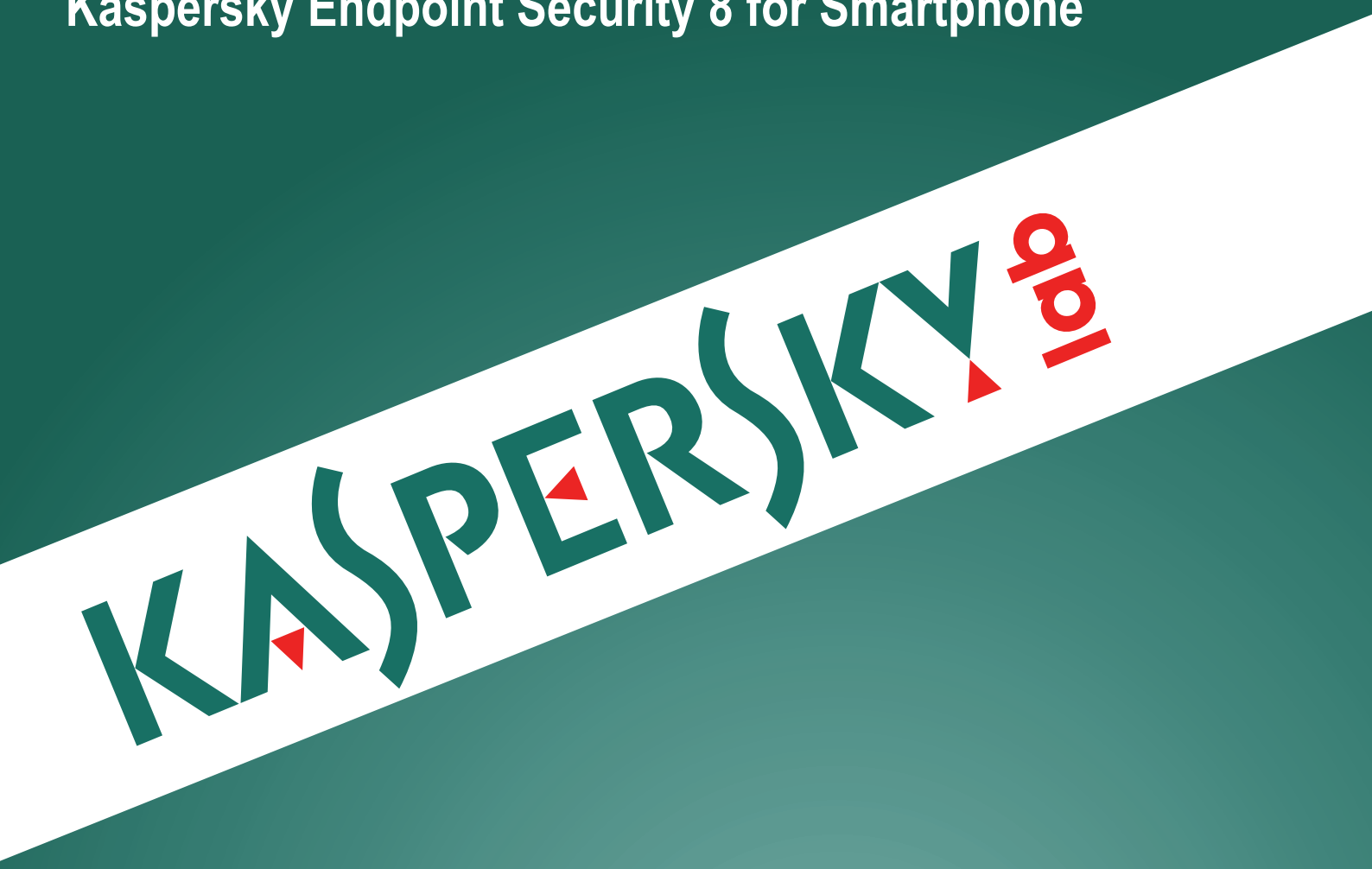
Kaspersky Endpoint Security 8 for Smartphone



Руководство по внедрению

ВЕРСИЯ ПРОГРАММЫ: 8.0

Уважаемый пользователь!

Спасибо за то, что выбрали наш продукт. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.

Дата редакции документа: 01.06.2011

http://www.kaspersky.ru
http://support.kaspersky.ru

СОДЕРЖАНИЕ

ОБ ЭТОМ РУКОВОДСТВЕ

Вас приветствуют специалисты «Лаборатории Касперского». Мы надеемся, что информация, представленная в этом руководстве, поможет вам в работе с Kaspersky Endpoint Security 8 for Smartphone.

Руководство ориентировано на администраторов корпоративных сетей. В нем содержится информация о том, как установить и настроить программу на мобильных устройствах пользователей через следующие платформы:

- Kaspersky Administration Kit.
- Microsoft® System Center Mobile Device Manager.
- Sybase Afaria.

Информация по использованию Антивируса Касперского на мобильных устройствах с различными операционными системами приведена в Руководствах пользователей Kaspersky Endpoint Security 8 for Smartphone для каждой операционной системы отдельно.

Если вы не нашли ответа на ваш вопрос о Kaspersky Endpoint Security 8 for Smartphone в этом документе, вы можете обратиться к другим источникам информации (см. раздел «Дополнительные источники информации» на стр. 8).

В ЭТОМ РАЗДЕЛЕ

В ЭТОМ ДОКУМЕНТЕ

В этом документе представлены следующие разделы:

- *Дополнительные источники информации* (на стр. 8). В разделе представлена информация о том, где, помимо набора документов, входящих в комплект поставки, можно получить сведения о программе и как в случае необходимости обратиться за информацией в «Лабораторию Касперского».
- *Управление лицензиями (на стр. 23).* В разделе представлена подробная информация об основных понятиях, связанных с лицензированием Kaspersky Endpoint Security 8 for Smartphone, а также о том, как установить и удалить лицензию для Kaspersky Endpoint Security 8 for Smartphone на мобильных устройствах пользователей.
- *Kaspersky Endpoint Security 8 for Smartphone* (на стр. 10). В разделе перечислены основные функции Kaspersky Endpoint Security 8 for Smartphone, отличия Kaspersky Endpoint Security 8 for Smartphone от предыдущей версии программы, а также представлены аппаратные и программные требования к мобильным устройствам пользователей и системе административного управления.
- *О компонентах Kaspersky Endpoint Security 8 for Smartphone* (на стр. 16). В разделе для каждого компонента описано его назначение, алгоритм работы и приведена информация об операционных системах, поддерживающих этот компонент и входящие в него функции.
- *Развертывание программы через Kaspersky Administration Kit* (на стр. 27). В этом разделе рассмотрен процесс развертывания Kaspersky Endpoint Security 8 for Smartphone через Kaspersky Administration Kit.
- *Развертывание программы через MS SCMDM* (на стр. 85). В этом разделе рассмотрен процесс развертывания Kaspersky Endpoint Security 8 for Smartphone через Mobile Device Manager.

- *Развертывание программы через Sybase Afaria* (на стр. 129). В этом разделе рассмотрен процесс развертывания Kaspersky Endpoint Security 8 for Smartphone через Sybase Afaria.
- *Обращение в Службу технической поддержки*. В разделе описаны правила обращения в Службу технической поддержки.
- *Глоссарий терминов*. В разделе перечислены термины, используемые в этом руководстве.
- *ЗАО «Лаборатория Касперского»* (см. стр. 164). В разделе приводится информация о ЗАО «Лаборатория Касперского».
- *Информация об использовании стороннего кода*. В разделе приводится информация о стороннем коде, используемом в программе.
- *Предметный указатель*. С помощью этого раздела вы можете быстро найти необходимые сведения в документе.

Условные обозначения

В руководстве используются условные обозначения, описанные в таблице ниже.

Таблица 1. Условные обозначения

Пример текста	Описание условного обозначения
Обратите внимание, что...	Предупреждения выделяются красным цветом и заключаются в рамку. В предупреждениях содержится важная информация, например, связанная с критическими для безопасности компьютера действиями.
Рекомендуется использовать...	Примечания заключаются в рамку. В примечаниях содержится вспомогательная и справочная информация.
Пример: ..	Примеры приводятся в блоке на желтом фоне под заголовком «Пример».
Обновление – это...	Новые термины выделяются курсивом.
ALT+F4	Названия клавиш клавиатуры выделяются полужирным шрифтом и прописными буквами. Названия клавиш, соединенные знаком «плюс», означают комбинацию клавиш.
Включить	Названия элементов интерфейса, например, полей ввода, команд меню, кнопок, выделяются полужирным шрифтом.
➡ *Чтобы настроить расписание задачи, выполните следующие действия:*	Инструкции отмечаются значком в виде стрелки. Вводные фразы инструкций выделяются курсивом.
`help`	Тексты командной строки или тексты сообщений, выводимых программой на экран, выделяются специальным шрифтом.
<IP-адрес вашего компьютера>	Переменные заключаются в угловые скобки. Вместо переменной в каждом случае подставляется соответствующее ей значение, угловые скобки при этом опускаются.

ДОПОЛНИТЕЛЬНЫЕ ИСТОЧНИКИ ИНФОРМАЦИИ

Если у вас возникли вопросы, связанные с выбором, приобретением, установкой или использованием Kaspersky Endpoint Security 8 for Smartphone, вы можете получить ответы на них, используя различные источники информации. Вы можете выбрать наиболее удобный для себя источник информации в зависимости от важности и срочности вопроса.

В ЭТОМ РАЗДЕЛЕ

Источники информации для самостоятельного поиска

Вы можете обратиться к следующим источникам информации о программе:

- странице программы на веб-сайте «Лаборатории Касперского»;
- странице программы на веб-сайте Службы технической поддержки (в Базе знаний);
- электронной справочной системе;
- документации.

Страница на веб-сайте «Лаборатории Касперского»

http://www.kaspersky.ru/endpoint-security-smartphone

На этой странице вы получите общую информацию по Kaspersky Endpoint Security 8 for Smartphone, его возможностям и особенностям работы. Вы можете приобрести Kaspersky Endpoint Security 8 for Smartphone или продлить срок его использования в нашем электронном магазине.

Страница на веб-сайте Службы технической поддержки (База знаний)

http://support.kaspersky.ru/kes8m

На этой странице вы найдете статьи, опубликованные специалистами Службы технической поддержки.

Эти статьи содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы, связанные с приобретением, установкой и использованием Kaspersky Endpoint Security 8 for Smartphone. Они сгруппированы по темам, например: «Работа с ключевыми файлами», «Обновление баз» или «Устранение сбоев в работе». Статьи могут отвечать на вопросы, относящиеся не только к Kaspersky Endpoint Security 8 for Smartphone, но и к другим продуктам «Лаборатории Касперского», а также содержать новости Службы технической поддержки в целом.

Электронная справочная система

В электронную справочную систему Kaspersky Endpoint Security 8 for Smartphone входит контекстная справка для плагина управления программой через Kaspersky Administration Kit, а также контекстные справки для мобильных устройств пользователей со следующими операционными системами:

- Microsoft Windows® Mobile.
- Symbian.
- BlackBerry®.
- Android™.

Контекстная справка содержит информацию об отдельных окнах / закладках программы.

Документация

Комплект документации к Kaspersky Endpoint Security 8 for Smartphone содержит большую часть информации, необходимой для работы с ним. В комплект входят следующие документы:

- **Руководства пользователя**. Руководства пользователя по использованию программы на мобильных устройствах с операционными системами Windows Mobile, Symbian, BlackBerry и Android. Каждое руководство пользователя содержит информацию, позволяющую пользователю самостоятельно установить, настроить и активировать программу на мобильном устройстве.
- **Руководство по внедрению**. Руководство по внедрению позволяет администратору установить и настроить программу на мобильных устройствах пользователей через следующие платформы:
  - Kaspersky Administration Kit.
  - Microsoft System Center Mobile Device Manager.
  - Sybase Afaria.

