

Kaspersky Internet Security 2013

KASPERSKY **lab**

USER GUIDE

APPLICATION VERSION: 13.0

Dear User!

Thank you for choosing our product. We hope that this document will help you in your work and will provide answers regarding this software product.

Attention! 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 result in civil, administrative or criminal liability by 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 graphic images related to it, may only be used for informational, non-commercial, and personal purposes.

Kaspersky Lab reserves the right to amend this document without additional notification. You can find the latest version of this document at 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.

Document revision date: 5/16/2012

© 2012 Kaspersky Lab ZAO. All Rights Reserved.

<http://www.kaspersky.com>
<http://support.kaspersky.com>

TABLE OF CONTENTS

ABOUT THIS GUIDE	6
In this guide	6
Document conventions	7
SOURCES OF INFORMATION ABOUT THE APPLICATION.....	9
Sources of information for independent research	9
Discussing Kaspersky Lab applications on the Forum.....	10
Contacting the Sales Department.....	10
Contacting Technical Writing and Localization Unit by email.....	10
KASPERSKY INTERNET SECURITY.....	11
What's new	11
Distribution kit.....	11
Main application features.....	12
Service for users.....	14
Hardware and software requirements.....	14
INSTALLING AND REMOVING THE APPLICATION.....	15
Standard installation procedure	15
Step 1. Finding a newer version of the application.....	16
Step 2. Starting the application installation	16
Step 3. Reviewing the License Agreement	16
Step 4. Kaspersky Security Network Data Collection Statement	17
Step 5. Installation	17
Step 6. Completing installation.....	17
Step 7. Activating the application.....	18
Step 8. Registering a user.....	18
Step 9. Completing the activation	18
Updating the previous version of Kaspersky Internet Security.....	19
Step 1. Finding a newer version of the application.....	19
Step 2. Starting the application installation	20
Step 3. Reviewing the License Agreement	20
Step 4. Kaspersky Security Network Data Collection Statement	20
Step 5. Installation	20
Step 6. Completing installation.....	21
Non-standard installation scenarios.....	21
Removing the application	22
Step 1. Saving data for future use.....	22
Step 2. Confirming application removal.....	22
Step 3. Removing the application. Completing removal.....	23
APPLICATION LICENSING	24
About the End User License Agreement.....	24
About the license.....	24
About the activation code	25
About data provision.....	25
SOLVING TYPICAL TASKS.....	27
Activating the application.....	28

Acquiring and renewing a license	28
Managing application notifications	29
Assessing the computer protection status and resolving security issues	29
Updating databases and application modules	31
Scanning critical areas of your computer for viruses	31
Full scan of the computer for viruses	31
Scanning a file, folder, disk, or another object for viruses	32
Scanning probably infected objects	33
Restoring an object deleted or disinfected by the application	33
Recovering the operating system after infection	34
Scanning email and filtering attachments in email messages	36
Blocking unwanted email (spam)	37
Scanning the computer for vulnerabilities	37
Handling unknown applications	37
Checking application reputation	37
Controlling activities of applications on the computer and on the network	38
Protecting privacy data against theft	40
Protection against phishing	40
Virtual Keyboard	41
Protection of data input from the computer keyboard	43
Safe Money	44
Privacy Cleaner	45
Assessing the safety status of a website	47
Blocking access to websites of various regions	48
Imposing Parental Control on computer users	48
Configuring Parental Control	49
Viewing the report on a user's activity	49
Using Gaming Profile for full-screen mode	50
Creating and using a Rescue Disk	50
Creating a Rescue Disk	50
Starting the computer from the Rescue Disk	52
Password-protecting access to Kaspersky Internet Security	53
Pausing and resuming computer protection	54
Viewing the application operation report	54
Restoring the default application settings	55
Importing the application settings to Kaspersky Internet Security installed on another computer	58
Using Kaspersky Gadget	58
Participating in the Kaspersky Security Network (KSN)	60
Enabling and disabling participation in Kaspersky Security Network	60
Checking the connection to Kaspersky Security Network	60
CONTACTING THE TECHNICAL SUPPORT SERVICE	62
How to get technical support	62
Technical support by phone	62
Obtaining technical support via My Kaspersky Account	62
Using the trace file and the AVZ script	64
Creating a system state report	64
Sending data files	64
AVZ script execution	66

GLOSSARY67

KASPERSKY LAB ZAO73

INFORMATION ABOUT THIRD-PARTY CODE.....74

TRADEMARK NOTICES.....74

INDEX75

ABOUT THIS GUIDE

This document is the User Guide for Kaspersky Internet Security.

For proper use of Kaspersky Internet Security, you should 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.

This Guide is intended to do the following:

- Help you install, activate, and use Kaspersky Internet Security.
- Ensure a quick search of information on application-related issues.
- Describe additional sources of information about the application and ways of receiving technical support.

IN THIS SECTION

In this guide.....	6
Document conventions.....	7

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 Internet Security

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 contains step-by-step instructions for application installation and removal.

Application licensing

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.

Solving typical tasks

This section contains step-by-step instructions for performing typical user tasks that the application provides.

Contacting the Technical Support Service

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

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.

Trademark notices

This section lists trademarks of third-party manufacturers that were used in the document.

Index

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

DOCUMENT CONVENTIONS

The document text is accompanied by semantic elements to which we recommend paying particular attention: warnings, hints, and examples.

Document conventions are used to highlight semantic elements. The following table shows document conventions and examples of their use.

Table 1. Document conventions

SAMPLE TEXT	DESCRIPTION OF DOCUMENT CONVENTION
Note that...	Warnings are highlighted in red and boxed. Warnings provide information about possible unwanted actions that may lead to data loss, failures in equipment operation or operating system problems.
We recommended that you use...	Notes are boxed. Notes may contain useful hints, recommendations, specific values for settings, or important special cases in operation of the application.
Example: ...	Examples are given on a yellow background under the heading "Example".

SAMPLE TEXT	DESCRIPTION OF DOCUMENT CONVENTION
<p><i>Update</i> means...</p> <p>The <i>Databases are out of date</i> event occurs.</p>	<p>The following semantic elements are italicized in the text:</p> <ul style="list-style-type: none"> • New terms • Names of application statuses and events
<p>Press ENTER.</p> <p>Press ALT+F4.</p>	<p>Names of keyboard keys appear in bold and are capitalized.</p> <p>Names of keys that are connected by a + (plus) sign indicate the use of a key combination. Those keys must be pressed simultaneously.</p>
<p>Click the Enable button.</p>	<p>Names of application interface elements, such as entry fields, menu items, and buttons, are set off in bold.</p>
<p>➤ <i>To configure a task schedule:</i></p>	<p>Introductory phrases of instructions are italicized and are accompanied by the arrow sign.</p>
<p>In the command line, type help.</p> <p>The following message then appears:</p> <p>Specify the date in dd:mm:yy format.</p>	<p>The following types of text content are set off with a special font:</p> <ul style="list-style-type: none"> • Text in the command line • Text of messages that the application displays on screen • Data that the user must enter.
<p><User name></p>	<p>Variables are enclosed in angle brackets. Instead of the variable, insert the corresponding value, not including the angle brackets.</p>

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 level of importance and urgency of the issue.

IN THIS SECTION

Sources of information for independent research.....	9
Discussing Kaspersky Lab applications on the Forum	10
Contacting the Sales Department.....	10
Contacting Technical Writing and Localization Unit by email	10

SOURCES OF INFORMATION FOR INDEPENDENT RESEARCH

You can use the following sources of information to research on your own:

- Application page on the Kaspersky Lab website
- Application page on the Technical Support website (Knowledge Base)
- Online help
- Documentation

If you cannot find a solution for your issue, we recommend that you contact Kaspersky Lab Technical Support (see the section "Technical support by phone" on page [62](#)).

An Internet connection is required to use information sources on the Kaspersky Lab website.

Application page on the Kaspersky Lab website

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

On a page (http://www.kaspersky.com/kaspersky_internet_security), you can view general information about an application and its functions and features.

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

Application page on the Technical Support website (Knowledge Base)

Knowledge Base is a section on the Technical Support website that provides advice on using Kaspersky Lab applications. The Knowledge Base consists of reference articles that are grouped by topic.

On the page of the application in the Knowledge Base (<http://support.kaspersky.com/kis2013>), 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 Internet Security, 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.

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

Full help provides detailed information about managing computer protection, configuring the application and solving typical user tasks.

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 immediate answer, you can discuss it with Kaspersky Lab experts and other users in our forum (<http://forum.kaspersky.com>).

In this forum you can view existing topics, leave your comments, and create new discussion 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 central office in Moscow by phone (<http://www.kaspersky.com/contacts>).
- By sending a message with your question to sales@kaspersky.com.

Service is provided in Russian and in English.

CONTACTING TECHNICAL WRITING AND LOCALIZATION UNIT BY EMAIL

To contact the Technical Writing and Localization Unit, send an email to docfeedback@kaspersky.com. Please use "Kaspersky Help Feedback: Kaspersky Internet Security" as the subject line in your message.

KASPERSKY INTERNET SECURITY

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	11
Distribution kit.....	11
Main functions and applications	12
Service for users	14
Hardware and software requirements	14

WHAT'S NEW

Kaspersky Internet Security provides the following new features:

- Safe Money (on page [44](#)) has been added to ensure a safe use of online banking services and payment systems, as well as to ease online shopping.
- Protection of data input from the computer keyboard (on page [43](#)) has been added to protect privacy data entered on various websites.
- In order to provide protection against intruders exploiting software vulnerabilities, the feature of protection against exploits has been added to the System Watcher component.
- The functionality of the Virtual Keyboard (see section "Virtual Keyboard" on page [41](#)) has been enhanced: now you can open it by clicking the quick launch icon displayed in data entry fields on websites.
- The application installation procedure has been simplified (see section "Installing and removing the application" on page [15](#)).
- The size of the application databases has been reduced, which allows lowering the size of data to download and speed up the installation of updates.
- The heuristic analysis performed when checking websites for phishing, has been improved.
- The Anti-Spam functionality has been enhanced, which ensures a more reliable filtering of unwanted email.
- The Parental Control functionality has been enhanced: the option to update rules of website checking by categories in the course of databases updating has been added. This ensures a more thorough control of children's access to websites with inadmissible content.

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 Internet Security at an online store, you copy the application from the website of the store. Information that is required for application activation is sent to you by email after payment.

For more details on ways of purchasing and the distribution kit, contact the Sales Department by sending a message to sales@kaspersky.com.

MAIN APPLICATION FEATURES

Kaspersky Internet Security provides comprehensive computer protection against known and new threats, network and phishing attacks, spam, and other unwanted content. Different functions and protection components are available as part of Kaspersky Internet Security to deliver comprehensive protection.

Computer Protection

Protection components are designed to protect the computer against known and new threats, network attacks, fraud, and spam and other unsolicited information. Every type of threat is handled by an individual protection component (see the description of components in this section). Components can be enabled or disabled independently of one another, and their settings can be configured.

In addition to the constant protection provided by the security components, we recommend that you regularly *scan* your computer for viruses. This is necessary in order to rule out the possibility of spreading malicious programs that have not been discovered by protection components, for example, because of a low security level set, or for other reasons.

To keep Kaspersky Internet Security up to date, you need to *update* the databases and software modules used by the application.

Some specific tasks that should be executed occasionally (such as removal of traces of a user's activities in the system) are executed using *advanced tools and wizards*.

The following protection components stand guard over your computer in real time:

Described below is the logic of operation of protection components in the Kaspersky Internet Security mode recommended by Kaspersky Lab specialists (that is, with default application settings).

File Anti-Virus

File Anti-Virus prevents infection of the computer's file system. The component starts upon startup of the operating system, continuously remains in the computer's RAM, and scans all files being opened, saved, or launched on your computer and all connected drives. Kaspersky Internet Security intercepts each attempt to access a file and scans the file for known viruses. The file can only be processed further if the file is not infected or is successfully treated by the application. If a file cannot be disinfected for any reason, it will be deleted. A copy of the file will be moved to Quarantine at that.

Mail Anti-Virus

Mail Anti-Virus scans incoming and outgoing email messages on your computer. The email is available to the addressee only if it does not contain dangerous objects.

Web Anti-Virus

Web Anti-Virus intercepts and blocks the execution of scripts on websites if they pose a threat. Web Anti-Virus also monitors all web traffic and blocks access to dangerous websites.

IM Anti-Virus

IM Anti-Virus ensures the safe use of Internet pagers. The component protects information that comes to your computer via IM protocols. IM Anti-Virus ensures safe operation of various applications for instant messaging.

