Kaspersky Anti-Virus

User Guide

APPLICATION VERSION: 15.0

Dear User,

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

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

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

This document, and graphic images related to it, may only be used for informational, non-commercial, and personal purposes.

Kaspersky Lab reserves the right to amend this document without additional notification. You can find the latest version of this document on the Kaspersky Lab website, at http://www.kaspersky.com/docs.

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

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

Document revision date: 4/8/2014

© 2014 Kaspersky Lab ZAO. All Rights Reserved.

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

TABLE OF CONTENTS

ABOUT THIS GUIDE

This document is the User Guide for Kaspersky Anti-Virus.

For proper use of Kaspersky Anti-Virus, 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 Anti-Virus.

- Provide a way to quickly find information on issues related to Kaspersky Anti-Virus.

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

IN THIS GUIDE

This document contains the following sections:

Sources of information about the application

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

Kaspersky Anti-Virus

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

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

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, ways of activating the application, and license renewal.

Managing application notifications

This section provides information about how to manage application notifications.

Assessing computer protection status and resolving security issues

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

Update databases and program modules

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

Scanning the computer

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

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

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

Configuring Mail Anti-Virus

This section contains step-by-step instructions on how to configure Mail Anti-Virus.

Protecting private data on the Internet

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

Removing traces of activity on the computer and on the Internet

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

Reserving operating system resources for computer games

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

Password-protecting access to control over Kaspersky Anti-Virus

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

Pausing and resuming computer protection

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

Restoring the default application settings

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

Viewing the application operation report

This section contains step-by-step instructions on how to view application reports.

Applying the application settings on another computer

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

Participating in Kaspersky Security Network

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

Participating in the Protect a Friend program

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

Switching from Kaspersky Anti-Virus to Kaspersky Internet Security

This section contains step-by-step instructions on how to switch to using Kaspersky Internet Security.

Using the application from the command prompt

This section provides information about how to use the application at the command prompt.

Contacting Technical Support

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

Glossary

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

Kaspersky Lab ZAO

This section provides information about Kaspersky Lab.

Information about third-party code

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

Trademark notices

This section lists trademarks of third-party manufacturers that 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.

IN THIS SECTION

SOURCES OF INFORMATION FOR INDEPENDENT RESEARCH

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

- Application page on the Kaspersky Lab website

- Application page on the Technical Support website (Knowledge Base)

- Online help

- Documentation

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

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/anti-virus), 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/kav2015), 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 Anti-Virus 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.

CONTACTING THE SALES DEPARTMENT

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

- By calling our central office in Moscow by phone (http://www.kaspersky.com/contacts).

- By sending a message with your question to sales@kaspersky.com.

Service is provided in English and in Russian.

CONTACTING THE TECHNICAL WRITING AND LOCALIZATION UNIT BY EMAIL

To contact the Technical Writing and Localization Unit, send an email to docfeedback@kaspersky.com. Please use "Kaspersky Help Feedback: Kaspersky Anti-Virus 15.0" as the subject line of your message.

KASPERSKY ANTI-VIRUS

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.

IN THIS SECTION

WHAT'S NEW

Kaspersky Anti-Virus provides the following new features:

- Functioning of the System Watcher component has been improved: protection against cryptors has been implemented. Kaspersky Anti-Virus creates backup copies of files before they are encrypted by a malicious cryptor. This allows restoring those files from their backup copies. Backup copies of files are stored in the system folder for temporary files (Temp).

  This feature has the following characteristics and limitations:

  - If there is not enough memory on the system disk on which the Temp folder is located, no backup can be performed, and no notification of failed copying (non-provided protection) is displayed.

  - Backup copies of files are saved in unencrypted format.

  - Backup copies of files are deleted when you close Kaspersky Anti-Virus or disable the System Watcher component.

  - In case of an emergency termination of Kaspersky Anti-Virus, backup copies are not deleted. In this case, you must delete them manually.

- The latest versions of popular web browsers are now supported: protection components (such as Kaspersky URL Advisor) support Mozilla™ Firefox™ 28.x, Internet Explorer® 11, and Google Chrome™ 33.x, 34.x, and 35.x.

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

- Less time is required to start the application.

- Application GUI performance and responsiveness have been improved.

- Support for Windows® 8.1 Update has been added.

- The application upgrade process has been improved.

- The size of the application distribution package has been reduced.

DISTRIBUTION KIT

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

- Boxed. Distributed via stores of our partners.

- At the online store. Distributed at online stores of Kaspersky Lab (for example, http://www.kaspersky.com, 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 Anti-Virus at an online store, you copy the application from the website of the store. Information that is required for activating the application, including an activation code, will be sent to you by email after your payment has been received.

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

MAIN APPLICATION FEATURES

Kaspersky Anti-Virus 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 Anti-Virus 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 Anti-Virus 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 Anti-Virus 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 Anti-Virus 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.

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.

Network Monitor

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

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 and IM Anti-Virus.

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 Anti-Virus with your friends. You can exchange your bonus points for a bonus activation code for Kaspersky Anti-Virus.

SERVICE FOR USERS

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

- Database updates and access to new versions of the application

- Consultations by phone and by email on issues that are related to installation, configuration, and use of the application

- Notifications about the release of new applications by Kaspersky Lab and of new viruses and virus outbreaks To use this service, subscribe to 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

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

General requirements:

- Intel® Pentium® III 1 GHz 32-bit (x86) / 64-bit (x64) processor or later (or a compatible equivalent)

- 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

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):

- 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), Windows 8.1 Pro (Windows 8.1 Update), and Windows 8.1 Enterprise (Windows 8.1 Update):

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

Requirements for laptops:

- 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 Anti-Virus 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 Anti-Virus to your computer:*

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

> To install Kaspersky Anti-Virus, 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 Anti-Virus.