Обсуждение программ «Лаборатории Касперского» на веб-форуме

Если ваш вопрос не требует срочного ответа, его можно обсудить со специалистами «Лаборатории Касперского» и другими пользователями на нашем форуме по адресу http://forum.kaspersky.com/index.php?showforum=5.

На форуме вы можете просматривать опубликованные темы, оставлять свои комментарии, создавать новые темы, пользоваться поиском.

Обращение в Группу разработки технической документации

Если у вас возникли вопросы, связанные с документацией, вы обнаружили в ней ошибку или хотите оставить отзыв о наших документах, вы можете обратиться к сотрудникам Группы разработки технической документации. Для обращения в Группу разработки документации отправьте письмо по адресу docfeedback@kaspersky.com. В качестве темы письма укажите «Kaspersky Help Feedback: Kaspersky Endpoint Security 8 for Smartphone».

KASPERSKY ENDPOINT SECURITY 8 FOR SMARTPHONE

Kaspersky Endpoint Security 8 for Smartphone обеспечивает защиту мобильных устройств, работающих на базе операционных систем Symbian, Microsoft Windows Mobile, BlackBerry и Android, от известных и новых угроз, нежелательных вызовов и SMS. Программа позволяет контролировать исходящие SMS, сетевую активность, а также защищать конфиденциальную информацию от несанкционированного доступа. Каждый тип угроз обрабатывают отдельные компоненты программы. Это дает возможность гибко настраивать параметры программы в зависимости от нужд конкретного пользователя.

Kaspersky Endpoint Security 8 for Smartphone поддерживает работу с системами удаленного администрирования Kaspersky Administration Kit, MS SCMDM и Sybase Afaria. Используя возможности этих систем, администратор сети может дистанционно:

- устанавливать программу на мобильные устройства;
- удалять программу с устройств через MS SCMDM;
- настраивать параметры работы программы как для нескольких устройств сразу, так и индивидуально для каждого отдельного устройства;
- формировать отчеты о работе компонентов программы, установленной на мобильных устройствах, через Kaspersky Administration Kit.

В Kaspersky Endpoint Security 8 for Smartphone включены следующие компоненты защиты:

- **Защита**. Защищает от заражения файловую систему мобильного устройства. Компонент Защита запускается при старте операционной системы, постоянно находится в оперативной памяти устройства и проверяет все открываемые, сохраняемые и запускаемые файлы на устройстве, в том числе и на картах памяти. Кроме того, Защита проверяет все входящие файлы на присутствие известных вирусов. Дальнейшая работа с файлом возможна, если объект не заражен или успешно вылечен.
- **Проверка устройства**. Помогает обнаружить и нейтрализовать вредоносные объекты на мобильном устройстве. Необходимо периодически проводить проверку устройства, чтобы предотвратить распространение вредоносных объектов, которые не были обнаружены Защитой.
- **Анти-Спам**. Проверяет все входящие SMS и вызовы на предмет спама. Компонент позволяет блокировать все SMS и вызовы, которые считаются нежелательными. Фильтрация сообщений и вызовов осуществляется с помощью «черного» и (или) «белого» списков номеров. Все SMS и вызовы с номеров, входящих в «черный» список, блокируются. SMS и вызовы с номеров, входящих в «белый» список, всегда доставляются на мобильное устройство. Компонент также позволяет настроить реакцию программы на SMS, приходящие с нечисловых номеров, и на вызовы и SMS с номеров не из Контактов.
- **Анти-Вор**. Защищает информацию на устройстве от несанкционированного доступа, когда оно потеряно или украдено. Компонент позволяет дистанционно заблокировать устройство в случае его потери или кражи, удалить конфиденциальную информацию, а также проконтролировать смену SIM-карты и определить географические координаты устройства (если мобильное устройство оснащено GPS-приемником).
- **Личные контакты**. Скрывает конфиденциальную информацию пользователя в то время, когда устройство используют другие лица. Компонент позволяет отображать или скрывать всю информацию, связанную с указанными номерами абонентов, например, данные в списке контактов, SMS-переписку, записи в журнале вызовов. Компонент позволяет также скрывать доставку входящих вызовов и SMS с указанных номеров абонентов.

- **Сетевой экран**. Контролирует сетевые подключения на мобильном устройстве. Компонент позволяет задать соединения, которые будут разрешены или заблокированы.

- **Шифрование**. Защищает информацию от просмотра посторонними лицами даже в том случае, если к устройству получен доступ. Компонент шифрует произвольное количество несистемных папок, сохраненных как в памяти устройства, так и на картах памяти. Данные в папке доступны только после ввода секретного кода.

Кроме того, программа содержит ряд следующих сервисных функций. Они предусмотрены для того, чтобы поддерживать программу в актуальном состоянии, расширить возможности использования программы, а также оказать пользователю помощь в работе.

- Обновление баз программы. Функция позволяет поддерживать базы Kaspersky Endpoint Security 8 for Smartphone в актуальном состоянии. Запуск обновления может выполняться пользователем устройства вручную или по расписанию с периодичностью, заданной в настройках программы.

- Статус защиты. На экране отображаются статусы компонентов программы. На основании представленной информации пользователь может оценить текущее состояние защиты своего устройства.

- Журнал событий. В программе для каждого компонента ведется свой журнал событий, в котором содержится информация о работе компонента (например, выполненная операция, данные о заблокированном объекте, отчет о проверке, обновлении).

- Лицензия. При покупке Kaspersky Endpoint Security 8 for Smartphone между вашей компанией и «Лабораторией Касперского» заключается лицензионное соглашение, на основе которого сотрудники компании могут использовать программу и получать доступ к обновлению баз программы и Службе технической поддержки в течение определенного времени. Срок использования, а также другая информация, необходимая для полнофункциональной работы программы, указаны в лицензии.

Kaspersky Endpoint Security 8 for Smartphone не выполняет резервного копирования данных и их последующего восстановления.

В ЭТОМ РАЗДЕЛЕ

Что нового

Отличия Kaspersky Endpoint Security 8 for Smartphone от предыдущей версии программы состоят в следующем:

- Поддержка новых платформ: Sybase Afaria и Microsoft System Center Mobile Device Manager (MS SCMDM).

- Установка программы на устройства с помощью рассылки писем по электронной почте.

- Доступ к программе защищен секретным кодом.

- Расширен список исполняемых файлов, проверяемых программой в случае ограничения типов файлов, проверяемых компонентами Защита и Проверка. Проверяются исполняемые файлы программ следующих форматов: EXE, DLL, MDL, APP, RDL, PRT, PXT, LDD, PDD, CLASS. Если функция проверки архивов включена, то программа распаковывает и проверяет архивы следующих форматов: ZIP, JAR, JAD, SIS, SISX, RAR и CAB.

- Компонент Личные контакты позволяет скрывать следующую информацию для конфиденциальных контактов: записи в Контактах, SMS-переписку, журнал звонков, а также новые поступившие SMS и входящие вызовы. Конфиденциальная информация доступна для просмотра, когда скрытие отключено.

- Компонент Шифрование позволяет зашифровать папки, сохраненные в памяти устройства или на карте расширения памяти. Компонент хранит конфиденциальные данные в зашифрованном виде и разрешает доступ к зашифрованной информации только после ввода секретного кода программы.

- В состав обновленного Анти-Вора включена новая функция GPS-Поиск, которая в случае потери или кражи устройства позволяет получить его географические координаты на номер телефона и на указанный адрес электронной почты. Кроме того, в Анти-Воре обновлена функция Удаление данных, которая позволяет дистанционно удалить не только персональную информацию пользователя, сохраненную в памяти телефона или на карте памяти, но и файлы из сформированного списка удаляемых папок.

- В целях экономии трафика добавлена возможность автоматического отключения обновления баз программы при нахождении мобильного устройства в зоне роуминга.

- Добавлена новая сервисная функция Отображение подсказок: Kaspersky Endpoint Security 8 for Smartphone показывает краткое описание компонента перед настройкой его параметров.

- Добавлена поддержка устройств с операционной системой Android.

Комплект поставки

Kaspersky Endpoint Security 8 for Smartphone вы можете приобрести у партнеров или в одном из интернет-магазинов (например, http://www.kaspersky.ru, раздел **Интернет-магазин**). Кроме того, Kaspersky Endpoint Security 8 for Smartphone поставляется в составе всех продуктов, входящих в линейку Kaspersky Open Space Security.

При покупке Kaspersky Endpoint Security 8 for Smartphone в интернет-магазине вы оформляете заказ, по факту оплаты которого вам по электронной почте отправляется информационное письмо, содержащее файл ключа для активации программы и ссылку, по которой можно скачать дистрибутив программы. За подробной информацией о способах покупки и комплекте вы можете обратиться в отдел продаж по адресу sales@kaspersky.com.

Если в вашей организации для развертывания Kaspersky Endpoint Security 8 for Smartphone используется Kaspersky Administration Kit, то в состав дистрибутива программы входит самораспаковывающийся архив KES8_forAdminKit_ru.exe, который содержит следующие файлы, необходимые для установки программы на мобильных устройствах:

- klcfginst.exe – установочный файл плагина управления Kaspersky Endpoint Security 8 for Smartphone через Kaspersky Administration Kit;

- endpoint_8_0_x_xx_ru.cab – установочный файл программы для операционной системы Microsoft Windows Mobile;

- endpoint8_mobile_8_x_xx_eu4_signed.sis – установочный файл программы для операционной системы Symbian;

- Endpoint8_Mobile_8_x_xx_release.zip – установочный файл программы для операционной системы BlackBerry;

- Endpoint8_8_x_xx_release.apk – установочный файл программы для операционной системы Android;

- AdbWinUsbApi.dll, AdbWinApi.dll, adb.exe – набор файлов, необходимый для установки программы на устройства с операционной системой Android;

- installer.ini – конфигурационный файл с параметрами подключения к Серверу администрирования;

- kmlisten.ini – конфигурационный файл с настройками для утилиты доставки инсталляционного пакета;

- kmlisten.kpd – файл с описанием программы;
- kmlisten.exe – утилита доставки инсталляционного пакета на мобильное устройство через рабочую станцию;
- комплект документации:
  - Руководство по внедрению Kaspersky Endpoint Security 8 for Smartphone;
  - Руководство пользователя Kaspersky Endpoint Security 8 for Smartphone для Microsoft Windows Mobile;
  - Руководство пользователя Kaspersky Endpoint Security 8 for Smartphone для Symbian OS;
  - Руководство пользователя Kaspersky Endpoint Security 8 for Smartphone для BlackBerry OS;
  - Руководство пользователя Kaspersky Endpoint Security 8 for Smartphone для Android OS;
  - контекстная справка плагина управления Kaspersky Endpoint Security 8 for Smartphone;
  - контекстная справка программы для Microsoft Windows Mobile;
  - контекстная справка программы для Symbian OS;
  - контекстная справка программы для BlackBerry OS;
  - контекстная справка программы для Android OS.

Если в вашей организации для развертывания Kaspersky Endpoint Security 8 for Smartphone используется Mobile Device Manager, то в состав дистрибутива программы входит самораспаковывающийся архив KES8_forMicrosoftMDM_ru.exe, который содержит следующие файлы, необходимые для установки программы на мобильных устройствах:

- endpoint_MDM_Afaria_8_0_x_xx_ru.cab – установочный файл программы для операционной системы Microsoft Windows Mobile;
- endpoint8_ru.adm – файл административного шаблона управления политиками, содержащий их параметры;
- endpoint8_ca.cer – файл сертификата центра сертификации;
- endpoint8_cert.cer – файл сертификата, которым подписан установочный файл программы;
- kes2mdm.exe – утилита для преобразования файла ключа программы;
- kl.pbv, licensing.dll, oper.pbv – набор файлов, обеспечивающий работу утилиты kes2mdm.exe;
- комплект документации:
  - Руководство по внедрению Kaspersky Endpoint Security 8 for Smartphone;
  - Руководство пользователя Kaspersky Endpoint Security 8 for Smartphone для Microsoft Windows Mobile;
  - контекстная справка программы для Microsoft Windows Mobile.

