Kaspersky Internet Security for Mac

User Guide

APPLICATION VERSION: 14.0

Dear User!

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

Attention! This document is the property of Kaspersky Lab and all rights to this document are reserved by the copyright laws of the Russian Federation and international treaties. Illegal reproduction and distribution of this document or parts hereof will result in civil, administrative or criminal liability by applicable law.

Any type of reproduction and distribution of any materials, including translation thereof, is allowed only with the written permission of Kaspersky Lab.

This document and graphic images related to it can be used exclusively for information, non-commercial or personal purposes.

Kaspersky Lab reserves the right to change the document at any time without notice. You can find the latest version of this document at the Kaspersky Lab website, at http://www.kaspersky.com/docs.

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

Document revision date: 4/25/2013

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

CONTENT

ABOUT THIS GUIDE

This document is the User Guide for Kaspersky Internet Security for Mac.

For proper use of Kaspersky Internet Security users should be acquainted with the interface of the Mac OS X operating system, master basic OS X skills, and know how to use email and the Internet.

This guide is intended to:

- Help you install, activate, and use Kaspersky Internet Security.
- Ensure quick search of information on issues related to Kaspersky Internet Security.
- Describe additional sources of information about the application and ways of contacting Technical Support.

IN THIS SECTION:

IN THIS DOCUMENT

The Kaspersky Internet Security User Guide is comprised of the following sections:

Sources of information about the application (see page 9)

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

Kaspersky Internet Security (see page 11)

This section contains a description of the application's new features, and brief information on its components and functionality. It describes the delivery kit and the range of services available to registered users of the application. This section contains hardware and software requirements that a computer must meet to allow the installation of Kaspersky Internet Security.

Installing and uninstalling the application (see page 14)

This section provides step-by-step instructions on how to install and uninstall the application.

Application interface (see page 19)

This section describes the basic GUI components of Kaspersky Internet Security: application icon and context menu of the application icon, main application window and application preferences window, and Parental Control window. This section also describes notification windows and popup messages of the application.

Application licensing (see page 25)

This section contains information about the basic concepts of application activation. This section describes the purpose of the End User License Agreement, the ways to activate the application and renew the license.

Starting and stopping the application (see page 34)

This section provides you with information about how to start the application and quit it.

Computer protection status (see page 35)

This section provides information about how to detect threats to the computer's security and how to configure the security level. Read this section to learn more about how to enable and disable protection when using the application.

Solving typical tasks (see page 39)

This section contains step-by-step instructions on how to manage basic user tasks that the application can perform.

Working with the application from the command line (see page 46)

This section contains a detailed description of the use of the application and its components using the command line.

Contacting Technical Support Service (see page 54)

This section contains information about how to contact Technical Support and on what terms assistance can be provided.

Glossary

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

Kaspersky Lab ZAO (see page 59)

This section provides information about Kaspersky Lab.

Information about third-party code (see page 60)

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

Trademark notices (see page 61)

This section lists trademarks of third-party right owners used in this document.

Index

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

DOCUMENT CONVENTIONS

The text herein is accompanied by semantic elements that should be given particular attention – warnings, hints, and examples.

Document conventions are used to highlight semantic elements. Document conventions and examples of their use are shown in the table below.

Table 1. Document conventions

SAMPLE TEXT	DOCUMENT CONVENTIONS DESCRIPTION
Please note that...	Warnings are highlighted with red color and boxed. Warnings contain information about probable unwanted actions that may lead to data losses and failures in hardware or the operating system.
It is recommended to use...	Notes are boxed. Notes may contain useful hints, recommendations, specific values of some parameters, or important particular cases in the application's operation.
Example: ...	Examples are set out on a yellow background under the heading "Example".
Update means... The *Databases are out of date* event occurs.	The following semantic elements are italicized in the text: • new terms; • names of application statuses and events.
Command-A	The names of keys appear in a bold typeface. Key names joined by a "minus" sign represent key combinations.
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 accompanied by the arrow sign.
kav update	The following types of text content are set off with a special font: • text in the command line; • text of messages displayed on the screen by the application; • data that the user should enter.
<IP address of your computer>	Variables are enclosed in angle brackets. Instead of a variable, the corresponding value should be inserted, with angle brackets omitted.

SOURCES OF INFORMATION ABOUT THE APPLICATION

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

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

IN THIS SECTION:

SOURCES OF INFORMATION FOR UNASSISTED SEARCH

You can use the following sources for unassisted search of information about the application:

- application page at the Kaspersky Lab website;
- application page at the Technical Support website (Knowledge Base);
- online help.

If you cannot solve an issue on your own, we recommend that you contact the Technical Support Service at Kaspersky Lab (see section "Technical support by phone" on page 54). To use information sources on the website of Kaspersky Lab, an Internet connection is required.

Application page at the Kaspersky Lab website

Kaspersky Lab website contains an individual page for each application.

The web page (http://www.kaspersky.com/mac-security) provides general information about the application, its features and functions.

The page http://www.kaspersky.com contains a link to the eStore. Here you can purchase the application or renew your license.

Application page at the Technical Support website (Knowledge Base)

Knowledge Base is a section of the Technical Support website that contains recommendations on how to use Kaspersky Lab applications. Knowledge Base comprises help articles that are grouped by topics.

On the page of the application in the Knowledge Base (http://support.kaspersky.com/kismac), you can read articles that provide useful information, recommendations, and answers to frequently asked questions on how to purchase, install, and use the application.

The articles may provide answers to questions that are related not only to Kaspersky Internet Security but to other Kaspersky Lab products as well, or may contain Technical Support news.

To switch to the Knowledge Base, open the main application window (see page 20), click the button and click the **Technical Support Service** button in the window that opens.

Online help

The online help of the application comprises context help files.

The context help provides information about each window and tab of Kaspersky Internet Security: a list of parameters with descriptions and a list of tasks being solved.

Discussing Kaspersky Lab applications in the Forum

If your question does not require an urgent answer, you can discuss it with Kaspersky Lab specialists and other users on our Forum (http://forum.kaspersky.com/index.php?showforum=117).

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

Contacting the Sales Department

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

- By calling our HQ office in Moscow by phone (http://www.kaspersky.com/about/contactinfo).
- By sending a message with your question by email to sales@kaspersky.com.

The service is provided in Russian and English.

Contacting the Doc & Loc Unit

To contact the Doc & Loc Unit, send an email to docfeedback@kaspersky.com. Specify "Kaspersky Help Feedback: Kaspersky Internet Security for Mac" as the message subject.

KASPERSKY INTERNET SECURITY

Kaspersky Internet Security for Mac is intended for use on computers that run on Mac OS X, to protect your Mac against viruses and malware.

The application includes the following components:

File Anti-Virus

This component protecting the computer file system in real time: intercepts and analyzes attempts to access the file system; disinfects, deletes infected objects, and quarantine probably infected objects for further analysis.

Web Anti-Virus and Anti-Phishing

The component protects incoming and outgoing data transferred over HTTP or HTTPS. Checking links on web pages for phishing and dangerous URLs with the help of URL Advisor. Preventing interception of personal data entered at the keyboard by using Virtual Keyboard.

Parental Control

This component monitors the activity of different users on the computer and on the Internet. It can be used to restrict Internet access by limiting the time of Internet usage and restricting access to web resources and applications, create lists of contacts blocked or allowed for messaging over social networks, and monitor transmission of specific personal data. The component also lets you view user activity reports.

The following functions are implemented in the application:

Virus Scan

Finding and neutralizing viruses and malware on user request: finding and analyzing infected and probably infected objects in specified scanning areas, disinfecting, deleting, or quarantining objects for further analysis.

The most-used virus scan tasks are included in the Kaspersky Internet Security package: full computer scan and quick scan of critical areas.

Update

Updating databases of Kaspersky Internet Security from Kaspersky Lab update servers, creating backup copies of all updatable files to allow a future rollback. The application can also download and install new versions of Kaspersky Internet Security automatically.

Quarantine

Creating a copy of each infected object in Quarantine before disinfecting or deleting it, so that the object may be restored later.

Reports

Compiling a detailed report on the performance of each component of Kaspersky Internet Security.

Notifications

Notifying the user of certain events in Kaspersky Internet Security operation by using notification windows and pop-up messages that can be supplemented with audio notification.

Kaspersky Internet Security displays protection status messages during its operation. Protection Center (see section "Using Protection Center" on page 37), included in the application package, provides a complete picture of the computer's current protection status and troubleshooting options.

IN THIS SECTION:

DISTRIBUTION KIT

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

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

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

- sealed envelope with the setup CD that contains application files and documentation files;
- brief User Guide with an activation code;
- License agreement that stipulates the terms, on which you can use the application.

The contents of the distribution package may vary with the region in which the application is distributed.

If you purchase Kaspersky Internet Security at an online store, you copy the application from the website of the store. Information needed to active the application, including the activation code, will be emailed to you when you complete payment.

For more information about ways to purchase the application and about the distribution package, contact the Sales Department at sales@kaspersky.com.

USER SERVICE

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

- Database updates and new versions of the application
- Support on issues related to the installation, configuration and use of the application by phone or via email
- Announcements of new Kaspersky Lab releases and information about new viruses and outbreaks To use this service, you should be subscribed to the news delivery from Kaspersky Lab on the Technical Support Service website.

> No consulting services are provided on issues related to the functioning of operating systems, third-party software and technologies.

HARDWARE AND SOFTWARE REQUIREMENTS

To ensure that Kaspersky Internet Security functions properly, your computer should meet the following requirements:

- Operating system Mac OS X 10.6, 10.7, OS X 10.8;
- 350 MB free disk space (depending on the anti-virus databases size).

