

ЛАБОРАТОРИЯ КАСПЕРСКОГО

Kaspersky Mobile Security 7.0

РУКОВОДСТВО
ПОЛЬЗОВАТЕЛЯ

KASPERSKY MOBILE SECURITY 7.0

Руководство пользователя

© ЗАО «Лаборатория Касперского»
Тел., факс: +7 (495) 797-8700, +7 (495) 645-7939,
+7 (495) 956-7000
<http://www.kaspersky.ru>

Дата редакции: февраль 2008 года

Содержание

ГЛАВА 1. KASPERSKY MOBILE SECURITY 7.0.....	5
1.1. Аппаратные и программные требования.....	6
1.2. Комплект поставки.....	6
ГЛАВА 2. KASPERSKY MOBILE SECURITY ДЛЯ SYMBIAN OS.....	7
2.1. Установка Kaspersky Mobile Security.....	7
2.2. Работа с приложением.....	8
2.2.1. Активация приложения.....	9
2.2.2. Запуск приложения.....	9
2.2.3. Графический интерфейс.....	10
2.2.4. Общие настройки.....	11
2.2.5. Антивирусная проверка и защита.....	12
2.2.6. Использование карантина.....	17
2.2.7. Использование Анти-Спама и модуля Anti-Theft.....	19
2.2.8. Обновление баз приложения.....	28
2.2.9. Использование модуля Firewall.....	31
2.2.10. Получение отчета о работе приложения.....	32
2.3. Удаление приложения.....	33
ГЛАВА 3. KASPERSKY MOBILE SECURITY ДЛЯ MICROSOFT WINDOWS MOBILE.....	35
3.1. Установка Kaspersky Mobile Security.....	35
3.2. Начало работы.....	36
3.2.1. Активация приложения.....	36
3.2.2. Запуск приложения.....	38
3.2.3. Графический интерфейс.....	39
3.3. Антивирусная проверка и защита.....	40
3.3.1. Постоянная защита и проверка по требованию.....	41
3.3.2. Проверка по расписанию.....	45
3.4. Использование карантина.....	46
3.5. Использование Анти-Спама и модуля Anti-Theft.....	47
3.5.1. Модуль Анти-Спам.....	47

3.5.2. Редактирование «черного» и «белого» списков	48
3.5.3. Действия над сообщениями.....	49
3.5.4. Модуль Anti-Theft	50
3.6. Обновление баз приложения	54
3.7. Сетевой экран	56
3.8. Получение отчетов о работе приложения	57
3.9. Удаление приложения	58
ПРИЛОЖЕНИЕ А. ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО».....	62
А.1. Другие разработки «Лаборатории Касперского»	63
А.2. Наши координаты	75

ГЛАВА 1. KASPERSKY MOBILE SECURITY 7.0

Kaspersky Mobile Security 7.0 предназначен для защиты смартфонов и коммуникаторов на базе операционных систем Symbian OS и Microsoft Windows Mobile от вредоносных программ, нежелательных сообщений и выполняет следующие функции:

- **постоянная защита** файловой системы устройства – перехват и проверка:
 - всех входящих объектов, передающихся с помощью беспроводных соединений (инфракрасный порт, Bluetooth), сообщений EMS и MMS, при синхронизации с персональным компьютером и загрузке файлов через браузер;
 - файлов, открываемых на мобильном устройстве;
 - программ, устанавливаемых из интерфейса устройства.
- **проверка объектов** файловой системы, находящихся на мобильном устройстве или на подключенных картах расширения памяти, по требованию пользователя и по расписанию;
- **надежное изолирование зараженных объектов** в карантинном хранилище;
- **обновление баз Kaspersky Mobile Security**, используемых при поиске вредоносных программ и удалении опасных объектов.
- **блокирование нежелательных SMS- и MMS-сообщений.**
- **блокирование доступа или удаление данных пользователя** в случае несанкционированных действий по отношению к устройству, например, его кражи.
- **защита мобильного устройства на сетевом уровне.**

Пользователю предоставляется возможность гибкого управления настройками Kaspersky Mobile Security, просмотра текущего состояния антивирусной защиты, а также журнала событий, где фиксируются действия приложения.

В приложении реализована система меню и поддерживается удобный пользовательский интерфейс.

Примечание

В случае обнаружения вредоносной программы Kaspersky Mobile Security позволяет вылечить зараженный объект (если лечение возможно), удалить или поместить его на карантин. При этом копия удаляемого объекта не сохраняется.

1.1. Аппаратные и программные требования

Kaspersky Mobile Security устанавливается на смартфоны и коммуникаторы, работающие под управлением следующих операционных систем:

- Symbian OS 9.1, 9.2 Series 60 UI.
- Microsoft Windows Mobile 5.0.
- Microsoft Windows Mobile 6.0.

1.2. Комплект поставки

Kaspersky Mobile Security можно приобрести через интернет (дистрибутив приложения и документация в электронном виде). Также Kaspersky Mobile Security распространяется через офисы мобильной связи. За подробной информацией обращайтесь к вашему сотовому оператору.

ГЛАВА 2. KASPERSKY MOBILE SECURITY ДЛЯ SYMBIAN OS

Эта глава содержит описание работы с Kaspersky Mobile Security 7.0 для смартфонов, работающих под управлением операционной системы Symbian версий 9.1, 9.2 и Series 60 UI.

2.1. Установка Kaspersky Mobile Security

Для того чтобы установить Kaspersky Mobile Security, выполните следующие действия:

1. Скопируйте дистрибутив приложения на смартфон.
2. Запустите установку (откройте файл дистрибутива на смартфоне).
3. Для подтверждения установки выберите **Да** (см. рис. 1).

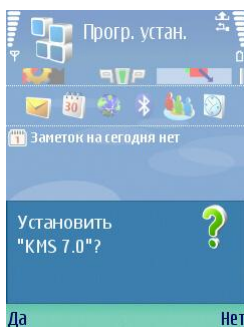


Рисунок 1. Запрос об установке

4. Выберите место установки: память телефона или карта расширения памяти (см. рис. 2).

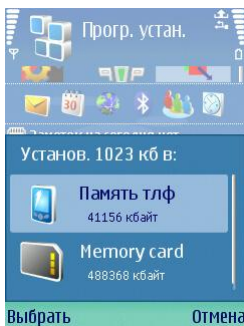


Рисунок 2. Выбор места установки

5. В случае несовпадения языковых версий операционной системы Kaspersky Mobile Security на экран будет выведено соответствующее сообщение. Для продолжения установки приложения на русском языке нажмите **ОК**.
6. Прочтите текст лицензионного соглашения. Если вы согласны с условиями соглашения, нажмите **ОК**. Для отказа от установки нажмите **Отмена** (см. рис. 3).

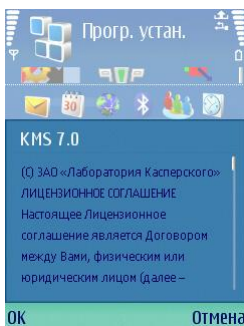


Рисунок 3. Лицензионное соглашение

2.2. Работа с приложением

В этом разделе содержатся сведения по настройке параметров антивирусной проверки и постоянной защиты, фильтрации SMS- и MMS-сообщений, выполнении антивирусной проверки смартфона, обновлении приложения, защиты смартфона на сетевом уровне и др.

2.2.1. Активация приложения

При первом запуске приложения на экране смартфона отображается окно активации Kaspersky Mobile Security (см. рис. 4).

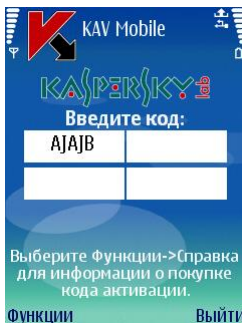


Рисунок 4. Окно активации приложения

Активация приложения необходима, без нее все функции Kaspersky Mobile Security недоступны. Код активации вы можете получить на сайте «Лаборатории Касперского».

Внимание!

Для активации Kaspersky Mobile Security на смартфоне необходимо иметь GPRS- или WLAN-подключение.

Код активации состоит из букв латинского алфавита и цифр, регистр не имеет значения. Введите код последовательно в 4 поля.

После ввода кода активации выберите **Активировать** в меню **Функции**. Приложение осуществит http-запрос на сервер активации «Лаборатории Касперского», скачает и установит ключ.

В случае если введенный вами код активации по каким-либо причинам окажется недействительным, на экране смартфона будет показано соответствующее сообщение.

2.2.2. Запуск приложения

Чтобы запустить Kaspersky Mobile Security, выполните следующие действия:

1. Откройте главное меню телефона.

2. Выберите **KMS 7.0** и запустите приложение, используя пункт **Открыть** в меню **Функции**.

Примечание

При первом запуске приложения, вам будет предложено включить функцию автостарта (см. п. 2.2.4 на стр. 11). Нажмите **OK** в случае согласия.

После запуска смартфона на экране смартфона отображается окно статуса основных компонентов Kaspersky Mobile Security (см. рис. 5).

- **Постоянная защита** – использование режима постоянной защиты (см. п. 2.2.5 на стр. 12).
- **Последн. проверка** – дата выполнения последней антивирусной проверки смартфона.
- **Дата выпуска баз** – дата выпуска баз антивируса, используемых приложением.
- **Анти-Спам** – режим работы Анти-Спама (см. п. 2.2.7 на стр. 19).
- **Уровень Firewall** – уровень защиты смартфона (см. п. 2.2.9 на стр. 31).

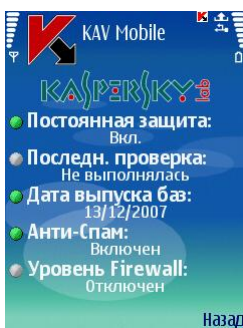


Рисунок 5. Окно статуса компонентов приложения

Для перехода к интерфейсу приложения нажмите **OK**.

2.2.3. Графический интерфейс

Графический интерфейс приложения состоит из шести закладок:

- Закладка **Проверка** позволяет выполнять антивирусную проверку смартфона, редактировать параметры антивирусной проверки и

режима постоянной защиты, настраивать расписание запуска автоматической проверки.

- Закладка **Карантин** позволяет управлять карантином – специальным хранилищем зараженных и подозрительных объектов.
- Закладка **Обновление** позволяет выполнять обновление баз антивируса, редактировать параметры обновления, настраивать расписание обновления.
- Закладка **Firewall** позволяет контролировать сетевую активность и защищать смартфон на сетевом уровне.
- Закладка **Прочее** позволяет настраивать фильтрацию входящих SMS- и MMS-сообщений (модуль Анти-Спам), а также блокировать смартфон и удалять информацию в случае кражи или потери устройства (модуль Anti-Theft).
- Закладка **Информация** позволяет просматривать журналы работы компонентов приложения, общую информацию о приложении и используемых базах, а также редактировать общие параметры работы приложения.

Для навигации между закладками воспользуйтесь джойстиком смартфона или в меню **Функции** выберите пункт **Открыть закладку** (см. рис. 6).

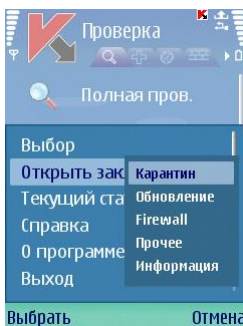


Рисунок 6. Меню **Функции**

Для того чтобы вернуться к окну статуса компонентов приложения выберите пункт **Текущий статус** в меню **Функции**.

2.2.4. Общие настройки

Параметры, расположенные на закладке **Информация** в пункте **Настройки** (см. рис. 7), позволяют вам настроить следующие функции приложения:

- **Автостарт** – режим работы автозапуска. При активном режиме автозапуска основные функции приложения запускаются при включении телефона. При выключении автозапуска работа основных функций будет остановлена. Выберите **Да**, если хотите, чтобы основные функции всегда защищали ваш телефон.
- **Показ. окно статуса** определяет, нужно ли отображать текущий статус при запуске приложения.
- **Размер журнала** определяет максимальный размер журнала. При достижении лимита старые сообщения журнала будут удаляться до максимального значения, указанного в настройке.
- **Подсветка экрана** определяет, используется ли подсветка экрана во время проверки на вирусы. По умолчанию подсветка отключена.
- **Звук** определяет использование звукового оповещения при возникновении определенных событий (обнаружение зараженного объекта, сообщения о статусе приложения и т.д.). Выберите **Вкл.**, если вы хотите использовать звуковое оповещение.
- **Вибрация** определяет, будет ли вибрировать смартфон при обнаружении зараженного объекта. По умолчанию вибрация включена.

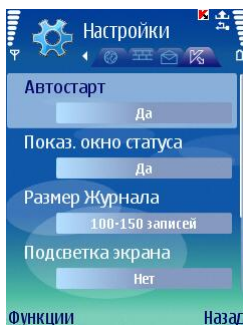


Рисунок 7. Меню **Настройки**

Для редактирования значений параметров воспользуйтесь джойстиком смартфона или выберите пункт **Изменить** в меню **Функции**.

2.2.5. Антивирусная проверка и защита

Используя закладку **Проверка**, вы можете выполнить антивирусную проверку как всей файловой системы и памяти смартфона, так и отдельного каталога или файла. Также вы можете изменить параметры антивирусной проверки и режима постоянной антивирусной защиты, просмотреть отчет о

результатах проверки и настроить расписание автоматического запуска проверки.