Если в вашей организации для развертывания Kaspersky Endpoint Security 8 for Smartphone используется Sybase Afaria, то в состав дистрибутива программы входит самораспаковывающийся архив KES8_forSybaseAfaria_ru.exe, который содержит следующие файлы, необходимые для установки программы на мобильных устройствах:

- endpoint_MDM_Afaria_8_0_x_xx_ru.cab – установочный файл программы для операционной системы Microsoft Windows Mobile;
- endpoint8_mobile_8_x_xx_eu4.sisx – установочный файл программы для операционной системы Symbian;
- Endpoint8_Mobile_Installer.cod – установочный файл программы для операционной системы BlackBerry;
- KES2Afaria.exe – утилита управления политикой программы Kaspersky Endpoint Security 8 for Smartphone;
- kl.pbv, licensing.dll, oper.pbv – набор файлов, входящий в состав утилиты KES2Afaria.exe и необходимый для ее работы;
- комплект документации:
  - Руководство по внедрению Kaspersky Endpoint Security 8 for Smartphone;
  - Руководство пользователя Kaspersky Endpoint Security 8 for Smartphone для Microsoft Windows Mobile;
  - Руководство пользователя Kaspersky Endpoint Security 8 for Smartphone для Symbian OS;
  - Руководство пользователя Kaspersky Endpoint Security 8 for Smartphone для BlackBerry OS;
  - контекстная справка программы для Microsoft Windows Mobile;
  - контекстная справка программы для Symbian OS;
  - контекстная справка программы для BlackBerry OS.

Аппаратные и программные требования

Для нормального функционирования Kaspersky Endpoint Security 8 for Smartphone мобильные устройства пользователей должны удовлетворять следующим требованиям.

Аппаратные требования:

- Symbian OS 9.1, 9.2, 9.3, 9.4 Series 60® UI, Symbian^3 (только для мобильных устройств Nokia®).
- Windows Mobile 5.0, 6.0, 6.1, 6.5.
- BlackBerry 4.5, 4.6, 4.7, 5.0, 6.0.
- Android 1.5, 1.6, 2.0, 2.1, 2.2, 2.3.

Для развертывания Kaspersky Endpoint Security 8 for Smartphone в сети система удаленного администрирования должна удовлетворять следующим минимальным требованиям:

Программные требования:

- Kaspersky Administration Kit 8.0 Critical Fix 2.
- Mobile Device Manager Software Distribution Microsoft Corporation Version: 1.0.4050.0000 (SP).
- System Center Mobile Device Manager Microsoft Corporation Version: 1.0.4050.0000.
- Sybase Afaria 6.50.4607.0.

О КОМПОНЕНТАХ KASPERSKY ENDPOINT SECURITY 8 FOR SMARTPHONE

В состав Kaspersky Endpoint Security 8 for Smartphone входят следующие компоненты:

- Файловый Антивирус (на стр. 16).
- Анти-Вор (на стр. 19).
- Личные контакты (на стр. 20).
- Анти-Спам (на стр. 20).
- Сетевой экран (на стр. 21).
- Шифрование (на стр. 21).

В разделе для каждого компонента описано его назначение, алгоритм работы и приведена информация об операционных системах, поддерживающих этот компонент и входящие в него функции.

В ЭТОМ РАЗДЕЛЕ

Файловый Антивирус

Компонент Файловый Антивирус обеспечивает антивирусную защиту мобильных устройств. В его состав входят следующие функции: Защита (на стр. 17), Проверка по требованию (на стр. 17), Обновление (на стр. 18).

В ЭТОМ РАЗДЕЛЕ

ЗАЩИТА

Защита проверяет все выполняемые процессы в файловой системе, отслеживает события на устройстве, проверяет все новые, открытые, измененные файлы (в том числе и расположенные на карте памяти), а также установленные программы на наличие вредоносного кода непосредственно перед обращением пользователя к ним.

Алгоритм работы Защиты следующий:

1. Защита запускается при старте операционной системы.

2. Защита проверяет файлы выбранного типа при обращении к ним пользователя. Проверка выполняется на основании антивирусных баз программы.

3. По результатам анализа Защита выполняет действие в зависимости от операционной системы.

   Для операционных систем Symbian, Microsoft Windows Mobile возможны следующие варианты поведения Защиты:

   - если в файле обнаружен вредоносный код, Защита блокирует файл, выполняет действие в соответствии с заданными параметрами, информирует пользователя об обнаружении вредоносного объекта и записывает информацию в журнал событий;

   - если в файле не обнаружено вредоносного кода, файл сразу же становится доступным для работы.

   Для операционной системы Android возможны следующие варианты поведения Защиты:

   - если в файле обнаружен вредоносный код, Защита выполняет действие в соответствии с заданными параметрами;

   - если в файле не обнаружено вредоносного кода, файл сразу же становится доступным для работы.

4. Защита записывает отчет о событиях и действиях пользователя в журнал событий (для операционных систем Symbian, Microsoft Windows Mobile).

   Отчеты о событиях и действиях пользователя отсутствуют в Kaspersky Endpoint Security 8 for Smartphone для операционной системы Android.

Защита не поддерживается для операционной системы BlackBerry.

ПРОВЕРКА ПО ТРЕБОВАНИЮ

Проверка по требованию обеспечивает проверку файловой системы мобильных устройств на присутствие вредоносных объектов. Kaspersky Endpoint Security 8 for Smartphone позволяет выполнять полную проверку файловой системы устройства или частичную – то есть проверить только содержимое встроенной памяти устройства или конкретной папки (в том числе и расположенной на карте расширения памяти). Полная проверка может запускаться вручную или автоматически по сформированному расписанию. Частичная проверка может запускаться только вручную пользователем непосредственно из программы, установленной на мобильном устройстве.

Проверка устройства выполняется по следующему алгоритму:

1. Kaspersky Endpoint Security 8 for Smartphone проверяет файлы выбранного типа, заданные в параметрах проверки.

2. Во время проверки Kaspersky Endpoint Security 8 for Smartphone анализирует файл на присутствие вредоносных объектов. Распознавание вредоносных объектов происходит на основании антивирусных баз программы.

3. По результатам анализа программа выполняет действие в зависимости от операционной системы.

   Для операционных систем Symbian и Microsoft Windows Mobile возможны следующие варианты поведения Kaspersky Endpoint Security 8 for Smartphone:

   - Если в файле обнаружен вредоносный код, Kaspersky Endpoint Security 8 for Smartphone блокирует файл, выполняет выбранное действие в соответствии с установленными параметрами и уведомляет пользователя.

     Для операционной системы Android если в результате анализа файла программа обнаруживает вредоносный код, она выполняет выбранное действие в соответствии с установленными параметрами.

   - Если вредоносного кода не обнаружено, файл сразу же становится доступным для работы.

4. Информация о ходе проверки и событиях проверки вносится в журнал событий (для операционных систем Symbian и Microsoft Windows Mobile).

   Отчеты о проверке отсутствуют в Kaspersky Endpoint Security 8 for Smartphone для операционной системы Android.

Проверка по требованию не поддерживается для операционной системы BlackBerry.

Параметры, заданные администратором через систему удаленного управления, используются как при полной, так и при частичной проверке устройства.

Администратор также может настроить автоматический запуск по расписанию полной проверки устройства. Запуск частичной проверки через систему удаленного управления не предусмотрен.

Обновление

Защита и Проверка по требованию работают на основании антивирусных баз, которые содержат описание всех известных в настоящий момент вредоносных программ и способов их обезвреживания, а также описания других нежелательных объектов. Крайне важно поддерживать антивирусные базы в актуальном состоянии. Обновление может запускаться вручную или автоматически по сформированному расписанию. Для обеспечения надежности системы антивирусной защиты следует своевременно обновлять антивирусные базы.

Обновление антивирусных баз программы выполняется по следующему алгоритму:

1. Программа устанавливает соединение с интернетом или использует уже существующее.

2. Антивирусные базы программы, которые установлены на мобильном устройстве, сравниваются с базами, расположенными на заданном сервере обновлений.

3. Kaspersky Endpoint Security 8 for Smartphone выполняет одно из следующих действий:

   - Если на устройстве установлены актуальные базы программы, то обновление будет отменено. Программа уведомляет пользователя об актуальности антивирусных баз.

   - Если установленные базы различаются, то на устройство будет загружен и установлен новый пакет обновлений.

     Когда процесс обновления завершится, соединение автоматически закроется. Если соединение было установлено до начала обновления, то оно продолжит работу.

4. Информация об обновлении фиксируется в журнале событий.

Обновление не поддерживается для операционной системы BlackBerry.

Анти-Вор

Анти-Вор защищает от несанкционированного доступа информацию, хранящуюся на мобильном устройстве.

Анти-Вор включает в себя следующие функции:

- Блокирование (на стр. 19).
- Удаление данных (на стр. 19).
- SIM-Контроль (на стр. 20).
- GPS-Поиск (на стр. 20).

Kaspersky Endpoint Security 8 for Smartphone позволяет пользователю дистанционно запустить функции Анти-Вора путем отправки SMS-команды с другого мобильного устройства. SMS-команда отправляется в виде зашифрованного SMS и также содержит секретный код программы, установленной на получающем команду устройстве. Получение SMS-команды будет незаметным на получающем SMS-команду устройстве. Отправка SMS оплачивается согласно тарифу оператора сотовой связи, который установлен на отправляющем SMS-команду устройстве.

Анти-Вор поддерживается для всех операционных систем.

В ЭТОМ РАЗДЕЛЕ

Блокирование

Функция Блокирование позволяет дистанционно заблокировать устройство и задать текст, который будет отображаться на экране заблокированного устройства.

Удаление данных

Функция Удаление данных позволяет дистанционно удалить с устройства персональные данные пользователя (например, записи в Контактах, сообщения, галерею изображений, календарь, журналы, параметры подключения к интернету), а также информацию с карт памяти и папки, выбранные администратором и пользователем для удаления. Пользователь не сможет восстановить эти данные!

Администратор может определить папки для удаления в политике. Администратор может выбрать папки, расположенные на карте памяти и сохраненные в памяти устройства. Для устройств с Android OS администратор может выбрать только те папки для удаления, которые сохранены на карте памяти. Невозможно выбрать папки для удаления, которые сохранены в памяти устройства.

Пользователь не может отменить удаление папок, заданных администратором, но может дополнительно указать папки для удаления на своем мобильном устройстве через локальный интерфейс программы (см. Руководство пользователя для соответствующей операционной системы). Если администратор не задал папки для удаления, то будут удаляться только папки, заданные пользователем.

SIM-Контроль

Функция SIM-Контроль позволяет получить текущий номер телефона в случае смены SIM-карты, а также блокировать устройство при смене SIM-карты или при включении устройства без нее. Информация о новом номере телефона отправляется в виде сообщения на указанный номер телефона и (или) на адрес электронной почты. Кроме того, SIM-контроль позволяет заблокировать устройство в случае смены SIM-карты или при включении устройства без нее.

GPS-Поиск

Функция GPS-Поиск позволяет определить местоположение устройства. Географические координаты устройства отправляются в виде сообщения на номер телефона, с которого отправлена специальная SMS-команда, а также на заданный адрес электронной почты.

В зависимости от операционной системы алгоритм работы GPS-Поиска следующий:

- Для операционных систем Symbian, Microsoft Windows Mobile и BlackBerry функция работает только с устройствами со встроенным GPS-приемником. Приемник включается автоматически после получения устройством специальной SMS-команды. Если устройство находится в зоне досягаемости спутников, функция GPS-Поиск получает и отправляет координаты устройства. Если в момент запроса спутники недоступны, GPS-Поиск периодически пытается их найти и отправляет результаты поиска устройства.

