

Kaspersky Internet Security

Downloaded from www.vandenborre.be

KASPERSKY **lab**

User Guide

APPLICATION VERSION: 14.0

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 incur civil, administrative, or criminal liability under 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 on the Kaspersky Lab website, at <http://www.kaspersky.com/docs>.

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

Registered trademarks and service marks used in this document are the property of their respective owners.

Document revision date: 6/3/2013

© 2013 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.....	12
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 Finding a newer version of the application.....	16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 Statement.....	16
Step 5. Installation.....	17
Step 6. Completing installation.....	17
Step 7. Activating the application.....	17
Step 8. Registering a user.....	18
Step 9. Completing the activation.....	18
Upgrading a previous version of the application.....	18
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 Statement.....	20
Step 5. Installation.....	20
Step 6. Completing installation.....	21
Removing the application.....	21
Step 1. Entering the password to remove the application.....	21
Step 2. Saving data for future use.....	22
Step 3. Confirming application removal.....	22
Step 4. Removing the application. Completing removal.....	22
APPLICATION LICENSING.....	23
About the End User License Agreement.....	23
About the license.....	23
About the activation code.....	24
About the subscription.....	24
About data provision.....	25

SOLVING TYPICAL TASKS.....	27
Activating the application	28
Acquiring and renewing a license.....	28
Managing application notifications.....	29
Assessing computer protection status and resolving security issues.....	30
Updating databases and application modules.....	31
Full scan of the computer for viruses.....	31
Scanning a file, folder, disk, or another object for viruses.....	32
Scanning the computer for vulnerabilities	33
Scanning critical areas of your computer for viruses	33
Scanning probably infected objects.....	33
Restoring an object deleted or disinfected by the application.....	34
Recovering the operating system after infection	35
Mail Anti-Virus Setup.....	36
Blocking unwanted email (spam)	37
Handling unknown applications.....	37
Checking application reputation.....	37
Control application activity on the computer and on the network	38
Using Trusted Applications mode	40
Protecting private data against theft	42
Virtual Keyboard	42
Protection of data input from the computer keyboard.....	45
Safe Money Setup	46
Privacy Cleaner	47
Verifying website safety.....	49
Using Parental Control	50
Control computer usage.....	51
Control Internet usage.....	52
Control running of games and applications.....	54
Control messaging on social networks	55
Control contents of messages	55
Viewing the report on a user's activity	57
Using Gaming Profile for full-screen mode	57
Creating and using a Rescue Disk	57
Creating a Rescue Disk.....	58
Starting the computer from the Rescue Disk	60
Password-protecting access to Kaspersky Internet Security.....	60
Pausing and resuming computer protection.....	61
Restoring the default application settings	61
Viewing the application report	64
Using Kaspersky Gadget	64
Participating in Kaspersky Security Network (KSN).....	65
Enabling and disabling participation in Kaspersky Security Network.....	66
Checking the connection to Kaspersky Security Network.....	66
Participating in Protect a Friend program.....	67
Logging in to your profile in the Protect a Friend program	67
How to share a link to Kaspersky Internet Security with friends.....	68
Exchanging points for a bonus activation code.....	69

CONTACTING TECHNICAL SUPPORT 71

- How to get technical support..... 71
- Technical support by phone..... 71
- Obtaining technical support via My Kaspersky Account.....71
- Using trace files and AVZ scripts 72
 - Creating a system state report..... 73
 - Sending data files 73
 - AVZ script execution 74

GLOSSARY 75

KASPERSKY LAB ZAO 81

INFORMATION ABOUT THIRD-PARTY CODE 82

TRADEMARK NOTICES..... 82

INDEX..... 83

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 document contains 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 End User License Agreement, 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 Technical Support

This section provides information about how to contact Technical Support 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 [71](#)).

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 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/kis2014>), 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 Technical Support.

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.....	12
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:

- To increase security of applications, Trusted Applications mode has been added. When Trusted Applications mode is enabled, Kaspersky Internet Security automatically detects secure applications and allows running secure applications only.
- The functionality of Safe Money has been improved. You can now select a web browser to open websites of banks or payment systems. The list of popular websites for financial operations with automatic enabling of the Safe Money mode has also been added.
- The functionality of Parental Control has been improved: the option of setting up permissions to run games and applications has been added. The preset templates of Parental Control settings that are appropriate to the age of controlled users have been added.
- It is now easier to set up Kaspersky Internet Security. Now only frequently used application settings are available for setup.
- The latest versions of popular web browsers are now supported: protection components (e.g., Kaspersky URL Advisor, Safe Money) support Mozilla™ Firefox™ 16.x, 17.x, 18.x, and 19.x; Internet Explorer® 8, 9, and 10; and Google Chrome™ 22.x, 23.x, 24.x, 25.x, and 26.x.
- Protection against screen lockers has been added. You can unlock the screen using the specified key shortcut. Protection against screen lockers detects and eliminates the threat.
- Protection against phishing is now more efficient: Anti-Phishing functionality has been improved and updated.
- Application performance has been improved and computer resource consumption has been optimized.
- The mode of limited activity when the computer is idle has been added. Now, when the computer is idle, Kaspersky Internet Security is less resource-intensive that allows saving power consumption while running on battery power.
- Less time is required to start the application.
- Application GUI performance has been improved, and the response time to user actions has been reduced.

- Application reporting has been improved. Now reports are simpler and more obvious.
- The option of participating in the Protect a Friend program has been added. You can now share a link to Kaspersky Internet Security with friends and receive bonus activation codes.

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 **Online store**) 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, which 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 activating the application, including an activation code, will be sent to you by email after your payment has been received.

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 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 from the installation CD)
- Internet access (for the application activation and for updating databases and software modules)
- Internet Explorer 8.0 or later.
- Microsoft® Windows® Installer 3.0 or later.
- Microsoft .NET Framework 4.

Requirements for Microsoft Windows XP Home Edition (Service Pack 3 or later), Microsoft Windows XP Professional (Service Pack 3 or later), and Microsoft Windows XP Professional x64 Edition (Service Pack 2 or later):

- 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 (Service Pack 1 or later), Microsoft Windows Vista Home Premium (Service Pack 1 or later), Microsoft Windows Vista Business (Service Pack 1 or later), Microsoft Windows Vista Enterprise (Service Pack 1 or later), Microsoft Windows Vista Ultimate (Service Pack 1 or later), Microsoft Windows 7 Starter, Microsoft Windows 7 Home Basic, Microsoft Windows 7 Home Premium, Microsoft Windows 7 Professional, Microsoft Windows 7 Ultimate, Microsoft Windows 8, Microsoft Windows 8 Pro, and Microsoft Windows 8 Enterprise:

- 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
Upgrading a previous version of the application.....	18
Removing the application.....	21

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 by using the **Back** and **Next** buttons. To close the Wizard after it completes 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 defined by the terms of the End User License Agreement), 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 Statement.....	16
Step 5. Installation.....	17
Step 6. Completing installation.....	17
Step 7. Activating the application.....	17
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 STATEMENT

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 personal data received from you is collected, processed, or stored.

Review the Kaspersky Security Network Statement. If you accept all of its terms, click the **Accept** button in the Wizard window.

If you do not want to participate in Kaspersky Security Network, click the **Decline** button.

After you accept or decline participation in Kaspersky Security Network, the application installation continues.

STEP 5. INSTALLATION

Some versions of Kaspersky Internet Security are distributed under subscription, and a password received from the service provider must be entered before installation.

After you enter the password, the application installation starts.

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 start using Kaspersky Internet Security immediately, make sure that the **Start Kaspersky Internet Security** check box is selected and click the **Finish** button.

If you have cleared the **Start Kaspersky Internet Security** check box before closing the Wizard, you should run the application manually.

In some cases, you may need to reboot your operating system to complete installation.

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 the application.** Select this option and enter an activation code if you have purchased a license for the application.

If you specify the activation code for Kaspersky Anti-Virus in the entry field, the procedure of switching to Kaspersky Anti-Virus will be started when the activation is completed.

- **Activate trial version of the application.** Select this activation option if you want to install the trial version of the application before making a decision on whether to purchase a license. You will be able to use the fully-functional version of the application during the term limited by the conditions of the trial use. 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 not available in all of the versions of Kaspersky Internet Security.

Registered users are able to send requests to Technical Support and the 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 license in effect is provided in this window: license 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.

UPGRADING A PREVIOUS VERSION OF THE APPLICATION

Installing a new version of Kaspersky Internet Security over a previous version of Kaspersky Internet Security

If an earlier version of Kaspersky Internet Security is already installed on your computer, you can upgrade it to the latest version of Kaspersky Internet Security. If you have a license in effect for an earlier version of Kaspersky Internet Security, you will not have to activate the application: the Setup Wizard will automatically retrieve the information about the license for the current version of Kaspersky Internet Security and apply it during installation of the latest version of Kaspersky Internet Security.

Installing a new version of Kaspersky Internet Security over a previous version of Kaspersky Anti-Virus

If you install a new version of Kaspersky Internet Security to a computer on which one of the previous versions of Kaspersky Anti-Virus has been already installed with a license in effect, the Activation Wizard prompts you to select one of the following options for further actions:

- Continue using Kaspersky Anti-Virus under the current license. In this case, the Migration Wizard will be started. When the Migration Wizard finishes, the new version of Kaspersky Anti-Virus will be installed on your computer. You can use Kaspersky Anti-Virus before the license for the previous version of Kaspersky Anti-Virus expires.
- Proceed with installation of the new version of Kaspersky Internet Security. In this case, the application will be installed and activated according to the standard scenario.

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 by using the **Back** and **Next** buttons. To close the Wizard after it completes 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 defined by the terms of the End User License Agreement), 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 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 STATEMENT

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 personal data received from you is collected, processed, or stored.

Review the Kaspersky Security Network Statement. If you accept all of its terms, click the **Accept** button in the Wizard window.

If you do not want to participate in Kaspersky Security Network, click the **Decline** button.

After you accept or decline participation in Kaspersky Security Network, the application installation continues.

STEP 5. INSTALLATION

Some versions of Kaspersky Internet Security are distributed under subscription, and a password received from the service provider must be entered before installation.

After you enter the password, the application installation starts.

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

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

REMOVING THE APPLICATION

After removing Kaspersky Internet Security, your computer and private 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 **All Programs** → **Kaspersky Internet Security** → **Remove Kaspersky Internet Security**.

IN THIS SECTION

Step 1. Entering the password to remove the application	21
Step 2. Saving data for future use	22
Step 3. Confirming application removal.....	22
Step 4. Removing the application. Completing removal.....	22

STEP 1. ENTERING THE PASSWORD TO REMOVE THE APPLICATION

To remove Kaspersky Internet Security, you should enter the password to access the application settings. If you cannot specify the password by any reason, the application removal will be prohibited.

This step is displayed only if a password was set for the application removal.

STEP 2. 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 the license.

- ◆ *To save data for further use, select the check boxes next to the pieces of data 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** are 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.

- **Operational settings of the application** are the values of the application settings selected during configuration.

Kaspersky Lab does not guarantee support of previous application version settings. After the new version is installed, we recommend checking the correctness of its settings.

You can also export protection settings at the command prompt, by using the following command:

```
avp.com EXPORT <file_name>
```

- **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 3. CONFIRMING APPLICATION REMOVAL

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

STEP 4. REMOVING THE APPLICATION. COMPLETING REMOVAL

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

After you finish the removal of Kaspersky Internet Security, you can specify reasons of the application removal on Kaspersky Lab website. To do this, you should go to Kaspersky Lab website by clicking the **Complete form** button.