INSTALLING AND REMOVING THE APPLICATION

This section provides step-by-step instructions on how to install and uninstall the application.

The Kaspersky Internet Security distribution package includes the Installer and the Uninstaller.

IN THIS SECTION:

PREPARING FOR INSTALLATION

Before installing Kaspersky Internet Security on your computer, we recommend that you take these preparatory steps:

- Make sure that your computer meets the hardware and software requirements (see section "Hardware and software requirements" on page 13).
- Check the Internet connection on your computer. Internet access is required to log in to the website of Kaspersky Protection Center (see section "About Kaspersky Protection Center website" on page 15) using a Kaspersky Account (see section "About Kaspersky Account" on page 15), download a new version of Kaspersky Internet Security to the computer, activate the application using the activation code, and receive updates.
- Remove any other anti-virus applications to avoid system conflicts and maximize system performance.

INSTALLING THE APPLICATION

The following methods of installation are available:

- Installing the application downloaded from the Kaspersky Protection Center website using a Kaspersky Account (see section "Installing the application downloaded from the Kaspersky Protection Center website" on page 15).

  This is done using a Kaspersky Account (see section "About Kaspersky Account" on page 15). It lets you download a new version of Kaspersky Internet Security from the Kaspersky Protection Center website (see section "About Kaspersky Protection Center website" on page 15) and install it on the computer.

- Installing the application from a setup CD or a distribution package (see page 16).

  This is done using the Installation Assistant. It lets you check the Kaspersky Protection Center website (see section "About Kaspersky Protection Center website" on page 15) for a new version of Kaspersky Internet Security, download it to the computer, and install the application.

IN THIS SECTION:

INSTALLING THE APPLICATION DOWNLOADED FROM THE KASPERSKY PROTECTION CENTER WEBSITE

After you sign in to the Kaspersky Protection Center website (see section "About Kaspersky Protection Center website" on page 15) with your Kaspersky Account (see section "About Kaspersky Account" on page 15) and download the Kaspersky Internet Security.dmg file, a window with the contents of the distribution package opens automatically.

If the window with the contents of the distribution package has not opened automatically, open the folder containing the Kaspersky Internet Security.dmg file on your computer and run it manually.

➡ *To install Kaspersky Internet Security,*

in the window showing the contents of the distribution package, open the **Install Kaspersky Internet Security** installation package.

The Kaspersky Security Installation Assistant starts. The Installation Assistant downloads a new version of Kaspersky Internet Security from the Kaspersky Protection Center website and installs it on the computer (see section "Installing the application from a setup CD or a distribution package" on page 16).

ABOUT KASPERSKY ACCOUNT

A Kaspersky Account is needed to access the Kaspersky Protection Center website (see section "About Kaspersky Protection Center website" on page 15). Kaspersky Account is your key to all Kaspersky Lab services.

To proceed to creating a Kaspersky Account or signing it to the Kaspersky Protection Center website using an existing Kaspersky Account, open the main application window (see page 20), click the button, and click the **Kaspersky Account** button in the window that opens.

Kaspersky Account is your email address and password that you specified upon registration. The password must contain at least eight characters, one numeral, and one upper-case letter.

Once you have created your Kaspersky Account, an email with the account activation link is sent to the email address you have specified.

After activation, you can use your Kaspersky Account to access the Kaspersky Protection Center website.

ABOUT KASPERSKY PROTECTION CENTER WEBSITE

The Kaspersky Protection Center website is a single online resource for managing the protection of all your devices and the licensing of Kaspersky Lab products.

On the Kaspersky Protection Center website, you can buy a license or renew an existing license for Kaspersky Internet Security, download a new application version to your computer, and view information about the anti-virus databases used by the application.

You can sign in to the Kaspersky Protection Center website using your Kaspersky Account (see section "About Kaspersky Account" on page 15).

INSTALLING THE APPLICATION FROM A SETUP CD OR A DISTRIBUTION PACKAGE

The **License Agreement** and **Participation in Kaspersky Security Network** windows of the Installation Assistant are shown only for German- and Russian-language versions of Kaspersky Internet Security. In other cases, you can view the text of the License Agreement and information about participation in Kaspersky Security Network by clicking the corresponding links in the window of the Kaspersky Internet Security Installation Assistant.

➡ *To install Kaspersky Internet Security from a setup CD or a distribution package:*

1. Open the contents of the Kaspersky Internet Security distribution package.

   - If you have purchased a boxed version of the application, insert the setup CD into the disk drive;

   - If you have purchased Kaspersky Internet Security at an online store and downloaded the application distribution package in DMG format on the Kaspersky Lab website, open the DMG file.

2. In the window showing the contents of the distribution package, open the **Install Kaspersky Internet Security** installation package.

   The Kaspersky Security Installation Assistant starts. The Installation Assistant checks the Kaspersky Protection Center website for a new version of Kaspersky Internet Security.

3. Select an action following the check for a new version:

   - To skip the check for a new version of Kaspersky Internet Security on the Kaspersky Protection Center website, click the **Skip** button and then the **Install** button.

     The Installation Assistant starts installing Kaspersky Internet Security on the computer from the setup CD or distribution package.

   - If the Installation Assistant has detected a new version of Kaspersky Internet Security on the Kaspersky Protection Center website, you can install it after downloading it to the computer. To do so, click **Download and install** button.

   - If the Installation Assistant has not detected a new version of Kaspersky Internet Security on the Kaspersky Protection Center website, you can install the Kaspersky Internet Security version from the setup CD or distribution package. To do so, click the **Install** button.

4. In the **License Agreement** window, read through the text of the Kaspersky Internet Security End User License Agreement between you and Kaspersky Lab. After reviewing the text of the License Agreement, do one of the following:

   - If you accept the terms of the License Agreement, click the **Accept** button.

     Installation of Kaspersky Internet Security will continue.

   - If you do not accept the terms of the License Agreement, click the **Cancel** button.

     Installation will be aborted.

5. In the **Participation in Kaspersky Security Network** window, read information about participation in Kaspersky Security Network.

   When you participate in Kaspersky Security Network, information about new threats detected on your computer, started applications, applications with signatures being loaded, the unique ID of your copy of Kaspersky Internet Security, and system information, is automatically sent to Kaspersky Lab. It is guaranteed that personal data are not sent.

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

   If you do not accept the terms of participation in Kaspersky Security Network, clear the **I agree to participate in Kaspersky Security Network** check box.

   > As you use Kaspersky Internet Security subsequently, you can join Kaspersky Security Network at any time or opt out of participation in Kaspersky Security Network.

7. To proceed with installation of the application, click the **Install** button.

8. Confirm installation of Kaspersky Internet Security in the window prompting you for administrator account credentials.

   Kaspersky Internet Security starts installing on the computer.

9. Click the **Finish** button to exit the Installation Assistant.

Kaspersky Internet Security starts automatically when installation is complete. You do not have to restart the computer.

PREPARING THE APPLICATION FOR USE

After Kaspersky Internet Security is installed, you are recommended to do the following:

- Activate Kaspersky Internet Security (see section "Activating Kaspersky Internet Security" on page 31). Activating the application allows you to update the Anti-Virus databases and software modules regularly and provides access to Technical Support.

- Assess the current status of computer protection (see section "Assessing the status of computer protection" on page 35).

- Update Kaspersky Internet Security (see section "Updating application databases" on page 41).

- Start a full scan of the computer for viruses and other malware (see section "Performing a full scan of the computer for viruses" on page 39).

REMOVING THE APPLICATION

Removing Kaspersky Internet Security will expose your computer and personal data to security threats.

Before removing the application, we recommend restoring all quarantined objects. All unprocessed objects will be removed from Quarantine and cannot be restored.

➧ *To uninstall Kaspersky Internet Security:*

1. Open the contents of the Kaspersky Internet Security distribution package.

   - If you have purchased a boxed version of the application, insert the setup CD into the disk drive;

   - If you have purchased Kaspersky Internet Security at an online store and downloaded the application distribution package in DMG format on the Kaspersky Lab website, open the DMG file.

2. In the window showing the contents of the distribution package, open the **Uninstall Kaspersky Internet Security** installation package.

   Follow the steps to uninstall Kaspersky Internet Security.

3. In the **Introduction** window, click **Uninstall**.

4. Confirm removal of Kaspersky Internet Security in the window prompting you for administrator account credentials.

   The process of uninstalling Kaspersky Internet Security from the computer starts.

5. In the **Completion** window, read the information about the completion of the uninstallation process. Click the **Finish** button to quit the Uninstall Assistant.

No restart of the computer is necessary after Kaspersky Internet Security is uninstalled.

APPLICATION INTERFACE

This section describes the basic GUI components of Kaspersky Internet Security: application icon and context menu of the application icon, main application window and application preferences window, and Parental Control window. This section also describes notification windows and popup messages of the application.

IN THIS SECTION:

KASPERSKY INTERNET SECURITY ICON

As soon as Kaspersky Internet Security has been installed, the application icon appears in the menu bar. The application icon is an indicator of the application's operation. If the application icon is active, it means that real-time protection against malware is enabled for the computer. The inactive application icon indicates that the protection is disabled.

The Kaspersky Internet Security icon is always present in the menu bar. If an application window is opened, the Kaspersky Internet Security icon also appears on the **Dock** quick launch panel.

The context menu of the application icon provides access to the main commands of Kaspersky Internet Security:

- disabling computer protection;
- resuming computer protection;
- switching to the Protection Center;
- starting the update task;
- starting a quick scan;
- switching to the Parental Control preferences window;
- switching to the application preferences window.

➡ *To open the context menu of the Kaspersky Internet Security icon,*

click the application icon in the menu bar.