Application Control

Application Control logs actions performed by applications in the system, and manages applications' activities based on which group the component assigns them to. A set of rules is specified for each group of applications. These rules manage the applications' access to various operating system resources.

Firewall

The Firewall ensures the security of your work in local networks and on the Internet. The component filters all network activities using rules of two types: *rules for applications* and *packet rules*.

Network Monitor

Network Monitor is designed for monitoring network activity in real time.

Network Attack Blocker

Network Attack Blocker loads at operating system startup and tracks incoming network traffic for activities characteristic of network attacks. Once an attempt to attack your computer is detected, Kaspersky Internet Security blocks any network activity of the attacking computer towards your computer.

Anti-Spam

Anti-Spam integrates into the mail client installed on your computer and scans all incoming email messages for spam. All messages containing spam are marked with a special header. You can configure Anti-Spam to handle spam messages in a particular way (for example, delete them automatically or move them to a special folder).

Anti-Phishing

Anti-Phishing allows checking URLs to find out if they are included in the list of phishing ones. This component is built into Web Anti-Virus, Anti-Spam, and IM Anti-Virus.

Anti-Banner

Anti-Banner blocks ad banners on websites and in application interfaces.

Safe Money

Safe Money provides protection of confidential data when using online banking services and payment systems, and prevents theft of assets when making online payments.

Parental Control

Parental Control is designed to protect children and teenagers from threats related to computer and Internet usage.

Parental Control allows you to set flexible restrictions on access to web resources and applications for different users depending on their age. Parental Control also allows viewing statistical reports on activities exerted by controlled users.

SERVICE FOR USERS

By acquiring a license for the application, you can benefit from the following services during the entire term of the license:

- Database updates and access to new versions of the application
- Consultations by phone and by email on issues that are related to installation, configuration, and use of the application
- Notifications about the release of new applications by Kaspersky Lab and of new viruses and virus outbreaks To use this service, subscribe to news delivery from Kaspersky Lab on the Technical Support Service website.

No consultations are provided on issues that are related to the functioning of operating systems or third-party software and technologies.

HARDWARE AND SOFTWARE REQUIREMENTS

To ensure the functioning of Kaspersky Internet Security, 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 Internet Security from a distribution CD).
- Internet access (for the application activation and for updating databases and software modules).
- Microsoft® Internet Explorer® 6.0 or later
- 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 later (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).

INSTALLING AND REMOVING THE APPLICATION

This section contains step-by-step instructions for application installation and removal.

IN THIS SECTION

Standard installation procedure.....	15
Updating the previous version of Kaspersky Internet Security	19
Non-standard installation scenarios	21
Removing the application	22

STANDARD INSTALLATION PROCEDURE

Kaspersky Internet Security 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's activity at any installation step, close the Wizard window.

If the application is meant to protect more than one computer (with the maximum number of computers depending on your license), it must be installed identically on all computers.

➤ *To install Kaspersky Internet Security on your computer,*

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

To install Kaspersky Internet Security, you can also use a distribution package downloaded from the Internet. The Setup Wizard displays a few additional installation steps for some of the localization languages at that.

IN THIS SECTION

Step 1. Finding a newer version of the application	16
Step 2. Starting the application installation.....	16
Step 3. Reviewing the License Agreement.....	16
Step 4. Kaspersky Security Network Data Collection Statement.....	17
Step 5. Installation.....	17
Step 6. Completing installation.....	17
Step 7. Activating the application	18
Step 8. Registering a user.....	18
Step 9. Completing the activation.....	18

STEP 1. FINDING A NEWER VERSION OF THE APPLICATION

Before setup, the Setup Wizard checks the update servers of Kaspersky Lab for a newer version of Kaspersky Internet Security.

If the Setup Wizard does not detect any newer version of the application on the update servers, it starts installing the current version.

If the Wizard detects a newer version of Kaspersky Internet Security on the update servers, it offers you to download and install it to your computer. It is recommended that you install the new version of the application, because newer versions include more enhancements that allow you to ensure more reliable protection of your computer. If you refuse to install the new version, the Wizard starts installing the current version of the application. If you agree to install the new version of the application, the Setup Wizard copies the setup files from the distribution package to your computer and starts installing the new version. For further details on how to install the new version of the application refer to the relevant documents.

STEP 2. STARTING THE APPLICATION INSTALLATION

At this step, the Setup Wizard offers you to install the application.

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

Depending on the installation type and the localization language, at this step the Wizard offers you to view the License Agreement concluded between you and Kaspersky Lab, also offering you to participate in Kaspersky Security Network.

STEP 3. REVIEWING THE LICENSE AGREEMENT

This step of the Setup Wizard is displayed for some of the localization languages when installing Kaspersky Internet Security from a distribution package downloaded from the Internet.

At this step, the Setup Wizard offers you to review the License Agreement concluded between you and Kaspersky Lab.

Read the License Agreement thoroughly and, if you agree with all of its terms, click the **Accept** button. The installation will then continue.

If the License Agreement is not accepted, the application will not be installed.

STEP 4. KASPERSKY SECURITY NETWORK DATA COLLECTION STATEMENT

This step of the Setup Wizard is displayed for some of the localization languages when installing Kaspersky Internet Security from a distribution package downloaded from the Internet.

At this step, the Setup Wizard invites you to participate in 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. No private data received from you is collected, processed, or stored.

Review the Kaspersky Security Network Data Collection Statement. If you agree with all of the terms of the Statement, select the **I want to participate in Kaspersky Security Network** check box in the Wizard window.

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

STEP 5. INSTALLATION

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.

Kaspersky Internet Security performs several checks during installation. Those checks may result in detection of the following problems:

- **Non-compliance of the operating system to the software requirements.** During installation the Wizard checks the following conditions:
 - Whether the operating system and the Service Packs meet the software requirements
 - Whether all of the required applications are available
 - Whether the amount of free disk space is enough for installation.

If any of the above-listed requirements is not met, a notification to that effect will be displayed on the screen.

- **Presence of incompatible applications on the computer.** 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 Internet Security cannot remove automatically should be removed manually. When removing incompatible applications, you will need to reboot your operating system, after which installation of Kaspersky Internet Security will continue automatically.
- **Presence of malware on the computer.** If any malicious applications that interfere with installation of anti-virus software are detected on the computer, the Setup Wizard prompts you to download a dedicated tool designed to neutralize infection and named *Kaspersky Virus Removal Tool*.

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 prompted to download it on your own by clicking the link provided.

STEP 6. COMPLETING INSTALLATION

At this step, the Wizard informs you of the completion of the application installation. To run Kaspersky Internet Security immediately, make sure that the **Run Kaspersky Internet Security 2013** check box is selected and click the **Finish** button.

In some cases, you may need to reboot your operating system to complete installation. If the **Run Kaspersky Internet Security 2013** check box is selected, the application will be run automatically after you reboot your operating system.

If you have cleared the **Run Kaspersky Internet Security 2013** check box before closing the Wizard, you will need to run the application manually.

STEP 7. ACTIVATING THE APPLICATION

At this step, the Setup Wizard offers you to activate the application.

Activation is a process of putting into operation a full-functional version of the application for a certain period of time.

If you have acquired a license for Kaspersky Internet Security and downloaded the application from an online store, the application activation can be performed automatically in the course of installation.

You will be offered the following options for Kaspersky Internet Security activation:

- **Activate commercial version.** Select this option and enter the activation code (see section "About the activation code" on page [25](#)) if you have purchased a commercial version of the application.

If you specify an activation code for Kaspersky Anti-Virus in the entry field, the procedure of switching to Kaspersky Anti-Virus 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 trial license. When the license expires, trial version cannot be activated for a second time.

You will need an Internet connection to activate the application.

STEP 8. 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.

Registered users are able to send requests to the Technical Support Service and Virus Lab through My Kaspersky Account on the Kaspersky Lab website, manage activation codes conveniently, and receive the latest information about new products and special offers.

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

In some cases user registration is required to start using the application.

STEP 9. COMPLETING THE ACTIVATION

The Wizard informs you that Kaspersky Internet Security has been successfully activated. In addition, information about the current license is provided in this window: license type (commercial or trial), expiration date, and number of hosts covered by the license.

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

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

UPDATING THE PREVIOUS VERSION OF KASPERSKY INTERNET SECURITY

If Kaspersky Internet Security 2011 or 2012 is already installed on your computer, you should update the application to Kaspersky Internet Security 2013. If you have a current license for Kaspersky Internet Security 2011 or 2012, you will not have to activate the application: the Setup Wizard will automatically retrieve the information about your license for Kaspersky Internet Security 2011 or 2012 and apply it in the course of the installation process.

Kaspersky Internet Security 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's activity at any installation step, close the Wizard window.

If the application is meant to protect more than one computer (with the maximum number of computers depending on your license), it must be installed identically on all computers.

► *To install Kaspersky Internet Security on your computer,*

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

To install Kaspersky Internet Security, you can also use a distribution package downloaded from the Internet. The Setup Wizard displays a few additional installation steps for some of the localization languages at that.

IN THIS SECTION

Step 1. Finding a newer version of the application	19
Step 2. Starting the application installation.....	20
Step 3. Reviewing the License Agreement.....	20
Step 4. Kaspersky Security Network Data Collection Statement.....	20
Step 5. Installation.....	20
Step 6. Completing installation.....	21

STEP 1. FINDING A NEWER VERSION OF THE APPLICATION

Before setup, the Setup Wizard checks the update servers of Kaspersky Lab for a newer version of Kaspersky Internet Security.

If the Setup Wizard does not detect any newer version of the application on the update servers, it starts installing the current version.

If the Wizard detects a newer version of Kaspersky Internet Security on the update servers, it offers you to download and install it to your computer. It is recommended that you install the new version of the application, because newer versions include more enhancements that allow you to ensure more reliable protection of your computer. If you refuse to install the new version, the Wizard starts installing the current version of the application. If you agree to install the new version of the application, the Setup Wizard copies the setup files from the distribution package to your computer and starts installing the new version. For further details on how to install the new version of the application refer to the relevant documents.

STEP 2. STARTING THE APPLICATION INSTALLATION

At this step, the Setup Wizard offers you to install the application.

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

Depending on the installation type and the localization language, at this step the Wizard offers you to view the License Agreement concluded between you and Kaspersky Lab, also offering you to participate in Kaspersky Security Network.

STEP 3. REVIEWING THE LICENSE AGREEMENT

This step of the Setup Wizard is displayed for some of the localization languages when installing Kaspersky Internet Security from a distribution package downloaded from the Internet.

At this step, the Setup Wizard offers you to review the License Agreement concluded between you and Kaspersky Lab.

Read the License Agreement thoroughly and, if you agree with all of its terms, click the **Accept** button. The installation will then continue.

If the License Agreement is not accepted, the application will not be installed.

STEP 4. KASPERSKY SECURITY NETWORK DATA COLLECTION STATEMENT

This step of the Setup Wizard is displayed for some of the localization languages when installing Kaspersky Internet Security from a distribution package downloaded from the Internet.

At this step, the Setup Wizard invites you to participate in 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. No private data received from you is collected, processed, or stored.

Review the Kaspersky Security Network Data Collection Statement. If you agree with all of the terms of the Statement, select the **I want to participate in Kaspersky Security Network** check box in the Wizard window.

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

STEP 5. INSTALLATION

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.

Kaspersky Internet Security performs several checks during installation. Those checks may result in detection of the following problems:

- **Non-compliance of the operating system to the software requirements.** During installation the Wizard checks the following conditions:
 - Whether the operating system and the Service Packs meet the software requirements
 - Whether all of the required applications are available

- Whether the amount of free disk space is enough for installation.

If any of the above-listed requirements is not met, a notification to that effect will be displayed on the screen.

- **Presence of incompatible applications on the computer.** 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 Internet Security cannot remove automatically should be removed manually. When removing incompatible applications, you will need to reboot your operating system, after which installation of Kaspersky Internet Security will continue automatically.
- **Presence of malware on the computer.** If any malicious applications that interfere with installation of anti-virus software are detected on the computer, the Setup Wizard prompts you to download a dedicated tool designed to neutralize infection and named *Kaspersky Virus Removal Tool*.

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 prompted to download it on your own by clicking the link provided.

STEP 6. COMPLETING INSTALLATION

This window of the Wizard informs you of the successful completion of the application installation.

Restart the operating system after the application has been installed.

If the **Run Kaspersky Internet Security** check box is selected, the application will be run automatically after you reboot your operating system.

If you have cleared the **Run Kaspersky Internet Security** check box before closing the Wizard, you will need to run the application manually.

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 Internet Security and activating it using an activation code for Kaspersky Anti-Virus

If, when installing Kaspersky Internet Security, at the Activating the application step you enter an activation code intended for Kaspersky Anti-Virus, the Migration Wizard launches, which results in Kaspersky Anti-Virus being installed on your computer.