- Для операционной системы Android, если на устройствах есть встроенный GPS-приемник, он включается автоматически после того, как устройство получает специальную SMS-команду. Если функция GPS-Поиск не может получить координаты устройства с помощью GPS, она определяет примерные координаты устройства по базовым станциям.

Личные контакты

Личные контакты скрывают конфиденциальную информацию на основании сформированного Списка контактов, в котором перечислены конфиденциальные номера. Для конфиденциальных номеров Личные контакты скрывают записи в Контактах, входящие, черновики, переданные SMS и записи в журнале вызовов. Личные контакты блокируют сигнал о получении нового SMS и скрывают его в списке входящих. Личные контакты блокируют входящий вызов с конфиденциального номера и не отображают на экране информацию о его приеме. Звонящий в этом случае получает сигнал «Занято». Чтобы посмотреть поступившие вызовы и SMS за период, когда скрытие конфиденциальной информации было включено, отключите скрытие. При повторном включении скрытия информация не отображается.

Личные контакты не поддерживаются для операционной системы BlackBerry.

Анти-Спам

Анти-Спам предотвращает доставку нежелательных вызовов и сообщений на основе сформированных пользователем «черного» и «белого» списков.

Списки состоят из записей. Запись в каждом списке содержит следующую информацию:

- Номер телефона, информацию с которого Анти-Спам блокирует для «черного» списка и доставляет для «белого» списка.

- Тип событий, которые Анти-Спам блокирует для «черного» списка и доставляет для «белого» списка. Представлены следующие типы информации: вызовы и SMS, только вызовы, только SMS.

- Ключевая фраза, по которой Анти-Спам распознает желательные и нежелательные SMS. Для «черного» списка Анти-Спам блокирует SMS, в которых есть эта фраза, и доставляет SMS, в которых нет этой ключевой фразы. Для «белого» списка Анти-Спам доставляет SMS, в которых есть эта фраза, и блокирует SMS, в которых нет этой фразы.

Анти-Спам фильтрует входящие SMS и вызовы в соответствии с выбранным пользователем режимом. Предусмотрены следующие режимы Анти-Спама:

- **Отключен** – доставляются все входящие вызовы и SMS.
- **«Черный» список** – доставляются вызовы и SMS со всех номеров, кроме номеров из «черного» списка.
- **«Белый» список** – доставляются вызовы и SMS только с номеров, внесенных в «белый» список.
- **Оба списка** – входящие вызовы и SMS с номеров из «белого» списка доставляются, с номеров из «черного» списка блокируются. После разговора или получения SMS с номера, не входящего ни в один из списков, Анти-Спам предложит пользователю внести номер в один из списков.

Согласно режиму, Анти-Спам проверяет каждое входящее SMS или вызов и определяет, является ли SMS или вызов желательным или нежелательным (спамом). Как только Анти-Спам присваивает SMS или вызову статус желательного или нежелательного, проверка завершается.

Информация о заблокированных SMS и вызовах фиксируется в журнале событий.

Анти-Спам поддерживается для всех операционных систем.

СЕТЕВОЙ ЭКРАН

Сетевой экран контролирует сетевые соединения на устройстве в соответствии с выбранным режимом. Предусмотрены следующие режимы Сетевого экрана:

- **Отключено** – разрешение любой сетевой активности.
- **Минимальная защита** – блокирование только входящих соединений. Исходящие соединения разрешены.
- **Максимальная защита** – блокирование всех входящих соединений. Пользователю доступны проверка почты, просмотр веб-сайтов, загрузка файлов. Исходящие соединения могут осуществляться только по портам SSH, HTTP, IMAP, SMTP, POP3.
- **Блокировать все** – блокирование любой сетевой активности, кроме обновления антивирусных баз и подключения к системе удаленного администрирования.

В соответствии с режимом Сетевой экран позволяет устанавливать соединения, которые разрешены, и блокирует соединения, которые запрещены. Информация о заблокированных соединениях фиксируется в журнале событий. Сетевой экран также позволяет настроить уведомления пользователя о заблокированном соединении.

Сетевой экран не поддерживается для операционных систем BlackBerry и Android.

ШИФРОВАНИЕ

Шифрование шифрует информацию в указанных администратором и пользователем папках. Работа функции Шифрование основана на действии одноименной функции, встроенной в операционную систему устройства.

Администратор может определить папки для шифрования в политике. Пользователь не может отменить шифрование папок, заданных администратором, но может дополнительно указать папки для шифрования на своем мобильном устройстве через локальный интерфейс программы (см. Руководство пользователя для соответствующей операционной системы). Если администратор не задал папки для шифрования, то будут шифроваться только папки, заданные пользователем.

Шифрование позволяет зашифровать папки любого типа, кроме системных. Поддерживается шифрование папок, хранящихся в памяти устройства или на карте памяти. Зашифрованная информация доступна пользователю после ввода секретного кода программы, установленного пользователем при ее первом запуске.

Шифрование позволяет задать промежуток времени, по истечении которого включится запрет доступа к зашифрованным папкам и для работы с ними потребуется ввести секретный код программы. Функция активизируется после перехода устройства в режим энергосбережения.

Шифрование не поддерживается для операционных систем BlackBerry и Android.

УПРАВЛЕНИЕ ЛИЦЕНЗИЯМИ

В контексте лицензирования программ «Лаборатории Касперского» важно знать о следующих понятиях:

- лицензионном соглашении;
- лицензии;
- файле ключа;
- активации программы.

Эти понятия неразрывно связаны друг с другом и формируют единую схему лицензирования. Рассмотрим подробнее каждое из понятий.

В ЭТОМ РАЗДЕЛЕ

О ЛИЦЕНЗИОННОМ СОГЛАШЕНИИ

Лицензионное соглашение – это договор между физическим или юридическим лицом, правомерно владеющим экземпляром Kaspersky Endpoint Security, и ЗАО «Лаборатория Касперского». Соглашение входит в состав каждой программы «Лаборатории Касперского». В нем приводится детальная информация о правах и ограничениях на использование Kaspersky Endpoint Security.

В соответствии с лицензионным соглашением, приобретая и устанавливая программу «Лаборатории Касперского», вы получаете бессрочное право на владение ее копией.

«Лаборатория Касперского» также рада предложить вам дополнительные услуги:

- техническую поддержку;
- обновление баз Kaspersky Endpoint Security.

Для их получения вам нужно приобрести лицензию и активировать программу.

О ЛИЦЕНЗИЯХ KASPERSKY ENDPOINT SECURITY 8 FOR SMARTPHONE

Лицензия – это право на использование Kaspersky Endpoint Security 8 for Smartphone на одном или нескольких мобильных устройствах и связанных с ним дополнительных услуг, предоставляемых вам «Лабораторией Касперского» или ее партнерами.

Каждая лицензия характеризуется сроком действия и типом.

Срок действия лицензии – период времени, в течение которого вам предоставляются дополнительные услуги. Объем предоставляемых услуг зависит от типа лицензии.

Предусмотрены следующие типы лицензий:

- *Пробная* – бесплатная лицензия с ограниченным сроком действия, например, 30 дней, предназначенная для ознакомления с Kaspersky Endpoint Security 8 for Smartphone.

  Пробная лицензия может использоваться только один раз и не может быть использована после коммерческой лицензии!

  Она поставляется вместе с пробной версией программы. Используя пробную лицензию, вы не можете обращаться в Службу технической поддержки. По завершении срока ее действия Kaspersky Endpoint Security 8 for Smartphone прекращает выполнять все свои функции. При этом доступны только следующие действия:

  - отключение компонентов Шифрование и Личные контакты;
  - администратор может расшифровать папки, выбранные им для шифрования;
  - пользователь может расшифровать папки, выбранные им для шифрования;
  - просмотр справочной системы программы;
  - синхронизация с системой удаленного управления.

- *Коммерческая* – платная лицензия со сроком действия, например, один год, предоставляемая при покупке Kaspersky Endpoint Security 8 for Smartphone. Эта лицензия распространяется с лицензионным ограничением, например, на количество защищаемых мобильных устройств.

  В период действия коммерческой лицензии доступны все функции программы и дополнительные услуги.

По окончании срока действия коммерческой лицензии Kaspersky Endpoint Security 8 for Smartphone функциональность программы ограничивается. Вы по-прежнему можете использовать компоненты Анти-Спам и Сетевой экран, осуществлять антивирусную проверку мобильного устройства и использовать компоненты защиты, но только на основе антивирусных баз, актуальных на дату окончания срока действия лицензии. Обновление антивирусных баз не производится. Для остальных компонентов доступны только следующие действия:

- отключение компонентов Шифрование, Анти-Вор и Личные контакты;
- администратор может расшифровать папки, выбранные им для шифрования;
- пользователь может расшифровать папки, выбранные им для шифрования;
- просмотр справочной системы программы;
- синхронизация с системой удаленного управления.

Чтобы воспользоваться программой и дополнительными услугами, нужно купить коммерческую лицензию и активировать программу.

Активация программы выполняется посредством установки файла ключа, связанного с лицензией.

О файлах ключей Kaspersky Endpoint Security 8 for Smartphone

Файл ключа – техническое средство, позволяющее установить лицензию и активировать программу, и вместе с тем – ваше право на использование программы и дополнительных услуг.

Файл ключа входит в комплект поставки программы, если вы приобретаете ее у дистрибьюторов «Лаборатории Касперского», или присылается вам по электронной почте, если программа приобретается в интернет-магазине.

В файле ключа содержится следующая информация:

- Срок действия лицензии.
- Тип лицензии (пробная, коммерческая).
- Лицензионные ограничения (например, на какое количество мобильных устройств распространяется лицензия).
- Контакты для обращения в Службу технической поддержки.
- Период действия файла ключа.

Период действия файла ключа – своего рода «срок годности», присваиваемый файлу ключа при его выписке. Это период, по истечении которого файл ключа становится недействительным и, соответственно, теряется возможность установки связанной с ним лицензии.

Рассмотрим на примере, как связаны период действия ключа и срок действия лицензии.

Пример:

Срок действия лицензии: 300 дней.

Дата выписки файла ключа: 01.09.2010.

Период действия файла ключа: 300 дней.

Дата установки файла ключа: 10.09.2010, то есть на 9 дней позже даты его выписки.

Результат:

Рассчитанный срок действия лицензии: 300 дней - 9 дней = 291 день.

Активация программы

После установки на мобильное устройство программа Kaspersky Endpoint Security 8 for Smartphone работает три дня без активации в режиме полной функциональности.

Если по истечении трех дней активация программы не будет выполнена, то программа автоматически переключится в режим работы с ограниченной функциональностью. В этом режиме работы большинство компонентов Kaspersky Endpoint Security 8 for Smartphone отключены (см. раздел «О лицензиях Kaspersky Endpoint Security 8 for Smartphone» на стр. 23).

Активация программы выполняется посредством установки лицензии на мобильное устройство. Лицензия доставляется на устройство вместе с политикой, сформированной в системе удаленного управления. В течение трех дней после установки программы устройство каждые шесть часов автоматически выходит на связь с системой удаленного управления. В течение этого периода администратор должен добавить лицензию в состав политики. Как только политика будет передана на устройство, программа, установленная на устройстве, будет активирована.

См. также

РАЗВЕРТЫВАНИЕ ПРОГРАММЫ ЧЕРЕЗ KASPERSKY ADMINISTRATION KIT

В этом разделе рассмотрен процесс развертывания Kaspersky Endpoint Security 8 for Smartphone через Kaspersky Administration Kit.

В ЭТОМ РАЗДЕЛЕ

КОНЦЕПЦИЯ УПРАВЛЕНИЯ ПРОГРАММОЙ ЧЕРЕЗ KASPERSKY ADMINISTRATION KIT

Kaspersky Endpoint Security 8 for Smartphone поддерживает управление через систему удаленного централизованного управления программами «Лаборатории Касперского» Kaspersky Administration Kit. Управление мобильными устройствами и установленной на них программой Kaspersky Endpoint Security 8 for Smartphone осуществляется точно так же, как управление клиентскими компьютерами и установленными на них программами «Лаборатории Касперского» (см. Руководство администратора для Kaspersky Administration Kit).

