KASPERSKY lab

Kaspersky Anti-Virus

User Guide

Application version: 16.0 Maintenance Release 1

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.

Document revision date: 11/30/2015

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

Table of Contents

About this Guide

This document is the User Guide to Kaspersky Anti-Virus 2016 (hereinafter 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 provides instructions on:

- Preparing Kaspersky Anti-Virus for installation, installing and activating the application
- Configuring and using Kaspersky Anti-Virus

This Guide also lists sources of information about the application and ways to get technical support.

In this section

In this Guide

This document contains the following sections:

Sources of information about the application (see page 13)

This section lists the sources of information about the application.

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

Kaspersky Anti-Virus (see page 16)

This section describes the functions, components, and distribution kit of Kaspersky Anti-Virus, and provides a list of hardware and software requirements of Kaspersky Anti-Virus.

Installing and removing the application (see page 22)

This section contains step-by-step instructions for Kaspersky Anti-Virus installation and removal.

Application licensing (see page 43)

This section covers the main aspects of application licensing.

Managing application notifications (see page 56)

This section provides information about how to manage application notifications.

Assessing computer protection status and resolving security issues (see page 57)

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

Updating databases and application modules (see page 58)

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

Scanning the computer (see page 61)

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

Restoring an object deleted or disinfected by the application (see page 65)

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

Troubleshooting the operating system after infection (see page 53)

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

Configuring Mail Anti-Virus (see page 66)

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

Protecting personal data on the Internet (see page 68)

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

Protecting financial transactions and online purchases

This section provides instructions on how you can protect your financial transactions and purchases online with Kaspersky Anti-Virus.

Removing traces of activity on the computer and on the Internet (see page 74)

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

Remote management of computer protection (see page 77)

This section describes how you can manage protection of your computer remotely via My Kaspersky portal.

Reserving operating system resources for computer games (see page 80)

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 (see page 81)

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

Pausing and resuming computer protection (see page 82)

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

Restoring the default application settings (see page 84)

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

Viewing the application operation report (see page 85)

This section contains instructions on how to view application reports.

Applying the application settings on another computer (see page 86)

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

Participating in Kaspersky Security Network (see page 88)

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

Participating in the Protect a Friend program (see page 91)

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

Using the application from the command prompt (see page 94)

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

Assistance from Kaspersky Lab Technical Support (see page 95)

This section describes the ways to get technical support and the terms on which it is available.

Limitations and warnings (see page 102)

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

Glossary (see page 107)

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

AO Kaspersky Lab (see page 117)

This section provides information about AO Kaspersky Lab.

Information about third-party code (see page 119)

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

Trademark notices (see page 120)

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

This document uses the following conventions (see table below).

Table 1. Document conventions

Sample text	Description of document convention
Note that...	Warnings are highlighted in red and boxed. Warnings show information about actions that may have unwanted consequences.
We recommended that you use...	Notes are boxed. Notes provide additional and reference information.
Example:	Examples are given on a light-blue background under the heading "Example".
Update means... The *Databases are out of date* event occurs.	The following 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.

Sample text	Description of document convention
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 to be entered using the keyboard
<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 lists the sources of information about the application.

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 about Kaspersky Anti-Virus to research on your own:

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

If you cannot find the solution to an issue on your own, we recommend that you contact Kaspersky Lab Technical Support (see the section "Technical support by phone" on page 95).

An Internet connection is required to use information sources on websites.

Kaspersky Anti-Virus page on the Kaspersky Lab website

On the Kaspersky Anti-Virus page (http://www.kaspersky.com/anti-virus), you can view general information about the application and its functions and features.

Kaspersky Anti-Virus page contains a link to the eStore. There you can purchase or renew the application.

Kaspersky Anti-Virus page in the Knowledge Base

Knowledge Base is a section on the Technical Support website.

On the Kaspersky Anti-Virus page in the Knowledge Base (http://support.kaspersky.com/kav2016), 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 in the Knowledge Base may provide answers to questions that relate both to Kaspersky Anti-Virus as well as to other Kaspersky Lab applications. Articles in the Knowledge Base may also contain news from Technical Support.

Online help

The application includes full help and context help.

Full help provides information on how to configure and use Kaspersky Anti-Virus.

Context help provides information about Kaspersky Anti-Virus windows, describes Kaspersky Anti-Virus settings and contains links to task descriptions where those settings are used.

Help can be included in the distribution kit or located on the Kaspersky Lab web resource. If online help is available, a browser window is opened when online help is accessed. Internet connection is required to display online help.

Documentation

The application user guide provides information about how to install, activate, and configure the application, as well as about use of the application. The document also describes the application interface and provides ways for solving typical user tasks during use of the application.

Discussing Kaspersky Lab applications on the Forum

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

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

Kaspersky Anti-Virus

This section describes the functions, components, and distribution kit of Kaspersky Anti-Virus, and provides a list of hardware and software requirements of Kaspersky Anti-Virus.

In this section

About Kaspersky Anti-Virus

Kaspersky Anti-Virus provides comprehensive protection against various types of information security threats. 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 various types of information security threats, network attacks, and fraud. 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. If an infected file is placed in the same location where the deleted file with the same name used to be, Quarantine saves only a copy of the last file. A copy of the previous file with the same name is not saved.

Mail Anti-Virus

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

Web Anti-Virus

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

IM Anti-Virus

IM Anti-Virus ensures the safe use of IM clients. 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.

System Watcher

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

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.

On-Screen Keyboard

On-Screen Keyboard prevents interception of data entered on the hardware keyboard and protects personal data against interception attempts that use screen shots.

Online Management

If Kaspersky Anti-Virus is installed on a computer and you have an account on My Kaspersky portal, you can manage protection of this computer remotely.

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.

What's new

Kaspersky Anti-Virus provides the following new features:

- Microsoft® Windows® 10 support limitations no longer apply.
- License expiration notifications consistent with the Microsoft standard have been added.
- In the Windows 10 operating system, application notifications have been replaced with pop-up messages consistent with the Microsoft standard.
- The Protect a Friend program has been moved to My Kaspersky portal. You can now register and sign in to the Protect a Friend program when connecting to My Kaspersky portal. Pages of the Protect a Friend program can be viewed on My Kaspersky portal.

- Support of the HTTP/2 protocol has been added.
- Partial support of Yandex.Browser and the Microsoft Edge browser has been added.
- Support for virtual desktops in Microsoft Windows 10 has been added.
- The graphic user interface has been improved.

Distribution kit

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

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

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

- Sealed envelope with the setup CD, which contains application files and documentation files
- Brief User Guide, with an activation code
- License Agreement, which stipulates the terms on which you can use the application

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

If you purchase Kaspersky 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.