If, when installing Kaspersky Internet Security, at the Activating the application step you select **Activate later** and then activate the installed application using an activation code intended for Kaspersky Anti-Virus, the Migration Wizard also launches, which results in Kaspersky Internet Security being switched to Kaspersky Anti-Virus.

Installing Kaspersky Internet Security 2013 over Kaspersky Anti-Virus 2011 or 2012

If you run the installation of Kaspersky Internet Security 2013 on a computer on which Kaspersky Anti-Virus 2011 or 2012 with a current license is already installed, the Setup Wizard detects this and prompts you to select one of the further scenarios:

- Keep using Kaspersky Anti-Virus under the current license. In this case, the Migration Wizard launches, which results in Kaspersky Anti-Virus 2013 being installed on your computer. You will be able to use Kaspersky Anti-Virus 2013 as long as the license for Kaspersky Anti-Virus 2011 or 2012 remains in effect.
- Proceed with installation of Kaspersky Internet Security 2013. In this case, the installation procedure will continue according to the standard scenario, starting from the Activating the application step.

REMOVING THE APPLICATION

After uninstalling Kaspersky Internet Security, your computer and personal data will be unprotected!

Kaspersky Internet Security is uninstalled with the help of the Setup Wizard.

➔ *To start the Wizard,*

in the **Start** menu, select **Programs** → **Kaspersky Internet Security 2013** → **Remove Kaspersky Internet Security 2013**.

IN THIS SECTION

Step 1. Saving data for future use	22
Step 2. Confirming application removal	22
Step 3. Removing the application. Completing removal	23

STEP 1. SAVING DATA FOR FUTURE USE

At this step you can specify which of the data used by the application you want to keep for further use at the next installation of the application (e.g., when installing a newer version of the application).

By default, the application prompts you to save information about activation.

➔ *To save application data for future use:*

1. Select check boxes next to the data types that you want to save:

- **License information** – a set of data that rules out the need to activate the new application by allowing you to use it under the current license unless the license expires before you start the installation.
- **Quarantine files** – files scanned by the application and moved to Quarantine.

After Kaspersky Internet Security is removed from the computer, quarantined files become unavailable. You should install Kaspersky Internet Security to handle those files.

- **Application operating settings** are the values of the application settings selected during configuration.
- **iChecker data** are files that contain information about objects that have already been scanned with iChecker technology.
- **Anti-Spam databases** are databases that contain samples of spam messages downloaded and saved by the application.

STEP 2. CONFIRMING 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.

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 must reboot your operating system. If you cancel 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.

APPLICATION LICENSING

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	24
About the license.....	24
About the activation code.....	25
About data provision.....	25

ABOUT THE END USER LICENSE AGREEMENT

The End User License Agreement is a binding agreement between you and Kaspersky Lab ZAO, stipulating the terms on which you may use the application.

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

It is deemed that you accept the terms of the License Agreement by confirming that you agree with the License Agreement when installing the application. If you do not accept the terms of the License Agreement, you must abort the application installation or renounce the use of the application.

ABOUT THE LICENSE

A *license* is a time-limited right to use the application, granted under the End User License Agreement. The license stipulates a unique code for activation of your copy of Kaspersky Internet Security.

A current license entitles you to the following kinds of services:

- The right to use the application on one or several devices.

The number of devices on which you may use the application is specified in the End User License Agreement.

- Assistance from Kaspersky Lab Technical Support.
- Other services available from Kaspersky Lab or its partners during the term of the license (see the section "Service for users" on page [14](#)).

The scope of services and application usage term depend on the type of license under which the application is activated.

The following license types are provided:

- *Trial* – a free license intended for trying out the application.

Trial license usually has a short term. As soon as the license expires, all Kaspersky Internet Security features are disabled. To continue using the application, you need to acquire a commercial license.

- *Commercial* – a paid license offered upon purchase of the application.

When the commercial license expires, the application continues running though with a limited functionality (for example, updating and using Kaspersky Security Network are not available). You still can benefit all of the application components and perform scans for viruses and other malware, but using only the databases that had been installed last before the license expired. To continue using Kaspersky Internet Security in fully functional mode, you must renew your commercial license.

We recommend renewing the license before its expiration to ensure maximum protection of your computer against all security threats.

ABOUT THE ACTIVATION CODE

Activation code is a code that you receive on acquiring the commercial license for Kaspersky Internet Security. This code is required for activation of the application.

The activation code is a unique sequence of twenty digits and Latin letters in the format xxxxx-xxxxx-xxxxx-xxxxx.

Depending on how you purchased the application, you can obtain the activation code in one of the following ways:

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

The license term countdown starts from the date when you activate the application. If you have acquired a license intended for the use of Kaspersky Internet Security on several devices, the term of the license starts counting down from the moment you have first applied the activation code.

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 [62](#)).

ABOUT DATA PROVISION

To increase the protection level, by accepting the provisions of the License Agreement, you agree to provide the following information to Kaspersky Lab in automatic mode:

- information about the checksums of processed files (MD5);
- information required for assessing the reputations of URLs;
- statistics of the use of product notifications;
- statistical data for protection against spam;
- data on activation of Kaspersky Internet Security and the version being currently in use;
- information about the types of detected threats;
- information about digital certificates being currently in use and information required to verify them.

If the computer is equipped with TPM (Trusted Platform Module), you also agree to provide Kaspersky Lab the TPM report on the operating system's booting and information required to verify it. If an error occurs while installing Kaspersky Internet Security, you agree to provide Kaspersky Lab information about the error code, distribution package being currently in use, and your computer, in automatic mode.

In case of participation in Kaspersky Security Network (see section "Participating in the Kaspersky Security Network (KSN)" on page [60](#)), the following information is automatically sent from the computer to Kaspersky Lab:

- information about the hardware and software installed on the computer;
- information about the anti-virus protection status of the computer, as well as all potentially malicious objects and actions, and decisions made in relation to those objects and actions;
- information about applications being downloaded and run;
- information about interface errors and the use of the interface of Kaspersky Internet Security;
- information about the version of the databases being currently in use;
- statistics of updates and connections to Kaspersky Lab servers.

Also, additional checking at Kaspersky Lab may require sending files (or parts of files) that are imposed to an increased risk of being exploited by intruders to do harm to the user's computer or data.

Transferred information 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. For more details on data provision refer to the website (<http://support.kaspersky.com>)

SOLVING TYPICAL TASKS

This section contains step-by-step instructions for performing typical user tasks that the application provides.

IN THIS SECTION

Activating the application.....	28
Acquiring and renewing a license.....	28
Managing application notifications.....	29
Assessing the computer protection status and resolving security issues	29
Updating databases and application modules.....	31
Scanning critical areas of your computer for viruses	31
Full scan of the computer for viruses.....	31
Scanning a file, folder, disk, or another object for viruses	32
Scanning probably infected objects.....	33
Restoring an object deleted or disinfected by the application.....	33
Recovering the operating system after infection.....	34
Scanning email and filtering attachments in email messages	36
Blocking unwanted email (spam).....	37
Scanning the computer for vulnerabilities.....	37
Handling unknown applications.....	37
Protecting privacy data against theft	40
Assessing the safety status of a website.....	47
Blocking access to websites of various regions.....	48
Imposing Parental Control on computer users	48
Using Gaming Profile for full-screen mode.....	50
Creating and using a Rescue Disk	50
Password-protecting access to Kaspersky Internet Security.....	53
Pausing and resuming computer protection.....	54
Viewing the application operation report	54
Restoring the default application settings.....	55
Importing the application settings to Kaspersky Internet Security installed on another computer	58
Using Kaspersky Gadget.....	58
Participating in the Kaspersky Security Network (KSN)	60

ACTIVATING THE APPLICATION

You need to activate the application to be able to use its functionality and associated services.

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 Internet Security messages appearing in the taskbar notification area. Kaspersky Internet Security is activated using the Activation Wizard.

➤ *To run the Kaspersky Internet Security activation wizard, perform one of the following:*

- Click the **Activate** link in the Kaspersky Internet Security 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 **Licensing** 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 (see section "About the activation code" on page [25](#)) 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. Entering registration data

Registered users are permitted to use the following features:

- Send requests to Technical Support Service and Anti-Virus Lab from My Kaspersky Account on the website of Kaspersky Lab.
- Manage activation codes.
- Receive information about new products and special offers from Kaspersky Lab.

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 Wizard window shows information about the activation results.

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

ACQUIRING AND RENEWING A LICENSE

If you have installed Kaspersky Internet Security without a license, you can acquire one after installation. On acquiring a license, you will receive an activation code that you have to apply to activate the application (see section "How to activate the application" on page [28](#)).

When your license expires, you can renew it. To do this, you can add a reserve activation code without waiting for the current license to expire. When the current license expires, Kaspersky Internet Security will be automatically activated by means of the reserve activation code.

➤ *To acquire a license:*

1. Open the main application window.
2. Click the **Insert your activation code here / Licensing** link in the bottom part of the main window to open the **Licensing** window.
3. In the window that opens, click the **Buy activation code** button.

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

➤ *To add a reserve activation code:*

1. Open the main application window.
2. Click the **Insert your activation code here / Licensing** link in the bottom part of the main window to open the **Licensing** window.
3. In the window that opens, 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 Internet Security then sends the data to the activation server for verification. If the verification is successful, the Activation Wizard automatically proceeds to the next step.

5. When you have finished with the Wizard, click the **Finish** button.

MANAGING APPLICATION NOTIFICATIONS

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 probably 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.

ASSESSING THE COMPUTER PROTECTION STATUS AND RESOLVING SECURITY ISSUES

Problems with computer protection are notified of by an indicator located in the left part of the main application window (see figure below). 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. You are advised to fix the problems and security threats immediately.



Figure 1. Protection status indicator

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.

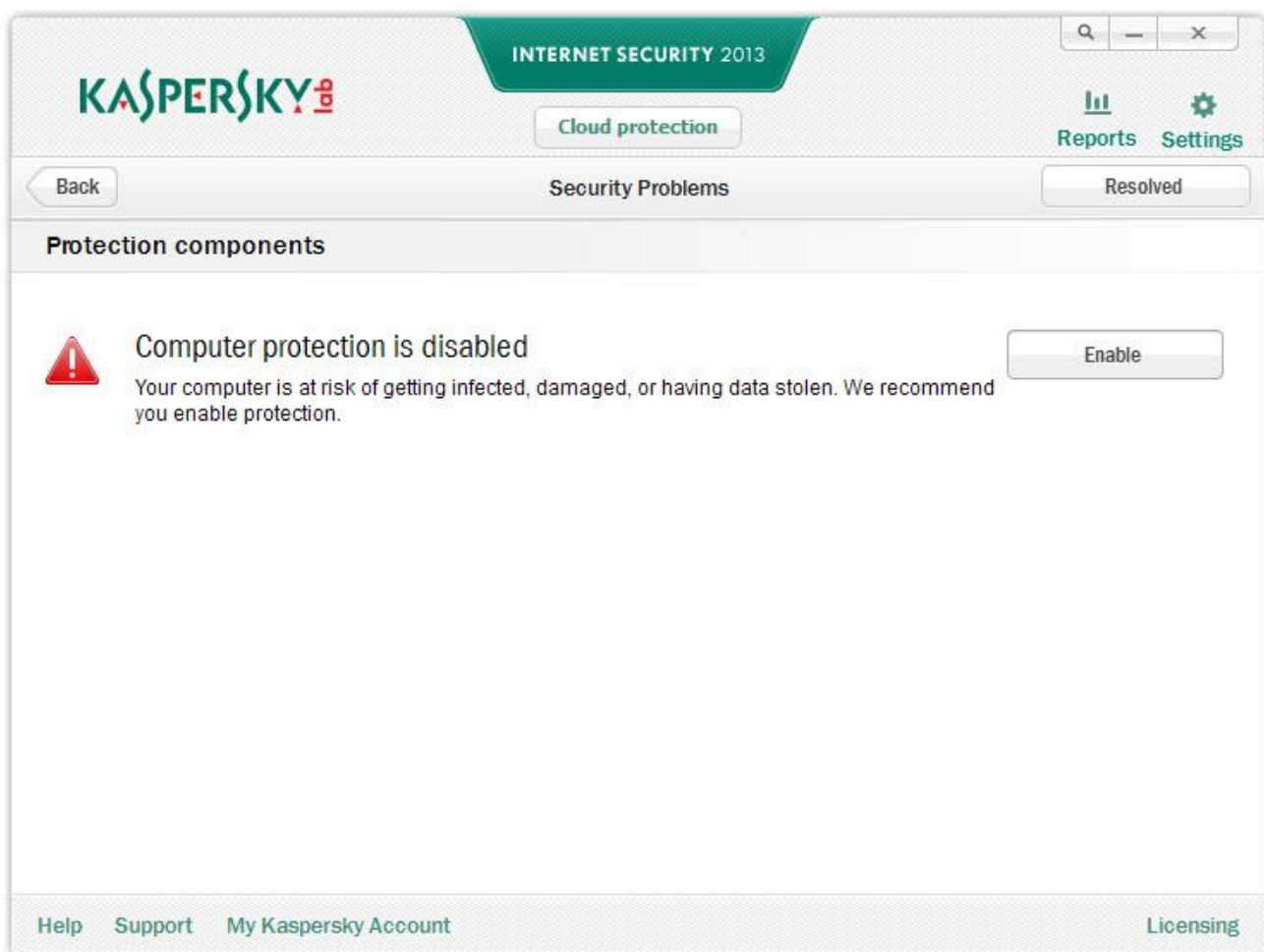


Figure 2. Security Problems window

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

UPDATING DATABASES AND APPLICATION MODULES


By default, Kaspersky Internet Security automatically checks for updates on the Kaspersky Lab update servers. If the server stores a set of recent updates, Kaspersky Internet Security downloads and installs them in background mode. You can run a Kaspersky Internet Security update manually at any time from the main application window or the context menu of the application icon in the taskbar notification area.

