

Kaspersky Anti-Virus 2012

**KASPERSKY** **lab**

User Guide

APPLICATION VERSION: 12.0

Dear User!

Thank you for choosing our product. We hope that you will find this documentation useful and that it will provide answers to most of your questions that may arise.

Warning! This document is the property of Kaspersky Lab ZAO (herein also referred to as Kaspersky Lab): all rights to this document are reserved by the copyright laws of the Russian Federation and by international treaties. Illegal reproduction and distribution of this document or parts hereof will result in civil, administrative or criminal liability in accordance with applicable law.

Any type of reproduction or distribution of any materials, including translations, is allowed only with the written permission of Kaspersky Lab.

This document and related graphic images can be used exclusively for informational, non-commercial or personal use.

This document may be amended without prior notification. The latest version of this document can be found on the Kaspersky Lab website at <http://www.kaspersky.com/docs>.

Kaspersky Lab assumes no liability for the content, quality, relevance, or accuracy of any materials used in this document the rights to which are held by third parties, or for any potential damages associated with the use of such documents.

This document uses registered trademarks and service marks which are the property of their respective owners.

Document revision date: 4/19/2011

© 1997-2011 Kaspersky Lab ZAO. All Rights Reserved.

<http://www.kaspersky.com>

<http://support.kaspersky.com>

# CONTENT

ABOUT THIS GUIDE .....	8
In this guide .....	8
Document conventions .....	10
SOURCES OF INFORMATION ABOUT THE APPLICATION .....	11
Sources of information for independent research .....	11
Discussing Kaspersky Lab applications on the Forum .....	12
Contacting the Sales Department.....	12
Contacting the Documentation Development Team by email .....	12
KASPERSKY ANTI-VIRUS .....	13
What's new .....	13
Distribution kit.....	13
Service for registered users.....	14
Hardware and software requirements.....	14
INSTALLING AND REMOVING THE APPLICATION .....	16
Standard installation procedure .....	16
Step 1. Searching for a newer version of the application .....	17
Step 2. Making sure the system meets the installation requirements .....	17
Step 3. Selecting installation type .....	18
Step 4. Reviewing the license agreement .....	18
Step 5. Kaspersky Security Network Data Collection Statement .....	18
Step 6. Searching for incompatible applications .....	18
Step 7. Selecting the destination folder.....	19
Step 8. Preparing for installation .....	19
Step 9. Installing .....	20
Step 10. Finishing the installation .....	20
Step 11. Activating the application .....	20
Step 12. Registering a user.....	20
Step 13. Completing the activation .....	21
Updating the previous version of Kaspersky Anti-Virus .....	21
Step 1. Searching for a newer version of the application .....	22
Step 2. Making sure the system meets the installation requirements .....	22
Step 3. Selecting installation type .....	22
Step 4. Reviewing the license agreement .....	22
Step 5. Kaspersky Security Network Data Collection Statement .....	23
Step 6. Searching for incompatible applications .....	23
Step 7. Selecting the destination folder.....	23
Step 8. Preparing for installation .....	24
Step 9. Installing .....	24
Step 10. Wizard completion .....	24
Non-standard installation scenarios.....	25
Getting started.....	25
Removing the application .....	25
Step 1. Saving data for reuse.....	26
Step 2. Confirmation of application removal.....	26

Step 3. Removing the application. Completing removal.....	26
LICENSING THE APPLICATION .....	27
About the End User License Agreement .....	27
About data provision.....	27
About the license .....	27
About the activation code .....	28
APPLICATION INTERFACE .....	29
The notification area icon.....	29
The context menu.....	30
The Kaspersky Anti-Virus main window .....	31
Notification windows and pop-up messages.....	32
The application settings window .....	34
The Kaspersky Gadget.....	35
News Agent .....	36
STARTING AND STOPPING THE APPLICATION .....	37
Enabling and disabling automatic launch .....	37
Launching and closing the application manually.....	37
MANAGING THE COMPUTER PROTECTION.....	38
Diagnostics and elimination of problems in your computer protection .....	38
Enabling and disabling the protection .....	39
Pausing and resuming protection .....	40
SOLVING TYPICAL TASKS.....	42
How to activate the application .....	42
How to purchase or renew a license.....	43
What to do when application notifications appear.....	44
How to update application databases and modules .....	44
How to scan critical areas of your computer for viruses .....	45
How to scan a file, folder, disk, or another object for viruses.....	45
How to perform a full scan of your computer for viruses.....	47
How to scan your computer for vulnerabilities .....	47
How to protect your personal data against theft .....	47
Protection against phishing.....	48
Protection against data interception at the keyboard .....	48
What to do if you suspect an object is infected with a virus .....	49
What to do if you suspect your computer is infected .....	50
How to restore a file that has been deleted or disinfected by the application .....	51
How to create and use a Rescue Disk.....	52
Creating a Rescue Disk .....	52
Starting the computer from the Rescue Disk.....	54
How to view the report on the application's operation.....	55
How to restore default application settings .....	55
How to transfer settings to Kaspersky Anti-Virus installed on another computer.....	56
How to switch from Kaspersky Anti-Virus to Kaspersky Internet Security .....	57
Switching to the commercial version .....	57
Temporary switching to the trial version.....	58
How to use the Kaspersky Gadget .....	59
How to know the reputation of an application .....	60

ADVANCED APPLICATION SETTINGS .....	62
General protection settings .....	62
Restricting access to Kaspersky Anti-Virus .....	63
Selecting a protection mode .....	63
Scan .....	64
Virus scan .....	64
Vulnerability Scan .....	72
Managing scan tasks. Task Manager .....	72
Update .....	72
Selecting an update source .....	73
Creating the update startup schedule .....	75
Rolling back the last update .....	76
Running updates under a different user account .....	76
Using a proxy server .....	76
File Anti-Virus .....	77
Enabling and disabling File Anti-Virus .....	78
Automatically pausing File Anti-Virus .....	78
Creating the protection scope of File Anti-Virus .....	78
Changing and restoring the file security level .....	80
Selecting file scan mode .....	80
Using heuristic analysis when working with File Anti-Virus .....	80
Selecting file scan technology .....	81
Changing the action to take on infected files .....	81
Scan of compound files by File Anti-Virus .....	81
Optimizing file scan .....	82
Mail Anti-Virus .....	83
Enabling and disabling Mail Anti-Virus .....	84
Creating the protection scope of Mail Anti-Virus .....	84
Changing and restoring the email security level .....	85
Using heuristic analysis when working with Mail Anti-Virus .....	85
Changing the action to take on infected email messages .....	86
Filtering attachments in email messages .....	86
Scan of compound files by Mail Anti-Virus .....	86
Email scanning in Microsoft Office Outlook .....	87
Email scanning in The Bat! .....	87
Web Anti-Virus .....	88
Enabling and disabling Web Anti-Virus .....	89
Changing and restoring the web traffic security level .....	89
Changing the action to take on dangerous objects from web traffic .....	90
Checking URLs on web pages .....	90
Using heuristic analysis when working with Web Anti-Virus .....	92
Blocking dangerous scripts .....	92
Scan optimization .....	93
Creating a list of trusted addresses .....	93
IM Anti-Virus .....	94
Enabling and disabling IM Anti-Virus .....	94
Creating the protection scope of IM Anti-Virus .....	95
Checking URLs in messages from IM clients .....	95

Using heuristic analysis when working with IM Anti-Virus .....	95
Proactive Defense .....	95
Enabling and disabling Proactive Defense .....	96
Creating a group of trusted applications .....	96
Using the dangerous activity list .....	97
Changing the action to be taken on applications' dangerous activity .....	97
System Watcher .....	97
Enabling and disabling System Watcher .....	98
Using patterns of dangerous activity (BSS) .....	98
Rolling back a malicious program's actions .....	99
Network protection .....	99
Encrypted connections scan .....	100
Configuring the proxy server .....	102
Creating a list of monitored ports .....	102
Trusted zone .....	103
Creating a list of trusted applications .....	104
Creating exclusion rules .....	104
Performance and compatibility with other applications .....	105
Selecting detectable threat categories .....	105
Battery saving .....	106
Advanced Disinfection .....	106
Distributing computer resources when scanning for viruses .....	106
Running tasks in background mode .....	107
Full-screen mode. Gaming Profile .....	108
Kaspersky Anti-Virus self-defense .....	108
Enabling and disabling self-defense .....	109
Protection against external control .....	109
Quarantine and Backup .....	109
Storing files in Quarantine and Backup .....	110
Working with quarantined files .....	110
Working with objects in Backup .....	112
Scanning files in Quarantine after an update .....	112
Additional tools for better protection of your computer .....	113
Privacy Cleaner .....	113
Configuring a browser for safe work .....	115
Rolling back changes made by Wizards .....	116
Reports .....	117
Creating a report for the selected protection component .....	117
Data filtering .....	118
Events search .....	119
Saving a report to file .....	119
Storing reports .....	120
Clearing application reports .....	120
Recording non-critical events into the report .....	120
Configuring the notification of report availability .....	121
Application appearance. Managing active interface elements .....	121
Translucence of notification windows .....	121
Animation of the application icon in the notification area .....	121
Text on Microsoft Windows logon screen .....	122

Notifications .....	122
Enabling and disabling notifications .....	122
Configuring the notification method.....	123
Disabling news delivery .....	123
Kaspersky Security Network.....	124
Enabling and disabling participation in Kaspersky Security Network .....	124
Verifying connection to Kaspersky Security Network.....	124
TESTING THE APPLICATION'S OPERATION.....	126
About the test file EICAR .....	126
Testing the application's functioning using the test file EICAR .....	126
About the types of the test file EICAR .....	127
CONTACTING THE TECHNICAL SUPPORT SERVICE .....	129
How to get technical support .....	129
Using the trace file and the AVZ script .....	129
Creating a system state report.....	130
Creating a trace file.....	130
Sending data files .....	130
AVZ script execution .....	131
Technical support by phone.....	132
Obtaining technical support via My Kaspersky Account .....	132
APPENDIX .....	134
Working with the application from the command line.....	134
Activating the application .....	136
Starting the application .....	136
Stopping the application.....	136
Managing application components and tasks .....	136
Virus scan .....	138
Updating the application .....	140
Rolling back the last update .....	141
Exporting protection settings.....	141
Importing protection settings.....	141
Creating a trace file.....	142
Viewing Help .....	142
Return codes of the command line .....	143
Kaspersky Anti-Virus notifications list .....	144
Notifications in any protection mode .....	144
Notifications in interactive protection mode.....	149
GLOSSARY .....	157
KASPERSKY LAB ZAO .....	166
INFORMATION ABOUT THIRD-PARTY CODE .....	167
INDEX .....	168

# ABOUT THIS GUIDE

Greetings from Kaspersky Lab specialists!

This guide contains information about how to install, configure, and use Kaspersky Anti-Virus. We hope that information provided by this guide, will help you work with the application with the maximum of ease.

This guide is intended to:

- help you install, activate, and use Kaspersky Anti-Virus;
- ensure a quick search of information on application-related issues;
- describe additional sources of information about the application and ways of cooperating with the Technical Support Service.

For proper use of the application, you should have basic computer skills: be acquainted with the interface of the operating system that you use, handle the main techniques specific for that system, know how to work with email and the Internet.

## IN THIS SECTION:

---

In this guide.....	<a href="#">8</a>
Document conventions.....	<a href="#">10</a>

## IN THIS GUIDE

This guide comprises the following sections.

### Sources of information about the application

This section describes sources of information about the application and lists websites that you can use to discuss the application's operation.

### Kaspersky Anti-Virus

This section describes the application's features and provides brief information about the application's functions and components. You will learn what items are included in the distribution kit, and what services are available for registered users of the application. This section provides information about software and hardware requirements that a computer should meet to allow a user to install the application on it.

### Installing and removing the application

This section provides information about how to install the application on a computer and how to uninstall it.

### Licensing the application

This section provides information about general terms related to the application activation. Read this section to learn more about the purpose of the license agreement, license types, ways of activating the application, and the license renewal.

## **Application interface**

This section provides information about basic elements of the graphic interface of the application: application icon and application icon context menu, main window, settings window, and notification windows.

## **Starting and stopping the application**

This section contains information on starting and shutting down the application.

## **Managing the computer protection**

This section provides information about how to detect threats to the computer's security and how to configure the security level. Read this section to learn more about how to enable, disable, and pause the protection when using the application.

## **Solving typical tasks**

This section provides information about how to resolve the most common issues related to protection of the computer using the application.

## **Advanced application settings**

This section provides detailed information about how to configure each of the application components.

## **Testing the application's operation**

This section provides information about how to ensure that the application detects viruses and their modifications and performs the correct actions on them.

## **Contacting the Technical Support Service**

This section provides information about how to contact the Technical Support Service at Kaspersky Lab.

## **Appendix**

This section provides information that complements the document text.

## **Glossary**

This section contains a list of terms mentioned in the document and their respective definitions.

## **Kaspersky Lab ZAO**

This section provides information about Kaspersky Lab.

## **Information about third-party code**

This section provides information about the third-party code used in the application.

## **Index**

This section allows you to quickly find required information within the document.

# DOCUMENT CONVENTIONS

The text herein is accompanied by semantic elements that should be given particular attention – warnings, hints, examples.

Document conventions are used to highlight semantic elements. Document conventions and examples of their use are shown in the table below.

Table 1. Document conventions

SAMPLE TEXT	DOCUMENT CONVENTIONS DESCRIPTION
<i>Note that...</i>	Warnings are highlighted with red color and boxed. Warnings provide information about probable unwanted actions that may lead to data losses or failures in the computer's operation.
It is recommended to use...	Notes are boxed. Notes may contain useful hints, recommendations, specific values, or important particular cases in the application's operation.
<b>Example:</b> ...	Examples are set out on a yellow background under the heading "Example".
<i>Update</i> means... The <i>Databases are out of date</i> event occurs.	The following semantic elements are italicized in the text: <ul style="list-style-type: none"> <li>• new terms;</li> <li>• names of application statuses and events.</li> </ul>
Press <b>ENTER</b> . Press <b>ALT+F4</b> .	Names of keyboard keys appear in a bold typeface and are capitalized. Names of keys connected by a + (plus) sign indicate the use of a key combination. Those keys should be pressed simultaneously.
Click the <b>Enable</b> button.	Names of application interface elements, such as entry fields, menu items, and buttons, are set off in bold.
➡ <i>To configure a task schedule:</i>	Introductory phrases of instructions are italicized and accompanied by the arrow sign.
Enter <i>help</i> in the command line. The following message then appears: <i>Specify the date in dd:mm:yy format.</i>	The following types of text content are set off with a special font: <ul style="list-style-type: none"> <li>• text in the command line;</li> <li>• text of messages displayed on the screen by the application;</li> <li>• data that the user should enter.</li> </ul>
<IP address of your computer>	Variables are enclosed in angle brackets. Instead of a variable, the corresponding value should be inserted, with angle brackets omitted.

# SOURCES OF INFORMATION ABOUT THE APPLICATION

This section describes sources of information about the application and lists websites that you can use to discuss the application's operation.

You can select the most suitable information source, depending on the issue's level of importance and urgency.

## IN THIS SECTION:

---

Sources of information for independent research.....	<a href="#">11</a>
Discussing Kaspersky Lab applications on the Forum .....	<a href="#">12</a>
Contacting the Sales Department .....	<a href="#">12</a>
Contacting the Documentation Development Team by email.....	<a href="#">12</a>

## SOURCES OF INFORMATION FOR INDEPENDENT RESEARCH

You can use the following sources to find information about the application:

- the application page on the Kaspersky Lab website;
- the application page on the Technical Support Service website (Knowledge Base);
- online help;
- documentation.

If you cannot solve an issue on your own, we recommend that you contact the Technical Support Service at Kaspersky Lab (see section "Technical support by phone" on page [132](#)).

To use information sources on the Kaspersky Lab website, an Internet connection should be established.

### The application page on the Kaspersky Lab website

The Kaspersky Lab website features an individual page for each application.

On such a page ([http://www.kaspersky.com/kaspersky\\_anti-virus](http://www.kaspersky.com/kaspersky_anti-virus)), you can view general information about an application, its functions and features.

The page <http://www.kaspersky.com> features a URL to the eStore. There you can purchase or renew the application.

### The application page on the Technical Support Service website (Knowledge Base)

Knowledge Base is a section of the Technical Support Service website that provides recommendations on how to work with Kaspersky Lab applications. Knowledge Base comprises reference articles grouped by topics.

On the page of the application in the Knowledge Base (<http://support.kaspersky.com/kav2012>), you can read articles that provide useful information, recommendations, and answers to frequently asked questions on how to purchase, install, and use the application.

Articles may provide answers to questions that are out of scope of Kaspersky Anti-Virus, being related to other Kaspersky Lab applications. They also may contain news from the Technical Support Service.

### Online help

The online help of the application comprises help files.

The context help provides information about each window of the application, listing and describing the corresponding settings and a list of tasks.

The full help provides detailed information about how to manage the computer's protection using the application.

### Documentation

The application user guide provides information about how to install, activate, and configure the application, as well as application operation data. The document also describes the application interface and provides ways of solving typical user tasks while working with the application.

## DISCUSSING KASPERSKY LAB APPLICATIONS ON THE FORUM

If your question does not require an urgent answer, you can discuss it with Kaspersky Lab specialists and other users on our Forum (<http://forum.kaspersky.com>).

In this forum you can view existing topics, leave your comments, create new topics.

## CONTACTING THE SALES DEPARTMENT

If you have any questions on how to select, purchase, or renew the application, you can contact our Sales Department specialists in one of the following ways:

- By calling our HQ office in Moscow by phone (<http://www.kaspersky.com/contacts>).
- By sending a message with your question to [sales@kaspersky.com](mailto:sales@kaspersky.com).

The service is provided in Russian and English.

## CONTACTING THE DOCUMENTATION DEVELOPMENT TEAM BY EMAIL

To contact the Documentation Development Team, send an email to [docfeedback@kaspersky.com](mailto:docfeedback@kaspersky.com). Please use "Kaspersky Help Feedback: Kaspersky Anti-Virus" as the subject line in your message.

# KASPERSKY ANTI-VIRUS

This section describes the application's features and provides brief information about the application's functions and components. You will learn what items are included in the distribution kit, and what services are available for registered users of the application. This section provides information about software and hardware requirements that a computer should meet to allow a user to install the application on it.

## IN THIS SECTION:

---

What's new.....	<a href="#">13</a>
Distribution kit.....	<a href="#">13</a>
Service for registered users .....	<a href="#">14</a>
Hardware and software requirements .....	<a href="#">14</a>

## WHAT'S NEW

Kaspersky Anti-Virus provides the following new features:

- The improved interface of the main window of Kaspersky Anti-Virus ensures quick access to the application's functions.
- The logic of operations with Quarantine and Backup (see page [109](#)) has been improved: now they are represented on two separate tabs, each of them with its respective unique scope.
- The Task Manager has been added for an easy task management in Kaspersky Anti-Virus (see section "Managing scan tasks. Task Manager" on page [72](#)).
- Participation in the Kaspersky Security Network (see page [124](#)) allows us to identify the reputation of applications and websites based on data received from users from all over the world.
- When Web Anti-Virus is enabled, you can separately enable the heuristic analysis to check web pages for phishing (see section "Using heuristic analysis when working with Web Anti-Virus" on page [92](#)). When checking pages for phishing, the heuristic analysis will be applied regardless of whether it has been enabled for Web Anti-Virus.
- The appearance of Kaspersky Gadget has been redesigned (see page [35](#)).

## DISTRIBUTION KIT

You can purchase the application in one of the following ways:

- **Boxed.** Distributed via stores of our partners.
- **At the online store.** Distributed at online stores of Kaspersky Lab (for example, <http://www.kaspersky.com>, section **eStore**) or via partner companies.

If you purchase the boxed version of the application, the distribution kit contains the following items:

- sealed envelope with the setup CD that contains application files and documentation files;
- brief User Guide with an activation code;
- license agreement that stipulates the terms, on which you can use the application.

The content of the distribution kit may differ depending on the region, in which the application is distributed.

If you purchase Kaspersky Anti-Virus at an online store, you copy the application from the website of the store. Information required for the application activation, will be sent to you by email on payment.

For more details on ways of purchasing and the distribution kit, contact the Sales Department.

## **SERVICE FOR REGISTERED USERS**

On purchasing a user license for the application, you become a registered user of Kaspersky Lab applications and can benefit from the following services during the entire validity term of the license:

- updating databases and providing new versions of the application;
- consulting by phone and by email on issues related to installation, configuration, and use of the application;
- notifying you of releases of new applications by Kaspersky Lab and new viruses. To use this service, you should be subscribed to the news delivery from Kaspersky Lab on the Technical Support Service website.

No consulting services are provided on issues related to the functioning of operating systems, third-party software and technologies.

## **HARDWARE AND SOFTWARE REQUIREMENTS**

To ensure the proper functioning of Kaspersky Anti-Virus, your computer should meet the following requirements:

General requirements:

- 480 MB free disk space on the hard drive (including 380 MB on the system drive).
- CD / DVD-ROM (for installing Kaspersky Anti-Virus from a distribution CD).
- Internet access (for the application activation and for updating databases and software modules).
- Microsoft Internet Explorer 6.0 or higher.
- Microsoft Windows Installer 2.0.

Requirements for Microsoft Windows XP Home Edition (Service Pack 2 or higher), Microsoft Windows XP Professional (Service Pack 2 or higher), and Microsoft Windows XP Professional x64 Edition (Service Pack 2 or higher):

- Intel Pentium 800 MHz 32-bit (x86) / 64-bit (x64) processor or higher (or a compatible equivalent);
- 512 MB free RAM.

Requirements for Microsoft Windows Vista Home Basic, Microsoft Windows Vista Home Premium, Microsoft Windows Vista Business, Microsoft Windows Vista Enterprise, Microsoft Windows Vista Ultimate, Microsoft Windows 7 Starter, Microsoft Windows 7 Home Basic, Microsoft Windows 7 Home Premium, Microsoft Windows 7 Professional, and Microsoft Windows 7 Ultimate:

- Intel Pentium 1 GHz 32-bit (x86) / 64-bit (x64) processor or higher (or a compatible equivalent).
- 1 GB free RAM (for 32-bit operating systems); 2 GB free RAM (for 64-bit operating systems).

Requirements for netbooks:

- Intel Atom 1.6 GHz processor or a compatible equivalent.
- Intel GMA950 video card with at least 64 MB of video RAM (or a compatible equivalent).
- Screen size no less than 10.1".

# INSTALLING AND REMOVING THE APPLICATION

This section provides information about how to install the application on a computer and how to uninstall it.

## IN THIS SECTION:

Standard installation procedure.....	<a href="#">16</a>
Updating the previous version of Kaspersky Anti-Virus.....	<a href="#">21</a>
Non-standard installation scenarios .....	<a href="#">25</a>
Getting started.....	<a href="#">25</a>
Removing the application .....	<a href="#">25</a>

## STANDARD INSTALLATION PROCEDURE

Kaspersky Anti-Virus will be installed on your computer in an interactive mode using the Setup Wizard.

The Wizard consists of a series of screens (steps) that you can navigate through using the **Back** and **Next** buttons. To close the Wizard once it has completed its task, click the **Finish** button. To stop the Wizard at any stage, click the **Cancel** button.

If the application protects more than one computer (the maximum number of computers depends on your license), it will be installed in the same manner on all computers. Note that in this case, according to the license agreement, the license term begins from the date of the first activation. When you activate the application on the second computers and so on, the license validity term decreases for the amount of time that has elapsed since the first activation. So, the license validity term will expire simultaneously for all installed copies of the application.

➡ *To install Kaspersky Anti-Virus on your computer,*

run the setup file (the file with an EXE extension) from the CD with the product.

Installation of Kaspersky Anti-Virus from a setup file downloaded online is identical to installation from the installation CD.

**IN THIS SECTION:**

Step 1. Searching for a newer version of the application .....	<a href="#">17</a>
Step 2. Making sure the system meets the installation requirements.....	<a href="#">17</a>
Step 3. Selecting installation type .....	<a href="#">18</a>
Step 4. Reviewing the license agreement .....	<a href="#">18</a>
Step 5. Kaspersky Security Network Data Collection Statement.....	<a href="#">18</a>
Step 6. Searching for incompatible applications.....	<a href="#">18</a>
Step 7. Selecting the destination folder .....	<a href="#">19</a>
Step 8. Preparing for installation .....	<a href="#">19</a>
Step 9. Installing.....	<a href="#">20</a>
Step 10. Finishing the installation.....	<a href="#">20</a>
Step 11. Activating the application .....	<a href="#">20</a>
Step 12. Registering a user.....	<a href="#">20</a>
Step 13. Completing the activation.....	<a href="#">21</a>

**STEP 1. SEARCHING FOR A NEWER VERSION OF THE APPLICATION**

Before setup, the Setup Wizard checks the Kaspersky Lab update servers for a newer version of Kaspersky Anti-Virus.

If it does not find a newer product version on the Kaspersky Lab update servers, the Setup Wizard for the current version will be started.

If the update servers offer a newer version of Kaspersky Anti-Virus, you will see a prompt to download and install it on the computer. It is recommended that you install the new version of the application, because newer versions include further enhancements that ensure you have the most reliable protection for your computer. If you cancel the new version download, the Setup Wizard for the current version will be started. If you decide to install the newer version, product distribution files will be downloaded to your computer and the Setup Wizard for that new version will be started automatically. For a further description of the installation procedure for the newer version, please refer to the corresponding documentation.

**STEP 2. MAKING SURE THE SYSTEM MEETS THE INSTALLATION REQUIREMENTS**

Before installation of Kaspersky Anti-Virus on your computer, the installer checks the operating system and service packs to make sure they meet the software requirements for product installation (see section "Hardware and software requirements" on page [14](#)). In addition, the installer checks for the presence of required software and the credentials necessary to install applications. If any of the above-listed requirements is not met, a notification to that effect will be displayed on the screen.

If the computer meets all the requirements, the Wizard searches for Kaspersky Lab applications which, when run together with Kaspersky Anti-Virus, may result in conflicts. If such applications are found, you will be asked to remove them manually.

If an earlier version of Kaspersky Anti-Virus or Kaspersky Internet Security is found, all data that can be used by Kaspersky Anti-Virus 2012 (for example, activation information or application settings) will be saved and used when installing the new application, while the one installed earlier will be automatically removed.

### STEP 3. SELECTING INSTALLATION TYPE

At this stage, you can choose the most suitable type of Kaspersky Anti-Virus installation:

- *Standard installation.* If you choose this option (the **Change installation settings** box is unchecked), the application will be fully installed on your computer with the protection settings recommended by Kaspersky Lab experts.
- *Custom installation.* In this case (the **Change installation settings** box is checked), you will be asked to specify the destination folder into which the application should be installed (see section "Step 7. Selecting the destination folder" on page [19](#)) and disable the installation process protection, if necessary (see section "Step 8. Preparing for installation" on page [19](#)).

To proceed with the installation, click the **Next** button.

### STEP 4. REVIEWING THE LICENSE AGREEMENT

At this step, you should review the license agreement between you and Kaspersky Lab.

Read the agreement carefully and, if you accept all its terms, click the **I agree** button. The installation will continue.

If you cannot accept the license agreement, cancel the application installation by clicking the **Cancel** button.

### STEP 5. KASPERSKY SECURITY NETWORK DATA COLLECTION STATEMENT

At this stage, you will be invited to participate in the Kaspersky Security Network. Participation in the program involves sending information about new threats detected on your computer, running applications, and downloaded signed applications, as well as your system information, to Kaspersky Lab. We guarantee that none of your personal data will be sent.

Review the Kaspersky Security Network Data Collection Statement. To read the complete version of the Statement, click the **Full KSN agreement** button. If you agree with all terms of the Statement, check the **I accept the terms of participation in Kaspersky Security Network** box in the Wizard window.

Click the **Next** button if you have selected the custom installation (see section "Step 3. Selecting installation type" on page [18](#)). If performing the standard installation, click the **Install** button. The installation will continue.

### STEP 6. SEARCHING FOR INCOMPATIBLE APPLICATIONS

At this step, the application checks whether any applications incompatible with Kaspersky Anti-Virus are installed on your computer.

If no such applications are found, the Wizard automatically proceeds to the next step.

If any incompatible applications are detected, they are displayed in a list on the screen, and you will be prompted to remove them. Applications that Kaspersky Anti-Virus cannot remove automatically should be removed manually. When removing incompatible applications, you will need to reboot your operating system, after which installation of Kaspersky Anti-Virus will continue automatically.

To proceed with the installation, click the **Next** button.

## STEP 7. SELECTING THE DESTINATION FOLDER

This step of the Setup Wizard is only available if the custom installation is selected (see section "Step 3. Selecting installation type" on page 18). When performing a standard installation, this step is skipped and the application is installed to the default folder.

At this stage you are asked to choose the folder to which Kaspersky Anti-Virus will be installed. The following path is set by default:

- <disk>\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 2012 – for 32-bit systems;
- <disk>\Program Files (x86)\Kaspersky Lab\Kaspersky Anti-Virus 2012 – for 64-bit systems.

To install Kaspersky Anti-Virus to a different folder, specify the path to the desired folder in the input field or click the **Browse** button and choose a folder in the window that opens.

Keep in mind the following restrictions:

- The application cannot be installed on network or removable drives, or on virtual drives (those created using the SUBST command).
- We recommend that you avoid installing the application in a folder that already contains files or other folders, because that folder will then become inaccessible for editing.
- The path to the installation folder cannot be longer than 160 characters or contain the special characters /, ?, :, \*, ", >, < or |.

To find out if there is enough disk space on your computer to install the application, click the **Disk Usage** button. In the window that opens you can view the disk space information. To close the window, click **OK**.

To proceed with the installation, click the **Next** button in the Wizard window.

## STEP 8. PREPARING FOR INSTALLATION

This step of the Setup Wizard is only available if the custom installation is selected (see section "Step 3. Selecting installation type" on page 18). For the standard installation, this step is skipped.

Since your computer may be infected with malicious programs that may impact the installation of Kaspersky Anti-Virus, the installation process should be protected.

By default, installation process protection is enabled – the **Protect the installation process** box is checked in the Wizard window.

You are advised to uncheck this box if the application cannot be installed (for example, when performing remote installation using Windows Remote Desktop). Enabled protection may be the reason.

In this case, you should interrupt installation, restart it, check the **Change installation settings** box at the Select installation type step (see section "Step 3. Selecting installation type" on page 18), and when you reach the Preparing for installation step, uncheck the **Protect the installation process** box.

To proceed with the installation, click the **Install** button.

When installing the application on a computer running under Microsoft Windows XP, active network connections are terminated. The majority of terminated connections are restored after a pause.

## STEP 9. INSTALLING

Installation of the application can take some time. Wait for it to finish.

Once the installation is complete, the Wizard will automatically proceed to the next step.

If an installation error occurs, which may be due to malicious programs that prevent anti-virus applications from being installed on your computer, the Setup Wizard will prompt you to download *Kaspersky Virus Removal Tool*, a special utility for neutralizing infections.

If you agree to install the utility, the Setup Wizard downloads it from the Kaspersky Lab servers, after which installation of the utility starts automatically. If the Wizard cannot download the utility, you will be asked to download it on your own by clicking the link provided.

After you finish working with the utility, you should delete it and restart the installation of Kaspersky Anti-Virus.

## STEP 10. FINISHING THE INSTALLATION

This window of the Wizard informs you of the successful completion of the application installation. To run Kaspersky Anti-Virus, make sure that the **Run Kaspersky Anti-Virus** box is checked and click the **Finish** button.

In some cases, you may need to reboot your operating system. If the **Run Kaspersky Anti-Virus 2012** box is checked, the application will be run automatically after you reboot your operating system.

If you unchecked the box before closing the Wizard, you should run the application manually (see section "Launching and closing the application manually" on page [37](#)).

## STEP 11. ACTIVATING THE APPLICATION

*Activation* is the procedure of activating a license that allows you to use a fully functional version of the application until the license expires.

You will need an Internet connection to activate the application.

You will be offered the following options for Kaspersky Anti-Virus activation:

- **Activate commercial version.** Select this option and enter the activation code if you have purchased a commercial version of the application.

If you specify an activation code for Kaspersky Internet Security in the entry field, the procedure of switching to Kaspersky Internet Security starts after the completion of activation.

- **Activate trial version.** Use this activation option if you want to install the trial version of the application before making the decision to purchase a commercial version. You will be able to use the fully-functional version of the application for the duration of a term limited by the license for the trial version of the application. When the license expires, it cannot be activated for a second time.

## STEP 12. REGISTERING A USER

This step is only available when activating the commercial version of the application. When activating the trial version, this step is skipped.

You need to register in order to be able to contact Kaspersky Lab Technical Support Service in the future.

If you agree to register, specify your registration data in the corresponding fields and click the **Next** button.

## STEP 13. COMPLETING THE ACTIVATION

The Wizard informs you that Kaspersky Anti-Virus has been successfully activated. In addition, information about the license is provided: license type (commercial or trial), date of expiry, and number of hosts for the license.

If you have activated a subscription, information about the subscription status is displayed instead of the license expiry date.

Click the **Finish** button to close the Wizard.

## UPDATING THE PREVIOUS VERSION OF KASPERSKY ANTI-VIRUS

If Kaspersky Anti-Virus 2010 or 2011 is already installed on your computer, you should update the application to Kaspersky Anti-Virus 2012. If you have an active license for Kaspersky Anti-Virus 2010 or 2011, you will not have to activate the application: the Setup Wizard will automatically retrieve the information about your license for Kaspersky Anti-Virus 2010 or 2011 and use it during the installation process.

Kaspersky Anti-Virus will be installed on your computer in an interactive mode using the Setup Wizard.

The Wizard consists of a series of screens (steps) that you can navigate through using the **Back** and **Next** buttons. To close the Wizard once it has completed its task, click the **Finish** button. To stop the Wizard at any stage, click the **Cancel** button.

If the application protects more than one computer (the maximum number of computers depends on your license), it will be installed in the same manner on all computers. Note that in this case, according to the license agreement, the license term begins from the date of the first activation. When you activate the application on the second computers and so on, the license validity term decreases for the amount of time that has elapsed since the first activation. So, the license validity term will expire simultaneously for all installed copies of the application.

➤ *To install Kaspersky Anti-Virus on your computer,*

run the setup file (the file with an EXE extension) from the CD with the product.

Installation of Kaspersky Anti-Virus from a setup file downloaded online is identical to installation from the installation CD.

### IN THIS SECTION:

Step 1. Searching for a newer version of the application .....	<a href="#">22</a>
Step 2. Making sure the system meets the installation requirements.....	<a href="#">22</a>
Step 3. Selecting installation type .....	<a href="#">22</a>
Step 4. Reviewing the license agreement .....	<a href="#">22</a>
Step 5. Kaspersky Security Network Data Collection Statement.....	<a href="#">23</a>
Step 6. Searching for incompatible applications.....	<a href="#">23</a>
Step 7. Selecting the destination folder .....	<a href="#">23</a>
Step 8. Preparing for installation .....	<a href="#">24</a>
Step 9. Installing.....	<a href="#">24</a>
Step 10. Wizard completion .....	<a href="#">24</a>

## STEP 1. SEARCHING FOR A NEWER VERSION OF THE APPLICATION

Before setup, the Setup Wizard checks the Kaspersky Lab update servers for a newer version of Kaspersky Anti-Virus.

If it does not find a newer product version on the Kaspersky Lab update servers, the Setup Wizard for the current version will be started.

If the update servers offer a newer version of Kaspersky Anti-Virus, you will see a prompt to download and install it on the computer. It is recommended that you install the new version of the application, because newer versions include further enhancements that ensure you have the most reliable protection for your computer. If you cancel the new version download, the Setup Wizard for the current version will be started. If you decide to install the newer version, product distribution files will be downloaded to your computer and the Setup Wizard for that new version will be started automatically. For a further description of the installation procedure for the newer version, please refer to the corresponding documentation.

## STEP 2. MAKING SURE THE SYSTEM MEETS THE INSTALLATION REQUIREMENTS

Before installation of Kaspersky Anti-Virus on your computer, the installer checks the operating system and service packs to make sure they meet the software requirements for product installation (see section "Hardware and software requirements" on page [14](#)). In addition, the installer checks for the presence of required software and the credentials necessary to install applications. If any of the above-listed requirements is not met, a notification to that effect will be displayed on the screen.

If the computer meets all the requirements, the Wizard searches for Kaspersky Lab applications which, when run together with Kaspersky Anti-Virus, may result in conflicts. If such applications are found, you will be asked to remove them manually.

If an earlier version of Kaspersky Anti-Virus or Kaspersky Internet Security is found, all data that can be used by Kaspersky Anti-Virus 2012 (for example, activation information or application settings) will be saved and used when installing the new application, while the one installed earlier will be automatically removed.

## STEP 3. SELECTING INSTALLATION TYPE

At this stage, you can choose the most suitable type of Kaspersky Anti-Virus installation:

- *Standard installation.* If you choose this option (the **Change installation settings** box is unchecked), the application will be fully installed on your computer with the protection settings recommended by Kaspersky Lab experts.
- *Custom installation.* In this case (the **Change installation settings** box is checked), you will be asked to specify the destination folder into which the application should be installed (see section "Step 7. Selecting the destination folder" on page [19](#)) and disable the installation process protection, if necessary (see section "Step 8. Preparing for installation" on page [19](#)).

To proceed with the installation, click the **Next** button.

## STEP 4. REVIEWING THE LICENSE AGREEMENT

At this step, you should review the license agreement between you and Kaspersky Lab.

Read the agreement carefully and, if you accept all its terms, click the **I agree** button. The installation will continue.

If you cannot accept the license agreement, cancel the application installation by clicking the **Cancel** button.

## STEP 5. KASPERSKY SECURITY NETWORK DATA COLLECTION STATEMENT

At this stage, you will be invited to participate in the Kaspersky Security Network. Participation in the program involves sending information about new threats detected on your computer, running applications, and downloaded signed applications, as well as your system information, to Kaspersky Lab. We guarantee that none of your personal data will be sent.

Review the Kaspersky Security Network Data Collection Statement. To read the complete version of the Statement, click the **Full KSN agreement** button. If you agree with all terms of the Statement, check the **I accept the terms of participation in Kaspersky Security Network** box in the Wizard window.

Click the **Next** button if you have selected the custom installation (see section "Step 3. Selecting installation type" on page 18). If performing the standard installation, click the **Install** button. The installation will continue.

## STEP 6. SEARCHING FOR INCOMPATIBLE APPLICATIONS

At this step, the application checks whether any applications incompatible with Kaspersky Anti-Virus are installed on your computer.

If no such applications are found, the Wizard automatically proceeds to the next step.

