taken in response to this kind of macro instruction.

suspicious object

An object whose actions or contents appear similar to a virus. A memory location, file, macro and other objects can be claimed to be suspicious.

system crack (hack)

Unauthorized access that is gained to the system's data or resources. Systems are frequently cracked using a malware.

Trojan

Named after the Trojan Horse of mythology, this is a class of malware that looks as if it is a harmless program but which in fact performs destructive or undesired actions, such as remote management, data stealing, monitoring, etc.

updating server

A server that stores the most up-to-date anti-virus bases or program modules.

virus

A computer program (that is, executable code and/or a collection of instructions) that can replicate itself (though the copy may not necessarily exactly match the original) and can penetrate files and other resources of computer systems and networks and make them perform tasks the virus dictates without the user's permission. Copies of the program are also capable of replicating themselves (for more details see Virus Encyclopedia <http://www.viruslist.com/eng/viruslist.asp>).

virus attack

A set of actions that are performed in order to infect a computer.

Windows virus

A virus that while infecting a file utilizes features of the Microsoft Windows operating system.

worm

A class of malware that spreads using a computer network such as the Internet. Worms penetrate computers from the computer network by finding computer network addresses and dispatching their copies to these addresses. Sometimes these viruses create work files on system disks, but they can avoid using system resources (with the exception of RAM).

APPENDIX C. KASPERSKY LABS LTD.

Kaspersky Labs is a privately-owned, international, anti-virus software-development group of companies headquartered in Moscow (Russia), and representative offices in the United Kingdom, United States of America, China, France and Poland. Founded in 1997, Kaspersky Labs concentrates its efforts on the development, marketing and distribution of leading-edge information security technologies and computer software.

Kaspersky Labs is one the world leaders in data-security and anti-virus technologies. The Company was the first to develop many features that are now an essential part of all modern anti-virus protection: an external anti-virus database with embedded specialized modules, a search capability within archived and compressed files, integrated anti-virus protection for Linux, etc. In addition to anti-virus software, Kaspersky Labs is committed to the development of general data-security software. Our current product line includes Kaspersky™ Inspector and Kaspersky® WEB Inspector, whose unique capabilities allow users full control over any unauthorized alteration to the file system and content of a Web server.

Upcoming add-on features include Kaspersky® Anti-Hacker for general workplace defense against any hacker attacks, and Kaspersky® Anti-Spam for enterprise-wide prevention of incoming "spam" messages and internal e-mail misusing. Kaspersky Labs' flagship product, Kaspersky® Anti-Virus (formerly known as AVP), has been in constant development since 1989, and has been rated consistently by numerous computer magazines and virus research centers as the best anti-virus product on the market.

Kaspersky® Anti-Virus covers all reliable methods of anti-virus protection: anti-virus scanners, resident "on-the-fly" virus interceptors, integrity checkers and behavior blockers. Kaspersky® Anti-Virus supports all of the most popular operating systems and applications. It provides strong anti-virus defense for e-mail gateways (MS Exchange Server, Lotus Notes/ Domino, Sendmail, Qmail, Postfix, and Exim), firewalls and WEB servers. All Kaspersky Labs products rely on Kaspersky's own database of over 60,000 known viruses and all other types of malicious code. The product is also powered by a unique heuristic technology combating even future threats: the built-in heuristic code analyzer, which is able to detect up to 92% of unknown viruses and the world's only behavior blocker for MS Office 2000 providing 100% guaranteed protection against any macro-viruses.

APPENDIX D. KASPERSKY LABS LTD.

Founded in 1997, Kaspersky Labs has become a recognized leader in information security technologies. It produces a wide range of data security software and delivers high-performance, comprehensive solutions to protect computers and networks against all types of malicious programs, unsolicited and unwanted e-mail messages, and hacker attacks.

Kaspersky Labs is an international company. Headquartered in Russian Federation, the company has subsidiary offices in United Kingdom, France, Germany, Japan, USA (CA), the Benelux countries, China and Poland. A new company department, the European Anti-Virus Research Centre, has recently been established in France. Kaspersky Labs' partner network incorporates more than 500 companies worldwide.