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

- *To run an update from the context menu of the application icon in the taskbar notification area,*
in the context menu of the application icon, select the **Update** item.
- *To run 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.

SCANNING 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.
- *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.


FULL SCAN OF THE COMPUTER FOR VIRUSES

During a full scan, Kaspersky Internet Security scans the following objects by default:

- system memory;
- objects loaded on operating system startup;
- system backup;
- hard drives and removable drives.

We recommend running a full scan immediately after installing Kaspersky Internet Security on the computer.

- *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.

- In the **Scan** window that opens, in the **Full Scan** section, click the  button.

SCANNING A FILE, FOLDER, DISK, OR ANOTHER OBJECT FOR VIRUSES

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

- from the context menu of the object;
- from the main application window;
- Using the Kaspersky Internet Security Gadget (see section "Using Kaspersky Gadget" on page [58](#)) (only for Microsoft Windows Vista and Microsoft Windows 7 operating systems).

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

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

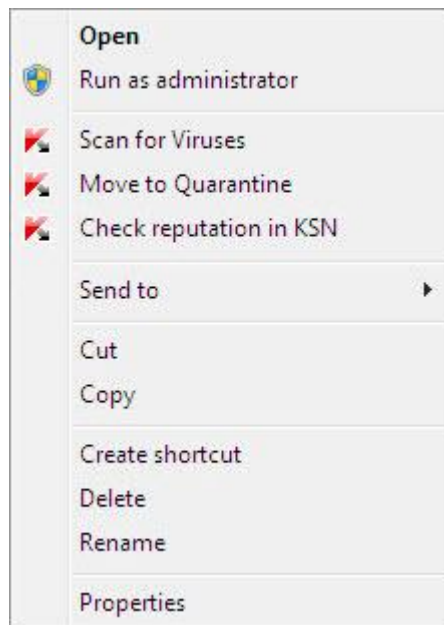


Figure 3. The context menu of an object in Microsoft Windows

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

- Open the main application window and select the **Scan** section in the lower part of the window.
- Click the **Specify** link in the bottom right part of the window to open the **Custom Scan** window, and select the check boxes next to folders and drives that you need to scan.

If the window displays no object to be scanned:

- Click the **Add** button.
- In the **Select object to scan** window that opens, select an object to be scanned.

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

drag the object to scan onto the gadget.

SCANNING PROBABLY INFECTED OBJECTS

If you suspect an object is infected, scan it using Kaspersky Internet Security (see section "How to scan a file, folder, disk, or another object for viruses" on page [32](#)).

If the application completes the scan and reports that an object is safe although you suspect the contrary, you can send such object to *Anti-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 "Updating databases and application modules" on page [31](#)).

- *To send a file to the Virus Lab:*

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

RESTORING AN OBJECT DELETED OR DISINFECTED BY THE APPLICATION

Kaspersky Lab recommends that you avoid restoring deleted and disinfected objects since they may pose a threat to your computer.

To restore a deleted or disinfected object, you can use its backup copy created by the application during a scan of the object.

- *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. In the **Quarantine** window that opens, select the required file from the list and click the **Restore** button (see figure below).

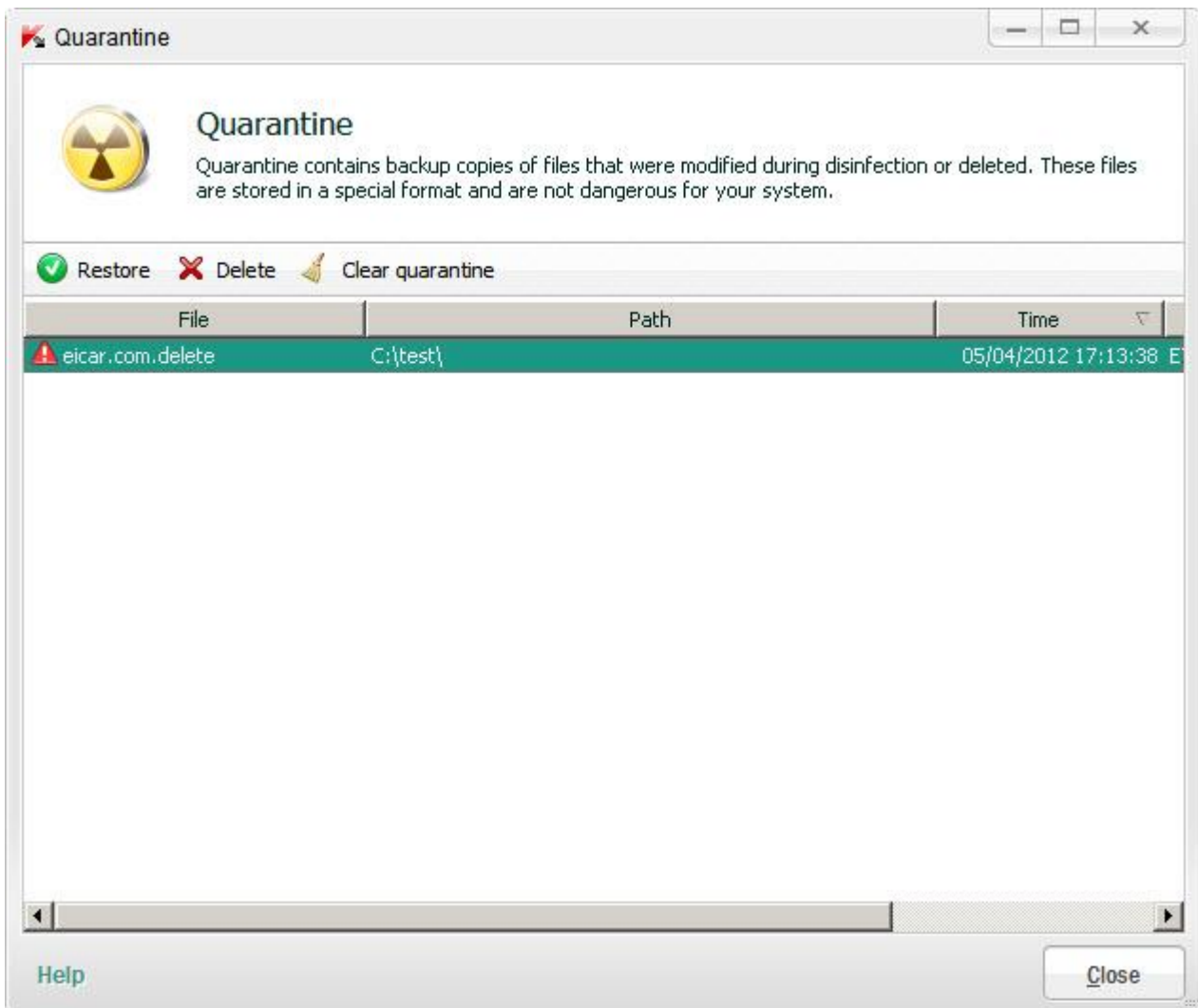


Figure 4. Quarantine window

RECOVERING THE OPERATING SYSTEM AFTER INFECTION

If you suspect the operating system of your computer to be corrupted or modified due to malware activity or a system failure, use the *post-infection Microsoft Windows troubleshooting wizard* that clears the system of any traces of malicious objects. 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.

The Wizard checks whether there are any changes to the system, such as the following: access to the network being blocked, known file format extensions have been changed, the toolbar is locked, etc. There are different reasons for these different kinds of damage. These reasons may include the activity of malicious programs, incorrect system configuration, system failures, or even 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 run the post-infection Microsoft Windows troubleshooting wizard:*

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 **Microsoft Windows Troubleshooting** section, click the **Start** button.

The post-infection Microsoft Windows troubleshooting 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 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, select the check 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, clear the check box next to it.

It is strongly recommended that you not clear the check 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. Fixing problems

The Wizard will perform the actions selected during the previous step. It may take a while to fix problems. 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.

SCANNING EMAIL AND FILTERING ATTACHMENTS IN EMAIL MESSAGES

Kaspersky Internet Security allows scanning email messages for dangerous objects using Mail Anti-Virus. Mail Anti-Virus starts when the operating system launches and remains in the RAM permanently, scanning all email messages that are sent or received over POP3, SMTP, IMAP, MAPI, and NNTP, as well as via encrypted connections (SSL) over POP3, SMTP and IMAP.

By default, Mail Anti-Virus scans both incoming and outgoing messages. If necessary, you can enable scanning of incoming messages only.

► *To scan only incoming email messages:*

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Mail Anti-Virus** component.
4. Click the **Settings** button in the right part of the window.

The **Mail Anti-Virus** window opens.

5. In the window that opens, use the **General** tab in the **Protection scope** section to select the **Incoming messages only** option.

If no threats have been detected in an email message, or if all infected objects have been successfully disinfected, the message becomes available for further operations. If the component fails to disinfect an infected object, Mail Anti-Virus renames or deletes the object from the message and expands the message subject with a notification stating that the message has been processed by Kaspersky Internet Security. Before deleting an object, Kaspersky Internet Security creates a backup copy of it and places this copy to Quarantine (see section "Restoring an object deleted or disinfected by the application" on page [33](#)).

Malicious programs may spread in the form of attachments in email messages. You can enable filtering of attachments in email messages. Filtering allows automatically renaming or deleting attached files of types that you have specified.

► *To enable attachment filtering in email messages:*

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Mail Anti-Virus** component.
4. Click the **Settings** button in the right part of the window.

The **Mail Anti-Virus** window opens.

5. In the window that opens, on the **Attachment filter** tab select an attachment filtering mode (**Rename selected attachment types** or **Delete selected attachment types**).
6. From the list of file types (extensions) select attachment types that should be filtered.

If you want to add a mask of a new file type:

- a. Click the **Add** link in the bottom part of the window to open the **Input file name mask** window.
- b. In the window that opens, enter a file type mask.
7. Click the **Apply** button in the **Settings** window.

BLOCKING UNWANTED EMAIL (SPAM)

If you receive large amounts of unwanted messages (spam), enable the Anti-Spam component and set the recommended security level for it.

➤ *To enable Anti-Spam and set the recommended security level:*


1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Anti-Spam** component.
4. In the right part of the window, select the **Enable Anti-Spam** check box.
5. Make sure that the **Recommended** security level is set in the **Security level** section.

If the security level is set to **Low** or **Custom**, click the **Default level** button. The security level will automatically be set to **Recommended**.

SCANNING THE 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.

➤ *To start a vulnerability 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 **Vulnerability Scan** section, click the  button.

HANDLING UNKNOWN APPLICATIONS

Kaspersky Internet Security helps to minimize the risk involved in using unknown applications (such as the risk of infection with viruses and unwanted changes to operating system settings).

Kaspersky Internet Security includes components and tools that allow checking an application's reputation and controlling its activities exerted on your computer.

IN THIS SECTION

Checking application reputation	37
Controlling activities of applications on the computer and on the network	38

CHECKING APPLICATION REPUTATION

Kaspersky Internet Security 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 Application Control or 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.

Application reputation check is available if you have agreed to participate in Kaspersky Security Network.

➔ To know the reputation of an application,

open the context menu of the application's executable file and select **Check reputation in KSN** (see figure below).