2.2.5.1. Постоянная защита и проверка по требованию

Постоянная защита – режим работы, при котором резидентная часть Kaspersky Mobile Security постоянно находится в оперативной памяти смартфона и контролирует все данные, в том числе и входящие (поступающие на смартфон извне).

Постоянная защита запускается с момента включения смартфона и работает до его выключения (если использование этого режима не отключено в настройках).

Также Kaspersky Mobile Security позволяет выполнять полную проверку файловой системы смартфона, включая анализ объектов, находящихся на подключенных картах расширения памяти.

Информация о результатах работы постоянной защиты и проверки по требованию заносится в отчет. Для просмотра отчета необходимо выбрать пункт **Журнал** на закладке **Проверка**.

Для того чтобы запустить режим использования постоянной защиты, выполните следующее:

1. На закладке **Проверка** выберите пункт **Настройки**.
2. Включите / выключите режим использования постоянной защиты, установив соответствующее значение параметра **Постоянная защита**.

Для того чтобы изменить параметры проверки по требованию, выполните следующее:

1. На закладке **Проверка** выберите пункт **Настройки**.
2. Задайте область проверки в блоке **Тип файлов** путем выбора типов файлов, которые необходимо проверять:
 - **Все файлы** – проверять все файлы.
 - **Исполняемые** – проверять только исполняемые файлы программ (например, *.exe, *.sis, *.mdl, *.app).
3. Определите действие при обнаружении зараженного объекта (параметр **Действие**).

Если вы хотите, чтобы при обнаружении зараженного объекта на экран смартфона выводился запрос о действии, выберите значение **Запрос**.

Для автоматического удаления без уведомления пользователя выберите значение **Удаление**.

Для автоматического перемещения обнаруженных объектов в карантин выберите **Карантин**. Помещение зараженного объекта на карантин является действием, которое выполняется по умолчанию.

4. Включите / выключите проверку ROM-памяти смартфона (параметр **Проверка ROM**).

При некоторых обстоятельствах ROM-память может быть уязвима для вредоносных программ. Для того чтобы разрешить Kaspersky Mobile Security проверять эту память, выберите значение **Да**.

5. Включите / выключите распаковку SIS- и ZIP-архивов (параметр **Распаковка архивов**).

Для того чтобы при проверке Kaspersky Mobile Security выполнял распаковку SIS- и ZIP-архивов, выберите **Да**. Если распаковка архивов при проверке не требуется, отключите эту функцию, выбрав **Нет**.

6. Включите / выключите режим проверки новой карты (параметр **Пров. новой карты**).

Для того чтобы Kaspersky Mobile Security проверял флеш-карты, устанавливаемые в смартфон, выберите **Проверка**. Для того чтобы отключить автоматическую проверку флеш-карт, выберите **Выкл**. Чтобы Kaspersky Mobile Security каждый раз при установке новой карты выводил запрос о необходимости ее проверки, выберите **Запрос**.

7. Включите / выключите отображение значка защиты (параметр **Значок защиты**).

Чтобы при включенной постоянной защите значок приложения отображался на экране смартфона, в соответствующем пункте меню выберите значение **Всегда**. Если вы хотите, чтобы значок отображался только в меню смартфона, выберите **Только в меню**. Чтобы значок не отображался, выберите **Никогда**.

Примечание

Для редактирования значения параметров воспользуйтесь джойстиком смартфона или выберите пункт **Изменить** в меню **Функции**.

По умолчанию приложение работает с настройками параметров, рекомендуемыми специалистами «Лаборатории Касперского». Если в процессе работы с приложением вы хотите вернуться к рекомендуемым настройкам, откройте закладку **Проверка** и в меню **Функции** выберите пункт **Восстановить**.

Для того чтобы запустить антивирусную проверку, выполните следующие действия:

1. Запустите Kaspersky Mobile Security (см. п. 2.2.2 на стр. 9).
2. На закладке **Проверка** (см. рис. 8) выберите пункт **Полная проверка**, если вы хотите проверить всю файловую систему смартфона, или **Пров. папки**, если вы хотите выполнить проверку отдельной папки.

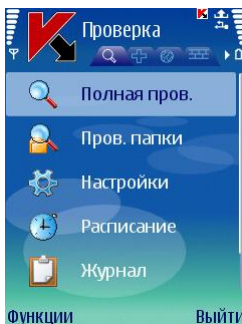


Рисунок 8. Закладка **Проверка**

При выборе пункта **Пров. папки** выполняется переход к окну, представляющему файловую систему смартфона. Для навигации по файловой системе используйте кнопки джойстика. Для того чтобы запустить проверку папки, переместите курсор на папку и выберите пункт **Проверить** в меню **Функции**.

После запуска проверки откроется окно процесса проверки, где будет указано текущее состояние: количество проверенных объектов, путь к объекту, который проверяется в данный момент, и индикатор, отображающий выполнение процесса проверки в процентах (см. рис. 9).

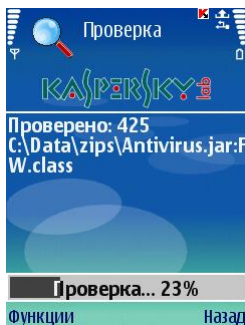


Рисунок 9. Окно процесса проверки

При обнаружении зараженного объекта вам будет предложено либо удалить зараженный файл (действие **Удалить**), либо переместить его в карантин (действие **В карантин**), либо оставить файл без изменений (действие **Пропустить**).

Внимание!

Запрос о действии над объектом выполняется приложением, только если параметру проверки **Действие** присвоено значение **Запрос** (подробнее см. п. 2.2.5.1 на стр. 13).

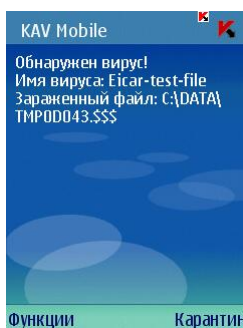


Рисунок 10. Сообщение об обнаружении вируса

По окончании проверки будет выведена общая статистика о найденных и удаленных вредоносных объектах.

Для того чтобы подсветка экрана не выключалась во время проверки, перейдите к закладке **Информация**, откройте меню **Настройки** и выберите значение **Вкл.** для параметра **Подсветка экрана**. По умолчанию, если не нажимаются клавиши смартфона, подсветка автоматически выключается в целях экономии заряда аккумулятора.

2.2.5.2. Проверка по расписанию

Kaspersky Mobile Security позволяет пользователю сформировать расписание для автоматической проверки смартфона. Проверка происходит в фоновом режиме. При обнаружении зараженного объекта над ним выполняется действие, заданное в настройках проверки (см. п. 2.2.5.1 на стр. 13).

По умолчанию проверка по расписанию выключена.

Для того чтобы настроить проверку по расписанию:

на закладке **Проверка** выберите пункт **Расписание** и настройте параметры **Автопроверки** (см. рис. 11):

- **Ежедневно** – проверка производится каждый день. В поле ввода укажите **Время проверки**.
- **Еженедельно** – проверка производится раз в неделю. Укажите **День проверки** и **Время проверки**.

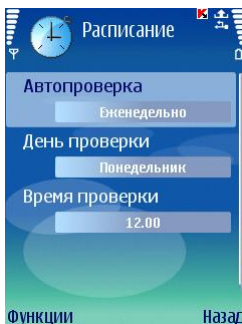


Рисунок 11. Меню **Расписание**

2.2.6. Использование карантина

Зараженные объекты, помещенные на карантин, не представляют угрозы для смартфона и могут быть впоследствии удалены либо восстановлены.

Обнаруженные зараженные объекты могут помещаться приложением на карантин автоматически, либо после вашего подтверждения.

Для того чтобы настроить приложение на автоматическое помещение зараженных объектов на карантин, перейдите на закладку **Проверка**, выберите пункт **Настройки**, и в качестве значения параметра **Действие** выберите **Карантин**.

Если в качестве действия вы выбрали **Запрос**, то при обнаружении зараженного объекта Kaspersky Mobile Security предложит вам либо удалить объект, либо поместить его на карантин.

Доступ к основным функциям карантина осуществляется при помощи закладки **Карантин** (см. рис. 12).

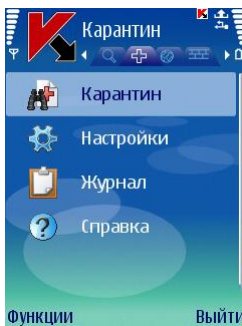


Рисунок 12. Меню **Карантин**

Выберите **Карантин** для того, чтобы просмотреть список всех объектов, содержащихся на карантине (см. рис. 13).



Рисунок 13. Зараженные объекты на карантине

Меню **Функции**, доступное в окне просмотра карантина, позволяет:

- Просмотреть детальную информацию о каждом из объектов, хранящихся на карантине (**Сведения**).
- Удалить текущий объект (**Удалить**).
- Очистить карантин, удалив все содержащиеся в нем объекты (**Удалить все**).

- Восстановить текущий объект из карантина в исходный каталог (**Восстановить**).
- Получить справку по работе с карантином (**Справка**).

Для настройки параметров карантина воспользуйтесь меню **Настройки**, расположенном на закладке **Карантин** (см. рис. 14).

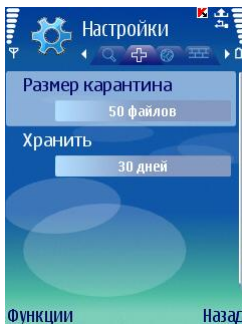


Рисунок 14. Настройки карантина

Параметр **Размер карантина** определяет максимальное количество зараженных объектов, которые могут храниться на карантине. В качестве возможных значений вы можете выбрать **20**, **50** или **100** файлов.

Параметр **Хранить** определяет период времени, в течение которого зараженные объекты могут храниться на карантине. По прошествии указанного срока зараженные объекты автоматически удаляются.

Примечание

Для того чтобы вернуть настройки параметров карантина, рекомендуемые специалистами «Лаборатории Касперского», выберите **Восстановить** в меню **Функции**.

2.2.7. Использование Анти-Спама и модуля Anti-Theft

Модуль Анти-Спам предназначен для защиты смартфона от нежелательных SMS- и MMS-сообщений.

Принцип фильтрации сообщений основан на использовании «черного» и «белого» списков. Входящие сообщения, поступившие с телефонных номеров, занесенных в «черный» список, блокируются Анти-Спамом. Получение сообщений, с номеров, занесенных в «белый» список, не блокируется.

Модуль Anti-Theft предназначен для блокирования смартфона и удаления информации, хранящейся в его памяти, в случае кражи или потери устройства.

2.2.7.1. Режимы работы Анти-Спама

Для того чтобы настроить режим работы Анти-Спама, перейдите к закладке **Прочее** и выберите пункт **Анти-Спам**, затем пункт **Настройки**. Определите один из следующих режимов работы при помощи параметра **Анти-Спам**:

- **Включен.** В данном режиме Анти-Спам выполняет фильтрацию входящих сообщений при помощи «черного» и «белого» списков. При получении сообщения с номера телефона, не занесенного ни в один из списков, Анти-Спам выдаст предупреждение пользователю и предложит заблокировать или разрешить получение сообщения, а также включить телефонный номер в «белый» или «черный» список.
- **Только списки.** В данном режиме Анти-Спам выполняет фильтрацию входящих сообщений только на основе данных, содержащихся в «белом» и «черном» списке. Получение сообщений с номеров, не включенных ни в один из списков, разрешается без запроса пользователя.
- **Выключен.** В данном режиме Анти-Спам отключен. Фильтрация входящих сообщений не выполняется.

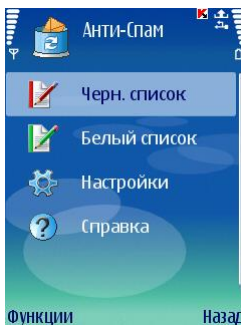
2.2.7.2. Редактирование «черного» и «белого» списка

«Черный» и «белый» списки содержат записи, определяющие телефонные номера, SMS- и/или MMS-сообщения с которых блокируются или пропускаются Анти-Спамом. Информация о заблокированных и удаленных сообщениях фиксируется в разделе **Журнал**.

Примечание

Получение сообщений, не внесенных ни в один из списков, не блокируется!

Для того чтобы отредактировать «черный» или «белый» список перейдите к закладке **Анти-Спам** (см. рис. 15) и выберите соответствующий список.

Рисунок 15. Меню **Анти-Спам**

Для редактирования списка воспользуйтесь меню **Функции**:

- **Добавить запись** – добавить новую запись в список.
- **Ред. запись** – отредактировать текущую запись.
- **Удалить запись** – удалить текущую запись из списка.
- **Удалить все записи** – очистить список, удалив все записи.
- **Справка** – получить справку по работе со списком.

При выборе пункта **Добавить запись** или **Ред. запись** вам будет предложено указать следующие параметры записи:

- **Тип сообщения.** Укажите, получение какого типа входящих сообщений должно быть заблокировано (для «черного» списка) или разрешено (для «белого» списка). Возможные значения: **только SMS, только MMS и Все сообщения.**
- **Тел. номер.** Укажите телефонный номер, для которого блокируется или разрешается получение сообщений. Номер может начинаться с цифры или со знака «+» и должен содержать только цифры. Также, при задании номера, возможно использование масок «?» и «*».
- В поле **Текст** укажите текст, при обнаружении которого приложением в полученном сообщении, будут выполняться следующие действия:
 - сообщение, в котором найден текст, заданный для «белого» списка, будет пропущено;
 - сообщение, в котором найден текст, заданный для «черного» списка, будет заблокировано.