MAIN APPLICATION WINDOW

➡ *To open the main application window:*

1. In the menu bar, click the Kaspersky Internet Security icon.
2. In the application icon context menu that opens, select **Kaspersky Internet Security**.

Purposes of the main application window

The main window of Kaspersky Internet Security lets you view information about the status of computer protection, the operation of File Anti-Virus and Web Anti-Virus, and performance of virus scan and update tasks.

In the main application window you can also do the following:

- run virus scan tasks and update tasks;
- switch to application license management;
- open the Protection Center window, applications preferences window, and reports window;
- view news about Kaspersky Internet Security and protection against computer threats in general.

Controls of the main application window

There are three probable statuses of the computer protection (see section "Assessing the status of computer protection" on page 35).

The color of the computer protection indicator shows the current protection status:

- green indicates that your computer's protection is at an optimal level;
- yellow and red warn of the presence of various problems related to Kaspersky Internet Security configuration or operation.

For more detailed information about these problems and how to solve them, use the Protection Center (see section "Using Protection Center" on page 37). To open the Protection Center window, click the computer protection status indicator.

In addition to the computer protection status indicator, the left part of the main application window contains a block of text that describes the computer protection status and lists security threats detected by the Protection Center. If a virus scan or update task is running, information on their progress (percentage complete) will also be displayed in the left part of the application main window.

You can perform the following actions by using the buttons in the main application window:

🔄 Start Kaspersky Internet Security update. When the update is complete, detailed information about the performance of the update task is displayed in the reports window.

🔍 Switch to virus scan tasks: Quick Scan, Full Scan, and Virus Scan in a user-defined area. When the virus scan is complete, detailed information about task performance is displayed in the reports window.

🔑 Switch to the window displaying information about the license (see section "Viewing license information" on page 29), and obtain access to the application license management.

The top part of the main window contains a navigation panel. You can use the navigation panel to perform the following actions:

📊	Open the Kaspersky Internet Security reports window and access Quarantine.
⚙	Open the application preferences window (see page 21).
?	Open the Kaspersky Internet Security help system.
☺	Open the Technical Support window (see section "Contacting Technical Support Service" on page 54).
✉	Open the News Agent window with a list of news (see section "News Agent" on page 24). The button is displayed after Kaspersky Internet Security receives a news item.

The ▼ button is located in the lower part of the main window. Click the button to expand the panel that displays summary statistics for File Anti-Virus, as well as information about the anti-virus databases that are used by the application. To minimize the panel, click the ▼ button again.

The lower part of the main application window also contains operation indicators for File Anti-Virus, Web Anti-Virus and Parental Control. A green indicator means that the component is enabled; red means that a failure has occurred in component operation, and gray means that the component is disabled or has not been installed.

By using the buttons that are located next to the operation indicators of File Anti-Virus, Web Anti-Virus, and Parental Control, you can switch to configuration of those components.

APPLICATION PREFERENCES WINDOW

You can use one of the following methods to open the Kaspersky Internet Security preferences window:

- by clicking the ⚙ button in the main application window (see section "Main application window" on page 20);
- by selecting **Preferences** from the context menu of the Kaspersky Internet Security icon (see section "Kaspersky Internet Security icon" on page 19).

Application preferences can be accessed quickly using the following tabs in the upper part of the preferences window:

- **Protection**. You can configure File Anti-Virus and Web Anti-Virus preferences on this tab.
- **Virus Scan**. You can configure virus scan task preferences on this tab.
- **KSN**. You can connect to Kaspersky Security Network or opt out of participating in Kaspersky Security Network on this tab.
- **Threats**. You can select the categories of threats to be detected and form the trusted zone on this tab.
- **Update**. You can configure update task preferences on this tab
- **Reports**. You can configure the preferences of Kaspersky Internet Security reports and Quarantine on this tab.
- **Appearance**. On this tab, you can configure the way notification windows of Kaspersky Internet Security are displayed.

By using the 🔓 button, you can prohibit users without administrator rights from editing the preferences of Kaspersky Internet Security. This button is located in the lower part of the preferences window. You will need to enter the administrator's user name and password to remove the restrictions on modifying preferences.

The ? button provides access to the Kaspersky Internet Security help system with a description of the preferences for the current application window. You can also open the Help for the currently active application window by selecting **Open Help for This Window** in the **Help** menu.

PARENTAL CONTROL PREFERENCES WINDOW

You can use one of the following methods to open the Parental Control preferences window:

- select **Parental Control** from the context menu of the Kaspersky Internet Security icon (see section "Kaspersky Internet Security icon" on page 19).
- click the button located next to the indicator of Parental Control, in the lower part of the main application window (see section "Main application window" on page 20).

The left part of the Parental Control preferences window contains a list of user accounts on the computer. Next to the name of each account, a Parental Control indicator is displayed. A green-colored indicator means that Parental Control is enabled, while red means that Parental Control is disabled. By default, Parental Control is disabled for all user accounts on the computer. You can enable it.

If Parental Control is enabled for a user account, you can select the user operations on the computer and on the Internet that you want to control, by opening the **Preferences** tab in the right part of the Parental Control preferences window.

Kaspersky Internet Security controls the following user operations by categories:

- **Web Control** – control of visited websites and downloaded files.
- **Time Control** – control of Internet access time.
- **Personal Data** – control of use of personal data.
- **Social Networks** – control of use of social networks.

By default, control of user operations is disabled for all categories. You can enable control for each category of user operations separately, and proceed to detailed configuration of a selected category in the right part of the Parental Control preferences window.

On the **Reports** tab in the right part of the Parental Control preferences window, you can also view user action and activity reports for each user account that is covered by Parental Control, for each category individually.

Users cannot configure Parental Control without administrator rights on the computer. To configure and view reports on Parental Control, click the 🔒 button and enter administrator credentials.

NOTIFICATION WINDOWS AND POP-UP MESSAGES

Events having different levels of importance occur during the operation of Kaspersky Internet Security.

The application informs you of events with *notification windows* and *pop-up messages* that can be accompanied by sound notification.

> Kaspersky Internet Security supports Growl notifications. If Growl technology is enabled, it is used to display pop-up messages on screen.

IN THIS SECTION:

ABOUT NOTIFICATION WINDOWS

Kaspersky Internet Security displays notifications when the user needs to be prompted to choose an action in response to an event. For example, when the application detects a malicious object, it prompts you to delete or disinfect the object. A notification window disappears from the screen only after you select one of the actions.

ABOUT EVENT TYPES

Kaspersky Internet Security events are divided into three types in terms of their importance:

- **Critical** – events posing a dangerous threat to computer security (detection of malicious objects, vulnerabilities, Kaspersky Internet Security problems). Critical events require the immediate attention of the user. It is recommended not to disable critical event notifications.
- **Important** – events that do not require the immediate attention of the user, but may pose a threat to computer security in the future.
- **Informational events** – reference-type events.

ABOUT POP-UP MESSAGES

Kaspersky Internet Security displays *pop-up messages* to inform you of events that do not prompt you to select an action. Pop-up messages appear under the application icon in the menu bar and automatically disappear from the screen shortly after.

DISABLING NOTIFICATION DELIVERY

By default, Kaspersky Internet Security notifies (see section "Notification windows and pop-up messages" on page 23) you about all important events relating to the operation of the application. You can disable notification delivery or select types of events about which you do not want to be notified, as well as disable sound notifications.

Regardless of whether notification delivery is enabled or disabled, information about events that occur during the operation of Kaspersky Internet Security is logged in an application operation report.

➡ *To disable notification delivery:*

1. Click the ⚙ button in the main application window (see section "Main application window" on page 20).

   The application preferences window opens.

2. On the **Appearance** tab of the application preferences window, in the **Notifications** section clear the **Enable notifications** check box to stop receiving notifications in the form of notification windows.

➡ *To select types of events that you do not want to be notified of:*

1. Click the ⚙ button in the main application window (see section "Main application window" on page 20).

   The application preferences window opens.

2. On the **Appearance** tab of the application preferences window, in the **Notifications** section clear the check boxes opposite the types of events (see section "About event types" on page 23) about which you do not want to be notified.

➡ *To disable sound notifications that accompany notification windows and pop-up messages:*

1. Click the ⚙ button in the main application window (see section "Main application window" on page 20).

   The application preferences window opens.

2. On the **Appearance** tab of the application preferences window, in the **Notifications** section, clear the **Enable notification sound** check box.

NEWS AGENT

Using News Agent, Kaspersky Lab informs you of news related to Kaspersky Internet Security and protection against computer threats.

The application notifies you of news by displaying an icon ✉ in the top part of the main application window (see section "Main application window" on page 20). Clicking this icon opens the **News** window.

APPLICATION LICENSING

This section contains information about the basic concepts of application activation. This section describes the purpose of the End User License Agreement, the ways to activate the application and renew the license.

IN THIS SECTION:

ABOUT THE END USER LICENSE AGREEMENT

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

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

You can review the terms of the End User License Agreement when installing the Kaspersky Lab application.

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

ABOUT LICENSE

The license is a right to use the application, limited in time, and provided to you on the basis of the License Agreement. The unique activation code for your copy of Kaspersky Internet Security is linked to a license.

A license includes the right to receive the following types of services:

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

> The number of devices on which you are allowed to use the application is defined by the terms of the License Agreement.

- Assistance from Kaspersky Lab Technical Support.
- Benefiting other services provided by Kaspersky Lab or its partners during the entire validity term of the license (see section "Service for users" on page 13).

The scope of services and application usage term depend on the type of license that is used to activate the application.

The following license types are available:

- *Trial* – a free license intended for getting acquainted with the application.

