

Kaspersky Mobile Security 9.0

USER GUIDE

PROGRAM VERSION: 9.0

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.

Reproduction or distribution of any materials in any format, including translations, is only allowed with the written permission of Kaspersky Lab.

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

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

Kaspersky Lab shall not be liable 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 or actual losses associated with the use of these materials.

In this document, registered trademarks and service trademarks are used which are the property of the corresponding rights holders.

Document last revised on: March 2, 2010

© 1997-2010 Kaspersky Lab ZAO. All Rights Reserved.

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

TABLE OF CONTENTS

KASPERSKY MOBILE SECURITY 9.0	7
What's new in Kaspersky Mobile Security 9.0	9
Hardware and software requirements	10
Distribution kit	10
KASPERSKY MOBILE SECURITY 9.0 FOR SYMBIAN OS	11
Installing Kaspersky Mobile Security 9.0	11
Uninstalling the application	13
Updating the application version 8.0 to version 9.0	14
Getting started	15
Activating the application	15
Entering the secret code	17
Starting the application.....	18
Updating the application's databases.....	18
Scanning the device for viruses	19
File system protection	19
About Protection.....	20
Enabling and disabling the Protection	20
Scanning the device	21
About scanning the device	22
Starting a scan manually	22
Starting a scheduled scan.....	24
Quarantine of possibly infected objects	25
Filtering of incoming calls and SMS messages.....	25
About Anti-Spam	26
Anti-Spam modes.....	27
Changing the Anti-Spam mode	28

Restricting outgoing calls and SMS messages. Parental Control	29
About Parental Control	29
Parental Control modes	29
Changing the Parental Control mode	30
Data protection in the event of loss or theft of the device	30
Blocking the device	31
Deleting personal data	31
Creating a list of objects to be deleted	33
Monitoring the replacement of a SIM card on the device	33
Determining the device's geographical coordinates	34
Remote start of the Anti-Theft functions	35
Hiding personal data	36
Privacy Protection	36
Privacy Protection modes	37
Changing Privacy Protection modes	37
Automatic start of Privacy Protection	38
Filtering network activity. Firewall	39
About Firewall	39
Selecting the Firewall's security level	39
Encrypting personal data	40
About Encryption	40
Data encryption	41
Data decryption	42
KASPERSKY MOBILE SECURITY 9.0 FOR MICROSOFT WINDOWS	
MOBILE	44
Installing Kaspersky Mobile Security 9.0	44
Uninstalling the application	45
Updating version 8.0 to version 9.0	46
Getting started	48

Activating the application	48
Entering the secret code	49
Starting the application.....	50
Updating the application's databases.....	51
Scanning the device for viruses	51
File system protection	52
About Protection.....	52
Enabling and disabling the Protection	53
Scanning the device	54
About on-demand scans	54
Starting a scan manually.....	55
Starting a scheduled scan	57
Quarantining malware objects	57
Filtering of incoming calls and SMS messages.....	58
About Anti-Spam	58
Anti-Spam modes.....	60
Changing the Anti-Spam mode	61
Restricting outgoing calls and SMS messages. Parental Control .	61
About Parental Control	62
Parental Control modes	62
Enabling/disabling Parental Control	63
Data protection in the event of loss or theft of the device	63
About Anti-Theft	63
Blocking the device	65
Deleting personal data	65
Creating the list of deleted data.....	67
Monitoring the replacement of a SIM card on the device	68
Determining the device's geographical coordinates	69
Remote start of the Anti-Theft functions	70

Hiding personal data	71
Privacy Protection	71
Privacy Protection modes	71
Enabling / disabling Privacy Protection	72
Automatic start of Privacy Protection	73
Filtering network activity. Firewall	74
About Firewall	74
Selecting the Firewall's security level	74
Encrypting personal data	75
About Encryption	75
Data encryption	75
Data decryption	77
CONTACTING THE TECHNICAL SUPPORT SERVICE	78

KASPERSKY MOBILE SECURITY 9.0

Kaspersky Mobile Security 9.0 ensures protection of mobile devices running Symbian OS and Microsoft Windows Mobile operating systems against known and new threats, unsolicited calls and SMS messages. The application allows to manage outgoing SMS messages, network activity, and protect confidential information from unauthorized access. Every type of threat is processed in separate components of the program. This allows to fine-tune the application settings depending on user needs.

Kaspersky Mobile Security 9.0 includes the following protection components:

- **Protection.** Protects the mobile device's file system against infections. The Protection component is initiated when starting the operating system, it is always in the device's operating memory and verifies all open, saved and started files on the device, including on memory cards. Furthermore, the Protection verifies all incoming files for the existence of known viruses. You can continue working with file if the object is not infected or has been successfully disinfected.
- **Scanning the device.** Helps to find and neutralize malicious objects on your device. You should scan the device regularly to prevent the spread of malicious objects that were not discovered by the Protection.
- **Anti-Spam.** Verifies all incoming SMS messages and viruses for spam. The component allows blocking all SMS messages and calls which are regarded as unwanted.
- **Parental Control.** Checks outgoing messages and prevents the sending of SMS messages and / or calls to previously specified subscriber numbers.
- **Anti-Theft.** Protects the information on the device from unauthorized access, when it is lost or stolen. This component

allows the blocking of the device in the event of theft or loss, deletes confidential information and controls SIM card usage and determines the geographical coordinates of the device (if a mobile device is equipped with a GPS receiver).

- **Privacy Protection.** Hides confidential user information when the device is used by other persons. The component allows the displaying or hiding of all information related to specified subscriber numbers, for instance details in the Contact list, SMS correspondence or entries in the calls log. The component allows the hiding of the delivery of incoming calls and SMS messages from favorite numbers.
- **Firewall.** Checks the network connections on your mobile device. The component allows setting of connections which are allowed or blocked.
- **Encryption.** Protects information from being viewed by third parties even if access to the device is achieved. The component encrypts any amount of non-system folders which are in the device memory or on a storage card. The data in the folder become available only after the secret code is entered.

Furthermore, the application contains a set of service features. They are designed to keep the application up-to-date, enhance its performance and help users.

- Updating the application's databases. This function keeps Kaspersky Mobile Security 9.0 databases up to date.
- Protection status. The status of the program's components is displayed on screen. On the basis of the information presented, you can assess the current status of protection of your device.
- Event log. Each of the application components has its own event log that includes the information on the component operation (for instance, completed operation, data on a blocked object, scan report, updates etc.).
- License. When you purchase Kaspersky Mobile Security 9.0, a license agreement is made between you and Kaspersky

Lab, according to which you can use the application and access to the application databases update and Technical Support Service within a certain time. The terms of use and other information required for full-feature application operation are indicated in the license.

Using the **License** option, you can get a detailed report on the current license as well as renew it.

Kaspersky Mobile Security 9.0 is not intended for backup and restore.

WHAT'S NEW IN KASPERSKY MOBILE SECURITY 9.0

Below is a detailed view of the novelties with Kaspersky Mobile Security 9.0.

New protection:

- Access to the application is protected by a secret code.
- The Kaspersky Mobile Security 9.0 package includes the Privacy Protection component, which prevents unauthorized access to the user's personal data during temporary use by unauthorized persons. The component hides the data events for a set list of numbers. Privacy Protection in no way reveals its activity, meaning that there is no indication of the existence of the hidden data on the device.
- In the updated Encryption module, the blocking of access to any amount of files stored in the device's memory or on a storage card is implemented. The component protects confidential data in encrypted mode and automatically blocks access on the expiry of a set period of time.
- A new approach to managing the protection of the device is implemented: the user can enable and disable any components depending on the required functionality.

- It is now possible to purchase an activation code and renew the license directly from the mobile device.

HARDWARE AND SOFTWARE REQUIREMENTS

Kaspersky Mobile Security 9.0 is designed for installation on mobile devices running one of the following operating systems:

- Symbian OS 9.1, 9.2, 9.3 and 9.4 Series 60 UI.
- Microsoft Windows Mobile 5.0, 6.0, 6.1 or 6.5.

DISTRIBUTION KIT

You can purchase Kaspersky Mobile Security online, in which case the application's distribution kit and documentation are provided in electronic form. Kaspersky Mobile Security can be also purchased from all good phone and technology retail stores. For detailed information about purchasing the application and receiving the distribution kit, please contact our sales department at sales@kaspersky.com.

KASPERSKY MOBILE SECURITY 9.0 FOR SYMBIAN OS

This section contains a description of the operation of Kaspersky Mobile Security 9.0 for mobile devices running Symbian version 9.1, 9.2, 9.3 and 9.4 Series 60 UI.

INSTALLING KASPERSKY MOBILE SECURITY 9.0

The application is installed on a mobile device in several steps.

To install Kaspersky Mobile Security 9.0:

1. Connect the mobile device to the computer.

For Nokia mobile devices, it is recommended to use the Nokia PC Suite or Nokia Ovi Suite application.

2. Perform one of the following actions:

- If you have purchased the program on a CD, run the automatic Kaspersky Mobile Security 9.0 installation on the CD purchased.
- If you have purchased the distribution package on the Internet, copy it to the mobile device, using one of these methods:
 - using the Nokia PC Suite application (for Nokia mobile devices);
 - using a memory card.

Start the installation using one of the following methods:

- from the Nokia PC Suite or Nokia Ovi Suite application (for Nokia mobile devices);
- open the sis archive containing the distribution package on your mobile device.

A window confirming the installation opens.

3. Confirm the installing of the application by pressing the **Yes** button.
4. Review the additional information about the application, which includes name, version, and certificates. Then press **Continue**.

If the language of the operating system does not match the language of Kaspersky Mobile Security 9.0, a message is displayed on the screen. To proceed with the installation in the current language, press **OK**.