Анализ сообщения производится в следующей последовательности:

- проверка номера на принадлежность «черному» списку;
- проверка номера на принадлежность «белому» списку;
- проверка текста сообщения на соответствие тому, что занесено в «черный» список;
- проверка текста сообщения на соответствие тому, что было занесено в «белый» список.

Если сообщение совпадает с каким-либо из этих правил, то дальнейшая проверка не производится и сообщение либо пропускается, либо блокируется, в зависимости от принадлежности к «черному» или «белому» списку.

Задав значения указанных параметров, нажмите на кнопку **Назад**, для того чтобы сохранить запись и перейти к окну просмотра списка (см. рис. 16).

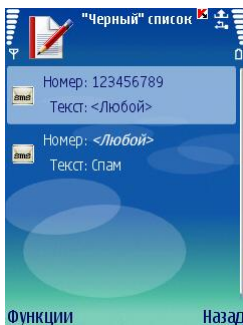


Рисунок 16. «Черный» список

2.2.7.3. Настройки Анти-Спама

Для настройки параметров работы Анти-Спама перейдите к закладке **Анти-Спам** и выберите пункт **Настройки** (см. рис. 17).

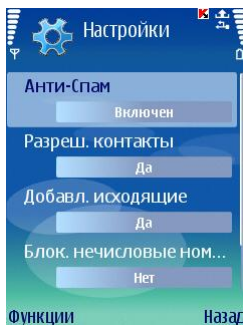


Рисунок 17. Настройки Анти-Спама

В меню **Настройки** доступны для редактирования следующие параметры Анти-Спама:

- **Разреш. контакты.** Если параметру присвоено значение **Да**, то Анти-Спам не будет блокировать получение сообщений с телефонных номеров, содержащихся в вашей телефонной книге. Если данная опция отключена (значение **Нет**), то в процессе фильтрации Анти-Спам будет руководствоваться наличием телефонного номера в «белом» или «черном» списке.
- **Добавл. исходящие.** Если параметру присвоено значение **Да**, то все телефонные номера, на которые вы отправляете SMS- или MMS-сообщения будут автоматически заноситься в «белый» список. Для отключения данной опции выберите **Нет**.
- **Блок. нечисловые номера.** Если параметру присвоено значение **Нет**, то Анти-Спам не будет блокировать все входящие сообщения с нечисловых номеров. Для включения данной опции выберите **Да**.
- **Различать типы.** Если параметру присвоено значение **Нет**, то для новых записей, создаваемых Анти-Спамом в «белом» или «черном» списке, в качестве типа сообщения будет использоваться значение **Все сообщения** (подробнее о параметрах записей в списках см. п. 2.2.7.2 на стр. 20), иначе записи будут создаваться для определенных типов сообщений (SMS или MMS).

Примечание

Данный параметр влияет только на записи, создаваемые Анти-Спамом в одной из следующих ситуаций:

- занесение исходящих номеров в «белый» список (включен параметр **Добавл. исходящие**);
- занесение в один из списков новых телефонных номеров, с которых поступило сообщение (см. п. 2.2.7.4 на стр. 24).

Для редактирования значения параметров воспользуйтесь джойстиком смартфона или выберите пункт **Изменить** в меню **Функции**.

2.2.7.4. Действия над сообщениями

При получении SMS- или MMS-сообщения с телефонного номера, который не содержится ни в «черном», ни в «белом» списке, оно перехватывается Анти-Спамом и на экран смартфона выводится предупреждение (см. рис. 18).

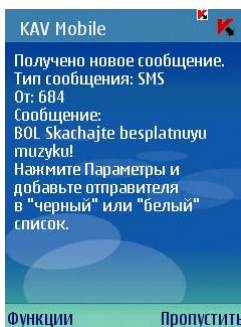


Рисунок 18. Предупреждение Анти-Спама

Используя меню **Функции**, вы можете выбрать одно из следующих действий над сообщением:

- **В «белый» список** – разрешить получение сообщения и добавить телефонный номер отправителя в «белый» список.
- **В «черный» список** – заблокировать получение сообщения и добавить телефонный номер отправителя в «черный» список.
- **Пропустить** – разрешить получение сообщения. Телефонный номер отправителя при этом не заносится ни в один из списков.

Если в настройках Анти-Спама для параметра **Различать типы** задано **Нет**, то при выборе действия **В «белый» список** или **В «черный» список** в соответствующем списке будет создана запись для всех типов сообщений (**Тип сообщения – Все сообщения**), иначе тип будет определяться типом полученного сообщения (подробнее о параметрах записей в списках см. п. 2.2.7.2 на стр. 20).

Информация о заблокированных сообщениях заносится в журнал приложения. Для просмотра отчета необходимо выбрать пункт **Журнал** на закладке **Прочее**.

2.2.7.5. Модуль Anti-Theft

Модуль предназначен для защиты данных, хранящихся на мобильном устройстве от несанкционированного доступа к ним, в случае кражи устройства или его потери.

При первоначальном доступе к настройкам модуля следует задать секретный код. С его помощью в дальнейшем можно будет получать доступ к настройкам модуля с целью их изменения. Секретный код необходим для того, чтобы отсечь несанкционированный доступ к настройкам, а также для того, чтобы пользователь мог блокировать и удалять информацию, сохраненную на смартфоне при его краже или потере.

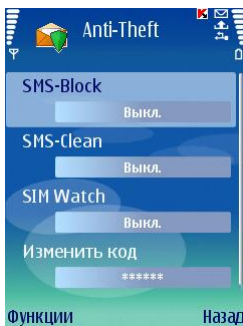
SMS-Block позволяет заблокировать устройство по желанию пользователя. Разблокировать его можно только после ввода секретного кода, используемого для обращения к модулю Anti-Theft. Настройка срабатывает после того, как пользователь, у которого украли устройство, посылает на свой украденный смартфон SMS: «*block:код*». Для того чтобы воспользоваться данной возможностью, выберите **вкл**.

SMS-Clean позволяет удалить персональные данные пользователя (контакты, входящие, персональные файлы). Настройка срабатывает после того, как пользователь, у которого украли устройство, посылает на украденное устройство SMS: «*clean:код*». Для того чтобы воспользоваться **SMS-Clean** выберите **вкл**.

SIM Watch позволяет в случае смены SIM-карты на украденном смартфоне, выслать на указанные номера новый номер телефона, а также заблокировать устройство. Для того чтобы воспользоваться данной возможностью, выберите **вкл**.

Если необходимо изменить секретный код для работы с модулем Anti-Theft, выберите пункт **Изменить код**. Введите новый код и его подтверждение и нажмите на кнопку **ОК**.

Каждый раз при доступе к настройкам модуля Anti-Theft (см. рис. 19) необходимо вводить заданный секретный код.

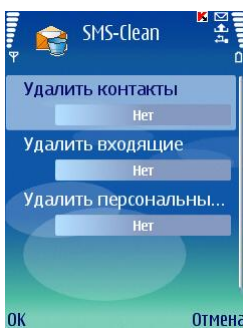
Рисунок 19. Закладка **Anti-Theft**

Информация о работе модуля заносится в журнал приложения. Для просмотра отчета необходимо выбрать пункт **Журнал** на закладке **Прочее**.

2.2.7.6. Настройки SMS-Clean

Для настройки параметров **SMS-Clean** перейдите к закладке **Прочее** и выберите пункт **Anti-Theft**. Введите секретный код (см. п. 2.2.7.5 на стр. 25) и в открывшемся окне выберите пункт **SMS-Clean**.

Раздел **SMS-Clean** содержит список данных, которые можно указать для удаления в том случае, если смартфон будет украден или утерян (см. рис. 20).

Рисунок 20. Закладка **SMS-Clean**

Если вы хотите, чтобы при утере мобильного устройства или его краже, была возможность удалить телефонную книгу, выберите пункт **Удалить контакты** и установите значение **Да**.

Для удаления почты, SMS- или MMS-сообщений (папки Inbox и Mailbox) выберите пункт **Удалить входящие** и установите значение **Да**.

Пункт **Удалить персональные файлы** отвечает за удаление персональных данных (данные из папки !:\Data\). По умолчанию удаление персональных файлов не предусмотрено. Если вы хотите, чтобы в случае кражи или потери смартфона персональные данные могли быть удалены, выберите этот пункт и установите значение **Да**.

Нажмите на кнопку **ОК**, чтобы зафиксировать внесенные изменения.

2.2.7.7. Настройки SIM Watch

Для настройки параметров SIM Watch перейдите к закладке Прочее и выберите пункт Anti-Theft. Введите секретный код (см. п. 2.2.7.5 на стр. 25) и в открывшемся окне выберите пункт **SIM Watch**.

Раздел **SIM Watch** предназначен для контроля смены SIM-карты на устройстве (см. рис. 21).

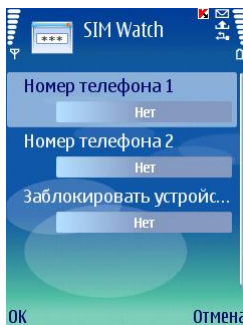


Рисунок 21. Закладка **SIM Watch**

В полях **Номер телефона 1** и **Номер телефона 2** введите те телефонные номера, на которые вы бы хотели получить новый номер телефона, в случае смены SIM-карты в вашем смартфоне. Номера могут начинаться с цифры или со знака «+» и должны содержать только цифры.

Дополнительно вы можете настроить блокировку смартфона при смене SIM-карты. Для этого выберите пункт **Заблокировать устройство** и установите значение **Да**. Разблокировать устройство можно путем ввода секретного кода, назначенного для доступа к модулю Anti-Theft. По умолчанию блокирование устройства не предусмотрено.

Нажмите на кнопку **ОК**, чтобы зафиксировать внесенные изменения.

2.2.8. Обновление баз приложения

Поиск вредоносных программ выполняется на основании записей баз приложения, содержащих описание всех известных на настоящий момент вредоносных программ. Крайне важно поддерживать базы в актуальном состоянии.

Обновить базы можно вручную или по расписанию. Обновление выполняется через интернет с серверов «Лаборатории Касперского».

Вы можете включить автоматическую антивирусную проверку смартфона после каждого обновления баз Kaspersky Mobile Security. Для этого на закладке **Обновление** перейдите к пункту **Настройки** и установите значение **Вкл.** для пункта **Провер. после обн.**

Значение параметра **Карантин после обн.** определяет, производится или нет проверка объектов на карантине после каждого обновления баз приложения. По умолчанию проверка выполняется. Чтобы отказаться от проверки, выберите **Выкл.**

Если вы не хотите выбирать точку доступа в интернет каждый раз при обновлении, выберите для параметра **Выбор тчк. доступа** значение **Нет**, при этом приложение запомнит последнюю точку доступа, через которую было проведено успешное обновление, и при последующих обновлениях будет использовать ее для сетевого соединения. Также можно настроить новую точку доступа.

Если возникла необходимость изменить активную точку доступа, используйте параметр **Точка доступа**. Затем выберите нужное значение параметра в списке. По умолчанию точкой доступа является дефолтная точка устройства.

Значение параметра **Сервер обновлений** определяет источник обновления баз приложения: серверы обновлений «Лаборатории Касперского» (значение **По умолчанию**) или сервер, указанный пользователем (значение **Задать**). При выборе значения **Задать**, введите в открывшемся окне URL обновлений. При необходимости можно указать альтернативный сервер обновлений.

Подробную информацию об используемых базах можно посмотреть в пункте **Инф. о базах**, расположенном на закладке **Информация**.

Информация об обновлении баз заносится в журнал. Для того чтобы просмотреть журнал, выберите пункт **Журнал** на закладке **Обновление**.

2.2.8.1. Настройка обновления

Чтобы настроить обновление баз приложения, выполните следующие действия:

1. Запустите Kaspersky Mobile Security (см. п. 2.2.2 на стр. 9).
2. На закладке **Обновление** перейдите к пункту **Настройки** (см. рис. 22).

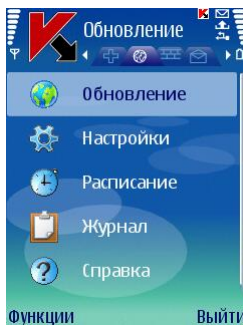


Рисунок 22. Закладка **Обновление**

3. Включите / выключите запрос точки доступа (параметр **Выбор тчк. доступа**).

Примечание

Настройка точки доступа производится по параметрам, предоставляемым сотовым оператором.

Если вы выберете **Нет**, то соединение будет происходить через точку доступа, использованную при последнем обновлении.

При включенном запросе будет предложено выбрать точку доступа из списка доступных (см. рис. 23).

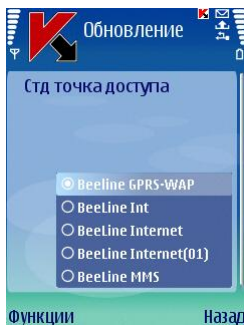


Рисунок 23. Выбор точки доступа

4. Введите адрес сервера обновлений (если это необходимо). Для этого выберите пункт **Сервер обновлений** и выберите значение **Задать**. В открывшемся окне введите URL обновлений (см. рис. 24).