If any incompatible applications are detected, they are displayed in a list on the screen, and you will be prompted to remove them. Applications that Kaspersky Anti-Virus cannot remove automatically should be removed manually. When removing incompatible applications, you will need to reboot your operating system, after which installation of Kaspersky Anti-Virus will continue automatically.

To proceed with the installation, click the **Next** button.

## STEP 7. SELECTING THE DESTINATION FOLDER

This step of the Setup Wizard is only available if the custom installation is selected (see section "Step 3. Selecting installation type" on page 18). When performing a standard installation, this step is skipped and the application is installed to the default folder.

At this stage you are asked to choose the folder to which Kaspersky Anti-Virus will be installed. The following path is set by default:

- <disk>\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 2012 – for 32-bit systems;
- <disk>\Program Files (x86)\Kaspersky Lab\Kaspersky Anti-Virus 2012 – for 64-bit systems.

To install Kaspersky Anti-Virus to a different folder, specify the path to the desired folder in the input field or click the **Browse** button and choose a folder in the window that opens.

Keep in mind the following restrictions:

- The application cannot be installed on network or removable drives, or on virtual drives (those created using the `SUBST` command).
- We recommend that you avoid installing the application in a folder that already contains files or other folders, because that folder will then become inaccessible for editing.
- The path to the installation folder cannot be longer than 160 characters or contain the special characters `/, ?, :, *, ", >, < or |`.

To find out if there is enough disk space on your computer to install the application, click the **Disk Usage** button. In the window that opens you can view the disk space information. To close the window, click **OK**.

To proceed with the installation, click the **Next** button in the Wizard window.

## STEP 8. PREPARING FOR INSTALLATION

This step of the Setup Wizard is only available if the custom installation is selected (see section "Step 3. Selecting installation type" on page [18](#)). For the standard installation, this step is skipped.

Since your computer may be infected with malicious programs that may impact the installation of Kaspersky Anti-Virus, the installation process should be protected.

By default, installation process protection is enabled – the **Protect the installation process** box is checked in the Wizard window.

You are advised to uncheck this box if the application cannot be installed (for example, when performing remote installation using Windows Remote Desktop). Enabled protection may be the reason.

In this case, you should interrupt installation, restart it, check the **Change installation settings** box at the Select installation type step (see section "Step 3. Selecting installation type" on page [18](#)), and when you reach the Preparing for installation step, uncheck the **Protect the installation process** box.

To proceed with the installation, click the **Install** button.

When installing the application on a computer running under Microsoft Windows XP, active network connections are terminated. The majority of terminated connections are restored after a pause.

## STEP 9. INSTALLING

Installation of the application can take some time. Wait for it to finish.

Once the installation is complete, the Wizard will automatically proceed to the next step.

If an installation error occurs, which may be due to malicious programs that prevent anti-virus applications from being installed on your computer, the Setup Wizard will prompt you to download *Kaspersky Virus Removal Tool*, a special utility for neutralizing infections.

If you agree to install the utility, the Setup Wizard downloads it from the Kaspersky Lab servers, after which installation of the utility starts automatically. If the Wizard cannot download the utility, you will be asked to download it on your own by clicking the link provided.

After you finish working with the utility, you should delete it and restart the installation of Kaspersky Anti-Virus.

## STEP 10. WIZARD COMPLETION

This window of the Wizard informs you of the successful completion of the application installation. To run Kaspersky Anti-Virus, make sure that the **Run Kaspersky Anti-Virus** box is checked and click the **Finish** button.

In some cases, you may need to reboot your operating system. If the **Run Kaspersky Anti-Virus 2012** box is checked, the application will be run automatically after you reboot your operating system.

If you unchecked the box before closing the Wizard, you should run the application manually (see section "Launching and closing the application manually" on page [37](#)).

## NON-STANDARD INSTALLATION SCENARIOS

This section describes application installation scenarios which differ from those of standard installation or update from the previous version.

### Installing Kaspersky Anti-Virus and activating later using a Kaspersky Internet Security activation code

If, when installing Kaspersky Anti-Virus, at the Activating the application step, you enter a Kaspersky Internet Security activation code, the upgrade process is launched then, which switches Kaspersky Anti-Virus to Kaspersky Internet Security.

If, when installing Kaspersky Anti-Virus, at the Activating the application step, you select **Activate later** and then activate the installed application with a Kaspersky Internet Security activation code, the upgrade process is also launched then, which switches Kaspersky Anti-Virus to Kaspersky Internet Security.

### Installing Kaspersky Anti-Virus 2012 over Kaspersky Internet Security 2010 or 2011

If you run the installation of Kaspersky Anti-Virus 2012 on a computer on which Kaspersky Internet Security 2010 or 2011 with an active license is already installed, the Installation Wizard detects the information about the license and prompts you to select one of the following further actions:

- Use the current license of Kaspersky Internet Security 2010 or 2011. In this case, the upgrade process is launched, which results in Kaspersky Internet Security 2012 being installed on your computer. You will be able to use Kaspersky Internet Security 2012 as long as the license for Kaspersky Internet Security 2010 or 2011 remains valid.
- Proceed with installation of Kaspersky Anti-Virus 2012. In this case, the installation procedure will continue according to the standard scenario, starting from the Activating the application step.

## GETTING STARTED

The application is ready to be used after installation. To ensure proper protection of your computer, we recommend performing the following immediately after installation and configuration:

- Update application databases (see section "How to update application databases and modules" on page [44](#)).
- Scan your computer for viruses (see section "How to perform a full scan of your computer for viruses" on page [47](#)) and vulnerabilities (see section "How to scan your computer for vulnerabilities" on page [47](#)).
- Check the protection status of your computer and eliminate problems in protection, if necessary.

## REMOVING THE APPLICATION

**After uninstalling Kaspersky Anti-Virus, your computer and personal data will be unprotected!**

Kaspersky Anti-Virus is uninstalled with the help of the Setup Wizard.

➤ *To start the Wizard,*

in the **Start** menu, select **Programs** → **Kaspersky Anti-Virus 2012** → **Remove Kaspersky Anti-Virus 2012**.

**IN THIS SECTION:**

---

Step 1. Saving data for reuse..... [26](#)

Step 2. Confirmation of application removal..... [26](#)

Step 3. Removing the application. Completing removal..... [26](#)

## STEP 1. SAVING DATA FOR REUSE

At this point you can specify which of the data used by the application you want to retain for reuse during the next installation of the application (e.g., a newer version of the application).

By default, the application is completely removed from the computer.

➤ *To save data for reuse:*

1. Choose the option **Save application objects**.
2. Check the boxes for the data types you want to save:
  - **Activation data** – data that eliminates the need to activate the application in the future by automatically using the current license as long as it has not expired by the time of the next installation.
  - **Backup and Quarantine files** – files checked by the application and placed into backup storage or quarantine.
  - **Operational settings of the application** – values of the application settings selected during configuration.
  - **iChecker data** – files which contain information about the objects that have already been scanned for viruses.

## STEP 2. CONFIRMATION OF APPLICATION REMOVAL

Since removing the application threatens the security of the computer and your personal data, you will be asked to confirm your intention to remove the application. To do this, click the **Remove** button.

To stop removal of the application at any time, you can cancel this operation by clicking the **Cancel** button.

## STEP 3. REMOVING THE APPLICATION. COMPLETING REMOVAL

At this step, the Wizard removes the application from your computer. Wait until removal is complete.

When removing the application, you may need to reboot your operating system. If you cancel the immediate reboot, completion of the removal procedure will be postponed until the operating system is rebooted or the computer is turned off and then restarted.

# LICENSING THE APPLICATION

This section provides information about general terms related to the application activation. Read this section to learn more about the purpose of the license agreement, license types, ways of activating the application, and the license renewal.

## IN THIS SECTION:

About the End User License Agreement .....	<a href="#">27</a>
About data provision .....	<a href="#">27</a>
About the license.....	<a href="#">27</a>
About the activation code.....	<a href="#">28</a>

## ABOUT THE END USER LICENSE AGREEMENT

License Agreement is a legal agreement concluded between you and Kaspersky Lab ZAO that stipulates the terms of use for the application.

**Read through the terms of the License Agreement carefully before you start using the application.**

You can read through the terms of the License Agreement when installing the Kaspersky Lab application.

The terms of the License Agreement are regarded as accepted in the following cases:

- Upon unsealing the box with the setup CD (only if you have purchased the application in the boxed version or at a store of any of our partners).
- Upon confirming your acceptance of the text of the License Agreement when installing the application.

If you do not accept the terms of the License Agreement, you have to interrupt the application installation.

## ABOUT DATA PROVISION

In order to increase the level of real-time protection, accepting the terms of the License Agreement means that you agree to send information about checksums of processed objects (MD5), information required to determine the reputation of URLs, and statistical data for anti-spam protection, in automatic mode. Information retrieved does not contain any private data and other types of confidential information. Information retrieved is protected by Kaspersky Lab pursuant to the requirements stipulated by the existing legislation. You can obtain more details on the website: <http://support.kaspersky.com>.

## ABOUT THE LICENSE

*License* is a time-limited right to use the application provided to you in accordance with the License Agreement. The license contains a unique code for the activation of your copy of Kaspersky Anti-Virus.

The license grants you the right to benefit the following services:

- Using the application on one or several devices.

Number of devices, on which you can use the application, is specified in the License Agreement.

- Contacting the Technical Support Service of Kaspersky Lab.
- Enjoying the complete set of services provided to you by Kaspersky Lab or its partners during the validity term of the license (see section "Service for registered users" on page [14](#)).

The scope of services provided and the validity term of the application depend on the type of license used to activate the application.

The following license types are provided:

- *Trial* – a free license with a limited validity period, offered to allow you to become familiar with the application.

If you copy the application from the website <http://www.kaspersky.com>, you automatically become the owner of the trial license. As soon as the license expires, all Kaspersky Anti-Virus features are disabled. To continue using the application, you should purchase the commercial license.

- *Commercial* – a paid license with a limited validity period, offered upon purchase of the application.

After the expiration of the commercial license, the application keeps on running in limited functionality mode. You will still be able to scan your computer for viruses and use other application components but only with databases installed before the license has expired. To continue using Kaspersky Anti-Virus, you should renew the commercial license.

We recommend that you renew the license on the day the current license expires at the latest in order to ensure the most comprehensible anti-virus protection of your computer.

## ABOUT THE ACTIVATION CODE

*Activation code* is a code that you receive on purchasing the commercial license for Kaspersky Anti-Virus. This code is required for activation of the application.

The activation code is an alphanumeric string of Latin characters in xxxxx-xxxxx-xxxxx-xxxxx format.

The activation code is provided in one of the following forms, depending on the way you purchase the application:

- If you have purchased the boxed version of Kaspersky Anti-Virus, the activation code is specified in the documentation or on the box containing the setup CD.
- If you have purchased Kaspersky Anti-Virus at an online store, the activation code is sent to the email address that you have specified when ordering the product.

The validity term of the license starts from the moment you have activated the application. If you have purchased a license intended for the use of Kaspersky Anti-Virus on several devices, the validity term of the license starts counting down from the moment you have entered the code on the first of those devices.

If you have lost or accidentally deleted your activation code after the activation, you should send a request to the Technical Support Service at Kaspersky Lab from My Kaspersky Account (see section "Obtaining technical support via My Kaspersky Account" on page [132](#)).

On completion of the application activation with a code, you are assigned a *client ID*. Client ID is the personal ID for a user, that is needed for receiving technical support by phone or via My Kaspersky Account (see section "Obtaining technical support via My Kaspersky Account" on page [132](#)).

# APPLICATION INTERFACE

This section provides information about basic elements of the graphic interface of the application: application icon and application icon context menu, main window, settings window, and notification windows.

## IN THIS SECTION:

---

The notification area icon .....	<a href="#">29</a>
The context menu .....	<a href="#">30</a>
The Kaspersky Anti-Virus main window .....	<a href="#">31</a>
Notification windows and pop-up messages .....	<a href="#">32</a>
The application settings window.....	<a href="#">34</a>
The Kaspersky Gadget.....	<a href="#">35</a>
News Agent.....	<a href="#">35</a>

## THE NOTIFICATION AREA ICON

Immediately after installation of the application, the application icon appears in the Microsoft Windows taskbar notification area.


In the Microsoft Windows 7 operating system the application icon is hidden by default, but you can display it to access the application more easily (see the operating system documentation).

The icon has the following purposes:


- It is an indicator of the application's operation.
- It provides access to the context menu, the main application window and the news window.


### Indication of application operation

This icon serves as an indicator of the application's operation. It also indicates the protection status and displays the basic functions currently being performed by the application:

 – scanning an email message;

 – scanning web traffic;


 – updating databases and application modules;


 – computer needs to be restarted to apply updates;

 – a failure occurred in the operation of an application component.

The icon is animated by default: for example, during the email message scan, a tiny letter symbol blinks in front of the application icon; when the update is in progress, you see a revolving globe. Animation can be deactivated (see section "Translucence of notification windows" on page [121](#)).


When the animation is disabled, the icon may take the following forms:

 (colored symbol) – all or some protection components are activated;

 (black-and-white symbol) – all protection components are disabled.

### Access to the context menu and application windows

Using the icon, you can open the context menu (on page [30](#)) (by right-clicking) and the main application window (see section "The Kaspersky Anti-Virus main window" on page [31](#)) (by left-clicking).

If news from Kaspersky Lab is available, the  icon appears in the Microsoft Windows taskbar notification area. Double-click this icon to open the News Agent (see section "News Agent" on page [35](#)).

## THE CONTEXT MENU

Using the context menu, you can quickly take various actions on the application.

The Kaspersky Anti-Virus menu contains the following items:

- **Task Manager** – opens the **Task Manager** window.
- **Update** – runs the update of application databases and modules.
- **Virtual Keyboard** – displays the Virtual Keyboard.
- **Kaspersky Anti-Virus** – opens the main application window.
- **Pause protection / Resume protection** – temporarily disables / enables real-time protection components. This menu item does not affect the application's updates or the execution of virus scans.
- **Settings** – opens the application settings window.
- **About** – opens a window containing information about the application.
- **News** – opens the News Agent window (see section "News Agent" on page [35](#)). This menu item is displayed if there is unread news.
- **Exit** – closes Kaspersky Anti-Virus (when this item is selected, the application is unloaded from the computer's RAM).



Figure 1. The context menu

If a virus scan or update task is running at the moment that you open the context menu, its name as well as its progress status (percentage complete) is displayed in the context menu. If you select a menu item with the name of a task, you can switch to the main window with a report of current task run results.

➔ To open the context menu,

position the cursor over the application icon in the taskbar notification area and right-click it.

In the Microsoft Windows 7 operating system the application icon is hidden by default, but you can display it to access the application more easily (see the operating system documentation).

## THE KASPERSKY ANTI-VIRUS MAIN WINDOW

The main application window contains interface elements that provide access to all the main features of the application.

The main window can be divided into two parts:

- The top part of the window provides information about the protection status of your computer.



Figure 2. Top part of the main window

- In the bottom part of the window, you can quickly switch to using the main features of the application (for example, running virus scan tasks, updating databases and software modules).



Figure 3. Bottom part of the main window

If you select any of the sections in the bottom part of the window, the window of the corresponding function opens. You can return to selecting functions by clicking the **Back** button in the top left corner of the window.

You can also use the following buttons and links:

- **Cloud protection** – to switch to information about Kaspersky Security Network (on page [124](#)).
- **Settings** – to open the application settings window (see section "The application settings window" on page [34](#)).
- **Reports** – to switch to the application operation reports.

- **News** – to switch to viewing news in the News Agent window (see section "News Agent" on page [35](#)). This link is displayed after the application receives a piece of news.
- **Help** – to view the Kaspersky Anti-Virus help system.
- **My Kaspersky Account** – to enter the user's personal account on the Technical Support Service website.
- **Support** – to open the window containing information about the system and links to Kaspersky Lab information resources (Technical Support Service website, forum).
- **Manage License** – to go to Kaspersky Anti-Virus activation and license renewal.

➔ You can open the main application window using one of the following methods:

- By left-clicking the application icon in the taskbar notification area.

In the Microsoft Windows 7 operating system the application icon is hidden by default, but you can display it to access the application more easily (see the operating system documentation).

- By selecting **Kaspersky Anti-Virus** from the context menu (see section "Context menu" on page [30](#)).
- By clicking the Kaspersky Anti-Virus icon located in the center of the Kaspersky Gadget (only for Microsoft Windows Vista and Microsoft Windows 7).

## NOTIFICATION WINDOWS AND POP-UP MESSAGES

Kaspersky Anti-Virus notifies you of important events occurring during its operation using *notification windows* and *pop-up messages* that appear over the application icon in the taskbar notification area.

*Notification windows* are displayed by Kaspersky Anti-Virus when various actions can be taken in connection with an event: for example, if a malicious object is detected, you can block access to it, delete it, or try to disinfect it. The application prompts you to select one of the available actions. A notification window only disappears from the screen if you select one of the actions.

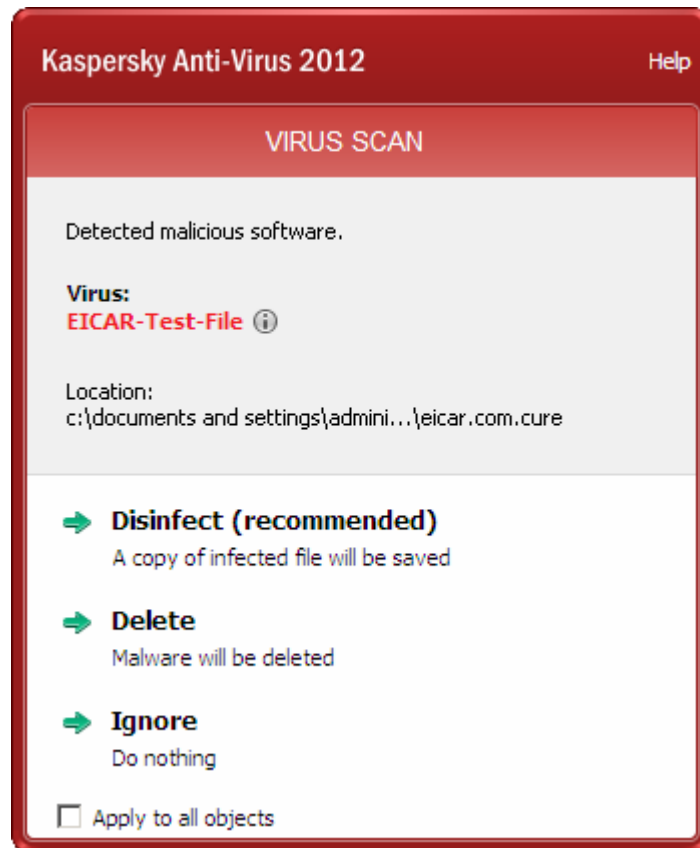


Figure 4. Notification window

*Pop-up messages* are displayed by Kaspersky Anti-Virus in order to inform you of events that do not require you to select an action. Some pop-up messages contain links that you can use to take an action offered by the application: for example, run a database update or initiate activation of the application). Pop-up messages automatically disappear from the screen soon after they appear.



Figure 5. Pop-up message

Depending on the importance of an event for the viewpoint of the computer's security, notifications and pop-up messages are divided into three types:

- **Critical notifications** – inform you of events that have a critical importance for the computer's security, such as detection of a malicious object or a dangerous activity in the system. Windows of critical notifications and pop-up messages are red-colored.

- Important notifications – inform you of events that are potentially important for the computer's security, such as detection of a potentially infected object or a suspicious activity in the system. Windows of important notifications and pop-up messages are yellow-colored.
- Information notifications – inform you of events that do not have critical importance for the computer's security. Windows of information notifications and pop-up messages are green-colored.

## THE APPLICATION SETTINGS WINDOW

The Kaspersky Anti-Virus settings window (also referred to as "settings window") is designed for configuring the entire application and separate protection components, scanning and update tasks, and for running other advanced configuration tasks (see section "Advanced application settings" on page 62).

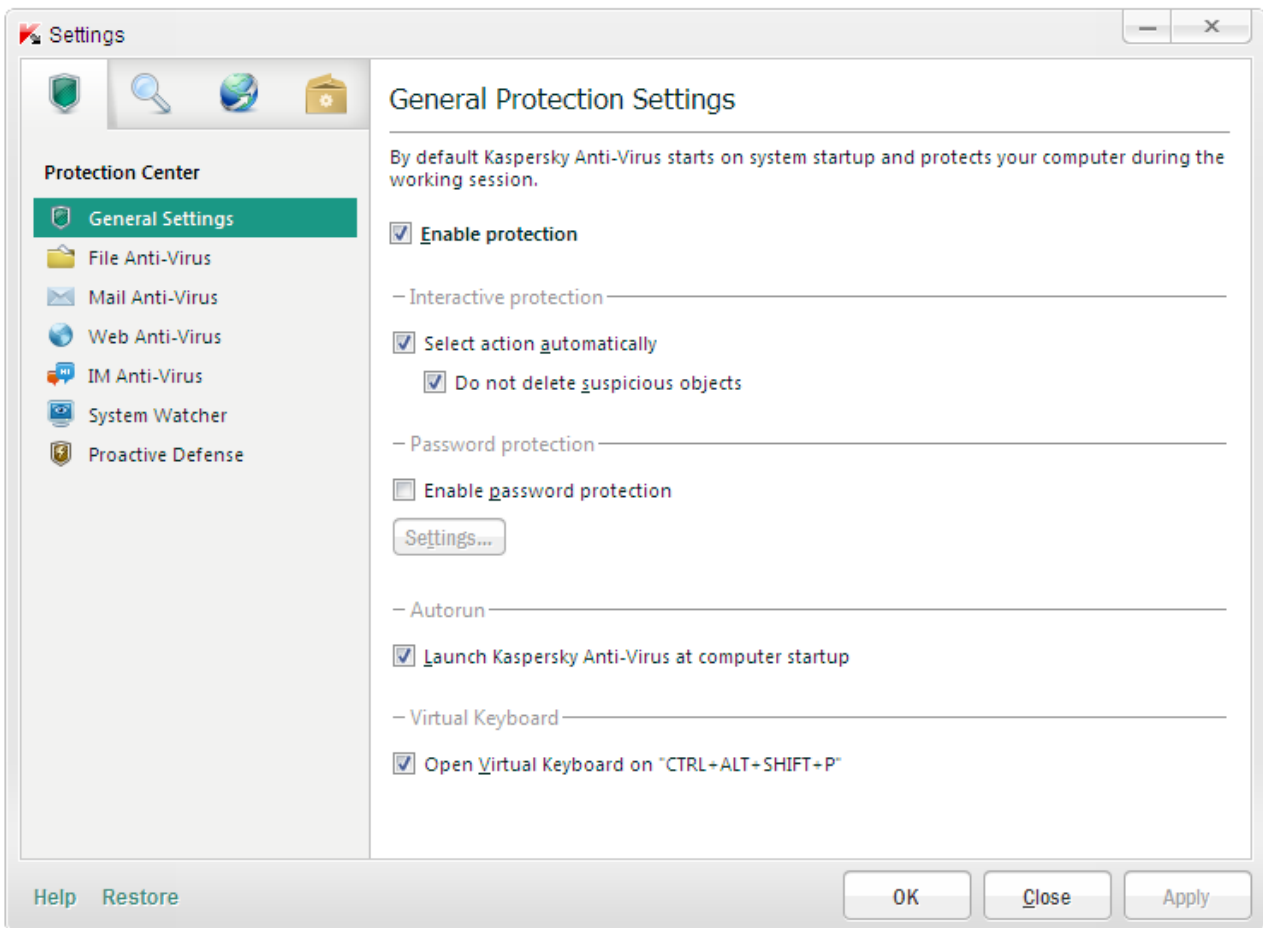


Figure 6. The application settings window

The application settings window consists of two parts:

- in the left part of the window you can choose the application component, task or another item that should be configured;
- the right part of the window contains the controls that you can use to configure the item selected in the left part of the window.

The components, tasks and other items in the left part of the window are grouped in the following sections:



– **Protection Center;**



– **Scan;**




– **Update;**



– **Advanced Settings.**

You can open the settings window using one of the following methods:

- by clicking the **Settings** link in the top part of the main application window (see section "The Kaspersky Anti-Virus main window" on page [31](#));
- by selecting **Settings** from the context menu (see section "Context menu" on page [30](#));
- by clicking the button with the  **Settings** icon in the Kaspersky Gadget interface (only for Microsoft Windows Vista and Microsoft Windows 7 operating systems). The function of opening the settings window should be assigned to the button (see section "How to use the Kaspersky Gadget" on page [59](#)).

## THE KASPERSKY GADGET

When using Kaspersky Anti-Virus on a computer running under Microsoft Windows Vista or Microsoft Windows 7, you can also use the Kaspersky Gadget (hereinafter the *gadget*). The Kaspersky Gadget is designed for quick access to the main features of the application (for example, protection status indication, virus scanning of objects, application operation reports).

After you install Kaspersky Anti-Virus on a computer running under Microsoft Windows 7, the gadget appears on your desktop automatically. After you install the application on a computer running under Microsoft Windows Vista, you should add the gadget to the Microsoft Windows Sidebar manually (see the operating system documentation).





Figure 7. The Kaspersky Gadget

## NEWS AGENT

Using *News Agent*, Kaspersky Lab informs you of all important events related to Kaspersky Anti-Virus and protection against computer threats.

The application will notify you of news by displaying a special icon in the taskbar notification area (see below) and a pop-up message. Information about the number of unread news items is also displayed in the main application window. A news icon appears in the Kaspersky Anti-Virus gadget interface.

You can read the news in one of the following ways:

- by clicking the  icon in the taskbar notification area;
- by clicking the **Read news** link in the pop-up news message;
- by clicking the **News** link in the main application window;
- by clicking the  icon which is displayed in the center of the Gadget when a piece of news appears (only for Microsoft Windows Vista and Microsoft Windows 7).

The above-listed methods of opening the News Agent window are only operable if any unread news is available.

If you do not want to receive any news, you can disable the news delivery.

# STARTING AND STOPPING THE APPLICATION

This section contains information on starting and shutting down the application.

## IN THIS SECTION:

Enabling and disabling automatic launch .....	<a href="#">37</a>
Launching and closing the application manually .....	<a href="#">37</a>

## ENABLING AND DISABLING AUTOMATIC LAUNCH

Automatic launch of the application means that Kaspersky Anti-Virus launches after the operating system startup. This is the default start mode.

◆ *To disable or enable automatic launch of the application:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **General Settings** subsection.
3. To disable automatic launch of the application, uncheck the **Launch Kaspersky Anti-Virus at computer startup** box in the **Autorun** section in the right part of the window. Check this box to enable automatic launch of the application.

## LAUNCHING AND CLOSING THE APPLICATION MANUALLY

Kaspersky Lab specialists do not recommend that you stop Kaspersky Anti-Virus, because the protection of your computer and personal data will then be at risk. It is recommended that you temporarily pause the computer's protection, without closing the application.

Kaspersky Anti-Virus should be started manually if you have disabled automatic launch of the application (see section "Enabling and disabling automatic launch" on page [37](#)).

◆ *To launch the application manually,*

in the **Start** menu, select **Programs** → **Kaspersky Anti-Virus 2012** → **Kaspersky Anti-Virus 2012**.

◆ *To exit the application,*

right-click to open the context menu of the application icon in the taskbar notification area and select **Exit**.

In the Microsoft Windows 7 operating system the application icon is hidden by default, but you can display it to access the application more easily (see the operating system documentation).

# MANAGING THE COMPUTER PROTECTION

This section provides information about how to detect threats to the computer's security and how to configure the security level. Read this section to learn more about how to enable, disable, and pause the protection when using the application.

## IN THIS SECTION:

---

Diagnostics and elimination of problems in your computer protection.....	<a href="#">38</a>
Enabling and disabling the protection .....	<a href="#">39</a>
Pausing and resuming protection.....	<a href="#">40</a>

## DIAGNOSTICS AND ELIMINATION OF PROBLEMS IN YOUR COMPUTER PROTECTION

Problems with computer protection are indicated by the computer indicator located in the left part of the main application window (see section "The Kaspersky Anti-Virus main window" on page [31](#)). The indicator is shaped as a monitor icon that changes color depending on the protection status of the computer: green means that the computer is protected, yellow indicates protection-related problems, red alerts of serious threats to the computer's security.



*Figure 8. Protection status indicator*

You are advised to fix the problems and security threats immediately.

Clicking the indicator in the main application window opens the **Security Problems** window (see the figure below) containing detailed information about the status of computer protection and troubleshooting suggestions for the detected problems and threats.

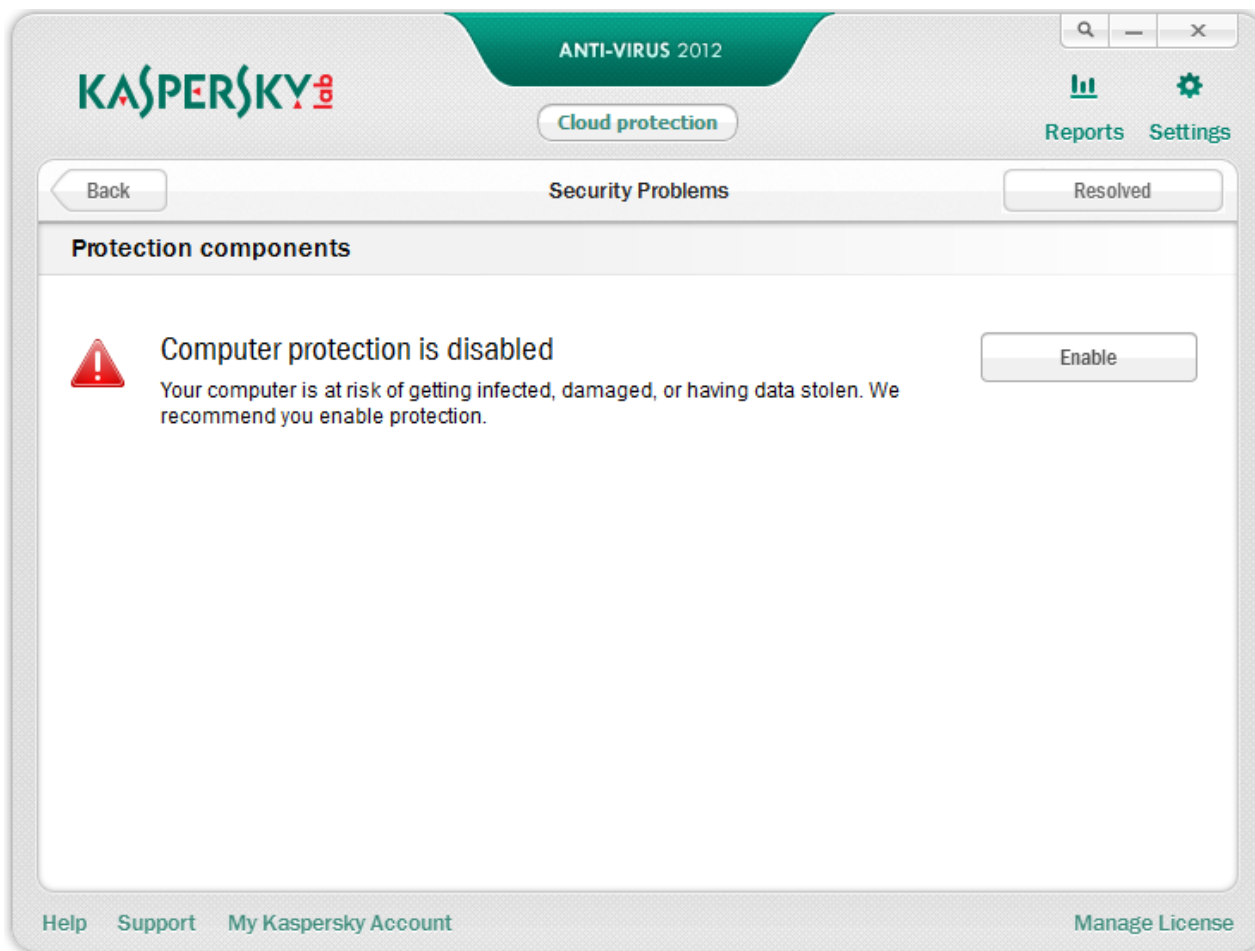


Figure 9. The Security Problems window

Problems with the protection are grouped by categories. For each problem, actions are listed that you can use to solve the problem.

## ENABLING AND DISABLING THE PROTECTION

By default, Kaspersky Anti-Virus is launched when the operating system loads and protects your computer until it is switched off. All protection components are running.

You can fully or partially disable the protection provided by Kaspersky Anti-Virus.

Kaspersky Lab specialists strongly recommend that you do not disable protection, since this may lead to an infection of your computer and data loss. It is recommended that you pause the protection for the required time interval (see section "Pausing and resuming protection" on page [40](#)).

The following signs indicate that the protection is paused or disabled:

- inactive (gray) application icon in the taskbar notification area (see section "The notification area icon" on page [29](#));
- a red security indicator in the upper part of the main application window.

In this case, the protection is regarded as the set of protection components. Disabling or pausing protection components does not affect the performance of virus scan tasks and Kaspersky Anti-Virus updates.

You can enable or disable the protection or individual application components from the application settings window (see section "The application settings window" on page [34](#)).

➤ *To completely enable or disable protection:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **General Settings** subsection.
3. Uncheck the **Enable protection** box if you need to disable protection. Check this box if you need to enable protection.

➤ *To disable or enable a protection component:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the component that should be enabled or disabled.
3. In the right part of the window, uncheck the **Enable <component name>** box if you need to disable this component. Check this box if you need to enable the component.

## PAUSING AND RESUMING PROTECTION

Pausing protection means temporarily disabling all protection components for a period of time.

The following signs indicate that the protection is paused or disabled:


- inactive (gray) application icon in the taskbar notification area (see section "The notification area icon" on page [29](#));
- a red security indicator in the upper part of the main application window.

In this case, the protection is regarded as the set of protection components. Disabling or pausing protection components does not affect the performance of virus scan tasks and Kaspersky Anti-Virus updates.

If network connections were established at the moment protection was paused, a notification about the termination of such connections is displayed.

When working on a computer running under Microsoft Windows Vista or Microsoft Windows 7, you can pause protection using the Kaspersky Gadget. To do this, you should assign the protection pausing function to a button of the gadget (see section "How to use the Kaspersky Gadget" on page [59](#)).

➤ *To pause the protection of your computer:*

1. Open the **Pause protection** window using one of the following methods:
  - select **Pause protection** from the context menu of the application icon (see section "The context menu" on page [30](#));
  - click the button with the  **Pause protection** icon in the Kaspersky Gadget interface (only for Microsoft Windows Vista and Microsoft Windows 7 operating systems).
2. In the **Pause protection** window, select the time interval after which protection should be resumed:
  - **Pause for the specified time** – protection will be enabled on expiration of the time interval selected from the dropdown list below.
  - **Pause until reboot** – protection will be enabled after the application is restarted or the operating system is rebooted (provided that automatic application launch is enabled (see section "Enabling and disabling automatic launch" on page [37](#))).
  - **Pause** – protection will be enabled when you decide to resume it (please see below).

➤ *To resume computer protection,*

select **Resume protection** from the context menu of the application icon (see section "The context menu" on page [30](#)).

You can use this method to resume computer protection when the **Pause** option has been selected, or when you have selected **Pause for the specified time** or **Pause until reboot**.

# SOLVING TYPICAL TASKS

This section provides information about how to resolve the most common issues related to protection of the computer using the application.

## IN THIS SECTION:

---

How to activate the application.....	<a href="#">42</a>
How to purchase or renew a license .....	<a href="#">43</a>
What to do when application notifications appear .....	<a href="#">44</a>
How to update application databases and modules .....	<a href="#">44</a>
How to scan critical areas of your computer for viruses .....	<a href="#">45</a>
How to scan a file, folder, disk, or another object for viruses .....	<a href="#">45</a>
How to perform a full scan of your computer for viruses .....	<a href="#">47</a>
How to scan your computer for vulnerabilities.....	<a href="#">47</a>
How to protect your personal data against theft.....	<a href="#">47</a>
What to do if you suspect an object is infected with a virus.....	<a href="#">49</a>
What to do if you suspect your computer is infected .....	<a href="#">50</a>
How to restore a file that has been deleted or disinfected by the application .....	<a href="#">51</a>
How to create and use a Rescue Disk .....	<a href="#">52</a>
How to view the report on the application's operation .....	<a href="#">55</a>
How to restore default application settings.....	<a href="#">55</a>
How to transfer settings to Kaspersky Anti-Virus installed on another computer .....	<a href="#">56</a>
How to switch from Kaspersky Anti-Virus to Kaspersky Internet Security .....	<a href="#">57</a>
How to use the Kaspersky Gadget.....	<a href="#">59</a>
How to know the reputation of an application.....	<a href="#">60</a>

## HOW TO ACTIVATE THE APPLICATION

*Activation* is the procedure of activating a license that allows you to use a fully functional version of the application until the license expires.

If you did not activate the application during installation, you can do so later. You will be reminded about the need to activate the application by Kaspersky Anti-Virus messages appearing in the taskbar notification area.

➤ *To run the Kaspersky Anti-Virus activation wizard, perform one of the following:*

- Click the **Activate** link in the Kaspersky Anti-Virus notice window that appears in the taskbar notification area.
- Click the **Insert your activation code here** link in the bottom part of the main application window. In the **Manage License** window that opens, click the **Activate the application** button.

When working with the application activation wizard, you should specify values for a collection of settings.

### Step 1. Enter activation code

Enter the activation code in the corresponding field and click the **Next** button.

### Step 2. Requesting activation

If the activation request is sent successfully, the Wizard automatically proceeds to the next step.

### Step 3. Entry of registration data

User registration is necessary for the user to be able to contact the Technical Support Service. Unregistered users receive only minimal support.

Specify your registration data and click the **Next** button.

### Step 4. Activation

If the application activation has been successful, the Wizard automatically proceeds to the next window.

### Step 5. Wizard completion

This window displays information on the activation results: the type of license used and the license expiry date.

Click the **Finish** button to close the Wizard.

## HOW TO PURCHASE OR RENEW A LICENSE

If you have installed Kaspersky Anti-Virus without a license, you can purchase one after installation. When purchasing a license, you receive an activation code that you should use to activate the application (see section "How to activate the application" on page [42](#)).

When your license expires, you can renew it. You can purchase a new license before the validity period of your current activation code expires. To do this, you should add the new code as a reserve activation code. When the validity term of the current license expires, Kaspersky Anti-Virus will be automatically activated using the reserve activation code.