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 Anti-Virus 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. For further details on how to install the new version of the application, refer to the relevant documentation.

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 Anti-Virus 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 Anti-Virus 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 Anti-Virus 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 Anti-Virus cannot remove automatically. When removing incompatible applications, you will need to restart your operating system, after which installation of Kaspersky Anti-Virus 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 Anti-Virus immediately, make sure that the **Run Kaspersky Anti-Virus** check box is selected and click the **Finish** button.

If you have cleared the **Run Kaspersky Anti-Virus** 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

During this step, the Setup Wizard asks you to activate the application.

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

If you have purchased a license for Kaspersky Anti-Virus and downloaded the application from an online store, the application can be activated automatically during installation.

The following options for Kaspersky Anti-Virus activation are offered:

- **Activate the 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 Internet Security in the entry field, the procedure for switching to Kaspersky Internet 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 the Kaspersky Protection Center portal.

STEP 8. REGISTERING A USER

This step is not available in all versions of Kaspersky Anti-Virus.

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

UPGRADING A PREVIOUS VERSION OF THE APPLICATION

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

If an earlier version of Kaspersky Anti-Virus is already installed on your computer, you can upgrade it to the latest version of Kaspersky Anti-Virus. If you have a current license for an earlier version of Kaspersky Anti-Virus, you do not need to activate the application: the Setup Wizard will automatically retrieve information about the license for the previous version of Kaspersky Anti-Virus and apply it during installation of the new version of Kaspersky Anti-Virus.

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

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

- Continue using Kaspersky Internet Security under the current license. In this case, the Migration Wizard will be started. When the Migration Wizard finishes, the new version of Kaspersky Internet Security will be installed to your computer. You can use Kaspersky Internet Security until the license for the previous version of Kaspersky Internet Security expires.

- Proceed with installation of the new version of Kaspersky Anti-Virus. In this case, the application is installed and activated according to the standard scenario.

Kaspersky Anti-Virus 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 Anti-Virus to your computer:*

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

> To install Kaspersky Anti-Virus, 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.

> During the process of upgrading a previous version of Kaspersky Anti-Virus, 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 installing a new version of Kaspersky Anti-Virus over Kaspersky Anti-Virus 2011 and earlier, objects in Quarantine and Backup may be lost, because the new version of the application does not contain a Backup.

IN THIS SECTION

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 Anti-Virus.

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 Anti-Virus 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. For further details on how to install the new version of the application, refer to the relevant documentation.

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 Anti-Virus 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 Anti-Virus 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 Anti-Virus 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 Anti-Virus cannot remove automatically. When removing incompatible applications, you will need to restart your operating system, after which installation of Kaspersky Anti-Virus 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 Anti-Virus** check box is selected, the application will be started automatically after you restart your computer.

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

REMOVING THE APPLICATION

After removing Kaspersky Anti-Virus, your computer and private data will be unprotected!

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

➡ *To start the Wizard:*

In the **Start** menu, select **All Programs** → **Kaspersky Anti-Virus** → **Remove Kaspersky Anti-Virus**.

IN THIS SECTION

STEP 1. ENTERING THE PASSWORD TO REMOVE THE APPLICATION

To remove Kaspersky Anti-Virus, 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 Anti-Virus is removed from the computer, quarantined files become unavailable. To perform operations with these files, Kaspersky Anti-Virus 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** consists of files that describe objects already scanned with iChecker technology.

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 Anti-Virus, 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.

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, ways of activating the application, and license renewal.

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 Anti-Virus.

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 14)

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 running, though 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 using only the databases that had been installed before the license expired. To continue using Kaspersky Anti-Virus 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 Anti-Virus. The trial version of Kaspersky Anti-Virus remains functional during a short evaluation period. After the evaluation period expires, all the features of Kaspersky Anti-Virus 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 Anti-Virus. 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 Anti-Virus, an activation code is provided in the manual or on the retail box that contains the installation CD.

- When you purchase Kaspersky Anti-Virus 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 55), 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 Anti-Virus 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 Anti-Virus* establishes use of the application within the selected parameters (expiration date and number of protected devices). You can obtain a subscription for Kaspersky Anti-Virus 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 Anti-Virus: 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 Anti-Virus 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 Anti-Virus 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 Anti-Virus 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 Anti-Virus is already in use under a current license when you register your subscription, after registration Kaspersky Anti-Virus 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 Anti-Virus.

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

ABOUT DATA PROVISION

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

- Information about the checksums of processed files (MD5)

- 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 Anti-Virus in use

- Information about licensing of the installed version of Kaspersky Anti-Virus

- 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 Anti-Virus, 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 53), you agree to automatically send the following information related to Kaspersky Anti-Virus 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 potentially 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 Anti-Virus

- 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 about the actual time spent by application components to scan objects

- Statistics about delays related to Kaspersky Anti-Virus when starting applications

- 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.

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 Anti-Virus messages that appear in the taskbar notification area.

➡ *To activate Kaspersky Anti-Virus:*

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 Account or to Kaspersky Protection Center. 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 Anti-Virus.