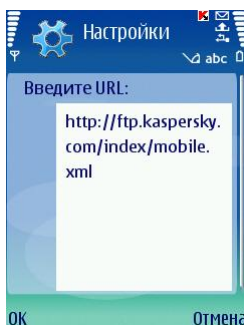


Рисунок 24. Адрес сервера обновлений

По умолчанию обновления производятся с сервера «Лаборатории Касперского»: <http://ftp.kaspersky.com/index/mobile.xml>.

Внимание!

Независимо от того, было ли раньше открыто соединение, оно будет закрыто после завершения обновления.

2.2.8.2. Обновление вручную

Для того чтобы запустить обновление баз вручную,

1. Запустите Kaspersky Mobile Security (см. п. 2.2.2 на стр. 9).

2. На закладке **Обновление** выберите пункт **Обновление** (см. рис. 22).

2.2.8.3. Обновление по расписанию

Для того чтобы настроить обновление баз по расписанию,

1. Запустите Kaspersky Mobile Security (см. п. 2.2.2 на стр. 9).
2. На закладке **Обновление** выберите пункт **Расписание** и настройте параметры **Автообновления**:
 - **Выкл.** – не производить обновление по расписанию.
 - **Ежедневно** – производить обновление каждый день. Укажите время обновления в соответствующем поле.
 - **Еженедельно** – производить обновление раз в неделю. Укажите день обновления и время обновления в соответствующих полях.

2.2.9. Использование модуля Firewall

Firewall предназначен для контроля сетевой активности и защиты смартфона на сетевом уровне (см. рис. 25).

Вы можете выбрать уровень защиты (параметр **Firewall**) для того, чтобы задать степень контроля входящего и исходящего трафика, из предложенных вариантов:

- **Блокировать все** – запрещена вся сетевая активность.
- **Средний** – блокированы все входящие подключения, исходящий трафик может осуществляться только обычными приложениями.
- **Низкий** – блокированы только входящие подключения.
- **Отключен** – сетевая активность разрешена.

С помощью параметра **Уведомление** вы можете настроить получение уведомлений пользователем в случае, если действия, им выполняемые, не соответствуют установленному уровню защиты. Чтобы отключить получение уведомлений, выберите **выкл.**

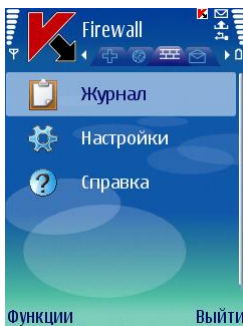


Рисунок 25. Закладка **Firewall**

Информация о работе модуля Firewall заносится в журнал приложения. Для просмотра отчета необходимо выбрать пункт **Журнал** на закладке **Firewall**.

2.2.10. Получение отчета о работе приложения

На закладке **Информация** вы можете просмотреть хронологический журнал событий в работе Kaspersky Mobile Security. Для этого перейдите к закладке и выберите пункт **Журнал** (см. рис. 26).

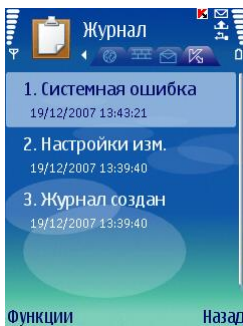


Рисунок 26. Отчет о работе приложения

2.3. Удаление приложения

Для удаления Kaspersky Mobile Security со смартфона выполните следующие действия:

1. Завершите работу Kaspersky Mobile Security. Для этого:
 - Нажмите и удерживайте кнопку **Меню**.
 - В списке запущенных приложений выберите **KMS7.0** и нажмите на кнопку **Функции**.
 - Выберите пункт меню **Выход** (см. рис. 27).

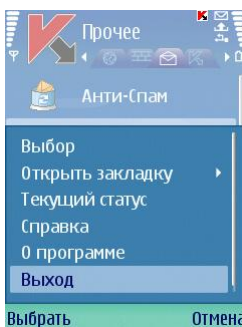


Рисунок 27. Завершение работы с приложением

2. Удалите Kaspersky Mobile Security:
 - Нажмите на кнопку **Меню** и выберите пункт меню **Диспетчер приложений** (см. рис. 28).

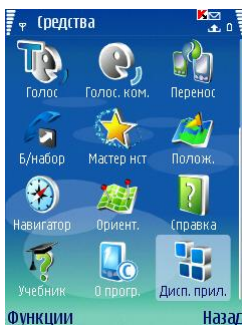


Рисунок 28. Запуск **Диспетчер приложений**

- В списке приложений выберите **KMS7.0** и нажмите на кнопку **Функции** (см. рис. 29).

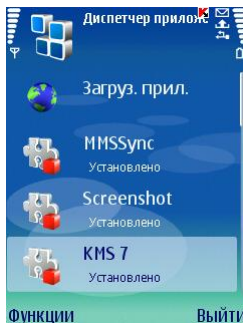


Рисунок 29. Выбор приложения

- Выберите пункт меню **Удалить** (см. рис. 30).

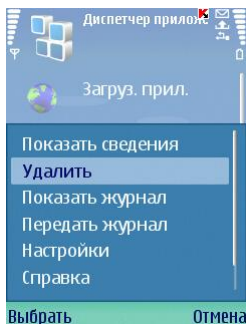


Рисунок 30. Удаление приложения

- В запросе о подтверждении удаления приложения нажмите на кнопку **Да**.

ГЛАВА 3. KASPERSKY MOBILE SECURITY ДЛЯ MICROSOFT WINDOWS MOBILE

Эта глава содержит описание работы с Kaspersky Mobile Security для мобильных устройств, работающих под управлением одной из следующих операционных систем:

- Microsoft Windows Mobile 5.0.
- Microsoft Windows Mobile 6.0.

Продукт работает только на тех смартфонах и коммуникаторах, которые поддерживают прием и передачу SMS-сообщений.

3.1. Установка Kaspersky Mobile Security

Для того чтобы установить Kaspersky Mobile Security, выполните следующие действия:

1. Скопируйте сав-архив с дистрибутивом приложения на мобильное устройство.
2. Запустите установку (откройте сав-архив дистрибутива на мобильном устройстве). Установка будет произведена в основную память мобильного устройства.
3. Прочтите текст лицензионного соглашения. Если вы согласны с условиями соглашения, нажмите **ОК**. Для отказа от установки нажмите **Отмена** (см. рис. 31).



Рисунок 31. Лицензионное соглашение

3.2. Начало работы

В этом разделе содержатся сведения о том, как активировать приложение, после его установки на мобильное устройство и как запустить приложение. Также представлена информация об общих принципах организации графического интерфейса.

3.2.1. Активация приложения

При первом запуске приложения на экране мобильного устройства отображается окно активации Kaspersky Mobile Security (см. рис. 32).

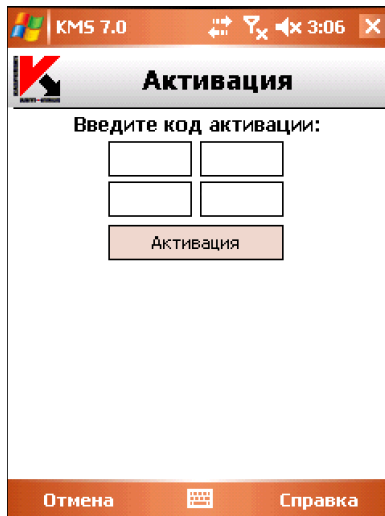


Рисунок 32. Окно активации приложения

Активация приложения необходима, без нее все функции Kaspersky Mobile Security недоступны. Код активации вы можете получить на сайте «Лаборатории Касперского».

Внимание!

Для активации Kaspersky Mobile Security на мобильном устройстве необходимо иметь GPRS-подключение.

Код активации состоит из букв латинского алфавита и цифр, регистр не имеет значения. Введите код последовательно в 4 поля.

После ввода кода активации нажмите **Активация**. Приложение осуществит http-запрос на сервер активации «Лаборатории Касперского», скачает и установит лицензионный ключ.

В случае если введенный вами код активации по каким-либо причинам окажется недействительным, на экране смартфона будет показано соответствующее сообщение.

3.2.2. Запуск приложения


Чтобы запустить Kaspersky Mobile Security, выполните следующие действия:

1. Откройте на мобильном устройстве меню **Программы**.
2. Выберите **KMS 7.0** для того, чтобы запустить приложение.

После запуска приложения на дисплее мобильного устройства отображается окно статуса основных компонентов Kaspersky Mobile Security (см. рис. 33):

- **Постоянная защита** – использование режима постоянной защиты.
- **Последняя проверка** – дата выполнения последней антивирусной проверки мобильного устройства.
- **Дата выпуска баз** – дата выпуска баз Kaspersky Mobile Security, используемых приложением.

Внимание!

Если антивирусная проверка мобильного устройства не проводилась и / или с момента последнего обновления баз антивируса прошло две недели, значок рядом с соответствующим пунктом принимает следующий вид . Также такой значок появляется, если отключен режим постоянной защиты и / или модуль Анти-Спама.

- **Сетевой экран** – уровень защиты смартфона.

Анти-Спам – статус модуля Анти-Спам, используемого для фильтрации SMS-сообщений.

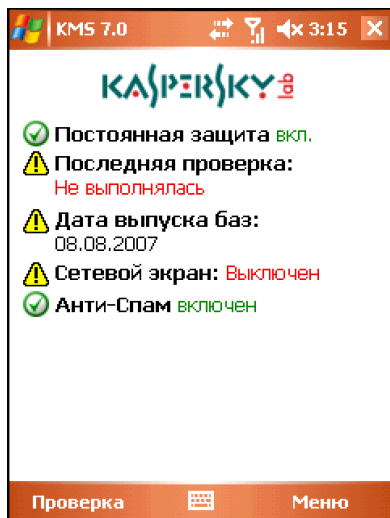


Рисунок 33. Окно статуса компонентов приложения

3.2.3. Графический интерфейс

Графический интерфейс приложения состоит из шести закладок, доступ к которым осуществляется при помощи **Меню** (см. рис. 34):

- Закладка **Проверка** позволяет выполнять антивирусную проверку мобильного устройства, редактировать параметры антивирусной проверки и режима постоянной защиты, настраивать расписание запуска автоматической проверки (см. п. 3.3 на стр. 40).
- Закладка **Сетевой экран** позволяет контролировать сетевую активность и защищать смартфон на сетевом уровне (см. п. 2.2.9 на стр. 31).
- Закладка **Обновление** позволяет выполнять обновление баз антивируса, редактировать параметры обновления, настраивать расписание обновления (см. п. 3.6 на стр. 54).
- Закладка **Карантин** позволяет управлять карантином – специальным хранилищем зараженных и подозрительных объектов (см. п. 3.4 на стр. 46).

- Закладка **Прочее** позволяет настраивать фильтрацию входящих SMS- и MMS-сообщений (модуль Анти-Спам), а также блокировать смартфон и удалять информацию, сохраненную на нем, в случае кражи или потери устройства (модуль Anti-Theft) (см. п. 2.2.7.5 на стр. 25).
- Закладка **Информация** позволяет просматривать журналы работы компонентов приложения, общую информацию о приложении и используемых базах, а также редактировать общие параметры работы приложения (см. п. 3.8 на стр. 57).

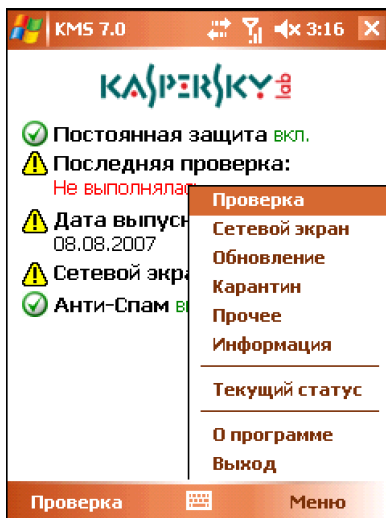


Рисунок 34. Меню приложения

Для того чтобы вернуться к окну статуса компонентов приложения выберите пункт **Текущий статус**.

Для того чтобы завершить работу приложения выберите **Выход**.

3.3. Антивирусная проверка и защита

Используя закладку **Проверка**, вы можете выполнить антивирусную проверку как всей файловой системы и памяти мобильного устройства, так и отдельного каталога или файла. Также вы можете изменить параметры антивирусной проверки и режима постоянной антивирусной защиты, про-

смотреть отчет о результатах проверки и настроить расписание автоматического запуска проверки.

3.3.1. Постоянная защита и проверка по требованию

Постоянная защита – режим работы, при котором резидентная часть Kaspersky Mobile Security постоянно находится в оперативной памяти мобильного устройства и контролирует все данные устройства.

Постоянная защита запускается с момента включения устройства и работает до его выключения (если использование режима не отключено в настройках).

Также Kaspersky Mobile Security позволяет выполнять полную проверку файловой системы мобильного устройства.

Информация о результатах работы постоянной защиты и проверки по требованию заносится в отчет. Для просмотра отчета необходимо выбрать пункт **Отчет проверки**. Также отчет доступен на закладке **Информация** (см. п. 3.8 на стр. 57).

Для того чтобы запустить режим использования постоянной защиты, выполните следующее:

1. На закладке **Проверка** выберите пункт **Настройки проверки**.
2. Включите / выключите режим использования постоянной защиты, установив / сняв флажок **Постоянная защита**.