➤ *To purchase a license:*

1. Open the main application window.
2. Click the **Manage License** link in the bottom part of the main window to open the **Manage License** window.
3. In the window that opens, click the **Buy activation code** button.

The eStore web page opens, where you can purchase a license.

➤ *To add a reserve activation code:*

1. Open the main application window.
2. Click the **Manage License** link in the bottom part of the main window to open the **Manage License** window.

The **Manage License** window opens.

3. In the window that opens, in the **New activation code** section, click the **Enter activation code** button.

The Application Activation Wizard opens.

4. Enter the activation code in the corresponding fields and click the **Next** button.

Kaspersky Anti-Virus then sends the data to the activation server for verification. If the verification is successful, the Wizard automatically proceeds to the next step.

5. Select **New code** and click the **Next** button.
6. When you have finished with the Wizard, click the **Finish** button.

## WHAT TO DO WHEN APPLICATION NOTIFICATIONS APPEAR

Notifications that appear in the taskbar notification area inform you of events occurring in the application's operation which require your attention. Depending on how critical the event is, you may receive the following types of notification:

- **Critical notifications** – inform you of events that have a critical importance for the computer's security, such as detection of a malicious object or a dangerous activity in the system. Windows of critical notifications and pop-up messages are red-colored.
- **Important notifications** – inform you of events that are potentially important for the computer's security, such as detection of a potentially infected object or a suspicious activity in the system. Windows of important notifications and pop-up messages are yellow-colored.
- **Information notifications** – inform you of events that do not have critical importance for the computer's security. Windows of information notifications and pop-up messages are green-colored.

If such a notification is displayed on the screen, you should select one of the options suggested in it. The optimal option is the one recommended as the default by Kaspersky Lab experts.

## HOW TO UPDATE APPLICATION DATABASES AND MODULES

By default, Kaspersky Anti-Virus automatically checks for updates on the Kaspersky Lab update servers. If the server stores a set of recent updates, Kaspersky Anti-Virus downloads and installs them in background mode. You can start updating Kaspersky Anti-Virus manually at any moment.

To download updates from Kaspersky Lab servers, you should be connected to Internet.

➤ *To start an update from the context menu,*

select **Update** from the context menu of the application icon.

➤ *To start an update from the main application window:*

1. Open the main application window and select the **Update** section in the lower part of the window.
2. In the **Update** window that opens, click the **Run update** button.

## HOW TO SCAN CRITICAL AREAS OF YOUR COMPUTER FOR VIRUSES

Critical areas scan means scanning the following objects:

- objects loaded at the startup of the operating system;
- system memory;
- boot sectors of the disk;
- objects added by the user (see section "Creating a list of objects to scan" on page [67](#)).


You can start the scan of critical areas using one of the following methods:

- using a shortcut created earlier (see page [71](#)).
- from the main application window (see section "The Kaspersky Anti-Virus main window" on page [31](#)).

➤ *To start the scan using a shortcut:*

1. Open the Microsoft Windows Explorer window and go to the folder where you created the shortcut.
2. Double-click the shortcut to start the scan.

➤ *To start a scan from the main application window:*

1. Open the main application window and select the **Scan** section in the lower part of the window.
2. In the **Scan** window that opens, in the **Critical Areas Scan** section, click the  button.

## HOW TO SCAN A FILE, FOLDER, DISK, OR ANOTHER OBJECT FOR VIRUSES

You can use the following methods to scan an object for viruses:

- using the context menu for the object;
- from the main application window (see section "The Kaspersky Anti-Virus main window" on page [31](#));
- using the Kaspersky Anti-Virus Gadget (only for Microsoft Windows Vista and Microsoft Windows 7 operating systems).

➤ *To start a virus scan task from the object context menu:*

1. Open Microsoft Windows Explorer and go to the folder which contains the object to be scanned.
2. Right-click to open the context menu of the object (see the figure below) and select **Scan for Viruses**.

The process and the outcome of the task will be displayed in the **Task Manager** window.

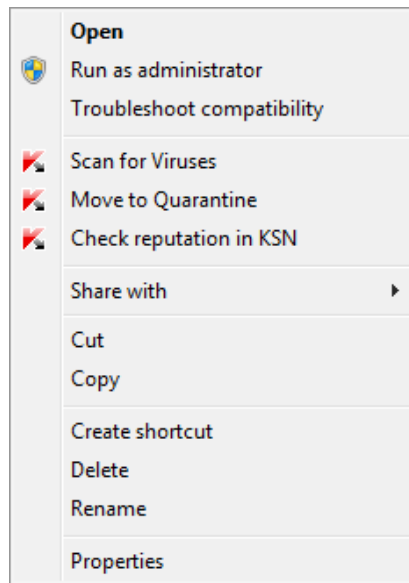


Figure 10. The context menu of an object in Microsoft Windows

➤ To start scanning an object from the main application window:

1. Open the main application window and select the **Scan** section in the lower part of the window.
  2. Specify the object to scan using one of the following methods:
    - Click the **specify** link in the bottom right part of the window to open the **Custom Scan** window, and check the boxes next to folders and drives that you need to scan.
- If the window displays no object to be scanned:
- a. Click the **Add** button.
  - b. In the **Select object to scan** window that opens, select an object to be scanned.
- Drag an object to scan into the dedicated area of the main window (see figure below).

The progress of the task will be displayed in the **Task Manager** window.

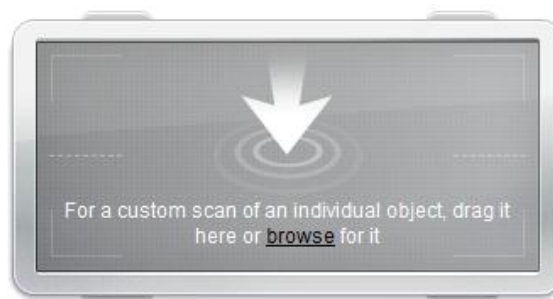


Figure 11. An area of the Scan window, into which you should drag an object to scan

➤ To scan an object for viruses using the gadget,

drag the object to scan onto the gadget.

The progress of the task will be displayed in the **Task Manager** window.

## HOW TO PERFORM A FULL SCAN OF YOUR COMPUTER FOR VIRUSES


You can start a full scan for viruses using one of the following methods:

- using a shortcut created earlier (see page [71](#));
- from the main application window (see section "The Kaspersky Anti-Virus main window" on page [31](#)).

➔ *To start a full scan using a shortcut:*

1. Open the Microsoft Windows Explorer window and go to the folder where you created the shortcut.
2. Double-click the shortcut to start the scan.

➔ *To start a full scan from the main application window:*

1. Open the main application window and select the **Scan** section in the lower part of the window.
2. In the **Scan** window that opens, in the **Full Scan** section, click the  button.

## HOW TO SCAN YOUR COMPUTER FOR VULNERABILITIES

*Vulnerabilities* are unprotected portions of software code which intruders may deliberately use for their purposes, for example, to copy data used in unprotected applications. Scanning your computer for vulnerabilities helps you to reveal any such weak points in your computer. You are advised to remove the detected vulnerabilities.


You can use the following methods to scan the system for vulnerabilities:

- from the main application window (see section "The Kaspersky Anti-Virus main window" on page [31](#));
- using a shortcut created earlier (see page [71](#)).

➔ *To start the task using a shortcut:*

1. Open the Microsoft Windows Explorer window and go to the folder where you created the shortcut.
2. Double-click the shortcut to start scanning the system for vulnerabilities.

➔ *To start the task from the main application window:*

1. Open the main application window and select the **Scan** section in the lower part of the window.
2. In the **Scan** window that opens, in the **Vulnerability Scan** section, click the  button.

## HOW TO PROTECT YOUR PERSONAL DATA AGAINST THEFT

With Kaspersky Anti-Virus, you can protect your personal data against theft; this includes data such as:

- passwords, usernames, and other registration data;
- account numbers and bank card numbers.

Kaspersky Anti-Virus comprises the following components and tools that help you protect your private data:

- Anti-Phishing. Protects against data thefts involving the phishing.
- Virtual Keyboard. Prevents interception of data entered at the keyboard.

**IN THIS SECTION:**

Protection against phishing ..... [48](#)

Protection against data interception at the keyboard ..... [48](#)

## PROTECTION AGAINST PHISHING

Protection against phishing is ensured by Anti-Phishing, implemented in the Web Anti-Virus and IM Anti-Virus components. Kaspersky Lab recommends that you enable the checking for phishing for all protection components.

➤ *To enable protection against phishing when Web Anti-Virus is running:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
3. Click the **Settings** button in the right part of the window.
4. The **Web Anti-Virus** window opens.
5. In the window that opens, on the **General** tab, in the **Kaspersky URL Advisor** section, check the **Check web pages for phishing** box.

➤ *To enable protection against phishing when IM Anti-Virus is running:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **IM Anti-Virus** component.
3. In the right part of the window, in the **Scan methods** section, check the **Check if URLs are listed in the database of phishing URLs** box.

## PROTECTION AGAINST DATA INTERCEPTION AT THE KEYBOARD

When working on the Internet, you frequently need to enter your personal data or your username and password. This happens, for example, during account registration on web sites, web shopping or Internet banking.

There is a risk that this personal information can be intercepted using hardware keyboard interceptors or keyloggers, which are programs that register keystrokes.

The Virtual Keyboard tool prevents the interception of data entered via the keyboard.

The Virtual Keyboard cannot protect your personal data if the website requiring the entry of such data has been hacked, because in this case the information is obtained directly by the intruders.

Many of the applications classified as spyware have the function of making screenshots which are then transmitted to an intruder for further analysis and extraction of the user's personal data. The Virtual Keyboard prevents the personal data being entered, from being intercepted through the use of screenshots.

The Virtual Keyboard only prevents the interception of personal data when working with Microsoft Internet Explorer, Mozilla Firefox and Google Chrome browsers.

The Virtual Keyboard has the following features:

- You can click the Virtual Keyboard buttons using the mouse.
- Unlike with real keyboards, there is no way to click several keys simultaneously on a Virtual Keyboard. Therefore, to use combinations of keys (e.g., **ALT+F4**), you have to click the first key (e.g., **ALT**), then the next key (e.g., **F4**), and then click the first key again. The second click of the key acts in the same way as the key release on a real keyboard.
- Input language for the Virtual Keyboard is toggled using the key combination **CTRL+SHIFT** (the **SHIFT** key should be clicked using the right mouse button) or **CTRL+LEFT ALT** (the **LEFT ALT** key should be clicked using the right mouse button), depending upon the specified settings.

You can open the Virtual Keyboard in the following ways:

- from the context menu of the application icon;
- from the main application window;
- from the Microsoft Internet Explorer, Mozilla Firefox or Google Chrome browser windows;
- using keyboard shortcuts.


➔ *To open the Virtual Keyboard from the context menu of the application icon,*

select **Virtual Keyboard** from the context menu of the application icon.

➔ *To open the Virtual Keyboard from the main application window,*

in the lower part of the main application window select **Virtual Keyboard**.

➔ *To open the Virtual Keyboard from the browser window,*

click the  **Virtual Keyboard** button in the toolbar of Microsoft Internet Explorer, Mozilla Firefox, or Google Chrome.

➔ *To open the Virtual Keyboard using the computer keyboard,*

press the **CTRL+ALT+SHIFT+P** shortcut.

## WHAT TO DO IF YOU SUSPECT AN OBJECT IS INFECTED WITH A VIRUS

If you suspect an object is infected, scan it using Kaspersky Anti-Virus (see section "How to scan a file, folder, disk, or another object for viruses" on page [45](#)).

If the application scans an object and then considers it as not infected although you suspect the contrary, you can perform any of the following actions:

- Move the object to *Quarantine*. Objects moved to Quarantine do not pose any threat to your computer. After the databases are updated, Kaspersky Anti-Virus may be able to clearly identify and remove the threat.
- Send the object to the *Virus Lab*. Virus Lab specialists scan the object. If it turns out to be infected with a virus, they add the description of the new virus into the databases that will be downloaded by the application with an update (see section "How to update application databases and modules" on page [44](#)).

You can move a file to Quarantine using one of two methods:

- by clicking the **Move to Quarantine** button in the **Quarantine** window;
- using the context menu for the file.

➤ *To move a file to Quarantine from the Quarantine window:*

1. Open the main application window.
2. In the lower part of the window, select the **Quarantine** section.
3. On the **Quarantine** tab click the **Move to Quarantine** button.
4. In the window that opens, select the file that you want to move to Quarantine.

➤ *To move a file to Quarantine using the context menu:*

1. Open Microsoft Windows Explorer and go to the folder that contains the file that you want to move to Quarantine.
2. Right-click to open the context menu of the file and select **Move to Quarantine**.

➤ *To send a file to the Virus Lab:*

1. Go to the Virus Lab request page (<http://support.kaspersky.com/virlab/helpdesk.html>).
2. Follow the instructions on this page to send your request.

## WHAT TO DO IF YOU SUSPECT YOUR COMPUTER IS INFECTED

If you suspect your operating system of being corrupted due to malware activity or system failures, use *Microsoft Windows Troubleshooting*, which removes any traces of malicious objects from the system. Kaspersky Lab recommends that you run the Wizard after the computer has been disinfected to make sure that all threats and damage caused by infections have been fixed.

Microsoft Windows Troubleshooting checks the system for modifications and faults (such as modifications of file extensions, blockage of the network environment and control panel). Modifications and faults may be caused by malware activity, an improper system configuration, system failures, or incorrect operation of system optimization applications.

After the review is complete, the Wizard analyzes the information to evaluate whether there is system damage which requires immediate attention. Based on the review, a list of actions necessary to eliminate the problems is generated. The Wizard groups these actions by category based on the severity of the problems detected.

➤ *To start the System Restore Wizard:*

1. Open the main application window (see page [31](#)).
2. In the lower part of the window, select the **Tools** section.
3. In the window that opens, in the **Microsoft Windows Troubleshooting** section, click the **Start** button.

The Microsoft Windows Troubleshooting window opens.

The Wizard consists of a series of screens (steps) that you can navigate through using the **Back** and **Next** buttons. To close the Wizard once it has completed its task, click the **Finish** button. To stop the Wizard at any stage, click the **Cancel** button.

### Step 1. Starting system restoration

Make sure that the Wizard option to **Search for problems caused by malware activity** is selected and click the **Next** button.

### Step 2. Problems search

The Wizard will search for problems and damage which should be fixed. Once the search is complete, the Wizard will proceed automatically to the next step.

### Step 3. Selecting troubleshooting actions

All damage found during the previous step is grouped on the basis of the type of danger it poses. For each damage group, Kaspersky Lab recommends a sequence of actions to repair the damage. There are three groups of actions:

- *Strongly recommended actions* eliminate problems posing a serious security threat. You are advised to perform all actions in this group.
- *Recommended actions* eliminate problems presenting a potential threat. You are also advised to perform all actions in this group.
- *Additional actions* repair system damage which does not pose a current threat, but may pose a danger to the computer's security in the future.

To view the actions within a group, click the **+** icon to the left of the group name.

To make the Wizard perform a certain action, check the box to the left of the corresponding action description. By default, the Wizard performs all recommended and strongly recommended actions. If you do not wish to perform a certain action, uncheck the box next to it.

**It is strongly recommended that you not uncheck the boxes selected by default, as doing so will leave your computer vulnerable to threats.**

Having defined the set of actions which the Wizard will perform, click the **Next** button.

### Step 4. Eliminating problems

The Wizard will perform the actions selected during the previous step. The elimination of problems may take some time. Once the troubleshooting is complete, the Wizard will automatically proceed to the next step.

### Step 5. Wizard completion

Click the **Finish** button to close the Wizard.

## HOW TO RESTORE A FILE THAT HAS BEEN DELETED OR DISINFECTED BY THE APPLICATION

**Kaspersky Lab recommends that you avoid restoring deleted and disinfected files, as they may pose a threat to your computer.**

If you want to restore a deleted or disinfected file, you can use a backup copy of it which was created by the application during the scan.

➤ To restore a file that has been deleted or disinfected by the application:

1. Open the main application window.
2. In the lower part of the window, select the **Quarantine** section.
3. On the **Storage** tab, select the required file from the list and click the **Restore** button.

## HOW TO CREATE AND USE A RESCUE DISK

After you install Kaspersky Anti-Virus and perform the first scan of your computer, it is recommended that you create the Rescue Disk.

The Rescue Disk is an application named Kaspersky Rescue Disk and recorded on a removable medium (CD or USB flash drive).

You will then be able to use Kaspersky Rescue Disk for scanning and disinfecting infected computers that cannot be disinfected using other methods (e.g., with anti-virus applications).

### IN THIS SECTION:

---

Creating a Rescue Disk.....	<a href="#">52</a>
Starting the computer from the Rescue Disk.....	<a href="#">54</a>

## CREATING A RESCUE DISK

Creating a Rescue Disk consists in creating a disk image (ISO file) with the up-to-date version of Kaspersky Rescue Disk, and writing it on a removable medium.

You can download the original disk image from the Kaspersky Lab server or copy it from a local source.

The Rescue Disk is created using the *Kaspersky Rescue Disk Creation Wizard*. The *rescuecd.iso* file created by the Wizard is saved on your computer's hard drive:

- in Microsoft Windows XP – in the following folder: Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Data\Rdisk\;
- in Microsoft Windows Vista and Microsoft Windows 7 operating systems – in the following folder: ProgramData\Kaspersky Lab\AVP12\Data\Rdisk\.

➤ To create a Rescue Disk:

1. Open the main application window.
2. In the lower part of the window, select the **Tools** section.
3. In the window that opens, in the **Kaspersky Rescue Disk** section, click the **Create** button.

The **Kaspersky Rescue Disk Creation Wizard** window opens.

The Wizard consists of a series of screens (steps) that you can navigate through using the **Back** and **Next** buttons. To close the Wizard once it has completed its task, click the **Finish** button. To stop the Wizard at any stage, click the **Cancel** button.

Let us review the steps of the Wizard in more detail.

## Step 1. Starting the Wizard. Searching for an existing disk image

The first window of the Wizard contains information about Kaspersky Rescue Disk.

If the Wizard detects an existing Rescue Disk ISO file in the dedicated folder (see above), the **Use existing ISO image** box will be displayed in the first window of the Wizard. Check the box to use the detected file as the original ISO image and go directly to the **Updating disk image** step (see below). Uncheck this box if you do not want to use the disk image that was detected. The Wizard will proceed to the **Select disk image source** window.

## Step 2. Selecting a disk image source

If you have checked the **Use existing ISO image** box in the first Wizard window, then this step will be skipped.

At this step, you should select a disk image source from the options suggested:

- If you already have a recorded copy of the Rescue Disk or an ISO image saved on your computer or on a local network resource, select **Copy ISO image from local or network drive**.
- If you have no ISO image file created for the Rescue Disk, and you want to download one from the Kaspersky Lab server (file size is about 175 MB), select **Download ISO image from Kaspersky Lab server**.

## Step 3. Copying (downloading) the disk image

If you have checked the **Use existing ISO image** box in the first Wizard window, then this step will be skipped.

If you have selected **Copy ISO image from local or network drive** at the previous step, click the **Browse** button. After you have specified the path to the file, click the **Next** button. The progress of copying the disk image is displayed in the Wizard window.

If you have selected **Download ISO image from Kaspersky Lab server** at the previous step, the progress of downloading the disk image is displayed immediately.

When copying or downloading of the ISO image is complete, the Wizard automatically proceeds to the next step.

## Step 4. Updating the ISO image file

The updating procedure for the ISO image file comprises the following operations:

- updating anti-virus databases;
- updating configuration files.

Configuration files determine whether the computer can be booted from a removable medium (such as a CD / DVD or a USB flash drive with Kaspersky Rescue Disk) created by the Wizard.

When updating anti-virus databases, those distributed at the last update of Kaspersky Anti-Virus are used. If databases are out of date, it is recommended that you run the update task and launch the Kaspersky Rescue Disk Creation Wizard again.

To begin updating the ISO file, click the **Next** button. The update's progress will be displayed in the Wizard window.

## Step 5. Recording the disk image on a medium

At this step, the Wizard informs you of a successful creation of a disk image and offers you to record it on a medium.

Specify a data medium for recording Kaspersky Rescue Disk:

- To record the disk image on a CD / DVD, select **Record to CD / DVD** and specify a medium, on which you want to record the disk image.
- To record the disk image on a USB flash drive, select **Record to USB flash drive** and specify a device, on which you want to record the disk image.

Kaspersky Lab recommends that you do not record the ISO image on devices which are not designed specifically for data storage, such as smartphones, cellphones, PDAs, and MP3 players. Recording ISO images on these devices may lead to their functioning incorrectly in the future.

- To record the disk image on the hard drive of your computer or on the hard drive of another one that you can access via a network, select **Save the disk image to file on local or network drive** and specify a folder, in which you want to record the disk image, and the name of the ISO file.

## Step 6. Wizard completion

To close the Wizard once it has completed its task, click the **Finish** button. You can use the newly created Rescue Disk to boot the computer (see page [54](#)) if you cannot boot it and run Kaspersky Anti-Virus in normal mode due to an impact caused by viruses or malware.

## STARTING THE COMPUTER FROM THE RESCUE DISK

If the operating system cannot be booted as a result of a virus attack, use the Rescue Disk.

To boot the operating system, you should use a CD / DVD or a USB flash drive with Kaspersky Rescue Disk copied on it (see section "Creating a Rescue Disk" on page [52](#)).

Booting a computer from a removable media is not always possible. In particular, this mode is not supported by some obsolete computer models. Before shutting down your computer for subsequent booting from a removable media, make sure that this operation can be performed.

➤ *To boot your computer from the Rescue Disk:*

1. In the BIOS settings, enable booting from a CD / DVD or a USB device (for detailed information, please refer to the documentation for your computer's motherboard).
2. Insert a CD / DVD into the CD / DVD drive of an infected computer or connect a USB flash device with Kaspersky Rescue Disk copied on it.
3. Restart your computer.


For detailed information about the use of the Rescue Disk, please refer to the Kaspersky Rescue Disk User Guide.

## HOW TO VIEW THE REPORT ON THE APPLICATION'S OPERATION

Kaspersky Anti-Virus creates operation reports for each component. Using a report, you can obtain statistical information about the application's operation (for example, learn how many malicious objects have been detected and neutralized for a specified time period, how many times the application has been updated for the same period, how many spam messages have been detected and much more).

When working on a computer running under Microsoft Windows Vista or Microsoft Windows 7, you can open reports using the Kaspersky Gadget. To do this, the Kaspersky Gadget should be configured so that the option of opening the reports window is assigned to one of its buttons (see section "How to use the Kaspersky Gadget" on page [59](#)).

➤ *To view the application operation report:*

1. Open the **Reports** window using any of the following methods:
  - click the **Reports** link in the top part of the main application window;
  - click the button with the  **Reports** icon in the Kaspersky Gadget interface (only for Microsoft Windows Vista and Microsoft Windows 7 operating systems).

The **Reports** window displays reports on the application's operation represented as diagrams.

2. If you want to view a detailed application operation report (for example, a report on the operation of each component), click the **Detailed report** button in the bottom part of the **Report** window.

The **Detailed report** window will open, where data are represented in a table. For convenient viewing of reports, you can select various entry sorting options.

## HOW TO RESTORE DEFAULT APPLICATION SETTINGS

You can restore the default application settings recommended by Kaspersky Lab for Kaspersky Anti-Virus, at any time. The settings can be restored using the *Application Configuration Wizard*.

When the Wizard completes its operation, the **Recommended** security level is set for all protection components. When restoring the recommended security level, you can save the previously specified values for some of the settings of application components.

➤ *To restore the default settings of the application:*

1. Open the application settings window.
2. Run the Application Configuration Wizard using one of the following methods:
  - click the **Restore** link in the bottom part of the window;
  - in the left part of the window, select the **Manage Settings** subsection in the **Advanced Settings** section and click the **Restore** button in the **Restore default settings** section.

Let us review the steps of the Wizard in more detail.

### Step 1. Starting the Wizard

Click the **Next** button to proceed with the Wizard.

## Step 2. Restore settings

This Wizard window shows which Kaspersky Anti-Virus protection components have settings that differ from the default value because they were changed by the user. If special settings have been created for any of the components, they will also be shown in this window.

Check the boxes for the settings that you want to save and click the **Next** button.

## Step 3. Finishing restoration

To close the Wizard once it has completed its task, click the **Finish** button.

# HOW TO TRANSFER SETTINGS TO KASPERSKY ANTI-VIRUS INSTALLED ON ANOTHER COMPUTER

Once you have configured the product, you can apply its settings to Kaspersky Anti-Virus installed on another computer. Consequently, the application will be configured identically on both computers. This is a helpful feature when, for example, Kaspersky Anti-Virus is installed on your home computer and in your office.

The application settings are stored in a special configuration file that you can transfer to another computer.

The settings of Kaspersky Anti-Virus can be transferred to another computer in three steps:

1. Saving the application settings in a configuration file.
2. Transferring a configuration file to another computer (for example, by email or on a removable medium).
3. Applying settings from a configuration file to the application installed on another computer.

### ➤ *To export the current settings of Kaspersky Anti-Virus:*

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Manage Settings** subsection.
3. Click the **Save** button in the right part of the window.
4. In the window that opens, enter the name of the configuration file and the path where it should be saved.
5. Click the **OK** button.

### ➤ *To import the application's settings from a saved configuration file:*

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Manage Settings** subsection.
3. Click the **Load** button in the right part of the window.
4. In the window that opens, select the file from which you wish to import the Kaspersky Anti-Virus settings.
5. Click the **OK** button.

# HOW TO SWITCH FROM KASPERSKY ANTI-VIRUS TO KASPERSKY INTERNET SECURITY

Kaspersky Anti-Virus allows you to switch to Kaspersky Internet Security without any additional downloads and installation of software.

*Kaspersky Internet Security* is an application designed to ensure comprehensive protection of your computer. It provides a whole range of advanced features implemented with the following modules and functions:

- Application Control;
- Parental Control;
- Firewall;
- Network Attack Blocker;
- Geo Filter;
- Blocking access to insecure websites;
- Network Monitor;
- Anti-Spam;
- Anti-Banner;
- Privacy Cleaner;
- Safe Run.

You can temporarily switch to the trial version of Kaspersky Internet Security in order to appreciate its features, or immediately begin using the commercial version of the application.

If you use the license with a subscription or handle the application in some specific regions, your copy of Kaspersky Internet Security does not allow the temporary switching to the trial version.

## IN THIS SECTION:

---

Switching to the commercial version .....	<a href="#">57</a>
Temporary switching to the trial version .....	<a href="#">58</a>

## SWITCHING TO THE COMMERCIAL VERSION

If you want to switch to the commercial version of Kaspersky Internet Security, you need an activation code for the commercial version of the application that you can use to activate it (see section "How to activate the application" on page [42](#)).

➤ *To purchase an activation code for Kaspersky Internet Security:*

1. Open the main application window.
2. In the bottom part of the window, select the **Upgrade** section.
3. In the window that opens, click the **Buy activation code** button.

You are redirected to the website of eStore, where you can purchase an activation code for Kaspersky Internet Security.

If you purchase the application in some specific regions or use the license with subscription, the **Upgrade** section is not represented in the main application window.

## TEMPORARY SWITCHING TO THE TRIAL VERSION

You can temporarily switch to the trial version of Kaspersky Internet Security in order to appreciate its functionality. After that, you can optionally purchase a license for further use of the application.

➤ *To temporarily switch to Kaspersky Internet Security:*

1. Open the main application window.
2. In the bottom part of the window, select the **Upgrade** section.
3. In the window that opens, click the **Trial version** button.

The Application Configuration Wizard then opens.

If you purchase the application in some specific regions or use the license with subscription, the **Upgrade** section is not represented in the main application window.

When working with the Application Configuration Wizard, you should specify values for a collection of settings.

### Step 1. Requesting activation of the trial version of Kaspersky Internet Security

If the activation request for Kaspersky Internet Security is sent successfully, the Wizard automatically proceeds to the next step.

### Step 2. Starting the upgrade

At this step, the Wizard displays a message on the screen, which informs you that all upgrade prerequisites are met. To proceed with the Wizard, click the **Next** button.

### Step 3. Removing incompatible applications

At this step, the Wizard checks if any applications incompatible with Kaspersky Internet Security are installed on your computer. If no such applications are found, the Wizard automatically proceeds to the next step. If such applications are found, the Wizard lists them in the window and offers you to uninstall them.

After incompatible applications are uninstalled, you may need to restart the operating system. After the operating system is restarted, the Wizard opens automatically to resume the upgrade process.

#### Step 4. Upgrading

At this step, the Wizard connects upgrade modules, which may take some time. When the process is complete, the Wizard automatically proceeds to the next step.

#### Step 5. Restarting the application

At the final step of the upgrade, the application should be restarted. To do this, click the **Finish** button in the Wizard window.

#### Step 6. Completing the activation

After the application is restarted, the Wizard opens automatically. After a successful activation of the trial version of Kaspersky Internet Security, the Wizard window displays information about the term, during which you can use the trial version.

#### Step 7. System analysis

At this stage, information about Microsoft Windows applications is collected. These applications are added to the list of trusted applications which have no restrictions imposed on the actions they perform in the system.

Once the analysis is complete, the Wizard will automatically proceed to the next step.

#### Step 8. Finishing the upgrade

To close the Wizard once it has completed its task, click the **Finish** button.

The application cannot be switched to the trial version of Kaspersky Internet Security for a second time.

## HOW TO USE THE KASPERSKY GADGET

When using Kaspersky Anti-Virus on a computer running under Microsoft Windows Vista or Microsoft Windows 7, you can also use the Kaspersky Gadget (hereinafter the *gadget*). After you install Kaspersky Anti-Virus on a computer running under Microsoft Windows 7, the gadget appears on your desktop automatically. After you install the application on a computer running under Microsoft Windows Vista, you should add the gadget to the Microsoft Windows Sidebar manually (see the operating system documentation).

The Gadget color indicator displays your computer's protection status in the same manner as the indicator in the main application window (see section "Diagnostics and elimination of problems in your computer protection" on page 38). Green indicates that your computer is duly protected, while yellow indicates that there are protection problems, and red indicates that your computer's security is at serious risk. Gray indicates that the application is stopped.

While updating the application databases and software modules, a revolving globe-shaped icon is displayed in the center part of the gadget.

You can use the gadget to perform the following actions:

- resume the application if it has been paused earlier;
- open the main application window;
- scan specified objects for viruses;
- open the news window.

Also, you can configure the buttons of the gadget so that they could initiate additional actions:

- run an update;
- edit the application settings;
- view application reports;
- pause the protection;
- open the Virtual Keyboard;
- open the Task Manager window.

➤ *To start the application using the gadget,*

click the icon  **Enable** icon located in the center of the gadget.

➤ *To open the main application window using the gadget,*


click the monitor icon in the center area of the gadget.

➤ *To scan an object for viruses using the gadget,*


drag the object to scan onto the gadget.

The progress of the task will be displayed in the **Task Manager** window.

➤ *To open the news window using the gadget,*

click the  icon which is displayed in the center of the gadget when news is released.

➤ *To configure the gadget:*

1. Open the gadget settings window by clicking the  icon that appears in the upper right corner of the gadget block if you position the cursor over it.
2. In the dropdown lists corresponding to gadget buttons, select actions that should be performed when you click those buttons.
3. Click the **OK** button.

## HOW TO KNOW THE REPUTATION OF AN APPLICATION

Kaspersky Anti-Virus allows you to learn the reputation of applications from users all over the world. Reputation of an application comprises the following criteria:

- name of the vendor;
- information about the digital signature (available if a digital signature exists);
- information about the group, in which the application has been included by a majority of users of Kaspersky Security Network;
- number of users of Kaspersky Security Network that use the application (available if the application has been included in the Trusted group in Kaspersky Security Network database);

- time, at which the application has become known in Kaspersky Security Network;
- countries, in which the application is the most widespread.

To verify the reputation of an application, you should agree to participate in Kaspersky Security Network (see page [124](#)) when installing Kaspersky Anti-Virus.

➤ *To know the reputation of an application,*

open the context menu of the executable file of the application and select **Check reputation in KSN**.

#### SEE ALSO:

---

Kaspersky Security Network ..... [124](#)

# ADVANCED APPLICATION SETTINGS

This section provides detailed information about how to configure each of the application components.

## IN THIS SECTION:

---

General protection settings .....	<a href="#">62</a>
Scan .....	<a href="#">64</a>
Update.....	<a href="#">72</a>
File Anti-Virus.....	<a href="#">77</a>
Mail Anti-Virus .....	<a href="#">83</a>
Web Anti-Virus .....	<a href="#">88</a>
IM Anti-Virus.....	<a href="#">94</a>
Proactive Defense.....	<a href="#">95</a>
System Watcher.....	<a href="#">97</a>
Network protection .....	<a href="#">99</a>
Trusted zone .....	<a href="#">103</a>
Performance and compatibility with other applications.....	<a href="#">105</a>
Kaspersky Anti-Virus self-defense .....	<a href="#">108</a>
Quarantine and Backup.....	<a href="#">109</a>
Additional tools for better protection of your computer .....	<a href="#">113</a>
Reports.....	<a href="#">117</a>
Application appearance. Managing active interface elements.....	<a href="#">121</a>
Notifications.....	<a href="#">122</a>
Kaspersky Security Network .....	<a href="#">124</a>

## GENERAL PROTECTION SETTINGS

In the application settings window, in the **General Settings** subsection of the **Protection Center** section, you can:

- disable all protection components (see section "Enabling and disabling protection" on page [39](#));
- select the interactive or automatic protection mode (see section "Selecting a protection mode" on page [63](#));
- restrict users' access to the application by setting a password (see section "Restricting access to Kaspersky Anti-Virus" on page [63](#));

- disable or enable automatic launching of the application at operating system startup (see section "Enabling and disabling automatic launch" on page [37](#));
- enable a custom key combination for displaying the virtual keyboard on the screen (see section "Protection against data interception at the keyboard" on page [48](#)).

### IN THIS SECTION:

Restricting access to Kaspersky Anti-Virus .....	<a href="#">63</a>
Selecting a protection mode .....	<a href="#">63</a>

## RESTRICTING ACCESS TO KASPERSKY ANTI-VIRUS

A computer may be used by several users with various levels of computer literacy. Unrestricted user access to Kaspersky Anti-Virus and its settings may lead to a reduced level of computer protection.

To restrict access to the application, you can set a password and specify which actions should require the password to be entered:

- changing application settings;
- closing the application;
- removing the application.

**Be careful when using a password to restrict access to application removal. If you forget the password, the application will be difficult to remove from your computer.**

➔ *To restrict access to Kaspersky Anti-Virus with a password:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **General Settings** subsection.
3. In the right part of the window, in the **Password protection** section, check the **Enable password protection** box and click the **Settings** button.
4. In the **Password protection** window that opens, enter the password and specify the area to be covered by the access restriction.

## SELECTING A PROTECTION MODE

By default, Kaspersky Anti-Virus runs in *automatic protection mode*. In this mode the application automatically applies actions recommended by Kaspersky Lab in response to dangerous events. If you wish Kaspersky Anti-Virus to notify you of all hazardous and suspicious events in the system and to allow you to decide which of the actions offered by the application should be applied, you can enable the *interactive protection mode*.

➤ To select a protection mode:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **General Settings** subsection.
3. In the **Interactive protection** section, check or uncheck the boxes depending on your choice of protection mode:
  - to enable the interactive protection mode, uncheck the **Select action automatically** box;
  - to enable automatic protection mode, check the **Select action automatically** box.

If you do not want Kaspersky Anti-Virus to delete suspicious objects when running in automatic mode, check the **Do not delete suspicious objects** box.

## SCAN

Scanning the computer for vulnerabilities, viruses and other riskware is one of the most important tasks when ensuring the computer's security.

It is necessary to regularly scan your computer for viruses and other riskware in order to rule out the possibility of spreading malicious programs that have not been detected by protection components, for example, due to a low security level set, or for other reasons.

The vulnerability scan performs diagnostics of operating system safety and detects software features that could be used by intruders to spread malicious objects and obtain access to personal information.

This section contains information about scan task features and configuration, security levels, scan methods, and scan technologies.

### IN THIS SECTION:

---

Virus scan .....	<a href="#">64</a>
Vulnerability Scan .....	<a href="#">72</a>
Managing scan tasks. Task Manager.....	<a href="#">72</a>

## VIRUS SCAN

To detect viruses and other riskware, Kaspersky Anti-Virus comprises the following tasks:

- **Full Scan.** Scan of the entire system. By default, Kaspersky Anti-Virus scans the following objects:
  - system memory;
  - objects loaded on operating system startup;
  - system backup;
  - email databases;
  - removable storage media, hard and network drives.

- **Critical Areas Scan.** By default, Kaspersky Anti-Virus scans objects loaded at the startup of the operating system.
- **Custom Scan.** Kaspersky Anti-Virus scans objects selected by the user. You can scan any object from the list below:
  - system memory;
  - objects loaded on operating system startup;
  - system backup;
  - email databases;
  - removable storage media, hard and network drives;
  - any file or folder that you have selected.

The Full Scan and the Critical Areas Scan tasks have their peculiarities. For these tasks, it is not recommended that you edit the lists of objects to scan.

Each scan task is performed in a specified area and can be started according to a previously created schedule. Each scan task is also characterized by a security level (a combination of settings that impact the depth of the scan). By default, the *signature mode* (the one using records from application databases to search for threats) is always enabled. You can also apply various scan methods and technologies.

After the full scan task or the critical areas scan task is started, the scan run progress is displayed in the **Scan** window, in the section with the name of the task running, and in the Task Manager (see section "Managing scan tasks. Task Manager" on page [72](#)).

If a threat is detected, Kaspersky Anti-Virus assigns one of the following statuses to the found object:

- Malicious program (such as a *virus* or *Trojan*).
- *Potentially infected* (suspicious) status if the scan cannot determine whether the object is infected or not. The file may contain a sequence of code characteristic of viruses, or modified code from a known virus.

The application displays a notification (see page [122](#)) about the detected threat and performs the prescribed action. You can change the actions to be taken when a threat is detected.

If you are working in automatic mode (see section "Selecting a protection mode" on page [63](#)), when dangerous objects are detected, Kaspersky Anti-Virus automatically applies the actions recommended by Kaspersky Lab specialists. For malicious objects, this action is **Disinfect. Delete if disinfection fails**, for suspicious objects – **Move to Quarantine**. If dangerous objects are detected when working in interactive mode (see section "Selecting a protection mode" on page [63](#)), the application displays a notification on the screen that you can use to select the required action the list of available ones.

Before attempting to disinfect or delete an infected object, Kaspersky Anti-Virus creates a backup copy for subsequent restoration or disinfection. Suspicious (potentially infected) objects are quarantined. You can enable automatic scanning of quarantined objects after each update.

