Kaspersky Internet Security

KASPERSKY LAB

User Guide

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.

TABLE OF CONTENTS

ABOUT THIS GUIDE

This document is the User Guide to Kaspersky Internet Security 2015 Maintenance Release 2 (hereinafter Kaspersky Internet Security).

For proper use of Kaspersky Internet Security, you should be acquainted with the interface of the operating system that you use, have experience with the main techniques specific for that system, and know how to work with email and the Internet.

This Guide is intended to do the following:

- Help you to install, activate, and use Kaspersky Internet Security.

- Provide a way to quickly find information on issues related to Kaspersky Internet Security.

- Describe additional sources of information about the application and ways of receiving technical support.

IN THIS SECTION

IN THIS GUIDE

This document contains the following sections:

Sources of information about the application (see page 11)

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

Kaspersky Internet Security (see page 13)

This section describes the application's features and provides brief information about the functions and components of the application. 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 the software and hardware requirements that a computer must meet so that a user can install the application on it.

Installing and removing the application (see page 18)

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

Application licensing (see page 29)

This section provides information about key terms related to activation of the application. Read this section to learn more about the purpose of the End User License Agreement and ways to activate the application and renew your license.

Managing application notifications (see page 34)

This section provides information about how to manage application notifications.

Assessing computer protection status and resolving security issues (see page 35)

This section provides information about how to evaluate the computer's security status and fix security threats.

Updating databases and program modules (see page 36)

This section contains step-by-step instructions on how to update databases and application software modules.

Scanning the computer (see page 37)

This section contains step-by-step instructions on how to scan your computer for viruses, malware, and vulnerabilities.

Restoring an object deleted or disinfected by the application (see page 40)

This section contains step-by-step instructions on how to restore an object that has been deleted or disinfected.

Troubleshooting the operating system after infection (see page 41)

This section provides information about how to restore the operating system after it has been infected with viruses.

Protecting email (see page 43)

This section provides information about how to protect your email against spam, viruses, and other threats.

Protecting private data on the Internet (see page 45)

This section provides information about how to make your Internet browsing safe and protect your data against theft.

Anti-Banner protection during website browsing (see page 56)

This section describes how you can use Kaspersky Internet Security to stop banners from showing on websites.

Removing traces of activity on the computer and on the Internet (see page 58)

This section provides information on how to clear traces of user activity from the computer.

Controlling users' activity on the computer and on the Internet (see page 60)

This section provides information about how to control users' actions on the computer and on the Internet by using Kaspersky Internet Security.

Reserving operating system resources for computer games (see page 67)

This section contains instructions on how to improve the performance of the operating system for computer games and other applications.

Handling unknown applications (see page 68)

This section provides information about how to prevent applications from performing unauthorized operations on your computer.

Trusted Applications mode (see page 74)

This section provides information about Trusted Applications mode.

Password-protecting access to control over Kaspersky Internet Security (see page 76)

This section contains instructions on how to protect the application settings with a password.

Pausing and resuming computer protection (see page 77)

This section contains step-by-step instructions on how to enable and disable the application.

Restoring the default application settings (see page 78)

This section contains instructions on how to restore the default application settings.

Viewing the application operation report (see page 80)

This section contains instructions on how to view application reports.

Applying the application settings on another computer (see page 81)

This section provides information about how to export the application settings and apply them on another computer.

Participating in Kaspersky Security Network (see page 82)

This section provides information about Kaspersky Security Network and how to participate in KSN.

Participating in the Protect a Friend program (see page 84)

This section provides information about the Protect a Friend program, which allows you to collect bonus points and receive discounts towards Kaspersky Lab applications.

Using the application from the command prompt (see page 89)

This section provides information on how to control the application via the command prompt.

Assistance from Kaspersky Lab Technical Support (see page 90)

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

Limitations and warnings (see page 97)

This section describes limitations that are not critical to operation of the application.

Glossary (see page 100)

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

Kaspersky Lab ZAO (see page 106)

This section provides information about Kaspersky Lab.

Information about third-party code (see page 107)

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

Trademark notices (see page)

This section lists trademarks of third-party manufacturers that are 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 hardware 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".
Update means... The *Databases are out of date* event occurs.	The following semantic elements are italicized in the text: • New terms • Names of application statuses and events
Press **ENTER**. Press **ALT+F4**.	Names of keyboard keys appear in bold and are capitalized. Names of keys that are connected by a + (plus) sign indicate the use of a key combination. Such keys must be pressed simultaneously.
Click the **ENABLE** button.	Names of application interface elements, such as entry fields, menu items, and buttons, are set off in bold.
➡ *To configure a task schedule:*	Introductory phrases of instructions are italicized and are accompanied by the arrow sign.
In the command line, type `help`. The following message then appears: `Specify the date in dd:mm:yy format.`	The following types of text content are set off with a special font: • Text in the command line • Text of messages that the application displays on screen • Data that the user must enter
<User name>	Variables are enclosed in angle brackets. Instead of the variable, insert the corresponding value, not including the angle brackets.

SOURCES OF INFORMATION ABOUT THE APPLICATION

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

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

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

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 this page (http://www.kaspersky.com/internet-security), you can view general information about the 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)

The 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, which are grouped by topic.

On the page of the application in the Knowledge Base (http://support.kaspersky.com/kis2015), 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 relate both to Kaspersky Internet Security as well as 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 about use of the application. The document also describes the application interface and provides ways for solving typical user tasks during use of 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 on our forum (http://forum.kaspersky.com).

On the forum you can view existing topics, leave your comments, and create new discussion topics.

KASPERSKY INTERNET SECURITY

This section describes the application's features and provides brief information about the functions and components of the application. 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 the software and hardware requirements that a computer must meet so that a user can install the application on it.

WHAT'S NEW

Kaspersky Internet Security provides the following new features:

- The latest versions of popular web browsers are now supported: protection components (such as Virtual Keyboard) now support the web browsers Mozilla™ Firefox™ 32.x, 33.x, 34.x and Google Chrome™ 37.x, 38.x.

- The Google Chrome browser for a 64-bit operating system is now supported.

- Application performance has been improved and computer resource consumption has been optimized.

- Less time is required to start the application.

- The application upgrade process has been improved.

- Functioning of the System Watcher component has been improved: protection against cryptors has been implemented. If a cryptor attempts to encrypt a file, Kaspersky Internet Security automatically creates a backup copy of this file before it is encrypted by a malicious cryptor. Backup copies are stored in the system folder for temporary files. If a cryptor has encrypted a file, Kaspersky Internet Security automatically restores it from the backup copy. Certain limitations apply to this functionality (see the section "Limitations and warnings" on page 97).

- Safe Money functionality has been improved: events involving the weakening of protection during operation of Protected Browser are recorded in the event log. The application now includes the functionality that checks the trusted secure connection to Kaspersky Lab services and websites of online banking and e-money systems by verifying the certificates of the relevant web resources.

DISTRIBUTION KIT

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

- Boxed. Distributed via stores of our partners.

- At the eStore. Distributed at online stores of Kaspersky Lab (for example, http://www.kaspersky.com, in the Online Shop section) 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, which 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.

ABOUT KASPERSKY INTERNET SECURITY

Kaspersky Internet Security provides comprehensive computer protection against known and new threats, network and phishing attacks, and spam. Various 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. 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 real-time protection provided by the security components, we recommend that you regularly *scan* your computer for viruses and other malware. This is necessary in order to prevent any possible spreading of malicious programs that have not been discovered by protection components, for example, because a low security level was set or for other reasons.

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

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

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

What follows is a description of the logic of how the protection components interact when Kaspersky Internet Security has been set to the mode that is recommended by Kaspersky Lab specialists (in other words, with the 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 that are 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 and other malware. Further access to the file is allowed only if the file is not infected or is successfully disinfected by the application. If a file cannot be disinfected for any reason, it is deleted. A copy of the file is moved to Quarantine when that happens. If an infected file is placed in the same location where the deleted file with the same name used to be, Quarantine saves only a copy of the last file. A copy of the previous file with the same name is not saved.

Mail Anti-Virus

Mail Anti-Virus scans incoming and outgoing email messages on your computer. An email message is available to the recipient 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 instant messengers. 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 operating system, and manages applications' activities based on the group to which the component has assigned an application. A set of rules is specified for each group of applications. These rules manage the applications' access to various operating system resources.

Firewall

Firewall ensures your security when you use local networks and the Internet. The component filters all network activities by using rules of two types: *rules for applications* and *packet rules*.

Network Monitor

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

System Watcher

System Watcher component can be used to roll back malware actions in the operating system.

Network Attack Blocker

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

Anti-Spam

Anti-Spam integrates into the email 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 URLs. 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 funds when making online payments.

Secure Keyboard Input

Secure Keyboard Input provides protection from keyloggers for personal data entered on websites. Virtual Keyboard prevents interception of data entered on the hardware keyboard and protects personal data against interception attempts that use screen shots.

Trusted Applications mode

Trusted Applications mode protects the computer from applications that may be unsafe. When Trusted Applications mode is enabled, Kaspersky Internet Security allows running only applications that are identified as trusted (for example, based on information about an application from Kaspersky Security Network, or a trusted digital signature).

Parental Control

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

Parental Control allows you to set flexible restrictions on access to web resources and applications for different users depending on their age. In addition, Parental Control allows viewing statistical reports on the activities of controlled users.

Participating in the Protect a Friend program

Participation in the Protect a Friend program allows you to receive bonus points when you share links to Kaspersky Internet Security with your friends. You can exchange your bonus points for a bonus activation code for Kaspersky Internet Security.

SERVICE FOR USERS

By purchasing 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 receive news from Kaspersky Lab on the Technical Support website.

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

HARDWARE AND SOFTWARE REQUIREMENTS

General requirements:

- 480 MB free disk space on the hard 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 or later

- Webcam access protection is provided only for compatible webcam models http://support.kaspersky.com/10978

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):

- Processor with a clock speed of 1 GHz or higher

- 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 (Service Pack 1 or later), Microsoft Windows 7 Home Basic (Service Pack 1 or later), Microsoft Windows 7 Home Premium (Service Pack 1 or later), Microsoft Windows 7 Professional (Service Pack 1 or later), Microsoft Windows 7 Ultimate (Service Pack 1 or later), Microsoft Windows 8, Microsoft Windows 8 Pro, Microsoft Windows 8 Enterprise, Microsoft Windows 8.1 (Windows 8.1 Update), Microsoft Windows 8.1 Pro (Windows 8.1 Update), Microsoft Windows 8.1 Enterprise (Windows 8.1 Update), and Microsoft Windows 10:

- Processor with a clock speed of 1 GHz or higher

- 1 GB free RAM (for 32-bit operating systems); 2 GB free RAM (for 64-bit operating systems)

Requirements for tablet computers:

- Microsoft Tablet PC

- Intel® Celeron® CPU 1.66 GHz or faster

- 1000 MB free RAM

Requirements for netbooks:

- Intel Atom™ CPU 1.60 GHz or faster

- 1024 MB free RAM

- 10.1-inch display with 1024x600 screen resolution

- Intel GMA 950 graphics core

INSTALLING AND REMOVING THE APPLICATION

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

STANDARD INSTALLATION PROCEDURE

Kaspersky Internet Security will be installed to your computer in interactive mode using the Setup Wizard.

The Wizard consists of a series of pages (steps), which you can navigate through by clicking the **Back** and **Next** buttons. To close the Wizard after it finishes, click the **Finish** button. To stop the Wizard's activity at any step of installation, close the Wizard window.

If the application will be used to protect more than one computer (with the maximum number of computers defined by the terms of the End User License Agreement), the installation procedure will be identical on all computers.

➡ *To install Kaspersky Internet Security to your computer:*

On the installation CD, run the installation package (the file with the .exe extension).

To install Kaspersky Internet Security, you can also use an installation package downloaded from the Internet. In this case, the Setup Wizard displays several additional installation steps for some localization languages.

Along with the application, plug-ins for web browsers are installed to ensure safe Internet browsing.

STEP 1. CHECKING FOR A NEWER VERSION OF THE APPLICATION

Before installation, 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 Kaspersky Lab update servers, it starts installing the current version.

If the Setup Wizard detects a newer version of Kaspersky Internet Security on Kaspersky Lab update servers, it prompts you to download and install it on 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 files from the installation package to your computer and starts installing the new version.

STEP 2. STARTING INSTALLATION OF THE APPLICATION

During this step, the Setup Wizard offers to install the application.

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

Depending on the installation type and the localization language, during this step the Setup Wizard may prompt you to view the License Agreement concluded between you and Kaspersky Lab, as well as ask whether you want to participate in Kaspersky Security Network.

STEP 3. REVIEWING THE LICENSE AGREEMENT

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

During this step, the Setup Wizard asks 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. Installation of the application to your computer then continues.

If the terms of the License Agreement are not accepted, the application will not be installed.

STEP 4. KASPERSKY SECURITY NETWORK STATEMENT

During 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 information about your operating system, 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, in the Wizard window, click the **Accept** button.

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, application installation continues.

STEP 5. INSTALLATION

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

After you enter the password, application installation starts.

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

When installation is complete, the Setup Wizard automatically proceeds to the next step.

Kaspersky Internet Security performs several checks during installation. These checks may detect the following problems:

- *Non-compliance of the operating system with the software requirements*. During installation the Wizard checks the following conditions:

    - Whether the operating system and Service Pack 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 corresponding notification is displayed.

- *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. You are advised to manually remove any applications that Kaspersky Internet Security cannot remove automatically. When removing incompatible applications, you will need to restart your operating system, after which installation of Kaspersky Internet Security continues automatically.

- *Presence of malicious programs on the computer*. If any malicious programs that interfere with installation of anti-virus software are detected on the computer, the Setup Wizard prompts you to download *Kaspersky Virus Removal Tool*, a special tool designed to neutralize infections.

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

STEP 6. COMPLETING INSTALLATION

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

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

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

STEP 7. ACTIVATING THE APPLICATION

The Activation Wizard is started at the first launch of Kaspersky Internet Security.

Activation is the process of making operational a fully functional version of the application for a specified period of time.

The following options for Kaspersky Internet Security activation are offered:

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

    If you specify an activation code for Kaspersky Anti-Virus or Kaspersky Total Security in the entry field, the procedure for switching to Kaspersky Anti-Virus or Kaspersky Total Security starts after 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 application and all of its features during a short evaluation period. When the trial license expires, the trial version of the application cannot be activated for a second time.

An Internet connection is required for activation of the application.

During application activation, you may have to register on My Kaspersky portal.

STEP 8. REGISTERING A USER

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

Registered users are able to send requests to Technical Support and the Virus Lab through My Kaspersky portal, manage activation codes conveniently, and receive the latest information about new applications and special offers from Kaspersky Lab.

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 ACTIVATION

The Wizard informs you that Kaspersky Internet Security has been successfully activated. In addition, information about the current license is provided in this window: the license expiration date and number of computers 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.

INSTALLING THE APPLICATION FROM THE COMMAND PROMPT

You can install Kaspersky Internet Security from the command prompt.

Command prompt syntax:

```
<path to the file of the installation package> [parameters]
```

Detailed instructions and a list of installation settings are available on the Technical Support website (http://support.kaspersky.com/11173#block2).