5. Read the License Agreement text, which is concluded between you and Kaspersky Lab. If you agree to all terms of the agreement, press **OK**. The installation of Kaspersky Mobile Security 9.0 will then start. If you do not agree to the terms of the License Agreement, press **Cancel**. Installation will be terminated.
6. Confirm that there are no other anti-virus applications on the device by pressing **OK**.
7. In order to complete the installation, restart the device.

The application is installed with the parameters recommended by the experts of Kaspersky Lab.

UNINSTALLING THE APPLICATION

To uninstall Kaspersky Mobile Security 9.0:

1. Decrypt the data on your device if it was encrypted with Kaspersky Mobile Security 9.0 (see the "Data decryption" section on page 42).
2. Disable Privacy Protection (see the "Privacy Protection modes" section on page 37).
3. Close Kaspersky Mobile Security 9.0. To do this, press **Options** → **Exit**.
4. Uninstall Kaspersky Mobile Security 9.0. To do this, perform the following actions:
 - a. Open the device's main menu.
 - b. Select the **Applications** → **My own** folder

The application installation folder may vary depending on the mobile device model.

- c. Select from **KMS 9.0** the list of applications and then select **Options** → **Remove**.
- d. Confirm the uninstalling of the application by pressing the **Yes** button.
- e. Enter the secret code and press **OK**.
- f. Specify whether or not to keep the program settings and objects in quarantine:
 - If you wish to save the application's parameters and objects to the quarantine, check the boxes opposite the parameters required and then press **OK** (see Figure below).
 - In order to uninstall the application completely, press **Cancel**.

5. Restart the device in order to complete the uninstalling of the application.

UPDATING THE APPLICATION VERSION 8.0 TO VERSION 9.0

If Kaspersky Mobile Security 8.0 is already installed on your mobile device, you can update it to Kaspersky Mobile Security 9.0.

Before updating the application version, disable Encryption – decrypt all data (see "Data decryption" section on page 42).

To update the program version:

1. Close the current version of Kaspersky Mobile Security. To do this, press **Options** → **Exit**.
2. Copy the application's distribution package to your device, using one of these methods:
 - from the Kaspersky Lab website;
 - using the Nokia PC Suite application (for Nokia mobile devices);
 - using a memory card.
3. Start the Kaspersky Mobile Security 9.0 distribution package on the device.
4. Confirm the installation of the application by pressing the **Yes** button.
5. Review the additional information about the application, which includes name, version, and certificates. Then press **Continue**.
6. Confirm the update of the application version by pressing **OK**.

7. Enter the secret code set in the previous version of the application.
8. Read the license agreement carefully. If you agree to its terms, press **OK**. If you do not agree to the terms of the License Agreement, press **Cancel**. Installation will be terminated.
9. Confirm that there are no other anti-virus applications on the device. To do this, press **OK**.
10. Delete the configured settings of the previous application version. To do this, press **Delete**.

The settings can only be kept when moving from one version to another within the same product generation. The parameters of 8.0 application version are incompatible with the 9.0 version.

The installation of Kaspersky Mobile Security 9.0 starts.

If the validity period of the Kaspersky Mobile Security 8.0 license has not expired, enable program version 9.0 using the activation code of version 8.0 (see the "Activating the application" section on page 15).

11. In order to complete the installation, restart the device.

GETTING STARTED

This section contains information about how to prepare Kaspersky Mobile Security 9.0 for operation (activating it and creating a secret code), run the application, update its databases and scan the device for viruses.

ACTIVATING THE APPLICATION

In order to use Kaspersky Mobile Security 9.0, it must be enabled. During the process of its activation, an activation code must be entered

which is verified and registered on the servers of Kaspersky Lab. Subsequently, the application obtains and installs the key file.

You can obtain an activation code as follows:

- online, by exiting the Kaspersky Mobile Security 9.0 application and going to the website <http://www.kaspersky.com/gotopartnersite/def71/buy> ;
- at the <http://www.kaspersky.com/globalstore> website;
- from Kaspersky Lab distributors.

To activate Kaspersky Mobile Security 9.0 on your device, you must have an Internet connection configured.

Before activating the application, make sure that the device's system date settings are correct.

You can activate the application as follows:

- **Activate trial license.** Select this activation method if you wish to get familiar with the application functions. A free license key file will be installed during activation. The validity period of the trial license will be displayed on screen after completing the activation. Once the validity period of the trial license expires, the application's functions will be limited. Only the following features will be available:
 - Activating the application;
 - managing the application license;
 - Kaspersky Mobile Security 9.0 Help system;
 - disabling Encryption;
 - disabling Privacy Protection.

It is impossible to reactivate a trial version.

- **Activate commercial license.** Select this method if you have purchased the commercial version of the application and obtained an activation code. After entering the activation code, the license key file is obtained and installed which provides access to the application's full range of functions. The validity period will be displayed on the device's screen. After expiry of the validity period, the application's functions will be limited; the application will no longer be updated.

ENTERING THE SECRET CODE

After activating the program, you will be asked to enter your secret code. The *secret code* prevents unauthorized access to the application settings. You can later change the secret code installed.

The secret code is requested in the following instances:

- for access to the application;
- for access to encrypted data;
- to enable/disable Privacy Protection;
- when sending a command with a special SMS message to start the following functions remotely: Block, Data Wipe, SIM Watch function, GPS Find, Privacy Protection;
- when uninstalling the application.

Please remember the secret code. If you forget it, it will be impossible to use the functions of Kaspersky Mobile Security 9.0 or to obtain access to encrypted data and uninstall the application.

You are advised to use a secret code consisting of at least 7 digits.

To enter the secret code:

1. After activating the application, enter in the **Enter new code** entry field, the digits of your new code.

2. Re-enter the same code in the **Confirm** field.

The code entered is automatically verified.

3. If the code is deemed invalid according to the results of the verification, a warning message is displayed and the application requests confirmation. In order to use the code, press **Yes**. In order to create a new code, press **No**.
4. To start using the application, press **OK**.

STARTING THE APPLICATION

To start Kaspersky Mobile Security 9.0:

1. Open the device's main menu.
2. Select the **Settings** → **Data mgr.** → **App. mgr.** folder → **KMS 9.0**.

The application installation folder may vary depending on the mobile device model.

3. Start the application. To do this, press **Options** → **Open**.
This will open the **KMS 9.0** window.
4. Enter the secret code and press **OK**.

The application displays a window showing the current status of Kaspersky Mobile Security 9.0. To go to the application's functions, press **OK**.

UPDATING THE APPLICATION'S DATABASES

Kaspersky Mobile Security 9.0 scans for threats based on the application databases, which contain descriptions of all the malicious programs known to date and methods for neutralizing them and descriptions of other unwanted objects. By the moment of the

application installation, databases included in the Kaspersky Mobile Security 9.0 installation package may become obsolete.

We recommend you to update the application databases immediately after the application installation.

To update the application's databases, you must have an Internet connection configured on your mobile device.

To start the database update process manually:

1. Select the **Update** item in the **Anti-Virus** tab.

This will open the **Update** window.

2. Select the **Update** item.

The application starts the process of updating the databases from the Kaspersky Lab server. Information on the update process is displayed on the screen.

SCANNING THE DEVICE FOR VIRUSES

After installing the application, it is recommended to immediately run a scan of your mobile device for malware objects.

The first scan is performed with the settings previously set by the Kaspersky Lab experts.

To run a full scan of the device:

1. Select **Scan** in the **Anti-Virus** tab.

This will open the **Scan** window.

2. Select **Full scan**.

FILE SYSTEM PROTECTION

This section provides information on the Protection component which enables avoidance of infections of your device's file system. It also

specifies how to activate/stop the Protection and adjust its operation settings.

ABOUT PROTECTION

Protection loads when the device's operating system starts, and stays resident in the device's memory, scanning all files that are opened, saved, or executed. Files are scanned according to the following algorithm:

1. The component intercepts every attempt by the user or by any program to access any file.
2. The file is scanned for the presence of malicious objects (malware). Malicious objects are detected by comparison with the application's databases, which contain descriptions of all known malicious objects, and methods for neutralizing them.
3. After the analysis, Kaspersky Mobile Security 9.0 may take the following courses of action:
 - If malicious code was detected in the file, the application blocks access to the file and performs the action specified in the settings.
 - If no malicious code is discovered in the file, it will be immediately restored.

Information about the scan's results is saved in the application's log.

ENABLING AND DISABLING THE PROTECTION

When activating the Protection, all actions in the system are under permanent control. To ensure the protection from malicious objects, the resources of the device are used. In order to reduce the load on the device when executing several tasks, you can temporarily stop Protection.

The Kaspersky Lab specialists strongly recommend that you do not disable Protection, since this could lead to the infection of your computer and data loss.

The current Protection status is displayed on the **Anti-Virus** tab next to the **Protection** menu item.

To edit the settings, the device's joystick can be used or select **Options**→ **Change**.

To enable Protection:

1. Select the **Protection** item in the **Anti-Virus** tab.
This will open the **Protection** window.
2. Select for the **Protection mode** setting the **On** value.
3. Press **Back** to save the changes.

To disable Protection:

1. Select the **Protection** item in the **Anti-Virus** tab.
This will open the **Protection** window.
2. Select for the **Protection mode** setting the **Off** value.
3. Press **Back** to save the changes.

SCANNING THE DEVICE

This section presents information on scanning for viruses which allows detecting and neutralizing threats in your device. Furthermore, this section specifies how to run the scan task, how to create a timetable to run tasks, how to select scan objects and install the action of the application with a detected threat.

ABOUT SCANNING THE DEVICE

Scanning the device helps to detect and neutralize malicious objects on your device. Kaspersky Mobile Security 9.0 allows a full or partial scan of the device's file system, i.e. scanning only the contents of the device's memory, messages or a specific folder (including one located on a memory card).

The device is scanned as follows:

1. Kaspersky Mobile Security 9.0 scans the file types set.
2. The file is scanned for the presence of malicious objects (malware). Kaspersky Mobile Security 9.0 detects malicious objects on the basis of the application's databases, which contain descriptions of all known malicious objects, and methods for neutralizing them.