When removing the application, you must reboot your operating system. If you cancel an 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 End User License Agreement, ways of activating the application, and the license renewal.

IN THIS SECTION

About the End User License Agreement	23
About the license	23
About the activation code.....	24
About the subscription	24
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](#)).

To manage the application, you should purchase a license for the application use.

The license has a limited term. When the license expires, the application continues running, though with a limited functionality (for example, you cannot update the application or use Kaspersky Security Network). 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 should renew your license.

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

Before purchasing a license, you can get acquainted the trial version of Kaspersky Internet Security without any fees. The trial version of Kaspersky Internet Security remains functional during a short evaluation period. After the evaluation period ends, Kaspersky Internet Security stops running all of its features. To continue using the application, you should purchase a license.

ABOUT THE ACTIVATION CODE

Activation code is a code that you receive on purchasing a 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.
- If you participate in the Protect a Friend program (see the section "Participation in the Protect a Friend program" on page 67), you can receive a bonus activation code in exchange for your bonus points.

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 application activation, contact Kaspersky Lab Technical Support to restore the activation code (<http://support.kaspersky.com>).

ABOUT THE SUBSCRIPTION

Subscription for Kaspersky Internet Security is an order for the application with the selected settings (the expiration date and the number of protected devices). You can order a subscription for Kaspersky Internet Security from a service provider (for example, from your Internet provider). You can pause or resume your subscription, renew it in automatic mode, or cancel it. You can manage your subscription via your personal cabinet on the service provider's website.

Service providers can provide two types of subscription for Kaspersky Internet Security: subscription for update and subscription for update and protection.

Subscription can be limited (for example, one-year) or unlimited (with no expiration date). To continue using Kaspersky Internet Security after the limited subscription expires, you should renew it. Unlimited subscription is renewed automatically provided a prepayment to the service provider was timely.

If the subscription term is limited, upon its termination a privileged period for subscription prolongation will be granted to you during which the application functionality remains unchanged.

If the subscription is not renewed when the privileged period expires, Kaspersky Internet Security stops updating the application databases (for subscription for update), as well as providing protection of the computer and running scan tasks (for subscription for update and protection).

To use Kaspersky Internet Security under subscription, you should apply the activation code received from the service provider. In some cases, an activation code can be downloaded and applied automatically. When using the application under subscription, you cannot apply another activation code to renew your license. You can do it only when the subscription term expires.

If Kaspersky Internet Security is already in use under the current license when you register your subscription, Kaspersky Internet Security will be used under subscription after registration. The activation code that you have used to activate the application can be applied on another computer.

To refuse the subscription, you need to contact the service provider from whom you purchased Kaspersky Internet Security.

Depending on the subscription provider, the set of subscription management options may vary. In addition, you may not be provided with a grace period during which you can renew the subscription.

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.
- application operation details and license details required to configure the display of trusted websites' content

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 the section "Participating in Kaspersky Security Network (KSN)" on page [65](#)), 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 about all potentially infected objects and decisions made in relation to those objects
- information about applications being downloaded and run;
- Information about licensing of the installed Kaspersky Internet Security version
- information about interface errors and the use of the interface of Kaspersky Internet Security
- application details, including application version, information about files of downloaded modules, and versions of current application databases
- statistics of updates and connections to Kaspersky Lab servers
- information about the currently used wireless connection

- statistics of the actual time spent by application components on objects scanning.
- statistics of delays occurring when starting applications related with the operation of Kaspersky Internet Security
- files that can be used by criminals to damage your computer, or fragments of such files, including files detected by malicious links.

Information to be sent to Kaspersky Lab can be stored on your computer no longer than 30 days since it was created. Data items are kept in an internal protected storage. The maximum volume of data to store is 30 MB.

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.

Kaspersky Lab protects any information received in this way as prescribed by the law. Kaspersky Lab uses any retrieved information as general statistics only. General statistics are automatically generated using original retrieved information and do not contain any personal data or other confidential information. Original retrieved information is stored in encrypted form; it is cleared as it is accumulated (twice per year). General statistics are stored indefinitely.

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 computer protection status and resolving security issues	30
Updating databases and application modules	31
Full scan of the computer for viruses	31
Scanning a file, folder, disk, or another object for viruses	32
Scanning the computer for vulnerabilities	33
Scanning critical areas of your computer for viruses	33
Scanning probably infected objects	33
Restoring an object deleted or disinfected by the application	34
Recovering the operating system after infection	35
Configuring Mail Anti-Virus	36
Blocking unwanted email (spam)	37
Handling unknown applications	37
Protecting private data against theft	42
Checking a website for safety	49
Using Parental Control	50
Using Gaming Profile for full-screen mode	57
Creating and using a Rescue Disk	57
Password-protecting access to Kaspersky Internet Security	60
Pausing and resuming computer protection	61
Restoring the default application settings	61
Viewing the application operation report	64
Using Kaspersky Gadget	64
Participating in Kaspersky Security Network (KSN)	65
Participating in Protect a Friend program	67

ACTIVATING THE APPLICATION

You need to activate the application to be able to use its functionality and associated services (see the section "About the activation code" on page [24](#)).

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.
- In the lower part of the main application window, click the **Licensing** link. 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 in the corresponding field and click the **Activate** 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

This step is not available in all of the versions of Kaspersky Internet Security.

Registered users are permitted to use the following features:

- Send requests to Technical Support and the 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 purchasing a license, you can purchase one after installation. When you purchase a license, you receive an activation code that is used to activate the application (see the section "Activating the application" on page [28](#)).

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

➤ *To acquire a license:*

1. Open the main application window.
2. In the lower part of the main window, click the **Enter activation code / Licensing** link. The **Licensing** window opens.
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 new activation code:*

1. Open the main application window.
2. In the lower part of the main window, click the **Enter activation code / Licensing** link. The **Licensing** window opens.
3. In the window that opens, click the **Activate the application** button.

The Application Activation Wizard opens.

4. Enter the activation code in the corresponding fields and click the **Activate** 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 and requiring 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 a notification is displayed on the screen, you should select one of the options that are suggested in the notification. The optimal option is the one recommended as the default by Kaspersky Lab experts. A notification can be closed automatically by restarting the computer, closing Kaspersky Internet Security, or enabling the Connected Standby mode in Windows 8. When closing a notification automatically, Kaspersky Internet Security performs the action recommended by default.

Notifications are not displayed during the first hour of the application operation if you have purchased a computer with preinstalled Kaspersky Internet Security (OEM distribution). The application processes detected objects in accordance with the recommended actions. Processing results are saved in a report.

ASSESSING 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 the following figure). 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, and red alerts of serious threats to the computer's security. You are advised to fix 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 following figure) 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 the Internet.

When working in Microsoft Windows 8, updates are not downloaded if a broadband Internet connection is established and a limit is imposed on traffic under this type of connection. To download updates, you should lift the limitations manually in the **Network** subsection of the application settings window.

- *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.
The window displays the **Update** section.
 2. In the **Update** section click the **Run update** 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.
The window displays the **Scan** section.
 2. Select the **Full Scan** section in the right part of the window.
The window displays the **Full Scan** section.
 3. Click the **Start scan** button.

Kaspersky Internet Security starts the full scan of your computer.

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
- By using the Kaspersky Internet Security Gadget (only on Microsoft Windows Vista and Microsoft Windows 7)

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

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

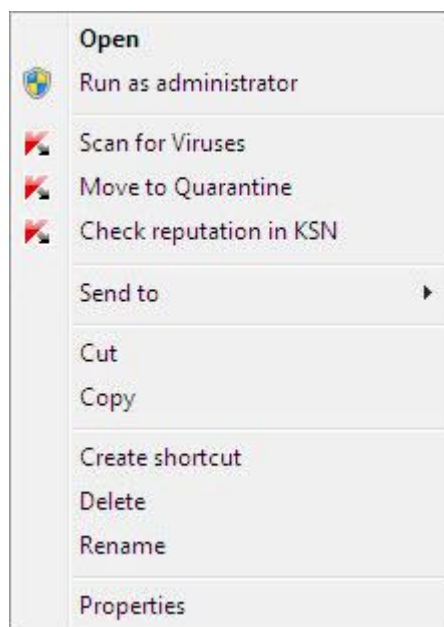


Figure 3. Context menu of an executable file in Microsoft Windows

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

1. Open the main application window and select the **Scan** section in the lower part of the window.
2. Proceed to the **Custom Scan** section in the right part of the window.
3. Specify objects to be scanned in one of the following ways:
 - Drag objects to the **Custom Scan** window.
 - Click the **Add** button and specify an object in the file or folder selection window that opens.
4. Click the **Start scan** button.

The **Task Manager** window opens displaying details on the scan progress.


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

drag the object to the gadget.

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:*

1. Open the main application window.
2. In the lower part of the window, click the  button and select the **Tools** section.

The window displays the **Tools** section.

3. In the **Vulnerability Scan** section, click the **Start** button.

Kaspersky Internet Security starts scanning your computer for vulnerabilities.

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 Critical Areas Scan from the main application window:*

1. Open the main application window and select the **Scan** section in the lower part of the window.

The window displays the **Scan** section.

2. Open the **Quick Scan** section in the right part of the window.

The window displays the **Quick Scan** section.

3. Click the **Start scan** button.

Kaspersky Internet Security starts the scanning process.

SCANNING PROBABLY INFECTED OBJECTS

If you suspect that an object is infected, scan it with Kaspersky Internet Security.

If the application completes the scan and reports that an object is safe although you suspect the contrary, you can send this object to the *Virus Lab*: Virus Lab specialists scan the object. If it turns out to be infected with a virus, they add the description of the new virus to the databases that will be downloaded by the application with an update.

➤ *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.

Kaspersky Internet Security does not disinfect applications from Windows Store. If after the scan the application is recognized as dangerous, it will be deleted from your computer.

When you delete an application from Windows Store, Kaspersky Internet Security does not create its backup copy. To restore such objects, you need to use recovery tools of the operating system (for detailed information, see the documentation for the operating system that is installed on your computer) or update the applications from Windows Store.

➤ 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 the following figure).