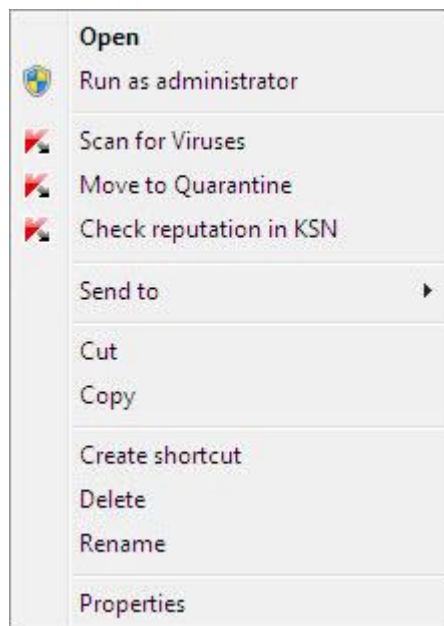


Figure 5. The context menu of an object in Microsoft Windows

A window with information about the reputation of the application in KSN opens.

SEE ALSO:

Participating in the Kaspersky Security Network (KSN) [60](#)

CONTROLLING ACTIVITIES OF APPLICATIONS ON THE COMPUTER AND ON THE NETWORK

Application Control prevents applications from performing actions that may be dangerous for the system and ensures control of access to operating system resources and your identity data.

The component tracks actions performed in the system by applications installed on the computer and regulates them based on the Application Control rules. These rules regulate potentially dangerous activity, including applications' access to protected resources, such as files and folders, registry keys, and network addresses.

Applications' network activity is controlled by the Firewall component.

When an application is first run on the computer, Application Control checks it for safety and moves to one of the groups (**Trusted**, **Untrusted**, **High Restricted**, or **Low Restricted**). The group defines the rules that Kaspersky Internet Security should apply for controlling the activity of this application.

You can edit application control rules manually.

➤ *To edit application rules manually:*

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the **Settings** window that opens, select the **Application Control** subsection in the **Protection Center** section.
4. In the right part of the window, in the **Configure application rules, protect digital identity data and other resources** section, click the **Applications** button.
5. In the **Applications** window that opens, select the desired application from the list and click the **Edit** button.
6. In the **Application rules** window that opens, set the application rules:
 - To configure rules of access to operating system resources for an application:
 - a. On the **Files and system registry** tab select the required resource category.
 - b. Right-click the column with an available action on the resource (**Read**, **Write**, **Delete**, or **Create**) to open the context menu and select the required value from it (**Allow**, **Block**, or **Prompt for action**).
 - To configure the rights of an application to perform various actions in the operating system:
 - a. On the **Rights** tab select the required category of rights.
 - b. Right-click the **Permission** column to open the context menu and select the required value from it (**Allow**, **Block**, or **Prompt for action**).
 - To configure the rights of an application to perform various actions on the network:
 - a. On the **Network rules** tab click the **Add** button.
The **Network rule** window opens.
 - b. In the window that opens, specify the required rule settings and click the **OK** button.
 - c. Assign a priority to the new rule by using the **Move up** and **Move down** buttons to move it up or down the list.
 - To exclude certain actions from the scope of Application Control, on the **Exclusions** tab select the check boxes for actions that should not be controlled.

All exclusions created in the rules for user applications are accessible in the application settings window in the **Threats and Exclusions** section.

7. Click the **Apply** button in the **Settings** window.

PROTECTING PRIVACY DATA AGAINST THEFT

Kaspersky Internet Security helps you protect your personal data against theft:

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

Kaspersky Internet Security includes components and tools that allow you to protect your personal data against theft attempts committed by hackers using such methods as phishing and interception of data entered at the keyboard.

Protection against phishing is ensured by Anti-Phishing, implemented in the Web Anti-Virus, Anti-Spam, and IM Anti-Virus components.

Protection against interception of data entered at the keyboard is provided by the Virtual Keyboard and protection of data entered using the computer keyboard.

The Privacy Cleaner Wizard is designed for clearing the computer of all information about the user's activities.

Protection of data when using Internet banking services and shopping at online stores is provided by Safe Money features.

Protection against transfer of privacy data over the Internet is provided by a tool of Parental Control (see section "Imposing Parental Control on computer users" on page [48](#)).

IN THIS SECTION

Protection against phishing	40
Virtual Keyboard.....	41
Protection of data input from the computer keyboard.....	43
Safe Money	44
Privacy Cleaner	45

PROTECTION AGAINST PHISHING

Protection against phishing is ensured by Anti-Phishing, implemented in the Web Anti-Virus, Anti-Spam, and IM Anti-Virus components. Enable these components to ensure comprehensive protection against phishing.

You can configure additional anti-phishing protection settings in the Web Anti-Virus and IM Anti-Virus components.

➤ *To configure anti-phishing protection when Web Anti-Virus is running:*

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the **Settings** window that opens, go to the **Protection Center** section, select the **Web Anti-Virus** subsection and click the **Settings** button.

The **Web Anti-Virus** window opens.

4. In the window that opens, on the **General** tab, in the **Kaspersky URL Advisor** section, select the **Check web pages for phishing** check box.

5. If you want Anti-Phishing to use heuristic analysis click the **Additional** button when scanning web pages.

The **Anti-Phishing settings** window opens.

6. In the window that opens, select the **Use Heuristic Analysis to check web pages for phishing** and set the scan detail level.
7. Click the **Apply** button in the **Settings** window.

➔ *To configure anti-phishing protection for use during IM Anti-Virus operation:*

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the **Settings** window that opens, select the **IM Anti-Virus** subsection in the **Protection Center** section.
4. In the right part of the window, in the **Scan methods** section, select the **Check if URLs are listed in the database of phishing URLs** check box.
5. Click the **Apply** button in the **Settings** window.

VIRTUAL 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, online 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 only prevents the interception of personal data when working with Microsoft Internet Explorer, Mozilla™ Firefox™ and Google Chrome™ browsers. When used with other browsers, Virtual Keyboard does not protect personal data being entered against interception.

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 programs classified as spyware can take screenshots, which then are automatically transmitted to an intruder for further analysis and for stealing 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 does not prevent making screenshots using Print Screen key and other combinations of keys provided by the operating system settings, as well as making screenshots using DirectX.

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. This is why using key combinations (such as **ALT+F4**) requires pressing the first key (for example, **ALT**), then the second key (for example, **F4**), and then the first key again. The second click of the key acts in the same way as the key release on a real keyboard.
- The Virtual Keyboard language can be switched using the same shortcut that is configured in the operating system settings for the physical keyboard. You have to right-click the other key (for example, if the **LEFT ALT+SHIFT** shortcut is configured in the operating system settings for switching the keyboard language, you have to left-click the **LEFT ALT** key and right-click the **SHIFT** key).

To ensure protection of data entered at the Virtual Keyboard, you should restart your computer after Kaspersky Internet Security is installed.

You can open the Virtual Keyboard in the following ways:

- from the context menu of the application icon in the taskbar notification area;
- from the main application window;
- from the Microsoft Internet Explorer, Mozilla Firefox or Google Chrome browser windows;
- using the quick launch icon of the Virtual Keyboard in entry fields on websites;

You can configure the display of the quick launch icon in entry fields on websites.

- using a combination of keys at the computer keyboard;
- using the Kaspersky Internet Security Gadget (only for Microsoft Windows Vista and Microsoft Windows 7 operating systems).

- To open Virtual Keyboard from the context menu of the application icon in the taskbar notification area, select **Tools** → **Virtual Keyboard** from the context menu of the application icon (see figure below).

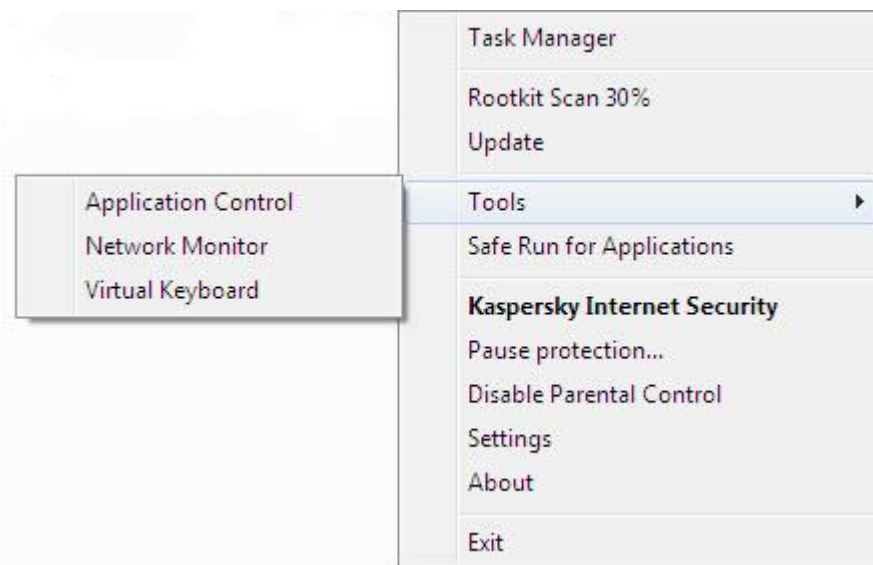



Figure 6. Application icon context menu

- To open the Virtual Keyboard from the main application window, in the lower part of the main application window select the **Virtual Keyboard** section.

- 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.

- *To open the Virtual Keyboard using the gadget,*

click the gadget button to which this action has been assigned (see section "Using Kaspersky Gadget" on page [58](#)).

- *To configure the display of the quick launch icon of the Virtual Keyboard in entry fields on websites:*

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the **Settings** window that opens, in the **Protection Center** section select the **Secure Data Input** subsection.
4. In the right part of the window, in the **Virtual Keyboard** section select the **Show quick launch icon in data entry fields** check box and click the **Settings** button.

The **Virtual Keyboard** window opens.

5. In the window that opens, set display rules for the quick launch icon:
 - On the **Categories** tab select the check boxes for categories of websites on which the quick launch icon should be displayed in entry fields.
 - If you want the quick launch icon to be displayed in entry fields on websites that are opened in Safe Run for Websites when using Safe Money, on the **Categories** tab select the **Show Virtual Keyboard quick launch icon in Safe Money fields** check box.
 - If you want to enable the display of the quick launch icon in entry fields on a specified website:
 - a. On the **Exclusions** tab, in the **Show quick launch icon on websites** list click the **Add** button.

The **Show quick launch icon** window opens.

- b. In the window that opens, enter the URL of a website in the **URL** field and select one of the options of the display of the quick launch icon on that website (**Show icon only on the specified web page** or **Show icon on the whole website**).
6. Click the **Apply** button in the **Settings** window.

PROTECTION OF DATA INPUT FROM THE COMPUTER 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, online 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.

Protection of data input from the computer keyboard allows avoiding interception of data entered at the keyboard.

Protection of data input from the computer keyboard is only available for Microsoft Internet Explorer, Mozilla Firefox, and Google Chrome browsers. When using other web browsers, data entered at the computer keyboard are not protected against interception.

Protection of data input from the computer keyboard cannot protect your personal data if a website that requires entering such data has been hacked, because in this case information will be directed directly to intruders.

You can configure protection of data input from the computer keyboard on various websites. After protection of data input from the computer keyboard is configured, you do not have to take any additional actions when entering data.

To protect data entered at the computer keyboard, you should restart your computer after Kaspersky Internet Security is installed.

➤ *To configure protection of data input from the computer keyboard:*

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the **Settings** window that opens, in the **Protection Center** section select the **Secure Data Input** subsection.
4. In the right part of the window, in the **Secure keyboard input** section select the **Enable secure keyboard input** check box and click the **Settings** button.

The **Secure Keyboard Input** window opens.

5. In the window that opens, specify the protection scope for data input at the computer keyboard:
 - On the **Categories** tab select the check boxes for categories of websites on which data entered at the keyboard should be protected.
 - If you want data input from the keyboard to be protected on websites that are opened in Safe Run for Websites in Safe Money mode, on the **Categories** tab select the **Enable secure keyboard input for Safe Money** check box.
 - If you want data input at the keyboard to be protected in password fields on all websites, on the **Categories** tab select the **Protect password fields on all websites** check box.
 - If you want to enable protection of data input from the keyboard on a specified website:
 - a. On the **Exclusions** tab, in the **Enable secure keyboard input on websites** list click the **Add** button.
The **Protected website** window opens.
 - b. In the window that opens, enter the URL of a website in the **URL** field and select one of the protection options for data input on this website (**Enable protection only on the specified web page** or **Enable protection on the whole website**).

6. Click the **Apply** button in the **Settings** window.

SAFE MONEY

To provide protection for confidential data that you enter on websites of banks and payment systems (such as banking card numbers, passwords for access to online banking services), as well as to prevent theft of assets when making online payments, Kaspersky Internet Security offers you to open such websites in Safe Run for Websites.