After the analysis, Kaspersky Mobile Security 9.0 may take the following courses of action:

- if a malicious object is found in the file, Kaspersky Mobile Security 9.0 performs the set task;
- if no malicious code is detected, the file immediately becomes accessible for operation.

A scan task is started manually or automatically in accordance with a previously set schedule (see the "Starting a scheduled scan" section on page 24).

Information about the on-demand scan's results is saved in the application's log.

STARTING A SCAN MANUALLY

You can launch an on-demand scan manually at any time: the best time is when the device's processor is free from performing other tasks.

To start an anti-virus scan manually:

1. Select **Scan** in the **Anti-Virus** tab.

This will open the **Scan** window.

2. Select the device scan area:
 - **Full scan**: scan the device's entire file system. The following objects are scanned by default: device memory and storage card.
 - **Folder scan**: scan a separate object in the device's file system or on the storage card. When the **Folder scan** item is selected, a window opens displaying the device's file system. Use the joystick buttons to navigate through the file system. In order to start the folder scan, select the necessary folder and select **Options**→**Scan**.
 - **Memory scan**: scans the processes started in the system memory and its corresponding files.
 - **Messages scan**: scan messages received by SMS, MMS or Bluetooth.

After starting the scan, a scan process window opens, stating its current status: number of objects scanned, path of the object being scanned and indicator with the results of the scan in percent.

If Kaspersky Mobile Security 9.0 detects an infected object, it performs an action in accordance with the scan parameters set.

By default, if Kaspersky Mobile Security 9.0 detects a threat, it tries to rectify it. If this is not possible, the program places the infected object in quarantine.

When the scan is completed, overall statistics are displayed on the screen with the following information:

- number of objects scanned;
- number of viruses detected, placed in the quarantine or deleted;

- number of objects passed through (for instance, a file is blocked by the operating system or a file is not executable, when scanning only executable program files);
- scan time.

In order to save battery power, the backlight of the screen is automatically disabled by default during the scan. You can edit the settings of the screen's backlight.

STARTING A SCHEDULED SCAN

Kaspersky Mobile Security 9.0 allows creation of a schedule of times at which scans will be automatically started. Scans are performed in background mode. When an infected object is detected, the action selected in the Scan settings will be performed on it.

By default, starting a scheduled scan is disabled.

To set a scan schedule:

1. Select **Scan** in the **Anti-Virus** tab.
This will open the **Scan** window.
2. Select the **Schedule** item.
This will open the **Schedule** screen.
3. Set the value for the **Auto scan** setting:
 - **Off**: disable scheduled scans.
 - **Weekly**: perform the scan once a week. Specify the **Scan day** and **Scan time** to set the day of the week, and time of day, at which the scan will start.
 - **Daily**: perform the scan every day. Specify the **Scan time** in the entry field to set the time of day at which the scan will start.
4. Press **Back** to save the changes.

QUARANTINE OF POSSIBLY INFECTED OBJECTS

Quarantine is a specific folder where Kaspersky Mobile Security 9.0 places potentially malicious objects.

Malicious objects can be detected and placed in quarantine during a device scan or during the operation of Protection.

Quarantined objects are stored in a packed format which prevents their activation, and thus they pose no threat to the device. Quarantined objects can either be deleted or restored by the user.

You can view objects placed in quarantine. For every object, its full name and date of detection are specified.

To view the list of quarantined objects:

Select the **Quarantine** item in the **Anti-Virus** tab.

This will open the **Quarantine** window, which contains a list of objects stored in Quarantine.

FILTERING OF INCOMING CALLS AND SMS MESSAGES

This section presents information on the Anti-Spam component which filters incoming messages and calls in accordance with the Black or White lists. Furthermore, this section specifies how to create the Black or White lists, select an Anti-Spam action in respect of incoming messages and calls and configure the settings of the component's operation.

ABOUT ANTI-SPAM

Anti-Spam protects the device from receiving unwanted messages and calls. Anti-Spam filters incoming SMS messages and calls using the Black and White lists created.

The lists consist of entries. Every entry can contain the following settings:

- data type (SMS message, calls, SMS message and calls), to which the filter settings apply (necessary setting);
- subscriber number from which the data is received;
- text, which may be contained in an SMS message.

Anti-Spam filters messages and calls on the basis of the settings selected (see the "Anti-Spam modes" section on page 27). According to these settings, Anti-Spam scans every incoming SMS message or call and then determines whether this message or call is wanted or unwanted (spam). As soon as Anti-Spam assigns the wanted or unwanted status to an SMS message or call, the scan is finished.

By default, the Anti-Spam algorithm consists of the following steps:

1. Scan of incoming SMS messages whether they are identical to the subscriber number and text:
 - a. From the Black list. If an entry is found in the list in which the number and text are identical to the data from the incoming SMS message, the SMS message is specified as unwanted and blocked. The program deletes the blocked SMS message.
 - b. From the White list. If an entry is found in the list in which the number and text are identical to the data from the incoming SMS message, the SMS message is specified as wanted and allowed.
2. Scanning calls and SMS messages for compliance only in respect of the number:
 - a. From the Black list. If an entry is found in the list in which the number is identical to the sender's number (while the

- text was not specified in the entry), the call or SMS message is specified as spam and blocked. The program deletes the blocked SMS message.
- b. From the White list. If an entry is found in the list in which the number is identical to the sender's number (while the text was not specified in the entry), the call or SMS message is regarded as desired and allowed.
3. Message scan for compliance only in respect of the text:
 - a. From the Black list. If an entry is found in the list in which the text is identical to the data from the incoming SMS message (while the number was not specified in the entry), the SMS message is specified as spam and blocked. The program deletes the blocked SMS message.
 - b. From the White list. If an entry is found in the list in which the text is identical to the data from the incoming SMS message (while the number was not specified in the entry), the SMS message is specified as wanted and allowed.
 4. Selection of action. If no compliance is found either in the Black or White lists, Anti-Spam by default allows calls and SMS messages through and suggests taking action in respect of calls/messages in the notification window. Furthermore, you can view additional information in the notification. A received call states the number of the caller. For an SMS message, the subscriber number and its contents are displayed.

Information about blocked SMS messages and calls is registered in the application's log.

ANTI-SPAM MODES

An Anti-Spam mode is a basic configuration, or collection of parameters, of the component which protects your device against unwanted messages and calls.

The following Anti-Spam modes are available:

- **Both lists:** filtration of incoming SMS messages and calls with the use of Black and White lists. When an SMS message or call is received from a phone number which is not entered in any of the lists, the user is notified. Then they are prompted to take action: allow the SMS message/call without adding the subscriber's phone number to the lists or add the phone number to the Black or White list.

This is the default mode.

- **Black List:** block SMS messages and calls which match Black List entries. Blocked SMS messages are deleted. All other SMS messages and calls are delivered.
- **White List:** deliver SMS messages and calls which match White List entries. All other SMS messages and calls will be blocked. Blocked SMS messages are deleted.
- **Off:** do not filter SMS messages and calls.

You can edit the Anti-spam mode (see the "Changing the Anti-Spam mode" section on page 28). The current Anti-Spam mode is displayed in the **Anti-Spam** tab next to the **Mode** menu item.

CHANGING THE ANTI-SPAM MODE

To edit the settings, either use the device's joystick or select **Options** → **Change**.

To select an Anti-Spam mode, perform the following steps:

1. Select **Mode** in the **Anti-Spam** tab.
This will open the **Mode** window.
2. Select a value for the **Anti-Spam mode** setting.
3. Press **Back** to save the changes.

RESTRICTING OUTGOING CALLS AND SMS MESSAGES. PARENTAL CONTROL

The section presents information on the Parental Control component, which allows limiting outgoing calls and SMS messages to defined numbers. Furthermore, the section describes how to create a list of allowed and banned numbers and set the Parental Control settings.

ABOUT PARENTAL CONTROL

The Parental Control component filters outgoing SMS messages and calls using the Black and White lists.

The filtering works in the same way as described above for the Anti-Spam component: SMS messages and calls which match an entry in the Black List are blocked, but are allowed if they match an entry in the White List.

Parental Control blocks SMS messages sent using the device's standard features only. SMS messages which are sent with third-party applications are not blocked.

Information about the component's operation is recorded in the application's log

PARENTAL CONTROL MODES

A Parental Control mode is a basic configuration, or collection of parameters, of the component which allows a parent to restrict a child's range of outgoing messages and unwanted calls.

The following Parental Control modes are available:

- **Off:** disable Parental Control. Do not filter outgoing SMS messages and calls.

This mode is selected by default.

- **Black List:** block the sending of SMS messages and/or calls only to numbers from the Black List and allow all other messages and calls.
- **White List:** allow the sending of SMS messages and/or calls only to numbers from the White List and block all other messages and calls.

You can edit the Parental Control mode (see the "Changing the Parental Control mode" section on page 30).

The current Parental Control operating mode is displayed on the **Parental Control** tab next to the **Mode** menu item.

CHANGING THE PARENTAL CONTROL MODE

To edit the settings, either use the device's joystick or select **Options** → **Change**.

To change the Parental Control mode:

1. Select the **Mode** item in the **Parental Control** tab.
This will open the **Mode** window.
2. Select one of the Parental Control modes suggested.
3. Press **OK** to save the changes.

DATA PROTECTION IN THE EVENT OF LOSS OR THEFT OF THE DEVICE

The section presents information on the Anti-Theft component which ensures a complex protection of personal data if the device is stolen or lost and facilitates the search for the device. This section also specifies how to enable/disable the Anti-Theft function, set the parameters of its operation and start the protection remotely in the event of theft or loss of the device.

BLOCKING THE DEVICE

If the device is lost or stolen, the Block function allows the remote blocking of access to the device and data stored on it. The device can only be unblocked by entering the secret code.