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 current license for an earlier version of Kaspersky Internet Security, you do not need to activate the application: the Setup Wizard will automatically retrieve information about the license for the previous version of Kaspersky Internet Security and apply it during installation of the new 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 on a computer on which a previous version of Kaspersky Anti-Virus has been already installed with a current license, the Activation Wizard prompts you to select one of the following options:

- 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 to your computer. You can use Kaspersky Anti-Virus until 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 is installed and activated according to the standard scenario.

Kaspersky Internet Security will be installed to your computer in interactive mode using the Setup Wizard.

The Wizard consists of a series of pages (steps), which you can navigate through by clicking the **Back** and **Next** buttons. To close the Wizard after it finishes, click the **Finish** button. To stop the Wizard's activity at any step of installation, close the Wizard window.

If the application will be used to protect more than one computer (with the maximum number of computers defined by the terms of the End User License Agreement), the installation procedure will be identical on all computers.

➡ *To install Kaspersky Internet Security to your computer:*

On the installation CD, run the installation package (the file with the .exe extension).

To install Kaspersky Internet Security, you can also use an installation package downloaded from the Internet. In this case, the Setup Wizard displays several additional installation steps for some localization languages.

Along with the application, plug-ins for web browsers are installed to ensure safe Internet browsing.

Certain limitations apply to the upgrade from the previous version (see the section "Limitations and warnings" on page 97).

STEP 1. CHECKING FOR A NEWER VERSION OF THE APPLICATION

Before installation, 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 Kaspersky Lab update servers, it starts installing the current version.

If the Setup Wizard detects a newer version of Kaspersky Internet Security on Kaspersky Lab update servers, it prompts you to download and install it on 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 files from the installation package to your computer and starts installing the new version.

STEP 2. STARTING INSTALLATION OF THE APPLICATION

During this step, the Setup Wizard offers to install the application.

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

Depending on the installation type and the localization language, during this step the Setup Wizard may prompt you to view the License Agreement concluded between you and Kaspersky Lab, as well as ask whether you want to participate in Kaspersky Security Network.

STEP 3. REVIEWING THE LICENSE AGREEMENT

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

During this step, the Setup Wizard asks 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. Installation of the application to your computer then continues.

If the terms of the License Agreement are not accepted, the application will not be installed.

STEP 4. KASPERSKY SECURITY NETWORK STATEMENT

During 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 information about your operating system, 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, in the Wizard window, click the **Accept** button.

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, application installation continues.

STEP 5. INSTALLATION

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

After you enter the password, application installation starts.

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

When installation is complete, the Setup Wizard automatically proceeds to the next step.

Kaspersky Internet Security performs several checks during installation. These checks may detect the following problems:

- *Non-compliance of the operating system with the software requirements*. During installation the Wizard checks the following conditions:

  - Whether the operating system and Service Pack 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 corresponding notification is displayed.

- *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. You are advised to manually remove any applications that Kaspersky Internet Security cannot remove automatically. When removing incompatible applications, you will need to restart your operating system, after which installation of Kaspersky Internet Security continues automatically.

- *Presence of malicious programs on the computer*. If any malicious programs that interfere with installation of anti-virus software are detected on the computer, the Setup Wizard prompts you to download *Kaspersky Virus Removal Tool*, a special tool designed to neutralize infections.

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

STEP 6. COMPLETING INSTALLATION

This page of the Setup Wizard informs you of the successful completion of application installation.

Restart the operating system after the application has been installed.

If the **Run Kaspersky Internet Security** check box is selected, the application will be started automatically after you restart your computer.

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

SWITCHING FROM KASPERSKY INTERNET SECURITY TO KASPERSKY TOTAL SECURITY

Kaspersky Internet Security allows you to switch to Kaspersky Total Security without any additional downloads or installation of software.

Kaspersky Total Security offers a number of additional features in comparison with Kaspersky Internet Security:

- Backup and Restore. Automatic scheduled backup functionality lets you save your data on removable and network drives or in Online storage.

- Identity Privacy Safeguards. Data Encryption protects your identity data. You can place your files in a data vault and lock it to prevent unauthorized access to the files.

- Password protection. Kaspersky Password Manager protects your online credentials. It lets you save your user names and passwords in a vault and automatically fill out entry fields in web forms.

- Manage Your Kaspersky Devices. Manage Your Kaspersky Devices functionality lets you manage protection of your computers remotely.

You can temporarily switch to the trial version of Kaspersky Total Security to try out the application's features, or purchase a license and start using Kaspersky Total Security.

IN THIS SECTION

TEMPORARY USE OF KASPERSKY TOTAL SECURITY

You can temporarily switch to the trial version of Kaspersky Total Security in order to evaluate its features. After that, you can choose to purchase a license for further use of the application.

➡ *To temporarily switch to the trial version of Kaspersky Total Security:*

1. Open the main application window.

2. Click the **Show Additional Tools** link to open the **Additional Tools** window.

3. In the **Additional Tools** window, click the **Switch to Kaspersky Total Security** link to start the migration wizard.

4. In the migration wizard window that opens, click the **Trial version** button.

5. Follow the wizard's instructions.

Step 1. Starting the upgrade

At this step, the wizard displays a message, informing you that all prerequisites for migration to the trial version of Kaspersky Total Security are met. To proceed with the wizard, click the **Continue** button.

Step 2. Removing incompatible applications

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

After incompatible applications are uninstalled, you may need to restart the operating system. After a restart, the wizard starts automatically, and the migration to the trial version of Kaspersky Total Security continues.

Step 3. Switching to the trial version of Kaspersky Total Security

At this step, the wizard prepares Kaspersky Total Security components for use, which may take some time. As soon as the process completes, the wizard automatically proceeds to the next step.

Step 4. Restarting the application

At this step of the migration to the trial version of Kaspersky Total Security, you must quit the application and start it again. To do this, in the wizard window, click the **Finish** button.

Step 5. Completing activation

After the application is restarted, the **Licensing** window of Kaspersky Total Security opens, showing information about the length of time during which you can use the trial version.

If your Kaspersky Internet Security license has not expired at the time when your switch to Kaspersky Total Security, you can continue using Kaspersky Internet Security under this license on a different computer.

SWITCHING TO PERMANENT USE OF KASPERSKY TOTAL SECURITY

If you want to switch to permanent use of Kaspersky Total Security, you must purchase a license for Kaspersky Total Security and then activate the application.

➡ *To purchase a license for Kaspersky Internet Security:*

1. Open the main application window.

2. In the **Show Additional Tools** drop-down list, select **Additional Tools**.

3. Click the **Switch to Kaspersky Total Security** link to start the migration wizard.

4. Click the **Purchase activation code** link to go to the website of the Kaspersky Lab eStore or a partner company on which you can purchase a license for Kaspersky Total Security.

When used in certain regions or by subscription, Kaspersky Anti-Virus does not allow switching to the trial version of Kaspersky Total Security. In such cases, the **Switch to Kaspersky Total Security** item is not displayed.

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**.

STEP 1. ENTERING THE PASSWORD TO REMOVE THE APPLICATION

To remove Kaspersky Internet Security, you must enter the password for accessing the application settings. If you cannot specify the password, for any reason, application removal will be prohibited.

This step is displayed only if a password has been set for application removal.

STEP 2. SAVING DATA FOR FUTURE USE

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

By default, the application offers to save information about the license.

➧ *To save data for further use, select the check boxes next to the types of data that you want to save:*

- **License information** is a set of data that rules out the need to activate the application during future installation, 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. To perform operations with these files, Kaspersky Internet Security must be installed.

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

  Kaspersky Lab does not guarantee support for 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** – databases containing specimens of spam messages added by the user.

- **Data Encryption** are files placed in storage using Data Encryption functionality.

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

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

After you remove Kaspersky Internet Security, you can specify the reason why you decided to remove the application by leaving a comment on the Kaspersky Lab website. To do this, visit the Kaspersky Lab website, by clicking the **Complete form** button.

This functionality may be unavailable in some regions.

During removal of the application, you must restart your operating system. If you cancel an immediate restart, completion of the removal procedure is postponed until the operating system is restarted or the computer is turned off and then started up.

APPLICATION LICENSING

This section provides information about key terms related to activation of the application. Read this section to learn more about the purpose of the End User License Agreement and ways to activate the application and renew your license.

IN THIS SECTION

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 application installation and not use 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 is related to the unique code that you have for activating your copy of Kaspersky Internet Security.

A 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 16)

To operate the application, you must purchase a license for application use.

The license has a limited term. When the license expires, the application continues to run, but with limited functionality (for example, you cannot update the application or use Kaspersky Security Network). You still can benefit from all of the application components and perform scans for viruses and other malware, but only using the databases installed before the license expired. To continue using Kaspersky Internet Security in fully functional mode, you must renew your license.

We recommend renewing the license before it expires, in order to ensure maximum protection of your computer against all security threats.

Before purchasing a license, you can get a free trial version of Kaspersky Internet Security. The trial version of Kaspersky Internet Security remains functional during a short evaluation period. After the evaluation period expires, all the features of Kaspersky Internet Security are disabled. To continue using the application, you must purchase a license.

ABOUT THE ACTIVATION CODE

An *activation code* is a code that you receive when you purchase 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:

- When you purchase a boxed version of Kaspersky Internet Security, an activation code is provided in the manual or on the retail box that contains the installation CD.

- When you purchase Kaspersky Internet Security from an online store, an activation code is emailed to the address that you have specified when ordering.

- If you participate in the Protect a Friend program (see the section "Participating in the Protect a Friend program" on page 84), 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 purchased a license for the use of Kaspersky Internet Security on several devices, the license term starts counting down from the moment you first apply the activation code.

If you lose or accidentally delete your activation code after activating the application, contact Kaspersky Lab Technical Support to restore the activation code (http://support.kaspersky.com).

ABOUT THE SUBSCRIPTION

A *subscription to Kaspersky Internet Security* establishes use of the application within the selected parameters (expiration date and number of protected devices). You can obtain 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 automatically, or cancel it. You can manage your subscription via your personal account page on the service provider's website.

Vendors can provide two types of subscriptions for Kaspersky Internet Security: update subscriptions and update and protection subscriptions.

A subscription can be limited (for example, to one year) or unlimited (with no expiration date). To continue using Kaspersky Internet Security after a limited subscription expires, you must renew it. Unlimited subscriptions are renewed automatically as long as timely prepayment has been made to the service provider.

When a limited subscription expires, you are given a grace period to renew your subscription. Application functionality remains unchanged during this time.

If the subscription is not renewed before the grace period expires, Kaspersky Internet Security stops updating the application databases (in the case of update subscriptions), stops interacting with Kaspersky Security Network, and also stops protecting the computer and running scan tasks (in the case of update and protection subscriptions).

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

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

To cancel your subscription, contact the service provider from whom you have 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, you agree to automatically provide the following information to Kaspersky Lab when you accept the provisions of the License Agreement:

- Information about the checksums of processed files (MD5, sha256)

- Information required for assessing the reputations of URLs

- Statistics on use of application notifications

- Statistical data for protection against spam

- Activation data and version of Kaspersky Internet Security in use

- Information about licensing of the installed version of Kaspersky Internet Security

- Information about the types of detected threats

- Information about digital certificates currently in use and information required to verify their authenticity

- Application operation details and licenses required to configure the display of content from trusted websites

If your computer is equipped with a TPM (Trusted Platform Module), you also agree to provide Kaspersky Lab with the TPM report on startup of the operating system and the information required to verify the report's authenticity. If an error occurs during installation of Kaspersky Internet Security, you agree to automatically supply Kaspersky Lab with information about the error code, the installation package that is currently in use, and your computer.

If you participate in Kaspersky Security Network (see the section "Participating in Kaspersky Security Network (KSN)" on page 82), you agree to automatically send the following information related to Kaspersky Internet Security use from your 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 probably infected objects and decisions made regarding those objects

- Information about applications that are downloaded and started

- Information about errors and use of the interface of Kaspersky Internet Security

- Application details, including application version, information about files of downloaded software modules, and versions of current application databases

- Statistics about updates and connections to Kaspersky Lab servers

- Information about the currently used wireless connection

- Statistics on delays caused by Kaspersky Internet Security while the user is using applications installed on the computer;

- Files that can be used by criminals to damage your computer, or fragments of such files, including files referenced by malicious links

> Information to be sent to Kaspersky Lab may be stored on your computer up to 30 days after it is created. Data items are kept in an internal protected storage. The maximum volume of data to store is 30 MB.

In addition, you agree to automatically send files (or parts of files) that are at higher risk of being exploited by intruders to do harm to the user's computer or data, to Kaspersky Lab for additional scanning.

Kaspersky Lab protects all received data as required by applicable laws. Kaspersky Lab uses all received information as aggregate statistics only. Aggregate statistics are automatically generated from the source information that is received, and do not contain any personal data or other confidential information. Source information is stored in encrypted form and is destroyed as it is accumulated (twice per year). Aggregate statistics are stored indefinitely.

PURCHASING A LICENSE

If you have installed Kaspersky Internet Security and have not purchased a license yet, you can purchase a license 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 32).

➡ *To purchase a license:*

1. Open the main application window.

2. In the lower part of the main window, click the **License** link to open the **Licensing** window.

3. In the window that opens, click the **Purchase activation code** button.

The web page of Kaspersky Lab eStore or a partner company opens on which you can purchase a license.

ACTIVATING THE APPLICATION

To make use of the features of the application and its additional services, you must activate it.

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 that appear in the taskbar notification area.

➡ *To activate Kaspersky Internet Security:*

1. Open the main application window.

2. In the lower part of the main application window, click the **Enter activation code** link. The **Activation** window opens.

3. In the **Activation** window, enter the activation code in the entry field and click the **Activate** button.

An application activation request is made.

4. Enter the user's registration data.

Depending on the terms of use, the application can prompt you to log in to My Kaspersky portal. If you are not a registered user, complete the registration form to gain access to additional features.

Registered users can perform the following actions:

- Contact Technical Support and the Virus Lab.

- Manage activation codes.

- Receive information about new applications and special offers from Kaspersky Lab.

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

5. Click the **Finish** button in the **Activation** window to complete the registration procedure.

RENEWING A LICENSE

You can renew a license when it is about to expire. To do this, you can specify a new activation code without waiting for the current license to expire. When the current license expires, Kaspersky Internet Security is activated automatically with the extra activation code.

➡ *To specify an extra activation code for automatic renewal of the license:*

1. Open the main application window.

2. In the lower part of the main window, click the **License** link to open the **Licensing** window.

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

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

   Kaspersky Internet Security then sends the data to the Kaspersky Lab activation server for verification.

5. Click the **Finish** button.

   The new activation code will be displayed in the **Licensing** window.

The application is automatically activated with the new activation code when the license expires. You can also activate the application manually with a new activation code, by clicking the **Activate now** button. This button is available if the application has not been activated automatically. This button is unavailable before the license expires.

> If the new activation code that you specify has already been applied on this computer or on another computer, the activation date for the purpose of renewing the license is the date on which the application was first activated with this activation code.

MANAGING APPLICATION NOTIFICATIONS

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

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

- *Important notifications* inform you of events that are potentially important for the computer's security, such as detection of a probably infected object or suspicious activity in the operating system. Windows used for important notifications and pop-up messages are yellow.

- *Information notifications* inform you of events that do not have critical importance for the computer's security. Windows used for information notifications and pop-up messages are green.