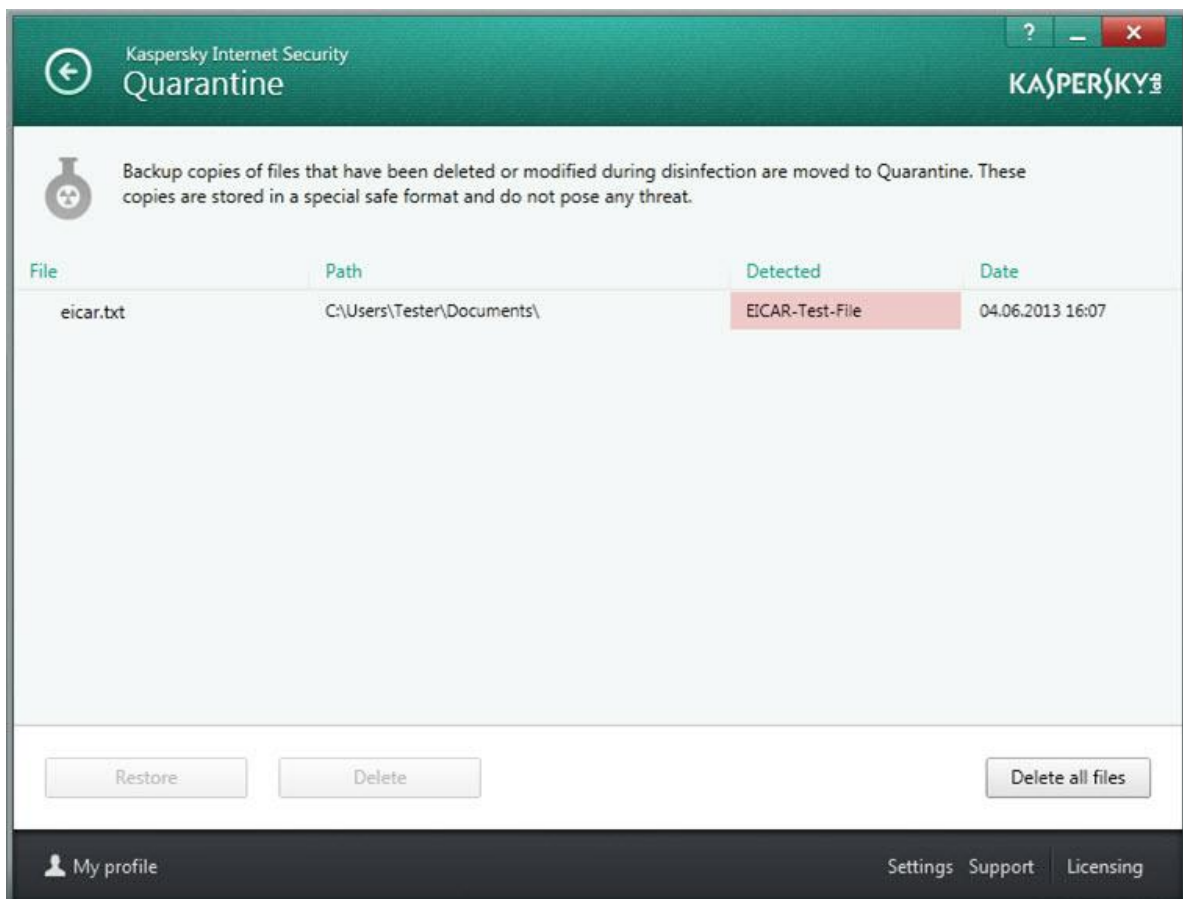


Figure 4. Quarantine window

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 by using the **Back** and **Next** buttons. To close the Wizard after it completes 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. When the search is complete, the Wizard proceeds 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* are aimed at repairing damage that poses a 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. 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.

After you define 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.

MAIL ANTI-VIRUS SETUP

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 configure Mail Anti-Virus:*

1. Open the main application window.
2. In the lower 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.

The Mail Anti-Virus settings are displayed in the window.

4. Make sure that the switch in the upper part of the window that enables / disables Mail Anti-Virus, is enabled.
5. Select a security level:
 - **Recommended.** If you select this security level, Mail Anti-Virus scans both incoming and outgoing messages and scans attached archives.
 - **Low.** If you select this security level, Mail Anti-Virus scans incoming messages only without scanning attached archives.
 - **High.** If you select this security level, Mail Anti-Virus scans both incoming and outgoing messages and scans attached archives. Selecting high security level means applying deep heuristic analysis.
6. In the **Action on threat detection** dropdown list select an action that Mail Anti-Virus should perform when an infected object is detected (for example, disinfect).

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 the section "Restoring an object deleted or disinfected by the application" on page [34](#)).

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. Click the **Settings** link in the lower part of the window to go to the **Settings** section.
3. In the left part of the window, select the **Protection Center** section.
4. In the right part of the **Protection Center** section, select **Anti-Spam** component.

The window displays the settings of Anti-Spam.

5. In the right part of the window, enable Anti-Spam using a switch.
6. Make sure that the **Recommended** security level is set in the **Security level** section.

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 application activities on the computer and on the network	38
Using Trusted Applications mode	40

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 the following figure).

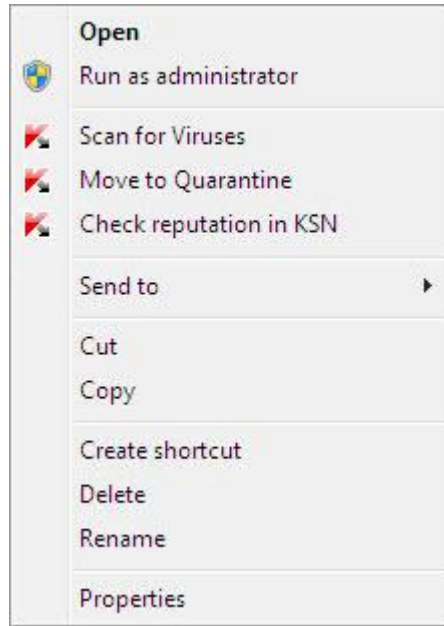


Figure 5. Context menu of an executable file in Microsoft Windows

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

SEE ALSO:

Participating in Kaspersky Security Network (KSN) [65](#)

CONTROL APPLICATION ACTIVITY 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 personal data.

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

When working under 64-bit operating systems, applications' rights to configuration of the following actions are unavailable:

- Direct access to physical memory
- Printer driver management
- Service creation

- Service reading
- Service editing
- Service reconfiguration
- Service management
- Service start
- Service removal
- Access to internal browser data
- Access to critical system objects
- Access to password storage
- Debugger rights setup
- Use of system interfaces
- Use of system interfaces (DNS).

When working under 64-bit Microsoft Windows 8, applications' rights to configuration of the following actions are also unavailable:

- Sending of window messages to other processes
- Suspicious operations
- Installation of interceptors
- Interception of inbound stream events
- Making of screenshots.

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 lower part of the window, click the  button and select the **Application Control** section.

The window displays the **Application Control** section.

3. In the **Applications** section, click the **Manage applications** link.

The window displays the **Application management** section.

4. Click the required application on the list.

The **Application rules** window opens.

5. Specify application control 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.

Application Control will monitor and restrict the application's actions in accordance with the specified settings.

USING TRUSTED APPLICATIONS MODE

In Kaspersky Internet Security, you can create a secure environment on your computer, Trusted Applications mode, in which only applications with trusted status are allowed to run. Trusted Applications mode will be useful to you if you use a stable set of well-known applications and you do not need to frequently download and run new unknown files from the Internet. When Trusted Applications mode is enabled, Kaspersky Internet Security blocks all applications that have not been classified as trusted by any criteria (for example, information about the application from KSN and trust in the installer and source of the application).

Trusted Applications mode may be missing or unavailable in the current version of Kaspersky Internet Security. The availability of Trusted Applications mode in Kaspersky Internet Security also depends from your region and provider. Please clarify if you need Trusted Applications mode when purchasing the application.

If Trusted Applications mode is provided for in your version of Kaspersky Internet Security but is not currently available, it may become available after you update (see the section "Updating databases and application modules" on page [31](#)) the application.

Also, Trusted Applications mode may be unavailable if system files are located on partitions of a hard drive with a non-NTFS file system.

Before enabling Trusted Applications mode, Kaspersky Internet Security analyzes your operating system and the applications installed on your computer. If the analysis detects software that cannot be classified as trusted, you are not advised to enable Trusted Applications mode. Blocking untrusted applications may affect your use of the computer. You can manually allow running applications that you trust and then enable Trusted Applications mode.

Analysis of the operating system and installed applications is performed when Trusted Applications mode is enabled for the first time. Analysis may take a long time (up to a few hours). Analysis can be run in the background.

To use Trusted Applications mode, make sure that all of the following protection components are enabled: Application Control, File Anti-Virus, and System Watcher. If any of these components stops running, Trusted Applications mode is disabled.

You can disable Trusted Applications mode at any time, if necessary.

➤ *To enable Trusted Applications mode:*

1. Open the main application window.

2. In the lower part of the window, click the  button and select the **Application Control** section.

The window displays the **Application Control** section.

3. In the lower part of the window, in the **Trusted Applications mode is disabled** section, click the **Enable** link.

If all of the required protection components are enabled, the **Enable Trusted Applications mode** window opens, providing information about protection components that must be enabled before you can enable Trusted Applications mode.

4. Click the **Continue** button.

Analysis of system files and installed applications starts. The progress of the analysis is displayed in the **Analysis of installed applications** window that opens.

Wait until the analysis of installed applications is complete. You can minimize the **Analysis of installed applications** window. The analysis will be performed in background mode. You can view the progress of the analysis of installed applications by clicking the **Progress of analysis of installed applications (<N> %)** link in the **Application Control** window.

5. View information about the results of the analysis in the **Analysis of installed applications is complete** window.

If system files with unrecognized properties are detected during analysis, you are advised to avoid enabling Trusted Applications mode. You are also advised to avoid enabling Trusted Applications mode if many applications have been detected, for which Kaspersky Internet Security does not have enough information to classify them as completely safe. Decide whether to use Trusted Applications mode.

6. Click the **Allow running unknown system files and continue** link.

You can view information about untrusted system files by clicking the **Go to the list of unknown system files** link. The list of untrusted system files is displayed in the **Unknown system files** window. You can also cancel the use of Trusted Applications mode by clicking the **Do not enable Trusted Applications mode** button.

7. Click the **Enable Trusted Applications mode** button.

Trusted Applications mode is now enabled. Kaspersky Internet Security will block all applications that have not been classified as trusted. After that, the application proceeds to the Application Control window.

➤ *To disable Trusted Applications mode:*

1. Open the main application window.

2. In the lower part of the window, click the  button and select the **Application Control** section.

The window displays the **Application Control** section.

- In the lower part of the window, in the **Trusted Applications mode is enabled** section, click the **Disable** link.
Trusted Applications mode is now disabled.

PROTECTING PRIVATE DATA AGAINST THEFT

Kaspersky Internet Security helps you to protect private data against theft:

- Passwords, user names, and other registration data
- Account numbers and bank card numbers

Kaspersky Internet Security includes components and tools that allow you to protect your private data against theft by criminals through phishing or interception of data entered on the keyboard.

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.

Protection against interception of data entered on the keyboard is provided by Virtual Keyboard and secure data input on the computer keyboard.

The Privacy Cleaner Wizard clears the computer of all information about the user's activities.

Safe Money protects data when you use Internet banking services and shop on online stores.

Protection against private data transfer via the Internet is provided by one of the Parental Control tools (see the section "Using Parental Control" on page [50](#)).

IN THIS SECTION

Virtual Keyboard.....	42
Protection of data input from the computer keyboard	45
Configuring Safe Money.....	46
Privacy Cleaner	47

VIRTUAL KEYBOARD

When using the Internet, you frequently need to enter your personal data or your user name and password. This happens, for example, during account registration on websites, online shopping, and Internet banking.

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

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

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

Virtual Keyboard is not available for Microsoft Internet Explorer 10 from the Windows Store and for Microsoft Internet Explorer 10 if the **Enhanced Protected Mode** check box is selected in the browser settings. In this case, we recommend opening Virtual Keyboard from the interface of Kaspersky Internet Security.

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

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. Virtual Keyboard protects personal data that is entered from attempts to intercept it through the use of screenshots.

Virtual Keyboard does not prevent screenshots that are made by using the **Print Screen** key and other combinations of keys provided by the operating system settings, or by using DirectX®.

Virtual Keyboard has the following features:

- You can click the Virtual Keyboard buttons with the mouse.
- Unlike hardware keyboards, it is impossible to press several keys simultaneously on Virtual Keyboard. This is why key combinations (such as **ALT+F4**) require that you click 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 releasing the key on a hardware keyboard.
- The Virtual Keyboard language can be switched by using the same shortcut that is specified by the operating system settings for the hardware keyboard. To do so, 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, left-click the **LEFT ALT** key and then right-click the **SHIFT** key).

To ensure protection of data entered via Virtual Keyboard, restart your computer after installing Kaspersky Internet Security.