Hardware and software requirements

General requirements:

- 480 MB free disk space on the hard drive
- CD-/DVD-ROM (for installing from the installation CD)

- Internet access (for the application installation and activation and for updating databases and software modules)
- Microsoft® Internet Explorer® 8.0 or later

  > To access My Kaspersky portal, we recommend using Microsoft Internet Explorer 9.0 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):

- Processor with a clock speed of 1 GHz or higher
- 512 MB free RAM

Requirements for Microsoft Windows Vista® Home Basic (Service Pack 1 or later), Microsoft Windows Vista Home Premium (Service Pack 1 or later), Microsoft Windows Vista Business (Service Pack 1 or later), Microsoft Windows Vista Enterprise (Service Pack 1 or later), Microsoft Windows Vista Ultimate (Service Pack 1 or later), Microsoft Windows 7 Starter (Service Pack 1 or later), Microsoft Windows 7 Home Basic (Service Pack 1 or later), Microsoft Windows 7 Home Premium (Service Pack 1 or later), Microsoft Windows 7 Professional (Service Pack 1 or later), Microsoft Windows 7 Ultimate (Service Pack 1 or later), Microsoft Windows 8, Microsoft Windows 8 Pro, Microsoft Windows 8 Enterprise, Microsoft Windows 8.1 (Windows 8.1 Update), Microsoft Windows 8.1 Pro (Windows 8.1 Update), Microsoft Windows 8.1 Enterprise (Windows 8.1 Update), Microsoft Windows 10 Home, Microsoft Windows 10 Enterprise, and Microsoft Windows 10 Pro:

- Processor with a clock speed of 1 GHz or higher
- 1 GB free RAM (for 32-bit operating systems); 2 GB free RAM (for 64-bit operating systems)

Requirements for tablet computers:

- Microsoft Tablet PC
- Intel® Celeron® CPU 1.66 GHz or faster
- 1000 MB free RAM

Requirements for netbooks:

- Intel Atom™ CPU 1.60 GHz or faster
- 1024 MB free RAM
- 10.1-inch display with 1024x600 screen resolution
- Intel GMA 950 graphics core

Installing and removing the application

This section contains step-by-step instructions for Kaspersky Anti-Virus installation and removal.

In this section

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 on your computer,*

On the installation CD, run the file with the .exe extension.

The application is then installed with the help of a standard Setup Wizard.

In some regions, the installation CD does not include the application installation package. The installation CD contains only the autorun file. When this file is executed, the application download window opens.

► *To install Kaspersky Anti-Virus using the autorun file:*

1. Click the **Download and Install** button in the application download window.

   By clicking the **Download and Install** button, you send information about the version of your operating system to Kaspersky Lab.

2. If the download failed, click the **Download and install manually from website** link that will take you to a website where you can download the application manually.

The application is then installed with the help of a standard Setup Wizard.

To install Kaspersky Anti-Virus, you can also download an installation package 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 browsers are installed to ensure safe Internet browsing.

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.

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 threats detected on your computer, running applications, and downloaded signed applications, as well as information about your operating system, to AO 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
  - Whether the user installing the application has administrator privileges

  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

The Activation Wizard is started at the first launch of Kaspersky Anti-Virus.

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

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

- **Activate application**. Select this option and enter an activation code (see the section "About the activation code" on page 47) if you have purchased a license for the application.

  If you specify an activation code for Kaspersky Internet Security or Kaspersky Total Security in the entry field, the procedure for switching to Kaspersky Internet Security or Kaspersky Total Security starts after activation is completed.

- **Activate trial version of the application**. Select this activation option if you want to install the trial version of the application before making a decision on whether to purchase a license. You will be able to use the application and all of its features during a short evaluation period. When the trial license expires, the trial version of the application cannot be activated for a second time.

An Internet connection is required for activation of the application.

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

Step 8. Registering a user

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

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

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

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

Installing the application from the command prompt

You can install Kaspersky Anti-Virus from the command prompt.

Command prompt syntax:

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

Detailed instructions and a list of installation settings are available on the Technical Support website (http://support.kaspersky.com/12257).

Getting started

In order for Kaspersky Anti-Virus to fully support browsers, the Kaspersky Protection extension has to be installed and enabled in browsers. Kaspersky Anti-Virus uses the Kaspersky Protection extension to inject a script into traffic. The application uses this script to interact with the web page. The application protects data transmitted by the script using a digital signature. Kaspersky Anti-Virus can embed the script without using the Kaspersky Protection extension.

> Kaspersky Anti-Virus signs data transmitted by the script using the installed anti-virus databases and requests to Kaspersky Security Network. The application sends requests to Kaspersky Security Network regardless of whether or not you accepted the terms of the Kaspersky Security Network Statement.

The Kaspersky Protection extension is installed in browsers during installation of Kaspersky Anti-Virus.

After installing Kaspersky Anti-Virus, you have to enable the Kaspersky Protection extension:

- To enable the extension in Mozilla™ Firefox™, you have to allow installation of the extension in the browser window.
- In Google Chrome™, you have to allow the Kaspersky Protection extension to be enabled. If you refuse to enable the extension, you will later need to install and enable the Kaspersky Protection extension manually by installing it from the Chrome™ web store.

In the Microsoft Internet Explorer, the Kaspersky Protection extension is enabled automatically.

If your computer is running the Windows 10 operating system, you have to install the Kaspersky Protection extension in the Microsoft Internet Explorer browser manually. You can proceed to installing the extension using the informational message in Notification Center (see the section "Assessing computer protection status and resolving security issues" on page 57).

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.

The application can be upgraded from a previous version automatically in the background if the **Download and install new versions automatically** option is selected in the **Update settings** window (**Settings** → **Additional**→ **Update**).

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 on your computer,*

On the installation CD, run the file with the .exe extension.

The application is then installed with the help of a standard Setup Wizard.

In some regions, the installation CD does not include the application installation package. The installation CD contains only the autorun file. When this file is executed, the application download window opens.

► *To install Kaspersky Anti-Virus using the autorun file:*

1. Click the **Download and Install** button in the application download window.

   By clicking the **Download and Install** button, you send information about the version of your operating system to Kaspersky Lab.

2. If the download failed, click the **Download and install manually from website** link that will take you to a website where you can download the application manually.

The application is then installed with the help of a standard Setup Wizard.

To install Kaspersky Anti-Virus, you can also download an installation package 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 browsers are installed to ensure safe Internet browsing.

Certain limitations apply to the upgrade from the previous version (see the section "Limitations and warnings" on page 102).

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.

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 threats detected on your computer, running applications, and downloaded signed applications, as well as information about your operating system, to AO 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
  - Whether the user installing the application has administrator privileges

  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.

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.

Switching from Kaspersky Anti-Virus to Kaspersky Internet Security or Kaspersky Total 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
- System Changes Control

- Network Monitor
- Webcam Access
- Private Browsing
- Anti-Spam
- Anti-Banner
- Secure Keyboard Input

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.

In certain regions, Kaspersky Anti-Virus allows switching to Kaspersky Total Security.

Kaspersky Total Security offers the same features as Kaspersky Internet Security and a range of additional features.

Kaspersky Total Security includes the following additional features:

- Backup and Restore
- Data Encryption
- Password protection

Switching to Kaspersky Total Security is performed in the same manner as switching to Kaspersky Internet Security.

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

In this section

Temporary use 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 purchase 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 **More 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 **Upgrade** option is not available in the **More 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 step, 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.

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 permanent use of Kaspersky Internet Security

If you want to switch to permanent use of Kaspersky Internet Security, you must purchase a license for Kaspersky Internet Security and then activate the application (see the section "Activating the application" on page 50).

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

1. Open the main application window.
2. In the **More 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** item is not available.

Removing the application

After removing Kaspersky Anti-Virus, your computer and personal data will be unprotected.

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

► *To start the Wizard on a computer with the Microsoft Windows 7 operating system or earlier versions,*

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

► *To start the Wizard on a computer with the Microsoft Windows 8 operating system or later versions:*

1. On the start screen, right click the Kaspersky Anti-Virus tile to call up the toolbar.
2. Click the **Uninstall** button on the toolbar.
3. In the window that opens, select Kaspersky Anti-Virus in the list.
4. Click the **Uninstall** button in the upper part of the list.