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 when the computer is restarted, when Kaspersky Internet Security is quit, or in Connected Standby mode in Windows 8. When a notification is closed automatically, Kaspersky Internet Security performs the default recommended action.

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

ASSESSING COMPUTER PROTECTION STATUS AND RESOLVING SECURITY ISSUES

Problems with computer protection are symbolized by an indicator located in the upper part of the main application window. Green indicates that your computer is protected. Yellow indicates that there are protection problems and red indicates that your computer's security is at serious risk. You are advised to fix problems and security threats immediately.

Clicking the indicator in the main application window opens the **Notification Center** window (see the following figure), which contains detailed information about the status of computer protection and suggestions for how to fix the detected problems and threats.
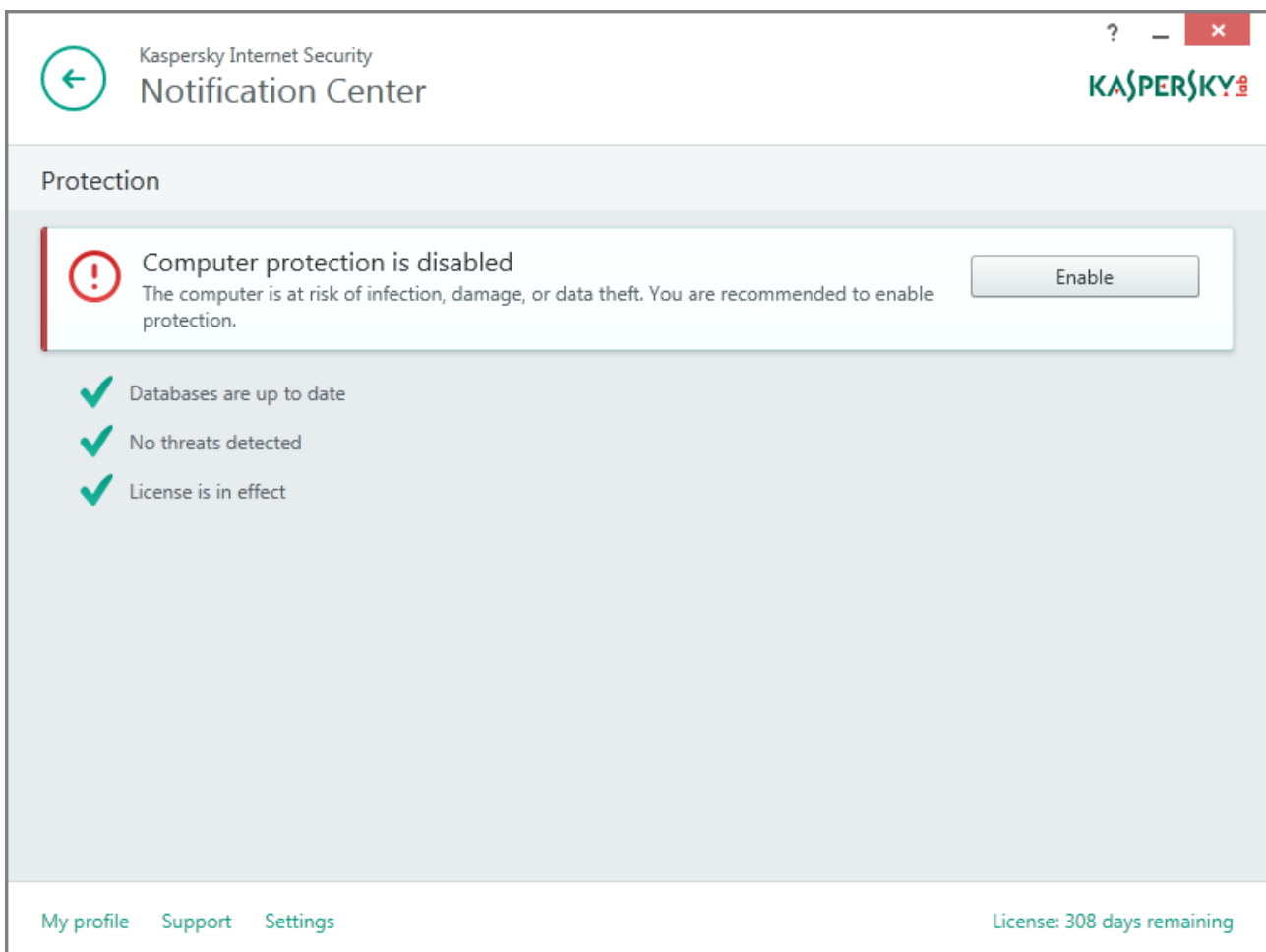
Figure 1. Notification Center window

Problems with protection are grouped by categories. For each problem, a list is displayed of actions that you can take to solve the problem.

UPDATING DATABASES AND APPLICATION SOFTWARE MODULES

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

To download an update package from Kaspersky Lab servers, an Internet connection is required.

On Microsoft Windows 8, update packages are not downloaded if a broadband Internet connection is established and a limit has been set in the application on traffic over this type of connection. To download the update package, you must manually disable the limit in the application settings window, in the **Network** subsection.

➡ *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 **Update**.

➡ *To run an update from the main application window:*

1. Open the main application window and click the **Update** button.

    The **Update** window opens.

2. In the **Update** window, click **Update**.

SCANNING THE COMPUTER

This section provides information about how to scan your computer for viruses and other threats.

IN THIS SECTION

FULL SCAN

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

- System memory

- Objects loaded on operating system startup

- Storage

- Hard drives and removable drives

We recommend running a full scan immediately after installing Kaspersky Internet Security to your computer.

➡ *To start a full scan:*

1. Open the main application window.

2. Click the **Scan** button.

   The **Scan** window opens.

3. In the **Scan** window, select the **Full Scan** section.

4. In the **Full Scan** section, click the **Run scan** button.

Kaspersky Internet Security starts a full scan of your computer.

CUSTOM SCAN

A custom scan lets you scan a file, folder, or drive for viruses and other threats.

You can start a custom scan in the following ways:

- From the context menu of the object

- From the main application window

➡ *To start a custom scan from the context menu of an object:*

1. Open Microsoft Windows Explorer and go to the folder that 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**.
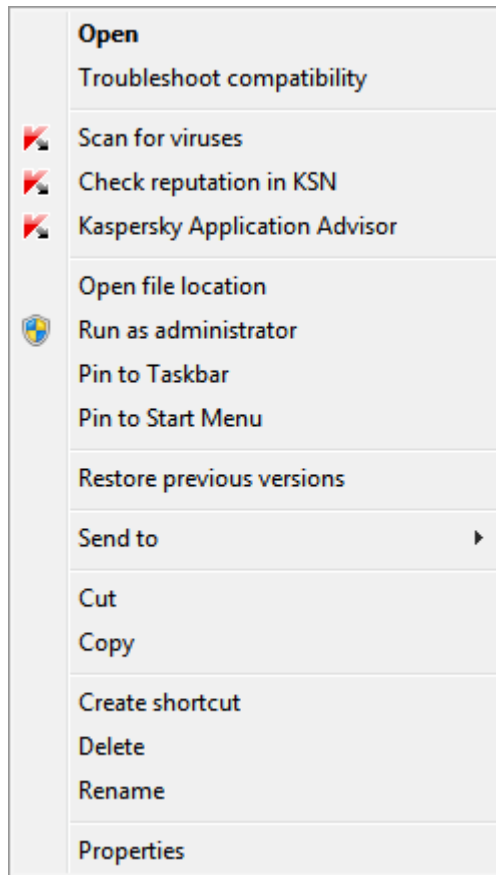
Figure 2. Object context menu

➡ *To start a custom scan from the main application window:*

1. Open the main application window.

2. Click the **Scan** button.

   The **Scan** window opens.

3. In the **Scan** window, select the **Custom Scan** section.

4. Specify objects to be scanned in one of the following ways:

   - Drag objects to the **Custom Scan** window.

   - Click the **Add** button and, in the file or folder selection window that opens, specify an object.

5. Click the **Run scan** button.

QUICK SCAN

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

- Objects loaded at the startup of the operating system

- System memory

- Boot sectors of the disk

➡ *To start a quick scan:*

1. Open the main application window.

2. Click the **Scan** button.

   The **Scan** window opens.

3. In the **Scan** window, select the **Quick Scan** section.

4. In the **Quick Scan** section, click the **Run scan** button.

Kaspersky Internet Security starts a quick scan of your computer.

VULNERABILITY SCAN

Vulnerabilities are unprotected places in software code that intruders may deliberately use for their purposes, for example, to copy the data used by applications that have unprotected code. Scanning your computer for vulnerabilities helps you to reveal any such weak points in the protection of your computer. You are advised to fix any vulnerabilities that are found.

➡ *To start a vulnerability scan:*

1. Open the main application window.

2. In the lower part of the main window, click the **Show Additional Tools** link. The **Tools** window opens.

3. In the left part of the **Tools** window, click the **Vulnerability Scan** link to open the **Vulnerability Scan** window.

4. In the **Vulnerability Scan** window, click the **Run scan** button.

Kaspersky Internet Security starts scanning your computer for vulnerabilities.

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 the backup copy of it that was created by the application during scanning of the object.

Kaspersky Internet Security does not disinfect Windows Store apps. If scanning results indicate that such an app is dangerous, it is deleted from your computer.

When a Windows Store app is deleted, Kaspersky Internet Security does not create a backup copy of it. To restore such objects, you must use the recovery tools included with the operating system (for detailed information, see the documentation for the operating system that is installed on your computer) or update apps via the 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 main window, click the **Show Additional Tools** link. The **Tools** window opens.

3. In the left part of the **Tools** window, click the **Quarantine** link to open the **Quarantine** window.

4. In the **Quarantine** window that opens, select the required file from the list and click the **Restore** button.

TROUBLESHOOTING THE OPERATING SYSTEM AFTER INFECTION

This section provides information about how to restore the operating system after it has been infected with viruses.

RECOVERING THE OPERATING SYSTEM AFTER INFECTION

If you suspect that the operating system of your computer has been corrupted or modified due to malware activity or a system failure, use the *Microsoft Windows Troubleshooting Wizard*, which 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, which can include access to the network being blocked, file name extensions for known formats being changed, Control Panel being blocked, etc. There are different reasons for these different kinds of damage. These reasons may include malware activity, incorrect system configuration, system failures, or malfunctioning applications for system optimization.

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

TROUBLESHOOTING THE OPERATING SYSTEM BY USING THE MICROSOFT WINDOWS TROUBLESHOOTING WIZARD

➡ *To run the Microsoft Windows Troubleshooting Wizard:*

1. Open the main application window.

2. In the lower part of the main window, click the **Show Additional Tools** link. The **Tools** window opens.

3. In the left part of the **Tools** window, click the **Microsoft Windows Troubleshooting** link to run the Microsoft Windows Troubleshooting Wizard.

The Microsoft Windows Troubleshooting Wizard window opens.

The Wizard consists of a series of pages (steps), which you can navigate through by clicking the **Back** and **Next** buttons. To close the Wizard after it finishes, 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 recovery of the operating system

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

Step 2. Problems search

The Wizard searches for problems and damage that should be fixed. When the search is complete, the Wizard proceeds automatically to the next step.

Step 3. Select actions to fix damage

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

- *Strongly recommended actions*, which eliminate problems that pose a serious security threat. You are advised to perform all actions in this group.

- *Recommended actions* are aimed at repairing damage that may pose a threat. You are advised to perform all actions in this group as well.

- *Additional actions* repair system damage that is not dangerous now, but may pose a threat 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, to the left of an action, select the corresponding check box. By default, the Wizard performs all recommended and strongly recommended actions. If you do not want 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 for the Wizard to perform, click the **Next** button.

Step 4. Fixing damage

The Wizard performs the actions selected during the previous step. It may take a while to fix damage. After fixing damage, the Wizard automatically proceeds to the next step.

Step 5. Wizard completion

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

PROTECTING EMAIL

This section provides information about how to protect your email against spam, viruses, and other threats.

CONFIGURING MAIL ANTI-VIRUS

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

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** 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. When you select the high security level, deep heuristic analysis is enabled.

6. In the **Action on threat detection** drop-down list, select the action that you want for Mail Anti-Virus to perform when an infected object is detected (for example, disinfect).

If no threats are detected in an email message, or if all infected objects have been successfully disinfected, the message becomes available for further access. If the component fails to disinfect an infected object, Mail Anti-Virus renames or deletes the object from the message and adds a notification to the message subject line, 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 in Quarantine (see the section "Restoring an object deleted or disinfected by the application" on page 40).

BLOCKING UNWANTED EMAIL (SPAM)

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

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

1. Open the main application window.

2. In the lower part of the window, click the **Settings** link. Go to the **Settings** section.

3. In the left part of the window, select the **Protection** section.

4. In the right part of the **Protection** section, select the **Anti-Spam** component.

   The window displays the settings of Anti-Spam.

5. In the right part of the window, enable Anti-Spam by using the switch.

6. In the **Security level** section, make sure that the **Recommended** security level is set.

PROTECTING PRIVATE DATA ON THE INTERNET

This section provides information about how to make your Internet browsing safe and protect your data against theft.

ABOUT PROTECTION OF PRIVATE DATA ON THE INTERNET

Kaspersky Internet Security helps you to protect your 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 who use methods such as phishing and interception of data entered on the keyboard.

Protection against phishing is provided by Anti-Phishing, which is 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 Keyboard Input.

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).

ABOUT 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.

Many programs classified as spyware can take screenshots, which then are automatically transmitted to an intruder for further analysis to steal the user's personal data. Virtual Keyboard protects entered personal data from attempts to intercept it by means of screenshots.

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.

The use of Virtual Keyboard has the following limitations:

- 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 and 11 with the new Windows user interface style or for Microsoft Internet Explorer 10 and 11 browsers if the **Enable 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.

- Virtual Keyboard does not prevent screenshots that are made by using the **PRINT SCREEN** key and other combinations of keys specified in the operating system settings.

- When running Virtual Keyboard, the AutoComplete feature of Microsoft Internet Explorer stops functioning, since the implementation of the automatic input scheme may allow criminals to intercept data.

- Kaspersky Internet Security does not provide protection against unauthorized screenshots in Microsoft Windows 8 and 8.1 (64-bit only) if the Virtual Keyboard window is open but the Protected Browser process is not started.

- In some browsers (such as Google Chrome), protection of data input may not work for certain types of data (such as email addresses or numbers).

The preceding list describes the main restrictions in functionality for protection of data input. A full list of restrictions is given in an article on the Kaspersky Lab Technical Support website http://support.kaspersky.com/11047.

STARTING VIRTUAL KEYBOARD

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 window of Microsoft Internet Explorer, Mozilla Firefox, or Google Chrome, by clicking the Virtual Keyboard quick access icon

- 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 (see the section "Configuring the display of the Virtual Keyboard icon" on page 48).
  >
  > When Virtual Keyboard is used, Kaspersky Internet Security disables the autofill option for entry fields on websites.

- By pressing a combination of keyboard keys.