Для того чтобы изменить параметры проверки по требованию, выполните следующее:

1. На закладке **Проверка** выберите пункт **Настройки проверки**.
2. Задайте область проверки в блоке **Параметры** путем выбора типов файлов, которые необходимо проверять:
 - **Проверять архивы** – проверять файлы, упакованные в архив.
 - **Только исполняемые** – проверять только исполняемые файлы программ.
3. Определите действие, которое будет выполняться приложением при обнаружении зараженного объекта в блоке **При обнаружении вируса**. Чтобы Kaspersky Mobile Security попытался вылечить обнаруженный зараженный объект, установите флажок **Пытаться вылечить**. Если лечение объекта не требуется, выберите возможное

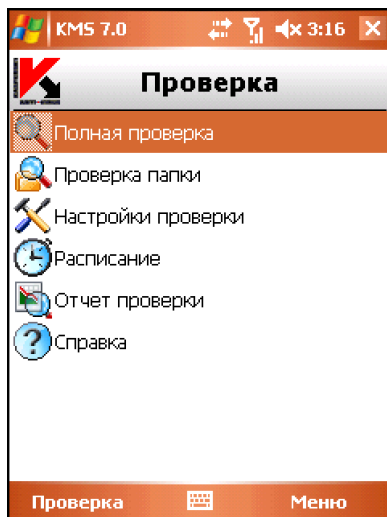
действие антивируса, установив для параметра **Основное действие** одно из следующих значений:

- **В карантин** – перемещать обнаруженные зараженные объекты на карантин.
- **Запрашивать действие** – отображать сообщение об обнаружении вируса на экране с предложением удалить зараженный объект, поместить его на карантин или пропустить.
- **Удалять** – удалять обнаруженные зараженные объекты.
- **Пропускать** – не выполнять никаких действий над зараженными объектами.

Также одно из этих действий вы можете задать для случая, когда попытка лечения зараженного объекта может закончиться неудачей. Для этого установите флажок **Пытаться вылечить** и выберите необходимое действие в списке **Если нельзя вылечить**.

Для того чтобы запустить антивирусную проверку, выполните следующие действия:

1. Запустите Kaspersky Mobile Security (см. п. 3.2.1 на стр. 36).
2. Перейдите на закладку **Настройка проверки**.
 - Задайте область проверки в блоке **Параметры** путем выбора типов файлов, которые необходимо проверять (см. выше).
 - Определите действие, которое будет выполняться приложением при обнаружении зараженного объекта (см. выше).
3. На закладке **Проверка** (см. рис. 35) выберите пункт **Полная проверка**, если вы хотите проверить всю файловую систему мобильного устройства, или **Проверка папки**, если вы хотите выполнить проверку отдельной папки.

Рисунок 35. Закладка **Проверка**

При выборе пункта **Проверка папки** выполняется переход к окну, представляющему файловую систему мобильного устройства. Для того чтобы запустить проверку папки, переместите курсор на папку и нажмите на кнопку **Проверка**.

После запуска проверки откроется окно процесса проверки, где будет указано текущее состояние: количество проверенных объектов и путь к объекту, который проверяется в данный момент (см. рис. 36).

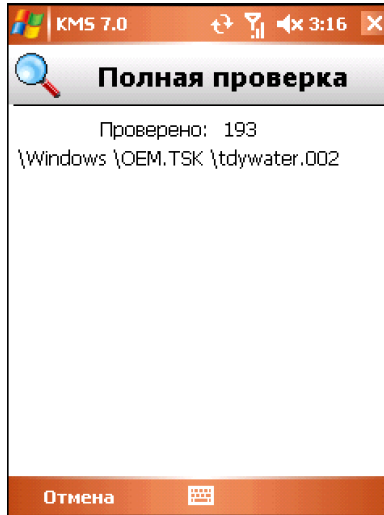


Рисунок 36. Окно процесса проверки

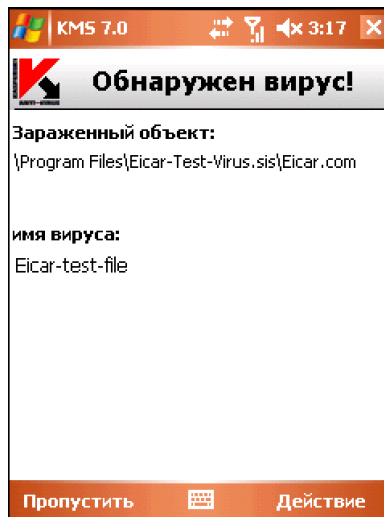


Рисунок 37. Сообщение об обнаружении вируса

По окончании проверки будет выведена общая статистика о найденных и удаленных вредоносных объектах.

3.3.2. Проверка по расписанию

Kaspersky Mobile Security позволяет пользователю формировать расписание автоматической антивирусной проверки мобильного устройства. Проверка происходит в фоновом режиме. При обнаружении зараженного объекта над ним выполняется действие, заданное в настройках проверки (пункт **Настройки проверки**).

По умолчанию проверка по расписанию выключена.

Для того чтобы настроить проверку по расписанию,

на закладке **Проверка** выберите пункт **Расписание** и настройте параметры проверки (см. рис. 38):

- **Ежедневно** – проверка производится каждый день. Время проверки определяется параметром **Время**.
- **Еженедельно** – проверка производится раз в неделю. День и время проверки определяются параметрами **День недели** и **Время**.
- **Отключить** – проверка будет запускаться пользователем самостоятельно.

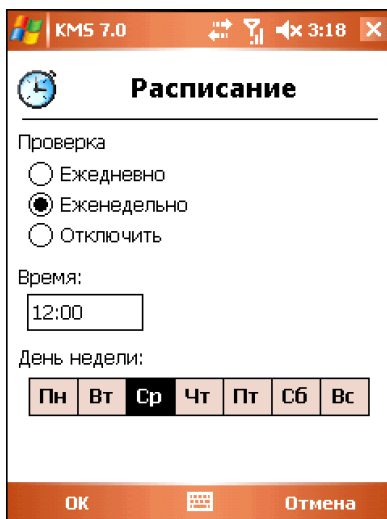


Рисунок 38. Меню **Расписание**

3.4. Использование карантина

Зараженные объекты, помещенные на карантин, не представляют угрозы для вашего мобильного устройства и могут быть впоследствии удалены либо восстановлены.

Обнаруженные зараженные объекты могут перемещаться приложением на карантин автоматически, либо после вашего подтверждения.

Для того чтобы настроить приложение на автоматическое перемещение зараженных объектов при выполнении антивирусной проверки, перейдите на закладку **Проверка**, выберите пункт **Настройки проверки** и в блоке **При обнаружении вируса** в качестве значения параметра **Основное действие** выберите **В карантин**. Для случая когда лечение зараженного объекта может закончиться неудачей, установите флажок **Пытаться вылечить** и выберите **В карантин** в списке **Если нельзя вылечить**.

Если в качестве действия вы выбрали **Запрашивать действие**, то при обнаружении зараженного объекта Kaspersky Mobile Security предложит вам либо удалить объект, либо поместить его на карантин.

Для того чтобы просмотреть содержимое карантина, перейдите к закладке **Карантин** (см. рис. 39).

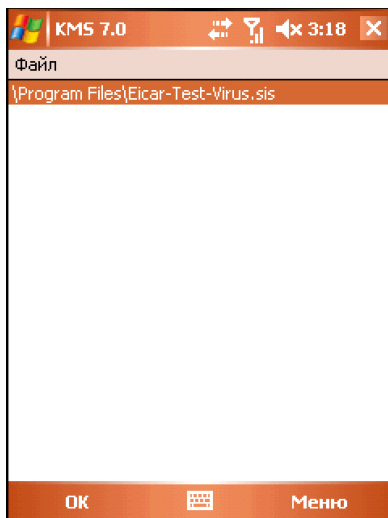


Рисунок 39. Карантин

Меню, доступное в окне просмотра карантина, позволяет вам:

- Просмотреть детальную информацию о выбранном объекте, хранящемся на карантине (пункт **Сведения**).
- Удалить текущий объект (пункт **Удалить**).
- Восстановить текущий объект из карантина в исходный каталог (пункт **Восстановить**).
- Очистить карантин, удалив все содержащиеся в нем объекты (пункт **Удалить все**).

3.5. Использование Анти-Спама и модуля Anti-Theft

Модуль Анти-Спам предназначен для защиты смартфона от нежелательных SMS- и MMS-сообщений.

Принцип фильтрации сообщений основан на использовании «черного» и «белого» списков. Входящие сообщения, поступившие с телефонных номеров, занесенных в «черный» список, блокируются Анти-Спамом. Получение сообщений, с номеров, занесенных в «белый» список, не блокируется.

Модуль Anti-Theft предназначен для блокирования смартфона и удаления информации, хранящейся в его памяти, в случае кражи или потери устройства.

3.5.1. Модуль Анти-Спам

Модуль Анти-Спама предназначен для защиты мобильного устройства от нежелательных SMS-сообщений.

Внимание!

На КПК модуль Анти-Спама отсутствует!

Принцип фильтрации сообщений основан на использовании так называемых «черного» и «белого» списков. Входящие сообщения, поступившие с телефонных номеров, занесенных в «черный» список, блокируются Анти-Спамом. Получение сообщений, с номеров, занесенных в «белый список», не блокируется.

Для того чтобы изменить параметры работы Анти-Спама, выполните следующее:

1. На закладке **Анти-Спам** выберите **Настройки**.
2. Включите / выключите использование Анти-Спама, установив или сняв флажок **Включить Анти-Спам**.
3. Укажите, разрешено ли получение SMS-сообщений с телефонных номеров, не включенных ни в один из списков, сняв или установив флажок **Получать SMS от: неизвестных номеров**.
4. Укажите, разрешено ли получение SMS-сообщений с телефонных номеров из контакт-листа, сняв или установив флажок **Получать SMS от: номеров из контакт-листа**.

3.5.2. Редактирование «черного» и «белого» списков

«Черный» список содержит номера телефонов, прием сообщений с которых блокируется Анти-Спамом.

«Белый» список содержит номера телефонов, прием сообщений с которых разрешен.

Для того чтобы отредактировать «черный» или «белый» список перейдите к закладке **Анти-Спам** (см. рис. 40) и выберите соответствующий список.

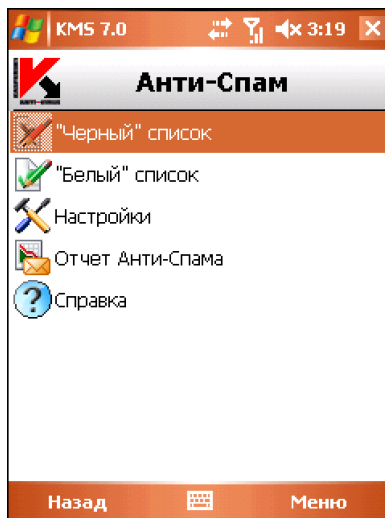
Для редактирования списка воспользуйтесь **Меню**:

- **Добавить запись** – добавить новую запись в список.
- **Удалить запись** – удалить текущую запись из списка.
- **Редакт. запись** – редактировать текущую запись в списке.

Выбрав пункт **Добавить запись**, укажите телефонный номер (поле **Введите номер**), который вы хотите включить в список. Номер может начинаться с цифры или со знака «+». Также, при задании номера, возможно использование масок «?» и «*».

Дополнительно вы можете задать текст (поле **Введите текст**), при обнаружении которого в полученном сообщении будут выполнены следующие действия:

- сообщение, в котором найден текст, заданный для «белого» списка, будет пропущено;
- сообщение, в котором найден текст, заданный для «черного» списка, будет заблокировано.

Рисунок 40. Меню **Анти-Спам**

Анализ сообщения производится в следующей последовательности:

- проверка номера на принадлежность «черному» списку;
- проверка номера на принадлежность «белому» списку;
- проверка текста сообщения на соответствие тому, что занесено в «черный» список;
- проверка текста сообщения на соответствие тому, что было занесено в «белый» список.

Если сообщение совпадает с каким-либо из этих правил, то дальнейшая проверка не производится и сообщение либо пропускается, либо блокируется, в зависимости от принадлежности к «черному» или «белому» списку.

Отредактировать список нажмите **ОК**, для того чтобы вернуться к закладке **Анти-Спам**.

3.5.3. Действия над сообщениями

При получении сообщений с телефонного номера, который не содержится ни в «черном», ни в «белом» списке, при условии, что в настройках Анти-Спама разрешено получение сообщений с неизвестных номеров (см. п. 3.5.1 на стр. 47), на экран мобильного устройства выводится предупреждение (см. рис. 41).

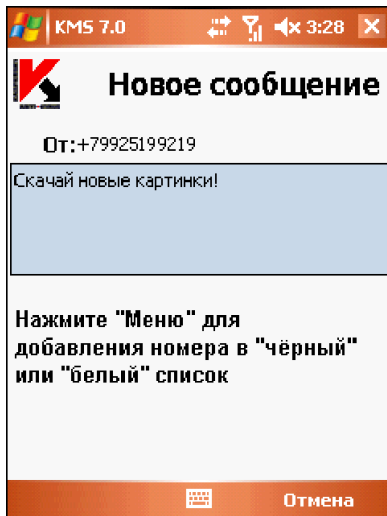


Рисунок 41. Предупреждение Анти-Спама

Используя **Меню**, вы можете выбрать одно из следующих действий над сообщением:

- **В «белый» список** – разрешить получение сообщения и добавить телефонный номер отправителя в «белый» список.
- **В «черный» список** – заблокировать получение сообщения и добавить телефонный номер отправителя в «черный» список.