Today, Kaspersky Labs hires more than 300 specialists, each of whom is proficient in anti-virus technologies, with 9 of them possessing M.B.A. degrees, 15 possessing Ph.D.'s, and two experts holding membership in the Computer Anti-Virus Researcher's Organization (CARO).

Kaspersky Labs offers best-of-breed security solutions, based on its unique experience and knowledge gained in a more than 14-year history of fighting computer viruses. A thorough analysis of computer virus activities enables the company to deliver comprehensive protection from current and even future threats. Resistance to future attacks is the basic policy implemented into all of Kaspersky Labs' products. At all times, the company's products remain at least one step ahead of many other vendors in delivering extensive anti-virus coverage for home users and corporate customers alike.

Years of hard work made the company one of the top security software manufacturers. Kaspersky Labs was one of the first businesses of its kind to develop the highest standards for anti-virus defense. The company's flagship product, Kaspersky Anti-Virus[®], provides full-scale protection to all tiers of a network, including workstations, file servers, mail gateways, firewalls, and handhelds. Its convenient and easy-to-use management tools ensure advanced automation for rapid virus protection across the enterprise. Many well-known manufacturers use the Kaspersky Anti-Virus[®] kernel, including Nokia ICG (USA), F-Secure (Finland), Aladdin (Israel), Sybari (USA), G Data (Germany), Deerfield (USA), Alt-N (USA), Microworld (India), BorderWare (Canada), etc.

Kaspersky Labs' customers take advantage of a wide range of additional services that ensure not only stable operation of the company products but also compliance with any specific business requirements. Kaspersky Labs' anti-virus database is updated in real-time every 3 hours. The company provides its

customer with 24-hour technical support service, which is available in several languages to accommodate its international clientele.

D.1. Other Kaspersky Labs Products

Kaspersky Anti-Virus® Lite

This is an optimal choice for even an unskilled user who wants to protect his/her home computer against viruses. The program operates on computers running Windows 98/Me, Windows 2000/NT Workstation, and Windows XP.

Kaspersky Anti-Virus® Lite includes:

- **anti-virus scanner** to scan all local and network drives on demand;
- **anti-virus monitor** to monitor all used files in real-time mode;
- a **module** to scan MS Outlook Express's mail databases for viruses on demand.

Kaspersky Anti-Virus® Personal

Kaspersky Anti-Virus® Personal protects home computers running Windows 98/ME, Windows 2000/NT, and Windows XP from all types of known viruses, including Trojan horses, Internet worms, script viruses, malicious ActiveX and Java applets, etc. The program constantly controls all possible sources of virus penetration, such as e-mail, Internet, floppy disks, CDs, etc. Kaspersky Anti-Virus® Personal is supplied with an easy-to-use application for automatic retrieval of daily updates from the Internet. A second-generation heuristic analyzer efficiently detects even unknown viruses. Kaspersky Anti-Virus® Personal includes many interface enhancements, making it easier than ever to use the program.

Kaspersky Anti-Virus® Personal features:

- **on-demand scans** of local disks to detect all possible kinds of viruses;
- **real-time protection** of all files from viruses;
- a **mail filter** that scans all incoming and outgoing messages in background mode.

Kaspersky Anti-Virus® Personal supports more than 700 formats of archives and compressed files and automatically scans their contents. The program removes malicious code from ZIP archives.

Kaspersky Anti-Virus® Personal Pro

This package has been designed to deliver comprehensive anti-virus protection to home computers running Windows 98/ME, Windows 2000/NT, and Windows

XP as well as MS Office 2000 applications. Kaspersky Anti-Virus® Personal Pro includes an easy-to-use application for automatic retrieval of daily updates to the anti-virus database and the program modules. A second-generation heuristic analyzer efficiently detects even unknown viruses. Kaspersky Anti-Virus® Personal includes many interface enhancements, making it easier than ever to use the program.

In addition to real-time protection, on-demand scans, and mail filtering, Kaspersky Anti-Virus® Personal Pro includes a **behavior blocker** to guarantee 100% protection against macro viruses.

Kaspersky® Anti-Hacker

Kaspersky® Anti-Hacker is a personal firewall that is designed to safeguard a computer running any Windows operating system. It protects your computer against unauthorized access and external hacker attacks from either the Internet or the local network.