  The trial license usually features a short validity term. As soon as the trial license expires, all Kaspersky Internet Security features are disabled. To continue using the application, you need to buy a commercial license.

- *Commercial* – a paid license provided when purchasing the application.

  When the commercial license expires, the application keeps running in limited functionality mode. You are still allowed to use all of the application components and perform scanning for viruses and other malware, but only using databases that were installed before the license expiration date. To continue using Kaspersky Internet Security in fully functional mode, you must renew the commercial license.

  You are advised to renew your license on the day it expires, or earlier, to ensure maximum protection against all security threats.

- *Commercial with subscription for updates* and *commercial with subscription for updates and protection* – a pay-for license that lets you manage subscription flexibly: you can pause or resume subscription, renew it automatically, or cancel your subscription. Licenses with subscription are distributed by vendors. Subscription can be managed via the user's personal workspace on the website of the vendor.

  Subscription can be limited (for one year, for example) or unlimited (without an expiry date). Limited subscription needs to be renewed manually when it expires. Unlimited subscription is renewed automatically if the vendor's services have been prepaid on time.

  In the case of limited subscription, upon its expiry you will be offered a grace period for renewing subscription, during which time the application will retain its functionality.

  If subscription has not been renewed, after the grace period is over Kaspersky Internet Security stops updating the application databases (in the case of a license with subscription for updates) and stops protecting computer and running scan tasks (in the case of a license with subscription for updates and protection).

  When you use subscription, you cannot use a different activation code for renewing the license. This will become possible only after your subscription expires.

  If at the time of subscription activation Kaspersky Internet Security is already being used under a valid license of another type, the valid license will be replaced with the license with subscription. To cancel your subscription, contact the vendor from which you bought Kaspersky Internet Security.

> The possible subscription management options may vary with each vendor. Some vendors may also choose not to provide a grace period during which subscription can be renewed.

ABOUT THE ACTIVATION CODE

The activation code is a code that you receive when purchasing a commercial license for Kaspersky Internet Security. This code is required for activation of the application.

An activation code is a unique combination of 20 Latin alphanumeric characters in the form xxxxx-xxxxx-xxxxx-xxxxx.

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

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

The license period countdown starts from the date when you activate the application. If you have purchased a license that allows using Kaspersky Internet Security on several devices, the license countdown starts when you apply the activation code for the first time.

If you have lost or accidentally deleted your activation code after the activation, contact Technical Support Service at Kaspersky Lab.

ABOUT DATA SUBMISSION

By accepting the terms of the License Agreement, you agree to submit information about the installation, application version and preferences, and activation to Kaspersky Lab, which is done to improve real-time protection.

When you participate in Kaspersky Security Network, the following information obtained as a result of Kaspersky Internet Security operation is automatically sent from the computer to Kaspersky Lab:

- Information about computer hardware and software, including the operating system version and service packs install, and objects downloaded.
- Information about the anti-virus protection status of the computer, as well as all potentially malicious objects and actions (including the name of the detected object, checksum (MD5), date and time of detection, the URL address from which it was downloaded, the names and sizes of infected files and paths to them, the IP address of the attacking computer and the number of the computer port targeted by the network attack, list of malware activity, potentially malicious URLs) and the decisions taken by the product and the user on them.
- Information about applications downloaded by the user (URL, attributes, file size, information about the process that downloaded the file).
- Information about the applications launched and their modules (size, attributes, creation date, PE header details, region, name, location, packers).
- Information about interface errors and usage of the interface of the installed Kaspersky Lab product.

If Kaspersky Internet Security returns an error, the user can send a file containing the following data to Kaspersky Lab:

- Process name and ID
- Path to the executable module
- Application version
- Bit version of the process (32- or 64-bit)
- Parent process name and ID
- Application crash date and time
- Operating system version
- Report version
- Type of error that caused the application crash

- Error information
- Number of the thread in which the error occurred
- Call stacks for each thread during the application crash (frame number, module name, address in the code, name of the function at the corresponding address)
- Registry values of the thread in which the error occurred
- List of loaded modules with the address at which the module is loaded, module name, module version, UUID, and path to the module

The following information is additionally transmitted in the case of the Mountain Lion operating system:

- User ID (UID)
- Call statistics of specific system calls for interaction of other processes with this process
- Memory distribution (statistics of the amount of memory allocated for specific areas)

Files or their parts which may be exploited by intruders to harm the computer or data can be also sent to Kaspersky Lab to be examined additionally.

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

VIEWING LICENSE INFORMATION

➡ *To view information about your license,*

open the main application window (see page 20) and click the 🔑 button.

The **License** window opens.

The **License** window that has opened contains the following application licensing information:

- License number
- License type (commercial, trial, subscription for updates, or subscription for updates and protection)
- Key type (active or backup)
- Key status (blocked, corrupted, expired or suspended)
- Subscription status (active, activated, expired, blocked or suspended)
- Limitation on the number of computers on which the application can be used
- License expiry date and time
- Number of days until license expiry

If there is no license, Kaspersky Internet Security will notify you of this. If the application is not activated, you can start the activation procedure (see section "Activating Kaspersky Internet Security" on page 31). If you use the trial license, you can purchase the commercial license (see section "Purchasing a license" on page 29).

You can add two keys under a commercial license: active and reserve. The active key starts functioning as soon as the application is activated. The reserve key comes into operation right after the commercial license linked to the active key expires. If no reserve key has been added and the commercial license linked to the active key is about to expire, you can renew it (see section "Renewing a license" on page 30).

If your subscription for Kaspersky Internet Security has expired and the grace period during which subscription renewal is available is over, you can renew your subscription manually (see section "Renewing subscription" on page 30). When using subscription, you can also update subscription status (see page 30).

PURCHASING A LICENSE

If you do not have any license for Kaspersky Internet Security, or if the application has been activated using a trial license, you can purchase a commercial license.

➡ *To purchase a license:*

1. Open the main application window (see page 20) and click the 🔑 button.
2. In the window that opens, click the **Purchase** button.

This opens a webpage with information on the terms of license purchases through the Kaspersky Lab eStore or Kaspersky partners. On purchasing a license at Kaspersky Lab eStore, an activation code for Kaspersky Security (see section "About the activation code" on page 26) will be sent to your email address specified in the order form.

RENEWING A LICENSE

An application license needs to be renewed when the active commercial license that is linked to the active key expires, if no reserve key has been added. If the license is not renewed, Kaspersky Internet Security continues to perform all functions, but without updates of the anti-virus databases.

➡ *To renew a license:*

1. Open the main application window (see page 20) and click the 🔑 button.
2. In the window that opens, click the **Renew** button.

This opens a webpage with information on the terms of license renewal through the Kaspersky Lab eStore or Kaspersky partners. On purchasing a license at Kaspersky Lab eStore, an activation code for Kaspersky Internet Security (see section "About the activation code" on page 26) will be sent to your email address specified in the order form.

RENEWING SUBSCRIPTION

When you use subscription, Kaspersky Internet Security automatically contacts the activation server at specific intervals to keep your subscription up-to-date during the entire subscription term.

If the active key has expired, Kaspersky Internet Security checks the activation server for a renewed key in background mode (without user involvement) and adds it by replacing the previous key. In this way, unlimited subscription for Kaspersky Internet Security is renewed without user involvement.

If you subscription has expired and the grace period during which subscription renewal is available is over, Kaspersky Internet Security notifies you accordingly and stops attempting to renew subscription automatically. Kaspersky Internet Security stops updating the application databases (in the case of a license with subscription for updates) and stops protecting computer and running scan tasks (in the case of a license with subscription for updates and protection).

You can renew your subscription manually by contacting the vendor that sold you Kaspersky Internet Security.

➡ *To renew subscription:*

1. Open the main application window (see page 20) and click the 🔑 button.
2. In the window that opens, click the **Visit Service Provider Website** button.

This page shows complete information on the terms of subscription renewal.

UPDATING SUBSCRIPTION STATUS

When using subscription, you can contact the activation server for information on the key used.

Subscription status needs to be updated when subscription has not been renewed automatically for some reason (for example, the computer was turned off the entire time that subscription renewal was available). Until subscription renewal, Kaspersky Internet Security stops updating the application databases (in the case of a license with subscription for updates) and stops protecting computer and running scan tasks (in the case of a license with subscription for updates and protection).

➡ *To update subscription status:*

1. Open the main application window (see page 20) and click the 🔑 button.
2. In the window that opens, click the **Update Subscription Status** button.

ACTIVATING KASPERSKY INTERNET SECURITY

Before activating Kaspersky Internet Security, make sure that the current system date value on your computer matches the actual date and time.

Activating the application requires you to add a key file, which is used to verify the license to use Kaspersky Internet Security.

If the application has not been activated, all options of Kaspersky Internet Security are available, except the retrieval of updates. An unactivated application can be updated only once after installation.

IN THIS SECTION:

ACTIVATING THE APPLICATION USING THE TRIAL LICENSE

You can activate the application by using the trial license only if the installed version of Kaspersky Internet Security has never been installed on your computer.

You are advised to activate the application using a trial license if you want to get acquainted with the application before deciding whether to purchase a commercial license. To activate the application under a trial license, you will be provided a free key with a validity term limited under the terms of the trial license.

Your computer must be connected to the Internet when activating the application by using the trial license. If an Internet connection is currently unavailable, you can activate the trial version of the application later.

➧ *To activate the application by using the trial license:*

1. Open the main application window (see page 20) and click the 🔑 button.
2. In the window that opens, click the **Try** button.
3. In the **Activate Trial Version** window click the **Activate Trial Version** button.