This function does not block the device but simply enables the remote blocking option.

To edit the settings, either use the device's joystick or select **Options** → **Change**.

To enable the Block function:

1. Select the **Block** item on the **Anti-Theft** tab.
This will open the **Block** window.
2. Select the **On** value for the **Block mode** setting.
3. In order to display text on the screen of a blocked device, select the **Text when blocked** and fill in the **Enter text** field. When the device is blocked, the text Device Blocked is displayed on the screen by default.

To prevent the text from being displayed, select the **Text when blocked** setting and then delete the contents of the **Enter text** field and press **OK**.

4. Press **Back** to save the changes.

DELETING PERSONAL DATA

In the event of theft or loss of the mobile device, the Data Wipe function allows deletion of the following information stored on it remotely:

- personal data of the user (all contacts, messages, gallery, calendar and network connection settings), while Anti-theft deletes the contacts saved in the phonebook of the device and on the SIM card;
- data from memory cards;
- files from the C:\Data folder and other folders specified.

This function does not delete the data saved on the device, but includes the option to delete them.

Only after the device has received a special SMS message, will Anti-Theft delete the data from the created list of objects to be deleted (see the "Creating a list of objects to be deleted" section on page 33).

To enable the Data Wipe function:

1. On the **Anti-Theft** tab, select **Data Wipe**.
This will open the **Data Wipe** screen.
2. Select the **Mode** item.
This will open the **Mode** window.
3. Select the **Data Wipe mode** item and set the **On** value.
4. Select the data to be erased when the device receives a special SMS message:
 - to delete personal data, in the **Delete data** check the **Yes** value;
 - to delete files from C:\Data and other specified folders, in the **Delete folders**, check **Yes**.
5. Press **Back** to save the changes.
6. Go to the creation of a list of folders to be deleted (see the "Creation of a list of objects to be deleted" section on page 33).

CREATING A LIST OF OBJECTS TO BE DELETED

To add a folder to the list of folders to be deleted:

1. On the **Anti-Theft** tab, select **Data Wipe**.
This will open the **Data Wipe** screen.
2. Select the **Folders to be del.** item.
This will open the **Folders to be deleted** screen.
3. Select **Options** → **Add folder**.
4. Select the necessary folder from the folder tree and press **OK**.
The folder is added to the list.
5. Press **Back** to save the changes.

To remove a folder from the list:

1. On the **Anti-Theft** tab, select **Data Wipe**.
This will open the **Data Wipe** screen.
2. Select the **Folders to be del.** item.
This will open the **Folders to be deleted** screen.
3. Select a folder from the list and select **Options** → **Delete folder**.
4. Confirm the uninstalling by pressing the **Yes** button.

MONITORING THE REPLACEMENT OF A SIM CARD ON THE DEVICE

SIM Watch sends a message containing the new number of the inserted SIM card to a specified phone number and/or e-mail address

and blocks the device if the SIM card is replaced on the lost or stolen device.

To enable the SIM Watch function and check the replacement of the SIM card:

1. Select the **SIM Watch** item on the **Anti-Theft** tab.

This will open the **SIM Watch** window.

2. Select the **SIM Watch mode** item and set the **On** value.

3. Configure the following SIM-Watch settings:

- **E-mail address.** To obtain an e-mail with the new number of your phone, enter an e-mail address.
- **Phone number.** To automatically send a message with the new number of your phone, enter the phone number which the message is to be sent to. The phone number may begin with a digit or with a "+", and must contain digits only.
- **If SIM card replaced.** To block the device if the SIM card is replaced or if the device is turned on without it, set the **Block** value. You can unblock the device only by entering the secret code. By default, blocking the device is disabled.
- **Text when blocked.** To display a message on the screen in blocked mode, enter it in the **Enter text** field. By default, the Device Blocked text is entered.

4. Press **Back** to save the changes.

DETERMINING THE DEVICE'S GEOGRAPHICAL COORDINATES

The GPS Find function can send the device's geographical coordinates to a requesting device using an SMS message, and to a specified e-mail address.

This function only works with devices with in-built GPS receiver. If necessary the receiver will be activated automatically.

The coordinates can only be obtained if the device is in the area reached by satellites. If satellites are not available at the time of request, attempts to find them will be made at specific intervals.

To enable the GPS Find function:

1. Select the **GPS Find** item on the **Anti-Theft** tab.
This will open the **GPS Find** window.
2. Select the **On** value for the **GPS Find mode** setting.
3. Enter for the **E-mail address** setting the e-mail address which the device's coordinates should be sent to.
4. Press **Back** to save the changes.

REMOTE START OF THE ANTI-THEFT FUNCTIONS

You can send a command with a special SMS message to start the Anti-Theft function on the lost/stolen device with Kaspersky Mobile Security installed remotely. The command is received on the blocked device unnoticeably.

To send a command to the lost/stolen device:

1. On the **Additional** tab, select **Send command**.
A send special command window will open.
2. Press **Start**.
3. Select one of the functions provided, which is to be started remotely:

- **Block** (see "Blocking the device" section on page 31).
- **Data Wipe** (see "Deleting personal data" section on page 31).
- **GPS Find**.
- **Privacy Protection** (see "Privacy Protection" section on page 36).

The function used must be enabled on the device receiving the message.

4. Press **Next**.
5. Enter the phone number to which the message is sent and press **Next**.
6. Enter the secret code specified in the device receiving the message and press **Send**.

HIDING PERSONAL DATA

The section provides information on the Privacy Protection component. The component enables the hiding of confidential user data while the device is temporarily used by other persons.

PRIVACY PROTECTION

The Privacy Protection component protects personal data and prevents unwanted access to personal information while other persons temporarily use the device. The component enables the hiding of confidential user data, such as contacts (stored in the device's memory, on the SIM card or on removable media), messages and calls.

The Privacy Protection component analyses data on the basis of a list of protected contacts. For numbers from this list, the component hides the following information:

- information in the contacts list;
- entry of the number in the call log (incoming, outgoing, missed).
- SMS messages in the list of incoming, outgoing, deleted and sent SMS messages.

Information about the operation of Privacy Protection is stored in the log.

PRIVACY PROTECTION MODES

Kaspersky Mobile Security 9.0 allows managing the protection of personal data. The Privacy Protection component is started manually. By default, it is disabled.

Privacy Protection can operate in one of the following modes:

- **Normal:** the protection of confidential data is disabled. The Privacy Protection settings are accessible for modification.
- **Private:** the protection of confidential data is enabled. The Privacy Protection component hides all data related to the protected contacts. The Privacy Protection settings cannot be changed.

The component's current operating status is displayed on the **Privacy Protection** tab next to the **Mode** menu item.

Changing the mode of Privacy Protection can take some time.

CHANGING PRIVACY PROTECTION MODES

The Privacy Protection mode can be changed as follows:

- from the application interface;
- with the secret code when the device is in active waiting mode.

To change the Privacy Protection mode:

1. Select the **Mode** item on the **Privacy Protection** tab.
The **Privacy Protection mode** window opens.
2. Select a value for the setting **Privacy Protection mode** window opens.
3. Press **Back** to save the changes.

To change the Privacy Protection mode with the secret code when the device is in active waiting mode,

enter the ***secret code#**.

When the Privacy Protection mode is changed, a notification appears on the device's screen.

AUTOMATIC START OF PRIVACY PROTECTION

The protection of confidential data starts by default immediately after enabling Privacy Protection.

You can set a time upon expiry of which the Privacy Protection component starts automatically.

Disable Privacy Protection before modifying its settings.

To configure the automatic start of Privacy Protection on expiry of a set time:

1. Select the **Mode** item on the **Privacy Protection** tab.
The **Privacy Protection mode** window opens.
2. Select a time on expiry of which the Privacy Protection component is enabled automatically. To do this, set one of the suggested values for the **Hide automatically** setting.
 - **No delay**.

- **After 1 minute.**
 - **After 5 minutes.**
 - **After 15 minutes.**
 - **After 1 hour.**
 - **Off.**
3. Press **Back** to save the changes.

FILTERING NETWORK ACTIVITY. FIREWALL

The section presents information on the Firewall component which monitors incoming and outgoing connections on your device. Furthermore, the section also describes how to enable/disable the operation of the component and select the security level required.

ABOUT FIREWALL

The Firewall analyzes all network connections on your device. It blocks or permits network activity on the basis of the security level selected.

After installation, Kaspersky Mobile Security 9.0 Firewall is disabled.

To know of all blocked connections, use the Firewall notification.

Information about the operation of the Firewall is entered in the application's log.

SELECTING THE FIREWALL'S SECURITY LEVEL

To edit the settings, the device's joystick can be used or select **Options**→ **Change**.

To set the Firewall's security level:

1. On the **Firewall** tab, select the **Mode** item.

This will open the **Mode** window.

2. Select one of the security levels suggested.
3. Press **Back** to save the changes.

ENCRYPTING PERSONAL DATA

This section presents information on the Encryption component which protects confidential data on your device. Furthermore, the section also describes how to enable/disable the operation of the component and encrypt/decrypt the folders selected.

ABOUT ENCRYPTION

Kaspersky Mobile Security 9.0 does not support data encryption on mobile devices running Symbian Series 60 5-th Edition.

The Encryption component protects data on the device from being viewed by persons even if they gain access to the mobile device. The component allows encrypting any amount of non-system folders.

To decrypt data, the secret code must be entered. When, after the device switches to the energy-saving mode, the set time expires, access to data is automatically blocked.

The data in the folder will be encrypted once the command **Encrypt** is executed. Subsequently data will be encrypted and decrypted "on the fly" when data is moved into the folder, extracted from it or accessed.

After installation, Kaspersky Mobile Security 9.0 the Encryption component is disabled.