Нажмите на кнопку **Пропустить**, для того чтобы разрешить получение сообщения. Телефонный номер отправителя при этом не заносится ни в один из списков.

Информация о заблокированных сообщениях заносится в журнал приложения. Для того чтобы просмотреть журнал, нажмите на кнопку **Отчет** на закладке **Анти-Спам** или на этой же закладке выберите пункт **Отчет Анти-Спама**. Также отчет доступен на закладке **Информация** (см. п. 3.8 на стр. 57).

3.5.4. Модуль Anti-Theft

Модуль Anti-Theft (закладка **Прочее** пункт **Anti-Theft** (см. рис. 42)) предназначен для защиты данных, хранящихся на мобильном устройстве от несанкционированного доступа к ним, в случае кражи устройства или его потери.

При первоначальном доступе к настройкам модуля следует задать секретный код. С его помощью в дальнейшем можно будет получать доступ к настройкам модуля с целью их изменения. Секретный код необходим для того, чтобы отсечь несанкционированный доступ к настройкам, а также для того, чтобы пользователь мог блокировать и удалять информацию, сохраненную на смартфоне при его краже или потере.

SMS-Block позволяет заблокировать устройство по желанию пользователя. Разблокировать его можно только после ввода секретного кода, используемого для обращения к модулю Anti-Theft. Настройка срабатывает после того, как пользователь, у которого украли устройство, посылает на свой украденный смартфон SMS: «*block:код*». Функция **SMS-Block** будет активирована при ее выборе: прочтите информационное сообщение и нажмите **OK**, если хотите использовать данную возможность.

SMS-Clean позволяет удалить персональные данные пользователя (контакты, входящие, персональные файлы). Настройка срабатывает после того, как пользователь, у которого украли устройство, посылает на украденное устройство SMS: «*clean:код*». Функция **SMS-Clean** будет активирована при ее выборе: укажите необходимые значения параметров (см. п. 3.5.4.1 на стр. 52), прочтите информационное сообщение и нажмите **OK**, если хотите использовать данную возможность.

SIM Watch позволяет в случае смены SIM-карты на украденном смартфоне, выслать на указанные номера новый номер телефона, а также заблокировать устройство. Разблокировать устройство можно путем ввода секретного кода, назначенного для доступа к модулю Anti-Theft. Функция SIM Watch будет активирована при ее выборе: укажите необходимые значения параметров (см. п. 3.5.4.2 на стр. 53), прочтите информационное сообщение и нажмите **OK**, если хотите использовать данную возможность.

Если необходимо изменить секретный код для работы с модулем Anti-Theft, выберите пункт **Сменить пароль**. Введите новый код и его подтверждение и нажмите на кнопку **OK**.

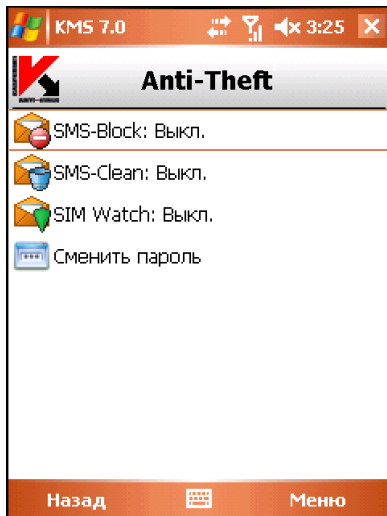


Рисунок 42. Закладка **Anti-Theft**

Информация о работе модуля Anti-Theft заносится в журнал приложения. Для того чтобы просмотреть журнал, выберите пункт **Отчет Anti-Theft** на закладке **Прочее**. Также отчет доступен на закладке **Информация** (см. п. 3.8 на стр. 57).

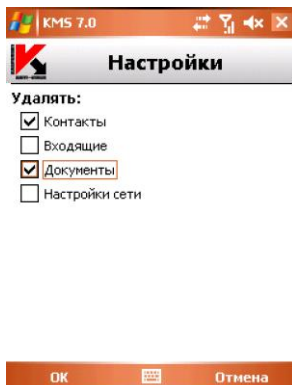
3.5.4.1. Настройки SMS-Clean

Раздел **SMS-Clean** содержит список данных, которые можно указать для удаления в том случае, если смартфон будет украден или утерян (см. рис. 43).

Для того чтобы изменить параметры работы SMS-Clean, выполните следующие действия:

1. На закладке **Прочее** выберите пункт **Anti-Theft**.
2. Введите секретный код, в открывшемся окне выберите пункт **SMS-Clean**.
3. Установите флажок **Контакты**, если вы хотите, чтобы при утере или краже мобильного устройства, телефонная книга была удалена.
4. Установите флажок **Входящие**, если вы хотите, чтобы удалялись почта, SMS- и MMS-сообщения.

5. Установите флажок **Документы**, если необходимо удалять персональные данные пользователя.
6. Установите флажок **Настройки сети**, если необходимо удалять сетевые настройки
7. Нажмите **ОК**, чтобы сохранить введенные данные.

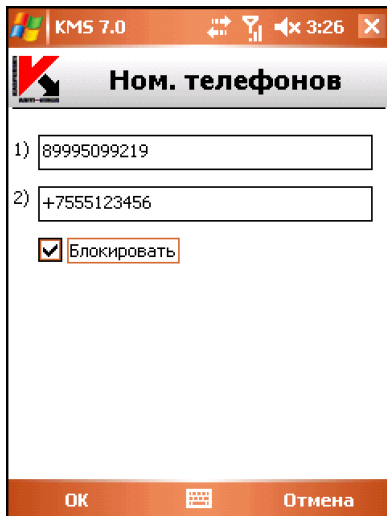
Рисунок 43. Закладка **SMS-Clean**

3.5.4.2. Настройки SIM Watch

Раздел **SIM Watch** предназначен для контроля смены SIM-карты на устройстве (см. рис. 44).

Для того чтобы изменить параметры работы SIM Watch, выполните следующие действия:

1. На закладке **Прочее** выберите пункт **Anti-Theft**.
2. Введите секретный код, в открывшемся окне выберите пункт **SIM Watch**.
3. В поля **1)** и **2)** введите телефонные номера, на которые вы бы хотели получить новый номер телефона, в случае смены SIM-карты в вашем смартфоне. Номера могут начинаться с цифры или со знака «+» и должны содержать только цифры.
4. Настройте блокировку мобильного устройства при смене на нем SIM-карты. Для этого установите флажок **Блокировать**.
5. Нажмите **ОК**, чтобы сохранить введенные данные.

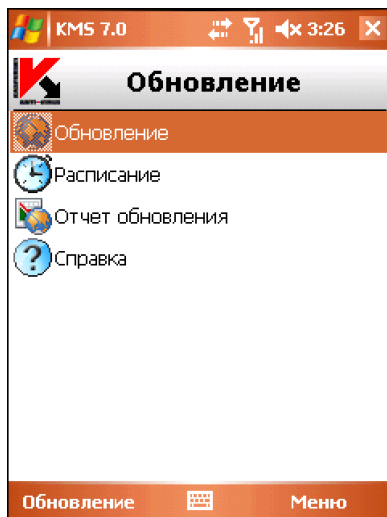
Рисунок 44. Закладка **SIM Watch**

3.6. Обновление баз приложения

Поиск вредоносных программ выполняется на основании записей баз Kaspersky Mobile Security, содержащих описание всех известных на настоящий момент вредоносных программ. Крайне важно поддерживать базы в актуальном состоянии.

Обновить базы можно вручную или по расписанию. Для настройки и запуска обновления служит закладка **Обновление** (см. рис. 45). Обновление выполняется через интернет с серверов «Лаборатории Касперского». В случае возникновения ошибки, убедитесь, что мобильное устройство имеет доступ в интернет.

Информация об обновлении баз заносится в журнал. Для того чтобы просмотреть журнал, на закладке **Обновление** выберите пункт **Отчет обновления**. Также отчет доступен на закладке **Информация** (см. п. 3.8 на стр. 57).

Рисунок 45. Закладка **Обновление**

Для того чтобы вручную запустить обновление баз приложения с серверов обновлений «Лаборатории Касперского», выполните следующие действия:

1. Запустите Kaspersky Mobile Security (см. п. 3.2.1 на стр. 36) и перейдите к закладке **Обновление**.
2. Выберите **Обновление**, для того чтобы запустить загрузку обновлений.

Для того чтобы настроить расписание автоматического обновления баз приложения, выполните следующее:

1. Запустите Kaspersky Mobile Security (см. п. 3.2.1 на стр. 36) и перейдите к закладке **Обновление**.
2. Выберите **Расписание**, для того чтобы перейти к редактированию параметров расписания автоматического обновления.
3. Укажите периодичность обновления в качестве значения параметра обновления:
 - **Ежедневно** – производить обновление каждый день. Дополнительно укажите **Время** обновления.
 - **Еженедельно** – производить обновление раз в неделю. Дополнительно укажите **День недели** и **Время** обновления.

- **Отключить** – проверка будет запускаться пользователем самостоятельно.

На закладке **Информация** вы можете узнать дату выпуска баз антивируса, установленных в настоящее время на мобильном устройстве и количество вирусных сигнатур. Для этого на закладке выберите пункт **Инф. о базах**.

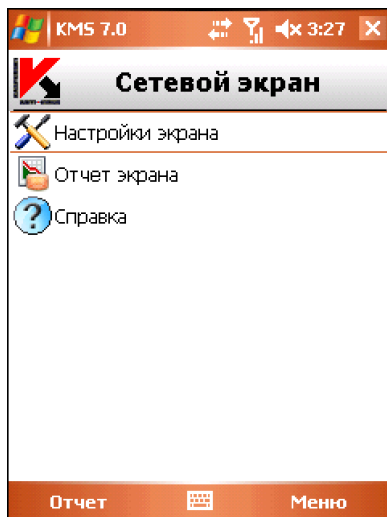
3.7. Сетевой экран

Модуль **Сетевой экран** предназначен для контроля сетевой активности и защиты мобильного устройства на сетевом уровне (см. рис. 46).

Для того чтобы изменить параметры работы сетевого экрана, выполните следующие действия:

1. Запустите Kaspersky Mobile Security (см. п. 3.2.1 на стр. 36) и перейдите к закладке **Сетевой экран**.
2. Выберите пункт **Настройки экрана**. В открывшемся окне установите уровень защиты для того, чтобы задать степень контроля входящего и исходящего трафика. Возможны следующие варианты:
 - **Высокий уровень** – запрещена вся сетевая активность.
 - **Средний уровень** – блокирован весь входящий трафик, исходящий трафик может осуществляться только обычными приложениями.
 - **Низкий уровень** – блокирован только входящий трафик.
 - **Выключен** – сетевая активность разрешена.

Информация о работе сетевого экрана заносится в журнал. Для того чтобы просмотреть журнал, на закладке **Сетевой экран** выберите пункт **Отчет экрана**. Также отчет доступен на закладке **Информация** (см. п. 3.8 на стр. 57).

Рисунок 46. Закладка **Сетевой экран**

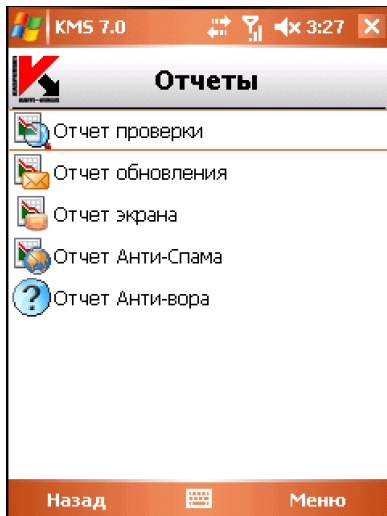
3.8. Получение отчетов о работе приложения

Отчеты о работе приложения собраны на закладке **Информация** в пункте **Отчеты**. Вы можете получить отчет по любой задаче, выполняемой Kaspersky Mobile Security:

- антивирусная проверка;
- обновление баз приложения;
- работа сетевого экрана;
- работа модуля Анти-Спам;
- работа модуля Anti-Theft.

Например, для того чтобы ознакомиться с отчетом об антивирусной проверке, выполните следующие действия:

1. Запустите Kaspersky Mobile Security (см. п. 3.2.1 на стр. 36).
2. На закладке **Информация** выберите пункт **Отчеты** (см. рис. 47).
3. В открывшемся окне выберите отчет о постоянной защите.

Рисунок 47. Закладка **Отчеты**

3.9. Удаление приложения

Для удаления Kaspersky Mobile Security выполните следующие действия:

1. Отключите постоянную защиту (подробнее см. п. 3.3 на стр. 40);

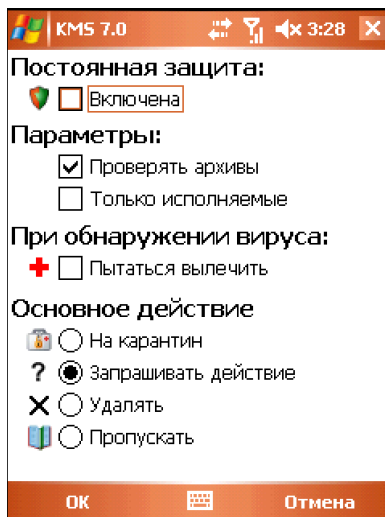


Рисунок 48. Выключение постоянной защиты

2. Завершите работу с Kaspersky Mobile Security. Для этого в меню приложения выберите пункт **Выход** (см. рис. 49).