Администратор создает группы, в состав которых добавляет мобильные устройства, и формирует политику для Kaspersky Endpoint Security 8 for Smartphone. Политика – это набор параметров работы программы. При помощи политик могут быть установлены одинаковые значения параметров работы программы для всех мобильных устройств, входящих в состав группы. Подробно о политиках и группах администрирования читайте в Руководстве администратора Kaspersky Administration Kit.

Особенностью Kaspersky Endpoint Security 8 for Smartphone является то, что для этой программы не предусмотрено создание задач. Все параметры работы программы, включая лицензию, расписание обновления баз программы, расписание проверки устройства, определяются через политику (см. раздел «Работа с политиками» на стр. 51) или локальные параметры программы (см. раздел «Настройка локальных параметров программы» на стр. 66).

Если в сети предприятия планируется установка и использование программы Kaspersky Endpoint Security 8 for Smartphone, администратор должен учесть это на этапе проектирования структуры групп администрирования и при установке программных компонентов Kaspersky Administration Kit.

При установке Сервера администрирования должен быть установлен компонент, обеспечивающий управление защитой мобильных устройств через Kaspersky Administration Kit (см. раздел «Установка Сервера администрирования» на стр. 31). При установке этого компонента создается *сертификат Сервера администрирования для мобильных устройств*. Он используется для аутентификации мобильных устройств при обмене данными с Сервером администрирования. Без сертификата для мобильных устройств установить соединение между Сервером администрирования и мобильными устройствами невозможно.

Взаимодействие между мобильными устройствами и Сервером администрирования осуществляется при синхронизации устройств с Сервером администрирования. Эту функциональность обеспечивает программа Kaspersky Endpoint Security 8 for Smartphone, поэтому Агент администрирования на мобильные устройства устанавливать не требуется.

Обмен данными между мобильными устройствами и Сервером администрирования выполняется по сети Интернет. Входящий и исходящий трафик оплачивается пользователями мобильных устройств по тарифам оператора мобильной связи. Средний объем передаваемых при одной синхронизации данных составляет 20-40 КБ. Объем данных зависит от количества передаваемых отчетов. Чем реже выполняется синхронизация, тем больше отчетов передается на Сервер администрирования.

Для управления защитой мобильных устройств рекомендуется в узле **Управляемые компьютеры** создать отдельную группу или группы (по количеству операционных систем, установленных на устройствах), а в случае установки программы через рабочие станции пользователей отдельную группу рекомендуется создать и для этих компьютеров (см. раздел «Создание групп» на стр. 34).

Схемы развертывания через Kaspersky Administration Kit

Схема развертывания Kaspersky Endpoint Security 8 for Smartphone зависит от того, какой способ установки программы на мобильные устройства пользователей выберет администратор. Установка программы может быть выполнена следующими способами:

- через рабочие станции, к которым пользователи подключают мобильные устройства (см. раздел «Установка программы через рабочую станцию» на стр. 34);
- через рассылку пользователям по электронной почте сообщения с дистрибутивом программы или с указанием по его скачиванию (см. раздел «Установка программы через рассылку по электронной почте» на стр. 49).

Администратор обеспечивает подготовку дистрибутива программы для установки на мобильные устройства пользователей. Копирование дистрибутива на мобильные устройства и установку программы на мобильных устройствах пользователи выполняют самостоятельно. После установки программы администратор должен включить мобильные устройства в состав управляемых компьютеров и создать политику, чтобы передать на мобильные устройства лицензию и параметры работы программы.

Таким образом, при управлении программой через Kaspersky Administration Kit администратор может использовать следующие схемы развертывания: развертывание программы через рабочие станции (см. раздел «Развертывание программы через рабочую станцию» на стр. 29) и развертывание программы через рассылку по электронной почте (см. раздел «Схема развертывания программы через рассылку по электронной почте» на стр. 29).

Перед развертыванием программы администратор должен убедиться, что установленная версия Kaspersky Administration Kit поддерживает управление защитой мобильных устройств.

В ЭТОМ РАЗДЕЛЕ

РАЗВЕРТЫВАНИЕ ПРОГРАММЫ ЧЕРЕЗ РАБОЧУЮ СТАНЦИЮ

Развертывание программы через рабочую станцию используется в том случае, когда пользователи подключают мобильные устройства к рабочим компьютерам, и состоит из следующих этапов:

1. Настройка управления мобильными устройствами через Kaspersky Administration Kit. На этом этапе обеспечивается возможность подключения мобильных устройств к Серверу администрирования (см. раздел «Подготовка к развертыванию программы через Kaspersky Administration Kit» на стр. 30).

2. Создание групп администрирования для размещения мобильных устройств и рабочих станций, через которые на мобильные устройства будет доставляться дистрибутив программы Kaspersky Endpoint Security 8 for Smartphone.

3. Создание инсталляционного пакета для задачи удаленной установки Kaspersky Endpoint Security 8 for Smartphone.

4. Настройка параметров инсталляционного пакета для задачи удаленной установки Kaspersky Endpoint Security 8 for Smartphone.

5. Создание задачи удаленной установки, с помощью которой на рабочие станции пользователей доставляется дистрибутив программы Kaspersky Endpoint Security 8 for Smartphone и устанавливается утилита доставки дистрибутива на мобильные устройства.

6. Доставка дистрибутива программы на мобильное устройство. На этом этапе пользователь при помощи утилиты kmlisten.exe копирует дистрибутив программы на мобильное устройство.

7. Установка программы на мобильном устройстве. На этом этапе пользователь выполняет установку программы на мобильном устройстве.

8. Создание политики для управления параметрами Kaspersky Endpoint Security 8 for Smartphone.

СХЕМА РАЗВЕРТЫВАНИЯ ПРОГРАММЫ ЧЕРЕЗ РАССЫЛКУ ПО ЭЛЕКТРОННОЙ ПОЧТЕ

Развертывание программы через рассылку по электронной почте используется в том случае, когда по каким-либо причинам установка программы через рабочую станцию невозможна или неудобна. Например, на рабочей станции пользователя установлена Mac OS. Схема состоит из следующих этапов:

1. Настройка управления мобильными устройствами через Kaspersky Administration Kit.

2. Размещение дистрибутива программы на FTP- / HTTP-сервере. На этом этапе администратор размещает дистрибутив программы на FTP- / HTTP-сервере и настраивает доступ к нему через интернет. В дальнейшем, при формировании письма, которое будет отправлено пользователям мобильных устройств, администратор сможет указать ссылку на этот дистрибутив. Если администратор планирует включить дистрибутив программы в состав письма как вложенный файл, то этот этап пропускается.

3. Создание групп администрирования для размещения мобильных устройств и рабочих станций, через которые на мобильные устройства будет доставляться дистрибутив программы Kaspersky Endpoint Security 8 for Smartphone.

4. Формирование и отправка письма с дистрибутивом программы пользователям мобильных устройств.

5. Скачивание дистрибутива программы на мобильное устройство. На этом этапе пользователь загружает на устройство дистрибутив программы, приложенный к письму или размещенный администратором на FTP- / HTTP-сервере.

6. Установка программы на мобильном устройстве.

7. Создание политики для управления параметрами Kaspersky Endpoint Security 8 for Smartphone.

8. Перемещение устройства в группу администрирования.

9. Активация лицензии программы на мобильных устройствах пользователей.

10. Настройка локальных параметров программы.

Подготовка к развертыванию программы через Kaspersky Administration Kit

Перед тем как приступать к развертыванию программы Kaspersky Endpoint Security 8 for Smartphone, администратор должен настроить управление мобильными устройствами через Kaspersky Administration Kit. Для этого следует выполнить следующие действия:

1. Установить или убедиться, что в сети установлены компоненты Kaspersky Administration Kit: Сервер администрирования и Консоль управления (см. Руководство по развертыванию Kaspersky Administration Kit).

2. Убедиться, что установленные компоненты соответствуют программным требованиям для установки программы Kaspersky Endpoint Security 8 for Smartphone.

   При установке Сервера администрирования должен быть установлен компонент, обеспечивающий управление защитой мобильных устройств через Kaspersky Administration Kit (см. раздел «Установка Сервера администрирования» на стр. 31). Если этот компонент не был установлен или версия Сервера администрирования не соответствует требованиям для установки Kaspersky Endpoint Security 8 for Smartphone, то администратору следует удалить старую версию компонента и установить ту версию, которая указана в программных требованиях, предварительно выполнив резервное копирование данных Сервера администрирования.

3. Настроить поддержку мобильных устройств в параметрах Сервера администрирования (см. раздел «Настройка параметров Сервера администрирования» на стр. 32).

4. Установить на рабочем месте администратора плагин управления программой Kaspersky Endpoint Security 8 for Smartphone.

В ЭТОМ РАЗДЕЛЕ

УСТАНОВКА СЕРВЕРА АДМИНИСТРИРОВАНИЯ

Установка Сервера администрирования описана в Руководстве по развертыванию Kaspersky Administration Kit. Для обеспечения управления защитой мобильных устройств через Kaspersky Administration Kit на шаге **Выбор компонентов** обязательно должен быть установлен флажок **Поддержка мобильных устройств** (см. рисунок ниже).

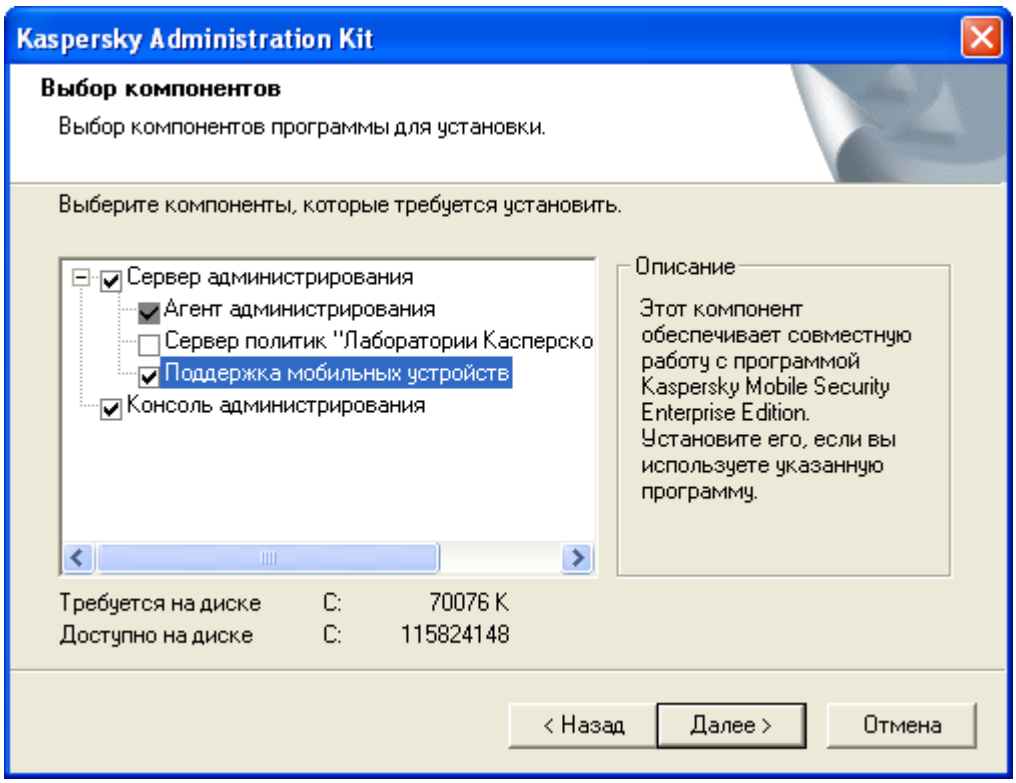


Рисунок 1. Установка компонентов Kaspersky Administration Kit. Выбор компонентов

При установке компонента Поддержка мобильных устройств создается *сертификат Сервера администрирования для мобильных устройств*. Он используется для аутентификации мобильных устройств при обмене данными с Сервером администрирования. Обмен информацией производится с использованием SSL-протокола (Secure Socket Layer). Без сертификата для мобильных устройств установить соединение между Сервером администрирования и мобильными устройствами невозможно.