   Kaspersky Internet Security connects to Kaspersky Lab servers and sends data for verification. If verification is successful, the application receives and adds a key with a validity term limited under the terms of the trial license.

   After the application has been activated successfully under the trial license, the **License** window opens where you can view the following information:

   - Key type (active)
   - License type (trial)
   - Limitation on the number of computers on which the application can be used
   - License expiry date and time

- Number of days until license expiry

4. Click the **Finish** button to return to the main application window (see page 20).

When the trial license expires for the installed version of Kaspersky Internet Security, a corresponding notification appears on the screen. To continue using the application, you can purchase the commercial license (see section "Purchasing a license" on page 29).

ACTIVATING THE APPLICATION WITH AN ACTIVATION CODE

This activation option is recommended if you have bought a commercial license for the application, a license with subscription for updates, or a license with subscription for updates and protection, and you have been provided an activation code. Using the activation code, you will obtain a key that provides access to the functionality of Kaspersky Internet Security throughout the license validity period.

Your computer must be connected to the Internet. If an Internet connection is currently unavailable, you can activate the trial version of the application later.

➡ *To activate the application with your activation code:*

1. Open the main application window (see page 20) and click the 🔑 button.
2. In the window that opens, click the **Activate** button.
3. In the **Application Activation** window, enter the activation code that you received when purchasing Kaspersky Internet Security.

   The activation code is a sequence of numbers and letters, separated by hyphens, in four groups of five characters without spaces, for example: 11AA1-11AAA-1AA11-1A111. The activation code must be entered using Latin characters.

   Kaspersky Internet Security connects to Kaspersky Lab servers and sends the activation code for verification. If the activation code is verified, the application downloads and adds the key file.

   Depending on the activation code provided, Kaspersky Internet Security may prompt the user for filling in a mandatory or optional registration form or for registering in the My Kaspersky Account (see section "Contacting Technical Support Service from My Kaspersky Account" on page 55).

   If the activation code is not verified, the Assistant will display this information on the screen. In this case, contact the software vendor from which you purchased Kaspersky Internet Security for details.

After the application has been activated successfully using the activation code, the **License** window opens where you can view the following information:

- License number
- Key type (active or backup)
- Subscription status
- License type (commercial, subscription for updates, or subscription for updates and protection)
- Limitation on the number of computers on which the application can be used
- License expiry date and time
- Number of days until license expiry

4. Click the **Finish** button to return to the main application window (see page 20).

STARTING AND STOPPING THE APPLICATION

This section provides you with information about how to start the application and quit it.

The application starts up immediately after the installation, and the Kaspersky Internet Security icon (on page 19) appears in the Menu Bar.

➧ *To quit Kaspersky Internet Security,*

click the Kaspersky Internet Security icon (see page 19) in the menu bar. In the context menu that opens, select **Quit**.

The application's operation will stop and the process will be discarded from the computer's RAM.

After Kaspersky Internet Security quits, the computer keeps running in unprotected mode and may become infected, thus placing your personal data at risk of loss.

COMPUTER PROTECTION STATUS

This section provides information about how to detect threats to the computer's security and how to configure the security level. Read this section to learn more about how to enable and disable protection when using the application.

Your computer's protection status indicates the presence or absence of threats, giving you a summary of your computer's overall security level. These threats include detected malicious programs, outdated anti-virus databases, and disabling of File Anti-Virus or Web Anti-Virus.

The Protection Center (see section "Using Protection Center" on page 37) helps you review all the current threats and start neutralizing them.

IN THIS SECTION:

ASSESSING THE STATUS OF COMPUTER PROTECTION

The computer protection status indicator located in the right part of the main application window informs you of problems with computer protection (see section "Main application window" on page 20). Depending on the condition of computer protection, the color of the indicator may change. If any security threats are detected, the change of the indicator color is supplemented with a message about threats.

The indicator can take the following values:

- **Green**. Your computer's protection is at the appropriate level.

  A green indicator signifies that the application anti-virus databases are up to date and all application components have been configured as recommended by Kaspersky Lab. No malicious objects have been detected, or detected malicious objects have been neutralized. Parental Control runs in standard mode.

- **Yellow**. The level of computer protection is reduced.

  A yellow indicator signifies a problem with Kaspersky Internet Security. Such problems include, for example: slight deviations from the recommended operation preferences or that the application databases have not been updated for several days.

- **Red**. Your computer is at risk of infection.

  A red indicator signifies that there are dangerous problems that may lead to the infection of your computer and loss of data. For example, the anti-virus databases of the application are obsolete, the application is not activated, or malicious objects have been detected.

You are advised to fix the problems and security threats immediately. You can click the computer protection status indicator in the main application window to open the Protection Center window (see section "Using Protection Center" on page 37), which provides detailed information about the computer protection status and suggests scenarios for neutralizing problems and threats.

DISABLING COMPUTER PROTECTION

By default, Kaspersky Internet Security is stated when the operating system loads and protects your computer until it is switched off. All the protection components (File Anti-Virus and Web Anti-Virus) are enabled and running.

You can fully or partially disable the protection that is provided by Kaspersky Internet Security.

> Kaspersky Lab strongly recommends that you do not disable the real-time protection provided by File Anti-Virus and Web Anti-Virus, since this may lead to infection of your computer and data loss.

The following signs indicate that computer protection is disabled:

- inactive application icon (see section "Kaspersky Internet Security icon" on page 19) in the Menu bar;
- red color of the computer protection status indicator in the right part of the main application window.

> Computer protection is looked at in the context of File Anti-Virus and Web Anti-Virus. Disabling or pausing those protection components does not impact virus scan tasks or the update task.

You can completely disable computer protection by using one of the following methods. You can disable protection components on the **Protection** tab of the application preferences window.

➡ *The following methods can be used to disable computer protection:*

- In the menu bar, click the Kaspersky Internet Security icon (see page 19). In the context menu that opens, select **Disable protection**.
- Open the application preferences window (see page 21), select the **Protection** tab and clear the **Enable protection** check box in the **General** section.

> If you have disabled computer protection, it will not be re-enabled automatically when Kaspersky Internet Security starts again. Computer protection should be enabled manually (see section "Restoring protection on your computer" on page 37).

➡ *To disable a protection component:*

1. Click the ⚙ button in the main application window (see section "Main application window" on page 20).

   The application preferences window opens.

2. On the **Protection** tab of the application preferences window, in the **<component name>** section, clear the **Enable <component name>** check box.

> If you have disabled a protection component, it will not be re-enabled automatically when Kaspersky Internet Security starts again. The protection component should be enabled manually (see section "Restoring protection on your computer" on page 37).

RESTORING COMPUTER PROTECTION

If computer protection or a protection component (File Anti-Virus or Web Anti-Virus) has been disabled, it can be re-enabled only manually, at the user's request. Computer protection or a protection component will not be re-enabled automatically when Kaspersky Internet Security is started again.

➡ *The following methods can be used to enable computer protection:*

- In the menu bar, click the Kaspersky Internet Security icon (see page 19). In the context menu that opens, select **Enable protection**.
- Open the application preferences window (see page 21), select the **Protection** tab, and select the **Enable protection** check box in the **General** section.

➡ *To enable a protection component:*

1. Clicking the ⚙ button in the main application window (see section "Main application window" on page 20).

   The application preferences window opens.

2. On the **Protection** tab of the application preferences window, in the **<component name>** section, select the **Enable <component name>** check box.

Also, to enable computer protection or protection components, you can use the Protection Center (see section "Using Protection Center" on page 37). Disabling computer protection or disabling protection components dramatically increases the risk of computer infection. Therefore, information about instances of disabled protection is stored in the Protection Center.

USING PROTECTION CENTER

Protection Center is a service for analyzing and fixing the existing problems and computer security threats.

➡ *To open the Protection Center,*

click the computer protection status indicator in the main application window (see section "Main application window" on page 20).

In the Protection Center window you can view a list of existing problems and security threats. Problems and threats are grouped by categories. For each problem or threat, actions are suggested that you can perform to resolve the problem or threat. You can fix a problem or neutralize a threat immediately or do this later.

➡ *To fix a problem or neutralize a threat immediately,*

click the button with the name of the recommended action to fix the problem or neutralize the threat.

For example, if infected objects have been detected on the computer, you should click the **Disinfect** button. If the anti-virus databases used by the application are out of date, you should click the **Update** button. The application performs the chosen operation.

➡ *To fix the problem or neutralize the threat later,*

click the **Hide** button.

The problem or threat notification will be hidden in the list. You can return to neutralizing this threat later.

You cannot postpone neutralizing dangerous computer security threats. Examples of dangerous threats include unprocessed malicious objects, protection component faults, or corrupted databases of Kaspersky Internet Security.

If you close the Protection Center without neutralizing dangerous threats, the color of the computer protection status indicator in the main application window continues to indicate their presence.

In the Protection Center window, you can also view information about the update task or current virus scan tasks and stop or restart any of those tasks, if necessary.

SOLVING TYPICAL TASKS

This section contains step-by-step instructions on how to manage basic user tasks that the application can perform.

IN THIS SECTION:

PERFORMING A FULL SCAN OF THE COMPUTER FOR VIRUSES

The full scan task created by default is included in Kaspersky Internet Security. While running this task, the application scans all the hard drives of the computer for viruses and other threats.

➡ *To launch a full computer scan:*

1. Open the main application window (see page 20) and click the button.
2. In the menu that opens, select the **Full Scan** task.

You can view the results of the task run in the reports window.

PERFORMING A QUICK SCAN OF THE COMPUTER

The quick scan task created by default is included in Kaspersky Internet Security. While running this task, the application performs scanning for viruses and other types of malware in critical areas of your computer, such as folders that contain operating system files and system libraries, which may, when infected with malware, cause corruption of your operating system.