Information on the scan results and events which have occurred during the execution of the task is logged in a Kaspersky Anti-Virus report (see page [117](#)).

**IN THIS SECTION:**

Changing and restoring the security level .....	<a href="#">66</a>
Creating the scan startup schedule .....	<a href="#">67</a>
Creating a list of objects to scan .....	<a href="#">67</a>
Selecting a scan method .....	<a href="#">68</a>
Selecting scan technology.....	<a href="#">68</a>
Changing the actions to be performed when a threat is detected .....	<a href="#">69</a>
Running a scan under a different user account.....	<a href="#">69</a>
Changing the type of objects to scan .....	<a href="#">69</a>
Scanning of compound files .....	<a href="#">70</a>
Scan optimization.....	<a href="#">70</a>
Scanning removable drives on connection.....	<a href="#">71</a>
Creating a task shortcut .....	<a href="#">71</a>

**CHANGING AND RESTORING THE SECURITY LEVEL**

Depending on your current needs, you can select one of the preset security levels or modify the scan settings manually.

When configuring scan task settings, you can always restore the recommended ones. These settings are considered optimal, recommended by Kaspersky Lab, and grouped in the **Recommended** security level.

➤ *To change the established security level:*

1. Open the application settings window.
2. In the left part of the window, in the **Scan** section, select the desired task (**Full Scan**, **Critical Areas Scan**, or **Custom Scan**).
3. In the **Security level** section, set the desired security level for the task selected, or click the **Settings** button to modify scan settings manually.

If you modify the settings manually, the name of the security level will change to **Custom**.

➤ *To restore the default scan settings:*

1. Open the application settings window.
2. In the left part of the window, in the **Scan** section, select the desired task (**Full Scan**, **Critical Areas Scan**, or **Custom Scan**).
3. In the **Security level** section, click the **Default level** button for the task selected.

## CREATING THE SCAN STARTUP SCHEDULE

You can create a schedule to automatically start virus scan tasks: specify task run frequency, start time (if necessary), and advanced settings.

If it is not possible to start the task for any reason (for example, the computer was not on at that time), you can configure the skipped task to start automatically as soon as it becomes possible. You can automatically pause the scan when a screensaver is inactive or the computer is unlocked. This functionality postpones launching the task until the user has finished working on the computer. The scan will then not take up system resources during work.

The special Idle Scan mode (see section "Running tasks in background mode" on page [107](#)) allows you to start automatic updates when your computer is idle.

➤ *To modify the schedule for scan tasks:*

1. Open the application settings window.
2. In the left part of the window, in the **Scan** section, select the desired task (**Full Scan**, **Critical Areas Scan**, or **Vulnerability Scan**).
3. Click the **Run mode** button in the right part of the window.
4. In the window that opens, on the **Run mode** tab, in the **Schedule** section, select **By schedule** and configure the scan run mode by specifying required values for the **Frequency** setting.

➤ *To enable automatic launching of a skipped task:*

1. Open the application settings window.
2. In the left part of the window, in the **Scan** section, select the desired task (**Full Scan**, **Critical Areas Scan** or **Vulnerability Scan**).
3. Click the **Run mode** button in the right part of the window.
4. In the window that opens, on the **Run mode** tab in the **Schedule** section, select **By schedule** and check the **Run skipped tasks** box.

➤ *To launch scans only when the computer is not being used:*

1. Open the application settings window.
2. In the left part of the window, in the **Scan** section, select the desired task (**Full Scan**, **Critical Areas Scan**, or **Vulnerability Scan**).
3. Click the **Run mode** button in the right part of the window.
4. In the window that opens, on the **Run mode** tab, in the **Schedule** section, select **By schedule** and check the **Run scheduled scan when screensaver is active or computer is locked** box.

## CREATING A LIST OF OBJECTS TO SCAN

Each virus scan task has its own default list of objects. These objects may include items in the computer's file system, such as logical drives and email databases, or other types of objects, such as network drives. You can edit this list.

If the scan scope is empty, or it contains no selected objects, a scan task cannot be started.

➤ To create a list of objects for a custom scan task:

1. Open the main application window.
2. In the bottom part of the window, select the **Scan** section.
3. In the bottom part of the window that opens, click the **specify** link to open a list of objects to be scanned.
4. In the **Custom Scan** window that opens, click the **Add** button.
5. In the **Select object to scan** window that opens, select the desired object and click the **Add** button. Click the **OK** button after you have added all the objects you need. To exclude any objects from the list of objects to be scanned, uncheck the boxes next to them.

You can also drag files to be scanned directly into a marked area located in the **Scan** section.

➤ To create a list of objects for Full Scan, Critical Areas Scan or Vulnerability Scan tasks:

1. Open the application settings window.
2. In the left part of the window, in the **Scan** section, select the desired scan task (**Full Scan**, **Critical Areas Scan**, or **Vulnerability Scan**).
3. In the right part of the window, click the **Scan scope** button.
4. In the **Scan scope** window that opens, use the **Add**, **Edit**, and **Delete** buttons to create a list. To exclude any objects from the list of objects to be scanned, uncheck the boxes next to them.

Objects which appear in the list by default cannot be edited or deleted.

## SELECTING A SCAN METHOD

During a virus scan, *signature analysis* is always used: Kaspersky Anti-Virus compares the object found with the database records.

You can use additional scan methods to increase scan efficiency: *heuristic analysis* (analysis of the actions an object performs within the system) and *rootkit scan* (a scan for tools that can hide malicious programs in your operating system).

➤ To select which scan method to use:

1. Open the application settings window.
2. In the left part of the window, in the **Scan** section, select the desired task (**Full Scan**, **Critical Areas Scan**, or **Custom Scan**).
3. In the **Security level** section, click the **Settings** button for the task selected.
4. In the window that opens, on the **Additional** tab in the **Scan methods** section, select the desired scan methods.

## SELECTING SCAN TECHNOLOGY

In addition to the scan methods you can use special object scan technologies which allow you to increase virus scan speed by excluding the files that have not been modified since they were last scanned.

➤ *To specify the object scan technologies:*

1. Open the application settings window.
2. In the left part of the window, in the **Scan** section, select the desired task (**Full Scan**, **Critical Areas Scan**, or **Custom Scan**).
3. In the **Security level** section, click the **Settings** button for the task selected.
4. In the window that opens, on the **Additional** tab in the **Scan technologies** section, select the desired values.

## CHANGING THE ACTIONS TO BE PERFORMED WHEN A THREAT IS DETECTED

If infected objects are detected, the application performs the selected action.

➤ *To change the action that should be performed when a threat is detected:*

1. Open the application settings window.
2. In the left part of the window, in the **Scan** section, select the desired task (**Full Scan**, **Critical Areas Scan**, or **Custom Scan**).
3. In the right part of the window, select the desired option in the **Action on threat detection** section.

## RUNNING A SCAN UNDER A DIFFERENT USER ACCOUNT

By default, the scan tasks are run under your system account. However, you may need to run a task under a different user account. You can specify an account to be used by the application when performing a scan task.

➤ *To start a scan under a different user's account:*

1. Open the application settings window.
2. In the left part of the window, in the **Scan** section, select the desired task (**Full Scan**, **Critical Areas Scan**, or **Vulnerability Scan**).
3. Click the **Run mode** button in the right part of the window.
4. In the window that opens, on the **Run mode** tab in the **User account** section, check the **Run task as** box. Specify the user name and password.

## CHANGING THE TYPE OF OBJECTS TO SCAN

When specifying the type of objects to scan, you establish which file formats will be scanned for viruses when the selected scan task runs.

When selecting file types, please remember the following:

- The probability of malicious code penetrating some file formats (such as TXT) and its subsequent activation is quite low. However, there are formats that contain or may contain an executable code (such as EXE, DLL, DOC). The risk of penetration and activation of malicious code in such files is quite high.
- An intruder can send a virus to your computer in an executable file renamed as a TXT file. If you have selected scanning of files by extension, such a file is skipped by the scan. If scanning of files by format is selected, then, regardless of the extension, File Anti-Virus will analyze the file header and reveal that the file is an EXE file. Such a file would be thoroughly scanned for viruses.

➤ *To change the type of objects to be scanned:*

1. Open the application settings window.
2. In the left part of the window, in the **Scan** section, select the desired task (**Full Scan**, **Critical Areas Scan**, or **Custom Scan**).
3. In the **Security level** section, click the **Settings** button for the task selected.
4. In the window that opens, on the **Scope** tab in the **File types** section, select the desired option.

## SCANNING OF COMPOUND FILES

A common method of concealing viruses is to embed them into compound files: archives, installation packages, embedded OLE objects, and mail file formats. To detect viruses that are hidden in this way, a compound file should be unpacked, which can significantly decrease scanning speed.

For each type of compound file, you can choose to scan either all files or only new ones. To make your selection, click the link next to the name of the object. It changes its value when you left-click it. If you select the scan new and changed files only mode (see page [70](#)), the links for choosing whether to scan all or only new files will not be available.

You can restrict the maximum size of a compound file to be scanned. Compound files larger than the specified value will not be scanned.

When large files are extracted from archives, they will be scanned even if the **Do not unpack large compound files** box is checked.

➤ *To modify the list of compound files to be scanned:*

1. Open the application settings window.
2. In the left part of the window, in the **Scan** section, select the desired task (**Full Scan**, **Critical Areas Scan**, or **Custom Scan**).
3. In the **Security level** section, click the **Settings** button for the task selected.
4. In the window that opens, on the **Scope** tab in the **Scan of compound files** section, select the desired types of compound files to be scanned.

➤ *To set the maximum size of compound files to be scanned:*

1. Open the application settings window.
2. In the left part of the window, in the **Scan** section, select the desired task (**Full Scan**, **Critical Areas Scan**, or **Custom Scan**).
3. In the **Security level** section, click the **Settings** button for the task selected.
4. In the window that opens, on the **Scope** tab in the **Scan of compound files** section, click the **Additional** button.
5. In the **Compound files** window that opens, check the **Do not unpack large compound files** box and specify the maximum file size.

## SCAN OPTIMIZATION

You can shorten the scan time and speed up Kaspersky Anti-Virus. This can be achieved by scanning only new files and those files that have altered since the last time they were scanned. This mode applies both to simple and compound files.

You can also set a restriction on scan duration for any one object. When the specified time interval expires, the object will be excluded from the current scan (except for archives and files comprised of several objects).

➤ *To scan only new and changed files:*

1. Open the application settings window.
2. In the left part of the window, in the **Scan** section, select the desired task (**Full Scan**, **Critical Areas Scan**, or **Custom Scan**).
3. In the **Security level** section, click the **Settings** button for the task selected.
4. In the window that opens, on the **Scope** tab in the **Scan optimization** section, check the **Scan only new and changed files** box.

➤ *To set a restriction on scan duration:*

1. Open the application settings window.
2. In the left part of the window, in the **Scan** section, select the desired task (**Full Scan**, **Critical Areas Scan**, or **Custom Scan**).
3. In the **Security level** section, click the **Settings** button for the task selected.
4. In the window that opens, on the **Scope** tab in the **Scan optimization** section, check the **Skip objects scanned longer than** box and specify the scan duration for a single file.

## SCANNING REMOVABLE DRIVES ON CONNECTION

Nowadays, malicious objects which use operating systems' vulnerabilities to replicate via networks and removable media have become increasingly widespread. Kaspersky Anti-Virus allows you to scan removable drives when connecting them to the computer.

➤ *To configure scanning of removable media on connection:*

1. Open the application settings window.
2. In the left part of the window, in the **Scan** section, select **General Settings**.
3. In the **Scan removable drives on connection** section, select the action and define the maximum size of a drive to be scanned in the field below, if necessary.

## CREATING A TASK SHORTCUT

The application provides the option of creating shortcuts for the full, quick, and vulnerability scan tasks. This allows you to start the required scan without opening the main application window or a context menu.

➤ *To create a shortcut to start a scan:*

1. Open the application settings window.
2. In the left part of the window, in the **Scan** section, select **General Settings**.
3. In the right part of the window, in the **Scan tasks quick run** section, click the **Create shortcut** button next to the name of the desired task (**Critical Areas Scan**, **Full Scan**, or **Vulnerability Scan**).
4. Specify the path for saving the shortcut and its name in the window that opens. By default, the shortcut is created with the name of the task in the My Computer folder of the current computer user.

## VULNERABILITY SCAN

Vulnerabilities may appear in the operating system, for example, due to programming errors, insecure passwords, or actions of malicious programs. When performing the vulnerability scan, the application refers to various security procedures, for example, examining the system, analyzing the settings of the operating system and the browser, and searching for vulnerable services.

The diagnostics may take some time. When it is complete, detected problems are analyzed from the standpoint of the danger they pose to the system.

After the vulnerability scan task is started (see page [47](#)), its run progress is displayed in the **Scan** window (in the **Vulnerability Scan** section) and in the Task Manager (see section "Managing scan tasks. Task Manager" on page [72](#)).

Information about results of the vulnerability scan task run is recorded in a report of Kaspersky Anti-Virus (see page [117](#)).

As with virus scan tasks, you can set a startup schedule for a vulnerability scan task, create a list of objects to scan (see page [67](#)), specify an account (see section "Running a scan under a different user account" on page [69](#)) and create a shortcut for quick start of the task. By default, the applications already installed on the computer are selected as scan objects.

## MANAGING SCAN TASKS. TASK MANAGER

Task Manager displays information about last scan tasks that have been run or that are currently running (for example, virus scan, vulnerability scan, rootkit scan, or advanced disinfection).

You can use Task Manager to view the progress and the result of a task run, or stop a task. For some tasks, additional actions are also available (for example, on completion of vulnerability scan, you can open the list of detected vulnerabilities and fix them).

➔ *To open Task Manager:*

1. Open the main application window.
2. In the bottom part of the window, select the **Scan** section.
3. In the **Scan** window that opens, click the **Manage Tasks** button in the top right corner of the window.

## UPDATE

Updating the databases and program modules of Kaspersky Anti-Virus ensures up-to-date protection for your computer. New viruses, Trojans, and other types of malware appear worldwide on a daily basis. Information about threats and ways of neutralizing them is provided by Kaspersky Anti-Virus databases. For timely detection of new threats, you should update databases and application modules on a regular basis.

Regular updates require an active license for application usage. If no license is installed, you can perform an update only once.

When performing an update, the application downloads and installs the following objects on your computer:

- Kaspersky Anti-Virus databases.

Protection of information is ensured by databases containing threat signatures, descriptions of network attacks, and information about how to resist them. Protection components use this information to search for and disinfect dangerous objects on your computer. The databases are supplemented every hour with records of new threats and ways to fight them. Therefore, you are strongly advised to update databases on a regular basis.

In addition to the Kaspersky Anti-Virus databases, the network drivers that enable the application's components to intercept network traffic are updated.

- Application modules.

In addition to the Kaspersky Anti-Virus databases, you can also update the program modules. The updates for the application modules fix Kaspersky Anti-Virus vulnerabilities and supplement or improve the existing functionality.

During an update, the application modules and databases on your computer are compared with the up-to-date version at the update source. If your current databases and application modules differ from those in the current version of the application, the missing portion of the updates will be installed on your computer.

If the databases are outdated, the update package may be large, which may cause additional Internet traffic (up to several dozen MB).

Prior to updating the databases, Kaspersky Anti-Virus creates backup copies of them in case you want to return to the previous version of the databases (see section "Rolling back the last update" on page 76).

Information about the current condition of Kaspersky Anti-Virus databases is displayed in the **Update** section of the main application window.

Information on the update results and events which occurred during the execution of the update task is logged in a Kaspersky Anti-Virus report (see page 117).

You can select an update source (see section "Selecting an update source" on page 73) and configure the automatic update startup.

**IN THIS SECTION:**

Selecting an update source .....	<a href="#">73</a>
Creating the update startup schedule .....	<a href="#">75</a>
Rolling back the last update .....	<a href="#">76</a>
Running updates under a different user account.....	<a href="#">76</a>
Using a proxy server .....	<a href="#">76</a>

**SELECTING AN UPDATE SOURCE**

An *update source* is a resource containing updates for databases and application modules of Kaspersky Anti-Virus.

The main update sources are the Kaspersky Lab update servers, where database updates and application module updates for all Kaspersky Lab products are stored.

Your computer should be connected to the Internet for successful downloading of updates from our servers. By default, the Internet connection settings are determined automatically. If you use a proxy server, you may need to adjust the connection settings (see section "Configuring the proxy server" on page 102).

When updating Kaspersky Anti-Virus, you can copy database and program module updates received from Kaspersky Lab servers into a local folder (see section "Updating the application from a shared folder" on page 74) and then provide access to other networked computers. This saves Internet traffic.

If you do not have access to Kaspersky Lab's update servers (for example, Internet access is restricted), you can call the Kaspersky Lab headquarters (<http://www.kaspersky.com/contacts>) to request the contact information of Kaspersky Lab partners who can provide you with updates on removable media.

When ordering updates on removable media, please specify whether you also require updates for the application modules.

## ADDING AN UPDATE SOURCE

By default, the list of update sources contains only Kaspersky Lab's update servers. You can add a local folder or a different server as update source. If several resources are selected as update sources, Kaspersky Anti-Virus tries to connect to them one after another, starting from the top of the list, and retrieves updates from the first available source.

➤ *To add an update source:*

1. Open the application settings window.
2. In the left part of the window, in the **Update** section, select the **Update Settings** component.
3. Click the **Update source** button in the right part of the window.
4. In the window that opens, on the **Source** tab, open the selection window by clicking the **Add** button.
5. In the **Select update source** window that opens, select the folder that contains the updates, or enter an address in the **Source** field to specify the server from which the updates should be downloaded.

## SELECTING THE UPDATE SERVER REGION

If you use Kaspersky Lab servers as the update source, you can select the optimal server location when downloading updates. Kaspersky Lab servers are located in several countries.

Using the closest Kaspersky Lab update server allows you to reduce the time required for receiving updates and increase operation performance speed. By default, the application uses information about the current region from the operating system's registry. You can select the region manually.

➤ *To select the server region:*

1. Open the application settings window.
2. In the left part of the window, in the **Update** section, select the **Update Settings** component.
3. Click the **Update source** button in the right part of the window.
4. In the window that opens, on the **Source** tab in the **Regional settings** section, select the **Select from the list** option, and then select the country nearest to your current location from the dropdown list.

## UPDATING THE APPLICATION FROM A SHARED FOLDER

To save Internet traffic, you can configure updates of Kaspersky Anti-Virus from a shared folder when updating the application on networked computers. If you do this, one of the networked computers receives an update package from Kaspersky Lab servers or from another web resource that contains the required set of updates. The updates received are copied into a shared folder. Other networked computers access this folder to receive updates for Kaspersky Anti-Virus.

When logged on under a guest account in Microsoft Windows 7, updates are not copied into the shared folder. It is recommended that you log on under a different account in order to allow copying updates.

➤ *To enable update distribution mode:*

1. Open the application settings window.
2. In the left part of the window, in the **Update** section, select the **Update Settings** component.
3. Check the **Copy updates to folder** box in the **Additional** section and specify the path to a public folder where all downloaded updates will be copied in the field below. You can also select a folder by clicking the **Browse** button.

➤ *To download updates for your computer from a specified shared folder:*

1. Open the application settings window.
2. In the left part of the window, in the **Update** section, select the **Update Settings** component.
3. Click the **Update source** button in the right part of the window.
4. In the window that opens, on the **Source** tab, open the selection window by clicking the **Add** button.
5. In the **Select update source** window that opens, select a folder or enter the full path to it in the **Source** field.
6. On the **Source** tab uncheck the **Kaspersky Lab update servers** box.

## CREATING THE UPDATE STARTUP SCHEDULE

You can create a schedule to automatically start an update task: specify the frequency, start time (if necessary), and advanced settings.

If it is not possible to start the task for any reason (for example, the computer was not on at that time), you can configure the skipped task to start automatically as soon as it becomes possible.

You can also postpone automatic startup of the task after the application is started. Note that all scheduled tasks will be run only after a specified time interval elapses from the startup of Kaspersky Anti-Virus.

The special Idle Scan mode (see section "Running tasks in background mode" on page [107](#)) allows you to start automatic updates when your computer is idle.

➤ *To configure the update task startup schedule:*

1. Open the application settings window.
2. In the left part of the window, in the **Update** section, select the **Update Settings** component.
3. Click the **Run mode** button in the right part of the window.
4. In the window that opens, on the **Run mode** tab in the **Schedule** section, select the **By schedule** option and configure the update run mode.

➤ *To enable automatic launching of a skipped task:*

1. Open the application settings window.
2. In the left part of the window, in the **Update** section, select the **Update Settings** component.
3. Click the **Run mode** button in the right part of the window.
4. In the window that opens, on the **Run mode** tab in the **Schedule** section, select **By schedule** and check the **Run skipped tasks** box.

➤ *To postpone running a task after application startup:*

1. Open the application settings window.
2. In the left part of the window, in the **Update** section, select the **Update Settings** component.
3. Click the **Run mode** button in the right part of the window.
4. In the window that opens, on the **Run mode** tab in the **Schedule** section, select the **By schedule** option and fill in the **Postpone running after application startup for** field to specify how long the task run should be postponed.


## ROLLING BACK THE LAST UPDATE

After the first update of Kaspersky Anti-Virus, the option of rolling back to the previous databases becomes available.

The update rollback feature is useful in case a new database version contains an invalid signature that makes Kaspersky Anti-Virus block a safe application.

In the event of damage done to Kaspersky Anti-Virus databases, it is recommended that you run the update task to download the up-to-date set of databases.

➔ *To roll back to the previous database version:*

1. Open the main application window.
2. Select the **Update** section in the lower part of the window.
3. In the **Update** window that opens, click the  button and select **Roll back to the previous databases** from the menu that opens.

## RUNNING UPDATES UNDER A DIFFERENT USER ACCOUNT

By default, the update procedure is run under your system account. However, Kaspersky Anti-Virus can update from a source for which you have no access rights (for example, from a network folder containing updates) or authorized proxy user credentials. You can run Kaspersky Anti-Virus updates on behalf of a user account that has such rights.

➔ *To start the update under a different user's account:*

1. Open the application settings window.
2. In the left part of the window, in the **Update** section, select the **Update Settings** component.
3. Click the **Run mode** button in the right part of the window.
4. In the window that opens, on the **Run mode** tab in the **User account** section, check the **Run task as** box. Specify the user name and password.

## USING A PROXY SERVER

If you use a proxy server for Internet connection, you should reconfigure it to allow proper updating of Kaspersky Anti-Virus.

➔ *To configure the proxy server:*

1. Open the application settings window.
2. In the left part of the window, in the **Update** section, select the **Update Settings** component.
3. Click the **Update source** button in the right part of the window.
4. In the window that opens, on the **Source** tab, click the **Proxy server** button.
5. Configure the proxy server settings in the **Proxy server settings** window that opens.

## FILE ANTI-VIRUS

File Anti-Virus prevents infection of the computer's file system. The component launches at the startup of the operating system, remains in the RAM of the computer, and scans all files opened, saved, or run on your computer and on all connected drives for viruses and other riskware.

You can create a protection scope and set a security level (a collection of settings that determine the scan's thoroughness).

When the user or a program attempts to access a protected file, File Anti-Virus checks whether iChecker and iSwift databases contain information about this file, and makes a decision on whether the file should be scanned.

By default, the *signature analysis* – a mode that uses records from application databases to search for threats – is always enabled. You can also enable heuristic analysis and various scan technologies.

If a threat is detected in a file, Kaspersky Anti-Virus assigns one of the following statuses to the file:

- Status designating the type of the malicious program detected (for example, *virus*, *Trojan*).
- *Potentially infected* (suspicious) status if the scan cannot determine whether the file is infected or not. The file may contain a code sequence typical of viruses and other malware, or the modified code of a known virus.

After that, the application displays a notification (see page [122](#)) of the detected threat on the screen and performs the action specified in the File Anti-Virus settings. You can change the action (see page [81](#)) that the application should perform if a threat is detected.

If you are working in automatic mode (see section "Selecting a protection mode" on page [63](#)), when dangerous objects are detected, Kaspersky Anti-Virus automatically applies the actions recommended by Kaspersky Lab specialists. For malicious objects, this action is **Disinfect. Delete if disinfection fails**, for suspicious objects – **Move to Quarantine**. If dangerous objects are detected when working in interactive mode (see section "Selecting a protection mode" on page [63](#)), the application displays a notification on the screen that you can use to select the required action the list of available ones.

Before attempting to disinfect or delete an infected object, Kaspersky Anti-Virus creates a backup copy for subsequent restoration or disinfection. Suspicious (potentially infected) objects are quarantined. You can enable automatic scanning of quarantined objects after each update.

### IN THIS SECTION:

Enabling and disabling File Anti-Virus .....	<a href="#">78</a>
Automatically pausing File Anti-Virus .....	<a href="#">78</a>
Creating the protection scope of File Anti-Virus .....	<a href="#">78</a>
Changing and restoring the file security level .....	<a href="#">80</a>
Selecting file scan mode .....	<a href="#">80</a>
Using heuristic analysis when working with File Anti-Virus .....	<a href="#">80</a>
Selecting file scan technology .....	<a href="#">81</a>
Changing the action to take on infected files .....	<a href="#">81</a>
Scan of compound files by File Anti-Virus .....	<a href="#">81</a>
Optimizing file scan .....	<a href="#">82</a>

## ENABLING AND DISABLING FILE ANTI-VIRUS

By default, File Anti-Virus is enabled, running in a mode recommended by Kaspersky Lab specialists. You can disable File Anti-Virus if necessary.

➤ *To disable File Anti-Virus:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.
3. In the right part of the window, uncheck the **Enable File Anti-Virus** box.

## AUTOMATICALLY PAUSING FILE ANTI-VIRUS

When doing resource-intensive work, you can pause File Anti-Virus. To reduce workload and ensure quick access to objects, you can configure automatic pausing of the component at a specified time or when handling specified programs.

Pausing File Anti-Virus in case of a conflict with some applications is an emergency measure. If any conflicts arise when working with the component, please contact Kaspersky Lab Technical Support Service (<http://support.kaspersky.com>). The support specialists will help you resolve the simultaneous operation of Kaspersky Anti-Virus with other applications on your computer.

➤ *To pause the component at a specified time:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.
3. In the **Security level** section in the right part of the window click the **Settings** button.
4. In the window that opens, on the **Additional** tab in the **Pause task** section, check the **By schedule** box and click the **Schedule** button.
5. In the **Pause task** window, specify the time (in 24-hour hh:mm format) for which protection will be paused (the **Pause task at** and **Resume task at** fields).

➤ *To pause the component when running specified applications:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.
3. In the **Security level** section in the right part of the window click the **Settings** button.
4. In the window that opens, on the **Additional** tab in the **Pause task** section, check the **At application startup** box and click the **Select** button.
5. In the **Applications** window, create a list of applications which pause the component when running.

## CREATING THE PROTECTION SCOPE OF FILE ANTI-VIRUS

The protection scope implies the location and type of files being scanned. By default, Kaspersky Anti-Virus scans only potentially infectable files stored on any hard drive, network drive or removable media.

➤ *To create the protection scope:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.
3. Click the **Settings** button in the right part of the window.
4. In the window that opens, on the **General** tab, in the **File types** section, specify the type of files that you want to be scanned by File Anti-Virus:
  - If you want to scan all files, select **All files**.
  - If you want to scan files of formats that are the most vulnerable to infection, select **Files scanned by format**.
  - If you want to scan files with extensions that are the most vulnerable to infection, select **Files scanned by extension**.

When selecting type of files to be scanned, you should note that:

- The probability of malicious code penetrating some file formats (such as TXT) and its subsequent activation is quite low. However, there are formats that contain or may contain an executable code (such as EXE, DLL, DOC). The risk of penetration and activation of malicious code in such files is quite high.
  - A hacker may send a virus or other riskware to your computer within an executable file renamed as one with the TXT extension. If you have selected scanning files by extension, such a file is skipped by the scan. If scanning of files by format is selected, then, regardless of the extension, File Anti-Virus will analyze the file header and reveal that the file is an EXE file. Such file is thoroughly scanned for viruses and other riskware.
5. In the **Protection scope** list, perform one of the following actions:
    - If you want to add a new object to the list of objects to be scanned, click the **Add** link.
    - If you want to change an object's location, select one from the list and click the **Edit** link.

The **Select object to scan** window opens.

- If you want to delete an object from the list of objects to be scanned, select one from the list and click the **Delete** link.
- The deletion confirmation window opens.
6. Perform one of the following actions:
    - If you want to add a new object to the list of objects to be scanned, select one in the **Select object to scan** window and click the **OK** button.
    - If you want to change an object's location, edit the path to one in the **Object** field in the **Select object to scan** window and click the **OK** button.
    - If you want to delete an object from the list of objects to be scanned, click the **Yes** button in the deletion confirmation window.
  7. If necessary, repeat steps 6 – 7 to add, relocate, or delete objects from the list of objects to be scanned.
  8. To exclude an object from the list of objects to be scanned, uncheck the box next to one in the **Protection scope** list. However, the object remains on the list of objects to be scanned, though it is excluded from the scan by File Anti-Virus.

## CHANGING AND RESTORING THE FILE SECURITY LEVEL

Depending on your current needs, you can select one of the preset file/memory security levels or configure File Anti-Virus on your own.

When configuring File Anti-Virus, you can always restore the recommended values. These settings are considered optimal, recommended by Kaspersky Lab, and grouped in the **Recommended** security level.

➤ *To change the file security level:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.
3. In the right part of the window, in the **Security level** section, set the desired security level, or click the **Settings** button to modify the settings manually.

If you modify the settings manually, the name of the security level will change to **Custom**.

➤ *To restore the default file security level:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.
3. Click the **Default level** button in the **Security level** section in the right part of the window.

## SELECTING FILE SCAN MODE

A *scan mode* means a condition, under which File Anti-Virus starts scanning files. By default, Kaspersky Anti-Virus runs in smart mode. When running in this file scan mode, File Anti-Virus makes decisions on file scan based on the analysis of actions that the user takes on files, and on the type of those files. For example, when working with a Microsoft Office document, Kaspersky Anti-Virus scans the file when it is first opened and last closed. Intermediate operations that overwrite the file do not cause it to be scanned.

➤ *To change the files scan mode:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.
3. In the **Security level** section in the right part of the window click the **Settings** button.
4. In the window that opens, on the **Additional** tab in the **Scan mode** section, select the desired mode.

When selecting scan mode, you should take account of the types of files, with which you have to work with the majority of time.

## USING HEURISTIC ANALYSIS WHEN WORKING WITH FILE ANTI-VIRUS

During File Anti-Virus operation, *signature analysis* is always used: Kaspersky Anti-Virus compares the object found with the database records.

To improve protection efficiency, you can use *heuristic analysis* (i.e., analysis of activity that an object performs in the system). This analysis makes it possible to detect new malicious objects which are not yet described in the databases.

➤ *To enable heuristic analysis:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.
3. In the **Security level** section in the right part of the window click the **Settings** button.
4. In the window that opens, on the **Performance** tab in the **Scan methods** section, check the **Heuristic Analysis** box and specify the detail level for the scan.

## SELECTING FILE SCAN TECHNOLOGY

In addition to the heuristic analysis, you can involve specific technologies that allow optimizing the file scan performance due to excluding files from scan if they have not been modified since the last scan.

➤ *To specify the object scan technologies:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.
3. In the **Security level** section in the right part of the window click the **Settings** button.
4. In the window that opens, on the **Additional** tab in the **Scan technologies** section, select the desired values.

## CHANGING THE ACTION TO TAKE ON INFECTED FILES

If infected objects are detected, the application performs the selected action.

➤ *To change the action that should be taken on infected objects:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.
3. In the right part of the window, select the desired option in the **Action on threat detection** section.

## SCAN OF COMPOUND FILES BY FILE ANTI-VIRUS

A common method of concealing viruses is to embed them into compound files: archives, installation packages, embedded OLE objects, and mail file formats. To detect viruses that are hidden in this way, a compound file should be unpacked, which can significantly decrease scanning speed.

For each type of compound file, you can choose to scan either all files or only new ones. To make your selection, click the link next to the name of the object. It changes its value when you left-click it. If you select the scan new and changed files only mode, the links for choosing whether to scan all or only new files will not be available.

By default, Kaspersky Anti-Virus scans only embedded OLE objects.

When large compound files are scanned, their preliminary unpacking may take a long time. This period can be reduced by enabling unpacking of compound files in background mode if they exceed the specified file size. If a malicious object is detected while working with such a file, the application will notify you about it.

You can restrict the maximum size of a compound file to be scanned. Compound files larger than the specified value will not be scanned.

When large files are extracted from archives, they will be scanned even if the **Do not unpack large compound files** box is checked.

➤ *To modify the list of compound files to be scanned:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.
3. In the **Security level** section in the right part of the window click the **Settings** button.
4. In the window that opens, on the **Performance** tab in the **Scan of compound files** section, select the desired type of compound files to be scanned.

➤ *To set the maximum size of compound files to be scanned:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.
3. In the **Security level** section in the right part of the window click the **Settings** button.
4. In the window that opens, on the **Performance** tab in the **Scan of compound files** section, click the **Additional** button.
5. In the **Compound files** window, check the **Do not unpack large compound files** box and specify the maximum file size.

➤ *To unpack large compound files in background mode:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.
3. In the **Security level** section in the right part of the window click the **Settings** button.
4. In the window that opens, on the **Performance** tab in the **Scan of compound files** section, click the **Additional** button.
5. In the **Compound files** window, check the **Extract compound files in the background** box and specify the minimum file size.

## OPTIMIZING FILE SCAN


You can shorten the scan time and speed up Kaspersky Anti-Virus. This can be achieved by scanning only new files and those files that have altered since the last time they were scanned. This mode applies both to simple and compound files.

➤ *To scan only new and changed files:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **File Anti-Virus** component.
3. Click the **Settings** button in the right part of the window.
4. In the window that opens, on the **Performance** tab in the **Scan optimization** section, check the **Scan only new and changed files** box.

## MAIL ANTI-VIRUS

Mail Anti-Virus scans incoming and outgoing messages for malicious objects. It starts when the operating system launches and runs continually, scanning all email messages sent or received via the POP3, SMTP, IMAP, MAPI and NNTP protocols, as well as over secure connections (SSL) via POP3 and IMAP (see section "Encrypted connections scan" on page [100](#)).

The indicator of the component's operation is the application icon in the taskbar notification area, which looks like  whenever an email message is being scanned.

Mail Anti-Virus intercepts and scans each email message received or sent by the user. If no threats are detected in an email message, it becomes available for the user.

You can specify the types of messages which should be scanned and select the security level (see page [85](#)) (configuration settings affecting the scan intensity).

By default, the *signature analysis* – a mode that uses records from application databases to search for threats – is always enabled. In addition, you can enable heuristic analysis. Furthermore, you can enable filtering of attachments (see page [86](#)), which allows automatic renaming or deletion of specified file types.

If a threat is detected in a file, Kaspersky Anti-Virus assigns one of the following statuses to the file:

- Status designating the type of the malicious program detected (for example, *virus*, *Trojan*).
- *Potentially infected* (suspicious) status if the scan cannot determine whether the file is infected or not. The file may contain a code sequence typical of viruses and other malware, or the modified code of a known virus.

After that, the application blocks the email message, displays a notification (see page [122](#)) of the detected threat on the screen, and performs the action specified in the settings of Mail Anti-Virus. You can change the actions to be taken when a threat is detected (see section "Changing the action to take on infected email messages" on page [86](#)).

If you are working in automatic mode (see section "Selecting a protection mode" on page [63](#)), when dangerous objects are detected, Kaspersky Anti-Virus automatically applies the actions recommended by Kaspersky Lab specialists. For malicious objects, this action is **Disinfect. Delete if disinfection fails**, for suspicious objects – **Move to Quarantine**. If dangerous objects are detected when working in interactive mode (see section "Selecting a protection mode" on page [63](#)), the application displays a notification on the screen that you can use to select the required action the list of available ones.

Before attempting to disinfect or delete an infected object, Kaspersky Anti-Virus creates a backup copy for subsequent restoration or disinfection. Suspicious (potentially infected) objects are quarantined. You can enable automatic scanning of quarantined objects after each update.

If disinfection is successful, the email message becomes available. If the disinfection fails, the infected object is deleted from the email message. Mail Anti-Virus expands the subject of the email message by adding text that notifies the user that this email message has been processed by Kaspersky Anti-Virus.

An integrated plug-in is provided for Microsoft Office Outlook that allows you to fine-tune the email client.

If you use The Bat!, Kaspersky Anti-Virus can be used in conjunction with other anti-virus applications. At that, the email traffic processing rules are configured directly in The Bat! and have a higher priority than the mail protection settings of Kaspersky Anti-Virus.

When working with other widespread mail clients, including Microsoft Outlook Express/Windows Mail, Mozilla Thunderbird, Eudora, and Incredimail, Mail Anti-Virus scans email on the SMTP, POP3, IMAP, and NNTP protocols.

**Note that when working with the Thunderbird mail client, email messages transferred via IMAP will not be scanned for viruses if any filters moving messages from the **Inbox** folder are used.**

**IN THIS SECTION:**

Enabling and disabling Mail Anti-Virus .....	<a href="#">84</a>
Creating the protection scope of Mail Anti-Virus .....	<a href="#">84</a>
Changing and restoring the email security level.....	<a href="#">85</a>
Using heuristic analysis when working with Mail Anti-Virus.....	<a href="#">85</a>
Changing the action to take on infected email messages .....	<a href="#">86</a>
Filtering attachments in email messages .....	<a href="#">86</a>
Scan of compound files by Mail Anti-Virus .....	<a href="#">86</a>
Email scanning in Microsoft Office Outlook.....	<a href="#">87</a>
Email scanning in The Bat!.....	<a href="#">87</a>

## ENABLING AND DISABLING MAIL ANTI-VIRUS

By default, Mail Anti-Virus is enabled, running in a mode recommended by Kaspersky Lab specialists. You can disable Mail Anti-Virus if necessary.

➤ *To disable Mail Anti-Virus:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Mail Anti-Virus** component.
3. In the right part of the window, uncheck the **Enable Mail Anti-Virus** box.

## CREATING THE PROTECTION SCOPE OF MAIL ANTI-VIRUS

Protection scope comprises a type of email messages to be scanned, protocols with traffic scanned by Kaspersky Anti-Virus, and settings for integration of Mail Anti-Virus into the system.

By default, Kaspersky Anti-Virus is integrated into Microsoft Office Outlook and The Bat!, scans both incoming and outgoing email messages, and scans traffic of POP3, SMTP, NNTP and IMAP email protocols.