Information about the component's operation is recorded in the application's log

DATA ENCRYPTION

The Encryption component allows encrypting any amount of non-system folders which are in the device memory or on a storage card.

The list of all previously encrypted and decrypted files is accessible in the **Encryption** tab from the **Folders list**.

You can also encrypt all folders which are in the folders list immediately.

To encrypt data:

1. On the **Encryption** tab, select the **Folders list**.

This will open the **Folders list** window.

2. Select **Options** → **Add folder**.

A screen will open with the system file tree of your device.

3. Select the folder to be encrypted and then start the encryption process of the selected folder. To do this, press **Options** → **Encrypt**.

To move around the file system use the device's stylus or joystick buttons, as follows: **Up** and **Down** – to move within the selected folder, **Left** and **Right** – to move one level up or down from the current folder.

4. Press **OK**.

The encrypted folder is added to the folders list.

When the encryption process is finished, the name of the **Encrypt** item is changed to **Decrypt** in the **Options** menu.

After the encryption process, the data are automatically decrypted and encrypted when you work with data from the encrypted folder, move them out of the encrypted folder or place new data in the latter.

To encrypt all folders from the list at the same time, perform the following steps:

1. On the **Encryption** tab, select the **Folders list**.
This will open the **Folders list** window.
2. Select **Options** → **Add. actions** → **Encrypt all**.
3. Press **OK**.

DATA DECRYPTION

You can completely decrypt previously encrypted data (see "Data encryption" section on page 41). You can decrypt one or all encrypted folders on the device.

To decrypt a previously encrypted folder:

1. On the **Encryption** tab, select the **Folders list**.
The **Folders list** window will open, which contains a list of all previously decrypted and encrypted folders.
2. Select the folder from the list which you wish to decrypt and then select **Options** → **Decrypt**.
3. Press **OK** on completion of the data decryption.

When the decryption process is finished, the name of the **Decrypt** item is changed to **Encrypt** in the **Options** menu. You can use data encryption again (see "Data encryption" section on page 41).

To decrypt all folders from the list at the same time, perform the following steps:

1. On the **Encryption** tab, select the **Folders list**.
This will open the **Folders list** window.

2. Select **Options** → **Add. actions** → **Decrypt all**.
3. Press **OK**.

KASPERSKY MOBILE SECURITY 9.0 FOR MICROSOFT WINDOWS MOBILE

This section describes the operation of Kaspersky Mobile Security for mobile devices running one of these operating systems:

- Microsoft Windows Mobile 5.0.
- Microsoft Windows Mobile 6.0, 6.1, 6.5.

INSTALLING KASPERSKY MOBILE SECURITY 9.0

The application is installed on a mobile device in several steps.

Before starting the installation, it is recommended to close all other applications running.

To install Kaspersky Mobile Security 9.0:

1. Connect the mobile device to the computer using the Microsoft ActiveSync application.
2. Perform one of the following actions:
 - If you have purchased the program on a CD, run the automatic Kaspersky Mobile Security 9.0 installation on the CD purchased.

- If you have purchased the distribution package on the Internet, copy it to the mobile device, using one of these methods:
 - from the Kaspersky Lab website;
 - using the Microsoft ActiveSync application;
 - using a memory expansion card.

Run the installation, by opening the cab archive containing the distribution package on your mobile device.

3. Read the License Agreement text, which is concluded between you and Kaspersky Lab. If you agree to all terms of the agreement, press **OK**. Kaspersky Mobile Security 9.0 will then be installed on the device. If you do not agree to the terms of the License Agreement, press **Cancel**.
4. Select the interface language for Kaspersky Mobile Security 9.0 and press **OK**.
5. In order to complete the installation, restart the device. To do it, press **Reboot**.

The application is installed with the parameters recommended by the experts of Kaspersky Lab.

UNINSTALLING THE APPLICATION

To uninstall Kaspersky Mobile Security 9.0:

1. the data on your device if it was encrypted with Kaspersky Mobile Security 9.0 (see the "Data decryption" section on page 77).
2. Disable the Privacy Protection component (see "Enabling/disabling the Privacy Protection component" section on page 72).

3. Close Kaspersky Mobile Security 9.0. To do this, press **Menu → Exit**.
4. Uninstall Kaspersky Mobile Security 9.0. To do this, perform the following actions:
 - a. Press **Start → Settings**.
 - b. Select **Remove Programs** on the **System** tab
 - c. Select **Kaspersky Mobile Security** from the list of installed programs, and press the **Uninstall** button.
 - d. In the window that opens, confirm the uninstalling of the application by pressing the **Yes** button.
 - e. Enter the secret code and press **OK**.
 - f. Specify whether or not to keep the program settings and objects in quarantine:
 - To keep the application settings and the quarantined objects, press **Keep** (see Figure below).
 - In order to uninstall the application in full, press **Uninstall**.
5. Restart the device in order to complete the uninstalling of the application.

UPDATING VERSION 8.0 TO VERSION 9.0

If Kaspersky Mobile Security 8.0 is already installed on your mobile device, you can update it to Kaspersky Mobile Security 9.0.

Before updating the application version, disable Encryption – decrypt all data (see "Data decryption" section on page 77).

To update the program version:

1. Close the current version of Kaspersky Mobile Security. To do this, press **Menu** → **Exit**.
2. Copy the application's distribution package to your device, using one of these methods:
 - from the Kaspersky Lab website;
 - using the Microsoft ActiveSync application;
 - using a memory expansion card.
3. Start the Kaspersky Mobile Security 9.0 distribution package on the device.
4. Read the license agreement carefully. If you agree to its terms, press **OK**. You will be asked to first uninstall the 8.0 version.
5. Confirm the uninstalling of the application version 8.0 by pressing the **OK** button.
6. Enter the secret code set in the previous version of the application.
7. Delete the configured settings of the previous application version. To do this, press **Delete**.

The settings can only be kept when moving from one version to another within the same product generation. The parameters of 8.0 application version are incompatible with the 9.0 version.

8. In order to complete the removal process, restart the device. To do it, press **Reboot**.
9. After restarting the device, run the Kaspersky Mobile Security 9.0 installation(see "Installation of Kaspersky Mobile Security 9.0" section on page44).

If the validity period of the Kaspersky Mobile Security 8.0 license has not expired, enable program version 9.0 using the activation code of version 8.0 (see the "Activating the application" section on page 48).

GETTING STARTED

This section contains information about how to prepare Kaspersky Mobile Security 9.0 for operation (activating it and creating a secret code), run the application, update its databases and scan the device for viruses.

ACTIVATING THE APPLICATION

In order to use Kaspersky Mobile Security 9.0, it must be enabled. During the process of its activation, an activation code must be entered which is verified and registered on the servers of Kaspersky Lab. Subsequently, the application obtains and installs the key file.

You can obtain an activation code as follows:

- online, by exiting the Kaspersky Mobile Security 9.0 application and going to the website ;
- at the website;
- from Kaspersky Lab distributors.

To activate Kaspersky Mobile Security 9.0 on your device, you must have an Internet connection configured.

Before activating the application, make sure that the device's system date settings are correct.

You can activate the application as follows:

- **Activate trial license.** Select this activation method if you wish to get familiar with the application functions. A free

license key file will be installed during activation. The validity period of the trial license will be displayed on screen after completing the activation. Once the validity period of the trial license expires, the application's functions will be limited. Only the following features will be available:

- Activating the application;
- managing the application license;
- Kaspersky Mobile Security 9.0 Help system;
- disabling Encryption;
- disabling Privacy Protection.

It is impossible to reactivate a trial version.

- **Activate commercial license.** Select this method if you have purchased the commercial version of the application and obtained an activation code. After entering the activation code, the license key file is obtained and installed which provides access to the application's full range of functions. The validity period will be displayed on the device's screen. After expiry of the validity period, the application's functions will be limited; the application will no longer be updated.

ENTERING THE SECRET CODE

After activating the program, you will be asked to enter your secret code. The *secret code* prevents unauthorized access to the application settings. You can later change the secret code installed.

The secret code is requested in the following instances:

- for access to the application;
- for access to encrypted data;
- to enable/disable Privacy Protection;
- when sending a command with a special SMS message to start the following functions remotely: Block, Data Wipe, SIM Watch function, GPS Find, Privacy Protection;

- when uninstalling the application.

Please remember the secret code. If you forget it, it will be impossible to use the functions of Kaspersky Mobile Security 9.0 or to obtain access to encrypted data and uninstall the application.

You are advised to use a secret code consisting of at least 7 digits.

To enter the secret code:

1. After activating the application, enter in the **Enter new code** entry field, the digits of your new code.
2. Re-enter the same code in the **Confirm** field.
The code entered is automatically verified.
3. If the code is deemed invalid according to the results of the verification, a warning message is displayed and the application requests confirmation. In order to use the code, press **OK**. In order to create a new code, press **No**.
4. On completion, press **OK**.

STARTING THE APPLICATION

To start Kaspersky Mobile Security 9.0:

1. Select **Start** → **Programms**.
2. Select **KMS 9.0** and run the application using the stylus or the central button of your joystick.
3. Enter the secret code and press **OK**.

The application displays a window showing the current status of Kaspersky Mobile Security 9.0. To go to the application's functions, press **Menu**.

UPDATING THE APPLICATION'S DATABASES

Kaspersky Mobile Security 9.0 scans for threats based on the application databases, which contain descriptions of all the malicious programs known to date and methods for neutralizing them and descriptions of other unwanted objects. By the moment of the application installation, databases included in the Kaspersky Mobile Security 9.0 installation package may become obsolete.

We recommend you to update the application databases immediately after the application installation.

To update the application's databases, you must have an Internet connection configured on your mobile device.

To start the database update process:

1. Select **Menu** → **Anti-Virus**.

This will open the **Anti-Virus** window.

2. Select the **Update** item.

This will open the **Update** window.

3. Select the **Update** item.

The application starts the process of updating the databases from the Kaspersky Lab server. Information on the update process is displayed on the screen.