➨ *To launch a quick scan of your computer:*

1. Open the main application window (see page 20) and click the 🔍 button.
2. In the menu that opens, select the ⏱ **Quick Scan** task.

You can view the results of the task run in the reports window.

SCANNING A FILE, FOLDER OR DISK FOR VIRUSES

If you want to scan an individual object (such as a hard drive, folder, file, or removable device) for viruses and other types of malware, use the integrated Virus Scan task.

➨ *To scan an individual object for viruses and other malware:*

1. Open the main application window (see page 20) and click the 🔍 button.
2. In the menu that opens, select the 📁 **Virus Scan** task.

   A window opens for selecting objects to scan.
3. Create a list of objects to scan.

   The scan task will start automatically.

You can view the results of the task run in the reports window.

PURCHASING A LICENSE

If you have installed Kaspersky Internet Security without a commercial license, you can purchase one after installation. When purchasing a license, you receive an activation code that you should use to activate the application (see section "Activating Kaspersky Internet Security" on page 31).

➨ *To purchase a license:*

1. Open the main application window (see page 20) and click the 🔑 button.
2. In the window that opens, click the **Purchase** button.

A window will open with the web page of the Kaspersky Lab online store, where you can buy a license.

RENEWING A LICENSE

If the commercial license used for activation of Kaspersky Internet Security is about to expire, you can renew it. When renewing a license, you receive an activation code that you should use to activate the application (see section "Activating Kaspersky Internet Security" on page 31).

➡ *To renew a license:*

1. Open the main application window (see page 20) and click the 🔑 button.
2. In the window that opens, click the **Renew** button.

The Kaspersky Lab eStore web page opens, where you can renew a license.

UPDATING APPLICATION DATABASES

Kaspersky Lab updates Kaspersky Internet Security databases by using update servers. *Kaspersky Lab update servers* are HTTP and FTP servers of Kaspersky Lab where Kaspersky Internet Security updates are regularly published.

An Internet connection is required to download updates from the update servers.

By default, Kaspersky Internet Security periodically checks for updates on Kaspersky Lab's servers. If a set of the latest updates is stored on a server, Kaspersky Internet Security downloads them in background mode and installs them to your computer.

➡ *To start updating Kaspersky Internet Security,*

open the main application window (see page 20) and click the 🔄 button.

You can view the results of the update task run in the reports window.

PROTECTION AGAINST KEYLOGGERS

When working on 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, web shopping, or Internet banking.

There is a risk that this personal information can be intercepted using keystroke logging software.

Virtual Keyboard prevents interception of data entered at the keyboard.

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

Virtual Keyboard protects users against interception of personal information only if they browse the Internet with the Safari, Firefox™, or Google Chrome™ web browsers.

Virtual Keyboard has the following features:

- Click the keys of Virtual Keyboard with the mouse pointer.

- Unlike a physical keyboard, you cannot activate multiple keys on Virtual Keyboard simultaneously. Therefore, to enter a character that requires pressing a combination including **ALT** key and (or) **SHIFT** key of a physical keyboard, first click the first key (for example, **ALT**) and then click the one with the required character.

- You can use the key in the lower-left corner to switch between input languages on Virtual Keyboard. You can click this key and select an input language from the drop-down list.

By default, Virtual Keyboard appears on the screen automatically if a password-entry field is selected in the browser window.

➡ *To open Virtual Keyboard,*

click the K button in the toolbar of your web browser.

LIMITING WEB SURFING TIME FOR A USER

Excessive duration of computer use by children and teenagers may endanger their health. If you need to limit the Internet surfing time for a user, you can use the Time control category of Parental Control.

➡ *To restrict the amount of time a user spent on the Internet:*

1. Open the Parental Control preferences window (see page 22).
2. In the left part of the window, select a user account for which you want to limit time spent on the Internet.
3. In the right part of the window, on the **Preferences** tab, select the **Time control** category. If time control is disabled, enable it.
4. In the **Daily Internet access limit** section select the **Maximum time on Internet** check box.
5. By moving the slider, select the number of hours per day during which Internet access will be allowed.
6. In the **Internet access schedule limit** section select the **Allow Internet access based on day of week** check box.
7. Impose time limit on Internet use for weekdays and weekends.

You can view the report on the user's attempts to connect to the Internet during the allowed and blocked periods on the **Reports** tab of the Parental Control preferences window.

RESTRICTING WEBSITE VISITS AND FILE DOWNLOADS

You can restrict the following operations in order to protect children and teenagers who use the computer:

- access to websites that could waste time (chat rooms, games) or money (e-stores, auctions);
- access to websites targeted at an adult audience, such as those displaying pornography, extremism, firearms, drug abuse, and explicit violence;
- downloads of certain file types.

You can use the Web control category of Parental Control.

➡ *To restrict website visits and file downloads from the Internet:*

1. Open the Parental Control preferences window (see page 22).
2. In the left part of the window, select a user account for which you want to limit access to websites.

3. In the right part of the window, on the **Preferences** tab, select the **Web control** category. If web control is disabled, enable it.
4. Select the **Web control** check box and the check boxes for the categories of websites to which you want to block access.
5. Select the **Control of downloaded files** check box and the check boxes for categories of files that are allowed for download.

If necessary, you can allow access to some websites included in a blocked category, or block access to specified websites, by creating a list of exclusions.

You can view the report on attempts to visit blocked websites and download prohibited categories of files on the **Reports** tab of the Parental Control preferences window.

RESTRICTING A USER'S CONTACTS AND MESSAGING ON SOCIAL NETWORKS

Controlling the contacts and messaging of children and teenagers on social networks helps to prevent contact with strangers who may attempt to extract personal information by pretending to be the same age. If you need to restrict a user's contacts and messaging on social networks, you can use the Social networks category of Parental Control.

➡ *To restrict messaging over social networks:*

1. Open the Parental Control preferences window (see page 22).
2. In the left part of the window, select a user account for which you want to restrict messaging over social networks.
3. In the right part of the window, on the **Preferences** tab, select the **Social networks** category. If control of social networks is disabled, enable it.
4. Create a list of blocked and allowed contacts. To do this, click the + button and, in the **ID** column of the field, enter the name of a contact from a social network (login). In the **Name** column of the field, enter the real name of the contact.

   After the contact has been added to the list, Parental Control blocks correspondence with this contact on social networks.
5. If you want to allow messaging with a contact temporarily, select one from the list and clear the check box in the **Blocked** column.

   Messaging with this contact will remain allowed until the check box is selected again.

If messaging with a contact is prohibited, Parental Control blocks all messages sent to or received from that contact.

You can view the following information on the **Reports** tab of the Parental Control preferences window:

- information about messages received from or sent to any blocked contact;
- information about inclusion of personal data in messages;
- logs of messaging with each contact.

BLOCKING TRANSMISSION OF PERSONAL DATA

Kaspersky Internet Security allows you to reduce the risks associated with use of computers and the Internet. You can block transmission of data that contains personal information through social networks and when submitting data to websites, by using the Personal data category of Parental Control.

➡ *To block transmission of personal data:*

1. Open the Parental Control preferences window (see page 22).
2. In the left part of the window, select a use account for which you want to block transmission of personal data.
3. In the right part of the window, on the **Preferences** tab, select the **Personal data** category. If control of personal data is disabled, enable it.
4. Create a list of personal data. To do this, click the ⊞ button and enter data in the **Description** and **Data** columns of the field. For example, you can create records for your credit card number, home address, and phone number.

After personal data has been added to the list, Parental Control blocks the transmission of such data via social networks or to websites.

Kaspersky Internet Security blocks all attempts to send the data that has been added to the list. You can view information about blocked messages on the **Reports** tab of the Parental Control preferences window.

WHAT TO DO IF FILE ACCESS IS BLOCKED

Kaspersky Internet Security blocks access to infected and probably infected files and applications. If a file is infected or probably infected, it must be disinfected before it can be accessed.

➡ *To disinfect detected dangerous objects:*

1. Open the main application window (see page 20) and click the 📊 button.

   The Kaspersky Internet Security reports window opens.

2. Select **Detected threats** in the left part of the reports window.

   The **Active** group in the right part of the window displays a list of detected dangerous objects with their respective statuses. You can expand the list of objects by clicking the ▸ icon.

3. Click the **Disinfect all** button.

The application starts disinfecting malicious objects. While object disinfection is in progress, the application shows a notification window where you can choose the action to be taken on the object. If you select the **Apply to all** check box in the notification window after choosing the action to be taken on the object, the application will apply this action to all objects with the same status.

If you know for sure that the objects being blocked by File Anti-Virus are safe, you can include them in a trusted zone.

Restoring an object that has been deleted or disinfected by the application

We recommend that you avoid restoring deleted and disinfected objects unless it is extremely necessary, because they may threaten your computer.

Sometimes it is not possible to save objects in their entirety during the disinfection process. If a disinfected file contained important information that is partly or completely inaccessible following disinfection, you can attempt to restore the original file from its backup copy.

➡ *To restore an object that has been deleted or modified by the application:*

1. Open the main application window (see page 20) and click the 📊 button.

   The Kaspersky Internet Security reports window opens.

2. In the left part of the reports window, select **Quarantine**.

   The right part of the window displays the contents of Quarantine in the form of a list of copies of objects.

3. Select the copy of the object you require in the list and click the **Restore** button. Confirm the action.

The object is restored to its original location with its original name. If there is an object with the same name in the original location (this situation is possible when restoring an object with a copy created prior to disinfection), a warning appears. You can change the location of the object that is being restored or rename it.