➤ *To disable scanning of outgoing emails:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Mail Anti-Virus** component.
3. Click the **Settings** button in the right part of the window.
4. Use the **General** tab in the **Protection scope** section of the displayed window to select the **Incoming messages only** option.

If you have selected scanning incoming messages only, it is recommended that you scan outgoing mail when first running Kaspersky Anti-Virus, since your computer may be infected with email worms that use your email to breed and spread. Scanning outgoing mail allows you to avoid problems occurring due to uncontrolled sending of email messages from your computer.

➤ To select the protocols to scan and the settings for integrating Mail Anti-Virus into the system:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Mail Anti-Virus** component.
3. Click the **Settings** button in the right part of the window.
4. In the window that opens, on the **Additional** tab in the **Connectivity** section, select the desired settings.

## CHANGING AND RESTORING THE EMAIL SECURITY LEVEL

Depending on your current needs, you can select one of the preset email security levels or configure Mail Anti-Virus on your own.

Kaspersky Lab advises you not to configure Mail Anti-Virus settings on your own. In most cases, it is sufficient to select a different security level.

When configuring Mail Anti-Virus, you can always restore the recommended values. These settings are considered optimal, recommended by Kaspersky Lab, and grouped in the **Recommended** security level.

➤ To change the current email security level:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Mail Anti-Virus** component.
3. In the right part of the window, in the **Security level** section, set the desired security level, or click the **Settings** button to modify the settings manually.

If you modify the settings manually, the name of the security level will change to **Custom**.

➤ To restore the default mail protection settings:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Mail Anti-Virus** component.
3. Click the **Default level** button in the **Security level** section in the right part of the window.

## USING HEURISTIC ANALYSIS WHEN WORKING WITH MAIL ANTI-VIRUS

During Mail Anti-Virus operation, *signature analysis* is always used: Kaspersky Anti-Virus compares the object found with the database records.

To improve protection efficiency, you can use *heuristic analysis* (i.e., analysis of activity that an object performs in the system). This analysis makes it possible to detect new malicious objects which are not yet described in the databases.

➤ To enable heuristic analysis:

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Mail Anti-Virus** component.

3. In the **Security level** section in the right part of the window click the **Settings** button.
4. In the window that opens, on the **General** tab in the **Scan methods** section, check the **Heuristic Analysis** box and specify the detail level for the scan.

## CHANGING THE ACTION TO TAKE ON INFECTED EMAIL MESSAGES

If infected objects are detected, the application performs the selected action.

➤ *To change the action that should be taken on infected email messages:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Mail Anti-Virus** component.
3. In the right part of the window, select the desired option in the **Action on threat detection** section.

## FILTERING ATTACHMENTS IN EMAIL MESSAGES

Malicious programs may spread via email as attachments in email messages. You can configure filtering by type of attachments in email messages, which allows the renaming or deleting files of specified types automatically.

➤ *To configure filtering of attachments:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Mail Anti-Virus** component.
3. Click the **Settings** button in the right part of the window.
4. Use the **Attachment filter** tab of the displayed window to select the filtering mode for attachments. When you select either of the last two modes, the list of file types (extensions) will be enabled; there you can select the desired types or add a new type mask.

To add a mask of a new type to the list, click the **Add** link to open the **Input file name mask** window and enter the required information.

## SCAN OF COMPOUND FILES BY MAIL ANTI-VIRUS

A common method of concealing viruses is to embed them into compound files: archives, installation packages, embedded OLE objects, and mail file formats. To detect viruses that are hidden in this way, a compound file should be unpacked, which can significantly decrease scanning speed.

You can enable or disable scanning of compound files, and limit the maximum size of compound files to be scanned.

*If your computer is not protected by any local network software (you access the Internet directly without a proxy server or a firewall), it is not recommended that you disable the scanning of compound files.*

➤ *To configure the scanning of compound files:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Mail Anti-Virus** component.

3. Click the **Settings** button in the right part of the window.
4. Use the **General** tab in the window that opens to define the necessary settings.

## EMAIL SCANNING IN MICROSOFT OFFICE OUTLOOK

While installing Kaspersky Anti-Virus, a special plug-in is integrated into Microsoft Office Outlook. It allows you to quickly switch to configuration of Mail Anti-Virus from Microsoft Office Outlook, and determine when email messages should be scanned for viruses and other riskware, whether this should be done when receiving, opening, or sending a message.

Configuration of Mail Anti-Virus from Microsoft Office Outlook is available if this option is selected in the protection scope settings of Mail Anti-Virus.

➤ *To switch to the email scan settings in Microsoft Office Outlook:*

1. Open the main Microsoft Office Outlook window.
2. Select **Tools** → **Options** from the application menu.
3. In the **Settings** window that opens, select the **Email protection** tab.

## EMAIL SCANNING IN THE BAT!

Actions with regard to infected email objects in The Bat! are defined using the application's own tools.

Mail Anti-Virus settings which determine whether incoming and outgoing messages should be scanned, which actions should be performed in regard to dangerous objects in email, and which exclusions should apply are ignored. The only thing that The Bat! takes into account is the scanning of attached archives.

The email protection settings extend to all the anti-virus components installed on the computer that support working with the Bat!.

Note that incoming email messages are first scanned by Mail Anti-Virus and only then by the plug-in for The Bat!. If a malicious object is detected, Kaspersky Anti-Virus immediately notifies you of this. If you select the **Disinfect (Delete)** action in the Mail Anti-Virus notification window, actions aimed at eliminating the threat are performed by Mail Anti-Virus. If you select the **Ignore** option in the notification window, the object will be disinfected by the plug-in for The Bat!. When sending email messages, they are first scanned by the plug-in and then by Mail Anti-Virus.

The settings of Mail Anti-Virus are available from The Bat! if this option is selected in the protection scope settings of Mail Anti-Virus.

To configure email scanning in The Bat! you must define the following criteria:

- which mail stream (incoming, outgoing) should be scanned;
- when mail objects should be scanned (when opening a message, before saving to disk);
- what actions are to be performed by the mail client if dangerous objects are detected in email messages. For example, you can select:
  - **Attempt to disinfect infected parts** – if this option is selected, the attempt is made to disinfect the infected object; if it cannot be disinfected, the object remains in the message.
  - **Delete infected parts** – if this option is selected, the dangerous object in the message is deleted regardless of whether it is infected or suspected to be infected.

By default, The Bat! places all infected email objects in Quarantine without attempting to disinfect them.

Email messages that contain dangerous objects are not marked with the special subject add-on when scanned by the plug-in for The Bat!.

➔ To switch to the email scan settings in The Bat!:

1. Open the main window of the The Bat!.
2. In the **Properties** menu, select **Settings**.
3. Select the **Virus protection** object from the settings tree.

## WEB ANTI-VIRUS

Each time you work on the Internet, you endanger information stored on your computer, by exposing it to a risk of being infected with viruses and other malware. They may penetrate your computer when you download free applications or view information on websites that had been attacked by hackers before you have visited them. Moreover, network worms may penetrate into your computer even before you open a web page or download a file, just at the moment your computer establishes an Internet connection.

Web Anti-Virus protects information received by your computer and sent from it over HTTP, HTTPS and FTP protocols, and prevents hazardous scripts from being run on your computer.

Web Anti-Virus only monitors web traffic transferred via ports specified on the list of monitored ports. A list of monitored ports that are most commonly used for data transfer, is included in the Kaspersky Anti-Virus distribution kit. If you use ports that are not included in the list of monitored ports, you should add them to the list of monitored ports (see section "Creating a list of monitored ports" on page [102](#)) to ensure protection of web traffic transferred via them.

Web Anti-Virus scans web traffic with regard for a specific collection of settings named security level. If Web Anti-Virus detects a threat, it will perform the prescribed action. Malicious objects are detected using both Kaspersky Anti-Virus databases and a heuristic algorithm.

Kaspersky Lab advises you not to configure Web Anti-Virus settings on your own. In most cases, it is sufficient to select an appropriate security level.

### Web traffic scan algorithm

Each web page or file that is accessed by the user or an application via the HTTP, HTTPS, or FTP protocols is intercepted and scanned for malicious code by Web Anti-Virus:

- If a web page or a file accessed by the user contains malicious code, access to it is blocked. A notification is displayed that the requested file or web page is infected.
- If the file or web page does not contain malicious code, the program immediately grants the user access to it.

### Script scan algorithm

Each script run is intercepted by Web Anti-Virus and is analyzed for malicious code:

- If a script contains malicious code, Web Anti-Virus blocks it and displays a notification on the screen.
- If no malicious code is discovered in the script, it is run.

Web Anti-Virus intercepts only scripts based on the Microsoft Windows Script Host functionality.

**IN THIS SECTION:**

Enabling and disabling Web Anti-Virus .....	<a href="#">89</a>
Changing and restoring the web traffic security level .....	<a href="#">89</a>
Changing the action to take on dangerous objects from web traffic .....	<a href="#">90</a>
Checking URLs on web pages .....	<a href="#">90</a>
Using heuristic analysis when working with Web Anti-Virus.....	<a href="#">92</a>
Blocking dangerous scripts .....	<a href="#">92</a>
Scan optimization.....	<a href="#">93</a>
Creating a list of trusted addresses.....	<a href="#">93</a>

**ENABLING AND DISABLING WEB ANTI-VIRUS**

By default, Web Anti-Virus is enabled, running in a mode recommended by Kaspersky Lab specialists. You can disable Web Anti-Virus, if necessary.

➤ *To disable Web Anti-Virus:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
3. In the right part of the window, uncheck the **Enable Web Anti-Virus** box.

**CHANGING AND RESTORING THE WEB TRAFFIC SECURITY LEVEL**

Depending on your current needs, you can select one of the preset web traffic security levels or configure Web Anti-Virus on your own.

When configuring Web Anti-Virus, you can always restore the recommended values. These settings are considered optimal, recommended by Kaspersky Lab, and grouped in the **Recommended** security level.

➤ *To change the web traffic security level:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
3. In the right part of the window, in the **Security level** section, set the desired security level, or click the **Settings** button to modify the settings manually.

If you modify the settings manually, the name of the security level will change to **Custom**.

➤ *To restore the default web traffic security level:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
3. Click the **Default level** button in the **Security level** section in the right part of the window.

## CHANGING THE ACTION TO TAKE ON DANGEROUS OBJECTS FROM WEB TRAFFIC

If infected objects are detected, the application performs the selected action.

Web Anti-Virus always blocks actions by dangerous scripts and displays messages that inform the user of the action taken. You cannot change the action to be taken on a dangerous script; all you can do is disable script scan (see section "Blocking dangerous scripts" on page [92](#)).

➔ *To change the action to be performed with regard to detected objects:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
3. In the right part of the window, select the desired option in the **Action on threat detection** section.

## CHECKING URLS ON WEB PAGES

Scanning web pages for phishing allows you to prevent *phishing attacks*. Phishing attacks are, as a rule, email messages from alleged financial organizations that contain URLs to websites of such organizations. The email message convinces the reader to click the URL and enter private information in the window that opens, for example, the number of a banking card or the login and the password of an online banking account. A phishing attack can be disguised, for example, as a letter from your bank with a link to its official website. By clicking the link, you go to an exact copy of the bank's website and can even see the bank site's address in the browser, even though you are on a counterfeit site. From this point forward, all your actions on the site are tracked and can be used to steal your money.

Since links to phishing web sites may be received not only in email, but also from other sources, such as ICQ messages, Web Anti-Virus monitors attempts to access a phishing web site on the level of web traffic and blocks access to such locations.

In addition to Kaspersky Anti-Virus databases, heuristic analysis (see page [92](#)) can also be used for scanning web pages for phishing.

### IN THIS SECTION:

---

Enabling and disabling the checking of URLs .....	<a href="#">90</a>
Using Kaspersky URL Advisor .....	<a href="#">91</a>

## ENABLING AND DISABLING THE CHECKING OF URLS

➔ *To enable URL checks using the databases of suspicious web addresses and phishing addresses:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
3. Click the **Settings** button in the right part of the window.

The **Web Anti-Virus** window opens.

4. On the **General** tab, in the **Kaspersky URL Advisor** section, check the **Check if URLs are listed in the database of suspicious URLs** and **Check web pages for phishing** boxes.

## USING KASPERSKY URL ADVISOR

Kaspersky URL Advisor is integrated into Microsoft Internet Explorer, Mozilla Firefox, and Google Chrome as a plug-in.

Kaspersky URL Advisor checks all URLs on a web page to find out if they are included in the list of suspicious URLs. It also checks them for phishing, highlighting each one in the browser window.

You can create a list of websites, on which all URLs should be checked, check URLs on all websites except those included in the list of exclusions, check URLs in search results only, or specify categories of websites with URLs that should be checked.

Not only can you configure Kaspersky URL Advisor in the application settings window, but also in the Kaspersky URL Advisor settings window, which is available from your web browser.

➤ *To specify websites, on which all URLs should be checked:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
3. Click the **Settings** button in the right part of the window.
4. The **Web Anti-Virus** window opens.
5. On the **Safe Surf** tab, in the **Kaspersky URL Advisor** section, check the **Check URLs** box.
6. Select the websites on which the links need to be scanned:
  - a. If you want to create a list of websites, on which all URLs should be checked, select **Only websites from the list** and click the **Specify** button. In the **Checked URLs** window that opens, create a list of websites to be checked.
  - b. If you want to check URLs on all websites except those specified, select **All but the exclusions** and click the **Exclusions** button. In the **Exclusions** window that opens, create a list of websites that do not need any check of URLs on them.

➤ *To check URLs in search results only:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
3. Click the **Settings** button in the right part of the window.
4. The **Web Anti-Virus** window opens.
5. On the **Safe Surf** tab, in the **Kaspersky URL Advisor** section, check the **Check URLs** box and click the **Settings** button.
6. In the **Kaspersky URL Advisor settings** window that opens, in the **Check mode** section, select **Only URLs in search results**.

➤ *To select categories of websites with URLs that should be checked:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
3. Click the **Settings** button in the right part of the window.
4. The **Web Anti-Virus** window opens.

5. On the **Safe Surf** tab, in the **Kaspersky URL Advisor** section, check the **Check URLs** box and click the **Settings** button.
  6. In the **Kaspersky URL Advisor settings** window that opens, in the **Websites categories** section, check the **Show information on the categories of websites content** box.
  7. In the list of categories, check the boxes next to categories of websites with URLs that should be checked.
- ➔ *To open the Kaspersky URL Advisor settings window from your web browser,*
- click the button with the Kaspersky Anti-Virus icon in the browser toolbar.

## USING HEURISTIC ANALYSIS WHEN WORKING WITH WEB ANTI-VIRUS

To improve protection efficiency, you can use *heuristic analysis* (i.e., analysis of activity that an object performs in the system). This analysis makes it possible to detect new malicious objects which are not yet described in the databases.

When Web Anti-Virus is running, you can separately enable the heuristic analysis for scanning web traffic and for checking web pages for phishing.

➔ *To enable the heuristic analysis for scanning web traffic:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
3. Click the **Settings** button in the right part of the window.

The **Web Anti-Virus** window opens.

4. On the **General** tab in the **Heuristic Analysis** section, check the **Use Heuristic Analysis** box and set a scan detail level.

➔ *To enable the heuristic analysis for checking web pages for phishing:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
3. Click the **Settings** button in the right part of the window.

The **Web Anti-Virus** window opens.

4. On the **General** tab, in the **Kaspersky URL Advisor** section, click the **Additional** button.
5. In the **Anti-Phishing settings** window that opens, check the **Use Heuristic Analysis to check web pages for phishing** box and set a scan detail level.

## BLOCKING DANGEROUS SCRIPTS

Web Anti-Virus scans all scripts processed in Microsoft Internet Explorer, as well as any other WSH scripts (for example, JavaScript, Visual Basic Script, etc.) launched when you are working on the computer. If a script presents a threat to your computer, it will be blocked.

➤ *To disable blocking of dangerous scripts:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
3. Click the **Settings** button in the right part of the window.

The **Web Anti-Virus** window opens.

4. On the **General** tab in the **Additional** section uncheck the **Block dangerous scripts in Microsoft Internet Explorer** box.

## SCAN OPTIMIZATION

To improve efficiency of detection of malicious code, Web Anti-Virus uses the caching of fragments of objects coming from the Internet. Using the caching, Web Anti-Virus scans objects only after they are received on the computer in their entirety.

The caching increases the amount of time required to process objects and pass it to the user for further operations. Caching can cause problems when downloading or processing large objects, as the connection with the HTTP client may time out.

You can solve this problem using the option of limiting the caching of fragments of objects coming from the Internet. Upon expiration of a certain time interval, each fragment of an object is passed to the user unscanned. When copying is complete, the object will be scanned entirely. This allows us to reduce the amount of time required to pass objects to the user and solving the problem with connection losses. The Internet security level is not reduced.

Lifting restrictions on the duration of web traffic caching leads to improved efficiency of virus scans, though it may slow down access to objects.

➤ *To set or remove a time limit for fragment buffering:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
3. Click the **Settings** button in the right part of the window.

The **Web Anti-Virus** window opens.

4. On the **General** tab, in the **Additional** section, check the **Limit traffic caching time to 1 sec to optimize scan** box.

## CREATING A LIST OF TRUSTED ADDRESSES

Web Anti-Virus does not scan web traffic for dangerous objects if it comes from trusted URLs.

➤ *To create a list of trusted web addresses:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Web Anti-Virus** component.
3. Click the **Settings** button in the right part of the window.

The **Web Anti-Virus** window opens.

4. On the **Trusted URLs** tab, check the **Do not scan web traffic from trusted URLs** box.

5. Create a list of websites / web pages with content that you trust. To do this:
  - a. Click the **Add** button.  
The **Address mask (URL)** window will open.
  - b. Enter the address of a website / web page or the address mask of a website / web page.
  - c. Click the **OK** button.  
A new record appears on the list of trusted URLs.
6. If necessary, repeat steps from a to c.

## IM ANTI-VIRUS

IM Anti-Virus scans the traffic of instant messaging clients (so-called *Internet pagers*).

IM messages may contain links to suspicious websites and to websites used by hackers to organize phishing attacks. Malicious programs use IM clients to send spam messages and links to programs (or the programs themselves) which steal users' ID numbers and passwords.

Kaspersky Anti-Virus ensures safe operation of various instant messaging applications, including ICQ, MSN, AIM, Yahoo! Messenger, Jabber, Google Talk, Mail.Ru Agent and IRC.

Some IM clients, such as Yahoo! Messenger and Google Talk, use encrypted connections. To scan the traffic generated by those programs, you have to enable encrypted connections scanning (see page [100](#)).

IM Anti-Virus intercepts messages and scans them for dangerous objects or URLs. You can select the types of messages to scan and various scanning methods.

If threats are detected in a message, IM Anti-Virus replaces this message with a warning message for the user.

Files transferred via IM clients are scanned by the File Anti-Virus component (on page [77](#)) when attempts are made to save them.

### IN THIS SECTION:

Enabling and disabling IM Anti-Virus.....	<a href="#">94</a>
Creating the protection scope of IM Anti-Virus.....	<a href="#">95</a>
Checking URLs in messages from IM clients.....	<a href="#">95</a>
Using heuristic analysis when working with IM Anti-Virus.....	<a href="#">95</a>

## ENABLING AND DISABLING IM ANTI-VIRUS

By default, IM Anti-Virus is enabled and functions in normal mode. You can disable IM Anti-Virus if necessary.

➔ *To disable IM Anti-Virus:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **IM Anti-Virus** component.
3. In the right part of the window, uncheck the **Enable IM Anti-Virus** box.

## CREATING THE PROTECTION SCOPE OF IM ANTI-VIRUS

The protection scope is the type of messages to be scanned. By default, Kaspersky Anti-Virus scans both incoming and outgoing messages. If you are sure that messages you send cannot contain any dangerous objects, you may disable scanning of outgoing traffic.

➤ *To disable scanning of outgoing messages:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **IM Anti-Virus** component.
3. In the right part of the window, in the **Protection scope** section, select the **Incoming messages only** option.

## CHECKING URLs IN MESSAGES FROM IM CLIENTS

➤ *To scan messages for suspicious and phishing URLs:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **IM Anti-Virus** component.
3. In the right part of the window, in the **Scan methods** section, check the **Check if URLs are listed in the database of suspicious URLs** and **Check if URLs are listed in the database of phishing URLs** boxes.

## USING HEURISTIC ANALYSIS WHEN WORKING WITH IM ANTI-VIRUS

To improve protection efficiency, you can use *heuristic analysis* (i.e., analysis of activity that an object performs in the system). This analysis makes it possible to detect new malicious objects which are not yet described in the databases.

When using heuristic analysis, any script included in an IM client's message is executed in a protected environment. If the script's activity is typical of malicious objects, the object is likely to be classed as malicious or suspicious. By default, heuristic analysis is enabled.

➤ *To enable heuristic analysis:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **IM Anti-Virus** component.
3. In the right part of the window, in the **Scan methods** section, check the **Heuristic Analysis** box and set the necessary scanning intensity level.

## PROACTIVE DEFENSE

Proactive Defense protects your computer against new threats which are not yet included in Kaspersky Anti-Virus databases.

The functioning of Proactive Defense is based on proactive technologies. Proactive technologies allow you to neutralize a new threat before it does any harm to your computer. Unlike responsive technologies, which analyze code based on records in Kaspersky Anti-Virus databases, preventative technologies recognize a new threat on your computer by the sequence of actions executed by a program. If, as a result of activity analysis, the sequence of an application's actions arouses suspicion, Kaspersky Anti-Virus blocks the activity of this application.

For example, when actions such as a program copying itself to network resources, the startup folder and the system registry are detected, it is highly likely that this program is a worm.

Hazardous sequences of actions also include attempts to modify the HOSTS file, hidden installation of drivers, etc. You can turn off monitoring (see page [97](#)) for any hazardous activity or edit its monitoring rules (see page [97](#)).

You can create a group of trusted applications (see page [96](#)) for Proactive Defense. You will not be notified of the activities of these applications.

If your computer runs under Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64, Microsoft Windows 7, or Microsoft Windows 7 x64, control will not apply to all events. This is due to specific features of these operating systems. For example, control will not apply fully to the sending of data through trusted applications and suspicious system activities.

**IN THIS SECTION:**

Enabling and disabling Proactive Defense .....	<a href="#">96</a>
Creating a group of trusted applications.....	<a href="#">96</a>
Using the dangerous activity list.....	<a href="#">97</a>
Changing the action to be taken on applications' dangerous activity .....	<a href="#">97</a>

## ENABLING AND DISABLING PROACTIVE DEFENSE

By default, Proactive Defense is enabled, running in a mode recommended by Kaspersky Lab specialists. You can disable Proactive Defense if necessary.

➤ *To disable Proactive Defense:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Proactive Defense** component.
3. In the right part of the window, uncheck the **Enable Proactive Defense** box.

## CREATING A GROUP OF TRUSTED APPLICATIONS

You can create a group of trusted applications exerting activity that should not be controlled by Proactive Defense. By default, the list of trusted applications includes applications with verified digital signatures and applications that are trusted in the Kaspersky Security Network database.

➤ *To change the settings of the trusted applications group:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Proactive Defense** component.
3. In the right part of the window, in the **Trusted applications** section, perform the following actions:
  - If you want applications with verified digital signatures to be included in the group of trusted applications, check the **Applications with digital signature** box.
  - If you want applications trusted by the Kaspersky Security Network database to be included in the group of trusted applications, check the **Trusted in Kaspersky Security Network database** box.

## USING THE DANGEROUS ACTIVITY LIST

The list of actions typical of dangerous activity cannot be edited. However, you can refuse to control a selected case of dangerous activity.

➤ *To turn off monitoring for one dangerous activity or another:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Proactive Defense** component.
3. Click the **Settings** button in the right part of the window.
4. In the **Proactive Defense** window that opens, uncheck the box next to the type of activity which you do not want to be monitored.

## CHANGING THE ACTION TO BE TAKEN ON APPLICATIONS' DANGEROUS ACTIVITY

The list of actions typical of dangerous activity cannot be edited. However, you can change the action that Kaspersky Anti-Virus takes when applications' dangerous activity is detected.

➤ *To change the action that Kaspersky Lab application takes on dangerous activity of another application:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **Proactive Defense** component.
3. Click the **Settings** button in the right part of the window.
4. In the **Proactive Defense** window that opens, in the **Event** column, select the desired event for which you want to edit the rule.
5. Configure the settings for the selected event using the links in the **Rule description** section. For example:
  - a. Click the link with the preset action and select the desired action in the **Select action** window that opens.
  - b. Click the **On / Off** link to indicate that a report on operation execution should be created.

## SYSTEM WATCHER

System Watcher collects data about application actions on your computer and provides information to other components for improved protection.

Based on information collected by System Watcher, Kaspersky Anti-Virus can roll back actions performed by malicious programs.

Rolling back actions performed by malicious programs can be initiated by one of the following protection components:

- System Watcher - based on patterns of dangerous activity;
- Proactive Defense;
- File Anti-Virus;
- when performing a virus scan.

If suspicious events are detected in the system, Kaspersky Anti-Virus protection components can request additional information from System Watcher. In interactive protection mode of Kaspersky Anti-Virus (see section "Selecting a protection mode" on page 63), you can view data collected by the System Watcher component and presented as a report on dangerous activity history. This data can help you make a decision when selecting an action in the notification window. When the component detects a malicious program, the link to the System Watcher's report is displayed in the top part of the notification window (see page 146), along with a prompt for action.

**IN THIS SECTION:**

Enabling and disabling System Watcher .....	<a href="#">98</a>
Using patterns of dangerous activity (BSS).....	<a href="#">98</a>
Rolling back a malicious program's actions.....	<a href="#">99</a>

## ENABLING AND DISABLING SYSTEM WATCHER

By default, System Watcher is enabled, running in a mode recommended by Kaspersky Lab specialists. You can disable System Watcher if necessary.

You are advised not to disable the component unless it is absolutely necessary, since this inevitably decreases the efficiency of Proactive Defense and other protection components that may request data collected by System Watcher in order to identify the potential threat detected.

➤ *To disable System Watcher:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **System Watcher** component.
3. In the right part of the window, uncheck the **Enable System Watcher** box.

## USING PATTERNS OF DANGEROUS ACTIVITY (BSS)

Patterns of dangerous activity (BSS – Behavior Stream Signatures) contain sequences of actions typical of applications classified as dangerous. If an application's activity matches a pattern of dangerous activity, Kaspersky Anti-Virus performs the prescribed action.

To provide real-time effective protection, Kaspersky Anti-Virus adds patterns of dangerous activity, which are used by System Watcher, during the database updates.

By default, when Kaspersky Anti-Virus is running in automatic mode, if an application's activity matches a pattern of dangerous activity, System Watcher moves this application to Quarantine. When running in interactive mode, System Watcher prompts for action. You can specify the action that the component should perform when an application's activity matches a pattern of dangerous activity.

In addition to exact matches between applications' activities and patterns of dangerous activity, System Watcher also detects actions that partly match patterns of dangerous activity and are considered suspicious based on the heuristic analysis. If suspicious activity is detected, System Watcher prompts for action regardless of the operation mode.

➤ *To select the action that the component should perform if an application's activity matches a pattern of dangerous activity:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **System Watcher** component.

3. In the right part of the window, in the **Heuristic Analysis** section, check the **Use updatable patterns of dangerous activity (BSS)** box.
4. Click **Select action** and then specify the desired action on the dropdown list.

## ROLLING BACK A MALICIOUS PROGRAM'S ACTIONS

You can use the option of rolling back the actions performed by malware in the system. To enable a rollback, System Watcher logs the history of program activity. You can limit the volume of information that System Watcher stores for a rollback.

By default, Kaspersky Anti-Virus rolls back relevant operations automatically when the protection components detect malicious activity. When running in interactive mode, System Watcher prompts for action. You can specify an action that should be taken if a rollback of actions performed by a malicious program is available.

The procedure of rolling back malware operations affects a strictly defined set of data. It causes no negative consequences for the operating system or data integrity on your computer.

➤ *To select an action that should be taken if a rollback of actions performed by a malicious program is available:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **System Watcher** component.
3. In the right part of the window, in the **Rollback of malware actions** section, choose **Select action**, and then select the required action from the dropdown list.

➤ *To limit the volume of information that System Watcher stores for a rollback:*

1. Open the application settings window.
2. In the left part of the window, in the **Protection Center** section, select the **System Watcher** component.
3. In the right part of the window, in the **Rollback of malware actions** section, check the **Limit data to be stored for rollback** box and specify the maximum data volume that System Watcher should store for a rollback.

## NETWORK PROTECTION

The tools and settings of Kaspersky Anti-Virus together ensure security and control of your network activities.

The sections below contain detailed information about the verification of network connections, proxy server settings, and monitoring of network ports.

### IN THIS SECTION:

Encrypted connections scan .....	<a href="#">100</a>
Configuring the proxy server .....	<a href="#">102</a>
Creating a list of monitored ports .....	<a href="#">102</a>

## ENCRYPTED CONNECTIONS SCAN

Connecting using the SSL / TLS protocols protects the data exchange channel on the Internet. The SSL / TLS protocols allow you to identify the parties exchanging data using electronic certificates, encode the data being transferred, and ensure their integrity during the transfer.

These features of the protocol are used by hackers to spread malicious programs, since most antivirus applications do not scan SSL / TLS traffic.

Kaspersky Anti-Virus scans encrypted connections using a Kaspersky Lab certificate.

If an invalid certificate is detected when connecting to the server (for example, if the certificate is replaced by an intruder), a notification will pop up containing a prompt to either accept or reject the certificate.

If you are sure that connection with a website is always secure, in spite of an invalid certificate, you can add the website into the list of trusted URLs. Kaspersky Anti-Virus will no longer scan the encrypted connection with this website.

You can use the Certificate Installation Wizard to install a certificate for scanning encrypted connections in semi-interactive mode in Microsoft Internet Explorer, Mozilla Firefox (if it is not launched) and Google Chrome, as well as to get instructions on installing Kaspersky Lab's certificate for Opera.

➔ *To enable encrypted connections scanning and install Kaspersky Lab's certificate:*

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Network** component.
3. In the window that opens, check the **Scan encrypted connections** box. When you first enable this setting, the Certificate Installation Wizard starts automatically.
4. If the wizard does not start, click the **Install certificate** button. This will start a Wizard with instructions to follow for successful installation of the Kaspersky Lab certificate.

### IN THIS SECTION:

---

Scanning encrypted connections in Mozilla Firefox.....	<a href="#">100</a>
Scanning encrypted connections in Opera.....	<a href="#">101</a>

## SCANNING ENCRYPTED CONNECTIONS IN MOZILLA FIREFOX

The Mozilla Firefox browser does not use Microsoft Windows certificate storage. To scan SSL connections when using Firefox, you should install the Kaspersky Lab certificate manually.

You can use the Certificate Installation Wizard, if the browser is not launched.

➔ *To install Kaspersky Lab's certificate:*

1. In the browser menu, select **Tools** → **Settings**.
2. In the window that opens, select the **Additional** section.
3. In the **Certificates** section, select the **Security** tab and click the **View Certificates** button.
4. In the window that opens, select the **Authorities** tab and click the **Restore** button.

5. In the window that opens, select the Kaspersky Lab certificate file. The path to Kaspersky Lab's certificate file is: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP12\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer.*
6. In the window that opens, check the boxes to select the actions that should be scanned with the certificate installed. To view information about the certificate, click the **View** button.

➡ *To install Kaspersky Lab's certificate for Mozilla Firefox version 3.x manually:*

1. In the browser menu, select **Tools** → **Settings**.
2. In the window that opens, select the **Additional** section.
3. On the **Encryption** tab, click the **View Certificates** button.
4. In the window that opens, select the **Authorities** tab and click the **Import** button.
5. In the window that opens, select the Kaspersky Lab certificate file. The path to Kaspersky Lab's certificate file is: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP12\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer.*
6. In the window that opens, check the boxes to select the actions that should be scanned with the certificate installed. To view information about the certificate, click the **View** button.

If your computer runs under Microsoft Windows Vista or Microsoft Windows 7, the path to Kaspersky Lab's certificate file is: *%AllUsersProfile%\Kaspersky Lab\AVP12\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer.*

## SCANNING ENCRYPTED CONNECTIONS IN OPERA

The Opera browser does not use Microsoft Windows certificate storage. To scan SSL connections when using Opera, you should install Kaspersky Lab's certificate manually.

➡ *To install Kaspersky Lab's certificate:*

1. In the browser menu, select **Tools** → **Settings**.
2. In the window that opens, select the **Additional** section.
3. In the left part of the window, select the **Security** tab and click the **Manage Certificates** button.
4. In the window that opens, select the **Vendors** tab and click the **Import** button.
5. In the window that opens, select the Kaspersky Lab certificate file. The path to Kaspersky Lab's certificate file is: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP12\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer.*
6. In the window that opens, click the **Install** button. Kaspersky Lab's certificate will be installed. To view information about the certificate and select the actions for which the certificate will be used, select the certificate in the list and click the **View** button.

➡ *To install Kaspersky Lab's certificate for Opera version 9.x:*

1. In the browser menu, select **Tools** → **Settings**.
2. In the window that opens, select the **Additional** section.
3. In the left part of the window, select the **Security** tab and click the **Manage Certificates** button.
4. In the window that opens, select the **Authorities** tab and click the **Import** button.

5. In the window that opens, select the Kaspersky Lab certificate file. The path to Kaspersky Lab's certificate file is: `%AllUsersProfile%\Application Data\Kaspersky Lab\AVP12\Data\Cert(fake)Kaspersky Anti-Virus personal root certificate.cer`.
6. In the window that opens, click the **Install** button. Kaspersky Lab's certificate will be installed.

If your computer runs under Microsoft Windows Vista or Microsoft Windows 7, the path to Kaspersky Lab's certificate file is: `%AllUsersProfile%\Kaspersky Lab\AVP12\Data\Cert(fake)Kaspersky Anti-Virus personal root certificate.cer`.

## CONFIGURING THE PROXY SERVER

If the computer's Internet connection is established via a proxy server, you may need to configure its connection settings. Kaspersky Anti-Virus uses these settings for certain protection components, as well as for updating the databases and application modules.

If your network includes a proxy server using a non-standard port, you should add the port number to the list of monitored ports (see section "Creating a list of monitored ports" on page [102](#)).

➤ *To configure connection with a proxy server:*

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Network** component.
3. In the **Proxy server** section, click the **Proxy server settings** button.
4. In the **Proxy server settings** window that opens, specify the required settings for connection to a proxy server.

## CREATING A LIST OF MONITORED PORTS

Such protection components as Mail Anti-Virus, Web Anti-Virus and IM Anti-Virus (see page [88](#)) monitor the data streams transferred via specific protocols and through certain open TCP ports on your computer. For example, Mail Anti-Virus scans information transferred via SMTP, while Web Anti-Virus scans information transferred via HTTP, HTTPS, and FTP.

You can enable monitoring of all or just selected network ports. If you configure the product to monitor the selected ports, you can create a list of applications for which all ports will be monitored. We recommend that you expand this list by including applications that receive or transfer data via FTP.

➤ *To add a port to the list of monitored ports:*

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Network** subsection.
3. In the **Monitored ports** section, select **Monitor selected ports only** and click the **Select** button.

The **Network ports** window will open.

4. Click the **Add** link located under the list of ports in the top part of the window to open the **Network port** window, and enter the number and description of a port.

➤ *To exclude a port from the list of monitored ports:*

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Network** subsection.

- In the **Monitored ports** section, select **Monitor selected ports only** and click the **Select** button.

The **Network ports** window will open.

- In the list of ports in the top part of the window, uncheck the box next to the description of the port that should be excluded.

➤ *To create a list of applications for which you wish to monitor all ports:*

- Open the application settings window.
- In the left part of the window, in the **Advanced Settings** section, select the **Network** subsection.
- In the **Monitored ports** section, select **Monitor selected ports only** and click the **Select** button.

The **Network ports** window will open.

- Check the **Monitor all ports for specified applications** box, and in the list of applications below, check the boxes for the names of the applications for which all ports should be monitored.

- If the desired application is not in the list, add it as follows:

- Click the **Add** link under the list of applications to open a menu, and select an item:
  - To specify the location of the executable file of an application, select **Browse** and specify the file's location on the computer.
  - To select an application from the list of applications currently running, select **Applications**. In the **Select application** window that opens, select the required application.
- In the **Application** window, enter a description for the application selected.

## TRUSTED ZONE

The *Trusted zone* is a list of objects which should not be monitored by the application. In other words, it is a set of exclusions from the scope of Kaspersky Anti-Virus protection.

The Trusted zone is created based on the list of trusted applications (see section "Creating a list of trusted applications" on page [104](#)) and exclusion rules (see section "Creating exclusion rules" on page [104](#)), depending on the features of the objects you work with and applications installed on the computer. Including objects in the trusted zone may be required if, for example, Kaspersky Anti-Virus blocks access to an object or application, even though you are certain that this object / application is absolutely harmless.

For example, if you think objects used by Microsoft Windows Notepad are harmless and require no scanning, that is, you trust this application, add Notepad to the list of trusted applications to exclude scanning of objects used by this process.

Some actions classified as dangerous may be safe in the framework of certain applications. For instance, applications that automatically toggle keyboard layouts, such as Punto Switcher, regularly intercept text being entered on your keyboard. To take into account the specifics of such applications and disable the monitoring of their activity, you are advised to add them to the list of trusted applications.

When an application is added into the list of trusted ones, its file and network activities (including suspicious ones) become uncontrolled. So do its attempts to access the system registry. At the same time, the executable file and the trusted application's process are scanned for viruses as they were before. To completely exclude an application from a scan, you should use exclusion rules.

Excluding trusted applications from scanning avoids problems related to the application's compatibility with other programs (e.g. the problems of double scanning of network traffic on a third-party computer by Kaspersky Anti-Virus and by another anti-virus application), and also increases the computer's performance rate, which is critical when using server applications.

In its turn, exclusion rules for the trusted zone ensure the option of working with legal applications that may be exploited by intruders to do harm to the user's computer or data. These applications have no malicious features, but they may be used as auxiliary components of a malicious program. This category includes remote administration applications, IRC clients, FTP servers, various utility tools for halting or concealing processes, keyloggers, password hacking programs, dialers, and others. Such applications may be blocked by Kaspersky Anti-Virus. To avoid blockage, you can configure exclusion rules.

An *Exclusion rule* is a set of conditions which determine that an object should not be scanned by Kaspersky Anti-Virus. In any other case, the object is scanned by all protection components according to their respective protection settings.

Exclusion rules for the trusted zone may be used by several application components, such as File Anti-Virus (see section "File Anti-Virus" on page 77), Mail Anti-Virus (see section "Mail Anti-Virus" on page 83), Web Anti-Virus (see section "Web Anti-Virus" on page 88)), or when running virus scan tasks.