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** are files that contain information about objects that have already been scanned using iChecker technology.

Step 3. Confirming application removal

Since removing the application threatens the security of your computer and personal 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.

> This functionality may be unavailable in some regions.

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

Application licensing

This section covers the main aspects of application licensing.

In this section

About the End User License Agreement

The *End User License Agreement* is a binding agreement between you and AO Kaspersky Lab, 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.

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 must 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

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

The license has a limited term. License expiration may be followed by a grace period during which you may use all application features without limitations.

If you have not renewed your license (see the section "Renewing a license" on page 51), the application may switch to limited functionality mode (see the section "About limited functionality mode" on page 45) when the grace period expires. Some application features are unavailable in limited functionality mode. The duration of limited functionality mode depends on your region and licensing terms. When limited functionality mode expires, all application features become unavailable. You may find information about the grace period and limited functionality mode in the **Licensing** window, which opens by clicking the **License** link in the lower part of the main window.

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.

If you do not wish to renew protection of your computer, you can remove Kaspersky Anti-Virus (see the section "Removing the application" on page 39).

About limited functionality mode

The table below shows which Kaspersky Anti-Virus features are available and which are unavailable when the application is in limited functionality mode. If the value in the Limited functionality mode column is "yes", this means that the relevant functionality is available in limited functionality mode. If the value in the Limited functionality mode column is "no", the relevant functionality is unavailable. Additional information is available in the Restrictions column.

Table 2. Kaspersky Anti-Virus functionality in limited functionality mode

Functionality	Restrictions	Limited functionality mode
File Anti-Virus		yes
Virus scan	Scan can be started only manually. Scheduled scan and scan settings are unavailable.	yes
Vulnerability scan		no
Update databases and program modules	Settings cannot be configured.	yes
Protection against adware and spyware		yes
Web Anti-Virus	Works without restrictions.	yes
Mail Anti-Virus	Works without restrictions.	yes
IM Anti-Virus	Works without restrictions.	yes
Heuristic analysis	Works without restrictions.	yes
Protection against rootkits		no

Functionality	Restrictions	Limited functionality mode
Automatic Exploit Prevention		no
System Watcher		no
Protection against phishing		yes
Checking of the reputation of files and links in Kaspersky Security Network		yes
Additional protection and management tools		yes
URL Advisor		no
Secure Keyboard Input		no
Rescue Disk	Downloading via the application interface is available.	yes
Password protection of application settings		yes
Performance	Application performance settings can be configured.	yes
Task Manager	Task Manager only displays the scan results without providing tools for controlling the scan or its settings.	yes
Gaming Profile	Works without restrictions.	yes
Threats and Exclusions	Works without restrictions.	yes
Self-Defense	Works without restrictions.	yes
Quarantine	Works without restrictions.	yes

Functionality	Restrictions	Limited functionality mode
Notifications	Only the setting that controls delivery of Kaspersky Lab advertisements can be configured.	yes
"Protect a Friend"	All features of participation in the Protect a Friend program are available.	yes
Configuration of application appearance	Works without restrictions.	yes
My Kaspersky Account		yes
Remote management of your devices	Only view and manage activation codes	yes

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 91), 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

In order to enhance data protection and to improve the performance of Kaspersky Anti-Virus, you agree to automatically supply Kaspersky Lab with statistical and operational information, including but not limited to information about the hardware and software installed on the computer, license data, information about detected threats and infections, checksums of scanned objects, technical information about the computer and devices connected to it, and information about the activity of a device on the Internet. You can find more detailed information on the website (http://help.kaspersky.com).

If you participate in Kaspersky Security Network, you agree to automatically send to Kaspersky Lab the following information generated by Kaspersky Anti-Virus (http://help.kaspersky.com). You can view the Kaspersky Security Network Statement in the **Additional protection tools settings** window.

Kaspersky Lab protects any information received in this way as prescribed by law and applicable rules of Kaspersky Lab.

Kaspersky Lab uses any received information in anonymized form and as general statistics only. Aggregate statistics are automatically generated from the source information that is received, and do not contain any personal or other confidential data. The original information received is destroyed as new information is accumulated (once a year). Aggregate statistics are stored indefinitely.

Purchasing a license

You can purchase a license or renew an existing license. 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 50).

► *To purchase a license:*

1. Open the main application window.
2. Open the **Licensing** window in one of the following ways:
   - By clicking the **License is missing** link in the lower part of the main window if the application is not activated.
   - By clicking the **License** link in the lower part of the main window if the application is activated.
3. In the window that opens, click the **Purchase activation code** button.

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

Activating the application

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

If you did not activate the application during installation, you can do so later. You will be reminded about the need to activate the application by Kaspersky 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 portal. If you are not a registered user, complete the registration form to gain access to additional features.

   Registered users can perform the following actions:

   - Contact Technical Support and the Virus Lab
   - Manage activation codes
   - Receive information about new applications and special offers from Kaspersky Lab

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

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

Renewing a license

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

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

1. Open the main application window.
2. In the lower part of the main window, click the **License** link to open the **Licensing** window.
3. In the window that opens, in the **New activation code** section, click the **Enter activation code** button.

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

   Kaspersky 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.

Troubleshooting the operating system after infection

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

In this section

Recovering the operating system after infection

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

The Wizard checks whether there are any changes to the system, which can include access to the network being blocked, file name extensions for known formats being changed, Control Panel being blocked, etc. There are different reasons for these different kinds of damage. These reasons may include malware activity, incorrect system configuration, system failures, or malfunctioning applications for system optimization.

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

Troubleshooting the operating system by using the Microsoft Windows Troubleshooting Wizard

► *To run the Microsoft Windows Troubleshooting Wizard:*

1. Open the main application window.
2. In the **More 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 **Search for damage caused by malware activity** is selected and click the **Next** button.

Step 2. Problems search

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

Step 3. Select actions to fix damage

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

- *Strongly recommended actions*, which eliminate problems that pose a serious security threat. You are advised to repair all damage in this group.
- *Recommended actions* are aimed at repairing damage that may pose a threat. You are also advised to repair damage in this group.
- *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 damage within a group, click the ▸ icon to the left of the group name.

To get the Wizard to fix a specific type of damage, select the check box to the left of the damage description. By default, the Wizard fixes damage belonging to the groups of recommended and strongly recommended actions. If you do not want to fix a specific type of damage, clear the check box next to it.

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

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

Step 4. Fixing damage

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

Step 5. Wizard completion

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

About Rescue Disk

The rescue disk is a copy of Kaspersky Rescue Disk stored on a removable drive (a CD or USB device). You can use Kaspersky Rescue Disk for scanning and disinfecting infected computers that cannot be disinfected using other methods (for example, with anti-virus applications).

If you have purchased a boxed version of Kaspersky Anti-Virus, in addition to the Kaspersky Anti-Virus installation package the installation CD also includes Kaspersky Rescue Disk. You can use this installation CD as a Rescue Disk.

More details on using Kaspersky Rescue Disk are available on the Technical Support website (http://support.kaspersky.com/viruses/rescuedisk/main).

Managing application notifications

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

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

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

A notification can be closed automatically when the computer is restarted, when Kaspersky Anti-Virus is quit, or in Connected Standby mode in Windows 8. Notifications about the startup of applications are closed after 1 hour. When a notification is closed automatically, Kaspersky Anti-Virus performs the default recommended action.

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. The results of this processing are saved in a report.