Safe Run for Websites cannot be run if the **Enable Self-Defense** check box is selected in the **Advanced Settings** section, the **Self-Defense** subsection of the application settings window.

You can configure Safe Money so that the application could automatically recognize websites of banks and payment systems.

➤ *To configure Safe Money:*

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the **Settings** window that opens, in the **Protection Center** section select the **Safe Money** subsection.

4. Select the **Enable Safe Money** check box.
5. To enable notification of vulnerabilities detected in the operating system before launching Safe Run for Websites, select the **Notify about operating system vulnerabilities** check box.
6. To configure Safe Money for a specified website:
 - a. In the **Banks and payment system websites** list click the **Add** button.
The **Website for Safe Money** window opens.
 - b. In the window that opens, in the **Bank or payment system website** field enter the URL of a website that should be opened in Safe Run for Websites.

The URL of a website should be preceded by <https://> protocol prefix that Safe Run for Websites uses by default.
 - c. If necessary, in the **Description** field enter the name or a description of that website.
 - d. Select a method for launching Safe Run for Websites when opening the website:
 - If you want Kaspersky Internet Security to offer you to launch Safe Run for Websites every time you open the website, select **Prompt for action**.
 - If you want Kaspersky Internet Security to open the website in Safe Run for Websites automatically, select **Run the protected browser automatically**.
 - If you want to disable Safe Money for the website, select **Do not run the protected browser**.
7. Click the **Apply** button in the **Settings** window.

PRIVACY CLEANER

User actions on a computer are logged in the operating system. The following information is saved:

- details of search queries entered by users and websites visited
- information about applications launched, files opened and saved;
- Microsoft Windows event log entries;
- other user activity information.

Information about user actions containing confidential information may become available to intruders and unauthorized persons.

Kaspersky Internet Security includes the Privacy Cleaner Wizard, which cleans up traces of user activity in the system.

➡ *To start the Privacy Cleaner Wizard:*

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.

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

Make sure that **Search for user activity traces** is selected and click the **Next** button to launch the Wizard.

Step 2. Activity signs search

This Wizard searches for traces of malware activities in your computer. The search may take a while. 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 recommends actions to clean them up (see figure below).

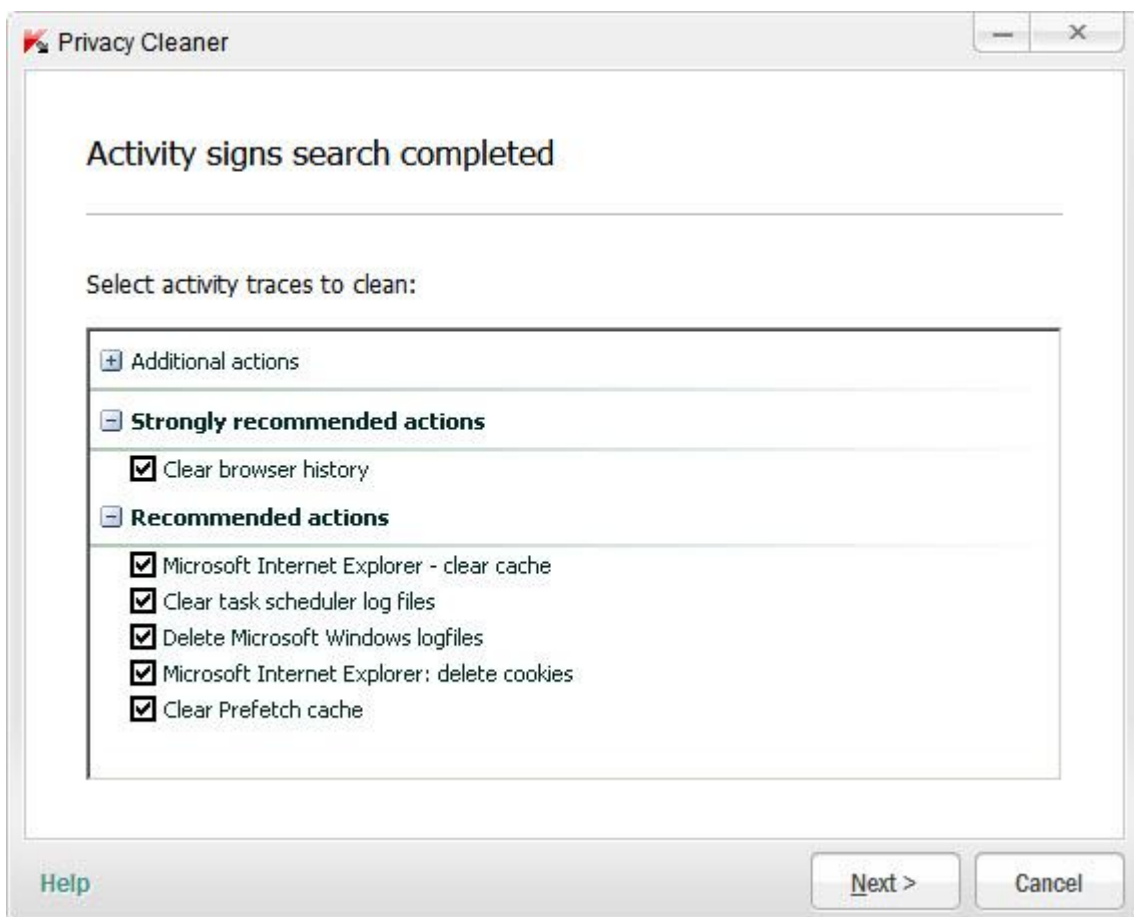


Figure 7. Activity traces detected and recommendations on eliminating them

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, select the check 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, clear the check box next to it.

Clearing the check boxes selected by default is not recommended. This may jeopardize the safety of your computer.

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 Internet Security completes its work, use the last screen of the Wizard to select the check box **Clean activity traces every time on Kaspersky Internet Security 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.

ASSESSING THE SAFETY STATUS OF A WEBSITE

Kaspersky Internet Security allows checking a website for security before going to the website by a link. To do this, a module named *Kaspersky URL Advisor* is used.

Kaspersky URL Advisor is integrated into Microsoft Internet Explorer, Google Chrome, and Mozilla Firefox browsers, checking links on web pages opened in the browser. Kaspersky Internet Security displays one of the following icons next to each link:

-  – if the web page opened by clicking the link is safe according to Kaspersky Lab
-  – if there is no information about the safety status of the web page opened by clicking the link
-  – if the web page opened by clicking the link is dangerous according to Kaspersky Lab.

When rolling the mouse pointer over an icon, a pop-up window with more details on the link is displayed.

By default, Kaspersky Internet Security checks links in search results only. You can enable link checking on every website.

➔ *To enable link checking on every website:*

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the **Settings** window that opens, go to the **Protection Center** section, select the **Web Anti-Virus** subsection and click the **Settings** button.

The **Web Anti-Virus** window opens.

4. In the window that opens, on the **Web Filter** tab, in the **Kaspersky URL Advisor** section click the **Settings** button.

The **Kaspersky URL Advisor settings** window opens.

5. In the window that opens, in the **Scan mode** section select **All URLs**.
6. Click the **Apply** button in the **Settings** window.

BLOCKING ACCESS TO WEBSITES OF VARIOUS REGIONS

According to statistics collected by Kaspersky Lab, the infection rates of websites may vary depending on the country of origin. Kaspersky Internet Security uses a component named Geo Filter to block access to websites that belong to specified regional domains with high infection rates.

When Geo Filter is enabled, Kaspersky Internet Security allows or blocks access to a regional domain, or requests access permission from you, depending on your choice.

► *To enable and configure Geo Filter:*

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the **Settings** window that opens, go to the **Protection Center** section, select the **Web Anti-Virus** subsection and click the **Settings** button.

The **Web Anti-Virus** window opens.

4. In the window that opens, on the **Geo Filter** tab select the **Enable filtering by regional domains** check box.
5. In the bottom part of the window, in the list of controlled domains specify domains to which access should be allowed or blocked, or specify those requiring an access permission request.
6. Click the **Apply** button in the **Settings** window.

IMPOSING PARENTAL CONTROL ON COMPUTER USERS

Parental Control allows the monitoring of actions users take on the computer and online. You can use Parental Control to restrict access to Internet resources and applications, as well as view reports on users' activities.

Nowadays, an ever-increasing number of children and teenagers are obtaining access to computers and web resources. The use of computers and the Internet imposes a whole range of risks on children:

- loss of time and / or money when visiting chat rooms, gaming resources, online stores, auctions;
- access to websites targeted at an adult audience, such as those displaying pornography, extremism, firearms, drug abuse, and explicit violence;
- downloading of files infected with malware;
- health damage inflicted by excessive use of computer;
- contacts with unfamiliar people who may pretend to be peers to obtain personal information from under-age users, such as real name, physical address, time of day when nobody is home.

Parental Control allows you to reduce risks posed by the computer and the Internet. To do this, the following module functions are used:

- limiting the time for computer and Internet use;
- creating lists of allowed and blocked applications, as well as temporarily limiting the number of startups for allowed applications;
- creating lists of allowed and blocked websites and selection of categories of websites with content not recommended for viewing;

- enabling a safe search mode through search engines (links to websites with dubious content are not displayed in the search results);
- restricting file downloads from the Internet;
- creating lists of contacts which are allowed or blocked for communication via IM clients and social networks;
- viewing message logs from IM clients and social networks;
- blocking sending of certain personal data;
- searching for specified key words in message logs.

All these restrictions can be enabled independently from each other, which allows you to flexibly configure Parental Control for various users. For each account, you can view reports of events in the categories to be controlled that the component has logged over a specified period.


IN THIS SECTION

Configuring Parental Control	49
Viewing the report on a user's activity	49

CONFIGURING PARENTAL CONTROL

If you have not protected access to Kaspersky Internet Security settings with a password, at the first launch of Parental Control Kaspersky Internet Security will suggest that you set a password to prevent unauthorized changes to the control settings. You can then configure restrictions for computer and Internet usage by all accounts on the computer.

➤ *To configure Parental Control for an account:*

1. Open the main application window.
2. In the lower part of the window, select the **Parental Control** section.
3. In the section containing the account in the window that opens, click the  button.


The **Parental Control** window opens.

4. In the window that opens, on the **Settings** tab, select the type of restriction in the left part of the window and specify the control settings in the right part of the window.
5. Click the **OK** button in the **Parental Control** window to save the control settings that you have selected.

VIEWING THE REPORT ON A USER'S ACTIVITY

You can access reports on the activity of each user account under Parental Control, reviewing individually each category of controlled events.

➤ *To view a report on the activity of a controlled user account:*

1. Open the main application window.
2. In the lower part of the window, select the **Parental Control** section.
3. In the section containing the account in the window that opens, click the  button.

The **Parental Control** window opens.

4. Select the **Reports** tab.
5. Use the left part of the window that opens to select the category of supervised operations or content, for example, **Internet Usage** or **Private Data**.

A report of actions and content being supervised will be displayed in the right part of the window.

USING GAMING PROFILE FOR FULL-SCREEN MODE

When Kaspersky Internet Security is running concurrently with some applications (particularly video games), the following inconveniences may occur in full-screen mode:

- Performance of the application or that of a game decreases due to lack of system resources
- Notification windows of Kaspersky Internet Security distract the user from the gaming process.

To avoid changing the settings of Kaspersky Internet Security manually every time you switch to full-screen mode, you can use Gaming Profile. When the Gaming Profile is enabled, switching to full-screen mode automatically changes the settings of all the components of Kaspersky Internet Security, ensuring 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. Select the **Use Gaming Profile** check box and specify the necessary Gaming Profile settings in the **Profile options** section below.

CREATING AND USING A RESCUE DISK

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

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

IN THIS SECTION

Creating a Rescue Disk.....	50
Starting the computer from the Rescue Disk.....	52

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\AVP13\Data\Rdisk\`;
- in Microsoft Windows Vista and Microsoft Windows 7 operating systems – in the following folder: `ProgramData\Kaspersky Lab\AVP13\Data\Rdisk\`.

➔ *To run the Kaspersky Rescue Disk Creation Wizard:*

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 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. Select the check box to use the detected file as the original ISO image and go directly to the **Updating disk image** step (see below). Clear this check 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 selected the **Use existing Kaspersky Rescue Disk image** check 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 selected the **Use existing Kaspersky Rescue Disk image** check 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 application 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 application databases, those distributed at the last update of Kaspersky Internet Security 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. After being used to store the disk image, such devices may malfunction.

- 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 [52](#)) if you cannot boot it and run Kaspersky Internet Security 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 [50](#)).