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

ACQUIRING AND RENEWING A LICENSE

If you have installed Kaspersky Anti-Virus 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 28).

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

➡ *To acquire a license:*

1. Open the main application window.

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

➡ *To specify a new activation code:*

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 Anti-Virus 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 events occurring in the application's operation 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 of critical notifications and pop-up messages are red-colored.

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

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

If a notification is displayed on the screen, you should select one of the options that are suggested in the notification. The optimal option is the one recommended as the default by Kaspersky Lab experts. A notification can be closed automatically when the computer is restarted, when Kaspersky Anti-Virus is quit, or in Connected Standby mode in Windows 8. When a notification is closed automatically, Kaspersky Anti-Virus performs the action that is recommended by default.

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

ASSESSING COMPUTER PROTECTION STATUS AND RESOLVING SECURITY ISSUES

Problems with computer protection are 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.
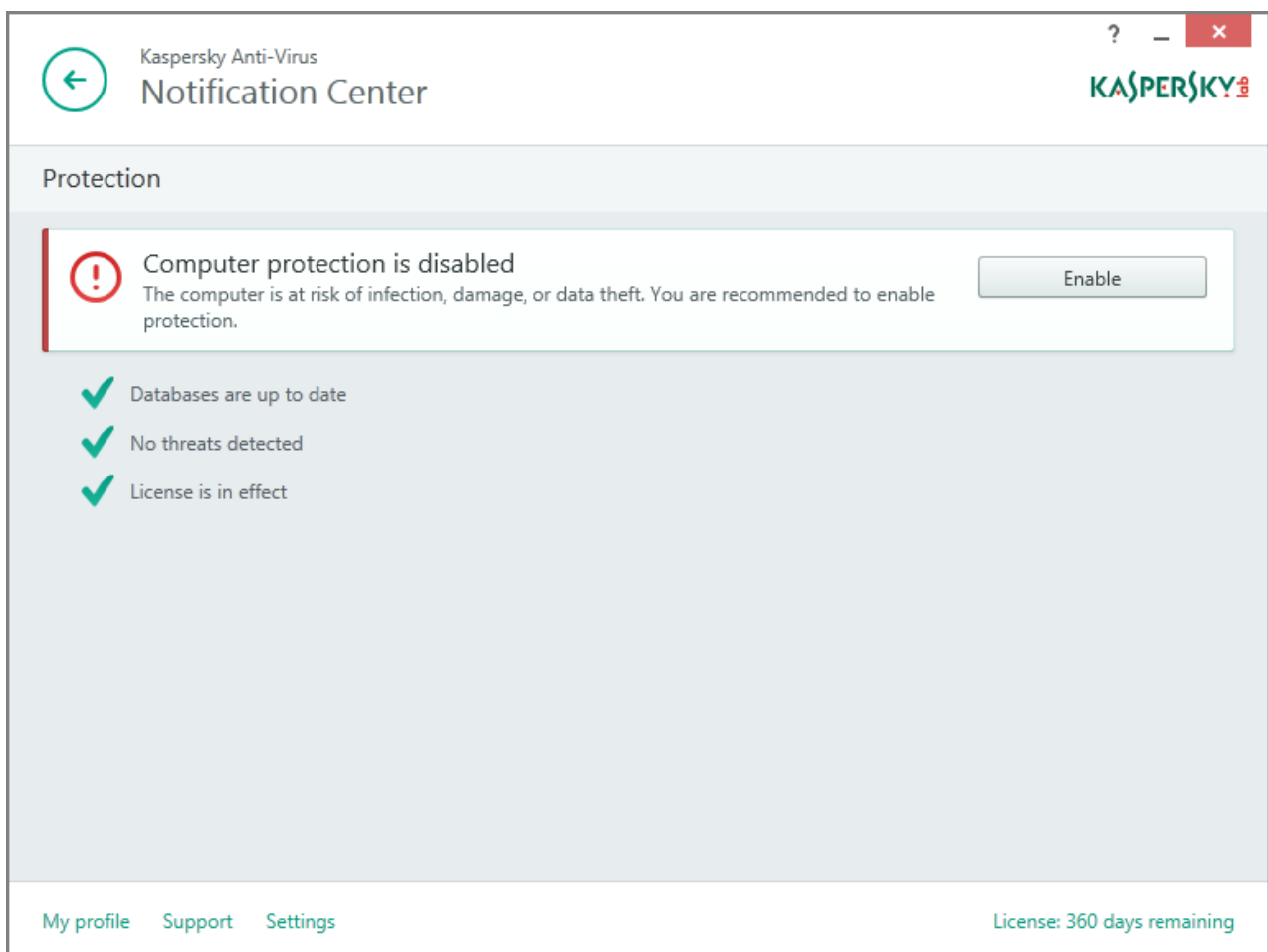
Figure 1. Notification Center window

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 Anti-Virus automatically checks for updates on the Kaspersky Lab update servers. If the server has a set of recent updates, Kaspersky Anti-Virus downloads and installs them in the background. You can run an update of Kaspersky Anti-Virus 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 updates from Kaspersky Lab update servers, you must be connected to the Internet.

On Microsoft Windows 8, updates 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 updates, 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 window displays the **Update** section.

2. In the **Update** section, click the **Run update** button.

SCANNING THE COMPUTER

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

FULL SCAN OF THE COMPUTER FOR VIRUSES

During a full scan, Kaspersky Anti-Virus scans the following objects by default:

- System memory

- Objects loaded on operating system startup

- Backup

- Hard drives and removable drives

We recommend running a full scan immediately after installing Kaspersky Anti-Virus to your computer.