Assessing computer protection status and resolving security issues

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

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

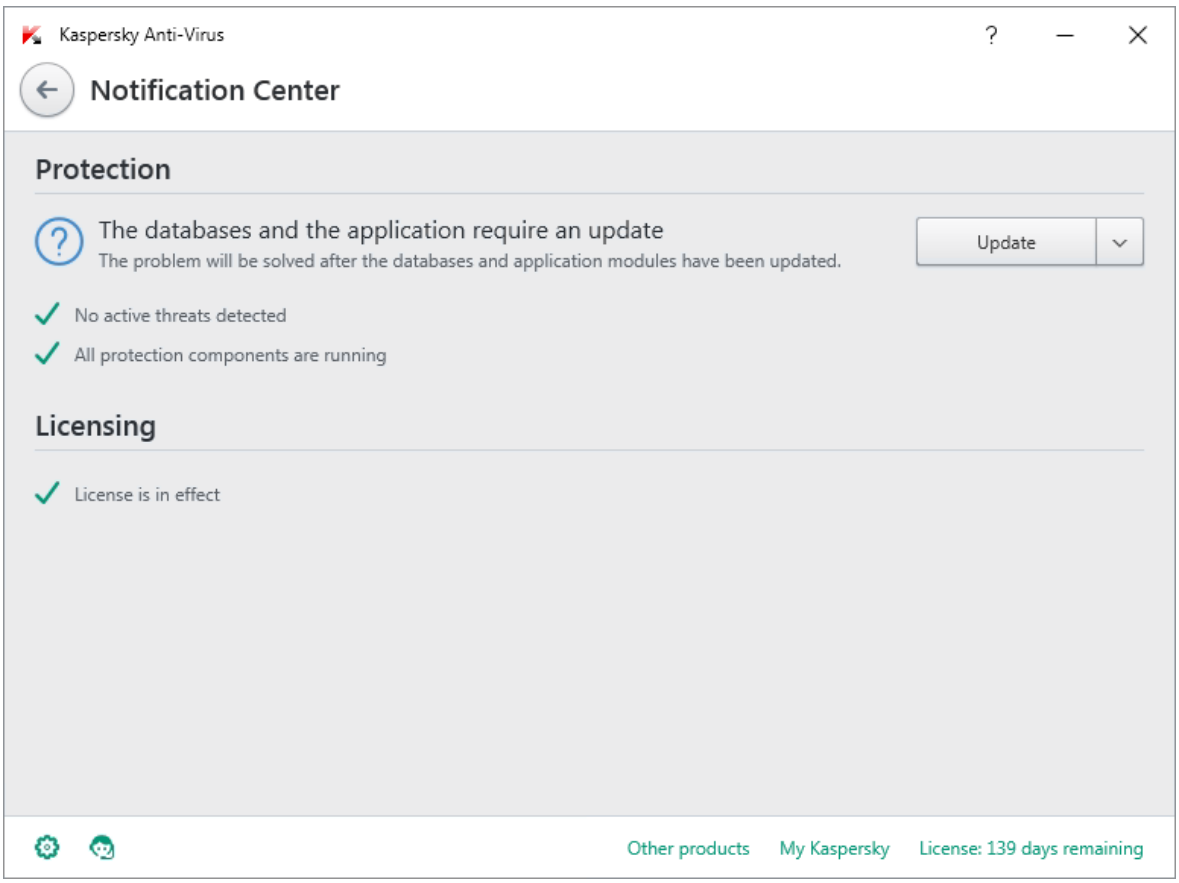

Figure 1. Notification Center window

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

Updating databases and application modules

This section contains information about database and application module updates.

In this section

About database and application module updates

The installation package of Kaspersky Anti-Virus includes databases and application modules. The application uses these databases to provide the *delivery security level*:

- Kaspersky Anti-Virus detects the majority of threats using Kaspersky Security Network, which requires an Internet connection.
- Kaspersky Anti-Virus does not detect adware, auto dialers, and other legitimate software that can be used by intruders to damage your computer or personal data.

To get full protection, we recommend updating the databases and application modules as soon as the application has been installed.

Databases and program modules are updated in stages:

1. Kaspersky Anti-Virus starts updating databases and application modules according to the specified settings: automatically, on schedule, or on demand. The application contacts an update source that stores a database and application module update package.
2. Kaspersky Anti-Virus compares the existing databases with the databases available at the update source. If the databases are different, Kaspersky Anti-Virus downloads the missing parts of the databases.

The application then uses the updated databases and application modules to scan the computer for viruses and other threats.

You can use the following update sources:

- Kaspersky Lab update servers
- HTTP or FTP server
- Network folder

Updates of databases and application modules are subject to the following restrictions and specifics:

- Databases become outdated after two days.
- To download an update package from Kaspersky Lab servers, an Internet connection is required.
- Updates of databases and application modules are unavailable in the following cases:
    - The license has expired, and the grace period or limited functionality mode is not available.
    - A metered mobile Internet connection is used. This limitation applies on computers running under Microsoft Windows 8 or more recent versions of this operating system if automatic updates or scheduled updates are enabled and a traffic limit has been set for a metered mobile connection. If you want the application to update databases and application modules in this case, clear the **Limit traffic on metered connections** check box under **Settings** → **Additional** → **Network**.
    - The application is used under subscription, and you have suspended your subscription on the website of the service provider.

Starting an update of databases and application modules

► *To start an update of databases and application modules,*

in the context menu of the application icon located in the taskbar notification area, select the **Update** item.

► *To run an update of databases and application modules from the main application window:*

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

   The **Update** window opens.

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

Scanning the computer

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

In this section

Full Scan

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

- System memory
- Objects loaded on operating system startup
- System backup storage
- 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:*

1. Open the main application window.
2. Click the **Scan** button.

   The **Scan** window opens.
3. In the **Scan** window, select the **Full Scan** section.
4. In the **Full Scan** section, click the **Run scan** button.

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

Selective Scan

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

You can start a Selective Scan in the following ways:

- From the context menu of the object
- From the main application window

► *To start a Selective Scan from the context menu of an object:*

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

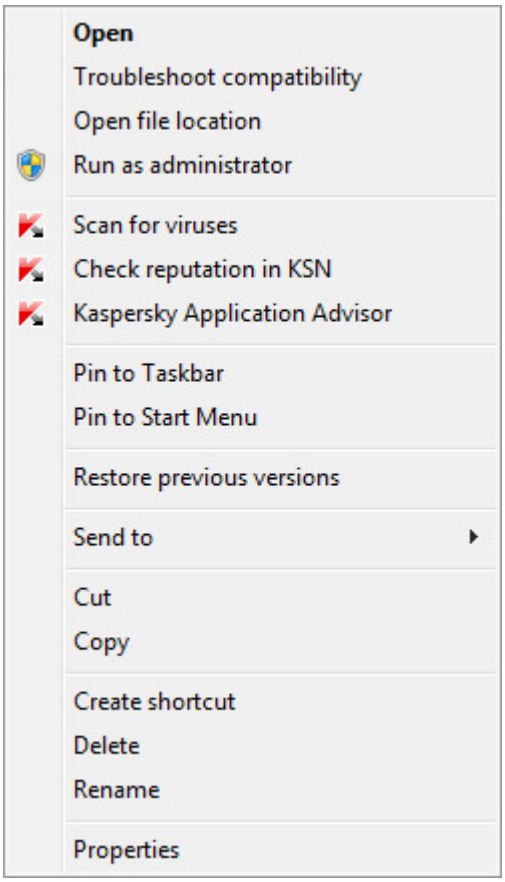

Figure 2. Object context menu

► *To start a Selective Scan from the main application window:*

1. Open the main application window.
2. Click the **Scan** button.

   The **Scan** window opens.
3. In the **Scan** window, select the **Selective Scan** section.
4. Specify objects to be scanned in one of the following ways:
   - Drag objects to the **Selective Scan** window.
   - Click the **Add** button and, in the file or folder selection window that opens, specify an object.
5. Click the **Run scan** button.