Kaspersky® Anti-Hacker monitors the TCP/IP network activity of all applications running on your machine. When it detects a suspicious action, the program blocks the suspicious application from accessing the network. This helps deliver enhanced privacy and 100% security of confidential data stored on your computer.

The product's SmartStealth™ technology prevents hackers from detecting your computer from the outside. In this stealthy mode, the program works seamlessly to keep your computer protected while you are on the Web: the program provides conventional transparency and accessibility of information.

- Kaspersky® Anti-Hacker also blocks most common network hacker attacks and monitors for attempts to scan computer ports.
- Configuration of the program is simply a matter of choosing one of five security levels. By default, the program starts in self-learning mode, which will automatically configure your security system, depending on your responses to various events. This makes your personal guard adjustable to your specific preferences and your particular needs.

Kaspersky® Security для PDA

Kaspersky® Security for PDA provides reliable anti-virus protection of data stored on PDAs running Palm OS or Windows CE. It also offers viral protection from any corrupted files transferred from a PC or an extension card, from ROM files, and from databases. This software package includes an optimal combination of the following anti-virus tools:

- **anti-virus scanner** to scan the data stored on both the PDA and an extension card on demand

- **anti-virus monitor** to intercept viruses in files that are either copied from other handhelds or are transferred using the HotSync™ technology.

Kaspersky® Security for PDA protects your handheld (PDA) from unauthorized intrusion by encrypting both access to the device and data stored on memory cards.

Kaspersky Anti-Virus® Business Optimal

This package provides a configurable security solution for small- and medium-sized corporate networks.

Kaspersky Anti-Virus® Business Optimal includes full-scale anti-virus protection⁵ for:

- *Workstations* running Windows 98/ME, Windows NT/2000/XP Workstation, and Linux;
- *File and application servers* running Windows NT 4.0 Server, Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD and OpenBSD, and Linux;
- *E-mail systems*, namely Microsoft Exchange 5.5/2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail, and Qmail.

The Kaspersky Anti-Virus® Business Optimal distribution kit includes Kaspersky® Administration Kit, a *unique tool for automated deployment and administration*.

You are free to choose from any of these anti-virus programs, according to the operating systems and applications you use.

Kaspersky® Corporate Suite

This package provides corporate networks of any size and complexity with comprehensive, scalable anti-virus protection. The package components have been developed to protect every tier of a corporate network, even in mixed computer environments. Kaspersky® Corporate Suite supports the majority of operating systems and applications installed across an enterprise. All package components are managed from one console and have a unified user interface. Kaspersky® Corporate Suite delivers a high-performance and reliable protection system that is fully compatible with the specific needs of your network configuration.

Kaspersky® Corporate Suite provides comprehensive anti-virus protection for:

- *Workstations* running Windows 98/ME, Windows NT/2000/XP, and Linux;

⁵ Depending on the type of distribution kit.

- *File and application servers* running Windows NT 4.0 Server, Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD, OpenBSD and Linux;
- *E-mail systems*, including Microsoft Exchange Server 5.5/2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim and Qmail;
- *Data streams transmitted via firewalls*;
- *Handheld computers (PDAs)*.

The Kaspersky® Corporate Suite distribution kit includes Kaspersky® Administration Kit, a *unique tool for automated deployment and administration*.

You are free to choose from any of these anti-virus programs, according to the operating systems and applications you use.

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam is a cutting-edge software suite that is designed to help organizations with small- and medium-sized networks wage war against the onslaught of undesired e-mail (spam). The product combines the revolutionary technology of linguistic analysis with all modern methods of e-mail filtration (including RBL lists and formal letter features). Its unique combination of services allows users to identify and wipe out up to 95% of unwanted traffic.

Installed at the entrance to a network, where it monitors incoming e-mail traffic streams for objects identified as spam, Kaspersky® Anti-Spam acts as an unsolicited e-mail barrier. The product is compatible with any mail system and can be installed on either an existing mail server or a dedicated one.

Kaspersky® Anti-Spam's high performance is ensured by daily updating of the content filtration database, with samples provided by the Company's linguistic laboratory specialists.