➡ *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**.
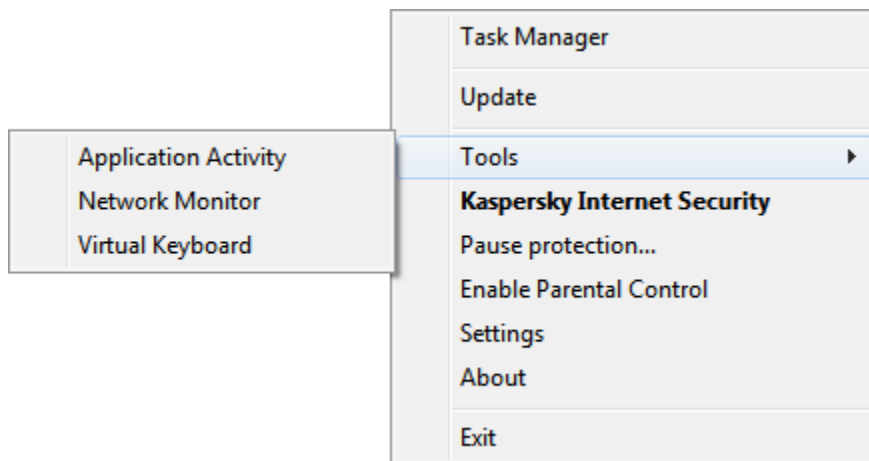
Figure 3. Kaspersky Internet Security context menu

➡ *To open Virtual Keyboard from the main application window:*

1. Open the main application window.

2. In the lower part of the main window, click the **Show Additional Tools** link. The **Tools** window opens.

3. In the left part of the **Tools** window, click the **Virtual Keyboard** link to open Virtual Keyboard.

➡ *To open Virtual Keyboard from the window of the Microsoft Internet Explorer or Mozilla Firefox browser,*

click the **Virtual Keyboard** button on the browser toolbar.

➡ *To open Virtual Keyboard from the window of the Google Chrome browser,*

1. Click the **Kaspersky Protection** button on the browser toolbar.

2. Select the **Virtual Keyboard** item in the menu that opens.

➡ *To open the Virtual Keyboard by using the hardware keyboard:*

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

CONFIGURING THE DISPLAY OF THE VIRTUAL KEYBOARD ICON

➡ *To configure 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 to open the **Secure Data Input settings** window.

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

      The Virtual Keyboard quick launch icon is 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:

      a. Click the **Configure exclusions** link to open the **Exclusions for Virtual Keyboard** window.

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

         A window opens for adding an exclusion for Virtual Keyboard.

      c. In the **URL mask** field, enter the web address of a website.

      d. If you want the Virtual Keyboard quick launch icon to be displayed (or not to be displayed) on a specified web page only, in the **Scope** section, select **Apply to the specified page**.

      e. In the **Virtual Keyboard icon** section, specify whether to display the Virtual Keyboard quick launch icon on the specified web page.

      f. 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 is displayed in the entry fields in accordance with the specified settings.

PROTECTING DATA ENTERED ON THE COMPUTER KEYBOARD

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

Secure Keyboard Input has the following limitations:

- Protection of data input from the computer keyboard is available only 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.

- Secure Keyboard Input is not available in Microsoft Internet Explorer from Windows Store.

- 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.

- In some browsers (such as Google Chrome), protection of data input may not work for certain types of data (such as email addresses or numbers).

The preceding list describes the main restrictions in functionality for protection of data input. A full list of restrictions is given in an article on the Kaspersky Lab Technical Support website http://support.kaspersky.com/11047.

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 configure protection of data input from the computer keyboard:*

1. Open the main application window.

2. In the lower part of the window, click the **Settings** link. Go to the **Settings** section.

3. In the **Additional** section, select the **Secure Data Input** subsection.

    The window displays the settings for secure data input.

4. In the lower part of the window, in the **Secure Keyboard Input** section, select the **Enable Secure Keyboard Input** check box.

5. Specify the protection scope for data input from the hardware keyboard:

    a. Open the **Secure Data Input settings** window by clicking the **Edit categories** link in the lower part of the **Secure Keyboard Input** 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 **Exclusions for Secure Keyboard Input** window by clicking the **Configure exclusions** link.

        b. In the window, click the **Add** button.

            A window opens for adding an exclusion to Secure Keyboard Input.

        c. In the window that opens, in the **URL mask** field, enter a website address.

     d.   Select one of the options for Secure Data Input on this website (**Apply to the specified web page** or **Apply to the entire website**).

     e.   Select the 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 **Exclusions for Secure Keyboard Input** window. When this website is accessed, Secure Data Input will be active, functioning in accordance with the settings that you have specified.

CONFIGURING NOTIFICATIONS ABOUT VULNERABILITIES IN WI-FI NETWORKS

When you are connected to a Wi-Fi network, your confidential data may be stolen if that network is protected poorly. Kaspersky Internet Security checks Wi-Fi networks every time you connect to one. If the Wi-Fi network is not secure (for example, a vulnerable encryption protocol is used, or the name of the Wi-Fi network (SSID) is very popular), the application displays a notification informing you that you are about to connect to an insecure Wi-Fi network. Click the link in the notification window to learn how to safely use the Wi-Fi network.

➡ *To configure notifications of vulnerabilities on Wi-Fi networks:*

1. Open the main application window.

2. In the lower part of the window, click the **Settings** link. Go to the **Settings** section.

3. In the left part of the window, select the **Protection** section.

4. In the right part of the **Protection** section, select the **Firewall** subsection.

   The window displays the settings of the Firewall component.

5. Select the **Notify of vulnerabilities in Wi-Fi networks** check box if it has been cleared. If you do not want to receive notifications, clear the check box. This check box is selected by default.

6. If the **Notify of vulnerabilities in Wi-Fi networks** check box is selected, you can edit the advanced settings for display of notifications:

   • Select the **Block and warn about insecure transmission of passwords over the Internet** check box to block all transmission of passwords in non-encrypted text format when you fill in the **Password** fields on the Internet. This check box is cleared by default.

   • Click the **Reset hidden alerts** link to roll back to the default values of settings for display of notifications about transfers of passwords in non-encrypted form. If you have previously blocked display of notifications about password transfer in non-encrypted form, display of these notifications will resume.

PROTECTING FINANCIAL TRANSACTIONS AND ONLINE PURCHASES

To provide protection for confidential data that you enter on websites of banks and payment systems (such as bank card numbers and passwords for accessing online banking services), as well as to prevent funds from being stolen when you make online payments, Kaspersky Internet Security prompts you to open such websites in Protected Browser.

Protected Browser is a special browser operating mode designed to protect your data as you access bank or payment system websites. Protected Browser is started in an isolated environment to prevent other applications from injecting their code into the process of Protected Browser.

In Protected Browser mode, the application provides protection against the following types of threats:

- Untrusted modules. The application runs a check for untrusted modules every time you visit a bank or payment system website.

- Rootkits. The application scans for rootkits at Protected Browser startup.

- Known operating system vulnerabilities. The application scans for operating system vulnerabilities at Protected Browser startup.

- Invalid certificates of bank or payment system websites. The application checks certificates when you visit a bank or payment system website. The check is performed against a database of compromised certificates.

When you open a website in Protected Browser, a frame appears on the borders of the browser window. The color of the frame indicates the protection status.

The frame of the browser window can display the following color indications:

- Green frame. Signifies that all checks have been performed successfully. You can continue using Protected Browser.

- Yellow frame. Signifies that checks have revealed security problems that need to be resolved.

  The application can detect the following threats and security problems:

  - Untrusted module. Computer scanning and disinfection is required.

  - Rootkit. Computer scanning and disinfection is required.

  - Operating system vulnerability. Operating system updates need to be installed.

  - Invalid certificate of a bank or payment system website.

  > If you do not eliminate the threats detected, the security of the bank or payment system website connection session is not guaranteed. Events involving the launch and use of Protected Browser with reduced protection are recorded in the Windows event log.

  The yellow color of the frame may also signify that Protected Browser cannot be started due to technical limitations. For example, a third-party hypervisor is running or your computer does not support hardware virtualization technology.

For proper functioning of Protected Browser, make sure that the Safe Money plug-ins are activated. The plug-ins are automatically activated in the browser when it is first restarted after the installation of Kaspersky Internet Security. If you have not quit and started your browser again after installing Kaspersky Internet Security, the plug-ins are not activated.

Automatic activation of plug-ins has the following limitations:

- Plug-ins are integrated and activated only in browsers that are supported by the application.

  The following browsers support Safe Money plug-ins:

  - Internet Explorer 8.0, 9.0, 10.0, and 11.0

    > Internet Explorer 10 and Internet Explorer 11 browsers with the new Windows user interface are not supported.

  - Mozilla Firefox 19.x, 20.x, 21.x, 22.x, 23.x, 24.x, 25.x, 26.x, 27.x, 28.x, 29.x, 30.x, 31.x, 32.x, 33.x, 34.x, and 35.x

- Google Chrome 33.x, 34.x, 35.x, 36.x, 37.x, and 38.x

  Kaspersky Internet Security supports Google Chrome 37.x and 38.x both in 32-bit and in 64-bit operating systems.

  Mozilla Firefox plug-ins are not activated automatically if no user profile has been created in the browser. To create a user profile, quit your browser and start it again.

  At the first startup of Google Chrome in protected mode, the web browser prompts you to install an extension named Kaspersky Protection Plugin, which activates plug-ins of the Safe Money component. If you have rejected installation of Kaspersky Protection Plugin, you can install it later by clicking this link: http://support.kaspersky.com/interactive/google/en/kisplugin.

- When your browser is updated, the plug-ins are activated automatically only if the new version supports the same plug-in activation method as the previous version. If the new version of the browser supports the same plug-in activation method as the previous version, the plug-ins are activated automatically.

If the plug-ins are not activated automatically when you start the browser again, you need to activate them manually. You can check if the plug-ins are activated and activate them manually in the browser settings. You can refer to the help system of your current browser for more details on plug-in activation.

You can enable or disable automatic activation of plug-ins (see the section "Enabling automatic activation of Safe Money plug-ins" on page 53) in the application settings window.

> Protected Browser cannot be run if the **Enable Self-Defense** check box is cleared in the **Self-Defense** subsection of the **Advanced Settings** section of the application settings window.

IN THIS SECTION

CONFIGURING SAFE MONEY

➡ *To configure Safe Money:*

1. Open the main application window.

2. In the lower part of the main window, click the **Settings** link to go to the **Settings** section.

3. In the left part of the window, select the **Protection** section.

4. In the right part of the **Protection** section, select the **Safe Money** subsection.

   The window displays the settings of the Safe Money component.

5. Enable Safe Money by clicking the switch in the upper part of the window.

6. To enable notifications regarding vulnerabilities detected in the operating system before running Protected Browser, select the **Notify about operating system vulnerabilities** check box.

CONFIGURING SAFE MONEY FOR A SPECIFIC WEBSITE

➡ *To configure Safe Money for a specified website:*

1. Open the main application window.

2. In the lower part of the main window, click the **Safe Money** button.

   The **Safe Money** window opens.

3. Click the **Add website to Safe Money** button.

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

4. In the **Website for Safe Money** field, enter the web address of the website that you want to open in Protected Browser.

   A website address must be preceded by the prefix for the https:// protocol, which is used by default by Protected Browser.

5. If necessary, in the **Description** field, enter the name or a description for the website.

6. Select the action that you want Protected Browser to perform when you open the website:

   - If you want the website to open in Protected Browser every time you visit it, select **Run Protected Browser**.

   - If you want Kaspersky Internet Security to prompt you for an action when the website is opened, select **Prompt for action**.

   - If you want to disable Safe Money for the website, select **Do not run Protected Browser**.

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

The website will be displayed in the list in the left part of the window.

ENABLING AUTOMATIC ACTIVATION OF SAFE MONEY PLUG-INS

➡ *To enable activation of Safe Money plug-ins in browsers:*

1. Open the main application window.

2. In the lower part of the main window, click the **Settings** link to go to the **Settings** section.

3. In the left part of the window, select the **Protection** section.

4. In the right part of the **Protection** section, select the **Web Anti-Virus** section.

5. In the **Web Anti-Virus settings** window that opens, click the **Advanced Settings** link to open the **Advanced settings of Web Anti-Virus** window.

6. In the **Web browser extensions** section, select the **Automatically activate application plug-ins in all web browsers** check box.

ABOUT PROTECTION AGAINST SCREENSHOTS

To protect your data when you browse protected websites, Kaspersky Internet Security prevents spyware from taking unauthorized screenshots. Protection against screenshots is enabled by default. If protection has been disabled manually, you can enable it in the application settings window (see the section "Enabling protection against screenshots" on page 54).

Kaspersky Internet Security uses hypervisor technology to provide protection against screenshots. On computers running on Microsoft Windows 8 x64, the protection against screenshots that is provided by the Kaspersky Internet Security hypervisor has the following limitations:

- This feature is not available when a third-party hypervisor, such as the VMware® virtualization hypervisor, is running. After you close the third-party hypervisor, protection against screenshots becomes available again.

- The feature is not available if the CPU of your computer does not support hardware virtualization technology. For more details on whether your CPU supports hardware virtualization, please refer to the documentation shipped with your computer or to the website of the CPU manufacturer.

- The feature is not available if a third-party hypervisor (such as the VMware hypervisor) is running when you start Protected Browser.

ENABLING PROTECTION AGAINST SCREENSHOTS

➡ *To enable protection against screenshots:*

1. Open the main application window.

2. In the lower part of the window, click the **Settings** link. Go to the **Settings** section.

3. In the left part of the window, select the **Protection** section.

4. In the right part of the **Protection** section, select the **Safe Money** subsection and make sure that the Safe Money switch is on.

   The **Safe Money settings** window opens.

5. In the **Additional** section, select the **Block capturing screenshots in Protected Browser** check box.

ABOUT CLIPBOARD DATA PROTECTION

Kaspersky Internet Security blocks unauthorized access by applications to the clipboard when you make online payments, thus preventing theft of data by criminals. Such blocking is active only if an untrusted application attempts to obtain unauthorized access to your clipboard. If you copy data manually from the window of an application to another application's window (for example, from Notepad to a text editor window), access to clipboard is allowed. If the Internet Explorer® browser opened in regular mode is the source of data being copied, only data from the browser address field can be copied to clipboard.

CHECKING A WEBSITE FOR SAFETY

Kaspersky Internet Security allows checking the safety of a website before you click a link to open it Websites are checked using *Kaspersky URL Advisor*, which is integrated into the Web Anti-Virus component.

Kaspersky URL Advisor is not available in Microsoft Internet Explorer 10 and 11 Windows 8 style browsers.

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

- – if the linked web page is safe according to Kaspersky Lab

- – if there is no information about the safety status of the linked web page

- – if the linked web page is dangerous according to Kaspersky Lab

To view a pop-up window with more details on the link, move the mouse pointer 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 to open the **Settings** window.

3. In the **Protection** 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 the checking status for the web page (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 websites** 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** window, 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 about the safety of links on all web pages, in the **Check 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, *Profanity, obscenity*):

    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 the specified web pages and displays information about categories of the links in accordance with the current settings.

ANTI-BANNER PROTECTION DURING WEBSITE BROWSING

The Anti-Banner component is designed to provide protection against banners while you browse the web. If this component is enabled, you can block banners directly on a web page or specify the website address and mask using which Kaspersky Internet Security will block banners on this website. By default, Kaspersky Internet Security provides protection against the most common types of banners.