Quick Scan

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

- Objects loaded at the startup of the operating system
- System memory
- Disk boot sectors

► *To start a quick scan:*

1. Open the main application window.
2. Click the **Scan** button.

   The **Scan** window opens.
3. In the **Scan** window, select the **Quick Scan** section.
4. In the **Quick Scan** section, click the **Run scan** button.

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

Vulnerability Scan

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

► *To start a vulnerability scan:*

1. Open the main application window.
2. In the **More 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 **More 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.

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. Click the ⚙ button in the lower part of the window.

   The **Settings** window opens.
3. In the left part of the window, in the **Protection** section, select the Mail Anti-Virus component.

   The Mail Anti-Virus settings are displayed in the window.
4. Make sure that the switch in the upper part of the window that enables / disables Mail Anti-Virus, is enabled.
5. Select a security level:

   - **Recommended**. When this security level is set, Mail Anti-Virus scans incoming and outgoing messages and attached archives, and performs heuristic analysis with the **Medium scan** level of detail.
   - **Low**. If you select this security level, Mail Anti-Virus scans incoming messages only, without scanning attached archives.
   - **High**. When this security level is set, Mail Anti-Virus scans incoming and outgoing messages and attached archives, and performs heuristic analysis with the **Deep scan** level of detail.
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 65).

If Kaspersky Anti-Virus detects the password for the archive in the message text during scanning, the password is used to scan the contents of that archive for malware. The password is not saved. The archive is unpacked before scanning. If the application crashes while unpacking the archive, you can manually delete the files that are unpacked at the following path: %systemroot%\temp. The files have the PR prefix.

Protecting personal data on the Internet

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

In this section

About protection of personal data on the Internet

Kaspersky Anti-Virus helps you to protect your personal 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 personal 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 On-Screen Keyboard.

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

About On-Screen 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 personal data can be intercepted by hardware keyboard interceptors or keyloggers, which are programs that record keystrokes. The On-Screen 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. On-Screen Keyboard protects entered personal data from attempts to intercept it by means of screenshots.

On-Screen Keyboard has the following features:

- You can click the On-Screen Keyboard buttons with the mouse.
- Unlike hardware keyboards, it is impossible to press several keys simultaneously on On-Screen 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 On-Screen 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 On-Screen Keyboard, restart your computer after installing Kaspersky Anti-Virus.

The use of On-Screen Keyboard has the following limitations:

- On-Screen 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, On-Screen Keyboard does not protect entered personal data against interception.
- On-Screen Keyboard is not available in Microsoft Internet Explorer browser (versions 10 and 11) with the new Windows user interface style. In this case, we recommend opening On-Screen Keyboard from the interface of Kaspersky Anti-Virus.
- On-Screen 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.
- On-Screen 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 On-Screen Keyboard, the AutoComplete feature of Microsoft Internet Explorer stops functioning, since the implementation of the automatic input scheme may allow criminals to intercept data.

The preceding list describes the main restrictions in functionality for protection of data input. A full list of restrictions is given in an article on the Kaspersky Lab Technical Support website (http://support.kaspersky.com/12000). This article lists restrictions on Secure Keyboard Input in Kaspersky Internet Security, these restrictions apply also to On-Screen Keyboard in Kaspersky Anti-Virus.

Starting On-Screen Keyboard

You can open On-Screen Keyboard in the following ways:

- From the context menu of the application icon in the taskbar notification area
- From the application window
- From the toolbar of Microsoft Internet Explorer, Mozilla Firefox, or Google Chrome
- By pressing a combination of keyboard keys

► *To open On-Screen Keyboard from the context menu of the application icon in the taskbar notification area:*

Select **On-Screen Keyboard** (see figure below).

Figure 3. Kaspersky Anti-Virus context menu

► *To open On-Screen Keyboard from the application window:*

1. Open the main application window.
2. Click the **On-Screen Keyboard** button.

► *To open On-Screen Keyboard from the toolbar of Google Chrome, Microsoft Internet Explorer or Mozilla Firefox:*

1. Click the **Kaspersky Protection** button on the browser toolbar.
2. Select the **On-Screen Keyboard** item in the menu that opens.

► *To open the On-Screen Keyboard by using the hardware keyboard:*

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

Checking 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 *URL Advisor.*

> URL Advisor is not available in Microsoft Internet Explorer browser (versions 10 and 11) with the new Windows user interface style.

URL Advisor checks links on the web page opened in Microsoft Internet Explorer, Google Chrome or Mozilla Firefox. Kaspersky Anti-Virus displays one of the following icons next to the checked link:

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

To view a pop-up window with more details on the link, 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. Click the button in the lower part of the window.

   The **Settings** window opens.
3. In the **Protection** section, select the **Web Anti-Virus** subsection.

   The window displays the settings for Web Anti-Virus.
4. In the lower part of the window, click the **Advanced Settings** link. The advanced settings window of Web Anti-Virus opens.
5. In the **URL Advisor** section, select the **Check URLs** check box.
6. If you want Kaspersky Anti-Virus to scan the content of all websites, select **On all websites except those specified**.
7. If necessary, specify web pages that you trust in the **Exclusions** window. Open this window by clicking the **Manage exclusions** link. Kaspersky Anti-Virus does not scan the content of the specified web pages or encrypted connections with the specified websites.

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

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

    b. Click the **Configure checked websites** link to open the **Checked websites** window.

    c. Click the **Add** button.

    d. Enter the address of the web page whose content you want to check.

    e. Select the checking status for the web page (if the status is *Active*, Kaspersky Anti-Virus checks web page content).

    f. Click the **Add** button.

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

9. To configure the advanced settings for URL checking, in the **Advanced settings of Web Anti-Virus** window, in the **URL Advisor** section, click the **Configure URL Advisor** link to open the **URL Advisor** window.

10. If you want Kaspersky Anti-Virus to notify you about the safety of links on all web pages, in the **Checked URLs** section, select **All URLs**.

11. If you want Kaspersky Anti-Virus to display information about whether a link belongs to a specific category of website content (for example, *Profanity, obscenity*):

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

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

Kaspersky 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 confidential data contained in information 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 **More 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 traces search

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

Step 3. Selecting Privacy Cleaner actions

When the search is complete, the wizard informs you about the detected activity traces and asks about the actions to take for elimination of these activity traces (see the following figure).