D.2. Contact Us

If you have any questions, comments, or suggestions, please refer them to one of our distributors or directly to Kaspersky Labs. We will be glad to advise you on any matters related to our product by phone or via e-mail. Rest assured that all of your recommendations and suggestions will be thoroughly reviewed and considered.

Technical support	Please find the technical support information at http://www.kaspersky.com/supportinter.html
-------------------	--

General information	WWW: http://www.kaspersky.com http://www.viruslist.com E-mail: sales@kaspersky.com
------------------------	---

APPENDIX E. LICENSE AGREEMENT

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT (“AGREEMENT”), FOR THE LICENCE OF SPECIFIED SOFTWARE (“SOFTWARE”) PRODUCED BY KASPERSKY LAB. (“KASPERSKY LAB”).

IF YOU HAVE PURCHASED THIS SOFTWARE VIA INTERNET BY CLICKING THE ACCEPT BUTTON, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) CONSENT TO BE BOUND BY AND BECOME A PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT AND DO NOT INSTALL THE SOFTWARE.

IF YOU HAVE PURCHASED THIS SOFTWARE ON A PHYSICAL MEDIUM, HAVING BROKEN THE CD’S SLEEVE, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT DO NOT BREAK THE CD’S SLEEVE, DOWNLOAD, INSTALL OR USE THIS SOFTWARE. YOU MAY RETURN THIS SOFTWARE FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM AN AUTHORISED KASPERSKY LABS DISTRIBUTOR OR RESELLER. THE RIGHT TO RETURN AND REFUND EXTENDS ONLY TO THE ORIGINAL PURCHASER.

All references to “Software” herein shall be deemed to include the software activation key (“Key Identification File”) with which you will be provided by Kaspersky Labs as part of the Software.

1. Licence Grant. Subject to the payment of the applicable licence fees, and subject to the terms and conditions of this Agreement, Kaspersky Labs hereby grants to you a non-exclusive, non-transferable right to use one copy of the specified version of the Software and the accompanying documentation (the “Documentation”) for the term of this Agreement solely for your own internal business purposes. You may install one copy of the Software on one computer, workstation, personal digital assistant, or other electronic device for which the Software was designed (each, a “Client Device”). If the Software is licensed as a suite or bundle with more than one specified Software produce, this licence applies to all such specified Software products, subject to any restrictions or usage terms specified on the applicable price list or product packaging that apply to any of such Software products individually.

1.1 Use. The Software is licensed as a single product; it may not be used on more than one Client Device or by more than one user at a time, except as set forth in this Section.

1.1.1 The Software is “in use” on a Client Device when it is loaded into the temporary memory (i.e., random-access memory or RAM) or installed into the permanent memory (e.g., hard disk, CD-ROM, or other storage device) of that Client Device. This licence authorizes you to make only as many back-up copies of the Software as are necessary for its lawful use and solely for back-up purposes, provided that all such copies contain all of the Software’s proprietary notices. You will maintain records of the number and location of all copies of the Software and Documentation and will take all reasonable precautions to protect the Software from unauthorised copying or use.

1.1.2 If you sell the Client Device on which the Software is installed, you will ensure that all copies of the Software have been previously deleted.

1.1.3 You shall not decompile, reverse engineer, disassemble or otherwise reduce any part of this Software to human readable form nor permit any third party to do so. The interface information necessary to achieve interoperability of the Software with independently created computer programs will be provided by Kaspersky Labs on request on payment of its reasonable costs and expenses for procuring and supplying such information. In the event Kaspersky Labs notifies you that it does not intend to make such information available for any reason, including (without limitation) costs, you shall be permitted to take such steps to achieve interoperability provided that you may only reverse engineer or decompile to the extent permitted by law.

1.1.4 You shall not, nor permit any third party to copy (other than as expressly permitted herein), make error corrections to or otherwise modify, adapt or translate the Software nor create derivative works of the Software.

1.1.5 You shall not rent, lease or lend the Software to any other person, nor transfer or sub-licence your licence rights to any other person.