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

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

   The **Scan** window opens.

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

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

   Kaspersky Anti-Virus starts a full scan of your computer.

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

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

- From the context menu of the object

- From the main application window

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

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**.
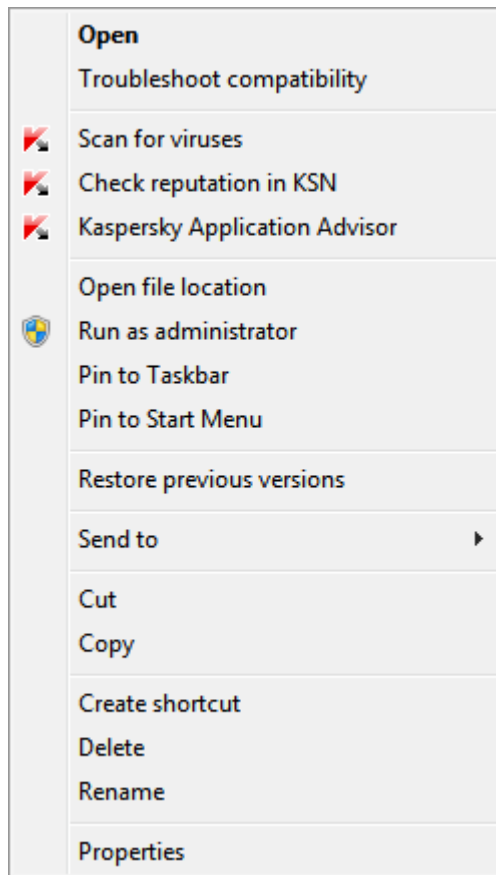
Figure 2. Context menu of an executable file in Microsoft Windows

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

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

     The **Scan** window opens.

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

3.   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.

4.   Click the **Run scan** button.

SCANNING CRITICAL AREAS OF YOUR COMPUTER FOR VIRUSES

A scan of critical areas performs scanning of the following objects:

- Objects loaded at the startup of the operating system

- System memory

- Boot sectors of the disk

➡ *To start a scan of critical areas from the main application window:*

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

    The **Scan** window opens.

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

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

Kaspersky Anti-Virus starts the scanning process.

SCANNING PROBABLY INFECTED OBJECTS

If you suspect that an object is infected, scan it with Kaspersky Anti-Virus.

If the application completes the scan and reports that the object is safe although you suspect that it is not, you can send this object to the *Virus Lab*. Virus Lab specialists scan the object. If it turns out to be infected with a virus, they add the description of the new virus to the databases that will be downloaded by the application during updates.

➡ *To send a file to the Virus Lab:*

1. Go to the Virus Lab (http://support.kaspersky.com/virlab/helpdesk.html) request page.

2. Follow the instructions on this page to send your request.

SCANNING THE COMPUTER FOR VULNERABILITIES

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 **Show Additional Tools** drop-down list, select **Vulnerability Scan**.

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

Kaspersky Anti-Virus 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 Anti-Virus 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 Anti-Virus 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 **Show Additional Tools** drop-down list, select **Quarantine**.

3. 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.

ABOUT TROUBLESHOOTING OF 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 **Show Additional Tools** drop-down list, select **Microsoft Windows Troubleshooting**.

   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 to **Search for problems 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. Selecting troubleshooting actions

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, to the left of the group name, click the plus sign (+).

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 problems

The Wizard performs the actions selected during the previous step. It may take a while to fix the problems. When troubleshooting is complete, the Wizard automatically proceeds to the next step.

Step 5. Wizard completion

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

CONFIGURING MAIL ANTI-VIRUS

Kaspersky Anti-Virus 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 Center** section, select the **Mail Anti-Virus** component.

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

4. Make sure that the switch in the upper part of the window that enables / disables Mail Anti-Virus, is enabled.

5. Select a security level:

    - **Recommended**. If you select this security level, Mail Anti-Virus scans both incoming and outgoing messages and scans attached archives.

    - **Low**. If you select this security level, Mail Anti-Virus scans incoming messages only, without scanning attached archives.

    - **High**. If you select this security level, Mail Anti-Virus scans both incoming and outgoing messages and scans attached archives. 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 Anti-Virus. Before deleting an object, Kaspersky Anti-Virus 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 36).

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 Anti-Virus helps you to protect your private data against theft:

- Passwords, user names, and other registration data

- Account numbers and bank card numbers

Kaspersky Anti-Virus 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 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.

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

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 Anti-Virus.

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 Modern UI style or for Microsoft Internet Explorer 10 and 11 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 Anti-Virus.

- 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.

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

- 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 **Virtual Keyboard**.

Figure 3. Kaspersky Anti-Virus context menu

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

1. Open the main application window.

2. Click the **Virtual Keyboard** button.

➡️ *To open Virtual Keyboard from a browser window:*

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

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

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

C HECKING A WEBSITE FOR SAFETY

Kaspersky Anti-Virus 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 Modern UI style.

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 Anti-Virus 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 Anti-Virus 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 Center** section, select the **Web Anti-Virus** subsection.

   The window displays the settings for Web Anti-Virus.

4. In the lower part of the window, click the **Advanced Settings** link. The advanced settings window of Web Anti-Virus opens.