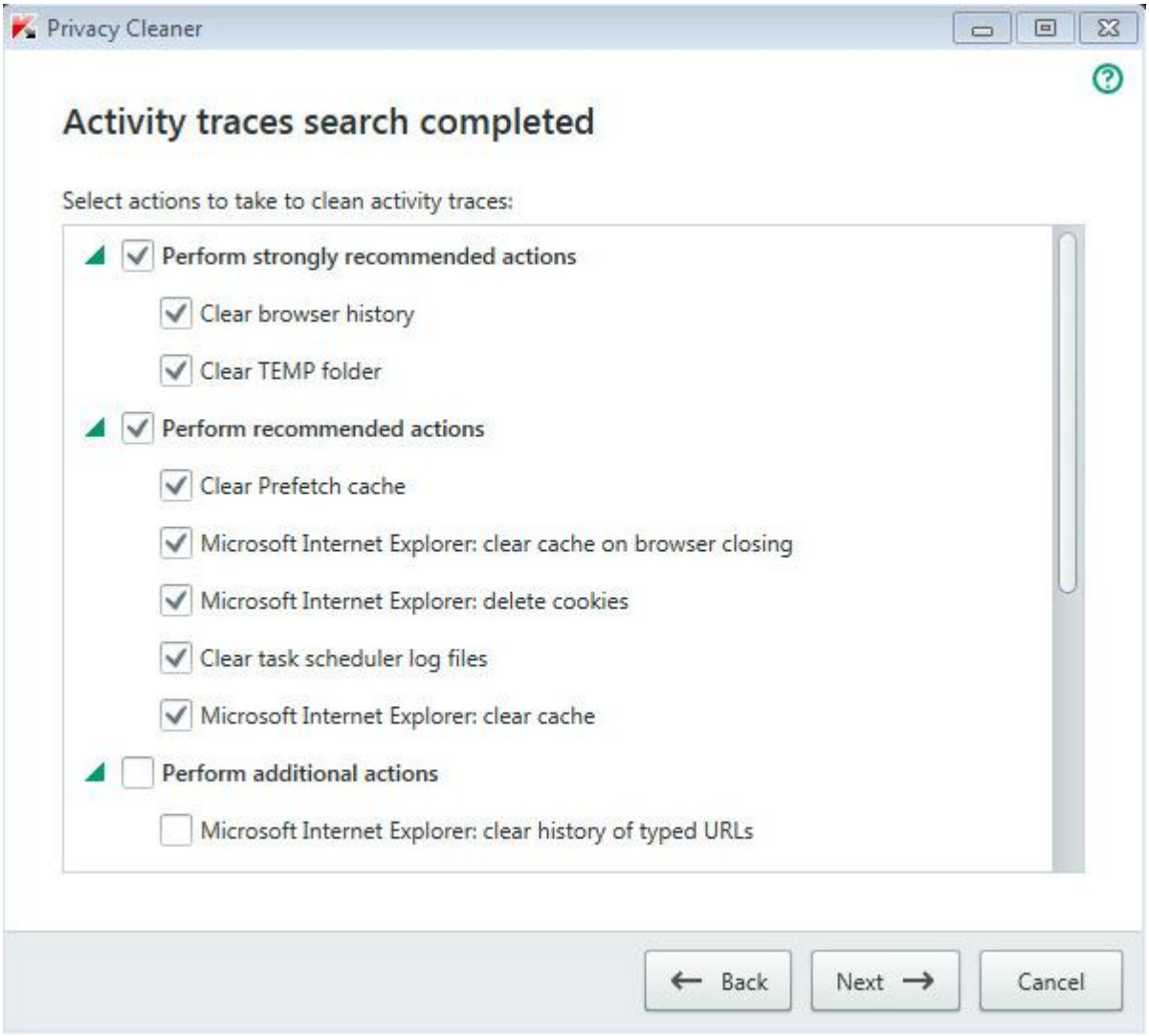

Figure 4. Activity traces detected and recommendations on eliminating them

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

The Wizard performs the actions selected during the previous step. Elimination of activity traces may take some time. To clean up certain activity traces, it may be necessary to restart the computer; if so, the Wizard notifies you.

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

Step 5. Wizard completion

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

Remote management of computer protection

This section describes how you can remotely manage protection of your computer with Kaspersky Anti-Virus installed.

In this section

About remote management of computer protection

If a computer has Kaspersky Anti-Virus installed, you can manage protection of this computer remotely. Computer protection can be managed remotely via My Kaspersky portal. To manage computer protection remotely, register on My Kaspersky portal, sign in to your My Kaspersky account, and go to **Devices** section.

My Kaspersky portal lets you accomplish the following computer security tasks:

- View the list of computer security problems and fix them remotely
- Scan the computer for viruses and other threats
- Update databases and application modules
- Configure Kaspersky Anti-Virus components

If a computer scan is started from My Kaspersky portal, Kaspersky Anti-Virus processes objects that are detected automatically without your involvement. On detecting a virus or other threat, Kaspersky Anti-Virus attempts to perform disinfection without rebooting the computer. If disinfection without restarting the computer is impossible, the list of computer security problems on My Kaspersky portal shows a message to the effect that the computer needs restarting to perform disinfection.

If the list of detected objects on My Kaspersky portal includes more than 10 items, they are grouped. In this case, the detected objects can be processed via the portal only together without the ability to examine each object separately. To view separately objects in this case, you are advised to use the interface of the application installed on the computer.

Detailed information on using the portal is available in My Kaspersky portal help (https://help.kaspersky.com/KPC/1.0/en-US/index.htm).

About My Kaspersky account

A *My Kaspersky account* is required to sign in to My Kaspersky portal https://center.kaspersky.com as well as to use the portal and certain Kaspersky Lab applications.

If you do not have a My Kaspersky account yet, you can create it on the portal or via applications compatible with the portal. You can also use accounts used with other Kaspersky Lab resources to sign in to the portal.

While creating a My Kaspersky account, you have to specify a valid email address and set a password. The password must contain at least 8 characters, one numeral, one uppercase letter, and one lowercase Latin letter. Blank spaces are not allowed.

> If the password is too weak or common, the account will not be created.

While creating an account, you can specify a secret question. This question provides additional security when recovering a forgotten password.

After your My Kaspersky account is created, you will receive an email message containing a link for activation of your account.

Please activate your My Kaspersky account within 7 days using the email link, otherwise your account will be deleted.

Proceeding to remote management of computer protection

► *To proceed to remote management of computer protection:*

1. Open the main application window.
2. In the **More Tools** drop-down list, select **Online Management**.
3. In the **Online Management** window, click the **Connect the computer to My Kaspersky** button.

   My Kaspersky portal logon form loads in the **Online Management** window, unless you have already logged on. Fill out the fields and log on to My Kaspersky portal.

   A connection to My Kaspersky portal may fail due to a portal malfunction. When this happens, Kaspersky Anti-Virus displays a notification about problems experienced by My Kaspersky portal that are being resolved by Kaspersky Lab staff. If you are unable to connect to My Kaspersky portal due to a portal malfunction, retry connecting later.

My Kaspersky portal page with the **Devices** section opens in the browser window by default.

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. Click the button in the lower part of the window.

   The **Settings** window opens.
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. Click the button in the lower part of the window.

   The **Settings** window opens.
3. In the left part of the window, select the **General** section and click the **Set up password protection** link to open the **Password protection** window.
4. In the window that opens, fill in the **New password** and **Confirm password** fields.
5. In the **Password scope** group of settings, specify the application actions to which you want to restrict access.

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

Pausing and resuming computer protection

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

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

► *To pause the protection of your computer:*

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

   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 computer 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.

3. Click the **Pause protection** button and confirm your choice in the window that opens.

► *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.

► *To run the Application Configuration Wizard:*

1. Open the main application window.
2. Click the button in the lower part of the window.

   The **Settings** window opens.
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

At this step, the application settings are reverted to the default settings configured by Kaspersky Lab.

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 application databases and modules have been updated during the same period, 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 filtering 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 drive).
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. Click the button in the lower part of the window.