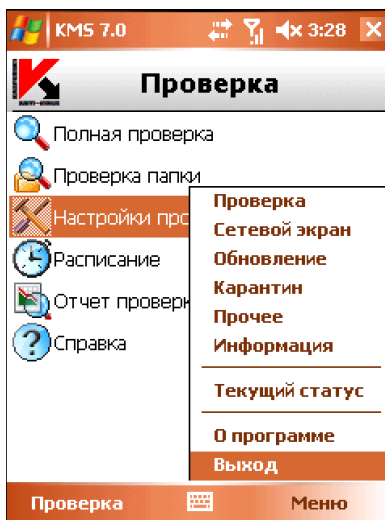


Рисунок 49. Завершение работы с приложением

3. Удалите приложение. Для этого:
- нажмите на кнопку **Пуск**, выберите меню **Настройка**, а затем **Удалить приложения** (см. рис. 50):



Рисунок 50. Запуск удаления приложения

- В списке установленных приложений выберите **KMS 7.0** и нажмите на кнопку **Удалить** (см. рис. 51).

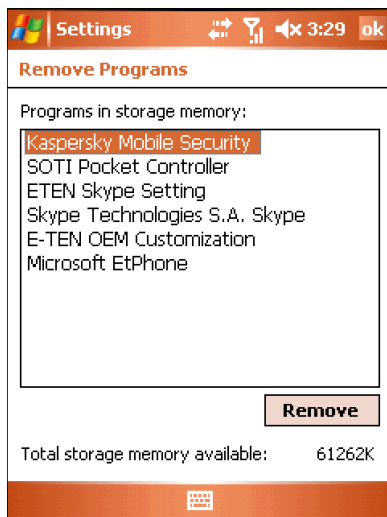


Рисунок 51. Выбор приложения

- В запросе подтверждения удаления приложения нажмите на кнопку **Да** (см. рис. 52).

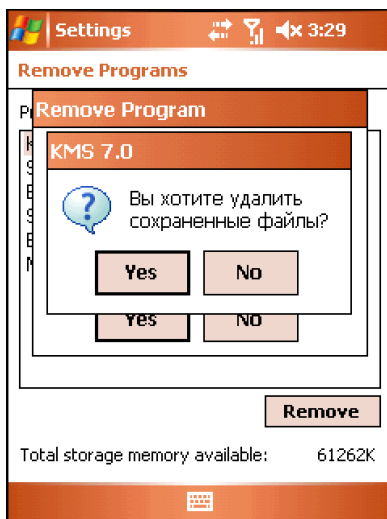


Рисунок 52. Запрос на удаление приложения

ПРИЛОЖЕНИЕ А. ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

ЗАО «Лаборатория Касперского» была основана в 1997 г. Сегодня это самый известный в России разработчик широкого спектра программных продуктов для обеспечения информационной безопасности: систем защиты от вирусов, нежелательной почты (спама) и хакерских атак.

«Лаборатория Касперского» – международная компания. Центральный офис находится в России, открыты локальные офисы в Великобритании, Франции, Германии, Японии, в странах Бенилюкса, Китае, Польше, Румынии и США (Калифорния). Во Франции открыто новое отделение компании – Европейский центр антивирусных исследований. Наша партнерская сеть объединяет более 500 компаний по всему миру.

«Лаборатория Касперского» сегодня – это более четырехсот пятидесяти высококвалифицированных специалистов, десять из которых имеют дипломы MBA, шестнадцать – степени кандидатов наук. Ведущие вирусные аналитики «Лаборатории Касперского» являются членами престижной организации Computer Anti-virus Researcher's Organization (CARO).

Главная ценность компании – уникальные знания и опыт, накопленные ее сотрудниками в течение более чем четырнадцати лет непрерывной борьбы с вирусами. Благодаря постоянному анализу вирусной активности мы умеем предугадывать тенденции развития вредоносных программ и заблаговременно обеспечиваем пользователей надежной защитой от новых видов атак. Это преимущество – основа продуктов и услуг «Лаборатории Касперского». Мы всегда на шаг впереди конкурентов и предоставляем нашим заказчикам наилучшую защиту.

Годы упорной работы позволили компании стать лидером в разработке технологий защиты от вирусов. «Лаборатория Касперского» первой разработала многие современные стандарты антивирусных программ. Основным продуктом компании, Антивирус Касперского[®], обеспечивает надежную защиту всех объектов вирусных атак: рабочих станций, файловых серверов, почтовых систем, сетевых экранов и интернет-шлюзов, карманных компьютеров. Удобные средства управления дают пользователям возможность максимально автоматизировать антивирусную защиту компьютеров и корпоративных сетей. Многие западные разработчики используют в своих продуктах программное ядро Антивируса Касперского[®], например, такие как: Nokia ICG (США), F-Secure (Финляндия), Aladdin (Израиль), Sybari (США), G Data

(Германия), Deerfield (США), Alt-N (США), Microworld (Индия), BorderWare (Канада).

Клиенты «Лаборатории Касперского» обеспечиваются широким спектром дополнительных услуг, гарантирующих бесперебойную работу продуктов и точное соответствие любым специфическим бизнес-требованиям. Мы проектируем, внедряем и сопровождаем корпоративные антивирусные комплексы. Наши базы обновляются каждый час. Мы обеспечиваем наших пользователей круглосуточной технической поддержкой на нескольких языках.

А.1. Другие разработки «Лаборатории Касперского»

Новостной Агент «Лаборатории Касперского»

Программа Новостной Агент предназначена для оперативной доставки новостей «Лаборатории Касперского», оповещения о «вирусной погоде» и появлении свежих новостей. С заданной периодичностью программа считывает с новостного сервера «Лаборатории Касперского» список доступных новостных каналов и содержащуюся в них информацию.

Новостной Агент также позволяет:

- визуализировать в системной панели состояние «вирусной погоды»;
- подписываться и отказываться от подписки на новостные каналы «Лаборатории Касперского»;
- получать с заданной периодичностью новости по каждому подписанному каналу; также осуществляется оповещение о появлении непрочитанных новостей;
- просматривать новости по подписанным каналам;
- просматривать списки каналов и их состояние;
- открывать в браузере страницы с подробным текстом новостей.

Новостной Агент работает под управлением операционной системы Microsoft Windows и может использоваться как отдельная программа, так и входить в состав различных интегрированных решений «Лаборатории Касперского».

Kaspersky® OnLine Scanner

Программа представляет собой бесплатный сервис, доступный посетителям веб-сайта компании, позволяющий произвести эффективную антивирусную проверку компьютера в онлайн-режиме. Kaspersky OnLine Scanner выполняется непосредственно в браузере. Таким образом, пользователи могут максимально оперативно получать ответ на вопросы, связанные с заражением вредоносными программами. В рамках проверки пользователь может:

- исключать архивы и почтовые базы из проверки;
- выбирать для проверки стандартные / расширенные базы;
- сохранять отчеты о результатах проверки в форматах txt и html.

Kaspersky® OnLine Scanner Pro

Программа представляет собой подписной сервис, доступный посетителям веб-сайта компании, позволяющий произвести эффективную антивирусную проверку компьютера и лечение зараженных файлов в онлайн-режиме. Kaspersky OnLine Scanner Pro выполняется непосредственно в браузере. В рамках проверки пользователь может:

- исключать архивы и почтовые базы из проверки;
- выбирать для проверки стандартные / расширенные базы;
- лечить обнаруженные зараженные объекты;
- сохранять отчеты о результатах проверки в форматах txt и html.

Антивирус Касперского® 7.0

Антивирус Касперского 7.0 предназначен для защиты персонального компьютера от вредоносных программ, оптимально сочетая в себе традиционные методы защиты от вирусов с новыми проактивными технологиями.

Программа позволяет осуществлять комплексную антивирусную проверку, включающую в себя:

- антивирусную проверку почтового трафика на уровне протокола передачи данных (POP3, IMAP и NNTP для входящих сообщений и SMTP – для исходящих) независимо от используемой почтовой программы, а также проверку и лечение почтовых баз;
- антивирусную проверку интернет-трафика, поступающего по HTTP-протоколу, в режиме реального времени;
- антивирусную проверку любых отдельных файлов, папок и дисков. Также, используя предустановленную задачу проверки, можно запустить анализ на присутствие вирусов только критических облас-

тей операционной системы и объектов, загружаемых при старте операционной системы Microsoft Windows.

Возможности проактивной защиты включают в себя:

- *Контроль изменений в файловой системе.* Программа позволяет создавать список приложений, компонентный состав которых будет контролироваться. Это помогает предотвратить нарушение целостности приложений вредоносными программами.
- *Наблюдение за процессами в оперативной памяти.* **Антивирус Касперского 7.0** своевременно предупреждает пользователя в случае появления опасных, подозрительных или скрытых процессов, а также в случае несанкционированного изменения активных процессов.
- *Мониторинг изменений в реестре операционной системы* благодаря контролю состояния системного реестра.
- *Контроль скрытых процессов* позволяет бороться с сокрытием вредоносного кода в операционной системе с использованием технологий rootkit.
- *Эвристический анализатор.* При проверке какой-либо программы анализатор эмулирует ее исполнение и протоколирует все ее подозрительные действия, например, открытие или запись в файл, перехват векторов прерываний и т.д. На основе этого протокола принимается решение о возможном заражении программы вирусом. Эмуляция происходит в искусственной изолированной среде, что исключает возможность заражения компьютера.
- *Восстановление системы* после вредоносного воздействия программ-шпионов **за счет** фиксации всех изменений реестра и файловой системы компьютера и их отката по решению пользователя.

Kaspersky® Internet Security 7.0

Kaspersky Internet Security 7.0 – комплексное решение для защиты персонального компьютера от основных информационных угроз – вирусов, хакеров, спама и шпионских программ. Единый пользовательский интерфейс обеспечивает настройку и управление всеми компонентами решения.

Функции антивирусной защиты включают в себя:

- *антивирусную проверку почтового трафика* на уровне протокола передачи данных (POP3, IMAP и NNTP для входящих сообщений и SMTP для исходящих) независимо от используемой почтовой программы. Для популярных почтовых программ Microsoft Office Outlook, Microsoft Outlook Express и The Bat! предусмотрены плагины и лечение вирусов в почтовых базах;

- *проверку интернет-трафика*, поступающего по HTTP-протоколу, в режиме реального времени;
- *защиту файловой системы*: антивирусной проверке могут быть подвергнуты любые отдельные файлы, папки и диски. Также возможна проверка только критических областей операционной системы и объектов, загружаемых при старте операционной системы Microsoft Windows;
- *проактивную защиту*: программа осуществляет постоянное наблюдение за активностью приложений и процессов, запущенных в оперативной памяти компьютера, предотвращает опасные изменения файловой системы и реестра, а также восстанавливает систему после вредоносного воздействия.

Защита от интернет-мошенничества обеспечивается благодаря распознаванию фишинговых атак, что позволяет предотвратить утечку вашей конфиденциальной информации (в первую очередь паролей, номеров банковских счетов и карт, а также блокированию выполнения опасных скриптов на веб-страницах, всплывающих окон и рекламных баннеров). Функция *блокирования автоматического дозвона на платные ресурсы интернета* помогает идентифицировать программы, которые пытаются использовать ваш модем для скрытого соединения с платными телефонными сервисами, и заблокировать их работу. Модуль *Защита конфиденциальных данных* обеспечивает защиту от несанкционированного доступа и передачи информации личного характера. Компонент *Родительский контроль* обеспечивает контроль доступа пользователей компьютера к интернет-ресурсам.

Kaspersky Internet Security 7.0 *фиксирует попытки сканирования портов вашего компьютера*, часто предшествующие сетевым атакам, и успешно отражает наиболее распространенные типы сетевых атак. На *основе заданных правил* программа осуществляет контроль всех сетевых взаимодействий, отслеживая все *входящие и исходящие пакеты данных*. Режим невидимости *предотвращает обнаружение компьютера извне*. При переключении в этот режим запрещается вся сетевая деятельность, кроме предусмотренных правилами исключений, которые определяются самим пользователем.

В программе применяется комплексный подход к фильтрации входящих почтовых сообщений на наличие спама:

- проверка по «черным» и «белым» спискам адресатов (включая адреса фишинговых сайтов);
- проверка фраз в тексте письма;
- анализ текста письма с помощью самообучающегося алгоритма;
- распознавание спама в виде изображений.

Антивирус Касперского для файловых серверов

Программный продукт обеспечивает надежную защиту файловых систем серверов под управлением операционных систем Microsoft Windows, Novell NetWare и Linux от всех видов вредоносных программ. В состав программного продукта входят следующие приложения «Лаборатории Касперского»:

- Kaspersky Administration Kit.
- Антивирус Касперского для Windows Server.
- Антивирус Касперского для Linux File Server.
- Антивирус Касперского для Novell Netware.
- Антивирус Касперского для Samba Server.