**IN THIS SECTION:**

---

Creating a list of trusted applications ..... [104](#)  
 Creating exclusion rules ..... [104](#)

## CREATING A LIST OF TRUSTED APPLICATIONS

By default, Kaspersky Anti-Virus scans objects being opened, run, or saved by any program process and monitors the activity of all applications and the network traffic they create. When you add an application to the list of trusted ones, Kaspersky Anti-Virus excludes it from scanning.

➔ *To add an application to the trusted list:*

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Threats and Exclusions** subsection.
3. In the **Exclusions** section, click the **Settings** button.
4. In the window that opens, on the **Trusted applications** tab, open the application selection menu by clicking the **Add** button.
5. In the menu that opens, select an application from the **Applications** list, or select **Browse** to specify the path to the executable files of the desired application.
6. In the **Exclusions for applications** window that opens, check the boxes for the types of application activity that should be excluded from scanning.

## CREATING EXCLUSION RULES

If you use applications recognized by Kaspersky Anti-Virus as legal ones that may be used by intruders to do harm to the user's computer or data, we recommend that you configure exclusion rules for them.

➔ *To create an exclusion rule:*

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Threats and Exclusions** subsection.
3. In the **Exclusions** section, click the **Settings** button.

4. In the window that opens, on the **Exclusion rules** tab, click the **Add** button.
5. In the **Exclusion rule** window that opens, edit the exclusion rule settings.

## PERFORMANCE AND COMPATIBILITY WITH OTHER APPLICATIONS

The performance of Kaspersky Anti-Virus is defined as the range of threats it can detect, as well as its consumption of energy and computer resources.

Kaspersky Anti-Virus allows you to select various categories of threats (see section "Selecting detectable threat categories" on page [105](#)) that the application should detect.

Energy consumption is of great importance for portable computers. Scanning a computer for viruses and updating the Kaspersky Anti-Virus databases often require significant amounts of resources. The special laptop mode of Kaspersky Anti-Virus (see section "Battery saving" on page [106](#)) allows you to automatically postpone scheduled scan and update tasks when using batteries, thus saving battery charge, while Idle Scan mode (see section "Running tasks in background mode" on page [107](#)) allows you to run resource-intensive tasks when your computer is not in use.

Consumption of the computer's resources by Kaspersky Anti-Virus may impact other applications' performance. To solve problems of simultaneous operations which increase the load on the CPU and disk subsystems, Kaspersky Anti-Virus may pause scan tasks and concede resources to other applications (see section "Distributing computer resources when scanning for viruses" on page [106](#)) running on your computer.

In the Gaming Profile (see page [108](#)) mode, the application automatically disables displaying notifications of Kaspersky Anti-Virus activity when starting other applications in full-screen mode.

In case of an active infection in the system, the advanced disinfection procedure requires restarting your computer, which may also impact other applications' performance. If necessary, you can disable the advanced disinfection technology (see page [106](#)) to avoid an unwanted restart of your computer.

### IN THIS SECTION:

Selecting detectable threat categories .....	<a href="#">105</a>
Battery saving .....	<a href="#">106</a>
Advanced Disinfection.....	<a href="#">106</a>
Distributing computer resources when scanning for viruses .....	<a href="#">106</a>
Running tasks in background mode .....	<a href="#">107</a>
Full-screen mode. Gaming Profile .....	<a href="#">108</a>

## SELECTING DETECTABLE THREAT CATEGORIES

Threats detected by Kaspersky Anti-Virus are divided into categories based on various attributes. The application always searches for viruses, Trojan programs, and malicious utility tools. These programs can do significant harm to your computer. To ensure a more reliable protection to your computer, you can extend the list of detected threats by enabling control of actions performed by legal applications that may be exploited by an intruder to do harm to the user's computer and data.

➤ *To select detectable threat categories:*

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Threats and Exclusions** subsection.
3. In the right part of the window, click the **Settings** button located under the **Detection of the following threat types is enabled** list.
4. In the **Threats** window that opens, check the boxes for the categories of threats that should be detected.

## BATTERY SAVING

To save power on a portable computer, virus scanning and scheduled update tasks can be postponed. If necessary, you can update Kaspersky Anti-Virus or start a virus scan manually.

➤ *To enable the power conservation mode when working from a battery:*

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Battery Saving** subsection.
3. In the right part of the window, check the **Disable scheduled scans while running on battery power** box.

## ADVANCED DISINFECTION

Today's malicious programs can invade the lowest levels of an operating system, which makes them practically impossible to delete. If a malicious activity is detected within the system, Kaspersky Anti-Virus offers you to apply the Advanced Disinfection technology, which eliminates the threat and removes it from the computer.

When the advanced disinfection procedure is complete, the application restarts the computer. After restarting your computer, you are advised to run the full virus scan (see section "How to perform a full scan of your computer for viruses" on page [47](#)).

➤ *To enable Kaspersky Anti-Virus to apply the Advanced Disinfection technology:*

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Compatibility** subsection.
3. Check the **Enable Advanced Disinfection technology** box.

## DISTRIBUTING COMPUTER RESOURCES WHEN SCANNING FOR VIRUSES

Executing scan tasks increases the load on the CPU and disk subsystems, thus slowing down other applications. By default, if such a situation arises, Kaspersky Anti-Virus pauses virus scan tasks and releases system resources for the user's applications.

However, there are a number of applications which start immediately when CPU resources become available and run in the background. For the scan not to depend on the performance of those applications, system resources should not be conceded to them.

➤ *For Kaspersky Anti-Virus to postpone scan tasks when they slow down other applications:*

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Compatibility** subsection.
3. Check the **Concede resources to other applications** box.

## RUNNING TASKS IN BACKGROUND MODE

To optimize the load on the computer's resources, Kaspersky Anti-Virus performs regular scanning for rootkits in background mode and running of resource-intensive tasks when the computer is idle.

Regular scanning for rootkits is run while you work at the computer. The scan takes 5 minutes at the most and involves a minimal share of the computer resources.

When the computer is idle, the following tasks can be run:

- automatic update of anti-virus databases and program modules;
- scanning of system memory, startup objects, and system partition.

Idle Scan tasks are run if the computer has been blocked by the user or if the screensaver is displayed on the screen for at least 5 minutes.

If your computer is battery-powered, no tasks are run when the computer is idle.

After tasks are run in background mode, their progress is displayed in the Task Manager (see section "Managing scan tasks. Task Manager" on page [72](#)).

### IN THIS SECTION:

Searching for rootkits in background mode .....	<a href="#">107</a>
Idle Scan .....	<a href="#">107</a>

## SEARCHING FOR ROOTKITS IN BACKGROUND MODE

By default, Kaspersky Anti-Virus performs regular rootkit scan. If necessary, you can disable rootkit scan.

➤ *To disable regular rootkit scan:*

1. Open the application settings window.
2. In the left part of the window, in the **Scan** section, select the **General Settings** subsection.
3. In the right part of the window, uncheck the **Perform regular rootkit scan** box.

## IDLE SCAN

The first stage of Idle Scan is checking whether the databases and application modules are up-to-date. If an update is required after scanning, an automatic update task starts. At the second stage, the application verifies the date and status of the last run of Idle Scan. If Idle Scan has not been run at all, or was run more than 7 days ago, or was interrupted, then the application runs the scan task for the system memory, startup objects, and system registry.

Idle Scan is performed using a deep level of heuristic analysis, which increases the probability of threat detection.

When the user returns to his or her work, the Idle Scan task is automatically interrupted. Note that the application remembers the stage at which the task was interrupted to resume the scan from this stage later.

If running Idle Scan tasks was interrupted while downloading an update package, the update will start from the beginning next time.

➔ *To disable Idle Scan mode:*

1. Open the application settings window.
2. In the left part of the window, in the **Scan** section, select the **General Settings** subsection.
3. In the right part of the window, uncheck the **Perform Idle Scan** box.

## FULL-SCREEN MODE. GAMING PROFILE

Certain programs (especially computer games) running in full-screen mode are only marginally compatible with some features of Kaspersky Anti-Virus: for example, pop-up notifications are undesirable in that mode. Quite often those applications require significant system resources, meaning that running certain Kaspersky Anti-Virus tasks may slow down their performance.

To avoid manually disabling notifications and pausing tasks every time you launch full-screen applications, Kaspersky Anti-Virus provides the option of temporarily changing the settings using the gaming profile. When the gaming profile is active, switching to full-screen mode automatically changes the settings of all product components to ensure optimal system functioning in that mode. Upon exit from the full-screen mode, product settings return to the initial values used before entering the full-screen mode.

➔ *To enable the gaming profile:*

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Gaming Profile** subsection.
3. Check the **Use Gaming Profile** box and specify the necessary gaming profile settings in the **Profile options** section below.

## KASPERSKY ANTI-VIRUS SELF-DEFENSE

Because Kaspersky Anti-Virus ensures your computer's protection against malware, malicious programs penetrating your computer attempt to block Kaspersky Anti-Virus or delete the application from your computer.

Stable performance of your computer defense is ensured by self-defense features and protection against external control implemented in Kaspersky Anti-Virus.

Kaspersky Anti-Virus self-defense prevents the modification and deletion of its own files on the hard disk, processes in the memory, and entries in the system registry. Protection against external control allows you to block all attempts to remotely control application services.

On computers running under 64-bit operating systems and Microsoft Windows Vista, Kaspersky Anti-Virus self-defense is only available for preventing the application's own files on local drives and system registry records from being modified or deleted.

**IN THIS SECTION:**

Enabling and disabling self-defense.....	<a href="#">109</a>
Protection against external control .....	<a href="#">109</a>

**ENABLING AND DISABLING SELF-DEFENSE**

By default, Kaspersky Anti-Virus self-defense is enabled. You can disable self-defense, if necessary.

➤ *To disable Kaspersky Anti-Virus self-defense:*

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Self-Defense** subsection.
3. In the right part of the window, uncheck the **Enable Self-Defense** box.

**PROTECTION AGAINST EXTERNAL CONTROL**

By default, protection against external control is enabled. You can disable protection, if necessary.

When using remote administration applications (such as RemoteAdmin) you will need to add such applications to the Trusted Applications list (see section "Trusted zone" on page [103](#)) when External Service Control is enabled and enable the **Do not monitor application activity** setting for them.

➤ *To disable protection against external control:*

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Self-Defense** subsection.
3. In the **External control** section, uncheck the **Disable external service control** box.

**QUARANTINE AND BACKUP**

*Quarantine* is a special area storing files probably infected with viruses and files that cannot be disinfected at the time when they are detected.

A potentially infected file can be detected and quarantined in the course of a virus scan or by File Anti-Virus, Mail Anti-Virus or Proactive Defense.

Files are quarantined in the following cases:

- File code resembles a known but partially modified threat or has a malware-like structure, but is not registered in the database. In this case, the file is moved to Quarantine after heuristic analysis performed by File Anti-Virus and Mail Anti-Virus, or during an anti-virus scan. Heuristic analysis rarely causes false alarms.
- The sequence of operations performed by an object looks suspicious. In this case, the file is moved to Quarantine after its behavior is analyzed by the Proactive Defense component.

Files in Quarantine pose no threat. With the course of time, information about new threats and ways of neutralizing them appears, which may cause Kaspersky Anti-Virus to disinfect a file stored in Quarantine.

*Backup storage* is designed for storing backup copies of files that have been deleted or modified during the disinfection process.

**IN THIS SECTION:**

---

Storing files in Quarantine and Backup ..... [110](#)

Working with quarantined files ..... [110](#)

Working with objects in Backup..... [111](#)

Scanning files in Quarantine after an update ..... [112](#)

## STORING FILES IN QUARANTINE AND BACKUP

The default maximum storage duration for objects is 30 days. After that the objects will be deleted. You can cancel the time restriction or change the maximum object storage duration.

In addition, you can specify the maximum size of Quarantine and Backup. If the maximum size value is reached, the content of Quarantine and Backup is replaced with new objects. By default, the maximum size restriction is disabled.

➤ *To modify the object maximum storage time:*

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Reports and Storages** subsection.
3. In the right part of the window, in the **Storing Quarantine and Backup objects** section, check the **Store objects no longer than** box and specify the maximum storage duration for quarantined objects.

➤ *To configure the maximum Quarantine and Backup size:*

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Reports and Storages** subsection.
3. In the right part of the window, in the **Storing Quarantine and Backup objects** section, check the **Maximum size** box and specify the maximum Quarantine and Backup size.

## WORKING WITH QUARANTINED FILES

The Kaspersky Anti-Virus quarantine lets you perform the following operations:

- quarantine files that you suspect are infected;
- scan files in Quarantine using the current version of Kaspersky Anti-Virus databases;
- restore files in original folders, from which they have been moved to Quarantine;
- delete selected files from Quarantine;
- send files from Quarantine to Kaspersky Lab for research.

You can use the following methods to move a file to Quarantine:

- using the **Move to Quarantine** button in the **Quarantine** window;
- using the context menu for the file.

➤ *To move a file to Quarantine from the Quarantine window:*

1. Open the main application window.
2. In the lower part of the window, select the **Quarantine** section.
3. On the **Quarantine** tab click the **Move to Quarantine** button.
4. In the window that opens, select the file that you want to move to Quarantine.

➤ *To move a file to Quarantine using the context menu:*

1. Open Microsoft Windows Explorer and go to the folder that contains the file that you want to move to Quarantine.
2. Right-click to open the context menu of the file and select **Move to Quarantine**.

➤ *To scan a quarantined file:*

1. Open the main application window.
2. In the lower part of the window, select the **Quarantine** section.
3. On the **Quarantine** tab, select a file that you need to scan.
4. Click the **Scan** button.

➤ *To restore a quarantined object:*

1. Open the main application window.
2. In the lower part of the window, select the **Quarantine** section.
3. On the **Quarantine** tab, select a file that you need to restore.
4. Click the **Restore** button.

➤ *To delete a quarantined object:*

1. Open the main application window.
2. In the lower part of the window, select the **Quarantine** section.
3. On the **Quarantine** tab, select a file that you need to delete.
4. Right-click the file to open its context menu and select **Delete**.

➤ *To send a quarantined object to Kaspersky Lab for analysis:*

1. Open the main application window.
2. In the lower part of the window, select the **Quarantine** section.
3. On the **Quarantine** tab, select a file that you need to send for research.
4. Right-click to open the context menu of the file and select the **Send for analysis** item.

## WORKING WITH OBJECTS IN BACKUP

The Kaspersky Anti-Virus backup storage lets you perform the following operations:

- restore files in a specified folder or in original ones, in which a file had been stored before it was processed by Kaspersky Anti-Virus;
- delete selected files or all files from Backup.

➔ *To restore an object from Backup:*

1. Open the main application window.
2. In the lower part of the window, select the **Quarantine** section.
3. On the **Storage** tab, select a file that you need to restore.
4. Click the **Restore** button.

➔ *To delete a file from Backup:*

1. Open the main application window.
2. In the lower part of the window, select the **Quarantine** section.
3. On the **Storage** tab, select a file that you need to delete.
4. Right-click the file to open its context menu and select **Delete**.

➔ *To delete all files from Backup:*

1. Open the main application window.
2. In the lower part of the window, select the **Quarantine** section.
3. On the **Storage** tab, click the **Clear storage** button.

## SCANNING FILES IN QUARANTINE AFTER AN UPDATE

If the application has scanned a file and has not been able to determine exactly what malicious programs have infected it, the file is quarantined. After the databases are updated, Kaspersky Anti-Virus may be able to clearly identify and remove the threat. You can enable automatic scanning of quarantined objects after each update.

We recommend that you periodically view quarantined files. Scanning may change their status. Some files can then be restored to their previous locations, and you will be able to continue working with them.

➔ *To enable scanning quarantined files after update:*

1. Open the application settings window.
2. In the left part of the window, in the **Update** section, select the **Update Settings** component.
3. Check the **Rescan Quarantine after update** box in the **Additional** section.

## ADDITIONAL TOOLS FOR BETTER PROTECTION OF YOUR COMPUTER

The following wizards and tools included with Kaspersky Anti-Virus are used to resolve specific issues concerning your computer's security:

- Kaspersky Rescue Disk Creation Wizard is designed for creating an ISO disk image and writing Kaspersky Rescue Disk on a removable medium, which allows you to recover the system's operability after a virus attack if you load the application from the removable medium. Kaspersky Rescue Disk should be used when the infection is at such a level that it is deemed impossible to disinfect the computer using anti-virus applications or malware removal utilities.
- The Privacy Cleaner Wizard is designed to search for and eliminate traces of a user's activities in the system, as well as operating system settings which allow the gathering of information about user activities.
- The System Restore Wizard is designed to eliminate system damage and traces of malware objects in the system.
- The Browser Configuration Wizard is designed to analyze and adjust the settings of Microsoft Internet Explorer in order to eliminate its potential vulnerabilities.

All the problems found by the Wizards (except the Kaspersky Rescue Disk Creation Wizard) are grouped based on the type of danger they pose to the operating system. Kaspersky Lab offers a set of actions for each group of problems which help eliminate vulnerabilities and weak points in the system's settings. Three groups of problems and, accordingly, three groups of actions to be taken when they are detected are distinguished:

- *Strongly recommended actions* will help eliminate problems posing a serious security threat. You are advised to perform all the actions in this group without delay to eliminate the threat.
- *Recommended actions* help eliminate problems posing a potential threat. You are advised to perform all actions in this group as well to provide the optimal level of protection.
- *Additional actions* help repair system damages which do not pose a current threat but may threaten your computer's security in the future. Performing these actions ensures comprehensive protection of your computer. However, in some cases, they may lead to deletion of user settings (such as cookies).

### IN THIS SECTION:

---

Privacy Cleaner .....	<a href="#">113</a>
Configuring a browser for safe work .....	<a href="#">115</a>
Rolling back changes made by Wizards .....	<a href="#">116</a>

## PRIVACY CLEANER

When working with the computer, a user's actions are registered in the system. Saved data includes the search queries entered by users and web sites visited, launched programs, opened and saved files, the Microsoft Windows system event log, temporary files, etc.

All these sources of information about the user's activity may contain confidential data (including passwords) and may become available to intruders for analysis. Frequently, the user has insufficient knowledge to prevent information being stolen from these sources.

Kaspersky Anti-Virus includes the Privacy Cleaner Wizard. This Wizard searches for traces of user activities in the system, as well as for operation system settings which contribute to the storing of information about user activity.

Please keep in mind that data related to user activity in the system, is accumulated constantly. The launch of any file or the opening of any document is logged. The Microsoft Windows system log registers many events occurring in the system. For this reason, repeated running of the Privacy Cleaner Wizard may detect activity traces which were not cleaned up by the previous run of the Wizard. Some files, for example the Microsoft Windows log file, may be in use by the system while the Wizard is attempting to delete them. In order to delete these files, the Wizard will prompt you to restart the system. However, during the restart, these files may be recreated and detected again as activity traces.

The Wizard consists of a series of screens (steps) that you can navigate through using the **Back** and **Next** buttons. To close the Wizard once it has completed its task, click the **Finish** button. To stop the Wizard at any stage, click the **Cancel** button.

➡ *To remove traces of the user's activity in the system:*

1. Open the main application window.
2. In the lower part of the window, select the **Tools** section.
3. In the window that opens, in the **Privacy Cleaner** section, click the **Start** button.

Let us review the steps of the Wizard in more detail.

### Step 1. Starting the Wizard

Make sure the option **Perform user's activity traces diagnostics** is selected and click the **Next** button to start the Wizard.

### Step 2. Activity signs search

This Wizard searches for traces of malware activities in your computer. The scan may take some time. Once the search is complete, the Wizard will proceed automatically to the next step.

### Step 3. Selecting Privacy Cleaner actions

When the search is complete, the Wizard displays the detected activity traces and actions suggested to eliminate them.

To view the actions within a group, click the **+** icon to the left of the group name.

To make the Wizard perform a certain action, check the box to the left of the corresponding action description. By default, the Wizard performs all recommended and strongly recommended actions. If you do not wish to perform a certain action, uncheck the box next to it.

**It is strongly recommended that you not uncheck the boxes selected by default, as doing so will leave your computer vulnerable to threats.**

Having defined the set of actions which the Wizard will perform, click the **Next** button.

### Step 4. Privacy Cleaner

The Wizard will perform the actions selected during the previous step. The elimination of activity traces may take some time. To clean up certain activity traces, a reboot may be required; if so, the Wizard will notify you.

Once the clean-up is complete, the Wizard will proceed automatically to the next step.

## Step 5. Wizard completion

If you wish to clean up the traces of user activity automatically whenever Kaspersky Anti-Virus completes its work, use the last screen of the Wizard to check the box **Clean activity traces every time on Kaspersky Anti-Virus exit**. If you plan to remove activity traces manually using the Wizard, do not check this box.

Click the **Finish** button to close the Wizard.

## CONFIGURING A BROWSER FOR SAFE WORK

The Microsoft Internet Explorer browser requires special analysis and configuration in certain cases, since some setting values selected by the user or set by default may cause security problems.

Here are some examples of the objects and parameters used in the browser and how they are associated with potential security threats:

- **Microsoft Internet Explorer cache.** The cache stores data downloaded from the Internet, so the user does not have to download them next time. This speeds up the download time of web pages and reduces Internet traffic. In addition to that, the cache contains confidential data and makes it possible to find out which sites the user has visited. Some malware objects also scan the cache while scanning the disk, and intruders can obtain, for example, the user's email addresses. You are advised to clear the cache every time you close your browser to improve protection.
- **Display of known file types extensions.** To edit file names conveniently, you can disable the display of their extensions. Nevertheless, it is sometimes useful to see the file extension. File names of many malicious objects contain combinations of symbols imitating an additional file extension before the real one (e.g., example.txt.com). If the real file extension is not displayed, users can see just the file name part with the imitated extension and so they may identify a malicious object as a harmless file. To improve protection, you are advised to enable the display of files of known formats.
- **List of trusted websites.** For some websites to run correctly, you should add them to the list of trusted sites. At the same time, malicious objects can add links to websites created by intruders to this list.

The browser configuration for Safe Run may cause problems with the display of certain websites (for example, if they use ActiveX elements). This problem can be solved by adding these websites to the trusted zone.

Browser analysis and configuration are performed in the Browser Configuration Wizard. The Wizard checks whether the latest browser updates are installed and makes sure that the current browser settings do not make the system vulnerable to malicious exploits. Once the Wizard is complete, a report is generated which can be sent to Kaspersky Lab for analysis.

The Wizard consists of a series of screens (steps) that you can navigate through using the **Back** and **Next** buttons. To close the Wizard once it has completed its task, click the **Finish** button. To stop the Wizard at any stage, click the **Cancel** button.

Close all Microsoft Internet Explorer windows before starting the diagnostics.

➔ *To configure the browser for safe work:*

1. Open the main application window.
2. In the lower part of the window, select the **Tools** section.
3. In the window that opens, in the **Browser Configuration** section, click the **Start** button.

Let us review the steps of the Wizard in more detail.

## Step 1. Starting the Wizard

Make sure the option **Perform diagnostics for Microsoft Internet Explorer** is selected and click the **Next** button to start the Wizard.

## Step 2. Microsoft Internet Explorer settings analysis

The Wizard analyzes the settings of Microsoft Internet Explorer. Searching the browser settings for problems may take some time. Once the search is complete, the Wizard will proceed automatically to the next step.

## Step 3. Selecting actions for browser configuration

When the search is complete, the Wizard displays the detected problems and actions suggested to eliminate them.

To view the actions within a group, click the **+** icon to the left of the group name.

To make the Wizard perform a certain action, check the box to the left of the corresponding action description. By default, the Wizard performs all recommended and strongly recommended actions. If you do not wish to perform a certain action, uncheck the box next to it.

**It is strongly recommended that you not uncheck the boxes selected by default, as doing so will leave your computer vulnerable to threats.**

Having defined the set of actions which the Wizard will perform, click the **Next** button.

## Step 4. Browser Configuration

The Wizard will perform the actions selected during the previous step. Browser configuration may take some time. Once configuration is complete, the Wizard proceeds automatically to the next step.

## Step 5. Wizard completion

Click the **Finish** button to close the Wizard.

# ROLLING BACK CHANGES MADE BY WIZARDS

Some changes made when running the Privacy Cleaner Wizard (see section "Privacy Cleaner" on page [113](#)), System Restore Wizard (see section "What to do if you suspect your computer is infected" on page [50](#)), and Browser Configuration Wizard (see section "Configuring a browser for safe work" on page [115](#)) can be rolled back.

➤ *To roll back changes made by Wizards:*

1. Open the main application window and select the **Tools** section in the lower part of the window.
2. In the right part of the window, click the **Start** button in the section with the name of a Wizard, for which you need to roll back changes made:
  - **Privacy Cleaner** – to roll back changes made by the Privacy Cleaner Wizard;
  - **Microsoft Windows Troubleshooting** – to roll back changes made by the Microsoft Windows Troubleshooting Wizard;
  - **Browser Configuration** – to roll back changes made by the Browser Configuration Wizard.

Let us take a closer look at Wizards' steps taken when rolling back changes.

### Step 1. Starting the Wizard

Select **Roll back changes** and click the **Next** button.

### Step 2. Search for changes

The Wizard searches for the changes that it made earlier and that can be rolled back. Once the search is complete, the Wizard will proceed automatically to the next step.

### Step 3. Selecting changes to roll back

When the search is completed, the Wizard informs you of changes found.

To make the wizard roll back an action taken earlier, check the box located to the left of the action's name.

After you have selected actions that you want to roll back, click the **Next** button.

### Step 4. Rolling back changes

The Wizard rolls back the actions selected at the previous step. When the changes are rolled back, the Wizard automatically proceeds to the next step.

### Step 5. Wizard completion

Click the **Finish** button to close the Wizard.

## REPORTS

Events that occur during the operation of the protection components or when the Kaspersky Anti-Virus tasks are run are logged in reports.

### IN THIS SECTION:

---

Creating a report for the selected protection component .....	<a href="#">117</a>
Data filtering .....	<a href="#">118</a>
Events search .....	<a href="#">118</a>
Saving a report to file .....	<a href="#">119</a>
Storing reports.....	<a href="#">120</a>
Clearing application reports.....	<a href="#">120</a>
Recording non-critical events into the report.....	<a href="#">120</a>
Configuring the notification of report availability .....	<a href="#">120</a>

## CREATING A REPORT FOR THE SELECTED PROTECTION COMPONENT

You can obtain a detailed report about events which occurred during the operation of each of the Kaspersky Anti-Virus protection components or during execution of its tasks.

For added convenience when working with reports, you can change the data display on the screen: group events by various parameters, select the report period, sort events by column or by importance, and hide columns.

➤ *To create a report on a certain protection component or a task:*

1. Open the main application window.
2. In the top part of the window, click the **Reports** link.
3. In the **Reports** window that opens, click the **Detailed report** button.
4. In the left part of the **Detailed report** window that opens, select the component or task, for which a report should be created. When you select the **Protection Center** item, a report is created for all protection components.

## DATA FILTERING

You can filter events in Kaspersky Anti-Virus reports by one or several values in the report columns, as well as define complex data filtering conditions.

➤ *To filter events by values:*

1. Open the main application window.
2. In the top part of the window, click the **Reports** link.
3. In the **Reports** window that opens, click the **Detailed report** button.
4. In the right part of the **Detailed report** window that opens, move the mouse pointer to the upper left corner of the column header and click it to open the filter menu.
5. Select the value which should be used to filter data in the filter menu.
6. Repeat the procedure for another column, if necessary.

➤ *To specify a complex filtering condition:*

1. Open the main application window.
2. Click the **Reports** link in the top part of the window to open the reports window.
3. In the window that opens, on the **Report** tab, click the **Detailed report** button.
4. In the right part of the **Detailed report** window that opens, right-click the appropriate report column to display the context menu for it and select **Custom**.
5. In the **Custom filter** window that opens, set the filtration conditions:
  - a. Define the query limits in the right part of the window.
  - b. In the left part of the window, select the necessary query condition from the **Condition** dropdown list (e.g., is greater or less than, equals or does not equal the value specified as the query limit).
  - c. If necessary, add a second condition using logical conjunction (logical AND) or disjunction (logical OR) operations. If you wish your data query to satisfy both specified conditions, select **AND**. If only one of the two conditions is required, select **OR**.

## EVENTS SEARCH

You can search a report for the desired event using a key word in the search line or special search window.

➤ *To find an event using the search line:*

1. Open the main application window.
2. In the top part of the window, click the **Reports** link.
3. In the **Reports** window that opens, click the **Detailed report** button.
4. Enter the key word in the search line in the right part of the **Detailed report** window that opens.

➤ *To find an event using the search window:*

1. Open the main application window.
2. In the top part of the window, click the **Reports** link.
3. In the **Reports** window that opens, click the **Detailed report** button.
4. In the right part of the **Detailed report** window that opens, right-click the appropriate column header to display the context menu for it and select **Search**.
5. Specify the search criteria in the **Search** window that opens:
  - a. In the **String** field, enter a key word to be searched for.
  - b. In the **Column** dropdown list, select the name of the column that should be searched for the specified key word.
  - c. If necessary, check the boxes for additional search settings.
6. Start the search using one of the following methods:
  - If you want to find an event that meets the specified search criteria and comes next after the one that you have highlighted on the list, click the **Find next** button.
  - If you want to find all events that meet the specified search criteria, click the **Mark all** button.

## SAVING A REPORT TO FILE

The report obtained can be saved to a text file.

➤ *To save the report to file:*

1. Open the main application window.
2. In the top part of the window, click the **Reports** link.
3. In the **Reports** window that opens, click the **Detailed report** button.
4. In the **Detailed report** window that opens, create a required report and click the **Save** link to select a location for the file that you want to save.
5. In the window that opens, select a folder into which you wish to save the report file and enter the file name.

## STORING REPORTS

The default maximum report storage duration is 30 days. After that the reports will be deleted. You can cancel the time restriction or change the maximum report storage duration.

In addition, you can also define the maximum report file size. By default, the maximum size is 1024 MB. Once the maximum size has been reached, the content of the file is replaced with new records. You can cancel any limits imposed on the report's size, or enter another value.

➤ *To modify the report maximum storage time:*

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Reports and Storages** subsection.
3. In the right part of the window, in the **Storing reports** section, check the **Store reports no longer than** box and specify the maximum storage period for reports.

➤ *To configure the maximum report file size:*

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Reports and Storages** subsection.
3. In the **Storing reports** section in the right part of the window, check the **Maximum file size** box and specify the maximum size for a report file.

## CLEARING APPLICATION REPORTS

You can clear the reports containing data that you no longer need.

➤ *To clear application reports:*

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Reports and Storages** subsection.
3. In the right part of the window, in the **Clear reports** section, click the **Clear** button.
4. In the **Clearing reports** window that opens, check the boxes for the reports you wish to clear.

## RECORDING NON-CRITICAL EVENTS INTO THE REPORT

By default, the product does not add non-critical events or registry and file system events to its reports. You can add records of such events to the report.


➤ *To add non-critical events to the report:*

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Reports and Storages** subsection.
3. In the right part of the window, check the **Log non-critical events** box.

## CONFIGURING THE NOTIFICATION OF REPORT AVAILABILITY

You can create a schedule according to which Kaspersky Anti-Virus will remind you that a report is ready.

➤ *To configure notification of a report's completion:*

1. Open the main application window.
2. In the top part of the window, click the **Reports** link.
3. In the **Reports** window that opens, click the  button.
4. In the **Notifications** window that opens, specify schedule settings.

## APPLICATION APPEARANCE. MANAGING ACTIVE INTERFACE ELEMENTS

Kaspersky Anti-Virus allows you to adjust the settings for display of text on the logon screen in Microsoft Windows and active interface elements (the application icon in the notification area, notification windows, and pop-up messages).

### IN THIS SECTION:

Translucence of notification windows .....	<a href="#">121</a>
Animation of the application icon in the notification area.....	<a href="#">121</a>
Text on Microsoft Windows logon screen.....	<a href="#">122</a>

## TRANSLUCENCE OF NOTIFICATION WINDOWS

➤ *To make notification windows translucent:*

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Appearance** subsection.
3. In the **Icon in the taskbar notification area** section, check the **Enable semi-transparent windows** box.

## ANIMATION OF THE APPLICATION ICON IN THE NOTIFICATION AREA

Animation of the application icon is displayed in the notification area when running an update or a scan.

By default, animation of the application icon in the notification area is enabled.

➤ *To disable animation of the application icon:*

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Appearance** subsection.
3. In the **Icon in the taskbar notification area** section, uncheck the **Animate taskbar icon when executing tasks** box.

## TEXT ON MICROSOFT WINDOWS LOGON SCREEN

By default, if Kaspersky Anti-Virus is enabled and protects your computer, the text "Protected by Kaspersky Lab" is displayed on the logon screen while Microsoft Windows is loading.

Text "Protected by Kaspersky Lab" is only displayed in Microsoft Windows XP.

➤ *To enable display of this text during the loading of Microsoft Windows:*

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Appearance** subsection.
3. In the **Icon in the taskbar notification area** section, uncheck the **Show "Protected by Kaspersky Lab" on Microsoft Windows logon screen** box.

## NOTIFICATIONS

By default, if any events occur during operation, Kaspersky Anti-Virus notifies you of them. If you are required to select further actions, notification windows will be displayed on the screen (see section "Notification windows and pop-up messages" on page [32](#)). The application notifies you of events which do not require selection of an action with audio signals, email messages, and pop-up messages in the taskbar notification area (see section "Notification windows and pop-up messages" on page [32](#)).

Kaspersky Anti-Virus comprises the News Agent (on page [35](#)) that Kaspersky Lab uses to notify you of various news. If you do not want to receive any news, you can disable the news delivery.

### IN THIS SECTION:

Enabling and disabling notifications .....	<a href="#">122</a>
Configuring the notification method .....	<a href="#">123</a>
Disabling news delivery .....	<a href="#">123</a>

## ENABLING AND DISABLING NOTIFICATIONS

By default, Kaspersky Anti-Virus uses various methods to notify you of all important events related to application operation (see section "Configuring the notification method" on page [123](#)). You can disable the delivery of notifications.

Regardless of whether notification delivery is enabled or disabled, information about events that occur during the operation of Kaspersky Anti-Virus is logged in an application operation report (see page [117](#)).

When you disable the notifications delivery, it does not impact the display of notification windows. To minimize the number of notification windows displayed on the screen, use the automatic protection mode (see section "Selecting a protection mode" on page [63](#)).

➤ *To disable notification delivery:*

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Notifications** subsection.
3. In the right part of the window, uncheck the **Enable events notifications** box.

## CONFIGURING THE NOTIFICATION METHOD

The application notifies you of events using the following methods:

- pop-up messages in the taskbar notification area;
- audio notifications;
- email messages.

You can configure an individual set of notification delivery methods for each type of event.

By default, critical notifications and notifications of application operation failures are accompanied by an audio signal. The Microsoft Windows sound scheme is used as the source of sound effects. You can modify the current scheme or disable sounds.

To allow Kaspersky Anti-Virus to notify you of events by email, you should adjust the email settings of notification delivery.

➤ *To select notifications delivery methods for various types of events:*

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Notifications** subsection.
3. In the right part of the window, check the **Enable events notifications** box and click the **Settings** button located under the box.
4. In the **Notifications** window that opens, check the boxes corresponding to how you want to be notified of various events: by email, with a pop-up message, or with an audio signal.

➤ *To modify the email settings for notification delivery:*

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Notifications** subsection.
3. In the right part of the window, check the **Enable email notifications** box and click the **Settings** button.
4. In the **Email notification settings** window that opens, specify the settings for sending notifications by email.

➤ *To configure the sound scheme used with notifications:*

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Notifications** subsection.
3. In the right part of the window, uncheck the **Enable audio notifications** box.

If you want to use the sound scheme of Microsoft Windows for notification of Kaspersky Anti-Virus events, check the **Use Windows Default sound scheme** box. If this box is unchecked, the sound scheme from previous Kaspersky Anti-Virus versions is used.

## DISABLING NEWS DELIVERY

➤ *To disable news delivery from the application settings window:*

1. Open the application settings window.
2. In the left part of the window, in the **Advanced Settings** section, select the **Appearance** subsection.

- In the right part of the window, uncheck the **Enable news notifications** box.

## KASPERSKY SECURITY NETWORK

To increase the efficiency of your computer's protection, Kaspersky Anti-Virus uses data received from users from all over the world. Kaspersky Security Network is designed for collecting this data.

The Kaspersky Security Network (KSN) is an infrastructure of online services that provides access to the online Knowledge Base of Kaspersky Lab, which contains information about the reputation of files, web resources, and software. Using data from the Kaspersky Security Network ensures a faster response time for Kaspersky Anti-Virus when encountering new types of threats, improves performance of some protection components, and reduces the risk of false positives.

User participation in Kaspersky Security Network enables Kaspersky Lab to gather real-time information about the types and sources of new threats, develop methods to neutralize them, and reduce the number of false positives.

Besides, participating in Kaspersky Security Network grants you access to information about reputation of various applications and websites.

When you participate in the Kaspersky Security Network, certain statistics collected while Kaspersky Anti-Virus protects your computer are sent to Kaspersky Lab automatically.

No private data is collected, processed, or stored.

Participating in the Kaspersky Security Network is voluntary. You should decide whether to participate when installing Kaspersky Anti-Virus; however, you can change your decision later.

### IN THIS SECTION:

Enabling and disabling participation in Kaspersky Security Network .....	<a href="#">124</a>
Verifying connection to Kaspersky Security Network .....	<a href="#">124</a>

## ENABLING AND DISABLING PARTICIPATION IN KASPERSKY SECURITY NETWORK

➤ *To participate in Kaspersky Security Network:*

- Open the application settings window.
- In the left part of the window, in the **Advanced Settings** section, select the **Feedback** subsection.
- In the right part of the window, check the **I agree to participate in Kaspersky Security Network** box.

## VERIFYING CONNECTION TO KASPERSKY SECURITY NETWORK

Connection to Kaspersky Security Network may be lost for the following reasons:

- your computer is not connected to the Internet;
- you do not participate in Kaspersky Security Network;
- your license for Kaspersky Anti-Virus is limited.

➤ *To test the connection to Kaspersky Security Network:*

1. Open the main application window.
2. In the top part of the window, click the **Cloud protection** button.
3. In the left part of the window that opens, the status of connection to Kaspersky Security Network is displayed.

# TESTING THE APPLICATION'S OPERATION

This section provides information about how to ensure that the application detects viruses and their modifications and performs the correct actions on them.