5. In the **Kaspersky URL Advisor** section, select the **Check URLs** check box.

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

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

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

   a. Select **On specified websites only**.

   b. Click the **Configure checked websites** link.

   c. In the **Configure checked websites** window that opens, click the **Add** button.

   d. In the **Add URL** window that opens, enter the URL of a web page whose content you want to check.

   e. Select 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 URLs** window. Web Anti-Virus checks URLs on this web page.

8. If you want to edit the advanced settings for URL checking, in the **Advanced settings of Web Anti-Virus** 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 of the safety of links on all web pages, in the **Checked URLs** section, select **All URLs**.

10. If you want Web Anti-Virus to display information about whether a link belongs to a specific category of website content (for example, *Explicit language*):

    a. Select the **Show information on the categories of website content** check box.

    b. Select the check boxes next to categories of website content about which information should be displayed in comments.

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

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 Anti-Virus 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 **Show Additional Tools** drop-down list, select **Privacy Cleaner** 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 signs 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).
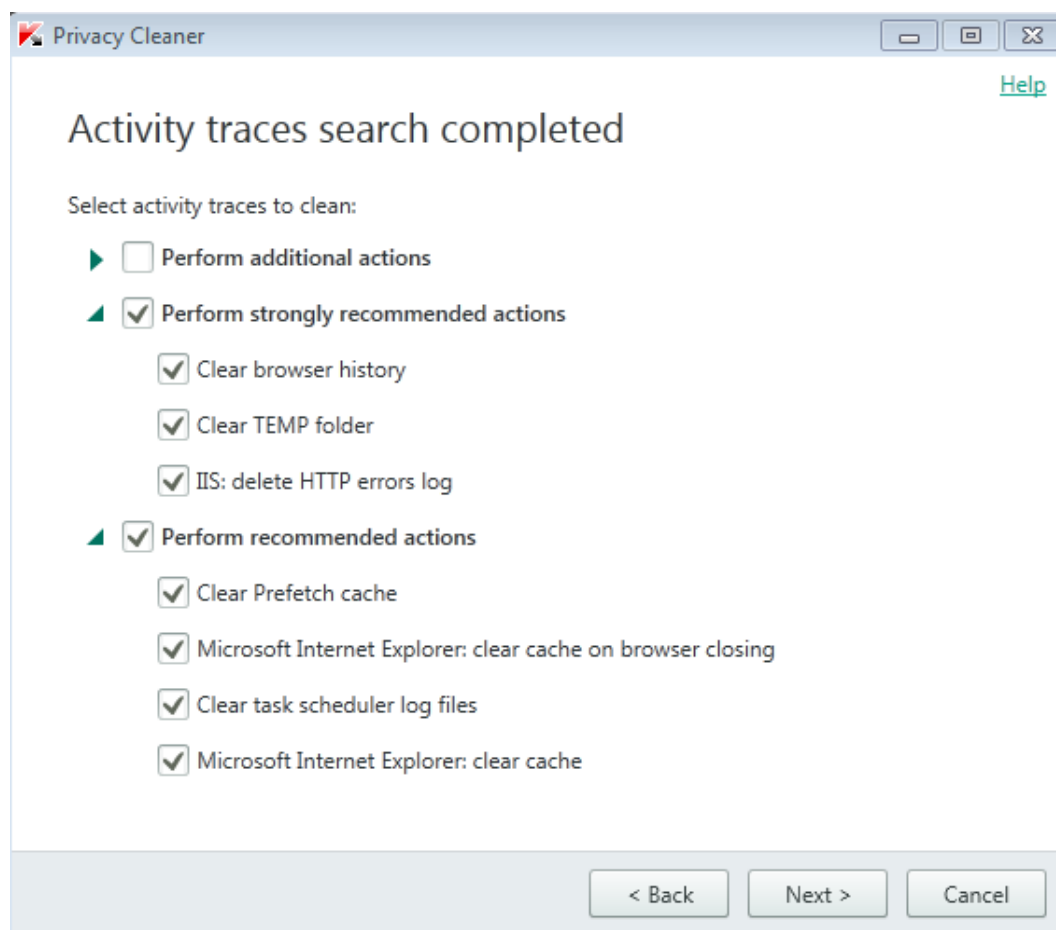
Figure 4. Activity traces detected and recommendations on eliminating them

To view 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.

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

After you define the set of actions for the Wizard to perform, click the **Next** button.

Step 4. Clearing activity traces

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.

RESERVING OPERATING SYSTEM RESOURCES FOR COMPUTER GAMES

When Kaspersky Anti-Virus 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 Anti-Virus distract the user from the gaming process.

To avoid changing the settings of Kaspersky Anti-Virus 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 Anti-Virus, 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 Anti-Virus.

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

PASSWORD-PROTECTING ACCESS TO KASPERSKY ANTI-VIRUS 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 Anti-Virus 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 Anti-Virus:*

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. To change a previously created password, type it in the **Old password** field.

6. 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 Anti-Virus settings.