You can open 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
- By using the quick launch icon of Virtual Keyboard in entry fields on websites

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

When Virtual Keyboard is used, Kaspersky Internet Security disables the autofill option for entry fields on websites.

- By pressing a combination of keyboard keys
- By using the Kaspersky Internet Security Gadget (only on Microsoft Windows Vista and Microsoft Windows 7)

- To open Virtual Keyboard from the context menu of the application icon in the taskbar notification area,

in the context menu of the application icon (see the following figure), select **Tools** → **Virtual Keyboard** (see the following figure)

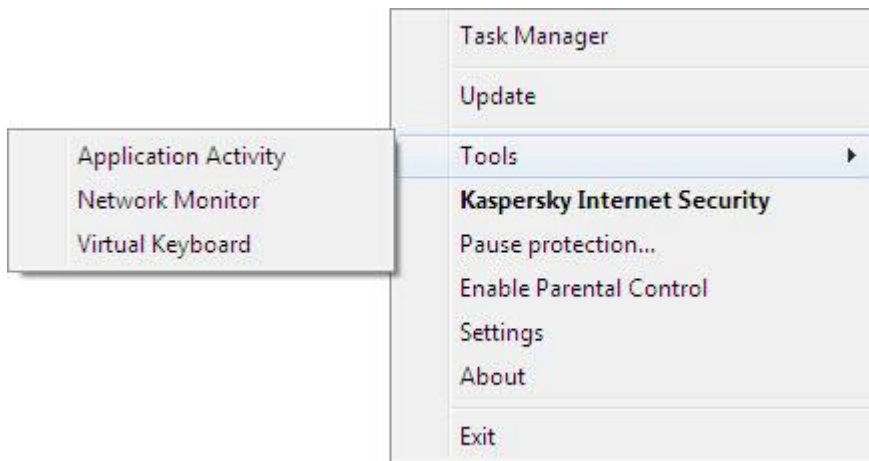



Figure 6. Kaspersky Internet Security context menu

- To open Virtual Keyboard from the main application window,

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

- To open Virtual Keyboard from a browser window,

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

- To open the Virtual Keyboard using the hardware 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.

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

1. Open the main application window.
2. In the lower part of the window, click the **Settings** link.
3. In the **Settings** window that opens, in the **Additional** section, select the **Secure Data Input** subsection.
The window displays the settings for secure data input.
4. If necessary, in the **Virtual Keyboard** section, select the **Open Virtual Keyboard by typing CTRL+ALT+SHIFT+P** check box.
5. If you want the Virtual Keyboard quick launch icon to be displayed in entry fields, select the **Show quick launch icon in data entry fields** check box.
6. If you want the Virtual Keyboard quick launch icon to be displayed only when specified websites are accessed:
 - a. In the **Virtual Keyboard** section, click the **Edit categories** link.

The **Categories for Virtual Keyboard** window opens.

- b. Select the check boxes for categories of websites on which the quick launch icon should be displayed in entry fields.

The Virtual Keyboard quick launch icon will be displayed when a website that belongs to any of the selected categories is accessed.

- c. If you want to enable or disable display of the Virtual Keyboard quick launch icon on a specific website:
- Click the **Configure exclusions** link.

The **Exclusions for Virtual Keyboard** window opens.

- In the lower part of the window, click the **Add** button.

A window opens for adding an exclusion for Virtual Keyboard.

- In the **URL** field, enter the URL of a website.
- If you want the Virtual Keyboard quick launch icon to be displayed (or not displayed) on a specified web page only, in the **Scope** section, select **Apply to specified page**.
- In the **Virtual Keyboard icon** section, specify whether to display the Virtual Keyboard quick launch icon on the specified web page.
- Click the **Add** button.

The specified website appears in the list in the **Exclusions for Virtual Keyboard** window. When the specified website is accessed, the Virtual Keyboard quick launch icon will be displayed in accordance with the specified settings.

PROTECTION OF DATA INPUT FROM THE COMPUTER KEYBOARD

Protection of data input on the computer keyboard allows avoiding interception of data that is entered via the keyboard.

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

Data input protection is not available for Microsoft Internet Explorer from Windows Store and for Microsoft Internet Explorer 10 if the **Enhanced Protected Mode** check box is selected in the browser settings.

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 is obtained by intruders directly from the website.

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 via the computer keyboard, restart your computer after installing Kaspersky Internet Security.

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

- Open the main application window.
- Click the **Settings** link in the lower part of the window to go to the **Settings** section.
- In the **Additional** section, select the **Secure Data Input** subsection.

The window displays the settings for secure data input.

- Select the **Enable Secure Keyboard Input** check box in the **Hardware keyboard** section in the lower part of the window.

5. Specify the protection scope for data input from the hardware keyboard:
 - a. Open the **Hardware keyboard categories** window by clicking the **Edit categories** link in the lower part of the **Hardware keyboard** section.
 - b. Select the check boxes for categories of websites on which you want to protect data that is entered via the keyboard.
 - c. If you want to enable protection of data input from the keyboard on a specified website:
 - a. Open the **Hardware keyboard exclusions** window by clicking the **Configure exclusions** link.
 - b. In the window that opens, click the **Add** button.
A window opens for adding an exclusion for hardware keyboard.
 - c. In the window that opens, in the **URL** field, enter a website URL.
 - d. Select one of the options for Secure Data Input on this website (**Apply to specified page** or **Apply to the entire website**).
 - e. Select an action to be performed by Secure Data Input on this website (**Protect** or **Do not protect**).
 - f. Click the **Add** button.

The specified website appears in the list in the **Hardware keyboard exclusions** window. When this website is accessed, Secure Data Input will be active, functioning in accordance with the settings that you have specified.

SAFE MONEY SETUP

To provide protection for confidential data that you enter on websites of banks and payment systems (such as banking card numbers and passwords for access to online banking services), as well as to prevent assets from being stolen when you make online payments, Kaspersky Internet Security prompts 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 cleared in the **Advanced Settings** section, the **Self-Defense** subsection of the application settings window.

You can configure Safe Money so that Safe Money runs automatically when you visit the websites of banks and payment systems.

This feature is not available in Microsoft Internet Explorer 10 if the **Enhanced Protected Mode** check box is selected in the browser settings. You can enable Safe Run for Websites mode from the interface of Kaspersky Internet Security.

When running under Microsoft Windows 8 x64, Kaspersky Internet Security does not protect windows of Safe Run for Websites against unauthorized screenshot capture.

➤ *To configure Safe Money:*

1. Open the main application window.
2. Click the **Settings** link in the lower part of the main window to go to the **Settings** section.
3. In the left part of the window, select the **Protection Center** section.
4. In the right part of the **Protection Center** section, select the **Safe Money** subsection.
The window displays the settings of the Safe Money component.
5. Enable Safe Money by using the switch in the upper part of the window.
6. To enable notification of vulnerabilities detected in the operating system before running Safe Run for Websites, select the **Notify about operating system vulnerabilities** check box.

➤ To configure Safe Money for a specified website:

1. Open the main application window.
2. In the lower part of the main window, select the **Safe Money** section.

The window displays the **Safe Money** section.

3. Click the **Add bank or payment system website** button.

The right part of the window displays fields for adding website details.

4. In the **Bank or payment system website** field, enter the URL of a website that you want to open in Safe Run for Websites.

A website address must be preceded by the protocol prefix <https://> which is inserted by default by the protected browser.

5. If necessary, in the **Description** field, enter the name or a description for the website.
6. Select the action that Safe Run for Websites performs when you open the website:
 - If you want Kaspersky Internet Security to prompt you to run 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 protected browser**.
 - If you want to disable Safe Money for the website, select **Do not run the protected browser**.

7. In the right part of the window, click the **Add** button.

The website of a bank or a payment system is displayed in the list in the left part of the window.

PRIVACY CLEANER

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

- Details of search queries entered by users and websites visited
- Information about started applications, and opened and saved files
- Microsoft Windows event log entries;
- Other information about user activity

Information about user actions containing confidential information can 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 run 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 by using the **Back** and **Next** buttons. To close the Wizard after it completes 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 the **Search for user activity traces** check box is selected. Click the **Next** button to start the Wizard.

Step 2. Activity signs search

This Wizard searches for traces of malware activities in your computer. The search may take a while. When the search is complete, the Wizard proceeds automatically to the next step.

Step 3. Selecting Privacy Cleaner actions

When the search is complete, the Wizard informs you about detected traces of activity and prompts for actions to be taken to eliminate the detected traces of activity (see the following figure).

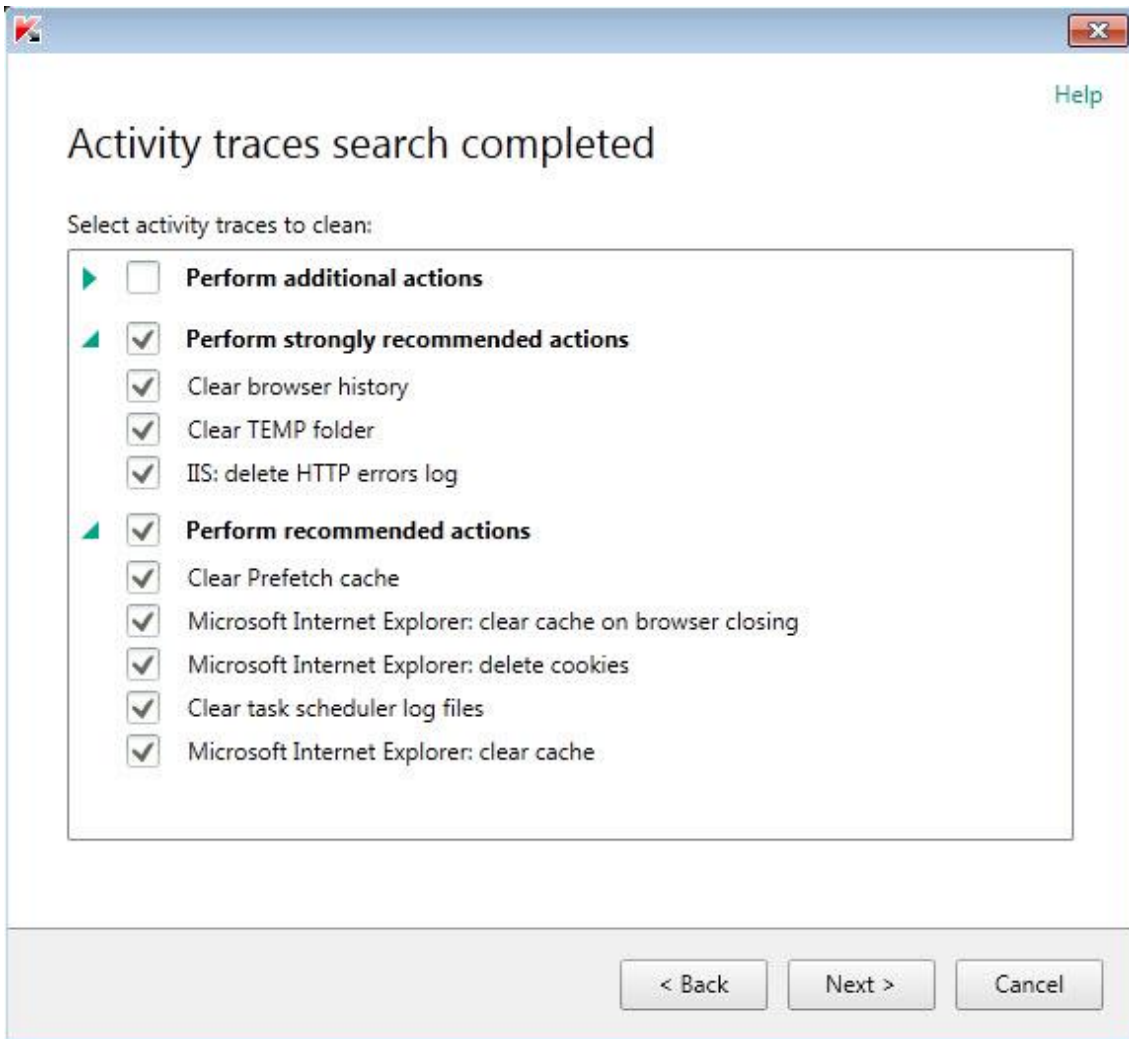



Figure 7. Activity traces detected and recommendations on eliminating them

To view actions within the 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. 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 that are selected by default is not recommended. This may jeopardize the safety of your computer.