Сертификат для мобильных устройств хранится в папке установки программы Kaspersky Administration Kit во вложенной папке Cert. При первой синхронизации мобильного устройства с Сервером администрирования копия сертификата доставляется на устройство и сохраняется на нем в специальной папке.

Если пользователь переименует или удалит с устройства сертификат для мобильных устройств, то при очередной синхронизации Сервер администрирования автоматически отправит на устройство копию сертификата.

Обновление компонента Сервер администрирования

Если при установке Сервера администрирования не был установлен флажок **Поддержка мобильных устройств** или установлена устаревшая версия Kaspersky Administration Kit, в которой не поддерживается работа с Kaspersky Endpoint Security 8 for Smartphone, то следует обновить установленную версию компонента Сервер администрирования.

- *Чтобы обновить установленную версию компонента Сервер администрирования, выполните следующие действия:*

1. Выполните резервное копирование данных Сервера администрирования (см. Справочное руководство Kaspersky Administration Kit).

2. Установите версию Сервера администрирования, которая указана в программных требованиях для установки программы Kaspersky Endpoint Security 8 for Smartphone (см. раздел «Аппаратные и программные требования» на стр. 14).

   Для обеспечения управления защитой мобильных устройств через Kaspersky Administration Kit на шаге **Выбор компонентов** обязательно должен быть установлен флажок **Поддержка мобильных устройств**.

3. Восстановите данные Сервера администрирования из резервной копии (см. Справочное руководство Kaspersky Administration Kit).

Настройка параметров Сервера администрирования

Для обеспечения синхронизации мобильных устройств с Сервером администрирования перед установкой Kaspersky Endpoint Security 8 for Smartphone следует настроить в свойствах Сервера администрирования параметры подключения мобильных устройств.

- *Чтобы настроить в свойствах Сервера администрирования параметры подключения мобильных устройств, выполните следующие действия:*

1. Выберите в дереве консоли Сервер администрирования.

2. Откройте контекстное меню и выберите пункт **Свойства**.

3. Откройте закладку **Параметры** в открывшемся окне свойств Сервера администрирования.

4. Установите флажок **Открывать порт для мобильных устройств** в блоке **Параметры подключения к Серверу администрирования**. В поле **Порт для мобильных устройств** укажите порт, по которому Сервер администрирования будет ожидать подключение мобильных устройств. По умолчанию используется порт 13292 (см. рисунок ниже). Если флажок не установлен или порт указан неверно, устройства не смогут подключиться к серверу и передать или получить информацию.

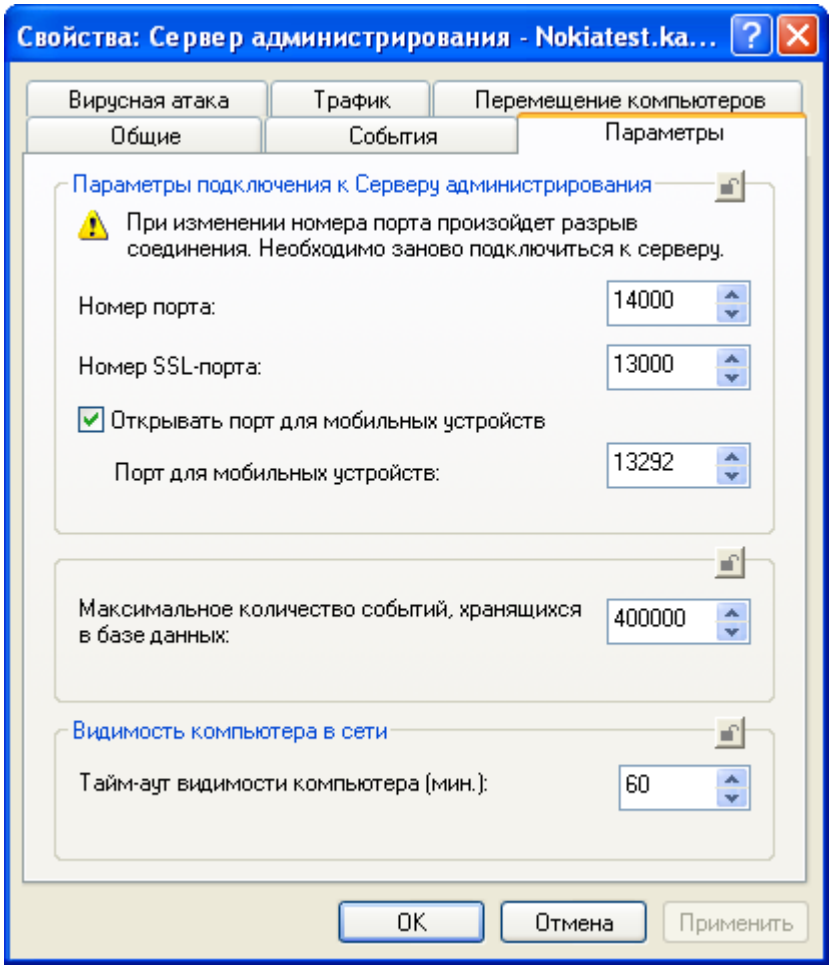


Рисунок 2. Настройка параметров подключения мобильных устройств к Серверу администрирования

УСТАНОВКА ПЛАГИНА УПРАВЛЕНИЯ KASPERSKY ENDPOINT SECURITY 8 FOR SMARTPHONE

Для получения доступа к интерфейсу управления программой при помощи Kaspersky Administration Kit на рабочее место администратора должен быть установлен плагин управления программой Kaspersky Endpoint Security 8 for Smartphone.

- *Чтобы установить плагин управления программой Kaspersky Endpoint Security 8 for Smartphone,*

  скопируйте из дистрибутива программы установочный файл плагина и запустите его на рабочем месте администратора.

  Убедиться, что плагин установлен, вы можете, просмотрев список плагинов в свойствах Сервера администрирования. Подробнее см. в Справочном руководстве Kaspersky Administration Kit.

Размещение дистрибутива программы на FTP- / HTTP-сервере

Если для установки программы была выбрана установка через рассылку по электронной почте (см. раздел «Установка программы через рассылку по электронной почте» на стр. 49), то вы можете разместить на FTP- / HTTP-сервере установочный файл, который будет использоваться при установке программы на мобильные устройства. К папке, в которую будет помещен установочный файл программы на FTP- / HTTP-сервере, должен быть настроен доступ через интернет. Если на мобильных устройствах пользователей установлены разные операционные системы, то вы можете добавить в папку несколько файлов, для каждой операционной системы.

Далее, при формировании письма с дистрибутивом программы для пользователей мобильных устройств, в теле письма следует указать ссылку на установочный файл. С помощью этой ссылки пользователь сможет загрузить установочный файл на свое мобильное устройство и выполнить установку программы (см. раздел «Установка программы через рассылку по электронной почте» на стр. 49).

Создание групп

Управление программами, установленными на мобильных устройствах, выполняется через применение к этим устройствам групповых политик. Поэтому перед тем как устанавливать на мобильные устройства программу, вам следует создать для этих устройств отдельную группу администрирования в узле **Управляемые компьютеры**. После завершения установки все устройства, на которые была установлена программа, следует переместить в эту группу (см. раздел «Перемещение устройств в группу Управляемые компьютеры» на стр. 62).

Если для установки Kaspersky Endpoint Security 8 for Smartphone была выбрана установка программы на мобильные устройства через рабочую станцию, то вы можете создать на Сервере администрирования отдельную группу для рабочих станций, к которым пользователи подключают мобильные устройства. Впоследствии вы сможете создать для этой группы групповую задачу для удаленной установки программы Kaspersky Endpoint Security 8 for Smartphone и с помощью этой задачи установить программу сразу на все рабочие станции, входящие в состав группы.

Подробно о создании групп читайте в Руководстве администратора Kaspersky Administration Kit.

Установка программы через рабочую станцию

Для установки Kaspersky Endpoint Security 8 for Smartphone через рабочую станцию следует сформировать инсталляционный пакет и настроить его параметры, создать и запустить задачу удаленной установки для тех рабочих станций, к которым подключаются мобильные устройства пользователей. Для создания задачи администратор может воспользоваться любым из предусмотренных в Kaspersky Administration Kit способов:

- создать групповую задачу удаленной установки, если рабочие станции входят в состав группы;
- создать задачу для набора компьютеров, если рабочие станции входят в состав разных групп или находятся в группе **Нераспределенные компьютеры**;
- воспользоваться мастером удаленной установки.

В результате выполнения задачи удаленной установки на рабочие станции пользователей доставляется инсталляционный пакет с дистрибутивом программы Kaspersky Endpoint Security 8 for Smartphone, а также устанавливается и автоматически запускается *утилита доставки дистрибутива программы на мобильные устройства kmlisten.exe*. Утилита отслеживает подключение мобильных устройств к компьютеру. Как только пользователь подключает к рабочей станции устройство, удовлетворяющее системным требованиям для установки Kaspersky Endpoint Security 8 for Smartphone, утилита выводит на экран сообщение с предложением установить программу на подключенное мобильное устройство. В случае если пользователь соглашается с установкой, утилита загружает дистрибутив программы на мобильное устройство. По окончании загрузки на устройстве запускается мастер установки программы. Следуя указаниям мастера, пользователь самостоятельно выполняет установку Kaspersky Endpoint Security 8 for Smartphone на своем устройстве.

В ЭТОМ РАЗДЕЛЕ

СОЗДАНИЕ ИНСТАЛЛЯЦИОННОГО ПАКЕТА

Инсталляционный пакет Kaspersky Endpoint Security 8 for Smartphone представляет собой самораспаковывающийся архив KES8_forAdminKit_ru.exe, в состав которого входят файлы, необходимые для установки программы на мобильных устройствах:

- endpoint_8_0_x_xx_ru.cab – установочный файл программы для операционной системы Windows Mobile;
- endpoint8_mobile_8_x_xx_eu4_signed.sis – установочный файл программы для операционной системы Symbian;
- Endpoint8_Mobile_8_x_xx_release.zip – установочный файл программы для операционной системы BlackBerry;
- Endpoint8_8_x_xx_release.apk – установочный файл программы для операционной системы Android;
- installer.ini – конфигурационный файл с параметрами подключения к Серверу администрирования;
- kmlisten.ini – конфигурационный файл с параметрами для утилиты доставки инсталляционного пакета;
- kmlisten.kpd – файл с описанием программы;
- AdbWinUsbApi.dll, AdbWinApi.dll, adb.exe – набор файлов, необходимый для установки программы на устройства с операционной системой Android;
- kmlisten.exe – утилита доставки дистрибутива программы на мобильное устройство через рабочую станцию.

Чтобы сформировать инсталляционный пакет для установки Kaspersky Endpoint Security 8 for Smartphone, выполните следующие действия:

1. Подключитесь к Серверу администрирования.
2. Выберите в дереве консоли в узле **Хранилища** папку **Инсталляционные пакеты**.
3. Откройте контекстное меню и выберите пункт **Создать** → **Инсталляционный пакет** или воспользуйтесь аналогичным пунктом в меню **Действие**. В результате запускается мастер, следуйте его указаниям.
4. Укажите имя инсталляционного пакета.
5. Укажите программу для установки (см. рисунок ниже).

   В раскрывающемся списке выберите элемент **Создать инсталляционный пакет для программы «Лаборатории Касперского»**.

При помощи кнопки **Выбрать** откройте папку с дистрибутивом программы и выберите самораспаковывающийся архив KES8_forAdminKit_ru.exe. Если архив был распакован ранее, то вы можете выбрать входящий в состав архива файл с описанием программы kmlisten.kpd. В результате автоматически заполняются поля с именем программы и номером версии.