## IN THIS SECTION:

---

About the test file EICAR.....	<a href="#">126</a>
Testing the application's functioning using the test file EICAR .....	<a href="#">126</a>
About the types of the test file EICAR .....	<a href="#">127</a>

## ABOUT THE TEST FILE EICAR

You can make sure that the application detects viruses and disinfects infected files by using a *test file EICAR*. The test file EICAR has been developed by the European Institute for Computer Antivirus Research (EICAR) in order to test the functionality of anti-virus applications.

The test file EICAR is not a virus. The test file EICAR does not contain any program code that could damage your computer. However, a major part of anti-virus applications identify the test file EICAR as a virus.

The test file EICAR is not intended for testing the functionality of the heuristic analyzer or searching for malware at the system level (rootkits).

**Do not use real viruses to test the functionality of anti-virus applications! This may damage your computer.**

**Do not forget to resume the anti-virus protection of Internet traffic and files after you have finished with the test file EICAR.**

## TESTING THE APPLICATION'S FUNCTIONING USING THE TEST FILE EICAR

You can use the test file EICAR to test the Internet traffic protection, anti-virus protection of files, and computer scan.

**Do not forget to resume the anti-virus protection of Internet traffic and files after you have finished with the test file EICAR.**

◆ *To test the Internet traffic protection using the test file EICAR:*

1. You can download this test file from EICAR's official website at [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm).
2. Try to save the EICAR test file in any folder on your computer.

Kaspersky Anti-Virus informs you that a threat has been detected at the requested URL and blocks the attempt to save the object on the computer.

3. If necessary, you can use various types of the test file EICAR (see section "About the types of the test file EICAR" on page [127](#)).

➤ *To test the anti-virus protection of files using the test file EICAR or a modification of it:*

1. Pause anti-virus protection of Internet traffic and anti-virus protection of files on your computer.

When protection is paused, it is not recommended that you connect the computer to local networks or use removable devices to prevent harm to your computer caused by malware.

2. You can download this test file from EICAR's official website at [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm).
3. Save the EICAR test file in any folder on your computer.
4. Add one of the prefixes to the head of the EICAR test file (see section "About the types of the test file EICAR" on page 127).

You can use any text or hypertext editor to do this, for example, Notepad. To open Notepad, select **Start** → **All programs** → **Accessories** → **Notepad**.

5. Save the resulting file under a name reflecting the modification of the file EICAR; for example, add the DELE- prefix and save the file as eicar\_dele.com.
6. Resume anti-virus protection of Internet traffic and anti-virus protection of files on your computer.
7. Try to run the file that you have saved.

Kaspersky Anti-Virus informs you of a threat detected on the hard drive of your computer and performs the action specified in the settings of the anti-virus protection of files.

➤ *To test the virus scan using the test file EICAR or a modification of it:*

1. Pause anti-virus protection of Internet traffic and anti-virus protection of files on your computer.

When protection is paused, it is not recommended that you connect the computer to local networks or use removable devices to prevent harm to your computer caused by malware.

2. You can download this test file from EICAR's official website at [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm).
3. Add one of the prefixes to the head of the EICAR test file (see section "About the types of the test file EICAR" on page 127).

You can use any text or hypertext editor to do this, for example, Notepad. To open Notepad, select **Start** → **All programs** → **Accessories** → **Notepad**.

4. Save the resulting file under a name reflecting the modification of the test file EICAR; for example, add the DELE- prefix and save the file as eicar\_dele.com.
5. Start the scan of the file that you have saved.

Kaspersky Anti-Virus informs you of a threat detected on the hard drive of your computer and performs the action specified in the settings of the virus scan.

6. Resume anti-virus protection of Internet traffic and anti-virus protection of files on your computer.

## ABOUT THE TYPES OF THE TEST FILE EICAR

You can test the application's functioning by creating various modifications of the test file EICAR. The application detects the test file EICAR (or a modification of it) and assigns it a status depending on the results of the scan. The application takes specified actions on the test file EICAR if they had been selected in the settings of the component that has detected the test file EICAR.

The first column of the table (see the table below) contains prefixes that you can use when creating modifications of the test file EICAR. The second column lists all possible statuses assigned to the file, based on the results of the scan by the application. The third column indicates how the application processes files with the specified status.

Table 2. Modifications of the test file EICAR

Prefix	File status	File processing information
No prefix, standard test virus.	<b>Infected.</b> File contains code of a known virus. File cannot be disinfected.	The application identifies this file as a file containing a virus that cannot be disinfected.  The action set for infected files is applied to the file. By default, the application displays an on-screen notification that the file cannot be disinfected.
CURE-	<b>Infected.</b> File contains code of a known virus. File can be disinfected.	The file contains a virus that can be disinfected or deleted. The application disinfects the file; the text of the virus body is replaced with the word CURE.  The application displays an on-screen notification that a disinfected file has been detected.
DELE-	<b>Infected.</b> File contains code of a known virus. File cannot be disinfected.	The application identifies the file as a virus that cannot be disinfected, and deletes it.  The application displays an on-screen notification that the disinfected file has been deleted.
WARN-	<b>Potentially infected.</b> File contains code of an unknown virus. File cannot be disinfected.	File is potentially infected.  The application applies the action set for potentially infected files on the file. By default, the application displays an on-screen notification that a potentially infected file has been detected.
SUSP-	<b>Potentially infected.</b> File contains modified code of a known virus. File cannot be disinfected.	The application detected a partial correspondence of a section of file code with a section of code of a known virus. When a potentially infected file is detected, the application databases do not contain a description of the full code of the virus.  The application applies the action set for potentially infected files on the file. By default, the application displays an on-screen notification that a potentially infected file has been detected.
CORR-	<b>Corrupted.</b>	The application does not scan this type of file because its structure is damaged (for example, the file format is invalid). You can find the information that the file has been processed in the report on the application's operation.
ERRO-	<b>Scan error.</b>	An error occurred during the scan of a file. The application could not access the file, since the integrity of the file has been breached (for example, no end to a multivolume archive) or there is no connection to it (if the file is scanned on a network drive). You can find the information that the file has been processed in the report on the application's operation.

# CONTACTING THE TECHNICAL SUPPORT SERVICE

This section provides information about how to obtain technical support and what conditions should be met to receive help from the Technical Support Service.

## IN THIS SECTION:

---

How to get technical support .....	<a href="#">129</a>
Using the trace file and the AVZ script .....	<a href="#">129</a>
Technical support by phone .....	<a href="#">132</a>
Obtaining technical support via My Kaspersky Account .....	<a href="#">132</a>

## HOW TO GET TECHNICAL SUPPORT

If you do not find a solution to your problem in the application documentation or in one of the sources of information about the application (see section "Sources of information about the application" on page [11](#)), we recommend that you contact Kaspersky Lab's Technical Support Service. Technical Support Service specialists will answer any of your questions about installing and using the application. If the computer is infected, our specialists will help to fix any problems caused by malware.

Before contacting the Technical Support Service, please read the support rules (<http://support.kaspersky.com/support/rules>).

You can contact the Technical Support Service in one of the following ways:

- By telephone. This method allows you to consult with specialists from our Russian-language or international Technical Support Service.
- By sending a query from your Kaspersky Account on the Technical Support Service website. This method allows you to contact our specialists using the query form.

To qualify for technical support, you must be a registered user of a commercial version of Kaspersky Anti-Virus. Technical support is not available to users of trial versions of the application.

## USING THE TRACE FILE AND THE AVZ SCRIPT

After you notify Technical Support Service specialists of a problem encountered, they may ask you to create a report that should contain information about your operating system, and send it to the Technical Support Service. Also, Technical Support Service specialists may ask you to create a *trace file*. The trace file allows you to trace the process of executing the application's commands step-by-step and find out on which stage of the application's operation an error has occurred.

After Technical Support Service specialists analyze the data that you have sent, they can create an AVZ script and send it to you. Running AVZ scripts allows you to analyze active processes for malicious code, scan the system for malicious code, disinfect / delete infected files, and create reports on results of system scans.

## CREATING A SYSTEM STATE REPORT

➤ *To create a system state report:*

1. Open the main application window.
2. Click the **Support** link at the bottom of the main window to open the **Support** window, then follow the **Support Tools** link.
3. In the **Support Tools** window that opens, click the **Create system state report** button.

The system state report is created in HTML and XML formats and is saved in the archive sysinfo.zip. Once the information has been gathered, you can view the report.

➤ *To view the report:*

1. Open the main application window.
2. Click the **Support** link at the bottom of the main window to open the **Support** window, then follow the **Support Tools** link.
3. In the **Support Tools** window that opens, click the **View** button.
4. Open the sysinfo.zip archive which contains the report files.

## CREATING A TRACE FILE

➤ *To create a trace file:*

1. Open the main application window.
2. Click the **Support** link at the bottom of the main window to open the **Support** window, then follow the **Support Tools** link.
3. In the **Support Tools** window that opens, specify the trace level from the drop-down list in **Traces** section.

It is recommended that the required trace level be clarified by a Technical Support Service specialist. In the absence of guidance from the Technical Support Service, you are advised to set the trace level to **500**.

4. To start the trace process, click the **Enable** button.
5. Reconstruct the situation in which the problem occurred.
6. To stop the trace process, click the **Disable** button.

You can switch to uploading tracing results (see section "Sending data files" on page [130](#)) to Kaspersky Lab's server.

## SENDING DATA FILES

After you have created the trace files and the system state report, you need to send them to Kaspersky Lab Technical Support Service experts.

You will need a request number to upload data files to the Technical Support Service server. This number is available in your My Kaspersky Account on the Technical Support Service website if your request is active.

➤ *To upload the data files to the Technical Support Service server:*

1. Open the main application window.
2. Click the **Support** link at the bottom of the main window to open the **Support** window, then follow the **Support Tools** link.
3. In the **Support Tools** window that opens, in the **Actions** section, click the **Upload information for Technical Support Service to the server** button.

The **Uploading information for Technical Support Service to the server** window will open.

4. Check the boxes next to the trace files that you want to send to the Technical Support Service and click the **Send** button.

The **Request number** window will open.

5. Specify the number assigned to your request by contacting the Technical Support Service through My Kaspersky Account and click the **OK** button.

The selected data files are packed and sent to the Technical Support Service server.

If for any reason it is not possible to contact the Technical Support Service, the data files can be stored on your computer and later sent from My Kaspersky Account.

➤ *To save data files on a disk:*

1. Open the main application window.
2. Click the **Support** link at the bottom of the main window to open the **Support** window, then follow the **Support Tools** link.
3. In the **Support Tools** window that opens, in the **Actions** section, click the **Upload information for Technical Support Service to the server** button.

The **Uploading information for Technical Support Service to the server** window will open.

4. Check the boxes next to the trace files that you want to send to the Technical Support Service and click the **Send** button.

The **Request number** window will open.

5. Click the **Cancel** button and confirm saving the files on the disk by clicking the **Yes** button in the window that opens.

The archive saving window will open.

6. Specify the archive name and confirm saving.

The created archive can be sent to the Technical Support Service from My Kaspersky Account.

## AVZ SCRIPT EXECUTION

You are advised not to change the text of an AVZ script received from Kaspersky Lab experts. If problems occur during script execution, please contact the Technical Support Service (see section "How to get technical support" on page [129](#)).

➡ To run the AVZ script:

1. Open the main application window.
2. Click the **Support** link at the bottom of the main window to open the **Support** window, then follow the **Support Tools** link.
3. In the **Support Tools** window that opens, click the **Execute AVZ script** button.

If the script successfully executes, the Wizard closes. If an error occurs during script execution, the Wizard displays a message to that effect.

## TECHNICAL SUPPORT BY PHONE

If an urgent issue arises, you can call specialists from the Russian-speaking or international Technical Support Service by phone ([http://support.kaspersky.com/support/support\\_local](http://support.kaspersky.com/support/support_local)).

Before contacting the Technical Support Service, you should collect information (<http://support.kaspersky.com/support/details>) about your computer and anti-virus applications installed on it. This will allow our specialists to help you more quickly.

## OBTAINING TECHNICAL SUPPORT VIA MY KASPERSKY ACCOUNT

*My Kaspersky Account* is your personal area (<https://my.kaspersky.com>) on the Technical Support Service website.

To obtain access to My Kaspersky Account, you should go through the registration procedure on the registration page (<https://my.kaspersky.com/registration>). Enter your email address and a password to log in to My Kaspersky Account.

In My Kaspersky Account, you can perform the following actions:

- contact the Technical Support Service and Virus Lab;
- contact the Technical Support Service without using email;
- track the status of your request in real time;
- view a detailed history of your requests to the Technical Support Service;
- receive a copy of the key file if it has been lost or removed.

### Technical Support by email

You can send an online request to the Technical Support Service in Russian, English, German, French, or Spanish.

You should specify the following data in the fields of the online request form:

- request type;
- application name and version number;
- request description;
- customer ID and password;
- email address.

A specialist from the Technical Support Service sends an answer to your question to your My Kaspersky Account and to the email address that you have specified in your online request.

### Online request to the Virus Lab

Some requests should be sent to the Virus Lab instead of the Technical Support Service.

You can send requests of the following types to the Virus Lab:

- *Unknown malicious program* – you suspect that a file contains a virus but Kaspersky Anti-Virus has not identified it as infected.

Virus Lab specialists analyze malicious code sent. If they detect a previously unknown virus, they add a corresponding description to the database, which becomes available when updating anti-virus applications.

- *False alarm* – Kaspersky Anti-Virus classifies the file as a virus, yet you are sure that the file is not a virus.
- *Request for description of malicious program* – you want to receive the description of a virus detected by Kaspersky Anti-Virus, using the name of the virus.

You can also send requests to the Virus Lab from the page with the request form (<http://support.kaspersky.com/virlab/helpdesk.html>) without being registered in My Kaspersky Account. On this page, you do not have to specify the application activation code.

# APPENDIX

This section provides information that complements the document text.

## IN THIS SECTION:

---

Working with the application from the command line .....	<a href="#">134</a>
Kaspersky Anti-Virus notifications list.....	<a href="#">144</a>

## WORKING WITH THE APPLICATION FROM THE COMMAND LINE

You can work with Kaspersky Anti-Virus from the command line. The capability is provided to perform the following operations:

- activating the application;
- starting and stopping the application;
- starting and stopping application components;
- starting and stopping tasks;
- obtaining information on the current status of components and tasks, as well as their statistics;
- starting and stopping virus scan tasks;
- scanning selected objects;
- updating databases and software modules, rolling back updates;
- exporting and importing security settings;
- opening help files using command line syntax in general and for individual commands.

Command prompt syntax:

```
avp.com <command> [options]
```

You should access the application from the command line from the application installation folder or by specifying the full path to avp.com.

The list of commands used to control the application and its components is provided in the table below.

<b>START</b>	Starts a component or a task.
<b>STOP</b>	Stops a component or a task. The command can only be executed if the password assigned via the Kaspersky Anti-Virus interface is entered.
<b>STATUS</b>	Displays the current status of a component or task on the screen.
<b>STATISTICS</b>	Displays the statistics for a component or task on the screen.
<b>HELP</b>	Displays the list of commands and command syntax information.
<b>SCAN</b>	Scans objects for viruses.
<b>UPDATE</b>	Starts the application update.
<b>ROLLBACK</b>	Rolls back to the last Kaspersky Anti-Virus update made. The command can only be executed if the password assigned via the Kaspersky Anti-Virus interface is entered.
<b>EXIT</b>	Closes the application. The command can only be run if the password assigned via the application interface is entered.
<b>IMPORT</b>	Imports application protection settings. The command can only be executed if the password assigned via the Kaspersky Anti-Virus interface is entered.
<b>EXPORT</b>	Exports the application protection settings.

Each command requires its own specific set of settings.

### IN THIS SECTION:

Activating the application.....	<a href="#">136</a>
Starting the application.....	<a href="#">136</a>
Stopping the application.....	<a href="#">136</a>
Managing application components and tasks.....	<a href="#">136</a>
Virus scan .....	<a href="#">138</a>
Updating the application.....	<a href="#">140</a>
Rolling back the last update .....	<a href="#">141</a>
Exporting protection settings .....	<a href="#">141</a>
Importing protection settings .....	<a href="#">141</a>
Creating a trace file .....	<a href="#">142</a>
Viewing Help .....	<a href="#">142</a>
Return codes of the command line.....	<a href="#">142</a>

## ACTIVATING THE APPLICATION

You can activate Kaspersky Anti-Virus using a key file.

Command syntax:

```
avp.com ADDKEY <filename>
```

The table below describes the settings of command execution.

<b>&lt;filename&gt;</b>	Application key file name with the *.key extension.
-------------------------	---

### **Example:**

```
avp.com ADDKEY 1AA111A1.key
```

## STARTING THE APPLICATION

Command syntax:

```
avp.com
```

## STOPPING THE APPLICATION

Command syntax:

```
avp.com EXIT /password=<your_password>
```

A description of parameters is provided in the table below.

<b>&lt;your_password&gt;</b>	Application password specified in the interface.
------------------------------	--

Note that this command is not accepted without a password.

## MANAGING APPLICATION COMPONENTS AND TASKS

Command syntax:

```
avp.com <command> <profile|task_name> [/R[A]:<report_file>]
avp.com STOP <profile|task_name> /password=<your_password> [/R[A]:<report_file>]
```

Descriptions of commands and settings are given in the table below.

<b>&lt;command&gt;</b>	<p>You can manage Kaspersky Anti-Virus components and tasks from the command prompt with the following commands:</p> <p>START – start a protection component or a task.</p> <p>STOP – stop a protection component or a task.</p> <p>STATUS – display the current status of a protection component or a task.</p> <p>STATISTICS – output statistics to the screen for a protection component or a task.</p> <p>Note that the STOP command will not be accepted without a password.</p>
<b>&lt;profile task_name&gt;</b>	<p>You can specify any protection component of Kaspersky Anti-Virus, component module, on-demand scan or update task as the value for the <b>&lt;profile&gt;</b> setting (the standard values used by the application are shown in the table below).</p> <p>You can specify the name of any on-demand scan or update task as the value for the <b>&lt;task_name&gt;</b> setting.</p>

<your_password>	Application password specified in the interface.
/R[A]:<report_file>	<p><b>/R:&lt;report_file&gt;</b> – log only important events in the report.</p> <p><b>/RA:&lt;report_file&gt;</b> – log all events in the report.</p> <p>You can use an absolute or relative path to the file. If the setting is not defined, scan results are displayed on the screen, and all events are shown.</p>

In the <profile> setting, you should specify one of the values given in the table below.

<b>RTP</b>	<p>All protection components.</p> <p>The <b>avp.com START RTP</b> command runs all the protection components if the protection has been completely disabled.</p> <p>If the component has been disabled using the <b>STOP</b> command from the command prompt, it is not launched by the <b>avp.com START RTP</b> command. In order to start it, you should execute the <b>avp.com START &lt;profile&gt;</b> command with the name of the specific protection component entered for &lt;profile&gt;, for example, <b>avp.com START FM</b>.</p>
<b>pdm</b>	Proactive Defense.
<b>FM</b>	File Anti-Virus.
<b>EM</b>	Mail Anti-Virus.
<b>WM</b>	<p>Web Anti-Virus.</p> <p>Values for Web Anti-Virus subcomponents:</p> <p><b>httpscan (HTTP)</b> – scan HTTP traffic;</p> <p><b>sc</b> – scan scripts.</p>
<b>IM</b>	IM Anti-Virus.
<b>Updater</b>	Update.
<b>Rollback</b>	Rolling back the last update.
<b>Scan_My_Computer</b>	Scan.
<b>Scan_Objects</b>	Objects Scan.
<b>Scan_Quarantine</b>	Quarantine scan.
<b>Scan_Startup (STARTUP)</b>	Startup Objects Scan.
<b>Scan_Vulnerabilities (SECURITY)</b>	Vulnerability Scan.

Components and tasks started from the command prompt are run with the settings configured in the application interface.

#### Examples:

- *To enable File Anti-Virus, enter the following command:*

```
avp.com START FM
```

- *To stop a computer scan, enter the following command:*

```
avp.com STOP Scan_My_Computer /password=<your_password>
```

## VIRUS SCAN

Starting a scan of a certain area for viruses and processing malicious objects from the command prompt generally looks like this:

```
avp.com SCAN [<object scanned>] [<action>] [<file types>] [<exclusions>]
[<configuration file>] [<report settings>] [<advanced settings>]
```

To scan objects, you can also use the tasks created in the application by starting the one you need from the command line. The task will be run with the settings specified in the Kaspersky Anti-Virus interface.

A description of parameters is provided in the table below.

<p><b>&lt;object to scan&gt;</b> – this parameter gives the list of objects that are scanned for malicious code.</p> <p>The parameter may include several space-separated values from the list provided.</p>	
<p><b>&lt;files&gt;</b></p>	<p>List of paths to the files and folders to be scanned.</p> <p>You can enter an absolute or relative path to the file. Items on the list are separated by a space.</p> <p>Comments:</p> <ul style="list-style-type: none"> <li>• if the object name contains a space, it must be placed in quotation marks;</li> <li>• if reference is made to a specific folder, all files in this folder are scanned.</li> </ul>
<p><b>/MEMORY</b></p>	<p>RAM objects.</p>
<p><b>/STARTUP</b></p>	<p>Startup objects.</p>
<p><b>/MAIL</b></p>	<p>Mailboxes.</p>
<p><b>/REMDRIVES</b></p>	<p>All removable media drives.</p>
<p><b>/FIXDRIVES</b></p>	<p>All internal drives.</p>
<p><b>/NETDRIVES</b></p>	<p>All network drives.</p>
<p><b>/QUARANTINE</b></p>	<p>Quarantined objects.</p>
<p><b>/ALL</b></p>	<p>Full computer scan.</p>
<p><b>/@:&lt;filelist.lst&gt;</b></p>	<p>Path to a file containing a list of objects and catalogs to be scanned. You can enter an absolute or relative path to the file with the list. The path must be indicated without quotation marks even if it contains a space.</p> <p>The file with the list of objects should be in a text format. Each scan object should be listed on a separate line.</p> <p>You are advised to specify absolute paths to objects to be scanned. When specifying a relative path, you must specify the path relative to the executable file of an application, not relative to the file with the list of objects to be scanned.</p>
<p><b>&lt;action&gt;</b> – this parameter determines what action will be taken with malicious objects detected during the scan. If this parameter has not been defined, the default action is the one with the value of <b>/i8</b>.</p> <p>If you are working in automatic mode, then Kaspersky Anti-Virus automatically applies the action recommended by Kaspersky Lab's specialists when dangerous objects are detected. An action which corresponds to the <b>&lt;action&gt;</b> parameter value is ignored.</p>	
<p><b>/i0</b></p>	<p>Take no action with regard to the object; record information about it in the report.</p>

<b>/i1</b>	Disinfect infected objects; skip if disinfection fails.
<b>/i2</b>	Disinfect infected objects; skip if disinfection fails; do not delete infected objects from compound objects; delete infected compound objects with executable headers (sfx archives).
<b>/i3</b>	Disinfect infected objects; skip if disinfection fails; delete all compound objects completely if infected embedded files cannot be deleted.
<b>/i4</b>	Delete infected objects. Delete all compound objects completely if the infected parts cannot be deleted.
<b>/i8</b>	Prompt the user for action if an infected object is detected.
<b>/i9</b>	Prompt the user for action at the end of the scan.
<b>&lt;file types&gt;</b> – this parameter defines the file types that are subject to an anti-virus scan. By default, if this parameter is not defined, only infectable files by contents are scanned.	
<b>/fe</b>	Scan only infectable files by extension.
<b>/fi</b>	Scan only infectable files by contents.
<b>/fa</b>	Scan all files.
<b>&lt;exclusions&gt;</b> – this parameter defines objects that are excluded from the scan. The parameter may include several space-separated values from the list provided.	
<b>-e:a</b>	Do not scan archives.
<b>-e:b</b>	Do not scan email databases.
<b>-e:m</b>	Do not scan plain text emails.
<b>-e:&lt;filemask&gt;</b>	Do not scan objects which match the mask.
<b>-e:&lt;seconds&gt;</b>	Skip objects that are scanned for longer than the time specified in the <b>&lt;seconds&gt;</b> parameter.
<b>-es:&lt;size&gt;</b>	Skip objects whose size (in MB) exceeds the value specified in the <b>&lt;size&gt;</b> setting.  This setting is only available for compound files (such as archives).
<b>&lt;configuration file&gt;</b> – defines the path to the configuration file that contains the application settings for the scan. The configuration file is in text format and contains the set of command line parameters for the anti-virus scan. You can enter an absolute or relative path to the file. If this parameter is not defined, the values set in the application interface are used.	
<b>/C:&lt;file_name&gt;</b>	Use the settings' values specified in the <b>&lt;file_name&gt;</b> configuration file.
<b>&lt;report settings&gt;</b> – this parameter determines the format of the report on scan results. You can use an absolute or relative path to the file. If the setting is not defined, scan results are displayed on the screen, and all events are shown.	
<b>/R:&lt;report_file&gt;</b>	Log important events in this file only.
<b>/RA:&lt;report_file&gt;</b>	Log all events in this file.

<b>&lt;advanced settings&gt;</b> – settings that define the use of anti-virus scan technologies.	
<b>/iChecker=&lt;on off&gt;</b>	Enable / disable the use of iChecker technology.
<b>/iSwift=&lt;on off&gt;</b>	Enable / disable the use of iSwift technology.

**Examples:**

- Start a scan of memory, Startup programs, mailboxes, the directories My Documents and Program Files, and the file test.exe:

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents" "C:\Program Files" "C:\Downloads\test.exe"
```

- Scan the objects listed in the file object2scan.txt, using the configuration file scan\_setting.txt for the job. Use the scan\_settings.txt configuration file. When the scan is complete, create a report to log all events:

```
avp.com SCAN /MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

A sample configuration file:

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

## UPDATING THE APPLICATION

The syntax for updating the modules of Kaspersky Anti-Virus and application databases from the command line is as follows:

```
avp.com UPDATE [<update_source>] [/R[A]:<report_file>] [/C:<file_name>]
```

A description of parameters is provided in the table below.

<b>&lt;update_source&gt;</b>	HTTP or FTP server or network folder for downloading updates. The value for the parameter may be in the form of a full path to an update source or a URL. If a path is not selected, the update source will be taken from the application update settings.
<b>/R[A]:&lt;report_file&gt;</b>	<p><b>/R:&lt;report_file&gt;</b> – log only important events in the report.</p> <p><b>/RA:&lt;report_file&gt;</b> – log all events in the report.</p> <p>You can use an absolute or relative path to the file. If the setting is not defined, scan results are displayed on the screen, and all events are shown.</p>
<b>/C:&lt;file_name&gt;</b>	<p>Path to the configuration file that contains the Kaspersky Anti-Virus update settings.</p> <p>A configuration file is a file in plain text format containing a list of command-line parameters for an application update.</p> <p>You can enter an absolute or relative path to the file. If this parameter is not defined, the values for the settings in the application interface are used.</p>

**Examples:**

- Update application databases and record all events in a report:

```
avp.com UPDATE /RA:avbases_upd.txt
```

- Update the Kaspersky Anti-Virus modules using the settings of the updateapp.ini configuration file:

```
avp.com UPDATE /C:updateapp.ini
```

A sample configuration file:

```
"ftp://my_server/kav updates" /RA:avbases_upd.txt
```

## ROLLING BACK THE LAST UPDATE

Command syntax:

```
avp.com ROLLBACK [/R[A]:<report_file>] [/password=<your_password>]
```

A description of parameters is provided in the table below.

<b>/R[A]:&lt;report_file&gt;</b>	<p><b>/R:&lt;report_file&gt;</b> – log only important events in the report.</p> <p><b>/RA:&lt;report_file&gt;</b> – log all events in the report.</p> <p>You can use an absolute or relative path to the file. If the setting is not defined, scan results are displayed on the screen, and all events are shown.</p>
<b>&lt;your_password&gt;</b>	Application password specified in the interface.

Note that this command is not accepted without a password.

### Example:

```
avp.com ROLLBACK /RA:rollback.txt /password=<your_password>
```

## EXPORTING PROTECTION SETTINGS

Command syntax:

```
avp.com EXPORT <profile> <filename>
```

The table below describes the settings of command execution.

<b>&lt;profile&gt;</b>	<p>Component or task for which the settings are being exported.</p> <p>For the <b>&lt;profile&gt;</b> setting, you can use any value listed in the "Managing application components and tasks" Help section.</p>
<b>&lt;filename&gt;</b>	<p>Path to the file to which the Kaspersky Anti-Virus settings are being exported. An absolute or a relative path may be specified.</p> <p>The configuration file is saved in binary format (DAT), if no other format is specified, or it is not specified at all; it can be used later to export application settings onto other computers. The configuration file can also be saved as a text file. To do so, type the .txt extension in the file name. Note that you cannot import protection settings from a text file. This file can only be used to specify the main settings for Kaspersky Anti-Virus operation.</p>

### Example:

```
avp.com EXPORT RTP c:\settings.dat
```

## IMPORTING PROTECTION SETTINGS

Command syntax:

```
avp.com IMPORT <filename>[/password=<your_password>]
```

The table below describes the settings of command execution.

<b>&lt;filename&gt;</b>	Path to the file from which the Kaspersky Anti-Virus settings are imported. An absolute or a relative path may be specified.
<b>&lt;your_password&gt;</b>	Kaspersky Anti-Virus password specified in the application interface. Security parameters can only be imported from a binary file.

Note that this command is not accepted without a password.

**Example:**

```
avp.com IMPORT c:\settings.dat /password=<your_password>
```

## CREATING A TRACE FILE

Trace file creation may be required in case of problems in Kaspersky Anti-Virus operation. This will help Technical Support Service specialists to diagnose problems more accurately.

We only recommend creating trace files for troubleshooting a specific problem. Regularly enabling traces may slow down your computer and fill up your hard drive.

Command syntax:

```
avp.com TRACE [file] [on|off] [<trace_level>]
```

A description of parameters is provided in the table below.

<b>[on off]</b>	Enable / disable trace file creation.
<b>[file]</b>	Output trace to file.
<b>&lt;trace_level&gt;</b>	This setting can be a value from 0 (minimum level, only critical messages) to 700 (maximum level, all messages).  Technical Support will tell you what trace level you need when you contact Technical Support. If the level is not specified, we recommend setting the value to 500.

**Examples:**

➤ *To disable trace file creation:*

```
avp.com TRACE file off
```

➤ *To create a trace file to be sent to Technical Support with a maximum trace level of 500:*

```
avp.com TRACE file on 500
```

## VIEWING HELP

The following command is used to view help about the command line syntax:

```
avp.com [ /? | HELP ]
```

You can use one of the following commands to view help information about the syntax of a specific command:

```
avp.com <command> /?
```

```
avp.com HELP <command>
```

## RETURN CODES OF THE COMMAND LINE

This section describes the return codes of the command line (see table below). The general codes may be returned by any command from the command line. The return codes include general codes, as well as codes specific to a certain type of task.

<b>GENERAL RETURN CODES</b>	
<b>0</b>	Operation completed successfully.
<b>1</b>	Invalid setting value.
<b>2</b>	Unknown error.
<b>3</b>	Task completion error.
<b>4</b>	Task cancelled.
<b>VIRUS SCAN TASK RETURN CODES</b>	
<b>101</b>	All dangerous objects processed.
<b>102</b>	Hazardous objects detected.

# KASPERSKY ANTI-VIRUS NOTIFICATIONS LIST

This section provides information about notifications that Kaspersky Anti-Virus may display on the screen.

## IN THIS SECTION:

---

Notifications in any protection mode .....	<a href="#">144</a>
Notifications in interactive protection mode .....	<a href="#">149</a>

## NOTIFICATIONS IN ANY PROTECTION MODE

This section provides information about notifications that are displayed both in automatic and in interactive protection mode (see section "Selecting a protection mode" on page [63](#)).

## IN THIS SECTION:

---


Special treatment required .....	<a href="#">144</a>
Removable drive connected .....	<a href="#">145</a>
Unreliable certificate detected .....	<a href="#">145</a>
An application that may be exploited by an intruder in order to do harm to the user's computer or data, has been detected .....	<a href="#">146</a>
Quarantined file not infected .....	<a href="#">146</a>
New product version released .....	<a href="#">147</a>
Technical update released .....	<a href="#">147</a>
Technical update downloaded .....	<a href="#">147</a>
Downloaded technical update not installed .....	<a href="#">148</a>
License expired .....	<a href="#">148</a>
We recommend that you update the databases before scan .....	<a href="#">148</a>

## SPECIAL TREATMENT REQUIRED

When you detect a threat that is currently active in the system (for example, a malicious process in the RAM or in startup objects), a notification is displayed on the screen requesting the confirmation of a special advanced disinfection procedure.

The notification provides the following information:

- Description of the threat.
- Type of threat and name of the malicious object as listed in the Kaspersky Lab Virus Encyclopedia.

The  icon is displayed next to the name of the malicious object. Clicking the icon opens a window with information about the object. Clicking the [www.securelist.com](http://www.securelist.com) link in this window allows you to go to the Virus Encyclopedia website and obtain more detailed information about the threat posed by the object.

- File name of the malicious object, including the path to it.

You can select one of the following actions:

- **Yes, disinfect with reboot** – perform the special disinfection procedure (recommended).

When the disinfection is in progress, all applications are blocked except for trusted ones. When the disinfection is complete, the operating system will be restarted, so it is recommended that you save the changes that you have made and close all applications before starting the disinfection. After restarting your computer, you are advised to run a full virus scan.

- **Do not run** – the detected object or process will be processed according to the selected action.

To apply the selected action automatically every time such situation reoccurs, check the **Apply to all objects** box.

## REMOVABLE DRIVE CONNECTED

When a removable drive is connected to the computer, a notification appears on the screen.

You can select one of the following actions:

- **Quick Scan** – scan only files stored on the removable drive that can pose a potential threat.
- **Full Scan** – scan all files stored on the removable drive.
- **Do not scan** – do not scan the removable drive.

To apply the selected action to all removable drives that may be connected in the future, check the **Always perform in such cases** box.

## UNRELIABLE CERTIFICATE DETECTED

Kaspersky Anti-Virus verifies security of the connection established via the SSL protocol using an installed certificate. If an invalid certificate is detected when the connection to the server is attempted (for example, if the certificate is replaced by an intruder), a notification is displayed on screen.

The notification provides the following information:

- description of the threat;
- a link for viewing the certificate;
- probable causes of the error;
- the URL of the web resource.

You can select one of the following actions:


- **Yes, accept the untrusted certificate** – proceed with connecting to the web resource.
- **Deny certificate** – interrupt the connection with the website.

## AN APPLICATION THAT MAY BE EXPLOITED BY AN INTRUDER IN ORDER TO DO HARM TO THE USER'S COMPUTER OR DATA, HAS BEEN DETECTED

When Activity Monitor detects an application that may be exploited by an intruder in order to do harm to the user's computer or data, a notification is displayed on the screen.

The notification provides the following information:

- Description of the threat.
- Type and name of the application that may be exploited by an intruder in order to do harm to the user's computer or data.

The  icon is displayed next to the name of the application. Clicking the icon opens a window with information about the application.

- ID of the process and name of the application file, including the path to it.
- Link to the window with the application emergence log.

You can select one of the following actions:

- **Allow** – allow the application to run.
- **Quarantine** – close the application, move the application file to Quarantine where it poses no threat to your computer's security.

With further scans of Quarantine, the status of the object may change. For example, the object may be identified as infected and can be processed using an updated database. Otherwise, the object could be assigned the *not infected* status and then restored.

The status of a file moved to Quarantine can be changed to *not infected* at a next scan, but not earlier than three days after it is moved to Quarantine.

- **Terminate application** – interrupt the execution of the application.
- **Add to exclusions** – always allow the application to perform such actions in the future.

## QUARANTINED FILE NOT INFECTED

By default, Kaspersky Anti-Virus scans quarantined files after each update of the databases. If the scan of a quarantined file shows that it is not infected, a notification is displayed on the screen.

The notification provides the following information:

- a recommendation to restore the quarantined file;
- the name of the file, including the path to the folder in which it had been stored before it was moved to Quarantine.

You can select one of the following actions:

- **Restore** – restore the file by removing it from Quarantine and moving it to the folder in which this file had been stored before it was moved to Quarantine.
- **Cancel** – leave the file in Quarantine.

## NEW PRODUCT VERSION RELEASED

When a new version of Kaspersky Anti-Virus has been released and is available for downloading from Kaspersky Lab servers, a notification is displayed on the screen.

The notification provides the following information:

- a link to a window with detailed information about the newly released version of the application;
- the size of the installation package.

You can select one of the following actions:

- **Yes, download** – download the installation package of the new application version into the selected folder.
- **No** – cancel the installation package download.

If you do not want the notification of the new application version to be displayed on the screen in the future, check the **Do not inform of this update** box.

## TECHNICAL UPDATE RELEASED

When a technical update of Kaspersky Anti-Virus has been released and is available for downloading from Kaspersky Lab servers, a notification is displayed on the screen.

The notification provides the following information:

- the number of the application version installed on your computer;
- the number of the application version after the expected technical update;
- a link to a window with detailed information about the technical update;
- the size of the update file.

You can select one of the following actions:

- **Yes, download** – download the update file into the selected folder.
- **No** – cancel the update download. This option is available if the **Do not inform of this update** box is checked (see below).
- **No, remind later** – cancel the immediate download and receive a reminder to update later. This option is available if the **Do not inform of this update** box is unchecked (see below).

If you do not want this notification to be displayed on the screen in the future, check the **Do not inform of this update** box.

## TECHNICAL UPDATE DOWNLOADED

When downloading of the technical update of Kaspersky Anti-Virus from Kaspersky Lab servers is completed, a notification is displayed on the screen.

The notification provides the following information:

- the number of the application version after the technical update;
- a link to the update file.

You can select one of the following actions:

- **Yes, install** – install the update.

After the update is installed, you need to reboot your operating system.

- **Postpone installation** – cancel installation to perform it later.

## DOWNLOADED TECHNICAL UPDATE NOT INSTALLED

If a technical update of Kaspersky Anti-Virus has been downloaded but not installed on your computer, a notification is displayed on the screen.

The notification provides the following information:

- the number of the application version after the technical update;
- a link to the update file.

You can select one of the following actions:

- **Yes, install** – install the update.

After the update is installed, you need to reboot your operating system.

- **Postpone installation** – cancel installation to perform it later.

If you do not want notification of this update to be displayed on the screen in the future, check the **Do not ask until new version is available** box.

## LICENSE EXPIRED

When the trial license expires, Kaspersky Anti-Virus displays a notification on the screen.

The notification provides the following information:

- the length of the trial period;
- information about the application operation outcome (may include a link to more details).