   The **Settings** window opens.
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. Click the button in the lower part of the window.

   The **Settings** window opens.
3. In the **Settings** window, select the **General** section.
4. In the **Manage Settings** drop-down list, select **Import settings**.

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

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

Participating in Kaspersky Security Network (KSN)

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

Kaspersky Security Network (KSN) is an infrastructure of cloud 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.

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 (KSN) 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. Click the button in the lower part of the window.

   The **Settings** window opens.
3. In the **Additional** section, select **Additional protection and management tools**.

   The window displays details of Kaspersky Security Network and Kaspersky Security Network participation settings.
4. Enable or disable participation in Kaspersky Security Network by clicking the **Enable** / **Disable** buttons:

   - If you want to participate in Kaspersky Security Network, click the **Enable** button.

     A window with the text of the Kaspersky Security Network Statement opens. If you accept the terms of the Statement, click the **I agree** button.
   - If you do not want to participate in Kaspersky Security Network, 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 **More Tools** drop-down list, select **Cloud Protection**.

The **Cloud Protection** window shows the status of your connection to Kaspersky Security Network.

Participating in the Protect a Friend program

With the Protect a Friend program, you can collect bonus points and exchange them for an activation code for Kaspersky Anti-Virus. To do this, you must publish a download link on Twitter and on your page in social networks. This link allows your friends to download an installation package for Kaspersky 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.

The number of bonus points depends on the application version.

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

To log in to your profile in the Protect a Friend program, you must use the user name and password of your My Kaspersky account (see the section "About My Kaspersky account" on page 78). If you do not have a My Kaspersky account yet, you can create one when you open your Protect a Friend profile for the first time.

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.

In this section

Creating an account on My Kaspersky portal

To participate in the Protect a Friend program, you must create an account on My Kaspersky portal.

► *To create your My Kaspersky account:*

1. Open the main application window and, in the lower part of the window, click the **My Kaspersky** link.
2. Create and activate your My Kaspersky account:
    a. On the right part of the web page, enter an email address in the **Email** field.
    b. Enter a password and then re-enter it for confirmation in the **Password** and **Confirm password** fields. The password must contain at least eight characters.
    c. Click the **Register** button.

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

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

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

Logging in to your profile in the Protect a Friend program

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

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

   A web page opens, containing fields for signing up or logging in to My Kaspersky portal.

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

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

4. Go to the **Protect a Friend** section.

Read more about the rules of participation in the Protect a Friend program on My Kaspersky portal.

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 describes the ways to get technical support and the terms on which it is available.

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, we recommend that you contact Kaspersky Lab Technical Support. Technical Support specialists will answer any of your questions about installing and using the application.

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

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

- By telephone. This method allows you to consult with specialists from our Russian-language or international Technical Support.
- Send request from My Kaspersky portal. This method allows you to contact our specialists using the query form.

Technical support is available only to users who have purchased a license for use of the application. No technical support is provided to users of trial versions.

Technical support by phone

You can call Technical Support from most regions throughout the world. You can find information about how to obtain technical support in your region and contact information for Technical Support on the Kaspersky Lab Technical Support website (http://support.kaspersky.com/b2c#region2).

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

Getting technical support on My Kaspersky portal

My Kaspersky (https://my.kaspersky.com) is a one-stop online resource for managing the protection of your devices and activation codes for Kaspersky Lab applications and for requesting technical support.

To access My Kaspersky portal, you have to register. To do so, enter your email address and create a password.

You can receive technical support via My Kaspersky portal in the following ways:

- Send email requests to Technical Support
- Contact Technical Support without using email
- Track the status of your requests in real time

You can also view a complete history of your technical support requests.

Email request to Technical Support

You have to specify the following information in your email request to Technical Support:

- Message subject
- Application name and version number
- Operating system name and version number
- Problem description

A specialist from Technical Support will send an answer to your question to My Kaspersky portal and to the email address that you have specified during registration.

Collecting information for Technical Support

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

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

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

- Activate collection of extended diagnostic information
- Configure individual components of the application by changing special settings that are not accessible through the standard user interface
- Reconfigure storage and sending of collected diagnostic information
- Set up interception of network traffic and saving of network traffic to a file

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

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

In this section

Creating a system state report

► *To create a system state report:*

1. Open the main application window.
2. Click the  button in the lower part of the window.

   The **Support** window opens.
3. In the window that opens, click the **Support Tools** link to open the **Support Tools** window.
4. In the window that opens, click the **How to create an operating system state report** link to open a Knowledge Base article on how to create an operating system state report.
5. Follow the instructions in the Knowledge Base article.

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 (see the section "Getting technical support on My Kaspersky portal" on page 96). This number is available on My Kaspersky portal when you have an active request.

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

1. Open the main application window.
2. Click the button in the lower part of the window.

   The **Support** window opens.
3. Click the **Support Tools** link to open the **Support Tools** window.
4. In the window that opens, click the **Send report to Technical Support** link to open the **Send report** window.
5. Select the check boxes next to the data that you want to send to Technical Support.
6. Enter the number assigned to your request by Technical Support.
7. Click the **Send report** button.

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

If you were unable to send the files for any reason, the data files can be stored on your computer and later sent from My Kaspersky portal.

► *To save data files to disk:*

1. Open the main application window.
2. Click the button in the lower part of the window.

   The **Support** window opens.
3. In the window that opens, click the **Support Tools** link to open the **Support Tools** window.

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

5. Select the types of data to save to disk:

   - **Operating system information**. Select this check box to save information about the operating system of your computer to disk.

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

6. Click the **Save report** link to open the window for saving an archive with data files.

7. Specify the archive name and confirm saving.

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

Contents and storage of trace files

Trace files are stored on the computer openly for seven days after the writing of trace files is disabled. Trace files are deleted permanently after seven days.

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

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

Trace files can contain confidential data. You can view the contents of a trace file by opening it in a text editor (such as Notepad).

Running AVZ scripts

You are advised not to change the text of an AVZ script received from Kaspersky Lab experts. If problems occur during script execution, please contact Technical Support.

► *To run an AVZ script:*

1. Open the main application window.
2. Click the  button in the lower part of the window.

   The **Support** window opens.
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 to open the **Script execution** window.
5. Copy the text from the script sent by Technical Support specialists, paste it in the entry field in the window that opens, and click the **Run** button.

The script runs.

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

Limitations and warnings

Kaspersky Anti-Virus has a number of limitations that are not critical to operation of the application.

Limitations on upgrades from a previous version of the application

The application can be upgraded if the following versions of Kaspersky Anti-Virus are installed on your computer:

- Kaspersky Anti-Virus 2013
- Kaspersky Anti-Virus 2014
- Kaspersky Anti-Virus 2015
- Kaspersky Anti-Virus 2016

Upgrades from earlier versions of the application are not supported.

After an upgrade from a previous version of the application, Kaspersky Anti-Virus starts automatically even if automatic startup of the application is disabled in the settings that have been saved. When the operating system restarts afterwards, Kaspersky Anti-Virus does not start automatically if automatic startup of the application is disabled in the settings that have been saved.

When a previous version of Kaspersky Anti-Virus is upgraded, the following application settings are replaced with default settings:

- Kaspersky Anti-Virus display settings
- Scan schedule
- Participation in Kaspersky Security Network
- File Anti-Virus protection level
- Mail Anti-Virus protection level
- Update sources
- List of trusted web addresses
- URL Advisor settings

Limitations on the operation of certain components and automatic processing of files

Infected files are processed automatically according to rules created by Kaspersky Lab specialists. You cannot modify these rules manually. Rules can be updated following an update of databases and application modules.