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.

PASSWORD-PROTECTING ACCESS TO KASPERSKY INTERNET SECURITY

A single computer may be shared by several users with various levels of experience and computer literacy. Unrestricted access of different users to Kaspersky Internet Security and its settings may compromise the level of computer security.

To restrict access to the application, you can set the administrator password and specify which actions should require entering this password:

- configuring the application settings;
- managing Parental Control;
- closing the application;
- removing the application.

➤ *To password-protect access to Kaspersky Internet Security:*

1. Open the main application window.
2. In the top right corner of the window, click the **Settings** link.
3. In the **Settings** window that opens, select the **General Settings** subsection in the **Protection Center** section.
4. Select the **Enable password protection** check box and click the **Settings** button.

The **Password protection** window opens.

5. In the window that opens, fill in the **New password** and **Confirm password** fields.
6. To change a previously created password, type it in the **Old password** field.
7. Under the **Apply password to** group of settings, specify the operations with the applications the access to which has to be password protected.
8. Click the **Apply** button in the **Settings** window.

A forgotten password cannot be recovered. If you have forgotten your password, contact Technical Support to restore access to Kaspersky Internet Security settings.

PAUSING AND RESUMING COMPUTER PROTECTION

Pausing protection means temporarily disabling all protection components for some time.

➤ *To pause the protection of your computer:*

1. In the context menu of the application icon in the taskbar notification area, select the **Pause protection** item.

The **Pause protection** window opens (see figure below).

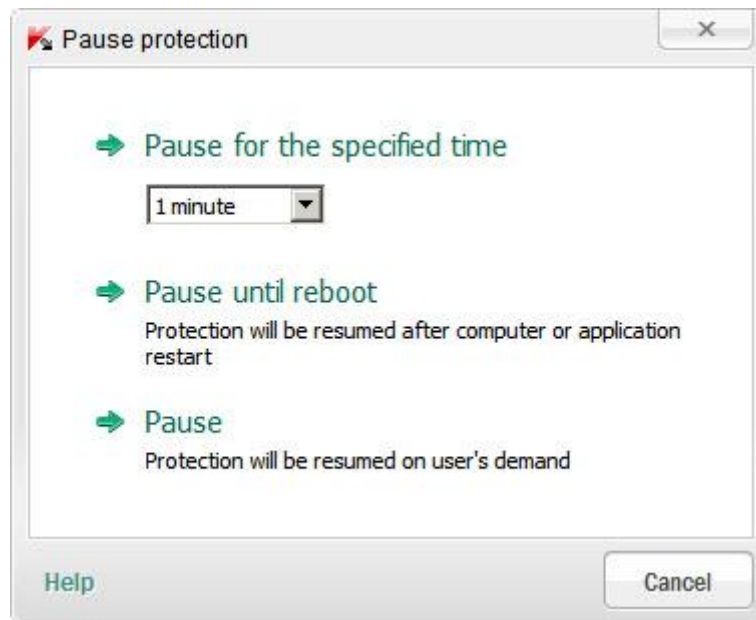


Figure 8. **Pause protection** window

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 drop-down 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).
- **Pause** – protection will be resumed when you decide to resume it.

➤ *To resume computer protection,*


select the **Resume protection** item in the context menu of the application icon in the taskbar notification area.

VIEWING THE APPLICATION OPERATION REPORT

Kaspersky Internet Security maintains operation reports for each of the protection components. 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 "Using Kaspersky Gadget" on page [58](#)).

➤ *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).

Application operation reports are shown as diagrams in the **Reports** window.

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

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

RESTORING THE DEFAULT APPLICATION SETTINGS

You can restore the default application settings recommended by Kaspersky Lab for Kaspersky Internet Security, 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 run the post-infection Microsoft Windows Troubleshooting wizard:*

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the **Settings** window that opens, run Application Configuration Wizard in one of the following ways:
 - click the **Restore** link in the bottom left corner of the window;

- in the upper part of the window, select the **Additional** section, **Manage Settings** subsection and click the **Restore** button in the **Restore default settings** section (see figure below).



Figure 9. Settings window, Manage Settings subsection

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 Internet Security protection components have settings that differ from the default value because they were either changed by the user or accumulated by Kaspersky Internet Security through training (Firewall or Anti-Spam). If special settings have been created for any of the components, they will also be shown in the window (see figure below).

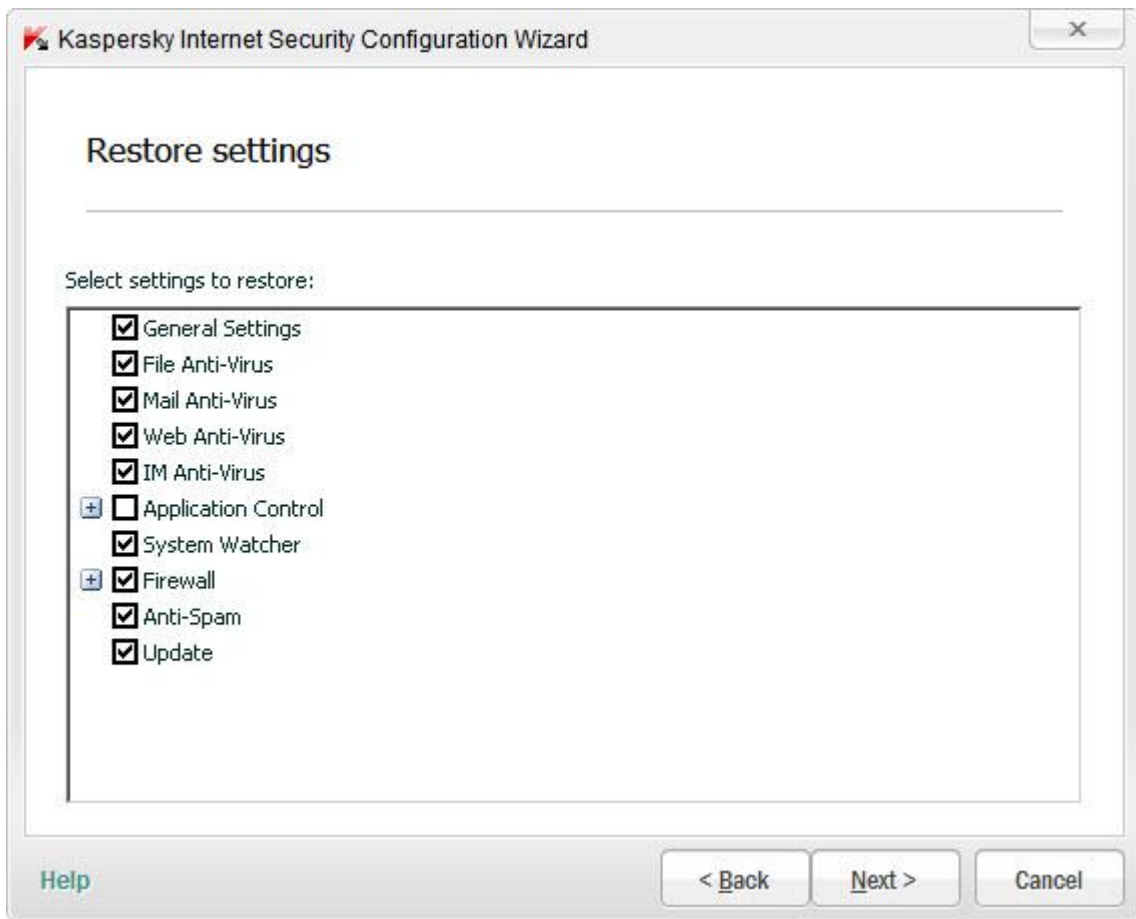


Figure 10. Restore settings window

Special settings include lists of allowed and blocked phrases and addresses used by Anti-Spam, lists of trusted web addresses and ISP phone numbers, protection exclusion rules created for application components, and filtering rules applied by Firewall to packets and applications.

The special settings are created when working with Kaspersky Internet Security with regard for individual tasks and security requirements. Kaspersky Lab recommends that you save your special settings when restoring the default application settings.

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

Step 3. 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 4. Finishing restoration

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

IMPORTING THE APPLICATION SETTINGS TO KASPERSKY INTERNET SECURITY INSTALLED ON ANOTHER COMPUTER

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

The settings of Kaspersky Internet Security can be transferred to another computer in three steps:

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

➤ *To save the settings of Kaspersky Internet Security to a configuration file:*

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the upper part of the **Settings** window, in the **Additional** section select the **Manage Settings** subsection.
4. Click the **Export** button in the **Manage Settings** subsection.
5. In the window that opens, enter the name of the configuration file and specify the location to which it should be saved.
6. Click **OK**.

➤ *To apply the settings from the configuration file to the application installed on another computer:*

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the upper part of the **Settings** window, in the **Additional** section select the **Manage Settings** subsection.
4. Click the **Import** button in the **Manage Settings** subsection.
5. In the window that opens, select the file from which you wish to import the Kaspersky Internet Security settings.
6. Click **OK**.

USING KASPERSKY GADGET

When using Kaspersky Internet Security on a computer running under Microsoft Windows Vista or Microsoft Windows 7, you can also use Kaspersky Gadget (hereinafter also referred to as *the gadget*). After you install Kaspersky Internet Security to 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 "Assessing the computer protection status and resolving security issues" on page [29](#)). 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.

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;
- view Parental Control reports;
- view information about network activity (Network Monitor) and applications' activity;
- pause the protection;
- open the Virtual Keyboard;
- open the Task Manager window.

➤ *To start the application using the gadget,*

click the  **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 drop-down lists corresponding to gadget buttons, select actions that should be performed when you click those buttons.
3. Click **OK**.

PARTICIPATING IN THE KASPERSKY SECURITY NETWORK (KSN)

To increase the efficiency of your computer's protection, Kaspersky Internet Security uses data received from users from all over the world. Kaspersky Security Network is designed for gathering this data.

Kaspersky Security Network (KSN) is an infrastructure of online services that provides access to the online Kaspersky Lab Knowledge Base, 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 Internet Security when encountering new types of threats, improves performance of some protection components, and reduces the risk of false positives.

Thanks to users who participate in Kaspersky Security Network, Kaspersky Lab is able to promptly gather information about types and sources of new threats, develop solutions for neutralizing them, and minimize the number of false positives. Participation in Kaspersky Security Network lets you access reputation statistics for applications and websites.

IN THIS SECTION

Enabling and disabling participation in Kaspersky Security Network.....	60
Checking the connection to Kaspersky Security Network	60

ENABLING AND DISABLING PARTICIPATION IN KASPERSKY SECURITY NETWORK

Participation in Kaspersky Security Network is voluntary. You can enable or disable the use of Kaspersky Security Network when installing Kaspersky Internet Security and / or at any moment after the application is installed.

➔ *To enable or disable participation in Kaspersky Security Network:*

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the **Settings** window that opens, in the **Advanced Settings** section select the **Feedback** subsection.
4. In the right part of the window, do one of the following:
 - If you want to participate in KSN, select the **I agree to participate in Kaspersky Security Network** check box.
 - If you do not want to participate in KSN, clear the **I agree to participate in Kaspersky Security Network** check box.

CHECKING THE CONNECTION TO KASPERSKY SECURITY NETWORK

Connection to Kaspersky Security Network may be lost for the following reasons:

- You do not participate in Kaspersky Security Network.
- Your computer is not connected to the Internet.
- Current key status does not allow to connect to the Kaspersky Security Network.

Current key status is displayed in the **Licensing** window (see section "**Acquiring and renewing a license**" on page [28](#)).

➤ *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.

In the left part of the window that opens, the status of connection to Kaspersky Security Network is displayed.

CONTACTING THE TECHNICAL SUPPORT SERVICE

This section provides information about how to obtain technical support and the requirements for receiving help from Technical Support.

IN THIS SECTION

How to get technical support	62
Technical support by phone	62
Obtaining technical support via My Kaspersky Account	62
Using the trace file and the AVZ script	64

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 [9](#)), 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.

Before contacting Technical Support, 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.
- 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.

Technical support is only available to users who acquired the commercial license. No technical support is provided to users of trial versions.

TECHNICAL SUPPORT BY PHONE

If an urgent issue arises, you can call specialists from Russian-speaking or international Technical Support (<http://support.kaspersky.com/support/international>) by phone.

Before contacting Technical Support, please read the support rules (<http://support.kaspersky.com/support/details>). 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 Technical Support and the Virus Lab.
- Contact Technical Support without using email.
- Track the status of your requests in real time.
- View a detailed history of your Technical Support requests.
- Receive a copy of the key file if it is lost or deleted.

Technical Support by email

You can send an online request to Technical Support in English, Russian, German, French, or Spanish.