IN THIS SECTION

ENABLING THE ANTI-BANNER COMPONENT

➡ *To enable the Anti-Banner component:*

1. Open the main application window.

2. Click the **Settings** link to open the **Settings** window.

3. Select the **Protection** section.

4. Enable the **Anti-Banner** component.

BLOCKING WEBSITE BANNERS

➡ *To block website banners:*

1. While on a website, place the mouse pointer over the banner that you want to hide.

2. Press the **CTRL** key on the keyboard.

3. In the menu that opens, select **Add to Anti-Banner**.

   The **Blocked URLs** window opens.

4. In the **Blocked URLs** window, click the **Add** button.

   The banner URL is added to the list of blocked URLs.

5. Refresh the web page in the browser to stop the banner from showing.

The banner will not be displayed the next time you visit this web page.

BLOCKING ALL WEBSITE BANNERS

You can block all banners on a certain website. To do so, specify the mask for this website and add it to the list of blocked web addresses.

➡ *To block all banners on a website:*

1. Open the main application window.

2. Click the **Settings** link to open the **Settings** window.

3. Select the **Protection** section.

4. Select the **Anti-Banner** component.

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

5. In the **Anti-Banner settings** window, click the **Configure blocked URLs** link to open the **Blocked URLs** window.

6. In the **Blocked URLs** window, click the **Add** button.

7. In the window that opens, in the **Web address mask (URL)** field enter the address mask for the website on which you want to block banners. For example: `http://example.com*`.

8. Specify **Active** as the status for this website.

9. Click the **Add** button.

Kaspersky Internet Security starts blocking banners on the http://example.com website.

REMOVING TRACES OF ACTIVITY ON THE COMPUTER AND ON THE INTERNET

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, as well as opened and saved files

- Microsoft Windows event log entries

- Other information about user activity

Intruders and unauthorized persons may be able to gain access to private information contained in data on past user actions.

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

➡ *To run the Privacy Cleaner Wizard:*

1. Open the main application window.

2. In the lower part of the main window, click the **Show Additional Tools** link. The **Tools** window opens.

3. In the left part of the **Tools** window, click the **Privacy Cleaner** link to run the Privacy Cleaner Wizard.

The Wizard consists of a series of pages (steps), which you can navigate through by clicking the **Back** and **Next** buttons. To close the Wizard after it finishes, 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 traces search

This Wizard searches for traces of activity on 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 the detected activity traces and asks about the actions to take for elimination of these activity traces (see the following figure).
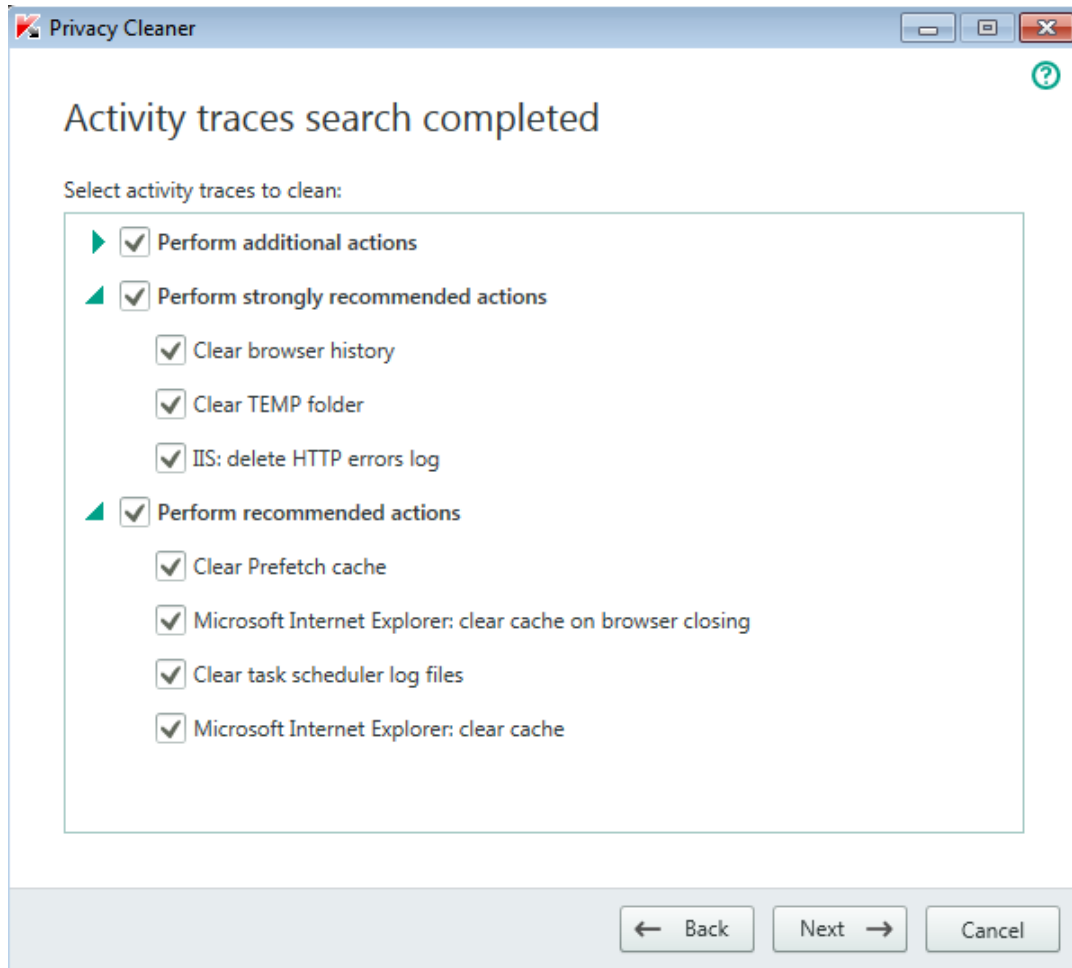
Figure 4. Activity traces detected and recommendations on eliminating them

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

To make the Wizard perform a certain action, to the left of an action, select the corresponding check box. By default, the Wizard performs all recommended and strongly recommended actions. If you do not want 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 for the Wizard to perform, click the **Next** button.

Step 4. Privacy Cleaner

The Wizard performs the actions selected during the previous step. 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.

CONTROLLING USERS' ACTIVITY ON THE COMPUTER AND ON THE INTERNET

This section provides information about how to control users' actions on the computer and on the Internet by using Kaspersky Internet Security.

IN THIS SECTION

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.

More and more children and teenagers are obtaining access to computers and web resources. The use of computers and the Internet presents a number of challenges and threats 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 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 on search engines (links to websites with questionable 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.

PROCEEDING TO THE PARENTAL CONTROL SETTINGS

➡ *To go to the Parental Control settings:*

1. Open the main application window.

2. In the main application window, click the **Parental Control** button.

3. When you open the **Parental Control** window for the first time, the application prompts you to set a password to protect Parental Control settings. Select one of the following options:

   - If you want to password-protect access to Parental Control settings, fill in the **Password** and **Confirm** fields and click the **Continue** button.

   - If you do not want to password-protect access to Parental Control settings, click the **Skip** link to continue to the Parental Control settings.

   The **Parental Control** window opens.

4. Select a user account and click the **Configure restrictions** link to open the Parental Control settings window.

CONTROLLING COMPUTER USE

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 a daily time limit on total computer use. You can specify different limit amounts for weekdays and for weekends.

➡ *To configure time limits on computer use:*

1. Go to the Parental Control settings window (see the section "Proceeding to the Parental Control settings" on page <u>61</u>).

2. In the Parental Control settings window, select the **Computer** section.

3. To specify a time interval during which Parental Control will block access to the computer, in the **Weekdays** and **Weekends** sections, select the **Block access from** check box.

4. In the drop-down list next to the **Block access from** check box, specify the block start time.

5. In the **to** drop-down list, specify the block end time.

    You can also set up a schedule of computer use by using a table. To view the table, click the ⏰ ⊞ button.

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

6. To set a time limit on total computer use during the day, in the **Weekdays** and **Weekends** sections, select the **Allow access for no longer than** check box and, from the drop-down list next to the check box, select a time interval.

    Parental Control blocks the user's access to the computer when the total computer use during a day exceeds the specified amount of time.

7. To set up breaks in the user's sessions of computer use, in the **Time breaks** section, select the **Take a break every** check box and then, from the drop-down lists next to the check box, select values for the frequency of breaks (for example, every hour) and their length (for example, 10 minutes).

8. In the **Parental Control** window, activate the **Parental Control** switch located next to the user account.

Parental Control blocks the user's access to the computer in accordance with the new settings.

CONTROLLING INTERNET USE

By using Parental Control, you can limit time spent on the Internet and prohibit users from accessing certain categories of websites or specified websites. You can also prohibit the user from downloading files of certain types (such as archives or videos) from the Internet.

➡ *To set a time limit on Internet use:*

1. Go to the Parental Control settings window (see the section "Proceeding to the Parental Control settings" on page 61).

2. In the Parental Control settings window, select the **Internet** section.

3. If you want to limit the total time for Internet use on weekdays, in the **Internet access restriction** section select the **Restrict access on weekdays to <HH:MM> hours per day** check box and then, from the drop-down list next to the check box, select a value for the time limit.

4. If you want to limit the total time for Internet use on weekends, select the **Restrict access on weekends to <HH:MM> hours per day** check box and then, from the drop-down list next to the check box, select a value for the time limit.

5. In the **Parental Control** window, activate the **Parental Control** switch located next to the user account.

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 visits to specific websites:*

1. Go to the Parental Control settings window (see the section "Proceeding to the Parental Control settings" on page 61).

2. In the Parental Control settings window, select the **Internet** section.

3. To keep adult content from being displayed in search results, in the **Control Web Browsing** section select the **Enable Safe Search** check box.

    When you search for information on such websites as Google™, YouTube™ (only for users who have not signed in to the youtube.com website under their account), Bing®, Yahoo!™, Mail.ru, VKontakte, and Yandex, no adult content will be displayed in the search results.

4. 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 website categories** window.

   c. Select the check boxes next to categories of websites that you want to block.

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

5. 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 in the list** and click the **Add exclusions** link to open the **Exclusions** 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 to which you want to prohibit visits, by filling in the **URL mask** field.

   e. In the **Scope** section, define the scope of what you want to block: 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 **Exclusions** window.

6. In the **Parental Control** window, activate the **Parental Control** switch located next to the user account.

Parental Control will block all of the user's attempts to open any listed website, in accordance with the current settings.

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

1. Go to the Parental Control settings window (see the section "Proceeding to the Parental Control settings" on page <u>61</u>).

2. In the Parental Control settings window, select the **Internet** section.

3. In the **Block file downloading** section, select the check boxes next to file types for which you want to block downloads.

4. In the **Parental Control** window, activate the **Parental Control** switch located next to the user account.

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

CONTROLLING STARTUP OF GAMES AND APPLICATIONS

By using Parental Control, you can allow or prohibit the user to start games depending on their age rating. You can also prohibit the user from starting specified applications (such as games or IM clients) or limit the time allowed for using applications.

➡ *To block games with age-inappropriate content:*

1. Go to the Parental Control settings window (see the section "Proceeding to the Parental Control settings" on page 61).

2. In the Parental Control settings window, select the **Applications** section.

3. In the **Block games by content** section, block startup of games that are inappropriate for the selected user based on age and/or content:

   a. If you want to block all games that contain content inappropriate for the user's age, select the **Block games by age rating** check box and, from the drop-down list next to the check box, select an age restriction option.

   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 **Block games by categories** window.

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

4. In the **Parental Control** window, activate the **Parental Control** switch located next to the user account.

➡ *To restrict startup of a specific application:*

1. Go to the Parental Control settings window (see the section "Proceeding to the Parental Control settings" on page 61).

2. In the Parental Control settings window, select the **Applications** section.

3. In the lower part of the window, click the **Add application to list** link to open the **Open** dialog box and select the executable file of an application.

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

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

5. If you want to restrict how long an application is used, select an application or a category of applications from the list and click the **Configure rules** link to open the **Application usage restriction** window.

6. If you want to set a time limit on use of an application on weekdays and weekends, in the **Weekdays** and **Weekends** sections, select the **Allow access for no longer than** check box and, in the drop-down list specify the number of hours that the user is allowed to use the application each day. You can also specify the time when the user is allowed / prohibited to use the application, by using a table. To view the table, click the ⬛ button.

7. If you want to set pauses in use of an application, in the **Time breaks** section, select the **Take a break every** check box and, from the drop-down lists, select values for the break frequency and length.

8. Click the **Save** button.

9. In the **Parental Control** window, activate the **Parental Control** switch located next to the user account.

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

CONTROLLING MESSAGING ON SOCIAL NETWORKS

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

➡ *To configure monitoring of a user's messaging:*

1. Go to the Parental Control settings window (see the section "Proceeding to the Parental Control settings" on page 61).

2. In the Parental Control settings window, select the **Communication** section.

3. To view messaging logs and, if necessary, block specified contacts:

   a. Select **Block messaging with all contacts except contacts that are allowed**.

   b. Click the **Known contacts** link to open the **Messaging report** window.

   c. View contacts with whom the user has been messaging. You can display specified contacts in the window by using one of the following methods:

      • To view logs of the user's messaging over a specific social network or an IM client, in the left part of the window, select the required item from the drop-down list.

      • To view contacts with whom the user has been writing most actively, in the drop-down list in the right part of the window, select **By number of messages**.

      • To view contacts with whom the user has been communicating on a specified day, in the drop-down list in the right part of the window, select **By date of messaging**.

   d. To view the user's messaging with a specified contact, click the contact in the list.

      The **Messaging log** window opens.

   e. If you want to block the user's messaging with the selected contact, click the **Block messaging** button.

4. In the **Parental Control** window, activate the **Parental Control** switch located next to the user account.

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

MONITORING MESSAGE CONTENTS

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. Go to the Parental Control settings window (see the section "Proceeding to the Parental Control settings" on page 61).

2. In the Parental Control settings window, select the **Content Control** section.

3. In the **Private data transfer control** section, select the **Block private data transfer to third parties** check box.

4. Click the **Edit list of private data** link to open the **Private data list** window.

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

   A window opens for adding private data.

6. Select a type of private data (for example, "phone number") by clicking the corresponding link or enter a description in the **Field name** field.

7. Specify private data (such as your last name or phone number) in the **Value** field.

8. Click the **Add** button.

    The private data is listed in the **Private data list** window.

9. In the **Parental Control** window, activate the **Parental Control** switch located next to the user account.

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 Keyword Control for messages:*

1. Go to the Parental Control settings window (see the section "Proceeding to the Parental Control settings" on page 61).

2. In the Parental Control settings window, select the **Content Control** section.

3. In the **Keyword Control** section, select the **Enable Keyword Control** check box.

4. Click the **Edit list of key words** link to open the **Keyword Control** window.

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

    A window opens for adding a keyword.

6. Enter a key phrase in the **Value** field and click the **Add** button.

    The specified key phrase appears in the list of keywords in the **Keyword Control** window.

7. In the **Parental Control** window, activate the **Parental Control** switch located next to the user account.

Parental Control will block transmission of messages that contain the specified key phrase, both during messaging over the Internet and in IM clients.

VIEWING THE REPORT ON A USER'S ACTIVITY

You can access reports on the activity of each user account that is controlled by Parental Control, with separate reporting on each category of controlled events.