SCANNING THE DEVICE FOR VIRUSES

After installing the application, it is recommended to immediately run a scan of your mobile device for malware objects.

The first scan is performed with the settings previously set by the Kaspersky Lab experts.

To run a full scan of the device:

1. Select **Menu** → **Anti-Virus**.

This will open the **Anti-Virus** window.

2. Select the **Scan** item.

This will open the **Scan** window.

3. Select **Full scan**.

FILE SYSTEM PROTECTION

This section provides information on the Protection component which enables avoidance of infections of your device's file system. It also specifies how to activate/stop the Protection and adjust its operation settings.

ABOUT PROTECTION

Protection loads when the device's operating system starts, and stays resident in the device's memory, scanning all files that are opened, saved, or executed. Files are scanned according to the following algorithm:

1. The component intercepts every attempt by the user or by any program to access any file.
2. The file is scanned for the presence of malicious objects (malware). Malicious objects are detected by comparison with the application's databases, which contain descriptions of all known malicious objects, and methods for neutralizing them.
3. After the analysis, Kaspersky Mobile Security 9.0 may take the following courses of action:
 - If malicious code was detected in the file, the application blocks access to the file and performs the action specified in the settings.
 - If no malicious code is discovered in the file, it will be immediately restored.

Information about the scan's results is saved in the application's log.

ENABLING AND DISABLING THE PROTECTION

When activating the Protection, all actions in the system are under permanent control. To ensure the protection from malicious objects, the resources of the device are used. In order to reduce the load on the device when executing several tasks, you can temporarily stop Protection.

The Kaspersky Lab specialists strongly recommend that you do not disable Protection, since this could lead to the infection of your computer and data loss.

The current Protection status is displayed on the **Anti-Virus** window next to the **Protection** item.

You can enable / disable the Protection as follows:

- from the component settings menu;
- from the **Anti-Virus** menu.

To modify the values of the settings, use the device's joystick or stylus.

To enable Protection:

1. Select **Menu** → **Anti-Virus**.
This will open the **Anti-Virus** window.
2. Select the **Protection** item.
This will open the **Settings** window.
3. Check the **Enable Protection** box.
4. Press **OK** to save the changes.

To disable Protection:

1. Select **Menu** → **Anti-Virus**.

This will open the **Anti-Virus** window.

2. Select the **Protection** item.

This will open the **Settings** window.

3. Uncheck the **Enable Protection** box.
4. Press **OK** to save the changes.

To quickly enable/disable the Protection:

1. Select **Menu** → **Anti-Virus**.
2. This will open the **Anti-Virus** window.
3. Press the **Enable / Disable**. The name of the button will change to the opposite depending on the Protection current status.

SCANNING THE DEVICE

This section presents information on scanning for viruses which allows detecting and neutralizing threats in your device. Furthermore, this section specifies how to run the scan task, how to create a timetable to run tasks, how to select scan objects and install the action of the application with a detected threat.

ABOUT ON-DEMAND SCANS

Scanning the device helps to detect and neutralize malicious objects. Kaspersky Mobile Security 9.0 allows performing a full or partial scan of the device included – i.e. scan only the content of the device's built-in memory or a specific folder (including that located on the storage card).

The device is scanned as follows:

1. Kaspersky Mobile Security 9.0 scans the file types set.

2. Each file is scanned for the presence of malicious objects (malware). Malicious objects are detected by comparison with the application's databases, which contain descriptions of all known malicious objects, and methods for neutralizing them.

After the analysis, Kaspersky Mobile Security 9.0 may take the following courses of action:

- If malicious code was detected in the file, Kaspersky Mobile Security 9.0 blocks access to the file, and performs the action specified in the settings.
- if no malicious code is detected, the file immediately becomes accessible for operation.

A scan task is started manually or automatically in accordance with a previously set schedule (see the "Starting a scheduled scan" section on page 57).

Information about the on-demand scan's results is saved in the application's log.

STARTING A SCAN MANUALLY

You can launch an on-demand scan manually at any time: the best time is when the device's processor is not occupied performing other tasks.

To start an anti-virus scan manually:

1. Select **Menu** → **Anti-Virus**.

This will open the **Anti-Virus** window.

2. Select the **Scan** item.

This will open the **Scan** window.

3. Select the device scan area:

- **Full scan:** scan the device's entire file system. The following objects are scanned by default: device memory and storage card.

- **Memory scan:** scan the processes started in the system memory and its corresponding files.
- **Folder scan:** scan a separate object in the device's file system or on the storage card. When **Folder scan** is selected, a window displaying the device's file system will open. Use the joystick buttons to navigate through the file system. In order to start the folder scan, select the necessary folder and select **Scan**.

When the scan is started, the scan process window opens and displays the scan's status, including the number of scanned objects, the path to the object currently being scanned and an indicator giving the scan's percentage completion.

If Kaspersky Mobile Security 9.0 detects an infected object, it performs an action in accordance with the scan parameters set.

By default, if Kaspersky Mobile Security 9.0 detects a threat, it places it in quarantine.

When the scan is completed, overall statistics are displayed on the screen with the following information:

- number of objects scanned;
 - number of viruses detected, placed in the quarantine or deleted;
 - number of objects passed through (for instance, a file is blocked by the operating system or a file is not executable, when scanning only executable program files);
 - scan time.
4. On completion, press **OK**.

STARTING A SCHEDULED SCAN

Kaspersky Mobile Security allows you to create a schedule of times at which scans will be automatically started. Scans are performed in background mode. When an infected object is detected, the action selected in the Scan settings will be performed on it.

By default, scheduled scans are disabled.

To configure a scheduled scan:

1. Select **Menu** → **Anti-Virus**.
This will open the **Anti-Virus** window.
2. Select the **Scan** item.
This will open the **Scan** window.
3. Select the **Scan schedule** item.
This will open the **Schedule** screen.
4. Check the **Scan by schedule** box.
5. Select one of the values for the **Frequency** setting:
 - **Daily**: perform the scan every day. Specify the **Time** in the entry field to set the time of day at which the scan will start.
 - **Weekly**: perform the scan once a week. Specify the **Time** and **Day of the week**.
6. Press **OK** to save the changes.

QUARANTINING MALWARE OBJECTS

Quarantine is a specific folder where Kaspersky Mobile Security 9.0 places potentially malicious objects.

Malicious objects can be detected and placed in quarantine during a device scan or during the operation of Protection.

Quarantined objects are stored in a packed format which prevents their activation, and thus they pose no threat to the device. Quarantined objects can either be deleted or restored by the user.

You can view objects placed in quarantine. For every object, its full name and date of detection are specified.

To view the list of objects in quarantine:

1. Select **Menu** → **Anti-Virus**.

This will open the **Anti-Virus** window.

2. Select the **Quarantine** item.

This will open the **Quarantine** window, which contains a list of objects stored in Quarantine.

FILTERING OF INCOMING CALLS AND SMS MESSAGES

This section presents information on the Anti-Spam component which filters incoming messages and calls in accordance with the Black or White lists. Furthermore, this section specifies how to create the Black or White lists, select an Anti-Spam action in respect of incoming messages and calls and configure the settings of the component's operation.

ABOUT ANTI-SPAM

Anti-Spam protects the device from receiving unwanted messages and calls. Anti-Spam filters incoming SMS messages and calls using the Black and White lists created.

The lists consist of entries. Every entry can contain the following settings:

- data type (SMS message, calls, SMS message and calls), to which the filter settings apply (necessary setting);
- subscriber number from which the data is received;
- text, which may be contained in an SMS message.

Anti-Spam filters SMS messages and calls on the basis of the settings selected (see the "Anti-Spam modes" section on page 60). According to these settings, Anti-Spam scans every incoming SMS message or call and then determines whether this message or call is wanted or unwanted (spam). As soon as Anti-Spam assigns the wanted or unwanted status to an SMS message or call, the scan is finished.

By default, the Anti-Spam algorithm consists of the following steps:

1. Scan of incoming SMS messages whether they are identical to the subscriber number and text:
 - a. From the Black list. If an entry is found in the list in which the number and text are identical to the data from the incoming SMS message, the SMS message is specified as unwanted and blocked. The program deletes the blocked SMS message.
 - b. From the White list. If an entry is found in the list in which the number and text are identical to the data from the incoming SMS message, the SMS message is specified as wanted and allowed.
2. Scanning calls and SMS messages for compliance only in respect of the number:
 - a. From the Black list. If an entry is found in the list in which the number is identical to the sender's number (while the text was not specified in the entry), the call or SMS message is specified as spam and blocked. The program deletes the blocked SMS message.
 - b. From the White list. If an entry is found in the list in which the number is identical to the sender's number (while the text was not specified in the entry), the call or SMS message is regarded as desired and allowed.

3. Message scan for compliance only in respect of the text:
 - a. From the Black list. If an entry is found in the list in which the text is identical to the data from the incoming SMS message (while the number was not specified in the entry), the SMS message is specified as spam and blocked. The program deletes the blocked SMS message.
 - b. From the White list. If an entry is found in the list in which the text is identical to the data from the incoming SMS message (while the number was not specified in the entry), the SMS message is specified as wanted and allowed.
4. Selection of action. If no compliance is found either in the Black or White lists, Anti-Spam by default allows calls and SMS messages through and suggests taking action in respect of calls / messages in the notification window. Furthermore, you can view additional information in the notification. A received call states the number of the caller. For an SMS message, the subscriber number and its contents are displayed.

Information about blocked SMS messages and calls is registered in the application's log.

ANTI-SPAM MODES

An Anti-Spam mode is a basic configuration, or collection of parameters, of the component which protects your device against unwanted messages and calls.

The following Anti-Spam modes are available:

- **Off:** all SMS messages and calls are delivered. Disabling Anti-Spam.
- **White List:** SMS messages and calls which match White List entries are passed through. All other SMS messages and calls will be blocked. Blocked SMS messages are deleted.