We recommend that you scan the object for viruses immediately after restoring it. It is possible that the object will be disinfected with the help of the updated databases without loss of integrity.

Viewing the report on the application's operation

Information about events that have occurred in the operation of File Anti-Virus, Web Anti-Virus, or while running the virus scan or update tasks, is displayed in the reports window.

➡ *To open the reports window,*

open the main application window (see page 20) and click the 📊 button.

What to do if notification windows or pop-up messages appear

Application notifications (see section "Notification windows and pop-up messages" on page 23) appearing as notification windows inform you of events that occur during the operation of the application and require your attention.

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

WORKING WITH THE APPLICATION FROM THE COMMAND LINE

You can work with Kaspersky Internet Security from the command line.

Command line syntax:

```
kav <command> [parameters]
```

The following commands can be inserted as <command>:

- **help –** helps with command syntax, displays the list of commands;
- **scan –** scans objects for malware;
- **update –** starts the application update;
- **rollback –** rolls back the latest update to Kaspersky Internet Security (administrator rights are required to run this command);
- **start –** starts a component or a task;
- **stop –** stops a component or a task (administrator rights are required to run this command);
- **status –** displays the current status of a component or task on the screen;
- **statistics –** displays operational statistics of a component or task;
- **export –** exports the parameters of a component or a task;
- **import –** imports the parameters of a component or a task (administrator rights are required to run this command);
- **addkey –** activates the application by using a key file (administrator rights are required to run this command);
- **exit –** quits the application (administrator rights are required to run this command).

Each command has its own range of parameters.

IN THIS SECTION:

VIEWING HELP

Use this command to view the application command line syntax:

```
kav [ -? | help ]
```

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

```
kav <command> -?
kav help <command>
```

SCANNING FOR VIRUSES

The text of the command to start a virus scan of a specified area has the following general form:

```
kav scan [<object scanned>] [<action>] [<file types>] [<exclusions>] [<report
parameters>] [<advanced parameters>]
```

To scan for viruses, you can also use the tasks created in the application by starting the one you need from the command line (see section "Starting / stopping a protection component or a task" on page 50). The task will be started with the parameters that are specified in the Kaspersky Internet Security interface.

Parameters description

<object to scan> – this parameter specifies a list of objects that are to be scanned for malicious code. The parameter may include several values (separated by a space) from the list provided.

> **<files>** – list of paths to files and / or folders to be scanned. You can enter an absolute or relative path to the file. Items in the list are separated by a space. Comments:

- if the name of an object or the path to it includes the space or special characters (such as $, &, @), it should be put in single quotes, or the character being excluded should be separated with the backslash on its left side;

- if reference is made to a specific folder, all files and folders in this folder are scanned.

-all – full scan of your computer;

-remdrives – all removable drives;

-fixdrives – all local drives;

-netdrives – all network drives;

-@:<filelist.lst> – path to the file with a list of objects and folders within the scan scope. The file must be in text format and each scan object must be listed on a separate line. Only an absolute path to the file may be entered.

> If no list of objects to be scanned is specified, Kaspersky Internet Security starts the Virus Scan task with the preferences that are selected in the application interface.

<action> – this parameter determines the action to take on malicious objects that are detected during the scan. If this parameter has not been defined, the default action is the one with the value for **-i8**. The following values are possible:

-i0 – take no actions on the object, only saving information about the object in a report;

-i1 – disinfect infected objects, skip them if they cannot be disinfected;

-i2 – disinfect infected objects, delete them if they cannot be disinfected; do not delete containers, except for those with executable headers (.sfx archives);

-i3 – disinfect infected objects, delete them if they cannot be disinfected; delete containers completely if embedded infected files cannot be deleted;

-i4 – delete infected objects; delete containers completely if infected files inside them cannot be deleted;

-i8 – prompt the user for action if an infected object is detected (used by default);

-i9 – prompt the user for action when the scan is completed.

<file types> – this parameter defines the file types that are subject to anti-virus scanning. By default, if this parameter is not defined, only infected files by contents are scanned. The following values are possible:

-fe – scan only infected files by extension;

-fi – scan only infected files by content (by default);

-fa – scan all files.

-<exclusions> – this parameter defines objects that are to be excluded from scanning. You can include several parameters from the list below, separating them with a space:

-e:a – do not scan archives;

-e:b – do not scan mail databases;

-e:m – do not scan email messages in text format;

-e:<mask> – do not scan objects by mask;

-e:<seconds> – skip objects that are scanned for longer than the specified time value (in seconds);

-es:<size> – skip objects with size larger than the specified value (in megabytes).

<report parameters> – these parameters define the format of the report on the scan results. You can use an absolute or relative path to the file for saving the report. If the parameter is not defined, scan results are displayed and all events are shown.

-r:<report_file> – log only important events to the specified report file;

-ra:<report_file> – log all events to the specified report file.

<advanced parameters> – parameters that define the use of anti-virus scanning technologies and the configuration file:

-iSwift=<on|off> – enable / disable the use of iSwift technology;

-c:<configuration_file_name> – defines the path to the configuration file that contains the application preferences applied when running virus scan tasks. You can enter an absolute or relative path to the file. If the parameter is not specified, the values set in the application interface are used together with the values that are already specified in the command line.

Example:

Start scan of the folders ~/Documents, /Applications, and the file named my test.exe:

```
kav scan ~/Documents /Applications 'my test.exe'
```

Scan the objects listed in the file object2scan.txt. Use the scan_settings.txt configuration file. When the scan is complete, create a report to log all events:

```
kav scan -@:objects2scan.txt -c:scan_settings.txt -ra:scan.log
```

A sample configuration file:

```
-netdrives -@:objects2scan.txt -ra:scan.log
```

UPDATING THE APPLICATION

The command for updating the application features the following syntax:

```
kav update [<update_source>] [-app=<on|off>] [<report_parameters>]
[<advanced_parameters>]
```

Parameters description

<update_source> – an HTTP server, an FTP server, or a network or local folder for downloading updates. If a path is not selected, the update source will be taken from the application update preferences.

-app=<on|off> – enable / disable application modules updating.

<report parameters> – these parameters define the format of the report on the scan results. You can use an absolute or relative path to the file. If the parameter is not defined, scan results are displayed and all events are shown. The following values are possible:

-r:<report_file> – log only important events to the specified report file;

-ra:<report_file> – log all events to the specified report file.

<advanced parameters> – a parameter that defines the use of the configuration file.

-c:<configuration_file_name> – defines the path to the configuration file that contains the application preferences applied when updating the application. You can enter an absolute or relative path to the file. If this parameter is not defined, the values set in the application interface are used.

Example:

Update the application databases from the default source, logging all events in the report:

```
kav update -ra:avbases_upd.txt
```

Update the Kaspersky Internet Security modules using the parameters of the updateapp.ini configuration file:

```
kav update -app=on -c:updateapp.ini
```

ROLLING BACK THE LAST UPDATE

Command syntax:

```
kav rollback [<report_parameters>]
```

Administrator rights are required to run this command.

Parameters description

<report parameters> – this parameter defines the format of the report on update rollback results. You can use an absolute and relative path to the file. If the parameter is not defined, scan results are displayed and all events are shown.

-r:<report_file> – log only important events to the specified report file;

-ra:<report_file> – log all events to the specified report file.

Example:

kav rollback -ra:rollback.txt

STARTING / STOPPING A PROTECTION COMPONENT OR TASK

The start command syntax:

```
kav start <profile|task_name> [<report_parameters>]
```

The stop command syntax:

```
kav stop <profile|task_name>
```

Computer administrator rights are required to run the stop command.

Parameters description

<report parameters> – these parameters define the format of the report on the scan results. You can use an absolute and relative path to the file. If the parameter is not defined, scan results are displayed and all events are shown. The following values are possible:

-r:<report_file> – log only important events to the specified report file;

-ra:<report_file> – log all events to the specified report file. You can use an absolute or relative path to the file. If the parameter is not defined, scan results are displayed and all events are shown.

<profile|task_name> – one of the following values is displayed:

file_monitoring (fm) – File Anti-Virus;

web_monitoring (wm) – Web Anti-Virus;

scan_my_computer (full) – Full Scan task;

scan_objects – Virus Scan task;

scan_critical_areas (quick) - Quick Scan task;

updater – update task;

rollback – update rollback task.

Components and tasks started from the command prompt are run with the parameters configured in the application interface.

Example:

To enable the File Anti-Virus component, type the following at the command prompt:

```
kav start fm
```

To stop the full scan task from the command prompt, enter the following:

```
kav stop scan_my_computer
```

STATISTICS ON A COMPONENT'S OPERATION OR A TASK

The status command syntax:

```
kav status [<profile|task_name>]
```

The statistics command syntax:

```
kav statistics <profile|task_name>
```

Parameters description

<profile|task_name> – one of the values listed for the start / stop command is specified (see section "Starting / stopping a protection component or a task" on page 50).

If the status command is run without specifying a value for the **<profile|task_name>** parameter, the current status of all tasks and components of the application is displayed on the screen. For the statistics command, a value must be specified for the **<profile|task_name>** parameter.

EXPORTING PROTECTION PREFERENCES

Command syntax:

```
kav export <profile|task_name> <file_name>
```

Parameters description

<profile|task_name> – one of the values listed for the start / stop command is specified (see section "Starting / stopping a protection component or a task" on page 50).

<file_name> – path to the file to which the application preferences are exported. An absolute or a relative path may be specified.

Example:

```
    kav export fm fm_settings.txt – text format
```

IMPORTING PROTECTION PREFERENCES

Command syntax:

```
    kav import <file_name>
```

Administrator rights are required to run this command.

Parameters description

<file_name> – path to the file from which the application preferences are imported. An absolute or a relative path may be specified.