After you define 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, it may be necessary to restart the computer; if so, the Wizard notifies you.

When the clean-up is complete, the Wizard proceeds automatically to the next step.

Step 5. Wizard completion




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

VERIFYING WEBSITE SAFETY

Kaspersky Internet Security allows checking a website for security before going to the website by a link. Websites are checked using *Kaspersky URL Advisor* and *Web Filter*, which are integrated into the Web Anti-Virus component.

Kaspersky URL Advisor is not available for Microsoft Internet Explorer browser 10 from Windows Store and for Microsoft Internet Explorer 10 if the **Enhanced Protected Mode** check box is selected in the browser settings.

Kaspersky URL Advisor is integrated into the 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.

To view a pop-up window with more details on the link, point to the corresponding icon.

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

➔ *To enable link checking on websites:*

1. Open the main application window.
2. In the lower part of the main window, click the **Settings** link. The **Settings** window opens.
3. In the **Protection Center** section select the **Web Anti-Virus** subsection.

The window displays the settings for Web Anti-Virus.

4. In the lower part of the window, click the **Advanced Settings** link. The advanced settings window of Web Anti-Virus opens.
5. In the **Kaspersky URL Advisor** section, select the **Check URLs** check box.

6. If you want Web Anti-Virus to scan the content of all websites, select **On all websites except those specified**.

If necessary, specify web pages that you trust, by clicking the **Configure exclusions** link. Web Anti-Virus does not scan the content of the specified web pages or encrypted connections with the specified websites.

7. If you want Web Anti-Virus to check the content of specific web pages only:

- a. Select **On specified websites only**.
- b. Click the **Configure checked websites** link.
- c. In the **Configure checked websites** window that opens, click the **Add** button.
- d. In the **Add URL** window that opens, enter the URL of a web page whose content you want to check.
- e. Select a status for the web page check (if the status is *Active*, Web Anti-Virus checks web page content).
- f. Click the **Add** button.

The specified web page appears in the list in the **Checked URLs** window. Web Anti-Virus checks URLs on this web page.

8. If you want to edit the advanced settings for URL checking, in the **Advanced settings of Web Anti-Virus**, in the **Kaspersky URL Advisor** section, click the **Configure Kaspersky URL Advisor** link.

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

9. If you want Web Anti-Virus to notify you of the safety of links on all web pages, in the **Checked URLs** section, select **All URLs**.
10. If you want Web Anti-Virus to display information about whether a link belongs to a specific category of website content (for example, *Explicit language*):
- a. Select the **Show information on the categories of website content** check box.
 - b. Select the check boxes next to categories of website content about which information should be displayed in comments.

Web Anti-Virus checks links on specified web pages and displays information about categories of the links in accordance with the current settings.

USING PARENTAL CONTROL

Parental Control allows monitoring actions performed by users on the local 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 presents a number of challenges for children:

- Loss of time and / or money when visiting chat rooms, gaming resources, online stores, and auctions
- Access to websites targeted at an adult audience, such as those featuring pornography, extremism, firearms, drug abuse, and explicit violence
- Downloading of files infected with malware
- Health damage inflicted by excessive computer use
- Contacts with strangers who may pretend to be peers to obtain personal information from underage users, such as real name, physical address, or time of day when nobody is home.

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

- Limiting the time for computer and Internet use
- Creating lists of allowed and blocked games and applications, as well as temporarily restricting use of allowed applications
- Creating lists of allowed and blocked websites and selectively blocking categories of websites with inappropriate content
- Enabling safe search mode through search engines (links to websites with dubious content are not displayed in search results)
- Restricting file downloads from the Internet
- Creating lists of contacts that are allowed or blocked for instant messaging (IM) clients and social networks
- Viewing message logs for IM clients and social networks
- Blocking sending of certain personal data
- Searching for specified keywords in message logs

You can configure features of Parental Control for each user account on a computer individually. You can also view Parental Control reports on the activities of monitored users.

IN THIS SECTION

Monitoring computer usage.....	51
Monitoring Internet usage	52
Monitoring games and applications	54
Monitoring messaging over social networks.....	55
Monitoring messaging contents.....	55
Viewing the report on a user's activity.....	57

CONTROL COMPUTER USAGE

Parental Control allows you to limit the amount of time spent by the user at the computer. You can specify a time interval during which Parental Control should block access to the computer (bedtime), as well as the overall time limit of everyday computer usage. You can specify different limit values for weekdays and weekends.



➤ *To set up restrictions imposed on computer usage time:*

1. Open the main application window.
2. In the lower part of the window, click the  button and select the **Parental Control** section.

The window displays the **Parental Control** section.

3. Click the link with the name of a user account to go to a window that provides statistics of the user's activities.
4. Click the **Settings** link in the **Computer** section to go to the settings window of Computer Usage Control.

- To specify a time interval during which Parental Control will block access to the computer, select the **Block access for bedtime** check box in the **Weekdays** and **Weekends** sections and select a time frame for the interval from the dropdown lists next to the check boxes.

You can also set up a schedule of computer usage using a table. To view the table, click the   button.

Parental Control will block the user's access to the computer during the specified time interval.

- To limit the total computer usage time, select the **Restrict daily access** check boxes in the **Weekdays** and **Weekends** sections and select a time interval from the dropdown lists next to the check boxes.

Parental Control will block the user's access to the computer when the total computer usage time over the day exceeds the specified interval.

- To set up breaks in the user's sessions of computer usage, in the **Outage** section, select the **Block access every** check box and then select values for the frequency (e.g., every hour) and the length (e.g., 10 minutes) of breaks from the dropdown lists next to the check box.

Parental Control will block the user's access to the computer in accordance with the current settings.

CONTROL INTERNET USAGE

By using Parental Control, you can limit the Internet usage time and prohibit users to access certain categories of websites or specified websites. Moreover, you can prohibit the user to download files of certain types (such as archives or videos) from the Internet.

➤ *To set up a limitation of Internet usage time:*

- Open the main application window.
- In the lower part of the window, click the  button and select the **Parental Control** section.

The window displays the **Parental Control** section.

- Click the link with the name of a user account to go to a window that provides statistics of the user's activities.
- Click the **Settings** link in the **Internet** section to open the settings window for Internet usage control.
- If you want to limit the total time of Internet usage on weekdays, in the **Internet access restriction** section, select the **Restrict access on weekdays** check box and then select a value for time limit from the dropdown list next to the check box.
- If you want to limit the total time of Internet usage on weekends, select the **Restrict access on weekends** check box and then select a value for time limit from the dropdown list next to the check box.

Parental Control will limit the total amount of time spent on the Internet by the user, in accordance with the values that you have specified.

➤ *To restrict visiting of specific websites:*

- Open the main application window.
- In the lower part of the window, click the  button and select the **Parental Control** section.

The window displays the **Parental Control** section.

- Click the link with the name of a user account to go to a window that provides statistics of the user's activities.
- Click the **Settings** link in the **Internet** section to open the settings window for Internet usage control.

5. To avoid sexual content in search results, in the **Control Web Browsing** section, select the **Enable Safe Search** check box.

No sexual content will be displayed in search results when searching for information using search engines (such as Google, Bing®, Yahoo!™).


6. To block access to websites of certain categories:
 - a. In the **Control Web Browsing** section, select the **Block access to the following websites** check box.
 - b. Select **Adult websites** and click the **Select categories of websites** link to open the **Block access to the following categories of websites** window.
 - c. Select the check boxes next to categories of websites that should be blocked.

Parental Control will block all of the user's attempts to open a website if its contents are classified among any of the blocked categories.

7. To block access to specific websites:
 - a. In the **Control Web Browsing** section, select the **Block access to the following websites** check box.
 - b. Select **All websites except for exclusions allowed on the list** and click the **Add exclusions** link to open the **Exclude websites** window.
 - c. In the lower part of the window, click the **Add** button.
The **Add new website** window opens.
 - d. Enter the address of a website that you intend to prohibit to visit, by filling in the **URL** field.
 - e. Define a block scope in the **Scope** section: the entire website or the specified web page only.
 - f. If you want to block the specified website, in the **Action** section, select **Block**.
 - g. Click the **Add** button.

The specified website appears in the list in the **Exclude websites** window. Parental Control will block all of the user's attempts to open any listed website, in accordance with the current settings.

➔ *To prohibit downloading of files of certain types from the Internet:*

1. Open the main application window.
2. In the lower part of the window, click the  button and select the **Parental Control** section.
The window displays the **Parental Control** section.
3. Click the link with the name of a user account to go to a window that provides statistics of the user's activities.
4. Click the **Settings** link in the **Internet** section to open the settings window for Internet usage control.
5. In the **Limit file downloading** section, select the check boxes next to file types that should be blocked at a download attempt.

Parental Control will block downloads of files of specified types from the Internet.

CONTROL RUNNING OF GAMES AND APPLICATIONS

By using Parental Control, you can allow or prohibit the user to start games depending on their age rating. Also, you can prohibit the user to start specified applications (such as games or IM clients) or limit the usage time for any of such applications.

➤ *To block games with content, which is inappropriate for the user's age:*

1. Open the main application window.

2. In the lower part of the window, click the  button and select the **Parental Control** section.

The window displays the **Parental Control** section.

3. Click the link with the name of a user account to go to a window that provides statistics of the user's activities.

4. Click the **Settings** link in the **Applications** section to go to the settings window of Application Startup Control.

5. In the **Block games by content** section, block startup of games that are inappropriate for the selected user due to the user's age and / or due to games' content:

a. If you want to block all games featuring content, which is inappropriate for the user's age, select the **Block games by age rating** check box and select an age restriction option from the dropdown list next to the check box.

b. If you want to block games with content of a certain category:

a. Select the **Block games from adult categories** check box.

b. Click the **Select categories of games** link to open the **Restrict games startup by content** window.

c. Select the check boxes next to the content categories corresponding to games that you want to block.

➤ *To restrict startup of a specific application:*

1. Open the main application window.

2. In the lower part of the window, click the  button and select the **Parental Control** section.

The window displays the **Parental Control** section.

3. Click the link with the name of a user account to go to a window that provides statistics of the user's activities.

4. Click the **Settings** link in the **Applications** section to go to the settings window of Application Startup Control.



5. In the lower part of the window, click the **Add application** button and select the executable file of an application in the window that opens.

The selected application appears on the list in the **Block specified applications** section. Kaspersky Internet Security automatically adds it to a specified category, for example, *Games*.

6. If you want to block an application, select the check box next to the name of one on the list. You can also block all applications belonging to a specified category by selecting the check box next to the name of a category on the list (for example, you can block the *Games* category).

7. If you want to set a limit on the usage time of an application, select an application or an application category from the list and click the **Configure rules** button.

The **Restrict application usage** window opens.