- **Black List:** SMS messages and calls which match Black List entries are blocked. Blocked SMS messages are deleted. All other SMS messages and calls will be blocked.
- **Both lists:** incoming SMS messages and calls are filtered using both the Black and White lists. If an SMS message or a call is received from a phone number not found in either list, Anti-Spam will notify you and will advise you either to block or receive the SMS message or call, and to add this phone number to the White or the Black List. This is the default mode.

You can edit the Anti-spam mode (see the "Changing the Anti-Spam mode" section on page 61). The current Anti-Spam mode is displayed in the **Anti-Spam** window next to the **Mode** menu item.

CHANGING THE ANTI-SPAM MODE

To select an Anti-Spam operation mode:

1. Select **Menu** → **Anti-Spam**.
This will open the **Anti-Spam** window.
2. Select the **Mode** item.
This will open the **Mode** window.
3. Select a value for the **Anti-Spam mode** setting.
4. Press **OK** to save the changes.

RESTRICTING OUTGOING CALLS AND SMS MESSAGES. PARENTAL CONTROL

The section presents information on the Parental Control component, which allows limiting outgoing calls and SMS messages to defined

numbers. Furthermore, the section describes how to create a list of allowed and banned numbers and set the Parental Control settings.

ABOUT PARENTAL CONTROL

The Parental Control component filters outgoing SMS messages and calls using the Black and White lists.

The filtering works in the same way as described above for the Anti-Spam component: SMS messages and calls which match an entry in the Black List are blocked, but are allowed if they match an entry in the White List.

Parental Control blocks SMS messages sent using the device's standard features only. SMS messages which are sent with third-party applications are not blocked.

Information about the component's operation is recorded in the application's log

PARENTAL CONTROL MODES

A Parental Control mode is a basic configuration, or collection of parameters, of the component which allows a parent to restrict a child's range of outgoing messages and unwanted calls.

The following Parental Control modes are available:

- **Off:** disable Parental Control. Do not filter outgoing SMS messages and calls.

This mode is selected by default.

- **White List:** allow the sending of SMS messages and/or calls only to numbers from the White List. All other messages and calls will be blocked.
- **Black List:** block the sending of SMS messages and/or calls only to numbers from the Black List. All other messages and calls will be passed through.

You can change the Parental Control mode (see "Enabling/disabling Parental Control" section on page 63). The current Parental Control

mode is displayed in the **Parental Control** window next to the **Mode** item.

ENABLING/DISABLING PARENTAL CONTROL

To change the Parental Control mode:

1. Select **Menu** → **Parental Control**.
2. This will open the **Parental Control** window.
3. Select the **Mode** item.

This will open the **Mode** window.

4. Select one of the Parental Control modes suggested.
5. Press **OK** to save the changes.

DATA PROTECTION IN THE EVENT OF LOSS OR THEFT OF THE DEVICE

The section presents information on the Anti-Theft component which ensures a complex protection of personal data if the device is stolen or lost and facilitates the search for the device. This section also specifies how to enable/disable the Anti-Theft function, set the parameters of its operation and start the protection remotely in the event of theft or loss of the device.

ABOUT ANTI-THEFT

Anti-Theft protects data stored on the device from unauthorized access. This function can be useful if the device is lost or stolen. Anti-Theft allows blocking the device remotely and deleting data on it.

This component includes the following functions:

- **Block:** allows blocking the device at the user's request and setting a text which is displayed on the screen in blocked mode.
- **Data Wipe:** allows irrecoverable deletion from the device of the user's personal data (all contacts, messages, gallery, calendar, logs, and network access settings), data from memory cards, and files from selected folders.
- **SIM Watch:** notifies the user and blocks the stolen device if the SIM card was replaced, or the device was turned on without the SIM card. SIM Watch sends a message to a specified phone number and/or e-mail address containing the device's new phone number.
- **GPS Find:** allows the user to determine remotely the location of the device, which can be sent as a message either to the requesting device or to a specified e-mail address.

This function only works with devices with in-built GPS receiver.

To use every function of Anti-Theft, you must remember the secret code created when running Kaspersky Mobile Security 9.0 for the first time.

After installing Kaspersky Mobile Security 9.0, all Anti-Theft functions are disabled.

Furthermore, Kaspersky Mobile Security 9.0 allows starting the Anti-Theft function remotely by sending a command to the lost/stolen device (see the "Remote start of Anti-theft functions" section on page 70).

The current status of every function is displayed in the **Anti-Theft** window next to the name of the function.

Information about the component's operation is recorded in the application's log

BLOCKING THE DEVICE

If the device is lost or stolen, the Block function allows the remote blocking of access to the device and data stored on it. The device can only be unblocked by entering the secret code.

This function does not block the device but simply enables the remote blocking option.

To enable the Block function:

1. Select **Menu** → **Anti-Theft**.

This will open the **Anti-Theft** window.

2. Select the **Block** item.

This will open the **Block** window.

3. Check the **Enable Block** box.

4. Enter the message which is displayed on the device's screen in blocked mode in the **Test when blocked** field. By default, the standard text in which you can add the owner's telephone is used for the message.

5. Press **OK** to save the changes.

DELETING PERSONAL DATA

In the event of theft or loss of the mobile device, the Data Wipe function allows deletion of the following information stored on it remotely:

- personal data of the user (all contacts, messages, gallery, calendar and network connection settings), while Anti-theft deletes the contacts saved in the phonebook of the device and on the SIM card;
- data from memory cards;

- files from the My Documents folder and other folders specified.

This function does not delete the data saved on the device, but includes the option to delete them.

Only after the device has received a special SMS message, will Anti-Theft delete the data from the created list of objects to be deleted (see the "Creating a list of objects to be deleted" section on page 67).

To enable the Data Wipe function:

1. Select **Menu** → **Anti-Theft**.

This will open the **Anti-Theft** window.

2. Select the **Data Wipe** item.

This will open the **Data Wipe** screen.

3. Select the **Mode** item.

This will open the **Data Wipe** screen.

4. Check the **Enable Data Wipe** box.

5. Select the type of data to be deleted. To do this, check the boxes next to the desired settings in the **Delete** block:

- to delete personal data, check the **Personal data** box;
- to delete files from the My Documents folder and other folders specified, check the **Folders** box.

6. Press **OK** to save the changes.

7. Go to the creation of a list of folders to be deleted (see the "Creation of a list of objects to be deleted" section on page 67).

CREATING THE LIST OF DELETED DATA

The Data Wipe function allows to create a list of folders to be deleted after receipt of the special SMS message..

To add a folder to the list of folders to be deleted:

1. Select **Menu** → **Anti-Theft**.
This will open the **Anti-Theft** window.
2. Select the **Data Wipe** item.
This will open the **Data Wipe** screen.
3. Select the **Folders to be deleted** item.
This will open the **Folders to be deleted** screen.
4. Select **Options** → **Add folder**.
5. Select the necessary folder from the folder tree and press **Select**.

The folder is added to the list.

To remove a folder from the list:

1. Select **Menu** → **Anti-Theft**.
This will open the **Anti-Theft** window.
2. Select the **Data Wipe** item.
This will open the **Data Wipe** screen.
3. Select the **Folders to be deleted** item.
This will open the **Folders to be deleted** screen.
4. Select a folder from the list and press **Menu** → **Delete**.

MONITORING THE REPLACEMENT OF A SIM CARD ON THE DEVICE

SIM Watch sends a message containing the new number of the inserted SIM card to a specified phone number and/or e-mail address and blocks the device if the SIM card is replaced on the lost or stolen device.

To enable the SIM Watch function and monitor the replacement of the SIM card:

1. Select **Menu** → **Anti-Theft**.

This will open the **Anti-Theft** window.

2. Select the **SIM Watch** item.

This will open the **SIM Watch** window.

3. Check the **Enable SIM Watch** box.

4. To check the replacement of the SIM card on the device, make the following settings:

- To automatically send a message about a new telephone number, enter the phone number which the message is sent to in the **Phone number** field in the **Send new number** block.

The phone number may begin with a digit or with a "+", and must contain digits only.

- To receive an e-mail about a new number of your telephone, enter an e-mail address in the **E-mail address** field of the **Send new number** field.
- To block the device when the SIM card is replaced or when the device is switched on without a card, for the **When replacing the SIM card** setting, check the **Block device** box. You can unblock the device only by entering the secret code.

- To display a message on the screen in blocked mode, enter it in the **Text when blocked** field. By default, the standard text in which you can add the owner's number is used for the message.
5. Press **OK** to save the changes.

DETERMINING THE DEVICE'S GEOGRAPHICAL COORDINATES

The GPS Find function can send the device's geographical coordinates to a requesting device using an SMS message, and to a specified e-mail address.

This function only works with devices with in-built GPS receiver. If necessary the receiver will be activated automatically.

The coordinates can only be obtained if the device is in the area reached by satellites. If satellites are not available at the time of request, attempts to find them will be made at specific intervals.

To enable the GPS Find function:

1. Select **Menu** → **Anti-Theft**.

This will open the **Anti-Theft** window.

2. Select the **GPS Find** item.

This will open the **GPS Find** window.

3. Check the **Enable GPS Find** box.

By default, Kaspersky Mobile Security 9.0 sends the device's coordinates in a response SMS message.

4. To receive the device's coordinates by e-mail too, for the **Send coordinates** setting enter the e-mail address.

5. Press **OK** to save the changes.

REMOTE START OF THE ANTI-THEFT FUNCTIONS

You can send a command with a special SMS message to start the Anti-Theft function on the lost/stolen device with Kaspersky Mobile Security installed remotely. The command is received on the blocked device unnoticeably.

It is recommended to use the Send command function because then the command and secret code of the stolen/lost device is transmitted with encryption.