1.2 Server-Mode Use. You may use the Software on a Client Device or on or as a server (“Server”) within a multi-user or networked environment (“Server-Mode”) only if such use is permitted in the applicable price list or product packaging for the Software. A separate licence is required for each Client Device or “seat” that may connect to the Server at any time, regardless of whether such licenced Client Devices or seats are concurrently connected to or actually accessing or using the Software. Use of software or hardware that reduces the number of Client Devices or seats directly accessing or utilizing the Software (e.g., “multiplexing” or “pooling” software or hardware) does not reduce the number of licences required (i.e., the required number of licences would equal the number of distinct inputs to the multiplexing or pooling software or hardware “front end”). If the number of Client Devices or seats that can connect to the Software can exceed the number of licences you have obtained, then you must have a reasonable mechanism in place to ensure that your use of the

Software does not exceed the use limits specified for the licence you have obtained. This licence authorises you to make or download such copies of the Documentation for each Client Device or seat that is licensed as are necessary for its lawful use, provided that each such copy contains all of the Documentation proprietary notices.

1.3 Volume Licences. If the Software is licensed with volume licence terms specified in the applicable product invoicing or packaging for the Software, you may make, use or install as many additional copies of the Software on the number of Client Devices as the volume licence terms specify. You must have reasonable mechanisms in place to ensure that the number of Client Devices on which the Software has been installed does not exceed the number of licences you have obtained. This licence authorizes you to make or download one copy of the Documentation for each additional copy authorized by the volume licence, provided that each such copy contains all of the Document's proprietary notices.

2. Term. This Agreement is effective for the period specified in the Key File (the unique file which is required to fully enable the Software, please see Help/ about Software or Software about, for Unix/Linux version of the Software see the notification about expiration date of the Key File) unless and until earlier terminated as set forth herein. This Agreement will terminate automatically if you fail to comply with any of the conditions, limitations or other requirements described herein. Upon any termination or expiration of this Agreement, you must immediately destroy all copies of the Software and the Documentation. You may terminate this Agreement at any point by destroying all copies of the Software and the Documentation.

3. Support.

(i) Kaspersky Labs will provide you with the support services ("Support Services") as defined below for a period of one year on:

(a) payment of its then current support charge; and

(b) successful completion of the Support Services Subscription Form as provided to you with this Agreement or as available on the Kaspersky Labs website, which will require you to produce the Key Identification File which will have been provided to you by Kaspersky Labs with this Agreement. It shall be in the absolute discretion of Kaspersky Labs whether or not you have satisfied this condition for the provision of Support Services.

(ii) Support Services will terminate unless renewed annually by payment of the then current annual support charge and by successful completion of the Support Services Subscription Form again.

(iii) By completion of the Support Services Subscription Form you consent to the terms of the Kaspersky Labs Privacy Policy which is attached to this Agreement, and you explicitly consent to the transfer of data to other countries outside your own as set out in the Privacy Policy.

- (iv) "Support Services" means
- (a) Daily updates of antivirus databases;
 - (b) Free software updates, including version upgrades;
 - (c) Extended technical support via E-mail and hot phone-line provided by Vendor and/or Reseller;
 - (d) Virus detection and curing updates in 24-hours period.

4. **Ownership Rights.** The Software is protected by copyright laws. Kaspersky Labs and its suppliers own and retain all right, title and interest in and to the Software, including all copyrights, patents, trademarks and other intellectual property rights therein. Your possession, installation, or use of the Software does not transfer to you any title to the intellectual property in the Software, and you will not acquire any rights to the Software except as expressly set forth in this Agreement.

5. **Confidentiality.** You agree that the Software and the Documentation, including the specific design and structure of individual programs and the Key Identification File constitute confidential proprietary information of Kaspersky Lab. You shall not disclose, provide or otherwise make available such confidential information in any form to any third party without the prior written consent of Kaspersky Lab. You shall implement reasonable security measures to protect such confidential information, but without limitation to the foregoing shall use best endeavours to maintain the security of the Key Identification File.

6. Limited Warranty

(i) Kaspersky Labs warrants that for [90] days from first download or installation the Software will perform substantially in accordance with the functionality described in the Documentation when operated properly and in the manner specified in the Documentation.