8. If you want to limit the application usage time on weekdays and weekends, select the corresponding check boxes in the **Weekdays** and **Weekends** sections and select time limit values from the dropdown lists. You can also specify a time when the user is allowed / prohibited to use the application, by using a table. To view the table, click the   button.
9. If you want to set pauses in the operation of an application, in the **Outage** section, select the **Block access every** check box and select a value for pause length from the dropdown list.
10. Click the **Save** button.

Parental Control will apply the specified restrictions when the user handles the application.

CONTROL MESSAGING ON SOCIAL NETWORKS

By using Parental Control, you can view the user's messaging over social networks and IM clients, as well as block messaging with specified contacts.

➤ *To configure monitoring of the user's messaging:*

1. Open the main application window.
2. In the lower part of the window, click the  button and select the **Parental Control** section.
The window displays the **Parental Control** section.
3. Click the link with the name of a user account to go to a window that provides statistics of the user's activities.
4. Click the **Settings** link in the **Messaging** section to go to the settings window of user's messaging control.
5. To view messaging logs and block specified contacts, if necessary:


- a. In the **Communication in instant messengers and social networks** section, select **Block communication with the specified contacts**.
- b. Click the **Contacts** link to open the **Contacts** window.
- c. View contacts with whom the user has been messaging. You can make specified contacts appear in the window using one of the following methods:
 - To view logs of the user's messaging over a specific social network or an IM client, select the required item from the dropdown list in the upper part of the window.
 - To view contacts with whom the user has been maintaining the most intense messaging, in the **Sorting** dropdown list select **By number of messages**.
 - To view contacts with whom the user has been messaging recently, in the **Sorting** dropdown list select **Recent messages on top**.
- d. To view the user's messaging with a specified contact, click one on the list.
The **Messaging log** window opens.
- e. If you want to block the user's messaging with the selected contact, click the **Block** button.

Parental Control will block exchange of messages between the user and the selected contact.

CONTROL CONTENTS OF MESSAGES


By using Parental Control, you can monitor and prohibit the user's attempts to insert specified private data (such as names, phone numbers, banking card numbers) and keywords (such as obscene words) into messages.

➤ *To configure control of private data transfer:*

1. Open the main application window.
2. In the lower part of the window, click the  button and select the **Parental Control** section.
The window displays the **Parental Control** section.
3. Click the link with the name of a user account to go to a window that provides statistics of the user's activities.
4. Click the **Settings** link in the **Content Control** section to go to the settings window of Data Sharing Control.
5. In the **Private data transfer control** section, select the **Block private data transfer to third parties** check box.
6. Click the **Edit the list of private data** link to open the **Private data list** window.
7. In the lower part of the window, click the **Add** button.
A window opens for adding private data.
8. Enter your private data (such as your last name or phone number) in the **Value** field.
9. To add a description for a private data item (for example, "phone number"), click the corresponding link in the **Private data types** section or enter a description in the **Field name** field.
10. Click the **Add** button.

The personal data will be listed in the **Private data list** window. Parental Control will monitor and block the user's attempts to use the specified private data in messaging over IM clients and on websites.

➤ *To configure Control Word Usage for use in messages:*

1. Open the main application window.
2. In the lower part of the window, click the  button and select the **Parental Control** section.
The window displays the **Parental Control** section.
3. Click the link with the name of a user account to go to a window that provides statistics of the user's activities.
4. Click the **Settings** link in the **Content Control** section to go to the settings window of Data Sharing Control.
5. In the **Keyword Control** section, select the **Enable Keyword Control** check box.
6. Click the **Edit the list of key words** link to open the **Keyword Control** window.
7. In the lower part of the window, click the **Add** button.
A window opens for adding a keyword.
8. Enter a key phrase in the **Value** field and click the **Add** button.

The specified key phrase appears on the list of keywords in the **Keyword Control** window. Parental Control will block transmission of messages that contain the specified key phrase, regardless of whether when messaging over the Internet or over IM clients.

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, click the  button and select the **Parental Control** section.

The window displays the **Parental Control** section.

3. Click the link with the name of a user account to go to a window that provides statistics of the user's activities.
4. In the section with the required type of restriction (for example, **Internet** or **Messaging**) open the report on monitored actions by clicking the **Details** link.

The window displays a report on monitored actions.

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 main application window.
2. Click the **Settings** link in the lower part of the main window to go to the **Settings** section.
3. In the left part of the window select the **Performance** section.

The window displays the performance settings of Kaspersky Internet Security.

4. In the **Gaming Profile** section, select the **Use Gaming Profile** check box.

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 disinfected using other methods (e.g., with anti-virus applications).

IN THIS SECTION

Creating a Rescue Disk [58](#)
 Starting the computer from the Rescue Disk [60](#)

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 rescued.iso file created by the Wizard is saved on your computer's hard drive.

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

1. Open the main application window.
2. In the lower part of the main window, click the  button and 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 by using the **Back** and **Next** buttons. To close the Wizard after it completes 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. To proceed with the Wizard, click the **Next** button. The Wizard will proceed to the **Select disk image source** window.

Step 2. Selecting a disk image source

At this step, you should select the disk image source from the list of options:

- 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**.
- If you have an existing Kaspersky Rescue Disk image, select **Use existing Kaspersky Rescue Disk image**.
- 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**.

Click the **Browse** button. After you have specified the path to the file, click the **Next** button.

Step 3. Copying (downloading) the disk image

If you have selected **Use existing Kaspersky Rescue Disk image** in the previous window of the Wizard, this step will be skipped.

When copying or downloading 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 to a CD / DVD, select **Record to CD/DVD**.
- To record the disk image to a USB drive, select **Record to USB flash drive**.

Kaspersky Lab specialists do not recommend saving the disk image on devices that are not intended exclusively for data storage, such as smartphones, mobile phones, pocket PCs, or MP3 players. After being used to store the disk image, such devices may malfunction.

- To record the disk image to the hard drive of your computer or another computer that you can access over the network, select **Save the disk image to file on local or network drive**.

Step 6. Selecting a device / file to record the disk image

At this step, the Wizard prompts you to specify the path to a device / file to which the disk image will be saved.

- If you have selected **Record to CD/DVD** at the previous step of the Wizard, select from the dropdown list a disk to which you want to record the disk image.
- If you have selected **Record to USB flash drive** at the previous step of the Wizard, select from the dropdown list a device to which you want to record the disk image.
- If you have selected **Save the disk image to file on local or network drive** at the previous step of the Wizard, specify a folder to which you want to record the disk image, and the name of the ISO file.

Step 7. Recording the disk image to a device / file

At this step of the Wizard you can monitor the progress of disk image recording to a CD / DVD or a USB drive, or disk image saving to a file.

Step 8. Wizard completion

To close the Wizard after it completes its task, click the **Finish** button. You can use the newly created Rescue Disk to boot the computer if you cannot boot it and run Kaspersky Internet Security in standard 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 the section "Creating a Rescue Disk" on page 58).

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;
- closing the application;
- removing the application.

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

1. Open the main application window.
2. Click the **Settings** link in the lower part of the main window to go to the **Settings** section.
3. In the left part of the window, select the **General** section and click the **Set up password protection** link to open the **Password protection** window.
4. In the window that opens, fill in the **New password** and **Confirm password** fields.
5. To change a previously created password, type it in the **Old password** field.
6. In the **Password scope** group of settings, specify the operations with the applications the access to which has to be password protected.

A forgotten password cannot be recovered. If you have forgotten your password, you need to contact Technical Support in order to restore access to the 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 the following figure).

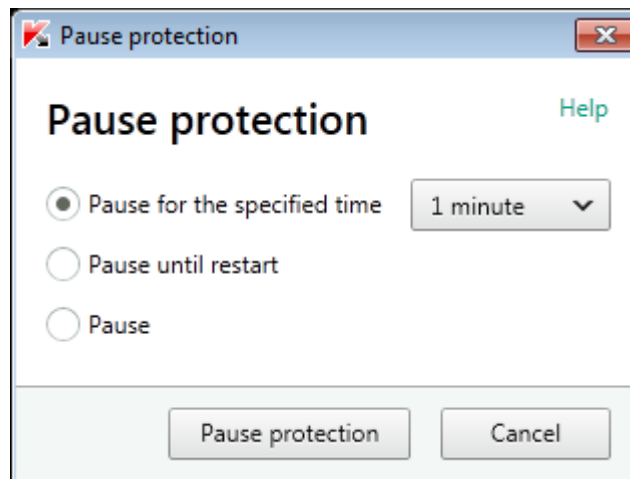


Figure 8. *Pause protection* window

2. In the **Pause protection** window, select the time interval after which protection should be resumed:
 - **Pause for the specified time** – protection is enabled on expiration of the time interval selected from the drop-down list below.
 - **Pause until restart** – protection is 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.

RESTORING THE DEFAULT APPLICATION SETTINGS

You can restore the 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 values of previously specified settings for application components.

➤ *To run the post-infection Microsoft Windows Troubleshooting wizard:*

1. Open the main application window.
2. In the lower part of the window, click the **Settings** link.

The window displays the **Settings** section.

3. Select the **General** section.

The window displays the settings of Kaspersky Internet Security.

4. In the lower part of the window, click the **Restore settings** link (see the following figure).

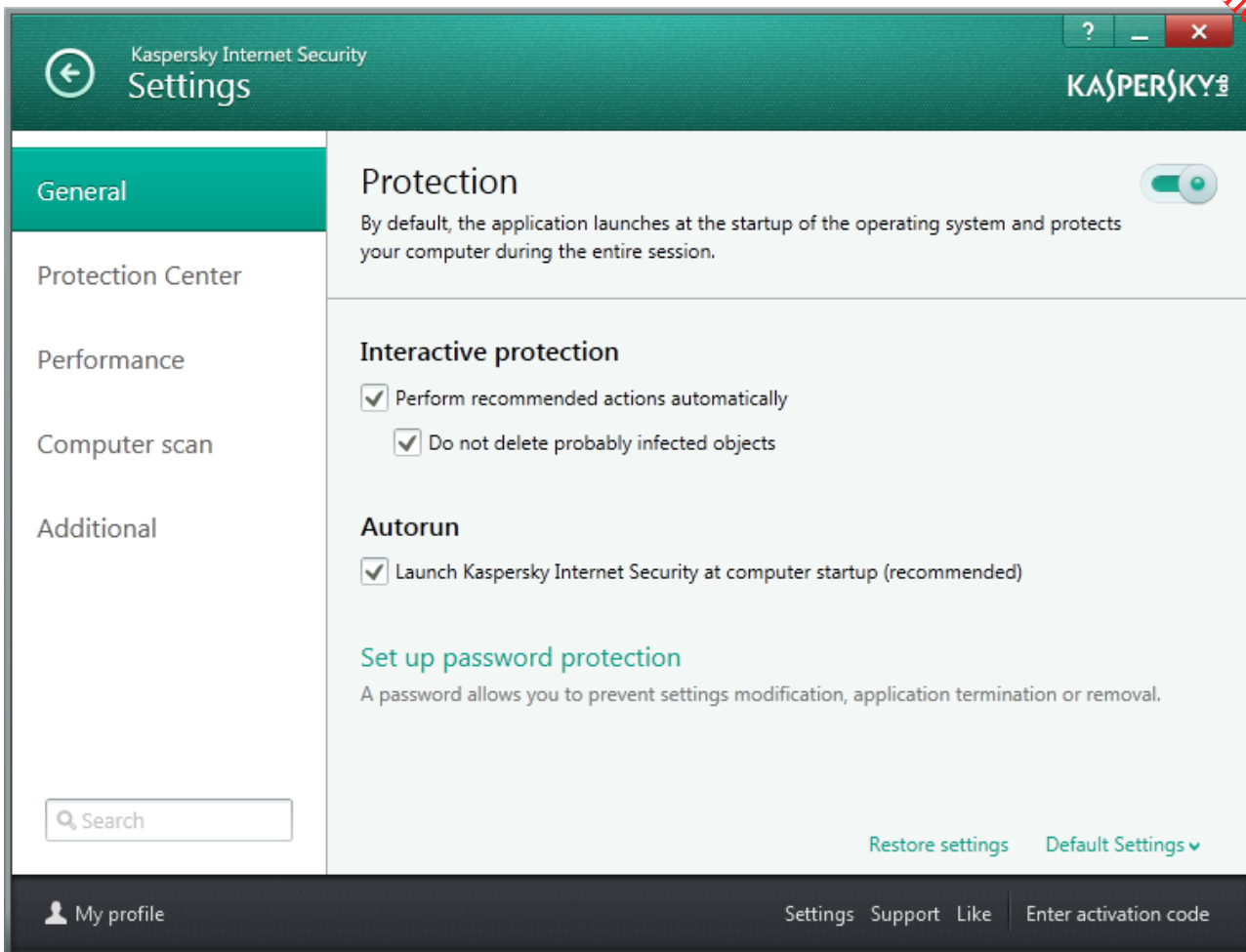


Figure 9. Settings window, General subsection

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 the following figure).