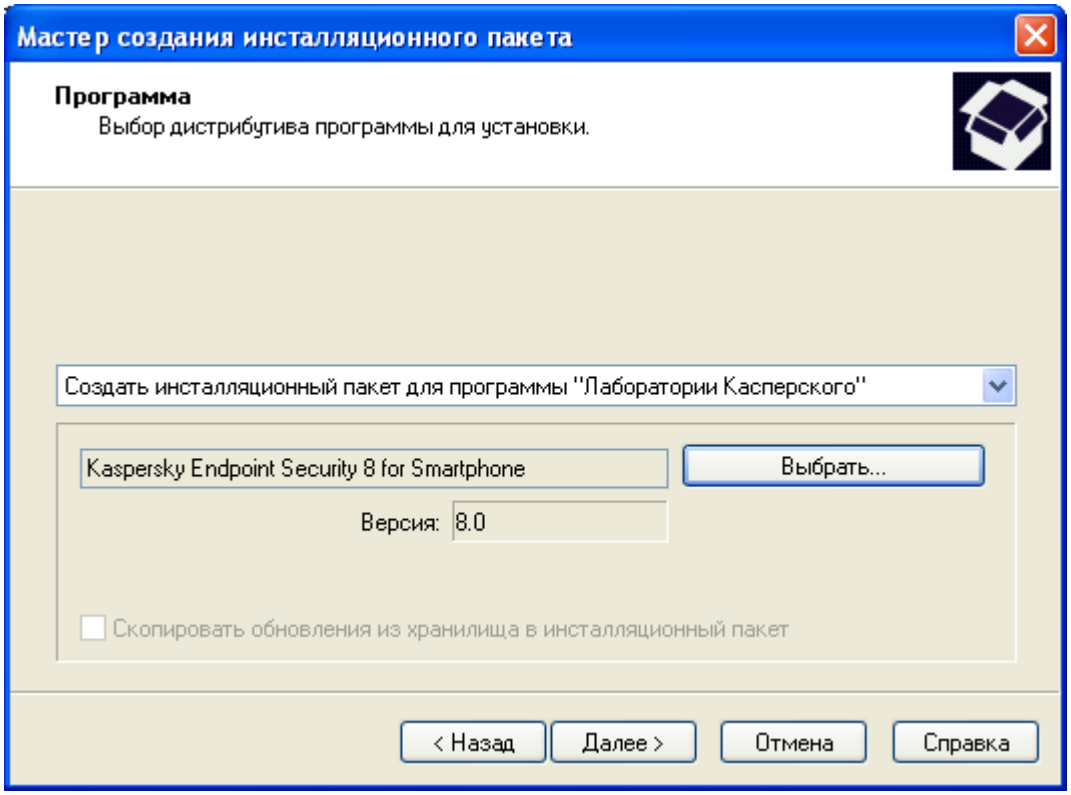


Рисунок 3. Создание инсталляционного пакета. Выбор программы для установки

6. На этом шаге будет выполнена загрузка инсталляционного пакета на Сервер администрирования в папку общего доступа.

После завершения работы мастера сформированный инсталляционный пакет будет добавлен в состав узла **Инсталляционные пакеты** и представлен в панели результатов.

Прежде чем использовать созданный инсталляционный пакет для установки программы, обязательно настройте параметры инсталляционного пакета (см. раздел «Настройка параметров инсталляционного пакета» на стр. 36).

Настройка параметров инсталляционного пакета

Чтобы настроить параметры инсталляционного пакета, выполните следующие действия:

1. Подключитесь к Серверу администрирования.
2. Выберите в дереве консоли в узле **Хранилища** папку **Инсталляционные пакеты**.
3. Выберите в панели результатов созданный инсталляционный пакет, параметры которого вы хотите настроить.
4. Откройте контекстное меню и выберите пункт **Свойства**.

5. На закладке **Параметры** укажите параметры подключения мобильных устройств к Серверу администрирования и имя группы, в которую будут автоматически добавлены мобильные устройства после первой синхронизации с Сервером администрирования (см. рисунок ниже). Для этого выполните следующие действия:

   - В блоке **Подключение к Серверу администрирования** в поле **Адрес сервера** укажите адрес Сервера администрирования в том формате, в каком он указан в свойствах Сервера администрирования на закладке **Общие** в поле **Адрес**. То есть если в свойствах Сервера администрирования указан IP-адрес, то и в поле **Адрес сервера** введите тот же IP-адрес. Если в свойствах Сервера администрирования указано DNS-имя, то в поле **Адрес сервера** введите то же DNS-имя. В поле **Номер SSL-порта** укажите номер порта, открытый на Сервере администрирования для подключения мобильных устройств. По умолчанию используется порт 13292.

   - В блоке **Размещение компьютеров по группам** в поле **Имя группы** введите имя группы, в которую будут добавлены мобильные устройства после первой синхронизации с Сервером администрирования (по умолчанию KES8). Указанная группа будет создана автоматически в папке **Нераспределенные компьютеры**. В блоке **Действия при установке** установите флажок **Запрашивать адрес эл. почты**, чтобы при первом запуске после указания секретного кода программа запрашивала у пользователя его адрес электронной корпоративной почты. Адрес электронной почты пользователя используется для формирования имени мобильных устройств при добавлении их в группу администрирования. Имя мобильного устройства пользователя формируется по следующему правилу:

     - Для мобильных устройств с операционной системой Microsoft Windows Mobile:

       ```
       <адрес электронной_почты пользователя (модель мобильного устройства – IMEI)>
       ```

     - Для мобильных устройств с операционной системой Symbian:

       ```
       <адрес электронной почты пользователя (модель мобильного устройства – IMEI)>
       ```

     - Для мобильных устройств с операционной системой BlackBerry:

       ```
       <адрес электронной почты пользователя (модель мобильного устройства – device pin)>
       ```

- Для мобильных устройств с операционной системой Android:

  `<адрес электронной почты пользователя (модель мобильного устройства – device ID)>`

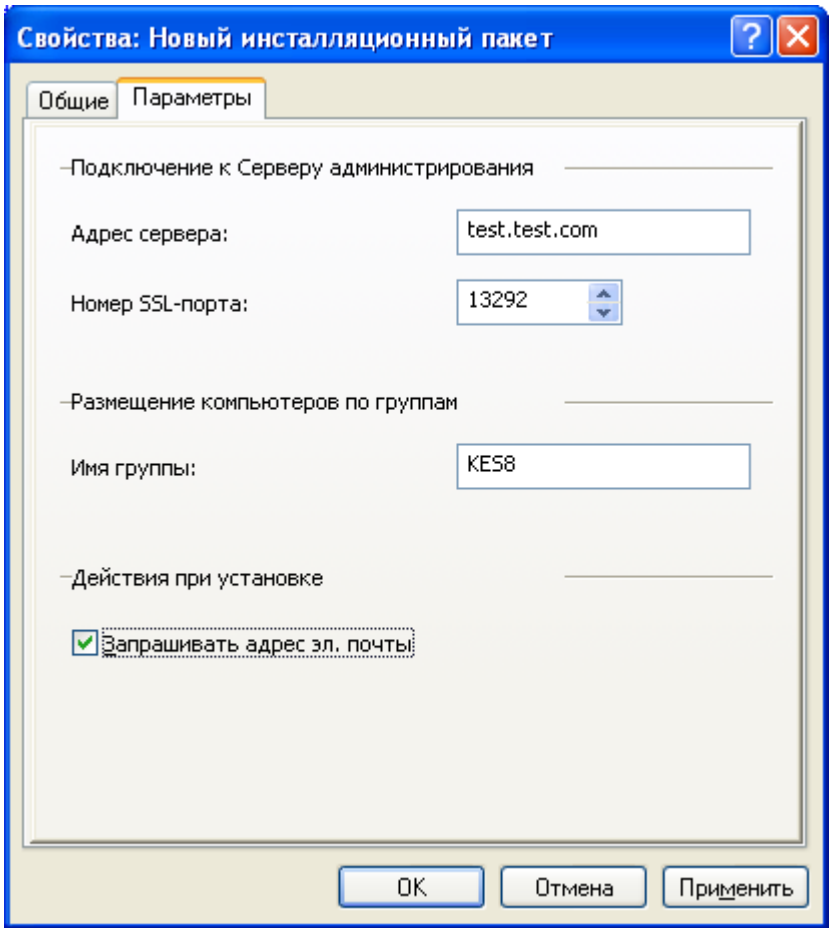


Рисунок 4. Настройка параметров инсталляционного пакета

Создание задачи удаленной установки

Создание задачи удаленной установки выполняется с помощью *мастера создания задачи удаленной установки* или *мастера удаленной установки*. В зависимости от того, какой способ установки был выбран, последовательность шагов мастера и настраиваемые параметры могут отличаться. Обратите внимание на настройку параметров на следующих шагах:

1. Выбор типа задачи. На этом шаге вам будет предложено указать программу, для которой создается задача, и тип задачи. Для установки Kaspersky Endpoint Security 8 for Smartphone создается задача для программы Kaspersky Administration Kit, тип задачи – **Удаленная установка программы**.

2. Выбор инсталляционного пакета. На этом шаге вам будет предложено выбрать инсталляционный пакет, который содержит дистрибутив программы Kaspersky Endpoint Security 8 for Smartphone. Вы можете выбрать уже сформированный инсталляционный пакет для Kaspersky Endpoint Security 8 for Smartphone либо создать инсталляционный пакет непосредственно на этом шаге. В случае создания инсталляционного пакета следует указать самораспаковывающийся архив KES8_forAdminKit_ru.exe. Если архив был распакован ранее, то вы можете указать входящий в состав архива файл с описанием программы kmlisten.kpd (см. раздел «Создание инсталляционного пакета» на стр. 35).

3. Выбор метода установки. Удаленная установка программ на рабочие станции в Kaspersky Administration Kit осуществляется одним из двух методов: методом форсированной установки или методом установки с помощью сценария входа. Метод форсированной установки позволяет провести удаленную установку программного обеспечения на конкретные рабочие станции. Метод установки с помощью сценария входа позволяет закрепить запуск задачи удаленной установки за конкретной учетной записью пользователя (нескольких пользователей).

   Для мастера удаленной установки и мастера создания групповой задачи этот шаг отсутствует, поскольку в этом случае выполняется установка на конкретные рабочие станции и используется метод форсированной установки. Для установки программы Kaspersky Endpoint Security 8 for Smartphone с помощью задачи для набора компьютеров администратор может воспользоваться любым методом.

   Подробно о методах удаленной установки программ см. в Справочном руководстве Kaspersky Administration Kit.

4. Выбор компьютеров для установки. На этом шаге вам будет предложено сформировать список рабочих станций, через которые программа будет устанавливаться на мобильные устройства. Вы можете выбрать один из следующих вариантов:

   - **Установить на группу управляемых компьютеров**. Используйте этот вариант, если на этапе подготовки к установке программы вы создали группу администрирования в узле **Управляемые компьютеры** и переместили в нее все компьютеры, к которым подключаются мобильные устройства (см. раздел «Создание групп» на стр. 34).

   - **Выбрать компьютеры для установки**. Выберите этот вариант, если группа не создавалась. На следующем шаге мастер предложит вам сформировать список компьютеров для установки программы.

5. Выбор способа загрузки инсталляционного пакета. На этом шаге вам будет предложено настроить параметры доставки инсталляционного пакета на рабочие станции. Доставка инсталляционного пакета на рабочие станции может быть выполнена двумя способами:

   - **С помощью Агента администрирования**. Выберите этот способ, если на рабочих станциях, через которые устанавливается Kaspersky Endpoint Security 8 for Smartphone, Агент администрирования установлен и подключен к текущему Серверу администрирования.

     Если Агент администрирования не установлен, но вы планируете его установить, вы можете воспользоваться совместной установкой, предлагаемой на следующем шаге мастера.