PAUSING AND RESUMING COMPUTER PROTECTION

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

➡ *To pause the protection of your computer:*

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

    The **Pause protection** window opens (see the following figure).
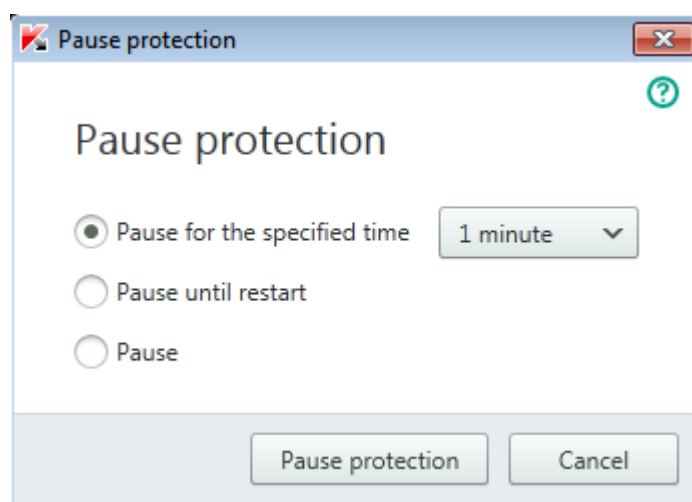
Figure 5. Pause protection window

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 Anti-Virus at any time. The settings can be restored using the *Application Configuration Wizard*.

When the Wizard completes its operation, the *Recommended* security level is set for all protection components. When restoring the recommended security level, you can save the 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 Anti-Virus.

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 page shows which protection components of Kaspersky Anti-Virus have settings that differ from their default values because of changes by the user. If special settings have been created for any of the components, they are also shown in the window (see the following figure).
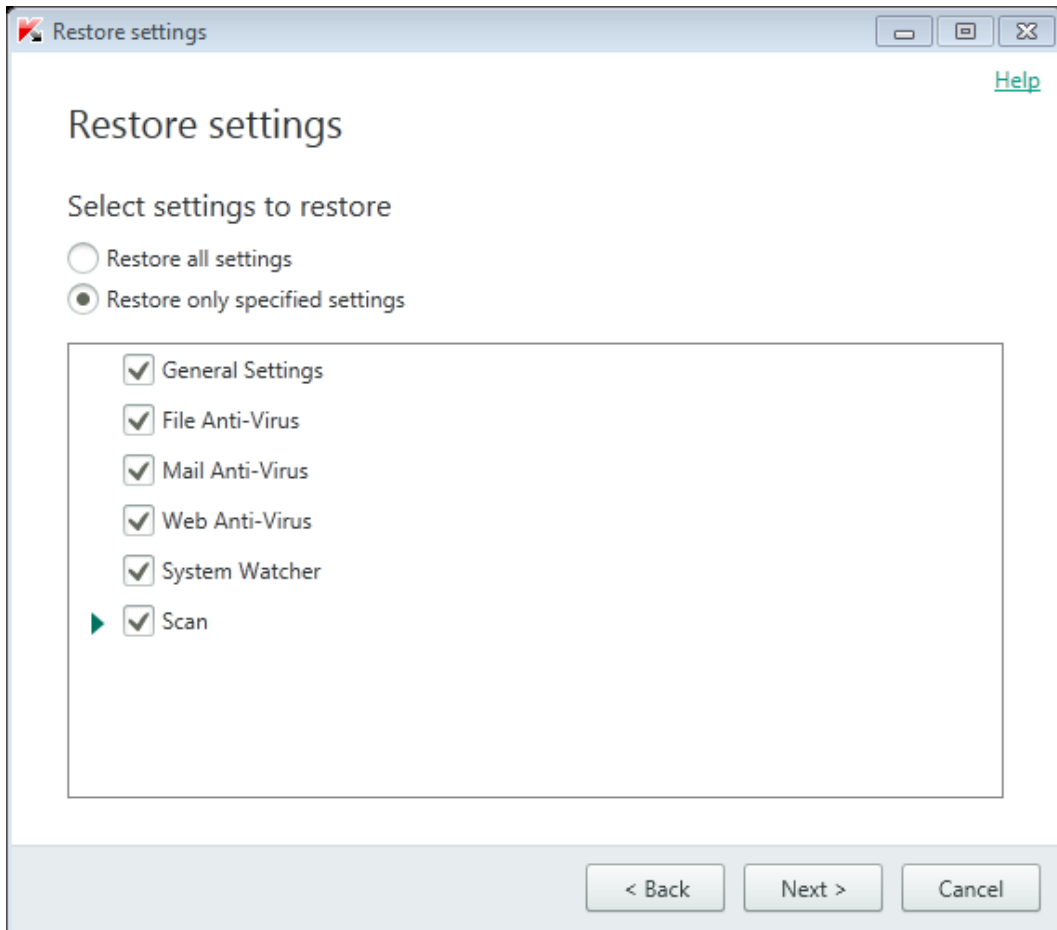

Figure 6. Restore settings window

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

Step 3. Finishing restoration

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

VIEWING THE APPLICATION OPERATION REPORT

Kaspersky Anti-Virus 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).

➡ *To view the application operation report:*

1. Open the main application window.

2. Click the **Reports** button.

   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).

3. 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 Anti-Virus 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 Anti-Virus 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 Anti-Virus.

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)

To protect your computer more effectively, Kaspersky Anti-Virus uses data received from users from all over the world. Kaspersky Security Network is designed for obtaining this data.

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 Anti-Virus 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 Anti-Virus to Kaspersky Lab (see the section "About data provision" on page 27).

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 Anti-Virus 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 the installation package for Kaspersky Anti-Virus with an extended evaluation period. When one of your friends on Twitter or on a social network downloads the Kaspersky Anti-Virus 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 Anti-Virus.

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

If you participate in the Protect a Friend program, a user rating is assigned to you. Your user rating depends on the application version and on the application features and components that you use the most frequently (for example, scanning).