(ii) You accept all responsibility for the selection of this Software to meet your requirements. Kaspersky Labs does not warrant that the Software and/or the Documentation will be suitable for such requirements nor that any use will be uninterrupted and error free;

(iii) Kaspersky Labs does not warrant that this Software identifies all known viruses, nor that the Software will not occasionally erroneously report a virus in a title not infected by that virus;

(iv) Your sole remedy and the entire liability of Kaspersky Labs for breach of the warranty at paragraph (i) will be at Kaspersky Labs option, to repair, replace or refund of the Software if reported to Kaspersky Labs or its designee during the warranty period. You shall provide all information as may be reasonably necessary to assist the Supplier in resolving the defective item;

(v) The warranty in (i) shall not apply if you (a) make or cause to be made any modifications to this Software without the consent of Kaspersky Lab, (b) use the Software in a manner for which it was not intended or (c) use the Software other than as permitted under this Agreement;

(vi) The warranties and conditions stated in this Agreement are in lieu of all other conditions, warranties or other terms concerning the supply or purported supply of, failure to supply or delay in supplying the Software or the Documentation which might but for this paragraph (v) have effect between the Kaspersky Labs and your or would otherwise be implied into or incorporated into this Agreement or any collateral contract, whether by statute, common law or otherwise, all of which are hereby excluded (including, without limitation, the implied conditions, warranties or other terms as to satisfactory quality, fitness for purpose or as to the use of reasonable skill and care).

7. Limitation of Liability

(i) Nothing in this Agreement shall exclude or limit Kaspersky Lab' liability for (i) the tort of deceit, (ii) death or personal injury caused by its breach of a common law duty of care or any negligent breach of a term of this Agreement, (iii) any breach of the obligations implied by s.12 Sale of Goods Act 1979 or s.2 Supply of Goods and Services Act 1982 or (iv) any liability which cannot be excluded by law.

(ii) Subject to paragraph (i), the Supplier shall have no liability (whether in contract, tort, restitution or otherwise) for any of the following losses or damage (whether such losses or damage were foreseen, foreseeable, known or otherwise):

- (a) Loss of revenue;
- (b) Loss of actual or anticipated profits (including for loss of profits on contracts);
- (c) Loss of the use of money;
- (d) Loss of anticipated savings;
- (e) Loss of business;
- (f) Loss of opportunity;
- (g) Loss of goodwill;
- (h) Loss of reputation;
- (i) Loss of, damage to or corruption of data; or
- (j) Any indirect or consequential loss or damage howsoever caused (including, for the avoidance of doubt, where such loss or damage is of the type specified in paragraph (ii), (a) to (i), (i).

(iii) Subject to paragraph (i), the Kaspersky Labs liability (whether in contract, tort, restitution or otherwise) arising out of or in connection with the supply of the Software shall in no circumstances exceed a sum equal to the amount equally paid by you for the Software.

8. The construction and interpretation of this Agreement shall be governed in accordance with the laws of England and Wales. The parties hereby submit to the jurisdiction of the courts of England and Wales save that Kaspersky Labs as claimant shall be entitled to initiate proceedings in any court of competent jurisdiction.

9. (i) This Agreement contains the entire understanding of the parties with respect to the subject matter hereof and supersedes all and any prior understandings, undertakings and promises between you and Kaspersky Lab, whether oral or in writing, which have been given or may be implied from anything written or said in negotiations between us or our representatives prior to this Agreement and all prior agreements between the parties relating to the matters aforesaid shall cease to have effect as from the Effective Date. Save as provided in paragraphs (ii) - (iii), you shall not have any remedy in respect of an untrue statement made to you upon which you relied in entering into this Agreement ("Misrepresentation") and Kaspersky Labs shall not have any liability to the other than pursuant to the express terms of this Agreement.

(ii) Nothing in this Agreement shall exclude or limit Kaspersky Lab' liability for any Misrepresentation made by it knowing that it was untrue.

(iii) The liability of Kaspersky Labs for Misrepresentation as to a fundamental matter, including a matter fundamental to the maker's ability to perform its obligations under this Agreement, shall be subject to the limitation of liability set out in paragraph 7(iii).