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

1. Go to the Parental Control settings window (see the section "Proceeding to the Parental Control settings" on page 61).

2. Select a user account and click the **View report** link to go to the reports window.

3. In the section with the relevant type of restriction (for example, **Internet** or **Communication**), open the report on monitored actions by clicking the **Details** link.

The window displays a report on monitored actions of the user.

RESERVING OPERATING SYSTEM RESOURCES FOR COMPUTER GAMES

When Kaspersky Internet Security runs in full-screen mode together with some other applications (particularly computer games), the following issues may occur:

- Application or game performance 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 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. After you exit from full-screen mode, application settings return to the initial values used before full-screen mode was activated.

➡ *To enable Gaming Profile:*

1. Open the main application window.

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

HANDLING UNKNOWN APPLICATIONS

Kaspersky Internet Security helps to minimize the risk associated with using unknown applications (such as the risk of infection with viruses and other malware 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 on your computer.

CHECKING APPLICATION REPUTATION

Kaspersky Internet Security allows you to verify the reputation of applications with users all over the world. The reputation of an application comprises the following criteria:

- Name of the vendor

- Information about the digital signature (if the application is digitally signed)

- Information about the group to which the application has been assigned by Application Control or most users of Kaspersky Security Network

- Number of users of Kaspersky Security Network who use the application (available if the application has been included in the Trusted group in the Kaspersky Security Network database)

- Time at which the application become known to Kaspersky Security Network

- Countries in which the application is the most widespread

Checking of application reputation is available if you have agreed to participate in Kaspersky Security Network.

➡ *To learn 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).
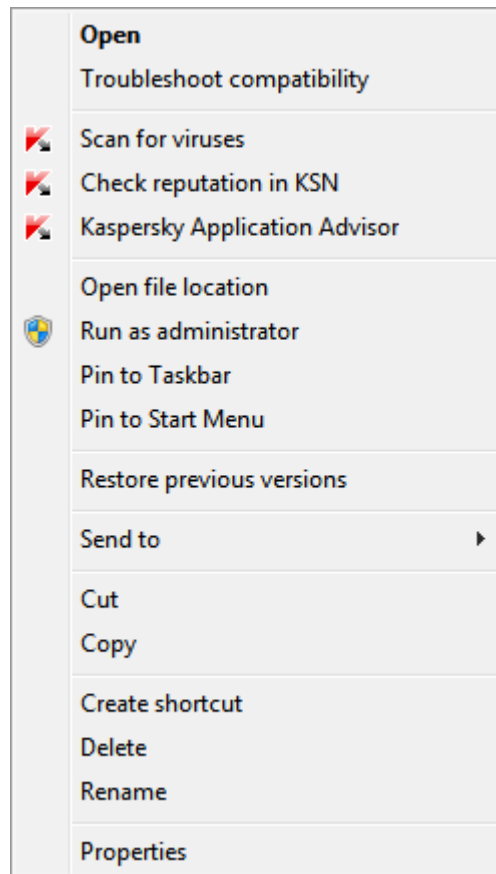
Figure 5. Object context menu

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

CONTROLLING APPLICATION ACTIVITY ON THE COMPUTER AND ON THE NETWORK

Application Control prevents applications from performing actions that may be dangerous for the operating system and controls access to operating system resources and your personal data.

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

On 64-bit operating systems, applications' rights for the following actions cannot be configured:

- 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 objects of the operating system

- Access to password storage

- Debugger rights setup

- Use of program interfaces of the operating system

- Use of program interfaces of the operating system (DNS)

On 64-bit Microsoft Windows 8, applications' rights for the following actions cannot be configured:

- 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 started on the computer for the first time, Application Control checks the safety of the application and assigns it to a group (Trusted, Untrusted, High Restricted, or Low Restricted). The group defines the rules that Kaspersky Internet Security applies for controlling the activity of the application.

Kaspersky Internet Security assigns applications to trust groups (Trusted, Untrusted, High Restricted, or Low Restricted) only if Application Control or Firewall is enabled, and also when both these components are enabled. If both these components are disabled, the functionality that assigns applications to trust groups does not work.

You can edit application control rules manually.

CONFIGURING APPLICATION CONTROL

➡ *To configure Application Control:*

1. Open the main application window of Kaspersky Internet Security.

2. In the lower part of the main window, click the **Show Additional Tools** link. The **Tools** window opens.

3. In the **Tools** window, click the **Application Control** link to open the **Application Control** window.

4. In the **Application Control** window, in the **Applications** section, click the **Manage applications** link to open the **Manage applications** window.

5. In the list, select the relevant application and double-click it to open the **Application rules** window.

    The **Application rules** window opens.

6. Specify application control rules:

   - To configure the rules for access by an application to operating system resources:

     a. On the **Files and system registry** tab, select the relevant resource category.

     b. Right-click the column with an available action for the resource (**Read**, **Write**, **Delete**, or **Create**) to open the context menu. In the context menu, select the relevant item (**Allow**, **Deny**, **Action**, or **Inherit**).

   - To configure the rights of an application to perform various actions in the operating system:

     a. On the **Rights** tab, select the relevant category of rights.

     b. Right-click the **Permission** column to open the context menu. In the context menu, select the relevant item (**Allow**, **Deny**, **Action**, or **Inherit**).

   - 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 **Save**.

     c. Assign a priority to the new rule by clicking the **Up** and **Down** buttons to move it up or down in the list.

   - To exclude certain actions from the restrictions of Application Control, on the **Exclusions** tab, select the check boxes for actions that you do not want to be controlled.

7. Click the **Save** button.

   All exclusions created in the rules for applications are accessible in the Kaspersky Internet Security settings window, in the **Threats and Exclusions** section.

Application Control monitors and restricts the actions of the application in accordance with the specified settings.

ABOUT APPLICATIONS' ACCESS TO THE WEBCAM

Criminals may attempt to obtain unauthorized access to your webcam by means of dedicated software. Kaspersky Internet Security blocks unauthorized access to the webcam and notifies you that access has been blocked. By default, Kaspersky Internet Security blocks access to the webcam for applications that have been included in the High Restricted or Untrusted groups.

You can allow access to the webcam for applications (see the section "Allowing application access to the webcam" on page 73) included in the High Restricted and Untrusted groups, in the Application Control settings window. If an application from the Low Restricted trust group attempts to connect to the webcam, Kaspersky Internet Security displays a notification and prompts you to decide whether to provide that application with access to the webcam.

If a webcam access attempt is made by an application that is denied access by default, Kaspersky Internet Security shows a notification. The notification shows information to the effect that an application installed on the computer (such as Skype™) is currently receiving video data from the webcam. In the notification drop-down list, you can block the application from accessing the webcam or proceed to configure the settings of application access to the webcam (see the section "Configuring the settings of application access to the webcam" on page 72). This notification is not displayed if applications are already running in full-screen mode on your computer.

In the drop-down list of the notification about video data received by the application, you can also choose to **Hide this notification** or proceed to configure notification display settings (see the section "Configuring the settings of application access to the webcam" on page 72).

By default, Kaspersky Internet Security allows webcam access to applications that require your permission if the application's GUI is still being loaded, unloaded, or not responding, and you cannot allow access manually.

Webcam protection has the following features and limitations:

- The application restricts video and still images derived from processing of webcam data.

- Kaspersky Internet Security controls only webcams connected via USB or IEEE1394 that are displayed in Windows Device Manager as Imaging Devices.

To view the list of supported webcams, click this link http://support.kaspersky.com/10978.

> To activate protection against unauthorized access to the webcam, the Application Control component must be enabled.

CONFIGURING THE SETTINGS OF APPLICATION ACCESS TO THE WEBCAM

➡ *To configure the settings of application access to the webcam:*

1. Open the main application window.

2. In the lower part of the main window, click the **Settings** link to open the **Settings** window.

3. In the **Protection** section, in the right part of the window select the **Webcam access** component.

4. Configure the settings of access to the webcam of your computer:

    - To block all applications from accessing the webcam, select the **Block access to webcam for all applications** check box.

    - To receive notifications when the webcam is used by an application that is allowed to do so, select the **Show notification when the webcam is in use by an application for which webcam access is allowed** check box.

    - To allow webcam access for all applications, in the **Settings** window on the **Protection** tab disable **Webcam access**.

ALLOWING APPLICATION ACCESS TO THE WEBCAM

➡ *To allow an application to access the webcam:*

1. Open the main application window.

2. In the lower part of the main window, click the **Show Additional Tools** link. The **Tools** window opens.

3. In the **Tools** window, click the **Application Control** link to open the **Application Control** window.

4. In the **Application Control** window, in the **Applications** section, click the **Manage applications** link to open the **Manage applications** window.

5. In the list, select the application for which you want to allow webcam access. Double-click the application to open the **Application rules** window.

6. In the **Application rules** window, go to the **Rights** tab.

7. In the list of rights categories, select **System modification** → **Suspicious system modifications** → **Access webcam**.

8. Right-click the **Permission** column to open the context menu and select **Allow**.

9. Click the **Save** button.

The selected application will be allowed access to the webcam.

TRUSTED APPLICATIONS MODE

This section provides information about Trusted Applications mode.

ABOUT TRUSTED APPLICATIONS MODE

In Kaspersky Internet Security, you can create on your computer a secure environment, called Trusted Applications mode, in which only trusted applications are allowed to start. Trusted Applications mode is useful if you use a stable set of well-known applications and you do not need to frequently run new unknown applications downloaded from the Internet. When running in Trusted Applications mode, Kaspersky Internet Security blocks all applications that have not been classified as trusted by Kaspersky Lab. The decision on whether to trust an application can be made based on information received from Kaspersky Security Network, details of the application's digital signature, and the trust level of the installer and the source of the application download.

Trusted Applications mode has the following features and limitations:

- 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.

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

- 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 depends on your region and service provider. If you need Trusted Applications mode, you are recommended to ask for it when purchasing the application.

- If Trusted Applications mode is supported in your version of Kaspersky Internet Security but is not currently available, it may become available after you update the databases and application software modules (see the section "Updating databases and application software modules" on page 36). After the databases and application software modules are updated, you can configure the run mode for unknown applications and modules.

Before enabling Trusted Applications mode, Kaspersky Internet Security analyzes your operating system and the applications installed on your computer. Analysis may take a long time (up to a few hours). If the analysis detects software that cannot be classified as trusted, you are not advised to enable Trusted Applications mode. When Trusted Applications mode is enabled, Kaspersky Internet Security may block applications that have not been recognized as trusted. You can allow such applications to be run (see the section "Controlling application activity on the computer and on the network" on page 69) if you use any, and then enable Trusted Applications mode.

Kaspersky Internet Security can perform analysis of the operating system and installed applications automatically in the background. If the analysis performed by Kaspersky Internet Security has shown that mainly trusted applications are used on the computer, Trusted Applications mode may be enabled automatically.

ENABLING TRUSTED APPLICATIONS MODE

➡ *To enable Trusted Applications mode:*

1. Open the main application window.

2. In the lower part of the main window, click the **Show Additional Tools** link. The **Tools** window opens.

3. In the **Tools** window, click the **Application Control** link to open the **Application Control** window.

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

   If required protection components are disabled, a window opens, providing information about protection components that must be enabled before you can enable Trusted Applications mode.

5. Click the **Continue** button.

   This runs analysis of the operating system and installed applications, except for temporary files and resource dynamic link libraries that contain executable code. The progress of the analysis is displayed in the **Analysis of installed applications** window that opens.

   Wait until the analysis of the operating system and installed applications completes. You can minimize the **Analysis of installed applications** window. Analysis is then performed in background mode. You can view the progress of the analysis by clicking the **Analysis of installed applications (<N> %)** link in the **Application Control** window.

6. View information about the results of the analysis in the **Analysis of installed applications and executable files 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 are detected for which Kaspersky Internet Security does not have enough information to classify them as completely safe.

   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 use of Trusted Applications mode, by clicking the **Do not enable Trusted Applications mode** button.

7. If you want to allow running untrusted applications and system files, in the **Analysis of installed applications and executable files is complete** window, click the **Allow running unknown system files and continue** link.

8. Click the **Enable Trusted Applications mode by default** button.

Trusted Applications mode is now enabled. Kaspersky Internet Security will block all applications and system files that have not been classified as trusted. The application then proceeds to the **Application Control** window.

After you enable Trusted Applications mode and restart the operating system for the first time, unknown applications are allowed to start until Kaspersky Internet Security starts. After later restarts of the operating system, Kaspersky Internet Security blocks unknown applications from starting.

DISABLING TRUSTED APPLICATIONS MODE

➡ *To disable Trusted Applications mode:*

1. Open the main application window.

2. In the lower part of the main window, click the **Show Additional Tools** link. The **Tools** window opens.

3. In the **Tools** window, click the **Application Control** link to open the **Application Control** window.

4. 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.

PASSWORD-PROTECTING ACCESS TO KASPERSKY INTERNET SECURITY MANAGEMENT OPTIONS

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 an administrator password and specify the actions for which this password must be entered:

- Configuring the application settings.

- Quitting the application.

- Removing the application.

➡ *To password-protect access to control over Kaspersky Internet Security:*

1. Open the main application window.

2. In the lower part of the main window, click the **Settings** link 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. In the **Password scope** group of settings, specify the application actions to which you want to restrict access.

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

PAUSING AND RESUMING COMPUTER PROTECTION

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

When protection is paused or Kaspersky Internet Security is not running, the activity of the applications running on your computer is monitored. Information about the results of monitoring of application activity is saved in the operating system. When Kaspersky Internet Security is started again or protection is resumed, Kaspersky Internet Security uses this information to protect your computer from malicious actions that may have been performed when protection was paused or when Kaspersky Total Security was not running. Information about the results of monitoring of application activity is stored indefinitely. This information is deleted if Kaspersky Internet Security is removed from your computer.

➡ *To pause the protection of your computer:*

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

   The **Pause protection** window opens (see the following figure).
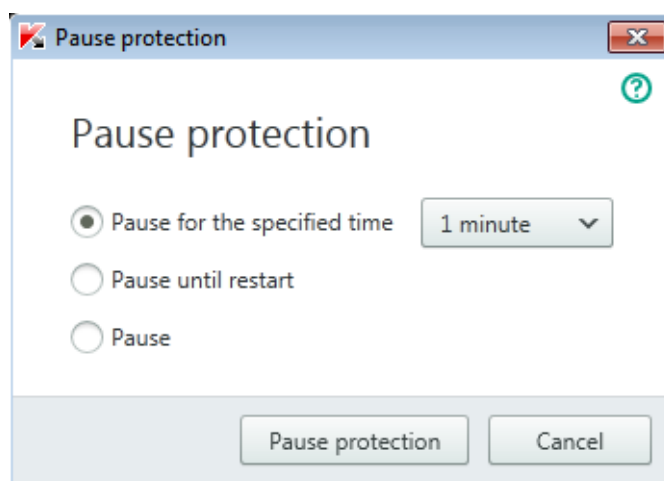
Figure 6. Pause protection window

2. In the **Pause protection** window, select the time interval after which protection will be resumed:

   - **Pause for the specified time** – protection is enabled after expiration of the time interval selected from the drop-down list.

   - **Pause until restart** – protection is enabled after the application is started again or the operating system is restarted (if the application automatically starts on startup).