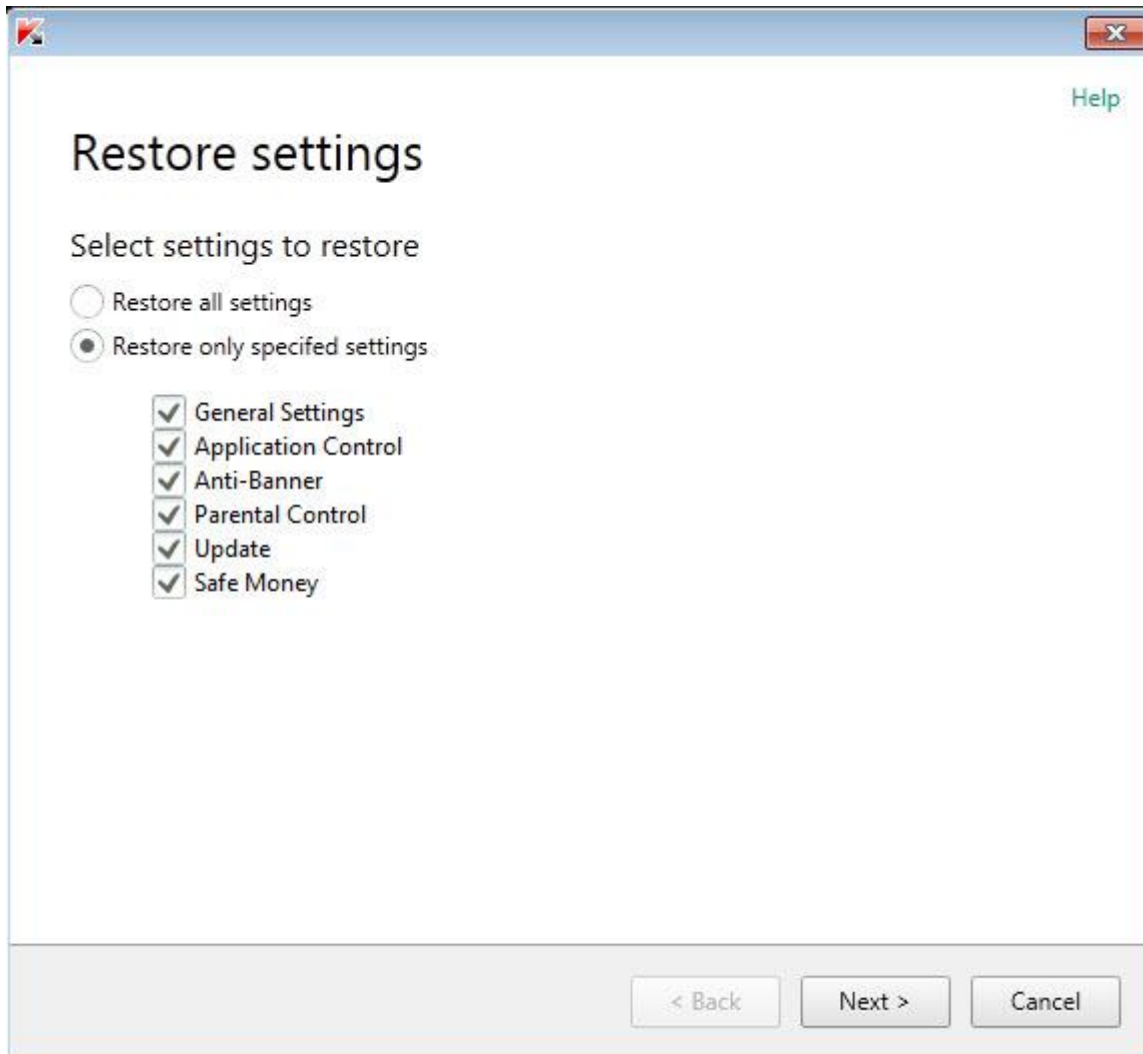


Figure 10. **Restore settings** window

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 after it completes its task, click the **Finish** button.

VIEWING THE APPLICATION 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 view reports using Kaspersky Gadget. To do this, the report opening option should be assigned to one of the buttons of Kaspersky Gadget.

➔ *To view the application operation report:*

1. Open the **Reports** window using any of the following methods:
 - In the lower part of the main application window, select the **Reports** section.
 - In the Kaspersky Gadget interface (for Microsoft Windows Vista and Microsoft Windows 7 only), click the button with the  **Reports** icon.

The **Reports** window displays reports on the application operation over the current day (in the left part of the window) and over the period (in the right part of the window).

2. If you want to view a detailed report on the application operation, open the **Detailed report** window by clicking the **All events** link located in the upper part of the **Reports** window.

The **Detailed report** window displays data in the form of a table. For a convenient view of reports, you can select various sorting options.

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 the section "Assessing computer protection status and resolving security issues" on page [30](#)). 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 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. The use of data from Kaspersky Security Network ensures faster responses by Kaspersky Internet Security to new threats, improves the performance of some protection components, and reduces the risk of false positives.

Users' participation in Kaspersky Security Network allows Kaspersky Lab 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.

When starting Kaspersky Internet Security, after the operating system is booted, the application sends to Kaspersky Security Network details of your system configuration, as well as information about the start time and completion time of Kaspersky Internet Security processes.

IN THIS SECTION

Enabling and disabling participation in Kaspersky Security Network [66](#)
 Checking the connection to Kaspersky Security Network [66](#)

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. Click the **Settings** link in the lower part of the main window to open the **Settings** window.
3. In the **Additional** section select the **Feedback** subsection.

The window displays details of Kaspersky Security Network (KSN) and KSN participation settings.

4. Enable or disable participation in Kaspersky Security Network by using the **Enable / Disable** buttons:
 - If you want to participate in KSN, click the **Enable** button.
 - If you do not want to participate in KSN, click the **Disable** button.

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 connecting to the Kaspersky Security Network.

The current status of the key is displayed in the **Licensing** window.

➤ *To test the connection to Kaspersky Security Network:*

1. Open the main application window.
2. Click the **Settings** link in the lower part of the main window to open the **Settings** window.
3. In the **Additional** section select the **Feedback** subsection.

The window displays the status of connection to Kaspersky Security Network.

PARTICIPATING IN PROTECT A FRIEND PROGRAM

Protect a Friend program allows you to publish on Twitter and on your page in Facebook or vk.com a link for downloading the distribution package of Kaspersky Internet Security with an extended evaluation period. If one of your friends on Twitter, Facebook, or vk.com downloads the distribution package of Kaspersky Internet Security by clicking the link that you published and then activates the application, you will be awarded bonus points. You can exchange collected bonus points for a bonus activation code for Kaspersky Internet Security.

Note that the option of participation in Protect a Friend program is not available for each of the users.

If you participate in Protect a Friend program, the user rating is assigned to you. The user rating depends on the application version and on application features and components that you use the most frequently (for example, scan, Parental Control, Safe Money).

To participate in Protect a Friend program, open the web page with your profile in Protect a Friend program. You can view the web page with your profile by clicking the **profile** link in the lower part of the main window of Kaspersky Internet Security. Your profile is automatically created when you first log in.

To log in to your profile in Protect a Friend program, you should go through authentication with Kaspersky Account. If you have no Kaspersky Account yet, you can create one when first opening your profile in Protect a Friend program.

On the web page with your profile in Protect a Friend program, you can perform the following actions:

- View your rating in Protect a Friend program and the number of bonus points collected
- Publish links for downloading the installation package of Kaspersky Internet Security
- Edit the properties of your profile (the user picture and the name that will be shown on Twitter, in social networks, and in your blog together with a link for downloading the installation package of Kaspersky Internet Security).

IN THIS SECTION

Logging in to your profile in Protect a Friend program	67
How to share a link to Kaspersky Internet Security with friends	68
Exchanging points for a bonus activation code.....	69

LOGGING IN TO YOUR PROFILE IN THE PROTECT A FRIEND PROGRAM

To log in to your profile in Protect a Friend program, you should go through authentication with Kaspersky Account. If you do not have Kaspersky Account yet, you should create one when first logging in to the web page of Protect a Friend program.

Kaspersky Account is the address of your email and the password (at least eight characters) that you have specified during registration.

After an account is created, a message will be sent to your email, containing a link for activation of your Kaspersky Account.

After the activation, you can use your Kaspersky Account to log in to the web page with your profile in Protect a Friend program.

◆ *To create your Kaspersky Account:*

1. Open the main application window and click the **My profile** link in the lower part of the window.

A web page of Protect a Friend program opens, containing fields for registration or authentication with Kaspersky Account.

2. Create and activate your Kaspersky Account:

- a. In the left part of the web page, enter an email address in the **Email** field.
- b. Enter a password and then re-enter it for confirmation in the **Password** and **Confirm password** fields. The password should contain at least eight characters.
- c. Click the **Register** button.

The web page displays a message informing you of a successful registration of your Kaspersky Account. A message will be sent to your email, containing a link that you should click to activate your Kaspersky Account.

- d. Click the link to activate your Kaspersky Account.

The web page displays a message informing you of a successful activation of your Kaspersky Account. You can use your newly created Kaspersky Account to log in to your profile in Protect a Friend program.

If you already have your Kaspersky Account, you can use it to log in to the web page with your profile.

➤ *To log in to the web page with your profile in Protect a Friend program:*

1. Open the main application window and click the **My profile** link in the lower part of the window.

A web page of Protect a Friend program opens, containing fields for registration or authentication with Kaspersky Account.

2. In the right part of the web page, fill in the fields by entering the email address and the password that you have specified during registration of Kaspersky Account.
3. Click the **Log in** button.

The web page displays your profile in Protect a Friend program.

HOW TO SHARE A LINK TO KASPERSKY INTERNET SECURITY WITH FRIENDS

When logged in to the web page with your profile in Protect a Friend program, you can publish a link for downloading the distribution package of Kaspersky Internet Security on Twitter and in social networks, such as Facebook and vk.com. Besides, you can share details on your profile in Protect a Friend program with a link to the distribution package by pasting them to your website or blog. Also, you can send a link to the distribution package of Kaspersky Internet Security by email or by using instant messaging clients (such as ICQ).

➤ *To publish a link for downloading the distribution package of Kaspersky Internet Security on Twitter or in social networks:*

1. Open the main window of Kaspersky Internet Security and click the **My profile** link in the lower part of the window.