Example:

kav import settings.dat

ACTIVATING THE APPLICATION

Kaspersky Internet Security can be activated by using a key file.

Command syntax:

```
    kav addkey <file_name>
```

Administrator rights are required to run this command.

Parameters description

<file_name> – application key file with the .key extension.

Example:

```
    kav addkey 1AA111A1.key
```

CLOSING THE APPLICATION

Command syntax:

```
    kav exit
```

Administrator rights are required to run this command.

RETURN CODES OF THE COMMAND LINE

The general codes may be returned by any command from the command line. The return codes include general codes as well as codes specific to a certain task.

General return codes:

- 0 – operation completed successfully;
- 1 – invalid parameter value;
- 2 – unknown error;
- 3 – task completion error;
- 4 – task canceled.

Virus scan task return codes:

- 101 – all dangerous objects processed;
- 102 – dangerous objects detected.

CONTACTING TECHNICAL SUPPORT

This section contains information about how to contact Technical Support and on what terms assistance can be provided.

IN THIS SECTION:

CONTACTING TECHNICAL SUPPORT

➡ *To view information about the ways you can receive technical support for Kaspersky Internet Security,*

open the main application window (see page 20) and click the button.

If you cannot find any solution to your issue in the application documentation or in an external source of information about the application, we recommend that you contact Technical Support at Kaspersky Lab. Technical Support specialists will answer to your questions concerning application installation and use.

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

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

- Call by phone. This option allows consulting with specialists of Russian-speaking or international Technical Support by phone.
- Send a request from My Kaspersky Account on the Technical Support website. This option allows contacting Technical Support specialists through a request form.

Technical support is provided only to users who have purchased the commercial license to use the application. Technical support is not provided to trial license owners.

TECHNICAL SUPPORT BY PHONE

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

Before contacting Technical Support Service, please read the support rules (http://support.kaspersky.com/support/details). This will help our support staff solve your problem more quickly.

CONTACTING TECHNICAL SUPPORT FROM MY KASPERSKY ACCOUNT

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

To obtain access to My Kaspersky Account, you should go through the registration procedure on the registration page (https://my.kaspersky.com/registration). Specify your email and a password to access My Kaspersky Account.

In your My Kaspersky Account you can take the following actions:

- send queries to Technical Support and the Anti-Virus Lab;
- exchange messages with Technical Support without using email;
- monitor queries in real time;
- view a complete history of all your queries;
- receive a copy of the key file in case it has been lost or stolen.

Email query to Technical Support

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

In the email query form, specify the following data:

- query type;
- application name and version number;
- query text;
- client ID and password;
- email address.

A Technical Support specialist forwards the answer to your question to your My Kaspersky Account and to the email address that you specified in your email query.

Email query to Anti-Virus Lab

Some queries must be sent to the Anti-Virus Lab, not Technical Support.

You can send queries of the following types to the Anti-Virus Lab:

- *Unknown malware* – you suspect a file of containing a virus, but Kaspersky Internet Security does not recognize it as infected.

  Specialists at Anti-Virus Lab analyze the malicious code and, if a previously unknown virus is detected, add a description of the virus to a database that becomes available after updating the anti-virus applications.

- *False positive* – Kaspersky Internet Security recognizes a file as containing a virus, but you are sure that it is not a virus.
- *Request for malware description* – you want to receive a description of a virus detected by Kaspersky Internet Security based on the name of the virus.

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

USING A TRACE FILE

After you inform Technical Support specialists of your issue, they may ask you to generate a report with information about your operating system and send it to Technical Support. Technical Support specialists may also ask you to generate a *trace file*. Trace files allow tracking the step-by-step process of command execution and finding out at which step an error occurs.

CREATING A TRACE FILE

➡ *To create a trace file:*

1. Click the ⚙ button in the main application window (see section "Main application window" on page 20).

   The application preferences window opens.

2. On the **Reports** tab of the application preferences window, in the **Traces** section, select the **Enable trace logs** check box.

3. Restart Kaspersky Internet Security to start the tracing process.

It is recommended to use this option when instructed to do so by a Kaspersky Lab Technical Support specialist.

Trace logs can occupy a significant amount of space on your hard drive. After finishing with trace files, it is recommended that you disable creation of such files by clearing the **Enable trace logs** check box on the **Reports** tab of the application preferences window. You have to restart Kaspersky Internet Security afterwards.

GLOSSARY

A

Activating the application

Conversion of the application into full-function mode. Activation is performed by the user during or after the application installation. To activate the application, the user needs an activation code or a key file.

Active key

A key that is currently in use for application operation.

B

Blocking the object

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

D

Database updates

A feature of the Kaspersky Lab application that allows maintaining computer protection in up-to-date condition. While being updated, the application copies updates for application databases and modules from Kaspersky Lab servers to the computer and then installs and applies them automatically.

Databases

Databases that contain information about computer security threats that are known to Kaspersky Lab at the time when such databases are issued. Records in the databases allow detecting malicious code in objects being scanned. The databases are compiled by Kaspersky Lab specialists and updated hourly.

F

False alarm

Situation when Kaspersky Lab's application considers a non-infected object as infected due to its code similar to that of a virus.

G

Growl technology

An all-purpose system for notifying users on the Mac OS X operating system. Supports popup notifications, voice notifications, SMS and email notifications.

The appearance of notifications generated using Growl can be configured in the Other section of the System Preferences panel into which Growl is automatically integrated after installation.

H

Heuristic analyzer

A technology designed to detect threats that have not yet been added to databases of Kaspersky Lab. The heuristic analyzer allows detecting objects behaving in a way that can pose a security threat to the system. Objects detected using the heuristic analyzer are considered to be potentially infected. For example, an object can be considered to be potentially infected if it contains combinations of commands that are typical of malicious objects (open file, write to file).

I

INFECTED OBJECT

An object a segment of whose code fully matches a code segment of a known threat. Kaspersky Lab specialists recommend that you avoid handling such objects.

K

KASPERSKY LAB UPDATE SERVERS

HTTP and FTP servers at Kaspersky Lab from which the application retrieves updates for the application databases and modules.

O

OBJECT DISINFECTION

A method of processing infected objects that results in full or partial data recovery. Not all infected objects can be disinfected.

P

POTENTIALLY INFECTED OBJECT

An object whose code contains a modified segment of code of a known threat, or an object resembling a threat in the way it behaves.

PROTECTION

The application's operating mode under which objects are scanned for the presence of malicious code in real time.

The application intercepts all attempts to open any object (read, write, or execute) and scans the object for threats. Uninfected objects are passed on to the user; objects containing threats or suspected of containing them are processed pursuant to the task settings (they are disinfected, deleted or quarantined).

PROTECTION STATUS

The current status of protection, summarizing the degree of a computer's security.

Q

QUARANTINE

Special storage designed to save backup copies of objects created before their first disinfection or deletion. The Kaspersky Lab application also quarantines potentially infected objects that have been detected. Quarantined objects are stored in encrypted form to avoid any impact on the computer.

R

RESERVE KEY

A key that confirms the right to use the application although it is not currently in use.

RESTORATION

Moving an original object from Quarantine the folder where it was originally found before being disinfected or deleted, or to a different folder specified by the user.

KASPERSKY LAB ZAO

Kaspersky Lab software is internationally renowned for its protection against viruses, malware, spam, network and hacker attacks, and other threats.

In 2008, Kaspersky Lab was rated among the world's top four leading vendors of information security software solutions for end users (IDC Worldwide Endpoint Security Revenue by Vendor). Kaspersky Lab is the preferred developer of computer protection systems among home users in Russia, according to the COMCON survey "TGI-Russia 2009".

Kaspersky Lab was founded in Russia in 1997. Today, it is an international group of companies headquartered in Moscow with five regional divisions that manage the company's activity in Russia, Western and Eastern Europe, the Middle East, Africa, North and South America, Japan, China, and other countries in the Asia-Pacific region. The company employs more than 2000 qualified specialists.

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

The personal product range includes anti-virus applications for desktop, laptop, and pocket computers, and for smartphones and other mobile devices.

Kaspersky Lab delivers applications and services to protect workstations, file and web servers, mail gateways, and firewalls. Used in conjunction with Kaspersky Lab's centralized management system, these solutions ensure effective automated protection for companies and organizations against computer threats. Kaspersky Lab's products are certified by the major test laboratories, are compatible with the software of many suppliers of computer applications, and are optimized to run on many hardware platforms.

Kaspersky Lab's virus analysts work around the clock. Every day they uncover hundreds of new computer threats, create tools to detect and disinfect them, and include them in the databases used by Kaspersky Lab applications. *Kaspersky Lab's Anti-Virus database is updated hourly*; and the *Anti-Spam database every five minutes*.

Technologies. Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky Lab. It is no coincidence that many other developers use the Kaspersky Anti-Virus kernel in their products, including: SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Israel), Clearswift (UK), CommuniGate Systems (USA), Critical Path (Ireland), D-Link (Taiwan), M86 Security (USA), GFI (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), NETASQ (France), NETGEAR (USA), Parallels (Russia), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Taiwan). Many of the company's innovative technologies are patented.

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

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

INFORMATION ABOUT THIRD-PARTY CODE

Information about third-party code is contained in the file named legal_notices.txt file:///Library/Application%20Support/Kaspersky%20Lab/KAV/Doc/legal_notices.txt, located in the application installation folder.

TRADEMARK NOTICES

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

Firefox is a trademark owned by Mozilla Foundation.

Google Chrome is a trademark owned by Google Inc.

Mac, Mac OS, Mountain Lion and Safari are registered trademarks owned by Apple Inc.

INDEX