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

➡ *To resume computer protection:*

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

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 Application Configuration 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, in the **Manage Settings** drop-down list, select **Restore settings**.

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 are also shown in the window (see the following figure).
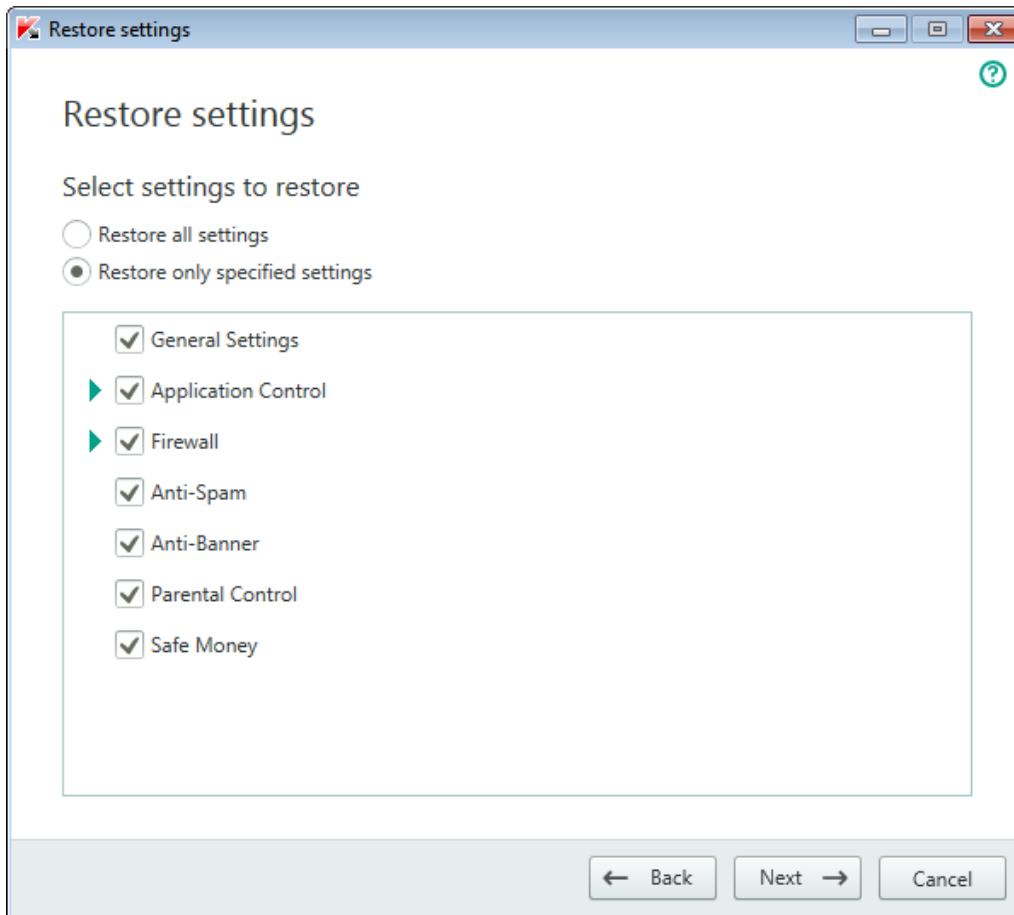
Figure 7. Restore settings window

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 to 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. Operating system analysis

At this stage, information about Microsoft Windows applications is searched for. These applications are added to the list of trusted applications. No restrictions are placed on the actions that trusted applications perform in the operating 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 OPERATION REPORT

Kaspersky Internet Security maintains operation reports for each of the protection components. Using a report, you can obtain statistical information about the application's operation (for example, how many malicious objects have been detected and neutralized during a specified time period, how many times the application has been updated during the same period, how many spam messages have been detected, and much more). Reports are kept in encrypted format.

➡ *To view the application operation report:*

1. Open the main application window.

2. In the lower part of the main window, click the **Show Additional Tools** link. The **Tools** window opens.

3. In the **Tools** window, click the **Report** link to open the **Reports** window.

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

4. If you want to view a detailed report on application operation, in the upper part of the **Reports** window, click the **Detailed reports** link. The **Detailed Reports** window opens.

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

APPLYING THE APPLICATION SETTINGS ON ANOTHER COMPUTER

After you have configured the application, you can apply its settings to a copy of Kaspersky Internet Security that is installed on another computer. As a result, the application will be configured identically on both computers.

The application settings are saved in a configuration file that you can move from one computer to another.

The settings of Kaspersky Internet Security are moved from one computer to another in three steps:

1. Save the application settings to configuration file.

2. Move the configuration file to the other computer (for example, by email or on a removable disk).

3. Import the settings from the configuration file to the application copy that is installed on the other computer.

➡ *To export the application settings:*

1. Open the main application window.

2. In the lower part of the window, click the **Settings** link to open the **Settings** window.

3. In the **Settings** window, select the **General** section.

4. In the **Manage Settings** drop-down list, select **Export settings**.

   The **Save as** window opens.

5. Specify a name for the configuration file and click the **Save** button.

   The application settings are now saved in the configuration file.

You can also export the application settings at the command prompt, by using the following command: `avp.com EXPORT <file_name>`.

➡ *To import settings into a copy of the application installed on another computer:*

1. On the other computer, open the main application window of Kaspersky Internet Security.

2. In the lower part of the window, click the **Settings** link to open the **Settings** window.

3. In the **Settings** window, select the **General** section.

4. In the **Manage Settings** drop-down list, select **Import settings**.

   The **Open** window opens.

5. Specify a configuration file and click the **Open** button.

   The settings are imported to the application that is installed on the other computer.

PARTICIPATING IN KASPERSKY SECURITY NETWORK (KSN)

Kaspersky Internet Security uses cloud protection to make protection of your computer more effective. Cloud protection is implemented using the Kaspersky Security Network infrastructure that uses data received from users all over the world.

Kaspersky Security Network (KSN) is an infrastructure of online services that provides access to the Kaspersky Lab database with constantly updated 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 likelihood of false positives.

Users' participation in Kaspersky Security Network allows Kaspersky Lab to promptly receive 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.

If you participate in Kaspersky Security Network, you automatically send information about the configuration of your operating system and the start and completion time of processes in Kaspersky Internet Security to Kaspersky Lab (see the section "About data provision" on page 31).

IN THIS SECTION

ENABLING AND DISABLING PARTICIPATION IN KASPERSKY SECURITY NETWORK

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

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

1. Open the main application window.

2. In the lower part of the main window, click the **Settings** link 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 clicking 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

Your 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 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. In the lower part of the main window, click the **Settings** link to open the **Settings** window.

3. In the **Additional** section, select the **Feedback** subsection.

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

PARTICIPATING IN THE PROTECT A FRIEND PROGRAM

With the Protect a Friend program, you can publish a download link on Twitter and on your page in social networks. This link allows your friends to download an installation package for Kaspersky Internet Security with an extended evaluation period. When one of your friends on Twitter or on a social network downloads the Kaspersky Internet Security installation package by clicking the link that you have published and then activates the application, you receive bonus points. You can exchange your bonus points for a bonus activation code for Kaspersky Internet Security.

Note that the option to participate in the Protect a Friend program may not be available to all users.

The number of bonus points depends on the application version.

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

To log in to your profile for the Protect a Friend program, you must first log in through your My Kaspersky account. If you do not have a My Kaspersky account yet, you can create one when you open your Protect a Friend profile for the first time.

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

- View the number of collected bonus points.

- Publish links for downloading the Kaspersky Internet Security installation package.

- Edit your profile (the user picture and name that are shown on Twitter, social networks, and your blog, together with a link for downloading the Kaspersky Internet Security installation package).

After you switch from Kaspersky Internet Security to Kaspersky Total Security, you can continue participation in the Protect a Friend program. In this case, you share with friends a link for downloading the installation package of Kaspersky Internet Security. After you switch to Kaspersky Total Security, your history of participation in the Protect a Friend program and collected bonus points are saved, and you can exchange points for a bonus activation code for Kaspersky Internet Security. During the next installation of Kaspersky Total Security or upgrade to a newer version of Kaspersky Total Security, participation in the Protect a Friend program is terminated.

IN THIS SECTION

LOGGING IN TO YOUR PROTECT A FRIEND PROFILE

To log in to your profile in the Protect a Friend program, you must first log in through your My Kaspersky account. If you do not have a My Kaspersky account yet, create one when you visit the web page of the Protect a Friend program for the first time.

Your My Kaspersky account is your email address and the password (at least eight characters) that you specified when signing up.

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

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

➡ *To create your My Kaspersky account:*

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

   The Protect a Friend web page opens, containing fields for signing up or logging in to your My Kaspersky account.

2. Create and activate your My Kaspersky account:

   a. On 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 must contain at least eight characters.

   c. Click the **Register** button.

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

   d. Click the link to activate your My Kaspersky account.

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

If you already have a My Kaspersky account, you can use it to log in to the web page that contains your profile.

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

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

   The Protect a Friend web page opens, containing fields for signing up or logging in to your My Kaspersky account.

2. On the right part of the web page, fill in the fields by entering the email address and the password that you specified during registration of your My Kaspersky account.

3. Click the **Log in** button.

   The web page displays your Protect a Friend profile.

SHARING A LINK TO KASPERSKY INTERNET SECURITY WITH FRIENDS

When logged in to the web page with your profile for the Protect a Friend program, you can publish a link for downloading the Kaspersky Internet Security installation package on Twitter as well as on social networks. You can also share details from your Protect a Friend profile with a link to the installation package, by pasting them on your website or blog. In addition, you can send a link for downloading the Kaspersky Internet Security installation package by email or by instant messengers (such as ICQ).

➡️ *To publish a link for downloading the Kaspersky Internet Security installation package on Twitter or on social networks:*

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

   The web page for signing in to the Protect a Friend program opens.

2. Sign in on the web page with your My Kaspersky account.

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

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

The website of the selected social network or Twitter opens. A link for downloading the installation package of Kaspersky Internet Security with an 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 social network or Twitter page, the sign-in page opens.

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

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

   The web page for signing in to the Protect a Friend program opens.

2. Sign in on the web page with your My Kaspersky account.

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

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

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

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

➡️ *To get a link for downloading the installation package of Kaspersky Internet Security to send by email or by instant messaging:*

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

   The web page for signing in to the Protect a Friend program opens.

2. Sign in on the web page with your My Kaspersky account.

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

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

   The **Link to installer package** window opens, displaying a link for downloading the Kaspersky Internet Security installation package.

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 the 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 download Kaspersky Internet Security from the link that you have shared in your profile and activate the application.

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 activates Kaspersky Internet Security.

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

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

A bonus activation code can be used to activate the application on another computer (for example, you can give it as a present to another user).

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

- The application is in use by subscription. In this case, you can use the bonus activation code when the subscription expires. You can also 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, in the lower part of the window, click the **My Kaspersky** link.

   The web page with your Protect a Friend profile opens.

2. Sign in on the web page with your My Kaspersky account.

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

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

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 about verification of the activation code. After the activation code is verified, a window opens, showing a message about successful activation of Kaspersky Internet Security.

➡ *To view the history of provided bonus activation codes and activate the application with a previously provided bonus activation code:*

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

    The web page with your Protect a Friend profile opens.

2. Sign in on the web page with your My Kaspersky account.

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

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

    The **Bonus points** window opens, with the **Bonus activation codes** tab displayed.

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 about verification of the activation code. After the activation code is verified, a window opens, showing a message about successful activation of Kaspersky Internet Security.

USING THE APPLICATION FROM THE COMMAND PROMPT

You can use Kaspersky Internet Security at the command prompt.

Command prompt syntax:

```
avp.com <command> [settings]
```

To view help on the command prompt syntax, enter the following command:

```
avp.com [ /? | HELP ]
```

This command allows you to obtain a full list of commands that are available for managing Kaspersky Internet Security through the command prompt.

To obtain help on the syntax of a specific command, you can enter one of the following commands:

```
avp.com <command> /?
avp.com HELP <command>
```

At the command prompt, you can refer to the application either from the application installation folder or by specifying the full path to avp.com.

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

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 11), 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.

- Send request from My Kaspersky portal. This method allows you to contact our specialists using the query form.

Technical support is available only to users who have purchased a license for use of the application. 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.

GETTING TECHNICAL SUPPORT ON MY KASPERSKY PORTAL

My Kaspersky (https://my.kaspersky.com) is a service designed for sending requests to Technical Support and managing the activation codes for Kaspersky Lab applications.

To obtain access to My Kaspersky portal, register on the registration page (https://my.kaspersky.com). Enter your email address and password to log in to My Kaspersky portal.

You can do the following on My Kaspersky portal:

- 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 your key file if it has been 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 will send an answer to your question via My Kaspersky portal 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 examination of suspicious files and web resources to the Virus Lab. You can also contact the Virus Lab if Kaspersky Internet Security generates a false positive with regard to files and web resources that you do not consider to be dangerous.

COLLECTING INFORMATION FOR TECHNICAL SUPPORT

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.

To provide better support on issues related to functioning of the application, Technical Support specialists may ask you to temporarily change application settings for debugging purposes while diagnostics are ongoing. To do so, you may need to perform the following actions:

- Activate collection of extended diagnostic information.

- Configure individual components of the application by changing special settings that are not accessible through the standard user interface.

- Reconfigure storage and sending of collected diagnostic information.

- Set up interception of network traffic and saving of network traffic to a file.

Technical Support specialists will give you all information necessary for performing these actions (step-by-step instructions, settings to be changed, scripts, additional command line features, debugging modules, special utilities, etc.) and will inform you of what data will be collected for debugging purposes. After the extended diagnostic information is collected, it is saved on the user's computer. The collected data is not sent automatically to Kaspersky Lab.

You are advised to perform the preceding actions only under the guidance of a Technical Support specialist after receiving instructions to do so. Changing application settings by yourself in ways not described in the Administrator's Guide or recommended by Technical Support specialists can cause slowdowns and crashes of the operating system, reduce the protection level of your computer, and damage the availability and integrity of the processed information.

IN THIS SECTION

CREATING A SYSTEM STATE REPORT

➡ *To create a system state report:*

1. Open the main application window.

2. In the lower part of the window, click the **Support** link 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 operating system state report** link.

The system state report is created in HTML and XML formats and is saved in the archive sysinfo.zip. When the information about the operating system is fully retrieved, you can view the report.

➡ *To view the report:*

1. Open the main application window.

2. In the lower part of the window, click the **Support** link 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.

   A Microsoft Windows Explorer window opens.

5. In the window that opens, open the archive named sysinfo.zip, which contains the 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 on My Kaspersky portal when you have an active request.

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

1. Open the main application window.

2. In the lower part of the window, click the **Support** link 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 portal.

➡ *To save data files to disk:*

1. Open the main application window.

2. In the lower part of the window, click the **Support** link 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 types of data that you want to send:

   - **Operating system information**. Select this check box to send information about the operating system on your computer to Technical Support.

   - **Data collected for analysis**. Select this check box to send application trace files to Technical Support. Click the **<number of files>, <data volume>** link to open the **Data collected for analysis** window. Select check boxes opposite the trace files that you want to send.

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 portal.

CONTENTS AND STORAGE OF TRACE FILES

Trace files are stored on the computer as long as the application is in use and are deleted permanently when the application is removed.