Преимущества и функциональные возможности:

- *защита файловых систем серверов в режиме реального времени:* все файлы серверов проверяются при попытке их открытия и сохранения на сервере.
- *предотвращение вирусных эпидемий;*
- *проверка по требованию* всей файловой системы или отдельных ее папок и файлов;
- *применение технологий оптимизации* при проверке объектов файловой системы сервера;
- *восстановление системы после заражения;*
- *масштабируемость программного продукта* в пределах доступных ресурсов системы;
- *соблюдение баланса загрузки системы;*
- *формирование списка доверенных процессов*, чья активность на сервере не подвергается контролю со стороны программного продукта;
- *удаленное управление* программным продуктом, включающее централизованную установку, настройку и управление;
- *хранение резервных копий зараженных и удаленных объектов* на тот случай, если потребуется их восстановление;
- *изоляция подозрительных объектов* в специальном хранилище;
- *оповещения о событиях* в работе программного продукта администратора системы;

- *ведение детальных отчетов;*
- *автоматическое обновление баз программного продукта.*

Kaspersky Open Space Security

Kaspersky Open Space Security – это программный продукт, реализующий новый подход к безопасности современных корпоративных сетей любого масштаба, обеспечивающий централизованную защиту информационных систем, а также поддержку удаленных офисов и мобильных пользователей.

Программный продукт включает в себя четыре продукта:

- Kaspersky Work Space Security.
- Kaspersky Business Space Security.
- Kaspersky Enterprise Space Security.
- Kaspersky Total Space Security.

Рассмотрим подробнее каждый продукт.

Kaspersky Work Space Security – это продукт для централизованной защиты рабочих станций в корпоративной сети и за ее пределами от всех видов современных интернет-угроз: вирусов, шпионских программ, хакерских атак и спама.

Преимущества и функциональные возможности:

- *целостная защита от вирусов, шпионских программ, хакерских атак и спама;*
- *проактивная защита от новых вредоносных программ, записи о которых еще не добавлены в базы;*
- *персональный сетевой экран с системой обнаружения вторжений и предупреждения сетевых атак;*
- *отмена вредоносных изменений в системе;*
- *защита от фишинг-атак и нежелательной почтовой корреспонденции;*
- *динамическое перераспределение ресурсов при полной проверке системы;*
- *удаленное управление программным продуктом, включающее централизованную установку, настройку и управление;*
- *поддержка Cisco® NAC (Network Admission Control);*
- *проверка электронной почты и интернет-трафика в режиме реального времени;*

- *блокирование всплывающих окон и рекламных баннеров* при работе в интернете;
- *безопасная работа в сетях любого типа*, включая Wi-Fi;
- *средства для создания диска аварийного восстановления*, позволяющего восстановить систему после вирусной атаки;
- *развитая система отчетов* о состоянии защиты;
- *автоматическое обновление баз*;
- *полноценная поддержка 64-битных операционных систем*;
- *оптимизация работы программного продукта на ноутбуках* (технология Intel® Centrino® Duo для мобильных ПК);
- *возможность удаленного лечения* (технология Intel® Active Management, компонент Intel® vPro™).

Kaspersky Business Space Security обеспечивает оптимальную защиту информационных ресурсов компании от современных интернет-угроз. Kaspersky Business Space Security защищает рабочие станции и файловые серверы от всех видов вирусов, троянских программ и червей, предотвращает вирусные эпидемии, а также обеспечивает сохранность информации и мгновенный доступ пользователей к сетевым ресурсам.

Преимущества и функциональные возможности:

- *удаленное управление* программным продуктом, включающее централизованную установку, настройку и управление;
- *поддержка Cisco® NAC (Network Admission Control)*;
- *защита рабочих станций и файловых серверов от всех видов интернет-угроз*;
- *использование технологии iSwift для исключения повторных проверок* в рамках сети;
- *распределение нагрузки между процессорами сервера*;
- *изоляция подозрительных объектов* рабочих станций в специальном хранилище;
- *отмена вредоносных изменений в системе*;
- *масштабируемость программного продукта* в пределах доступных ресурсов системы;
- *проактивная защита* рабочих станций от новых вредоносных программ, записи о которых еще не добавлены в базы;

- *проверка электронной почты и интернет-трафика* в режиме реального времени;
- *персональный сетевой экран* с системой обнаружения вторжений и предупреждения сетевых атак;
- *защита при работе в беспроводных сетях Wi-Fi*;
- *технология самозащиты антивируса от вредоносных программ*;
- *изоляция подозрительных объектов* в специальном хранилище;
- *автоматическое обновление баз*.

Kaspersky Enterprise Space Security

Программный продукт включает компоненты для защиты рабочих станций и серверов совместной работы от всех видов современных интернет-угроз, удаляет вирусы из потока электронной почты, обеспечивает сохранность информации и мгновенный безопасный доступ пользователей к сетевым ресурсам.

Преимущества и функциональные возможности:

- *защита рабочих станций и серверов от вирусов, троянских программ и червей*;
- *защита почтовых серверов Sendmail, Qmail, Postfix и Exim*;
- *проверка всех сообщений на сервере Microsoft Exchange*, включая общие папки;
- *обработка сообщений, баз данных и других объектов серверов Lotus Domino*;
- *защита от фишинг-атак и нежелательной почтовой корреспонденции*;
- *предотвращение массовых рассылок и вирусных эпидемий*;
- *масштабируемость программного продукта* в пределах доступных ресурсов системы;
- *удаленное управление* программным продуктом, включающее централизованную установку, настройку и управление;
- *поддержка Cisco® NAC (Network Admission Control)*;
- *проактивная защита* рабочих станций от новых вредоносных программ, записи о которых еще не добавлены в базы;

- *персональный сетевой экран с системой обнаружения вторжений и предупреждения сетевых атак;*
- *безопасная работа в беспроводных сетях Wi-Fi;*
- *проверка интернет-трафика в режиме реального времени;*
- *отмена вредоносных изменений в системе;*
- *динамическое перераспределение ресурсов при полной проверке системы;*
- *изоляция подозрительных объектов в специальном хранилище;*
- *система отчетов о состоянии системы защиты;*
- *автоматическое обновление баз.*

Kaspersky Total Space Security

Решение контролирует все входящие и исходящие потоки данных – электронную почту, интернет-трафик и все сетевые взаимодействия. Продукт включает компоненты для защиты рабочих станций и мобильных устройств, обеспечивает мгновенный и безопасный доступ пользователей к информационным ресурсам компании и сети Интернет, а также гарантирует безопасные коммуникации по электронной почте.

Преимущества и функциональные возможности:

- *целостная защита от вирусов, шпионских программ, хакерских атак и слама на всех уровнях корпоративной сети: от рабочих станций до интернет-шлюзов;*
- *проактивная защита рабочих станций от новых вредоносных программ, записи о которых еще не добавлены в базы;*
- *защита почтовых серверов и серверов совместной работы;*
- *проверка интернет-трафика (HTTP/FTP), поступающего в локальную сеть, в режиме реального времени;*
- *масштабируемость программного продукта в пределах доступных ресурсов системы;*
- *блокирование доступа с зараженных рабочих станций;*
- *предотвращение вирусных эпидемий;*
- *централизованные отчеты о состоянии защиты;*
- *удаленное управление программным продуктом, включающее централизованную установку, настройку и управление;*

- *поддержка Cisco® NAC (Network Admission Control);*
- *поддержка аппаратных прокси-серверов;*
- *фильтрация интернет-трафика по списку доверенных серверов, типам объектов и группам пользователей;*
- *использование технологии iSwift для исключения повторных проверок в рамках сети;*
- *динамическое перераспределение ресурсов при полной проверке системы;*
- *персональный сетевой экран с системой обнаружения вторжений и предупреждения сетевых атак;*
- *безопасная работа пользователей в сетях любого типа, включая WiFi;*
- *защита от фишинг-атак и нежелательной почтовой корреспонденции;*
- *возможность удаленного лечения (технология Intel® Active Management, компонент Intel® vPro™);*
- *отмена вредоносных изменений в системе;*
- *технология самозащиты антивируса от вредоносных программ;*
- *полноценная поддержка 64-битных операционных систем;*
- *автоматическое обновление баз.*

Kaspersky Security для почтовых серверов

Программный продукт для защиты почтовых серверов и серверов совместной работы от вредоносных программ и спама. Продукт включает в себя приложения для защиты всех популярных почтовых серверов: Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix и Exim, а также позволяет организовать выделенный почтовый шлюз. В состав решения входят:

- Kaspersky Administration Kit.
- Kaspersky Mail Gateway.
- Антивирус Касперского для Lotus Notes/Domino.
- Антивирус Касперского для Microsoft Exchange.
- Антивирус Касперского для Linux Mail Server.

Среди его возможностей:

- *надежная защита от вредоносных и потенциально опасных программ;*
- *фильтрация нежелательной почтовой корреспонденции;*
- *проверка входящих и исходящих почтовых сообщений и вложений;*
- *антивирусная проверка всех сообщений на сервере Microsoft Exchange, включая общие папки;*
- *проверка сообщений, баз данных и других объектов серверов Lotus Notes/Domino;*
- *фильтрация сообщений по типам вложений;*
- *изоляция подозрительных объектов в специальном хранилище;*
- *удобная система управления программным продуктом;*
- *предотвращение вирусных эпидемий;*
- *мониторинг состояния системы защиты с помощью уведомлений;*
- *система отчетов о работе приложения;*
- *масштабируемость программного продукта в пределах доступных ресурсов системы;*
- *автоматическое обновление баз.*

Kaspersky Security для интернет-шлюзов

Программный продукт обеспечивает безопасный доступ к сети Интернет для всех сотрудников организации, автоматически удаляя вредоносные и потенциально опасные программы из потока данных, поступающего в сеть по протоколам HTTP/FTP. В состав продукта входят:

- Kaspersky Administration Kit.
- Антивирус Касперского для Proxy Server.
- Антивирус Касперского для Microsoft ISA Server.
- Антивирус Касперского для Check Point FireWall-1.

Среди его возможностей:

- *надежная защита от вредоносных и потенциально опасных программ;*
- *проверка интернет-трафика (HTTP/FTP) в режиме реального времени;*

- *фильтрация интернет-трафика* по списку доверенных серверов, типам объектов и группам пользователей;
- *изоляция подозрительных объектов* в специальном хранилище;
- *удобная система управления*;
- *система отчетов о работе приложения*;
- *поддержка аппаратных прокси-серверов*;
- *масштабируемость программного продукта* в пределах доступных ресурсов системы;
- *автоматическое обновление баз*.

Kaspersky® Anti-Spam

Kaspersky Anti-Spam – первый российский программный комплекс для защиты от нежелательных писем (спама) для предприятий средних и малых масштабов. Продукт сочетает революционные технологии лингвистического анализа текстов, все современные методы фильтрации электронной почты (включая списки DNS Black List и формальные признаки письма) и уникальный набор сервисов, которые позволяют пользователям распознать и уничтожить до девяноста пяти процентов нежелательного трафика.

Kaspersky® Anti-Spam представляет собой фильтр, который устанавливается на «входе» в сеть предприятия и проверяет входящий поток писем на предмет обнаружения спама. Продукт совместим с любой почтовой системой, используемой в сети заказчика, и может быть установлен как на уже существующий почтовый сервер, так и на выделенный.

Высокая эффективность работы программы достигается благодаря ежедневному автоматическому обновлению баз контентной фильтрации образцами, предоставляемыми специалистами лингвистической лаборатории. Обновления баз выпускаются каждые 20 минут.

Антивирус Касперского® для MIMESweeper

Антивирус Касперского® для MIMESweeper обеспечивает высокоскоростную антивирусную проверку трафика на серверах, использующих Clearswift MIMESweeper for SMTP / Clearswift MIMESweeper for Exchange / Clearswift MIMESweeper for Web.

Программа выполнена в виде плагина (модуля расширения) и осуществляет в режиме реального времени антивирусную проверку и обработку входящих и исходящих почтовых сообщений.

А.2. Наши координаты

Если у вас возникнут какие-либо вопросы, вы можете обратиться к нашим дистрибьюторам или непосредственно в ЗАО «Лаборатория Касперского». Вам всегда будут предоставлены подробные консультации по телефону или электронной почте. На все ваши вопросы вы получите полные и исчерпывающие ответы.

Адрес:	Россия, 123060, Москва, 1-й Волоколамский проезд, д.10, стр.1
Факс:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00
Экстренная круглосуточная помощь:	+7 (495) 797-87-07, +7 (495) 645-79-29, +7 (495) 956-87-08
Поддержка пользователей персональных и бизнес-продуктов:	+7 (495) 797-87-07, +7 (495) 645-79-29, +7 (495) 956-87-08 (с 10 до 19 часов) http://support.kaspersky.ru/helpdesk.html
Поддержка корпоративных пользователей:	контактная информация предоставляется при покупке корпоративных продуктов в зависимости от пакета технической поддержки.
Веб-форум «Лаборатория Касперского»:	http://forum.kaspersky.com
Антивирусная лаборатория:	newvirus@kaspersky.com (только для отправки новых вирусов в архивированном виде)
Группа подготовки пользовательской документации:	docfeedback@kaspersky.com (только для отправки отзывов о документации и электронной справочной системе)
Департамент продаж:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00 sales@kaspersky.com
Общая информация:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00 info@kaspersky.com

WWW:

<http://www.kaspersky.ru>

<http://www.viruslist.ru>