In the fields of the online request form, specify the following data:

- 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 must be sent to the Virus Lab instead of Technical Support.

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 Internet Security has not identified it as infected.

Virus Lab specialists analyze malicious code that is 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 Internet Security 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 Internet Security, 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.

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 performing application commands step by step and determine the stage of application operation at which an error occurs.

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.

IN THIS SECTION

Creating a system state report	64
Sending data files.....	64
AVZ script execution	66

CREATING A SYSTEM STATE REPORT

➤ *To create a system state report:*

1. Open the main application window.
2. Click the **Support** link in the bottom part of the window to open the **Support** window.
3. In the window that opens, click the **Support Tools** button.
The **Support Tools** window opens.
4. In the 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. When the information about the system is collected, you can view the report.

➤ *To view the report:*

1. Open the main application window.
2. Click the **Support** link in the bottom part of the window to open the **Support** window.
3. In the window that opens, click the **Support Tools** button.
The **Support Tools** window opens.
4. In the window that opens, click the **View report** link.
The Microsoft Windows Explorer window opens.
5. In the window that opens, open the archive named sysinfo.zip that contains report files.

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 files to the server of Technical Support Service (see section "Obtaining technical support via My Kaspersky Account" on page [62](#)). 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 in the bottom part of the window to open the **Support** window.
3. In the window that opens, click the **Support Tools** button.

The **Support Tools** window opens.

4. In the window that opens, click the **Send service data to Technical Support** button.

The **Send report** window opens.

5. Select the check boxes next to the data that you want to send to the Technical Support Service and click the **Send** button.

The **Enter request number** window opens.

6. 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 in the bottom part of the window to open the **Support** window.
3. In the window that opens, click the **Support Tools** button.

4. The **Support Tools** window opens.

5. In the window that opens, click the **Send service data to Technical Support** button.

The **Send report** window opens.

6. Select the check boxes next to the data that you want to send to the Technical Support Service and click the **Send** button.

The **Enter request number** window opens.

7. 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.

8. 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 obtain technical support" on page [62](#)).

➤ *To run the AVZ script:*

1. Open the main application window.
2. Click the **Support** link in the bottom part of the window to open the **Support** window.
3. In the window that opens, click the **Support Tools** button.

The **Support Tools** window opens.

4. In the window that opens, click the **Run script** button.

The **AVZ script execution** window opens.

5. Copy the text from the script sent by Technical Support Service specialists, paste it to the entry field in the window that opens, and click the **Next** button.

The script is running then.

If the script is successfully executed, the Wizard closes automatically. If an error occurs during script execution, the Wizard displays a message to that effect.

GLOSSARY

A

ACTIVATING THE APPLICATION

Switching the application into full-function mode. Application activation is performed by the user during or after the application installation. The user should have an activation code to activate the application.

ACTIVATION CODE

A code that you receive on acquiring the commercial license for Kaspersky Internet Security. This code is required for activation of the application.

The activation code is a unique sequence of twenty alphanumeric characters in the format xxxxx-xxxxx-xxxxx-xxxxx.

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 Quarantine settings.

ARCHIVE

One or several file(s) packaged into a single file through compression. A dedicated archived application file is required for packing and unpacking data.

AVAILABLE UPDATE

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

BLOCKING AN OBJECT

Denying access to an object from external applications. A blocked object cannot be read, executed, changed, or deleted.

C

COMPRESSED FILE

An archive file that contains a decompression program and instructions for the operating system for executing it.

D

DATABASE OF MALICIOUS WEB ADDRESSES

A list of web addresses whose content may be considered to be dangerous. The list was created by Kaspersky Lab specialists. It is regularly updated and is included in the Kaspersky Lab application package.

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.

DATABASES

Databases that contain descriptions of computer security threats that are known to Kaspersky Lab by the moment of release of the databases. Records that are contained in databases allow detecting malicious code in scanned objects. The databases are created by Kaspersky Lab specialists and updated hourly.

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 disinfected.

DIGITAL SIGNATURE

An encrypted block of data embedded in a document or application. A digital signature is used to identify the document or application author. To create a digital signature, the document or application author must have a digital certificate proving the author's identity.

A digital signature lets you verify the data source and data integrity and protect yourself against counterfeits.

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.

E

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 using wildcards. The standard wildcards used in file masks are * and ?, where * represents any number of any characters and ? stands for any single character.

H

HEURISTIC ANALYZER

A technology for detecting threats information about which has not yet been added to Kaspersky Lab databases. The heuristic analyzer allows detecting objects whose behavior within the system is similar to that typical of threats. Objects detected by the heuristic analyzer are considered probably infected. For example, an object may be considered probably infected if it contains sequences of commands that are typical of malicious objects (open file, write to file).

I

ICHECKER TECHNOLOGY

A technology that allows increasing the speed of anti-virus scanning by excluding objects that have remained unchanged since their last scan, provided that the scan parameters (the databases and the settings) have not been altered. 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 a 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 have changed the archive content by adding a new object to it, modified the scan settings, or updated the application databases, the archive will be 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.

INCOMPATIBLE APPLICATION

An antivirus application from a third-party developer or a Kaspersky Lab application that does not support management through Kaspersky Internet Security.

INFECTABLE OBJECT

An object which, due to its structure or format, can be used by intruders as a "container" to store and spread malicious code. 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.

INFECTED OBJECT

An object a section of whose code completes matches a section of a known threat. Kaspersky Lab does not recommend using such objects.

K

KASPERSKY LAB'S UPDATE SERVERS

Kaspersky Lab HTTP servers to which the updated anti-virus database and the application modules are uploaded.

KASPERSKY SECURITY NETWORK (KSN)

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. The use of data from Kaspersky Security Network ensures faster response by Kaspersky Lab applications to new types of threats, improves the effectiveness of some protection components, and reduces the risk of false positives.

KEYLOGGER

A program designed for hidden logging of information about keys pressed by the user. Keyloggers are also called key interceptors or key spies.

L

LICENSE TERM

License term is a time period during which you have access to the application features and rights to use additional services.

M

MESSAGE DELETION

The method of processing an email message where the message is physically removed. We recommend that this method be applied to messages that definitely contain spam or malware. Before deleting a message, a copy of it is saved in Quarantine (unless this option is disabled).

P**PHISHING**

A kind of Internet fraud, when email messages are sent with the purpose of stealing confidential information. As a rule, this information relates to financial data.

PROBABLE SPAM

A message that cannot be unambiguously considered spam, but has several spam attributes (e.g., certain types of mailings and advertising messages).

PROBABLY INFECTED OBJECT

An object whose code contains modified code of a known threat or code, which is similar to that of a threat, judging by its behavior.

PROTECTION COMPONENTS

Integral parts of Kaspersky Internet Security intended for protection against specific types of threats (for example, Anti-Spam, Anti-Phishing). Each of the components is relatively independent of other ones so it can be disabled or configured individually.

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, FTP, and NNTP.

Q**QUARANTINE**

A dedicated storage to which the application places backup copies of files that have been modified or deleted during disinfection. Copies of files are stored in a special format, imposing no threat for the computer.

R**ROOTKIT**

A program or a set of programs for hiding traces of an intruder or malware in the operating system.

On Windows-based operating systems, a rootkit usually means a program that penetrates into the operating system and intercepts system functions (Windows APIs). Above all, interception and modification of low-level API functions allow such a program to make its presence in the operating system quite stealthy. A rootkit can usually also mask the presence of any processes, folders, and files that are stored on a disk drive, in addition to registry keys, if they are described in the configuration of the rootkit. Many rootkits install their own drivers and services on the operating system (these 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 specific task. It is most often used with programs that are embedded in hypertext. Scripts are run, for example, when you open specified websites.

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 scanning, you may block or allow the execution of a script.

SECURITY LEVEL

The security level is defined as a predefined collection of settings for an application component.

SPAM

Unsolicited mass email mailings, most often including advertising messages.

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.

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.

THREAT LEVEL

An index showing the probability of an application imposing a threat to the operating system. The threat level is calculated using heuristic analysis based on two types of criteria:

- static (such as information about the executable file of an application: size, creation date, etc.);
- dynamic, which are used while simulating the application's operation in a virtual environment (analysis of the application's requests to system functions).

Threat level allows detecting behavior typical of malware. The lower the threat level is, the more actions the application will be allowed to perform in the system.

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

Real-time scanning that uses information from the current (latest) version of the databases for objects transferred over 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. When detecting a suspicious activity of a trusted process, Kaspersky Internet Security excludes the process from the list of trusted ones and blocks all of its activities.

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 probably infected.

UPDATE

The procedure of replacing/adding new files (databases or application modules) retrieved from the Kaspersky Lab update servers.

UPDATE PACKAGE

A file package for updating application modules. A Kaspersky Lab's application copies update packages from Kaspersky Lab's update servers and automatically installs and applies them.

V**VIRUS**

A program that infects other ones by adding its code to them in order to gain control when infected files are run. This simple definition allows exposing the main action performed by any virus – infection.

VIRUS OUTBREAK

A series of deliberate attempts to infect a computer with a virus.

VULNERABILITY

A flaw in an operating system or an application that may be exploited by malware makers to penetrate into the system or the application and corrupt its integrity. A large number of vulnerabilities in a system makes it unreliable, because viruses that have penetrated into the system may cause operation failures in the system itself and in installed applications.

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 hundreds 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 therefore logical for many third-party software developers to use the kernel of Kaspersky Anti-Virus in their own applications. Those companies include 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), and 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 received several top Advanced+ awards in a test administered by AV-Comparatives, a respected Austrian anti-virus laboratory. 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's website:

<http://www.kaspersky.com>

Virus encyclopedia:

<http://www.securelist.com>

Anti-virus laboratory:

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's web forum:

<http://forum.kaspersky.com>

INFORMATION ABOUT THIRD-PARTY CODE

Information about third-party code is contained in the file legal_notices.txt, in the application installation folder.

TRADEMARK NOTICES

Registered trademarks and service marks are the property of their respective owners.

Google Chrome is a trademark owned by Google, Inc.

Intel and Pentium are trademarks of Intel Corporation registered in the United States of America and elsewhere.

Microsoft, Windows, Windows Vista and Internet Explorer are trademarks of Microsoft Corporation registered in the United States of America and elsewhere.

Mozilla and Firefox are trademarks of Mozilla Foundation.

INDEX

A

Activating the application.....	30
Activation code.....	26
Additional Tools	
Microsoft Windows Troubleshooting.....	37
Privacy Cleaner.....	50
Rescue Disk.....	56
Anti-Phishing.....	44
Anti-Spam.....	40
Application Control	
exclusions.....	42
Application activation	
activation code.....	26
license.....	25
trial version.....	19
Application components.....	12
Application Control	
creating an application rule.....	42
device access rules.....	42
Application databases.....	33

C

Confidential data.....	44
------------------------	----

D

Diagnostics.....	32
Disinfected object.....	36
Domain region.....	53

E

End User License Agreement.....	25
Event log.....	60

F

Firewall	
creating an application rule.....	42
Full-screen application operation mode.....	55

G

Gadget.....	65
Gaming Profile.....	55

H

Hardware requirements.....	14
----------------------------	----

I

Importing / exporting the settings.....	64
Infected object.....	75
INSTALLING THE APPLICATION.....	16

K

KASPERSKY.....	79
KASPERSKY LAB.....	79
Kaspersky Security Network	66
Kaspersky URL Advisor Web Anti-Virus.....	52
Key.....	25
Keyboard interceptor protection against data interception at the keyboard	48
Keyboard interceptors Virtual Keyboard	45

L

License.....	25
activation code.....	26
End User License Agreement.....	25

M

Mail Anti-Virus	39
Microsoft Windows Troubleshooting.....	37

N

Notifications.....	31
--------------------	----

O

Online Banking.....	49
---------------------	----

P

Parental Control	53
enabling and configuring.....	54
statistics on component operation	55
Protection status.....	32

Q

Quarantine restoring an object	36
---	----

R

Removing the application	23
Reports.....	60
Rescue Disk	56
Restoring the default settings.....	61
Restricting access to the application	58

S

Security analysis	32
Security problems.....	32
Security threats	32
Software requirements	14
Spam.....	40
Statistics.....	60

T

The Kaspersky Gadget.....	65
---------------------------	----

Traces
 uploading tracing results71

U

Unknown applications41
 Unwanted email.....40
 Update.....33
 Update source.....33
 User account54

V

Viewing statistics60
 Virtual Keyboard.....45
 Vulnerability.....40
 Vulnerability Scan.....40

W

Web Anti-Virus
 Geo Filter.....53
 Kaspersky URL Advisor52
 Safe Surf.....52