You can select one of the following actions:

- **Yes, purchase** – selecting this option opens a browser window and loads the eStore web page where you can purchase the commercial license.
- **Cancel** – stop using the application. If you select this option, the application stops performing all of its main functions (virus scan, update, real-time protection, etc.).

## WE RECOMMEND THAT YOU UPDATE THE DATABASES BEFORE SCAN

If you initiate scan tasks before or during the first update of the databases, a notification is displayed on the screen.

The notification contains a recommendation to update the databases or wait until the update is completed before scan.

You can select one of the following actions:

- **Update databases before scan** – start updating the databases, after which the scan task starts automatically. This action option is unavailable if you have started the scan task before the first update of the databases.
- **Start scan after update** – wait until the update of the databases is completed and start the scan task automatically. This action option is unavailable if you have started the scan task during the first update of the databases.
- **Start scan now** – start the scan task without waiting for the update of the databases is completed.

## NOTIFICATIONS IN INTERACTIVE PROTECTION MODE

This section provides information about notifications that are displayed in interactive protection mode (see section "Selecting a protection mode" on page [63](#)).

### IN THIS SECTION:

---

A suspicious / malicious object detected .....	<a href="#">149</a>
Vulnerability detected .....	<a href="#">150</a>
Dangerous activity detected in the system .....	<a href="#">151</a>
Rolling back changes made by the application that may be exploited by an intruder in order to do harm to the user's computer or data .....	<a href="#">151</a>
Malicious application detected .....	<a href="#">152</a>
An application that may be exploited by intruders, is detected .....	<a href="#">152</a>
Suspicious / malicious link detected .....	<a href="#">153</a>
Dangerous object detected in traffic .....	<a href="#">154</a>
Attempt to access a phishing website detected .....	<a href="#">154</a>
Attempt to access the system registry detected .....	<a href="#">155</a>
Object cannot be disinfected .....	<a href="#">155</a>
Hidden process detected .....	<a href="#">155</a>


## A SUSPICIOUS / MALICIOUS OBJECT DETECTED

While File Anti-Virus, Mail Anti-Virus, or a virus scan is running, a notification is displayed on the screen if any of the following objects is detected:

- malicious object;
- object that contains the code of an unknown virus;
- object that contains the modified code of an unknown virus.

The notification provides the following information:

- Description of the threat.
- Type of threat and name of the malicious object as listed in the Kaspersky Lab Virus Encyclopedia.

The  icon is displayed next to the name of the malicious object. Clicking the icon opens a window with information about the object. Clicking the [www.securelist.com](http://www.securelist.com) link in this window allows you to go to the Virus Encyclopedia website and obtain more detailed information about the threat posed by the object.

- File name of the malicious object, including the path to it.

You can select one of the following responses to the object:

- **Disinfect** – attempt to disinfect the malicious object. This option is suggested if the threat is known.

Before disinfecting the object, a backup copy of it is created.

- **Quarantine** – move the object to Quarantine where it will pose no threat to your computer. This option is suggested if neither the threat nor any ways of disinfecting the object are known.

With further scans of Quarantine, the status of the object may change. For example, the object may be identified as infected and can be processed using an updated database. Otherwise, the object could be assigned the *not infected* status and then restored.

The status of a file moved to Quarantine can be changed to *not infected* at a next scan, but not earlier than three days after it is moved to Quarantine.

- **Delete** – delete the object. Before deleting the object, a backup copy of it is created.
- **Ignore / Block** – block access to the object, but perform no actions with regard to it; simply record information about it in a report.

You can return to the processing of skipped objects in the report window. However, you cannot postpone the processing of objects detected in email messages.

To apply the selected action to all threats of the same type detected in the current session of a protection component or task, check the **Apply to all objects** box. The current session is the time from when the component is started until it is disabled or Kaspersky Anti-Virus is restarted or the time from beginning a virus scan until it is complete.


If you are sure that the object detected it is not malicious, we recommend adding it to the trusted zone to keep the program from making repeat false positives when you use the object.

## VULNERABILITY DETECTED

A notification is displayed on the screen if a vulnerability is detected.

The notification contains the following information:

- Descriptions of the vulnerability.
- The name of the vulnerability as listed in the Kaspersky Lab Virus Encyclopedia.

The  icon is displayed next to the name. Clicking the icon opens a window with information about the vulnerability. Clicking [www.securelist.com](http://www.securelist.com) in the window takes you to the Virus Encyclopedia website, where you can obtain more detailed information about the vulnerability.

- File name of the vulnerable object, including the path to it.

You can select one of the following responses to the object:


- **Yes, fix** – eliminate the vulnerability.
- **Ignore** – take no actions on the vulnerable object.

## **DANGEROUS ACTIVITY DETECTED IN THE SYSTEM**

When Proactive Defense detects dangerous application activity on your system, a notification pops up.

The notification contains the following information:

- Description of the threat.
- Type of threat and name of the malicious object as listed in the Kaspersky Lab Virus Encyclopedia.

The  icon is displayed next to the name of the malicious object. Clicking the icon opens a window with information about the object. Clicking the [www.securelist.com](http://www.securelist.com) link in this window allows you to go to the Virus Encyclopedia website and obtain more detailed information about the threat posed by the object.

- ID of the process and name of the application file, including the path to it.

You can select one of the following actions:

- **Allow** – allow the application to run.
- **Quarantine** – close the application, move the application file to Quarantine where it poses no threat to your computer's security.

With further scans of Quarantine, the status of the object may change. For example, the object may be identified as infected and can be processed using an updated database. Otherwise, the object could be assigned the *not infected* status and then restored.

The status of a file moved to Quarantine can be changed to *not infected* at a next scan, but not earlier than three days after it is moved to Quarantine.

- **Terminate application** – interrupt the execution of the application.
- **Add to exclusions** – always allow the application to perform such actions in the future.


If you are sure that the program detected is not dangerous, we recommend adding it to the trusted zone to avoid Kaspersky Anti-Virus making repeat false positives when detecting it.

## **ROLLING BACK CHANGES MADE BY THE APPLICATION THAT MAY BE EXPLOITED BY AN INTRUDER IN ORDER TO DO HARM TO THE USER'S COMPUTER OR DATA**

We recommend that you roll back (discard) changes made by the application that may be exploited by an intruder in order to do harm to the user's computer or data. When such an application ceases its activity, a notification is displayed on the screen, requesting a rollback of changes.

The notification provides the following information:

- Requesting a rollback of changes made by the application that may be exploited by an intruder in order to do harm to the user's computer or data.
- Type and name of the application.

The  icon is displayed next to the name of the application. Clicking the icon opens a window with information about the application.

- ID of the process and name of the application file, including the path to it.

You can select one of the following actions:


- **Skip** – cancel changes rollback.
- **Yes, roll back** – roll back the changes made by the application.

## MALICIOUS APPLICATION DETECTED

When System Watcher detects an application whose behavior completely matches the activities of malicious applications, a notification is displayed on the screen.

The notification provides the following information:

- Description of the threat.
- Type and name of the malicious application.

The  icon is displayed next to the name of the application. Clicking the icon opens a window with information about the application.

- ID of the process and name of the application file, including the path to it.
- Link to the window with the application emergence log.

You can select one of the following actions:

- **Allow** – allow the application to run.
- **Quarantine** – close the application, move the application file to Quarantine where it poses no threat to your computer's security.

With further scans of Quarantine, the status of the object may change. For example, the object may be identified as infected and can be processed using an updated database. Otherwise, the object could be assigned the *not infected* status and then restored.

The status of a file moved to Quarantine can be changed to *not infected* at a next scan, but not earlier than three days after it is moved to Quarantine.


- **Terminate application** – interrupt the execution of the application.
- **Add to exclusions** – always allow the application to perform such actions in the future.

## AN APPLICATION THAT MAY BE EXPLOITED BY INTRUDERS, IS DETECTED

If File Anti-Virus, Mail Anti-Virus, or the virus scan task detects an application that may be exploited by intruders, a notification is displayed on the screen.

The notification provides the following information:

- Description of the threat.
- Type of the threat and name of the object as listed in the Kaspersky Lab Virus Encyclopedia.

The  icon is displayed next to the name of the object. Clicking the icon opens a window with information about the object. Clicking the [www.securelist.com](http://www.securelist.com) link in the window allows you to go to the Virus Encyclopedia website and obtain more details.

- Name of the object file, including the path to it.

You can select one of the following responses to the object:

- **Quarantine** – move the object to Quarantine where it will pose no threat to your computer. This option is suggested if neither a threat nor any ways of disinfecting the object are known.

With further scans of Quarantine, the status of the object may change. For example, the object may be identified as infected and can be processed using an updated database. Otherwise, the object could be assigned the *not infected* status and then restored.

The status of a file moved to Quarantine can be changed to *not infected* at a next scan, but not earlier than three days after it is moved to Quarantine.

- **Delete** – delete the object. Before deleting the object, a backup copy of it is created.
- **Delete archive** - delete password-protected archive.
- **Ignore / Block** – block access to the object, but perform no actions with regard to it; simply record information about it in a report.

You can return to the processing of skipped objects in the report window. However, you cannot postpone the processing of objects detected in email messages.

- **Add to exclusions** – create an exclusion rule for this threat type.

To apply the selected action to all threats of the same type detected in the current session of a protection component or task, check the **Apply to all objects** box. The current session is the time from when the component is started until it is disabled or Kaspersky Anti-Virus is restarted or the time from beginning a virus scan until it is complete.

If you are sure that the object detected it is not malicious, we recommend adding it to the trusted zone to keep the program from making repeat false positives when you use the object.

## SUSPICIOUS / MALICIOUS LINK DETECTED

When Kaspersky Anti-Virus detects an attempt to go to a website with suspicious or malicious content, a notification is displayed on the screen.

The notification provides the following information:

- description of the threat;
- the name of the application (browser) using which the website was loaded;
- the URL of the website or web page with suspicious or malicious content.

You can select one of the following actions:

- **Allow** – continues the website download.
- **Block** – blocks the website download.


To apply the selected action to all websites with threats of the same type detected in the current session of a protection component, check the **Apply to all objects** box. The current session is the time from the moment the component was started until the moment it was closed or Kaspersky Anti-Virus was restarted.

## DANGEROUS OBJECT DETECTED IN TRAFFIC

When Web Anti-Virus detects a malicious object in traffic, a special notification is displayed on the screen.

The notification contains the following information:

- A description of the threat or the actions performed by the application.
- Name of the application which performs the action.
- Type of threat and name of the malicious object as listed in the Kaspersky Lab Virus Encyclopedia.

The  icon is displayed next to the name of the malicious object. Clicking the icon opens a window with information about the object. Clicking the [www.securelist.com](http://www.securelist.com) link in this window allows you to go to the Virus Encyclopedia website and obtain more detailed information about the threat posed by the object.

- Object location (URL).

You can select one of the following actions:

- **Allow** – continue the object download.
- **Block** – block the object download from the web resource.

To apply the selected action to all threats of the same type detected in the current session of a protection component or task, check the **Apply to all objects** box. The current session is the time from the moment the component was started until the moment it was closed or Kaspersky Anti-Virus was restarted.

## ATTEMPT TO ACCESS A PHISHING WEBSITE DETECTED

When Kaspersky Anti-Virus detects an attempt to access a website that is or may be a phishing site, a notification is displayed on the screen.

The notification provides the following information:

- description of the threat;
- the URL of the website.

You can select one of the following actions:

- **Allow** – continues the website download.
- **Block** – blocks the website download.

To apply the selected action to all websites with threats of the same type detected in the current session of Kaspersky Anti-Virus, check the **Apply to all objects** box. The current session is the time from the moment the component was started until the moment it was closed or Kaspersky Anti-Virus was restarted.

## ATTEMPT TO ACCESS THE SYSTEM REGISTRY DETECTED

When Proactive Defense detects an attempt to access system registry keys, a notification pops up.

The notification provides the following information:

- the registry key being accessed;
- the file name of the process that initiated the attempt to access the registry keys, including the path to it.

You can select one of the following actions:

- **Allow** – allows the execution of the dangerous action once;
- **Block** – blocks the dangerous action once.

To apply the selected action to each attempt of obtaining access to registry keys, check the **Create a rule** box.


If you are sure that no activity of the application that attempted to access system registry keys is dangerous, add the application to the trusted application list.

## OBJECT CANNOT BE DISINFECTED

In some cases, an object cannot be disinfected: for example, if the file is so corrupted that the application is unable to remove malicious code from it and restore its integrity. Besides, the disinfection procedure cannot be applied to several types of malicious objects, such as Trojans. If an object cannot be disinfected, a notification is displayed on the screen.

The notification provides the following information:

- Description of the threat.
- Type of threat and name of the malicious object as listed in the Kaspersky Lab Virus Encyclopedia.

The  icon is displayed next to the name of the malicious object. Clicking the icon opens a window with information about the object. Clicking the [www.securelist.com](http://www.securelist.com) link in this window allows you to go to the Virus Encyclopedia website and obtain more detailed information about the threat posed by the object.

- File name of the malicious object, including the path to it.

You can select one of the following actions:

- **Delete** – delete the object. Before deleting the object, a backup copy of it is created.
- **Ignore / Block** – block access to the object, but perform no actions with regard to it; simply record information about it in a report.

You can return to the processing of skipped objects in the report window. However, you cannot postpone the processing of objects detected in email messages.

- **Add to exclusions** – create an exclusion rule for this threat type.


To apply the selected action to all threats of the same type detected in the current session of a protection component or task, check the **Apply to all objects** box. The current session is the time from when the component is started until it is disabled or Kaspersky Anti-Virus is restarted or the time from beginning a virus scan until it is complete.

## HIDDEN PROCESS DETECTED

If Proactive Defense detects a hidden process in the system, a notification is displayed on the screen.

The notification provides the following information:

- Description of the threat.
- Type and name of threat as listed in the Kaspersky Lab Virus Encyclopedia.

The  icon is displayed next to the name. Clicking the icon opens a window with information about the threat. Clicking [www.securelist.com](http://www.securelist.com) in the window takes you to the Virus Encyclopedia website, where you can obtain more detailed information about the threat.

- Name of the process file, including the path to it.

You can select one of the following actions:

- **Quarantine** – close the process and move the process file to Quarantine, where it poses no threat to your computer's security.

With further scans of Quarantine, the status of the object may change. For example, the object may be identified as infected and can be processed using an updated database. Otherwise, the object could be assigned the *not infected* status and then restored.

The status of a file moved to Quarantine can be changed to *not infected* at a next scan, but not earlier than three days after it is moved to Quarantine.

- **Terminate** – interrupt the process.
- **Allow** – allow the execution of the process.

To apply the selected action to all threats of the same type detected in the current session of Proactive Defense, check the **Apply to all such cases** box. The current session is the time from the moment the component was started until the moment it was closed or Kaspersky Anti-Virus was restarted.

If you are sure that the process detected is not dangerous, we recommend adding it to the trusted zone to avoid Kaspersky Anti-Virus making repeat false positives when detecting it.

# GLOSSARY

## A

### **ACTIVATING THE APPLICATION**

Switching the application into full-function mode. The user needs a license to activate the application.

### **ACTIVE LICENSE**

The license currently used for the operation of a Kaspersky Lab application. The license defines the expiration date for full functionality and the license policy for the application. The application cannot have more than one license with active status.

### **ADDITIONAL LICENSE**

A license that has been added for the operation of Kaspersky Lab application but has not been activated. The additional license enters into effect when the active license expires.

### **ADMINISTRATION SERVER CERTIFICATE**

A certificate which allows Administration Server authentication when connecting the Administration Console to it and when exchanging data with users' computers. The Administration Server certificate is created when Administration Server is installed and then stored in the folder %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert.

### **ALTERNATE NTFS STREAMS**

NTFS data streams (alternate data streams) designed to contain additional attributes or file information.

Each file in an NTFS file system is a set of streams. One of them contains the file content that one is able to view after opening the file, other streams (called alternate) are designed to contain meta information and ensure, for example, NTFS compatibility with other systems, such as an older file system by Macintosh called the Hierarchical File System (HFS). Streams can be created, deleted, stored separately, renamed, and even run as a process.

Alternate streams can be used by intruders to transfer data secretly, or to steal them from a computer.

### **APPLICATION MODULES**

Files included in the Kaspersky Lab installation package that are responsible for performing its main tasks. A particular executable module corresponds to each type of task performed by the application (real-time protection, on-demand scan, updates). By running a full scan of your computer from the main window, you initiate the execution of this task's module.

### **APPLICATION SETTINGS**

Application settings which are common for all task types, regulating the application's operation as a whole, such as application performance settings, report settings, and backup storage settings.

### **ARCHIVE**

File "containing" one or several other objects, which may also be archives.

### **AVAILABLE UPDATES**

A set of updates for Kaspersky Lab application modules, including critical updates accumulated over a certain period of time and changes to the application's architecture.

## B

### **BLACK LIST OF KEY FILES**

A database containing information on blacklisted Kaspersky Lab key files. The content of the black list file is updated along with the product databases.

## **BLOCKING AN OBJECT**

Denying access to an object from external applications. A blocked object cannot be read, executed, changed, or deleted.

## **BOOT VIRUS**

A virus that infects the boot sectors of a computer's hard drive. The virus forces the system to load it into memory during reboot and to direct control to the virus code instead of the original boot loader code.

## **C**

### **COMPRESSED FILE**

An archive file that contains a decompression program and instructions for the operating system for executing it.

## **D**

### **DANGEROUS OBJECT**

An object containing a virus. You are advised not to access these objects, because it may result in infection of your computer. Once an infected object is detected, we recommend that you disinfect it using one of Kaspersky Lab's applications, or delete it if disinfection is not possible.

### **DATABASE OF PHISHING WEB ADDRESSES**

List of web addresses which are defined as phishing by Kaspersky Lab specialists. The database is regularly updated and is part of the Kaspersky Lab application.

### **DATABASE OF SUSPICIOUS WEB ADDRESSES**

List of web addresses whose content can be considered to be potentially dangerous. The list was created by Kaspersky Lab specialists. It is regularly updated and is included in the Kaspersky Lab application package.

### **DATABASE UPDATE**

One of the functions performed by a Kaspersky Lab application that enables it to keep protection current. In doing so, the databases are downloaded from the Kaspersky Lab update servers onto the computer and are automatically connected to the application.

### **DATABASES**

Databases created by Kaspersky Lab's experts and containing a detailed description of all current threats to computer security, as well as methods used for their detection and disinfection. These databases are constantly updated by Kaspersky Lab as new threats appear.

### **DELETING AN OBJECT**

The method of processing objects which ends in it being physically deleted from its original location (hard drive, folder, network resource). We recommend that this method be applied to dangerous objects which, for whatever reason, cannot be disinfecting.

### **DISINFECTING OBJECTS ON RESTART**

A method of processing infected objects that are being used by other applications at the moment of disinfection. Consists of creating a copy of the infected object, disinfecting the copy created, and replacing the original infected object with the disinfected copy after the next system restart.

### **DISK BOOT SECTOR**

A boot sector is a particular area on a computer's hard drive, floppy, or other data storage device. It contains information on the disk's file system and a boot loader program that is responsible for starting the operating system.

There exist a number of viruses that infect boot sectors, which are thus called boot viruses. The Kaspersky Lab application allows scanning of boot sectors for viruses and disinfecting them if an infection is found.

## **DOMAIN NAME SERVICE (DNS)**

A distributed system for converting the name of a host (a computer or other network device) to an IP address. DNS functions in TCP/IP networks. As a special case, DNS can also store and process reverse requests and determine the name of a host by its IP address (PTR record). Resolution of DNS names is usually carried out by network applications, not by users.

## **DUAL-HOMED GATEWAY**

Computer equipped with two network adapters (each of which is connected to a different network) which transfers data from one network to the other.

## **E**

### **EVENT SEVERITY LEVEL**

Description of an event logged during the operation of the Kaspersky Lab application. There are four severity levels:

- **Critical event.**
- **Functional failure.**
- **Warning.**
- **Information message.**

Events of the same type may have different severity levels, depending on the situation when the event occurred.

### **EXCLUSION**

An Exclusion is an object excluded from the scan by a Kaspersky Lab application. You can exclude files of certain formats, file masks, a certain area (for example, a folder or a program), application processes, or objects by threat type, according to the Virus Encyclopedia classification from the scan. Each task can be assigned a set of exclusions.

## **F**

### **FALSE ALARM**

A situation when a Kaspersky Lab application considers a non-infected object to be infected because its code is similar to that of a virus.

### **FILE MASK**

Representation of a file name and extension using wildcards. The two standard wildcards used in file masks are \* and ?, where \* represents any number of any characters and ? stands for any single character. Using these wildcards, you can represent any file. Note that the name and extension are always separated by a period.

## **H**

### **HARDWARE PORT**

Socket on a hardware component of a computer in which a cable or a plug can be connected (LPT port, serial port, USB port).

### **HEADER**

The information in the beginning of a file or a message, which is comprised of low-level data on file (or message) status and processing. In particular, the email message header contains such data as information about the sender and recipient and the date.

## HEURISTIC ANALYZER

A technology designed for detecting threats that cannot be identified using the Kaspersky Lab application databases. It allows detection of objects suspected of being infected with an unknown virus or a new modification of known viruses.

The use of a heuristic analyzer detects up to 92% of threats. This mechanism is fairly effective and very rarely leads to false positives.

Files detected by the heuristic analyzer are considered suspicious.

## I

## iCHECKER TECHNOLOGY

iChecker is a technology that increases the speed of anti-virus scans by excluding objects that have remained unchanged since their last scan, provided that the scan parameters (the anti-virus database and settings) have not changed. The information for each file is stored in a special database. This technology is used in both real-time protection and on-demand scan modes.

For example, you have an archive file that was scanned by the Kaspersky Lab application and assigned not infected status. The next time the application will skip this archive unless it has been altered or the scan settings have been changed. If you altered the archive content by adding a new object to it, modified the scan settings, or updated the anti-virus database, the archive is re-scanned.

Limitations of iChecker technology:

- this technology does not work with large files, since it is faster to scan a file than check whether it was modified since it was last scanned;
- the technology supports a limited number of formats (**EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR**).

## INCOMPATIBLE APPLICATION

An antivirus application from a third-party developer or a Kaspersky Lab application that does not support management through Kaspersky Anti-Virus.

## INFECTED OBJECT

Object containing a malicious code. It is detected when a section of the object's code completely matches a section of the code of a known threat. Kaspersky Lab does not recommend using such objects since they may infect your computer.

## INPUT/OUTPUT PORT

Used in processors (such as Intel) for exchanging data with hardware components. The input/output port is associated with a certain hardware component and allows applications to address it for data exchange.

## INSTALLATION USING A LOGON SCRIPT

A method of remote installation of Kaspersky Lab applications which allows the startup of the remote installation task to be assigned to an individual user account (or to several user accounts). Registering a user in a domain leads to an attempt to install the application on the client computer on which the user has been registered. This method is recommended for installing the applications on computers running under Microsoft Windows 98 / Me operating systems.

## INTERCEPTOR

Subcomponent of the application responsible for scanning specific types of email. The set of interceptors specific to your installation depends on what role or what combination of roles the application is being deployed for.

## INTERNET PROTOCOL (IP)

The basic protocol for the Internet, used without change since the time of its development in 1974. It performs basic operations for transmitting data from one computer to another and serves as the foundation for higher-level protocols like TCP and UDP. It manages connection and error processing. Technologies such as NAT and masking make it possible to

hide a large number of private networks using a small number of IP addresses (or even one address), which makes it possible to meet the demands of the constantly growing Internet using the relatively restricted IPv4 address space.

## K

### **KASPERSKY LAB'S UPDATE SERVERS**

A list of Kaspersky Lab's HTTP and FTP servers from which the application downloads databases and module updates to your computer.

### **KASPERSKY SECURITY NETWORK**

The Kaspersky Security Network (KSN) is an infrastructure of online services that provides access to the online Knowledge Base of Kaspersky Lab, which contains information about the reputation of files, web resources, and software. Using data from the Kaspersky Security Network ensures a faster response time for Kaspersky Anti-Virus when encountering new types of threats, improves performance of some protection components, and reduces the risk of false positives.

### **KEY FILE**

A file with the KEY extension, which is your personal "key" and is necessary for working with the Kaspersky Lab application. A key file is included with the product if you purchased it from Kaspersky Lab distributors, or is emailed to you if you purchased the product online.

## L

### **LICENSE VALIDITY PERIOD**

The period of time during which you are able to use all features of your Kaspersky Lab application. The license validity period generally runs for one calendar year from the date of installation. After the license expires, the application has reduced functionality. You will not be able to update the application databases.

### **LIST OF ALLOWED URLS**

A list of masks and addresses of web resources to which access is not blocked by the Kaspersky Lab application. The list of addresses is created by the user during application settings configuration.

### **LIST OF BLOCKED URLS**

A list of masks and addresses of web resources, access to which is blocked by the Kaspersky Lab application. The list of addresses is created by the user during application settings configuration.

### **LIST OF TRUSTED URLS**

A list of masks and addresses of web resources whose content the user trusts. A Kaspersky Lab application does not scan web pages corresponding to a list item for the presence of malicious objects.

### **LIST OF WEB ADDRESSES TO BE CHECKED**

A list of masks and addresses of web resources which are mandatorily scanned for malicious objects by the Kaspersky Lab application.

## M

### **MEMORY DUMP**

Content of the working memory of a process or the entire RAM of the system at a specified moment of time.

### **MONITORED OBJECT**

A file transferred via HTTP, FTP, or SMTP protocols across the firewall and sent to a Kaspersky Lab application to be scanned.

## **MOVING OBJECTS TO QUARANTINE**

A method of processing a potentially infected object by blocking access to the file and moving it from its original location to the Quarantine folder, where the object is saved in encrypted form, which rules out the threat of infection.

## **N**

### **NETWORK PORT**

A TCP and UDP parameter that determines the destination of data packets in IP format that are transmitted to a host over a network and makes it possible for various programs running on a single host to receive data independently of each other. Each program processes data received via a certain port (this is sometimes referred to as the program "listening" to that port).

For some common network protocols, there are usually standard port numbers (for example, web servers usually receive HTTP requests on TCP port 80); however, generally, a program can use any protocol on any port. Possible values: 1 to 65535.

### **NOTIFICATION TEMPLATE**

A template based on which a notification about infected objects detected by a scan is generated. A notification template includes a combination of settings regulating the mode of notification, the means of distribution, and the text of messages to be sent.

## **O**

### **OLE OBJECT**

An attached object or an object embedded into another file. The Kaspersky Lab application allows scanning of OLE objects for viruses. For example, if you insert a Microsoft Office Excel table into a Microsoft Office Word document, the table is scanned as an OLE object.

### **OBJECT DISINFECTION**

A method used for processing infected objects that results in complete or partial recovery of data or the decision that the objects cannot be disinfected. Objects are disinfected using the database records. Part of the data may be lost during disinfection.

### **OBSCENE MESSAGE**

Email message containing offensive language.

## **P**

### **PHISHING**

A kind of Internet fraud which consists of sending email messages with the purpose of stealing confidential information - as a rule, various financial data.

### **POTENTIALLY INFECTABLE OBJECT**

An object which, due to its structure or format, can be used by intruders as a "container" to store and distribute a malicious object. As a rule, they are executable files, for example, files with the extensions COM, EXE, DLL, etc. The risk of penetration of malicious code into such files is fairly high.

### **POTENTIALLY INFECTED OBJECT**

An object that contains modified code of a known virus or code that resembles code of a virus, but is not yet known to Kaspersky Lab. Potentially infected files are detected using a heuristic analyzer.

### **PROTECTION STATE**

The current status of protection, summarizing the degree of security of the computer.

**PROTOCOL**

A clearly defined and standardized set of rules governing the interaction between a client and a server. Well-known protocols and the services associated with them include HTTP (WWW), FTP, and NNTP (news).

**PROXY SERVER**

A computer network service which allows users to make indirect requests to other network services. First, a user connects to a proxy server and requests a resource (e.g., a file) located on another server. Then the proxy server either connects to the specified server and obtains the resource from it or returns the resource from its own cache (if the proxy has its own cache). In some cases, a user's request or a server's response can be modified by the proxy server for certain purposes.

**Q****QUARANTINE**

A certain folder where all potentially infected objects which were detected during scans or by real-time protection are placed.

**R****REAL-TIME PROTECTION**

The application's operating mode under which objects are scanned for the presence of malicious code in real time.

The application intercepts all attempts to open any object (read, write, or execute) and scans the object for threats. Uninfected objects are passed on to the user; objects containing threats or suspected of containing them are processed pursuant to the task settings (they are disinfected, deleted or quarantined).

**RECOMMENDED LEVEL**

The level of security based on application settings recommended by Kaspersky Lab experts and providing an optimal level of protection for your computer. This level is set to be used by default.

**RESTORATION**

Moving an original object from Quarantine or Backup to the folder where it was originally found before being moved to Quarantine, disinfected, or deleted, or to a different folder specified by the user.

**ROOTKIT**

An application or a set of applications developed for masking traces of an intruder or malware in the system.

In Windows-based systems, rootkit usually means a program that penetrates in the system and intercepts system functions (Windows API). First of all, intercepting and modifying low-level API functions allow such program to mask its presence in the system in a quite sophisticated manner. Besides, a rootkit may, as a rule, mask the presence of any processes, folders and files on the disk, and registry keys if they are described in the rootkit's configuration. Many rootkits install their own drivers and services in the system (they also are "invisible").

**S****SCRIPT**

A small computer program or an independent part of a program (function) which, as a rule, has been developed to execute a small specific task. It is most often used with programs embedded into hypertext. Scripts are run, for example, when you open a certain website.

If real-time protection is enabled, the application tracks the launching of scripts, intercepts them, and scans them for viruses. Depending on the results of the scan, you may block or allow the execution of a script.

**SECURITY LEVEL**

The security level is defined as a pre-set component configuration.

## SOCKS

Proxy server protocol that allows establishment of a point-to-point connection between computers in the internal and external networks.

## STARTUP OBJECTS

The set of programs needed to start and correctly operate the operating system and software installed on your computer. These objects are executed every time the operating system is started. There are viruses capable of infecting such objects specifically, which may lead, for example, to blocking of operating system startup.

## SUBNET MASK

The subnet mask (also known as netmask) and network address determine the addresses of computers on a network.

## SUSPICIOUS MESSAGE

A message that cannot be unambiguously considered spam, but seems suspicious when scanned (e.g., certain types of mailings and advertising messages).

## SUSPICIOUS OBJECT

An object that contains modified code of a known virus or code that resembles code of a virus, but is not yet known to Kaspersky Lab. Suspicious objects are detected using the heuristic analyzer.

## T

### TASK

Functions performed by Kaspersky Lab's application are implemented as tasks, such as: **Real-time file protection**, **Full computer scan**, **Database update**.

### TASK SETTINGS

Application settings which are specific for each task type.

### TRACES

Running the application in debugging mode; after each command is executed, the application is stopped, and the result of this step is displayed.

### TRAFFIC SCAN

A real-time scan using information from the latest version of the databases for objects transmitted via all protocols (for example, HTTP, FTP, etc.).

### TRUSTED PROCESS

A program process, whose file operations are not monitored by Kaspersky Lab's application in real-time protection mode. In other words, no objects run, open, or saved by the trusted process are scanned.

## U

### UNKNOWN VIRUS

A new virus about which there is no information in the databases. Generally, unknown viruses are detected by the application in objects using the heuristic analyzer, and those objects are classified as potentially infected.

### UPDATE

The procedure of replacing/adding new files (databases or application modules) retrieved from the Kaspersky Lab update servers.

### UPDATE PACKAGE

File package for updating the software. It is downloaded from the Internet and installed on your computer.

**URGENT UPDATES**

Critical updates to Kaspersky Lab application modules.

**V****VIRUS ACTIVITY THRESHOLD**

The maximum permissible level of a specific type of event over a limited time period that, when exceeded, is considered to be excessive virus activity and a threat of a virus outbreak. This feature is highly significant during virus outbreaks and enables an administrator to react in a timely fashion to threats of virus outbreaks that arise.

**VIRUS OUTBREAK**

A series of deliberate attempts to infect a computer with a virus.

**VIRUS OUTBREAK COUNTER**

A template based on which a notification of a virus outbreak threat is generated. A virus outbreak counter includes a combination of settings which determine the virus activity threshold, means of spreading, and the text in messages sent.

# KASPERSKY LAB ZAO

Kaspersky Lab software is internationally renowned for its protection against viruses, malware, spam, network and hacker attacks, and other threats.

In 2008, Kaspersky Lab was rated among the world's top four leading vendors of information security software solutions for end users (IDC Worldwide Endpoint Security Revenue by Vendor). Kaspersky Lab is the preferred developer of computer protection systems among home users in Russia, according to the COMCON survey "TGI-Russia 2009".

Kaspersky Lab was founded in Russia in 1997. Today, it is an international group of companies headquartered in Moscow with five regional divisions that manage the company's activity in Russia, Western and Eastern Europe, the Middle East, Africa, North and South America, Japan, China, and other countries in the Asia-Pacific region. The company employs more than 2000 qualified specialists.

**Products.** Kaspersky Lab's products provide protection for all systems—from home computers to large corporate networks.

The personal product range includes anti-virus applications for desktop, laptop, and pocket computers, and for smartphones and other mobile devices.

Kaspersky Lab delivers applications and services to protect workstations, file and web servers, mail gateways, and firewalls. Used in conjunction with Kaspersky Lab's centralized management system, these solutions ensure effective automated protection for companies and organizations against computer threats. Kaspersky Lab's products are certified by the major test laboratories, are compatible with the software of many suppliers of computer applications, and are optimized to run on many hardware platforms.

Kaspersky Lab's virus analysts work around the clock. Every day they uncover thousands of new computer threats, create tools to detect and disinfect them, and include them in the databases used by Kaspersky Lab applications. *Kaspersky Lab's Anti-Virus database is updated hourly; and the Anti-Spam database every five minutes.*

**Technologies.** Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky Lab. It is no coincidence that many other developers use the Kaspersky Anti-Virus kernel in their products, including: SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Israel), Clearswift (UK), CommuniGate Systems (USA), Critical Path (Ireland), D-Link (Taiwan), M86 Security (USA), GFI (Malta), IBM (USA), Juniper Networks (USA), LANdesk (USA), Microsoft (USA), NETASQ (France), NETGEAR (USA), Parallels (Russia), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Taiwan). Many of the company's innovative technologies are patented.

**Achievements.** Over the years, Kaspersky Lab has won hundreds of awards for its services in combating computer threats. For example, in 2010 Kaspersky Anti-Virus was given several top Advanced+ awards after a series of tests held by AV-Comparatives, a renowned Austrian anti-virus lab. But Kaspersky Lab's main achievement is the loyalty of its users worldwide. The company's products and technologies protect more than 300 million users, and its corporate clients number more than 200,000.

Kaspersky Lab official site:

<http://www.kaspersky.com>

Virus Encyclopedia:

<http://www.securelist.com>

Anti-Virus Lab:

[newvirus@kaspersky.com](mailto:newvirus@kaspersky.com) (only for sending probably infected files in archive format)

<http://support.kaspersky.com/virlab/helpdesk.html> (for queries addressed to virus analysts)

Kaspersky Lab web forum:

<http://forum.kaspersky.com>

# INFORMATION ABOUT THIRD-PARTY CODE

Information about third-party code is contained in a file named legal\_notices.txt and stored in the application installation folder.

# INDEX

## A

Application self-defense ..... 108

## B

Browser Configuration ..... 115

## C

Computer performance ..... 106

## D

Database of phishing web addresses  
    IM Anti-Virus ..... 95  
    Web Anti-Virus ..... 90  
Disabling / enabling real-time protection ..... 39

## E

EICAR ..... 125

## F

File Anti-Virus  
    heuristic analysis ..... 80  
    pausing ..... 78  
    protection scope ..... 78  
    response to a threat ..... 81  
    scan mode ..... 80  
    scan of compound files ..... 81  
    scan optimization ..... 82  
    scan technology ..... 81  
    security level ..... 80

## H

Heuristic analysis  
    File Anti-Virus ..... 80  
    Mail Anti-Virus ..... 85  
    Web Anti-Virus ..... 92

## I

IM Anti-Virus  
    database of phishing web addresses ..... 95  
    protection scope ..... 95  
Installation folder ..... 19

## K

Kaspersky URL Advisor  
    Web Anti-Virus ..... 91

## L

License  
    activating the application ..... 42  
    End User License Agreement ..... 27  
License renewal ..... 43

**M**

Mail Anti-Virus	
attachment filtering .....	86
heuristic analysis .....	85
protection scope .....	84
response to a threat.....	86
scanning of compound files .....	86
security level.....	89

**N**

Network	
encrypted connections.....	100
monitored ports.....	102
Notifications.....	44
delivery of notifications using email .....	122
disabling .....	122
disabling the audio signal .....	122
notification types.....	122

**P**

Proactive Defense	
dangerous activity list .....	97
dangerous activity monitoring rule .....	97
group of trusted applications.....	96
Protection scope	
File Anti-Virus .....	78
IM Anti-Virus .....	95
Mail Anti-Virus .....	84
Web Anti-Virus.....	93

**Q**

Quarantine and Backup.....	109
----------------------------	-----

**R**

Reports	
events search .....	118
filtering .....	118
saving to file.....	119
selecting a component or a task .....	117
view .....	55
Rescue Disk.....	52
Response to a threat	
File Anti-Virus .....	81
Mail Anti-Virus .....	86
virus scan .....	69
Web Anti-Virus.....	90
Restoring the default settings.....	55
Restricting access to the application .....	63

**S**

Scan	
account.....	69
action with regard to a detected object .....	69
automatic startup of a skipped task .....	67
scan optimization.....	70
scan technologies.....	68
scanning of compound files .....	70
schedule .....	67
security level.....	66
type of objects to scan.....	69

vulnerability scan .....	72
Schedule	
update.....	75
virus scan .....	67
Security level	
File Anti-Virus .....	80
Mail Anti-Virus .....	89
Web Anti-Virus.....	89
<b>T</b>	
The context menu .....	30
The main application window .....	31
The taskbar notification area icon .....	29
Traces	
creating a trace file .....	129
uploading tracing results.....	129
Trusted zone	
exclusion rules.....	104
trusted applications.....	104
<b>U</b>	
Uninstallation	
application .....	25
Update	
proxy server.....	76
regional settings .....	74
rolling back the last update.....	76
Updating	
from a local folder .....	74
update source.....	73
<b>V</b>	
Virtual Keyboard.....	48
<b>W</b>	
Web Anti-Virus	
database of phishing web addresses .....	90
heuristic analysis .....	92
Kaspersky URL Advisor.....	91
protection scope .....	93
response to a threat.....	90
scan optimization.....	93
security level.....	89