To participate in the Protect a Friend program, open the web page with your Protect a Friend profile. Clicking the **My profile** link in the lower part of the main window of Kaspersky Anti-Virus 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 Kaspersky Account. If you do not have a 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 your rating in the Protect a Friend program and the number of bonus points you have collected.

- Publish links for downloading the Kaspersky Anti-Virus 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 Anti-Virus installation package).

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 Kaspersky Account. If you do not have a Kaspersky Account yet, create one when you visit the web page of the Protect a Friend program for the first time.

Your 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 Kaspersky Account.

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

◆   *To create your Kaspersky Account:*

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

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

2.   Create and activate your 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 Kaspersky Account. A message will be sent to your email address, containing a link that you must click to activate your Kaspersky Account.

     d.   Click the link to activate your Kaspersky Account.

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

If you already have a 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 profile** link.

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

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

     The web page displays your Protect a Friend profile.

SHARING A LINK TO KASPERSKY ANTI-VIRUS 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 Anti-Virus 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 Anti-Virus installation package by email or by instant messengers (such as ICQ).

◆   *To publish a link for downloading the Kaspersky Anti-Virus installation package on Twitter or on social networks:*

1.   Open the main window of Kaspersky Anti-Virus and, in the lower part of the window, click the **My profile** link.

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

2.   Sign in on the web page with your 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 Anti-Virus 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 Anti-Virus:*

1. Open the main window of Kaspersky Anti-Virus and, in the lower part of the window, click the **My profile** link.

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

2. Sign in on the web page with your 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 Anti-Virus to send by email or by instant messaging:*

1. Open the main window of Kaspersky Anti-Virus and, in the lower part of the window, click the **My profile** link.

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

2. Sign in on the web page with your 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 Anti-Virus 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 Anti-Virus in exchange for a specified number of bonus points. Bonus points are awarded to you when users download Kaspersky Anti-Virus 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 Anti-Virus.

- When a user with whom you have shared the link activates Kaspersky Anti-Virus.

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 Anti-Virus and, in the lower part of the window, click the **My profile** link.

   The web page with your Protect a Friend profile opens.

2. Sign in on the web page with your 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 Anti-Virus.

→ *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 Anti-Virus and, in the lower part of the window, click the **My profile** link.

   The web page with your Protect a Friend profile opens.

2. Sign in on the web page with your 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 Anti-Virus.

SWITCHING FROM KASPERSKY ANTI-VIRUS TO KASPERSKY INTERNET SECURITY

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

Kaspersky Internet Security is an application designed to ensure comprehensive protection of your computer. Compared to Kaspersky Anti-Virus, Kaspersky Internet Security provides a range of additional advanced options as part of the following components and features:

- Application Control

- Trusted Applications mode

- Parental Control

- Firewall

- Network Attack Blocker

- Safe Money

- Blocking access to dangerous websites

- Network Monitor

- Anti-Spam

- Anti-Banner

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

When used in certain regions or by subscription, temporary switching to the trial version of Kaspersky Internet Security is not available.

IN THIS SECTION

SWITCHING TO THE TRIAL VERSION OF KASPERSKY INTERNET SECURITY

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

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

1. Open the main application window.

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

3. In the window that opens, click the **Trial version** button.

    The migration wizard starts.

4. Follow the wizard's instructions.

When used in certain regions or by subscription, temporary switching to the trial version of Kaspersky Internet Security is not available. In these cases, the **Protection extension** option is not available in the **Show advanced tools** list.

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

If the request for activation of the trial version of Kaspersky Internet Security is successful, the wizard automatically proceeds to the next step.

Step 2. Starting the upgrade

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

Step 3. Removing incompatible applications

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

Step 4. Switching to the trial version of Kaspersky Internet Security

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

Step 5. Restarting the application

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

Step 6. Completing activation

After the application starts again, the wizard runs automatically. After successful activation of the trial version of Kaspersky Internet Security, the wizard window displays information about the length of time during which you can use the trial version.

Step 7. Operating system analysis

At this stage, information about Microsoft Windows applications is collected. 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.

SWITCHING FROM KASPERSKY ANTI-VIRUS TO KASPERSKY INTERNET SECURITY

Step 8. Completing the migration

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

After the license for the trial version of Kaspersky Internet Security expires, you cannot temporarily switch from Kaspersky Anti-Virus to the trial version of Kaspersky Internet Security again.

SWITCHING TO KASPERSKY INTERNET SECURITY

If you want to switch to Kaspersky Internet Security, you must have an activation code (see the section "About the activation code" on page 26).

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

1. Open the main application window.

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

3. 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 Internet Security.

When used in certain regions or by subscription, Kaspersky Anti-Virus does not allow switching to the trial version of Kaspersky Internet Security. In these cases, the **Upgrade** feature is not available.

USING THE APPLICATION FROM THE COMMAND PROMPT

You can use Kaspersky Anti-Virus 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 Anti-Virus 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 10), we recommend that you contact Kaspersky Lab Technical Support. Technical Support specialists will answer any of your questions about installing and using the application.

Before contacting Technical Support, please read the support rules (http://support.kaspersky.com/support/rules).

You can contact Technical Support in one of the following ways:

- By telephone. This method allows you to consult with specialists from our Russian-language or international Technical Support.

- By sending a query from your Kaspersky Account on the Technical Support website. This method allows you to contact our specialists using the query form.

Technical support is 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.