Trace files are stored in the ProgramData\Kaspersky Lab folder.

The format of trace file names is as follows: `KAV<version number_dateXX.XX_timeXX.XX_pidXXX.><trace file type>.log.enc1`.

All trace files contain the following common data:

- Event time.

- Number of the thread of execution.

- Application component that caused the event.

- Degree of event severity (informational event, warning, critical event, error).

- A description of the event involving command execution by a component of the application and the result of execution of this command.

Contents of SRV.log, GUI.log, and ALL.log trace files

SRV.log and GUI.log trace files may store the following information:

- Personal data, including the last name, first name, and patronymic, if such data is included in the path to files on a local computer.

- The user name and password if they were transmitted openly. This data can be recorded in trace files during Internet traffic scanning. Traffic is recorded in trace files only from trafmon2.ppl.

- The user name and password and cookie files if they are contained in HTTP headers.

- The name of the Microsoft Windows account if the account name is included in a file name.

- Your email address or a web address containing the name of your account and password if they are contained in the name of the object detected.

- Websites that you visit and redirects from these websites. This data is written to trace files when the application scans websites.

- Proxy server address, computer name, port, IP address, and user name used to sign in to the proxy server. This data is written to trace files if the application uses a proxy server.

- Remote IP addresses to which your computer established connections.

- Message subject, ID, sender's name and address of the message sender's web page on a social network. This data is written to trace files if the Parental Control component is enabled.

- Information about activation of the application, which may include the current and previous activation codes, localization of the application, IDs of the application, product, or customization, application version, unique ID generated for each unique installation of the operating system, ID of the user's computer, date and time (UTC) on the user's computer at the time of activation.

Contents of HST.log, BL.log, and Dumpwriter.log trace files

The HST trace file contains information about database and application module updates.

The BL trace file contains information about events occurring during operation of the application, as well as data required to troubleshoot application errors. This file is created if the application is started with the avp.exe –bl parameter. The BL file can also contain information about activation of the application, which may include the current and previous activation codes, localization of the application, IDs of the application, product, or customization, application version, unique ID generated for each unique installation of the operating system, ID of the user's computer, date and time (UTC) on the user's computer at the time of activation.

The dumpwriter.log trace file contains service information required for troubleshooting errors that occur when the application memory dump is written.

Contents of trace files of application plug-ins

Trace files of application plug-ins contain the following information:

- VirtualKeyboard (VKB.log) contains service information about operation of the plug-in and data required for troubleshooting plug-in errors.

- Online Banking (OB.log) contains service information about plug-in operation, including information about website scanning events and scan results, connections to remote IP addresses and proxy server settings, and cookies. The file also contains data required for troubleshooting plug-in errors.

- ContentBlocker (CB.log) contains service information about plug-in operation, including information about web address scanning events and scan results, connections to remote IP addresses, and proxy server settings. The file also contains data required for troubleshooting plug-in errors.

- Office Anti-Virus (OA.log) contains information about scanning of Microsoft Office documents. This file may also contain information about the full path to a document or address of the website from which this document was downloaded.

- Trace file of the plug-in for starting a scan task from a context menu (shellex.dll.log). Contains information about execution of a scan task and data required for troubleshooting plug-in errors.

- Trace files of the Microsoft Outlook® plug-in:

  - mcouas.OUTLOOK.EXE. Anti-Spam plug-in

  - mcou.OUTLOOK.EXE. Mail Anti-Virus plug-in.

  Files can contain portions of email messages, including addresses.

- Trace file of the plug-in for registering a Google Chrome extension (NativeMessagingHost.log). Contains service information about operation of the plug-in.

RUNNING AVZ SCRIPTS

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.

➡ *To run an AVZ script:*

1. Open the main application window.

2. In the lower part of the window, click the **Support** link 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 **Run script** 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 **Run** button.

    The script runs.

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

LIMITATIONS AND WARNINGS

Kaspersky Internet Security has a number of limitations that are not critical to operation of the application.

Limitations on upgrades from a previous version of the application

- During an upgrade of a previous version of Kaspersky Internet Security, the following application settings are reset to their default values: update sources, the list of trusted URLs, and the settings of Kaspersky URL Advisor.

- When a new version of Kaspersky Internet Security is installed over Kaspersky Internet Security 2011 and earlier, backup copies of files and quarantined objects are lost because their format is not supported and cannot be converted to the new format. During an upgrade from Kaspersky Internet Security 2012, the backup copies of files and quarantined objects can be converted to the new format. The backup storage in Kaspersky Internet Security 2013 or later format is supported and does not require converting to the new format.

Limitations on the operation of certain components and automatic processing of files

Infected files are processed automatically according to rules created by Kaspersky Lab specialists. You cannot modify these rules manually. Rules can be updated following an update of databases and application modules. Firewall, Application Control, and Trusted Applications mode rules are also updated automatically.

Website certificate check and file scan limitations

When checking a website certificate or scanning website files, the application may contact Kaspersky Security Network for information. If data from Kaspersky Security Network could not be retrieved, the application decides whether or not the file is infected and the certificate untrusted based on local anti-virus databases.

Limitations of System Watcher functionality

Protection against cryptors (malware that encrypts user files) has the following limitations:

- The Temp system folder is used to support this functionality. If the system drive with the Temp folder has insufficient disk space to create temporary files, protection against cryptors is not provided. In this case, the application does not display a notification that files are not backed up (protection is not provided).

- Temporary files are deleted automatically when you close Kaspersky Internet Security or disable the System Watcher component.

- In case of an emergency termination of Kaspersky Internet Security, temporary files are not deleted automatically. To delete temporary files, clear the Temp folder manually. To do so, open the **Run** window (**Run** command under Windows XP) and in the **Open** field type `%TEMP%`. Click **OK**.

Warning about diagnostic information collected

Diagnostic information about the operation of the application, which you collect for Technical Support, is encrypted while it is being collected. If necessary, you can disable encryption.

Limitations of Secure connections functionality

Due to technical limitations of the implementation of scanning algorithms, scanning of secure connections does not support certain extensions of the TLS 1.0 protocol and later versions (particularly NPN and ALPN). Connections via these protocols may be limited. Web browsers with SPDY protocol support use the HTTP over TLS protocol instead of SPDY even if the server to which the connection is established supports SPDY. This does not affect the level of connection security.

Warning about operation of the Anti-Spam component

Anti-Spam functionality can be configured by editing the settings file for the Anti-Spam component.

Specifics of kernel memory scanning for rootkits in Protected Browser mode

When an untrusted module is detected in Protected Browser mode, a new browser tab opens with a notification about malware detection. If this happens, you are recommended to exit the browser and run a Full Scan of the computer.

Specifics of clipboard data protection

Kaspersky Internet Security allows an application to access clipboard in the following cases:

- An application with the active window attempts to place data in clipboard. The active window is the window that you are currently using.

- A trusted process of an application attempts to place data in clipboard.

- A trusted process of an application or a process with the active window attempts to receive data from clipboard.

- A an application process that previously placed data in clipboard attempts to receive this data from clipboard.

Warning about compatibility with Kaspersky Lab applications

Kaspersky Internet Security is compatible with the following Kaspersky Lab applications:

- Kaspersky Fraud Prevention 2.0

- Kaspersky Fraud Prevention 2.5

- Kaspersky Fraud Prevention 3.0

- Kaspersky Fraud Prevention 3.5

- Kaspersky Password Manager 2.0

- Kaspersky Password Manager 5.0

- Kaspersky Password Manager 7.0

Specifics of processing of malicious objects by application components

By default, the application can delete files that cannot be disinfected. Removal by default can be performed during file processing by such components as Application Control, Mail Anti-Virus, File Anti-Virus, during scan tasks, and also when System Watcher detects malicious activity of applications.

Limitations applicable to certain components in case of application installation together with Kaspersky Fraud Prevention for Endpoint

Operation of the following Kaspersky Internet Security components is limited in Protected Browser if the application is installed together with Kaspersky Fraud Prevention for Endpoint:

- Web Anti-Virus, except Anti-Phishing

- Parental Control

- Kaspersky URL Advisor

- Anti-Banner

Kaspersky Internet Security limitations under Microsoft Windows 10

The following functionality is unavailable in the application installed on the Microsoft Windows 10 operating system:

- Protection against screenshots

- Clipboard data protection

- Webcam access protection

- Advanced Disinfection

The following application functionality is also partly limited under Microsoft Windows 10:

- Self-Defense. Self-Defense of the application GUI does not work even when it is enabled.

- System Watcher

- Protection against cryptors and screen lockers. The application can detect only the most basic varieties of cryptors and screen lockers.

- Application Control. Custom application rules do not work. Application categorization in the new Windows user interface style is performed incorrectly.

GLOSSARY

A

ACTIVATING THE APPLICATION

Switching the application to fully functional mode. Application activation is performed by the user during or after installation of the application. To activate the application, the user must have an activation code .

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.

ANTI-VIRUS DATABASES

Databases that contain information about computer security threats known to Kaspersky Lab as of when the anti-virus databases are released. Entries in anti-virus databases allow detecting malicious code in scanned objects. Anti-virus databases are created by Kaspersky Lab specialists and updated hourly.

APPLICATION MODULES

Files included in the Kaspersky Lab installation package that are responsible for performing the main tasks of the corresponding application. A particular application module corresponds to each type of task performed by the application (protection, scan, updates of databases and application modules).

B

BLOCKING AN OBJECT

Denying access to an object from third-party 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 on social networks or pastes the link in an email message, and the user's friend then downloads the application installation package via this link and activates the application.

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. Created by Kaspersky Lab specialists, the list is regularly updated and is included in the Kaspersky Lab application package.

DATABASE OF PHISHING WEB ADDRESSES

List of web addresses which have been defined as phishing addresses by Kaspersky Lab specialists. The databases are regularly updated and are part of the Kaspersky Lab application package.

DIGITAL SIGNATURE

An encrypted block of data embedded in a document or application. A digital signature is used to identify the author of the document or application. 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 special area on a computer's hard drive, floppy disk, or other data storage device. It contains information on the disk's file system and a boot loader program, which 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 boot sectors for viruses and disinfecting them if an infection is found.

F

FALSE POSITIVE

A situation when a Kaspersky Lab application considers a non-infected object to be infected because the object's 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 about which information has not yet been added to Kaspersky Lab databases. The heuristic analyzer detects objects whose behavior in the operating system may pose a security threat. Objects detected by the heuristic analyzer are considered to be 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).

HYPERVISOR

An application supporting the parallel operation of several operating systems on one computer.

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. Next time, the application will skip this archive unless the archive 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 to check whether the file has been modified since it was last scanned.

- The technology supports a limited number of formats.

INCOMPATIBLE APPLICATION

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

INFECTED OBJECT

An object of which a portion of its code completely matches part of the code of known malware. Kaspersky Lab does not recommend accessing such objects.

K

KASPERSKY LAB UPDATE SERVERS

Kaspersky Lab HTTP servers from which updates of databases and software modules are downloaded.

KASPERSKY SECURITY NETWORK (KSN)

An infrastructure of online services that provides access to the Kaspersky Lab database with constantly updated information about the reputation of files, web resources, and software. Use of data from Kaspersky Security Network ensures faster responses by Kaspersky Lab applications to new threats, improves the performance of some protection components, and reduces the likelihood of false positives.

KEYLOGGER

A program designed for hidden logging of information about keys pressed by the user. Keyloggers function as keystroke interceptors.

L

LICENSE TERM

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

P

PHISHING

A type of Internet fraud aimed at obtaining unauthorized access to users' confidential data.

PROBABLE SPAM

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

PROBABLY INFECTED OBJECT

An object whose code contains portions of modified code from a known threat, or an object whose behavior is similar to that of a threat.

PROTECTED BROWSER

A dedicated operation mode of a standard web browser designed for financial activities and online shopping. Using Protected Browser ensures safety of confidential data that you enter on the websites of banks and payment systems (such as banking card numbers or passwords for access to online banking services); it also prevents theft of assets when making money transfers online. Meanwhile, the standard browser used for accessing the website displays a message informing you that Protected Browser is being started.

P ROTECTION COMPONENTS

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

P ROTOCOL

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

Q UARANTINE

A dedicated storage in 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 that is not dangerous for the computer.

R

R OOTKIT

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 refers to a program that penetrates the operating system and intercepts system functions (Windows APIs). Interception and modification of low-level API functions are the main methods that allow these programs to make their 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

S CRIPT

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 some websites.

If real-time protection is enabled, the application tracks the execution 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.

S ECURITY LEVEL

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

S PAM

Unsolicited mass email mailings, most often including advertising messages.

S TARTUP 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

T ASK

The functions of the Kaspersky Lab application are implemented in the form of tasks, such as: Full Scan task or Update task.

TASK SETTINGS

Application settings that are specific for each task type.

THREAT LEVEL

An index showing the probability that an application poses 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 system calls)

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

Real-time scanning that uses information from the current (latest) version of the databases for objects transferred over all protocols (for example, HTTP, FTP, and other protocols).

TRUST GROUP

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

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

TRUSTED PROCESS

A software process whose file operations are not restricted by the Kaspersky Lab application in real-time protection mode. When suspicious activity is detected in a trusted process, Kaspersky Internet Security removes the process from the list of trusted processes and blocks its actions.

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 by using the heuristic analyzer. These 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 designed for updating databases and application modules. The Kaspersky Lab application copies update packages from Kaspersky Lab 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 number of collected bonus points, a link to the page for downloading Kaspersky Internet Security, and bonus activation codes granted to the user.

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 identifying 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 the operating system or application and corrupt its integrity. Presence of a large number of vulnerabilities in an operating system makes it unreliable, because viruses that penetrate the operating system may cause disruptions in the operating 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 operations 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 2,000 highly skilled professionals.

PRODUCTS. Kaspersky Lab's products provide protection for all systems, from home computers to large corporate networks.

The personal product range includes anti-virus software for all the devices used in digital life today, spanning desktop, laptop, and tablet computers, 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 major test laboratories, compatible with software from diverse vendors, and 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 *is updated* every five minutes.

TECHNOLOGIES. Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky Lab. This is one of the reasons why many third-party software developers have chosen to use the Kaspersky Anti-Virus engine 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), Openwave Messaging (Ireland), D-Link (Taiwan), M86 Security (USA), GFI Software (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), Netasq+Arkoon (France), NETGEAR (USA), Parallels (USA), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Taiwan). Many of the company's innovative technologies are patented.

ACHIEVEMENTS. Over the years, Kaspersky Lab has won hundreds of awards for its services in combating computer threats. For example, in 2010 Kaspersky Anti-Virus 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 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)
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, Google Chrome, and YouTube are Trademarks of Google, Inc.

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

Intel, Celeron, and Atom are Trademarks of Intel Corporation in the U.S. and/or other countries.

Bing, Internet Explorer, Microsoft, Windows, Windows Vista, and Outlook are registered trademarks of Microsoft Corporation in the United States and other countries.

Mail.ru is a Trademark of Mail.ru LLC.

Mozilla and Firefox are Trademarks of the Mozilla Foundation.

Skype is a trademark of Skype.

VMware is a trademark of VMware, Inc., or trademark of VMware, Inc. registered in the USA or in other jurisdictions.

INDEX

U

V

W