To send a command to the lost/stolen device:

1. Select **Menu** → **Additional**.
This will open the **Additional** window.
2. Select the **Send command** item.
3. This will open the **Send command** window.
4. Select one of the values suggested for the **Function** setting:
 - **Block**.
 - **Data Wipe**.
 - **GPS Find**.
 - **Privacy Protection** (see "Hiding personal data" section on page 71).
5. In the **Phone number** field, enter the device's phone number to which the SMS message must be sent.
6. In the **Remote code** field, enter the secret code set on the device receiving the message.
7. Press **Send**.

HIDING PERSONAL DATA

The section provides information on the Privacy Protection component. The component enables the hiding of confidential user data while the device is temporarily used by other persons.

PRIVACY PROTECTION

The Privacy Protection component protects personal data and prevents unwanted access to personal information while other persons temporarily use the device. The component enables the hiding of confidential user data, such as contacts (stored in the device's memory, on the SIM card or on removable media), messages and calls.

The component analyses personal data on the basis of the list of protected numbers. For numbers from this list, the component hides the following information:

- information in the contacts list;
- entry of the number in the call log (incoming, outgoing, missed).
- SMS messages in the list of incoming, outgoing, deleted and sent SMS messages.

Information about the operation of Privacy Protection is stored in the log.

PRIVACY PROTECTION MODES

Kaspersky Mobile Security 9.0 allows managing the protection of personal data. The Privacy Protection component is started manually. By default, it is disabled.

Privacy Protection can operate in one of the following modes:

- **Normal:** the protection of confidential data is disabled. The Privacy Protection settings are accessible for modification.

- **Private:** the protection of confidential data is enabled. The Privacy Protection component hides all data related to the protected contacts. The Privacy Protection settings cannot be changed.

The component's current operating status is displayed on the **Privacy Protection** window next to the **Mode** menu item.

Changing the mode of Privacy Protection can take some time.

ENABLING / DISABLING PRIVACY PROTECTION

The Privacy Protection mode can be changed as follows:

- from the component settings menu;
- from the **Privacy Protection** menu.

To change the Privacy Protection mode:

1. Select **Menu** → **Privacy Protection**.
This will open the **Privacy Protection** window.
2. Select the **Mode** item.
This will open the **Mode** window.
3. Select a value for the **Mode** setting.
4. Press **OK**.
5. Confirm changing the mode of Privacy Protection. To do so, press the **OK** button.

To quickly change the Privacy Protection mode:

1. Select **Menu** → **Privacy Protection**.
This will open the **Privacy Protection** window.

2. Press **Private / Normal**. The name of the button will change to the opposite depending on the Privacy Protection current status.
3. Confirm changing the mode of Privacy Protection. To do so, press the **OK** button.

AUTOMATIC START OF PRIVACY PROTECTION

The protection of confidential data starts by default immediately after enabling Privacy Protection.

You can set a time upon expiry of which the Privacy Protection component starts automatically.

Disable the Privacy Protection component before modifying its settings.

To configure the automatic start of Privacy Protection on expiry of a set time:

1. Select **Menu** → **Privacy Protection**.
This will open the **Privacy Protection** window.
2. Select the **Mode** item.
3. This will open the **Mode** window.
4. Check the **Block access** box.
5. Select a time on expiry of which the Privacy Protection component is enabled automatically. To do this, set one of the suggested values for the **Time-out** setting:
 - **No delay**.
 - **After 1 minute**.
 - **After 5 minutes**.

- **After 15 minutes.**
 - **After 1 hour.**
6. Press **OK**.

FILTERING NETWORK ACTIVITY. FIREWALL

The section presents information on the Firewall component which monitors incoming and outgoing connections on your device. Furthermore, the section also describes how to enable/disable the operation of the component and select the security level required.

ABOUT FIREWALL

The Firewall analyzes all network connections on your device. It blocks or permits network activity on the basis of the security level selected.

After installation, Kaspersky Mobile Security 9.0 Firewall is disabled.

Information about the operation of the Firewall is entered in the application's log.

SELECTING THE FIREWALL'S SECURITY LEVEL

To modify the values of the settings, use the device's joystick or stylus.

To set the Firewall's security level:

1. Select **Menu** → **Firewall**.
This will open the **Firewall** window.
2. Select the **Mode** item.
This will open the **Settings** window.

3. Select one of the security levels suggested.
4. and press **OK**.

ENCRYPTING PERSONAL DATA

This section presents information on the Encryption component which protects confidential data on your device. Furthermore, the section also describes how to enable/disable the operation of the component and encrypt/decrypt the folders selected.

ABOUT ENCRYPTION

The Encryption component protects data on the device from being viewed by persons even if they gain access to the mobile device. The component allows encrypting any amount of non-system folders.

To encrypt/decrypt data, the secret code must be entered (see "Entering the secret code" section on page 49). When, after the device switches to the energy-saving mode, the set time expires, access to data is automatically blocked.

The data in the folder will be encrypted once the command **Encrypt** is executed. Subsequently data will be encrypted and decrypted "on the fly" when data is moved into the folder, extracted from it or accessed.

Executable (.exe) files cannot be run from an encrypted folder.

After installation, Kaspersky Mobile Security 9.0 the Encryption component is disabled.

Information about the component's operation is recorded in the application's log

DATA ENCRYPTION

The Encryption component allows encrypting any amount of non-system folders which are in the device memory or on a storage card.

The list of all previously encrypted and decrypted files is accessible in the **Encryption** window from the **Folders list**.

You can also encrypt all folders which are in the folders list immediately.

To encrypt data:

1. Select **Menu** → **Encryption**.

This will open the **Encryption** window.

2. Select the **Folders list** item.

This will open the **Folders list** window.

3. Press **Menu** → **Add folder**.

A screen will open with the system file tree of your device.

4. Select the folder to be encrypted and then press **Encrypt**.

To move around the file system use the device's stylus or joystick buttons.

When the encryption procedure is completed, Kaspersky Mobile Security 9.0 notifies you of this. The notification window will appear.

5. Press **OK**.

For an encrypted folder, the name of the **Encrypt** item changes to **Decrypt** in the **Menu**.

After the encryption process, the data are automatically decrypted and encrypted when you work with data from the encrypted folder, move them out of the encrypted folder or place new data in the latter.

To encrypt all folders from the list at the same time, perform the following steps:

1. Select **Menu** → **Encryption**.

This will open the **Encryption** window.

2. Select the **Folders list** item.

This will open the **Folders list** window.

3. Select **Menu** → **Add. actions** → **Encrypt all**.

When the encryption procedure is completed, Kaspersky Mobile Security 9.0 notifies you of this. The notification window will appear.

4. Press **OK**.

DATA DECRYPTION

You can completely decrypt previously encrypted data (see "Data encryption" section on page 75). You can decrypt one or all encrypted folders on the device.

To decrypt a previously encrypted folder:

1. Select **Menu** → **Encryption**.

This will open the **Encryption** window.

2. Select the **Folders list** item.

The **Folders list** window will open, which contains a list of all previously decrypted and encrypted folders.

3. Select the encrypted folder from the list and press **Menu** → **Decrypt**.

When the decryption procedure is completed, Kaspersky Mobile Security 9.0 notifies you of this. The notification window will appear.

4. Press **OK**.

For an decrypted folder, the name of the **Decrypt** item changes to **Encrypt** in the **Menu**. You can use data encryption again (see "Data encryption" section on page 75).

To decrypt all folders from the list at the same time, perform the following steps:

1. Select **Menu** → **Firewall**.

This will open the **Firewall** window.

2. Select the **Folders list** item.

This will open the **Folders list** window.

3. Select **Menu** → **Add. actions** → **Decrypt all**.

When the decryption procedure is completed, Kaspersky Mobile Security 9.0 notifies you of this. The notification window will appear.

4. Press **OK**.

CONTACTING THE TECHNICAL SUPPORT SERVICE

If you have already purchased Kaspersky Internet Security, you can obtain information about it from the Technical Support Service, either over the phone or via the Internet.

Technical Support Service specialists will answer any of your questions about installing and using the application. They will also help you to eliminate the consequences of malware activities if your device has been infected.

Before contacting the Technical support service, please read the Support rules for Kaspersky Lab's products (<http://support.kaspersky.com/support/rules>).

E-mailing your question to the Technical Support Service

You can forward your question to the Technical Support Service specialists by filling out a Helpdesk web form at (<http://support.kaspersky.com/helpdesk.html>).

You can write your inquiry in Russian, English, German, French or Spanish.

To send an e-mail message with your question, you must include the **Customer ID** and **password** you received when you registered at the Technical Support Service's website.

If you are not a registered user of Kaspersky Lab's applications, you can fill out a registration form (<https://support.kaspersky.com/personalcabinet/registration/form/>). During registration enter the *activation code* for your application, or the *key filename*.

The Technical Support Service will respond to your request in your Personal Cabinet (<https://support.kaspersky.com/PersonalCabinet>) and to the e-mail address you specified in your inquiry.

In your inquiry, please describe the problem you have encountered. Specify the following in the mandatory fields:

- **Request type.** Select a topic which corresponds to the arising problem most closely, for instance "Product Installation/Removal Problem" or "Anti-Virus scan/virus removal problem". If you do not find an appropriate topic, select "General question".
- **Application name and version number.**
- **Request text.** Describe the problem you encountered, providing as much relevant detail as possible.
- **Customer ID and password.** Enter the customer ID and password you received when you registered at the Technical Support Service's website.

- **E-mail address.** The Technical Support Service will reply to your question at this email address.

Technical support by phone

If you have an urgent problem, you can call your local Technical Support Service. Before contacting your local (http://support.kaspersky.com/support/support_local) or international (<http://support.kaspersky.com/support/international>) Technical Support Service, please collect the necessary information (<http://support.kaspersky.com/support/details>) about your device and the installed anti-virus application. This will enable our specialists to help you more quickly.