OBTAINING TECHNICAL SUPPORT VIA MY KASPERSKY ACCOUNT

My Kaspersky Account is your personal area (https://my.kaspersky.com) on the Technical Support website.

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

In My Kaspersky Account, you can perform the following actions:

- Contact Technical Support and the Virus Lab.

- Contact Technical Support without using email.

- Track the status of your requests in real time.

- View a detailed history of your Technical Support requests.

- Receive a copy of 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 to your My Kaspersky Account and to the email address that you have specified in your online request.

Online request to the Virus Lab

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

You can send requests for examination of suspicious files and web resources to the Virus Lab. You can also contact the Virus Lab if Kaspersky Anti-Virus generates a false positive with regard to files and web resources that you do not consider to be dangerous.

You can also send requests to the Virus Lab from the page with the request form (http://support.kaspersky.com/virlab/helpdesk.html) without being registered in My Kaspersky Account. On this page, you do not have to specify an application activation code.

USING TRACE FILES AND AVZ SCRIPTS

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

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

IN THIS SECTION

CREATING A SYSTEM STATE REPORT

➡ *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 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 in your My Kaspersky Account on the Technical Support website if 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 Account.

➡ *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 check boxes next to the data that you want to send to Technical Support.

7. Click the **Save report** link.

    A window for saving the archive opens.

8. Specify the archive name and confirm saving.

The created archive can be sent to Technical Support from My Kaspersky Account.

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 (see the section "How to obtain technical support" on page 63).

➡ *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 **Script execution** window opens.

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

    The script runs.

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

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 Anti-Virus. 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 (real-time protection, on-demand scan, updates). By starting a scan of your computer, you run the application module of that task.

AVAILABLE UPDATE

A set of updates for Kaspersky Lab application modules, including critical updates accumulated over a certain period of time and changes to the application's architecture.

B

BLOCKING AN OBJECT

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

BONUS ACTIVATION CODE

An activation code for Kaspersky Anti-Virus 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).

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 Anti-Virus.

INFECTABLE FILE

A file that, due to its structure or format, can be used by criminals as a "container" to store and spread malicious code. As a rule, they are executable files, for example, files with the extensions COM, EXE, DLL, etc. The risk of penetration of malicious code into such files is quite high.

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 kind of Internet fraud in which email messages are sent with the purpose of stealing confidential information, most often financial 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.

PROTECTION COMPONENTS

Integral parts of Kaspersky Anti-Virus 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.

PROTOCOL

A clearly defined and standardized set of rules governing the interaction between a client and a server. Well-known protocols and the services associated with them include HTTP, FTP, and NNTP.

Q

QUARANTINE

A dedicated storage 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

ROOTKIT

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

On Windows-based operating systems, a rootkit usually 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

SCRIPT

A small computer program or an independent part of a program (function) which, as a rule, has been developed to execute a specific task. It is most often used with programs that are embedded in hypertext. Scripts are run, for example, when you open 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.

SECURITY LEVEL

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

SPAM

Unsolicited mass email mailings, most often including advertising messages.

STARTUP OBJECTS

The set of programs needed to start and correctly operate the operating system and software installed on your computer. These objects are executed every time the operating system is started. There are viruses capable of infecting autorun objects specifically, which may lead, for example, to blocking of operating system startup.

T

TASK

Functions performed by the Kaspersky Lab application are implemented as tasks, such as: Real-time file protection, Full computer scan, and Database update.

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 in KSN, 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 Anti-Virus 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 user rating, number of collected bonus points, a link to the page for downloading Kaspersky Anti-Virus, and bonus activation codes granted to the user.

USER RATING

The index of user activity in use of Kaspersky Anti-Virus. The user rating is displayed in the user profile and depends on the settings and the version of the application.

V

VIRUS

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

VIRUS OUTBREAK

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

VULNERABILITY

A flaw in an operating system or an application that may be exploited by malware makers to penetrate 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), Critical Path (Ireland), D-Link (Taiwan), M86 Security (USA), GFI (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), NETASQ (France), NETGEAR (USA), Parallels (Russia), SonicWALL (USA), WatchGuard Technologies (USA), and ZyXEL Communications (Taiwan). Many of the company's innovative technologies are patented.

ACHIEVEMENTS. Over the years, Kaspersky Lab has won hundreds of awards for its services in combating computer threats. For example, in 2010 Kaspersky Anti-Virus received several top Advanced+ awards in a test administered by AV-Comparatives, a respected Austrian anti-virus laboratory. But Kaspersky Lab's main achievement is the loyalty of its users worldwide. The company's products and technologies protect more than 300 million users, and its corporate clients number more than 200,000.

Kaspersky Lab website:	http://www.kaspersky.com
Virus encyclopedia:	http://www.securelist.com
Virus Lab:	newvirus@kaspersky.com (only for sending probably infected files in archive format)
	http://support.kaspersky.com/virlab/helpdesk.html
	(for queries addressed to virus analysts)
Kaspersky Lab's web forum:	http://forum.kaspersky.com

INFORMATION ABOUT THIRD-PARTY CODE

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

TRADEMARK NOTICES

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

Google Chrome is a trademark of Google, Inc.

ICQ is Trademark and/or Service mark of ICQ LLC.

Intel, Celeron, Atom, and Pentium are trademarks of Intel Corporation in the U.S. and/or other countries.

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

Mozilla and Firefox are trademarks of the Mozilla Foundation.

INDEX