The web page of authentication in Protect a Friend program opens.

2. Go through authentication on the web page with your Kaspersky Account.

The web page displays details of your profile in Protect a Friend program.

3. In the left part of the web page, click the button with the logo of the required social network (Facebook or vk.com) with the logo of Twitter.

The website of the selected social network or Twitter opens. A link for downloading the distribution package of Kaspersky Internet Security with extended evaluation period will appear in the news feeds of your friends. You can enter additional text in the publishing form, if necessary.

If you have not yet logged in to your page in a social network or Twitter, the authorization page opens.

➤ *To publish a web widget with a link for downloading the distribution package of Kaspersky Internet Security:*

1. Open the main window of Kaspersky Internet Security and click the **My profile** link in the lower part of the window.

The web page of authentication in Protect a Friend program opens.

2. Go through authentication on the web page with your Kaspersky Account.

The web page displays details of your profile in Protect a Friend program.

3. In the upper part of the web page, in the **Share** dropdown list, select **Get web widget code**.

The **Web widget code** window opens containing web widget code to paste to your website.

You can copy the web widget code to the clipboard and then paste it to the HTML code page of your website or blog.

➤ *To get a link for downloading the distribution package of Kaspersky Internet Security to send by email or by using an instant messaging client:*

1. Open the main window of Kaspersky Internet Security and click the **My profile** link in the lower part of the window.

The web page of authentication in Protect a Friend program opens.

2. Go through authentication on the web page with your Kaspersky Account.

The web page displays details of your profile in Protect a Friend program.

3. In the left part of the web page, click the **Get a link** link.

The **Link to installer download** window opens containing a link for downloading the distribution package of Kaspersky Internet Security.

You can copy the link to the clipboard and then send it by email or by using an instant messaging client.

EXCHANGING POINTS FOR A BONUS ACTIVATION CODE

When you participate in Protect a Friend program, you can receive a bonus activation code for Kaspersky Internet Security in exchange for a specified number of bonus points. Bonus points are awarded to you when users activate Kaspersky Internet Security downloaded from the link that you shared via your profile.

Bonus activation codes are provided in the following cases:

- When a user with whom you have shared the link performs one-time activation of the trial version of Kaspersky Internet Security
- When a user with whom you have shared the link performs activation of a license for Kaspersky Internet Security version 2013 or later.

On the web page with your profile, you can view the history of bonus points income and information about bonus activation codes provided to you. Each bonus activation code provided to you will also be sent to your email.

A bonus activation code can also be specified in the application as the new activation code.

A bonus activation code can be used for the application activation on another computer (for example, you can grant one to another user).

A bonus activation code cannot be used in the following cases:

- The application is in use under subscription. In this case, you can use the bonus activation code when the subscription expires. Also, you can apply your bonus activation code on another computer.
- An activation code is already set in the application as the new code. In this case, you can use the bonus activation code when the license expires.

➤ *To receive a bonus activation code and activate the application with it:*

1. Open the main window of Kaspersky Internet Security and click the **My profile** link in the lower part of the window.

The web page with your profile in Protect a Friend program opens.

2. Go through authentication on the web page with your Kaspersky Account.

The web page displays details of your profile in Protect a Friend program.

You can view information about bonus points awarded to you in the **My bonus points** section. If you have collected enough bonus points to get a bonus activation code, a notification **1** appears next to the **Receive a bonus activation code** button in the right part of the web page.

3. To receive a bonus activation code and activate the application with it:

- a. Click the **Receive a bonus activation code** button.

Wait until an activation code is received. The received bonus activation code is displayed in the window that opens.

- b. Click the **Activate** button.

The **Activation** window opens showing a message on activation code verification. After verifying the activation code, a window opens showing a message on successful activation of Kaspersky Internet Security.

➤ *To view the history of bonus activation codes provided and activate the application with one provided earlier:*

1. Open the main window of Kaspersky Internet Security and click the **My profile** link in the lower part of the window.

The web page with your profile in Protect a Friend program opens.

2. Go through authentication on the web page with your Kaspersky Account.

The web page displays details of your profile in Protect a Friend program.

3. In the lower part of the web page, click the **Bonus activation codes** link.

The **Bonus points** window opens on the **Bonus activation codes** tab.

4. In the list of received bonus activation codes, click the one that you want to use to activate the application.

A window opens containing a bonus activation code.

5. Click the **Activate** button.

The **Activation** window opens showing a message on activation code verification. After verifying the activation code, a window opens showing a message on successful activation of Kaspersky Internet Security.

CONTACTING TECHNICAL SUPPORT

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	71
Technical support by phone	71
Obtaining technical support via My Kaspersky Account	71
Using trace files and AVZ scripts	72

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 the section "Sources of information about the application" on page [9](#)), we recommend that you contact Kaspersky Lab Technical Support. Technical Support 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 Technical Support 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 website. This method allows you to contact our specialists using the query form.

Technical support is only available to users who have purchased a license for the application use. 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/rules>). 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 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 Technical Support 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 for research of suspicious files and web resources to the Virus Lab. You can also contact the Virus Lab in case of false positives of Kaspersky Internet Security to files and web resources that you do not consider dangerous.

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 TRACE FILES AND AVZ SCRIPTS

After you notify Technical Support specialists of a problem, they may ask you to create a report that contains information about your operating system, and send it to Technical Support. Technical Support specialists may also ask you to create a *trace file*. The trace file allows tracing the process of performing application commands step by step and determining the stage of application operation at which an error occurs.

After Technical Support specialists analyze the data that you have sent, they can create an AVZ script and send it to you. Running AVZ scripts allows analyzing active processes for malicious code, scanning the system for malicious code, disinfecting / deleting infected files, and creating reports on results of system scans.

IN THIS SECTION

Creating a system state report	73
Sending data files	74
AVZ script execution.....	74

CREATING A SYSTEM STATE REPORT

➤ *To create a system state report:*

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

The **Support Tools** window opens.

4. In the window that opens, click the **Create system state report** link.

The system state report is created in HTML and XML formats and is saved in the sysinfo.zip archive. 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 lower part of the window to open the **Support** window.
3. In the window that opens, click the **Support Tools** link.

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 specialists.

You will need a request number to upload files to the Technical Support server. This number is available in your My Kaspersky Account on the Technical Support website if your request is active.

➤ *To upload the data files to the Technical Support server:*

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

The **Support Tools** window opens.

4. In the window that opens, click the **Send report to Technical Support** link.

The **Send report** window opens.

5. Select the check boxes next to the data that you want to send to Technical Support.
6. Click the **Send report** button.

The selected data files are packed and sent to the Technical Support server.

If for any reason it is not possible to contact Technical Support, the data files can be stored on your computer and later sent from My Kaspersky Account.

◆ *To save data files to disk:*

1. Open the main application window.
2. Click the **Support** link in the lower part of the window to open the **Support** window.
3. In the window that opens, click the **Support Tools** link.
4. The **Support Tools** window opens.
5. In the window that opens, click the **Send report to Technical Support** link.

The **Send report** window opens.

6. Select the check boxes next to the data that you want to send to Technical Support.
7. Click the **Save report** link.

A window for saving the archive opens.

8. Specify the archive name and confirm saving.

The created archive can be sent to Technical Support 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 Technical Support (see the section "How to obtain technical support" on page 71).

◆ *To run an AVZ script:*

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

The **Support Tools** window opens.

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

The **Script execution** window opens.

5. Copy the text from the script sent by Technical Support specialists, paste it in 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 when purchasing a 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.

B

BLOCKING AN OBJECT

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

BONUS ACTIVATION CODE

An activation code for Kaspersky Internet Security provided to the user in exchange for bonus points.

BONUS POINTS

Bonus points are points that Kaspersky Lab awards to users who participate in the Protect a Friend program. Bonus points are provided to the user if the user publishes a link to a Kaspersky Lab application in social networks or pastes the link in an email message, and the user's friend then downloads the application installation package via this link.

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

These databases contain information on the computer security threats known to Kaspersky Lab by the time of database release. Records that are contained in databases allow detecting malicious code in scanned objects. The databases are created by Kaspersky Lab specialists and updated hourly.

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.

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 detects objects which activities in the system can pose security threat. 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.

INFECTED OBJECT

It is the object, which contains a part of code that matches completely a part of code of a well-known harmful application. 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. Using data from Kaspersky Security Network ensures a faster response by Kaspersky Lab's applications to unknown 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**

A time period during which you have access to the application features and rights to use additional services.

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 autorun 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.).

TRUST GROUP

A group to which Kaspersky Internet Security places an application or a process depending on the following criteria: presence of a digital signature, reputation in KSN, trust level of the application source, and potential danger of actions performed by the application or the process. Based on the trust group to which an application belongs, Kaspersky Internet Security can restrict the actions that the application may perform.

In Kaspersky Internet Security, applications belong to one of the following trust groups: Trusted, Low Restricted, High Restricted, or Untrusted.

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.

USER PROFILE

Summary on the user's participation in the Protect a Friend program. The user profile contains the user rating, number of collected bonus points, a link to the page for downloading Kaspersky Internet Security, and bonus activation codes granted to the user.

USER RATING

The user's activity index when using Kaspersky Internet Security. The user rating is displayed in the user profile and depends on the settings and the version of the application.

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.

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>

Virus Lab:

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.

ICQ is a trademark and/or service mark of ICQ LLC.

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

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

Mozilla and Firefox are trademarks of the Mozilla Foundation.

INDEX

A

Activating the application	28
Additional Tools	
Microsoft Windows Troubleshooting.....	35
Rescue Disk.....	57
Anti-Spam	37
Application activation	
activation code.....	24
license	23
trial version	17
Application components.....	12
Application Control	
creating an application rule.....	38
device access rules	38
exclusions.....	38
Application databases.....	31

C

Code	
activation code.....	24

D

Diagnostics	30
Disinfected object	34

E

End User License Agreement.....	23
---------------------------------	----

F

Full-screen application operation mode	57
--	----

G

Gaming Profile.....	57
---------------------	----

H

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

I

Installing the application.....	15
---------------------------------	----

K

Kaspersky Account.....	67
Kaspersky Gadget.....	64
Kaspersky Security Network	65
Kaspersky URL Advisor	
Web Anti-Virus.....	49
Keyboard interceptor	
protection against data interception at the keyboard	45
Keyboard interceptors	
Virtual Keyboard.....	42

L

License
 activation code 24
 End User License Agreement 23

M

Mail Anti-Virus 36
 Microsoft Windows Troubleshooting 35

N

Notifications..... 29

O

Object recovery 34
 Online Banking 46

P

Parental Control 50
 computer usage 51
 Internet usage 52
 messages 55
 report 57
 running of applications 54
 running of games 54
 social networks 55
 Privacy Cleaner 47
 Protect a Friend program 67
 bonus activation code..... 69
 Protection status 30

Q

Quarantine
 restoring an object..... 34

R

Removing
 application 21
 Reports 64
 Rescue Disk 57
 Restoring the default settings 61
 Restricting access to the application..... 60

S

Security analysis..... 30
 Security problems..... 30
 Security threats 30
 Software requirements 14
 Spam 37
 Statistics 64

T

Traces
 creating a trace file 72
 uploading tracing results 73
 Trusted Applications 40

Trusted Applications mode..... 40

U

Unknown applications..... 37

Unwanted email..... 37

Update..... 31

Update source..... 31

V

Virtual Keyboard..... 42

Vulnerability..... 33

Vulnerability Scan..... 33

W

Web Protection..... 49

Downloaded from www.vandenborre.be