Website certificate check and file scan limitations

When scanning a file, the application can contact Kaspersky Security Network for information about this file. If data from Kaspersky Security Network could not be retrieved, the application decides whether or not the file is infected based on local anti-virus databases.

Limitations of System Watcher functionality

Protection against cryptors (malware that encrypts user files) has the following limitations:

- The Temp system folder is used to support this functionality. If the system drive with the Temp folder has insufficient disk space to create temporary files, protection against cryptors is not provided. In this case, the application does not display a notification that files are not backed up (protection is not provided).
- Temporary files are deleted automatically when you close Kaspersky Anti-Virus or disable the System Watcher component.
- In case of an emergency termination of Kaspersky Anti-Virus, temporary files are not deleted automatically. To delete temporary files, clear the Temp folder manually. To do so, open the **Run** window (**Run** command under Windows XP) and in the **Open** field type `%TEMP%`. Click **OK**.

Encrypted connections scan limitations

Due to technical limitations of the implementation of scanning algorithms, scanning of encrypted connections does not support certain extensions of the TLS 1.0 protocol and later versions (particularly NPN and ALPN). Connections via these protocols may be limited. Browsers with SPDY protocol support use the HTTP over TLS protocol instead of SPDY even if the server to which the connection is established supports SPDY. This does not affect the level of connection security. If the server supports only the SPDY protocol and it is impossible to establish the connection via the HTTPS protocol, the application does not monitor the connection established.

Kaspersky Anti-Virus does not support processing of HTTPS/2 Proxy traffic. The application does not process traffic transmitted via extensions of the HTTP/2 protocol.

Kaspersky Anti-Virus monitors only those protected connection which it is able to decrypt. The application does not monitor connections added to the list of exclusions (**Websites** link in the **Network settings** window). The following components perform decryption and scanning of encrypted traffic by default:

- Web Anti-Virus
- URL Advisor

Kaspersky Anti-Virus decrypts encrypted traffic while the user is using the Google Chrome browser if the Kaspersky Protection extension is disabled in this browser.

Specifics of infected file processing by application components

By default, Kaspersky Anti-Virus can delete infected files that cannot be disinfected. Removal by default can be performed during file processing by such components as Mail Anti-Virus, File Anti-Virus, during scan tasks, and also when System Watcher detects malicious activity of applications.

Warning about changes in IM Anti-Virus functionality

Beginning with the 2016 version of Kaspersky Anti-Virus, the IM Anti-Virus component does not scan messages transmitted via the IRC protocol.

About personal data contained in report files

Report files are stored locally on your computer.

Path to report files: %allusersprofile%\Kaspersky Lab\AVP16.0.0\Report\Database.

Reports are stored in the following files:

- reports.db
- reports.db-wal
- reports.db-shm (does not contain any personal data)

Report files are protected against unauthorized access if self-defense is enabled in Kaspersky Anti-Virus. If self-defense is disabled, report files are not protected.

Report files can contain personal data obtained during operation of protection components, such as File Anti-Virus component, Mail Anti-Virus, and Web Anti-Virus.

Report files can contain the following personal data:

- IP address of the user's device
- Online browsing history
- Versions of the browser and operating system
- Names of cookies and other files and paths to them
- Email address, sender, message subject

Specifics of the Autorun process operation

The autorun process logs the results of its operation. Data is logged in text files named "kl-autorun-<date><time>.log". To view data, open the **Run** window (**Run** command under Windows XP) and in the **Open** field type %TEMP% and click **OK**.

All trace files are saved at the path to setup files that were downloaded during operation of the autorun process. Data is stored for the duration of operation of the autorun process and deleted permanently when this process is terminated. Data is not sent anywhere.

Kaspersky Anti-Virus limitations under Microsoft Windows 10 with the Device Guard mode enabled:

Operation of the following functionality is partly limited:

- Rootkit search and disinfection (postponed disinfection of files after computer restart; detection of malware that creates autorun keys in the registry)
- Heuristic Analysis (emulation of the startup of suspicious applications)

About logging of events in the Windows event log that are related to the License Agreement and Kaspersky Security Network

Events involving accepting and declining the terms of the License Agreement, and also accepting and declining participation in Kaspersky Security Network, are recorded in the Windows event log.

Limitations on local address reputation checks in Kaspersky Security Network

Links to local resources are not scanned in Kaspersky Security Network.

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 (protection, scan, updates of databases and application modules).

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 cloud 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 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 data, 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.

Protect a Friend profile

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

Protection components

Integral parts of Kaspersky Anti-Virus intended for protection against specific types of threats (for example, 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 advertisements.

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

The functions of the Kaspersky Lab application are implemented in the form of tasks, such as: Full Scan task or Update task.

Task settings

Application settings that are specific for each task type.

Threat level

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

- Static (such as information about the executable file of an application: size, creation date, etc.)
- Dynamic, which are used while simulating the application's operation in a virtual environment (analysis of the application's system calls)

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

Traces

Running the application in debugging mode; after each command is executed, the application is stopped, and the result of this step is displayed.

Traffic scanning

Real-time scanning that uses information from the current (latest) version of the databases for objects transferred over all protocols (for example, HTTP, FTP, and other protocols).

Trust group

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

In Kaspersky Anti-Virus, 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 rating

The index of user activity in use of Kaspersky Anti-Virus. The user rating is displayed in the Protect a Friend program 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.

AO Kaspersky Lab

Kaspersky Lab is a world-renowned vendor of systems protecting computers against various threats, including viruses and other malware, unsolicited email (spam), network and hacking attacks.

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 vendor of computer protection systems for home users in Russia ("IDC Endpoint Tracker 2014").

Kaspersky Lab was founded in Russia in 1997. It has since grown into an international group of companies with 34 offices in 31 countries. The company employs more than 3,000 skilled professionals.

PRODUCTS. Kaspersky Lab's products provide protection for all systems, from home computers to large corporate networks.

The personal product range includes security applications for desktop, laptop, and tablet computers, smartphones and other mobile devices.

The company offers protection and control solutions and technologies for workstations and mobile devices, virtual machines, file and web servers, mail gateways, and firewalls. The company's portfolio also features specialized products providing protection against DDoS attacks, protection for industrial control systems, and prevention of financial fraud. Used in conjunction with Kaspersky Lab's centralized management system, these solutions ensure effective automated protection for companies and organizations of any size 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 thousands of new computer threats, create tools to detect and disinfect them, and include signatures of those threats in the databases used by Kaspersky Lab applications.

TECHNOLOGIES. Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky Lab. It is no coincidence that many other developers use the Kaspersky Anti-Virus kernel in their products, including: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, ZyXEL. 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. Following tests and research conducted by the reputed Austrian test laboratory AV-Comparatives in 2014, Kaspersky Lab ranked among the top two vendors by the number of Advanced+ certificates earned and was eventually awarded the Top Rated certificate. But Kaspersky Lab's main achievement is the loyalty of its users worldwide. The company's products and technologies protect more than 400 million users, and its corporate clients number more than 270,000.

Kaspersky Lab website:	http://www.kaspersky.com
Virus encyclopedia:	http://www.securelist.com
Virus Lab:	http://newvirus.kaspersky.com (for analyzing suspicious files and websites)
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 and Chrome are Trademarks of Google, Inc.

Intel, Celeron, and Atom 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

A

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W