   - **Средствами Microsoft Windows из папки общего доступа**. Выберите этот способ, если Агент администрирования на рабочих станциях не установлен или подключен к другому Серверу администрирования. В этом случае передача необходимых для установки программы файлов осуществляется средствами Windows через папки общего доступа.

6. Выбор дополнительного пакета для установки. На этом шаге вам будет предложено установить Агент администрирования на рабочие станции. Воспользуйтесь совместной установкой, если на предыдущем шаге был выбран способ загрузки инсталляционного пакета **С помощью Агента администрирования**, но Агент администрирования на рабочих станциях пока не установлен. В этом случае на рабочие станции сначала устанавливается Агент администрирования, после этого с помощью Агента администрирования доставляется инсталляционный пакет программы.

   Совместная установка не требуется, если доставка дистрибутива на рабочие станции выполняется средствами Microsoft Windows или версия Агента администрирования, удовлетворяющая системным требованиям для установки Kaspersky Endpoint Security 8 for Smartphone, уже установлена.

   Создание задач и работа мастера установки подробно описаны в Руководстве по внедрению Kaspersky Administration Kit. Приведем описание создания групповой задачи удаленной установки.

Чтобы создать групповую задачу удаленной установки Kaspersky Endpoint Security 8 for Smartphone, выполните следующие действия:

1. Подключитесь к Серверу администрирования.
2. Выберите в дереве консоли группу, для которой вы будете создавать задачу.
3. Выберите входящую в ее состав папку **Групповые задачи**.
4. Откройте контекстное меню и выберите пункт **Создать** → **Задачу** или воспользуйтесь ссылкой **Создать новую задачу** в панели задач. В результате запускается мастер. Следуйте его указаниям.
5. Определите имя задачи. Если вы зададите имя уже существующей в данной группе задачи, к нему автоматически будет добавлено окончание «_1».
6. Выберите тип задачи **Удаленная установка программы** для программы **Kaspersky Administration Kit** (см. рисунок ниже).

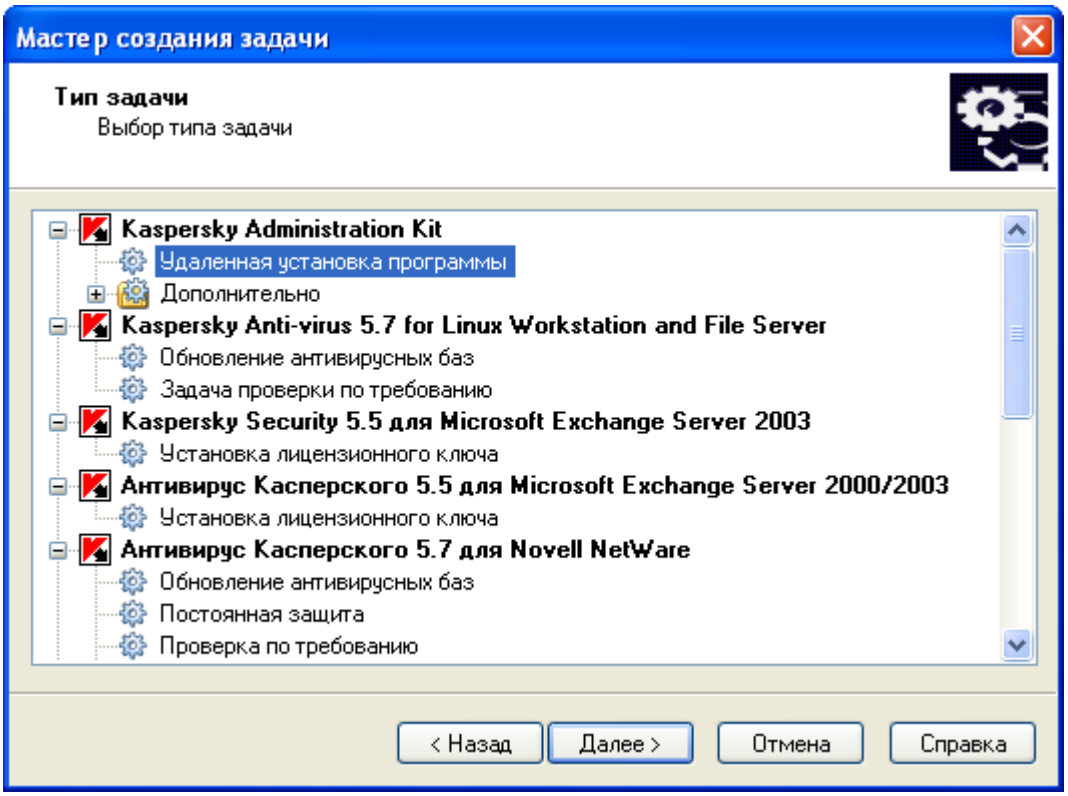


Рисунок 5. Создание задачи. Выбор программы и типа задачи

7. Выберите в списке инсталляционный пакет, сформированный вами ранее для установки программы Kaspersky Endpoint Security 8 for Smartphone, либо создайте новый инсталляционный пакет при помощи кнопки **Новый** (см. рисунок ниже).

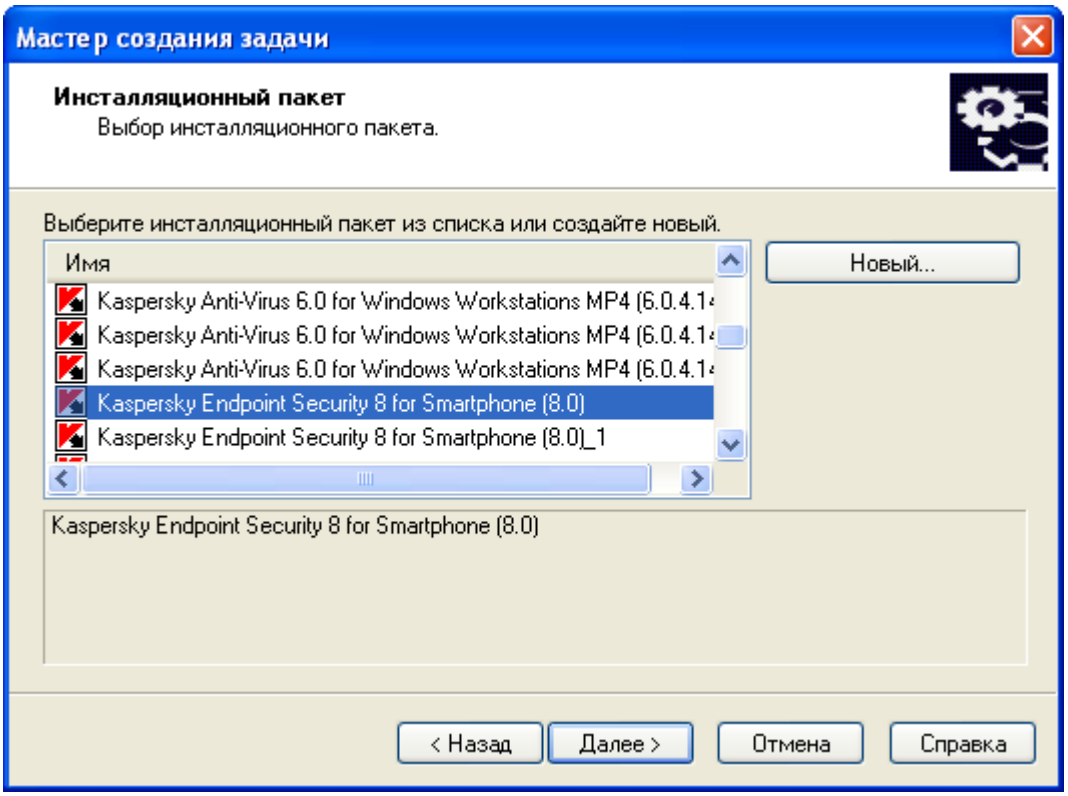


Рисунок 6. Создание задачи. Выбор инсталляционного пакета

8. Выберите способ загрузки инсталляционного пакета (см. рисунок ниже). Для этого установите или снимите следующие флажки:

   - **С помощью Агента администрирования**. В этом случае доставку файлов на рабочие станции осуществляет установленный на каждой из них Агент администрирования.

- **Средствами Microsoft Windows из папки общего доступа**. В этом случае передача необходимых для установки программы файлов на рабочие станции осуществляется средствами Windows через папки общего доступа.

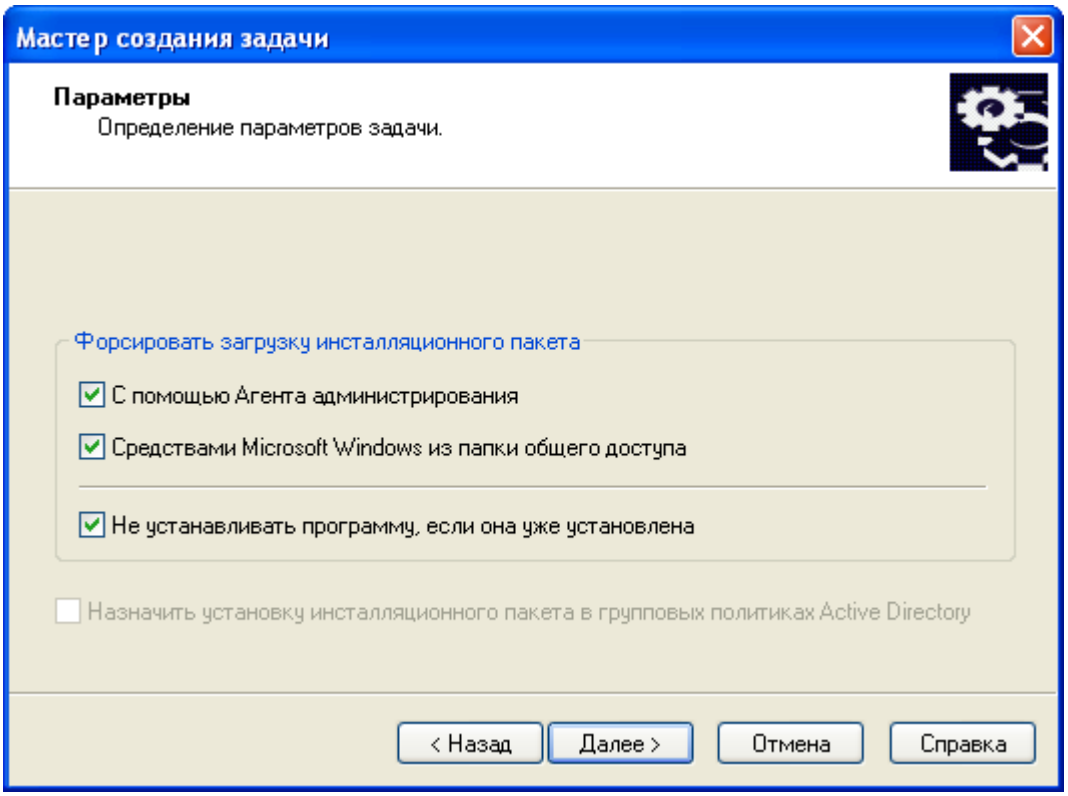


Рисунок 7. Создание задачи. Настройка параметров загрузки инсталляционного пакета

9. Установите флажок **Установить Агент администрирования совместно с данной программой**, если на предыдущем шаге вы выбрали загрузку инсталляционного пакета **С помощью Агента администрирования**, но этот компонент на рабочих станциях не установлен либо установленная версия несовместима с версией Сервера администрирования (см. рисунок ниже). В этом случае на рабочую станцию сначала устанавливается Агент администрирования, а потом с помощью Агента администрирования на рабочую станцию доставляется инсталляционный пакет программы Kaspersky Endpoint Security 8 for Smartphone.

Если на предыдущем шаге вы выбрали загрузку инсталляционного пакета **Средствами Microsoft Windows из папки общего доступа**, то снимите флажок **Установить Агент администрирования совместно с данной программой**. В этом случае на рабочую станцию Агент администрирования установлен не будет.

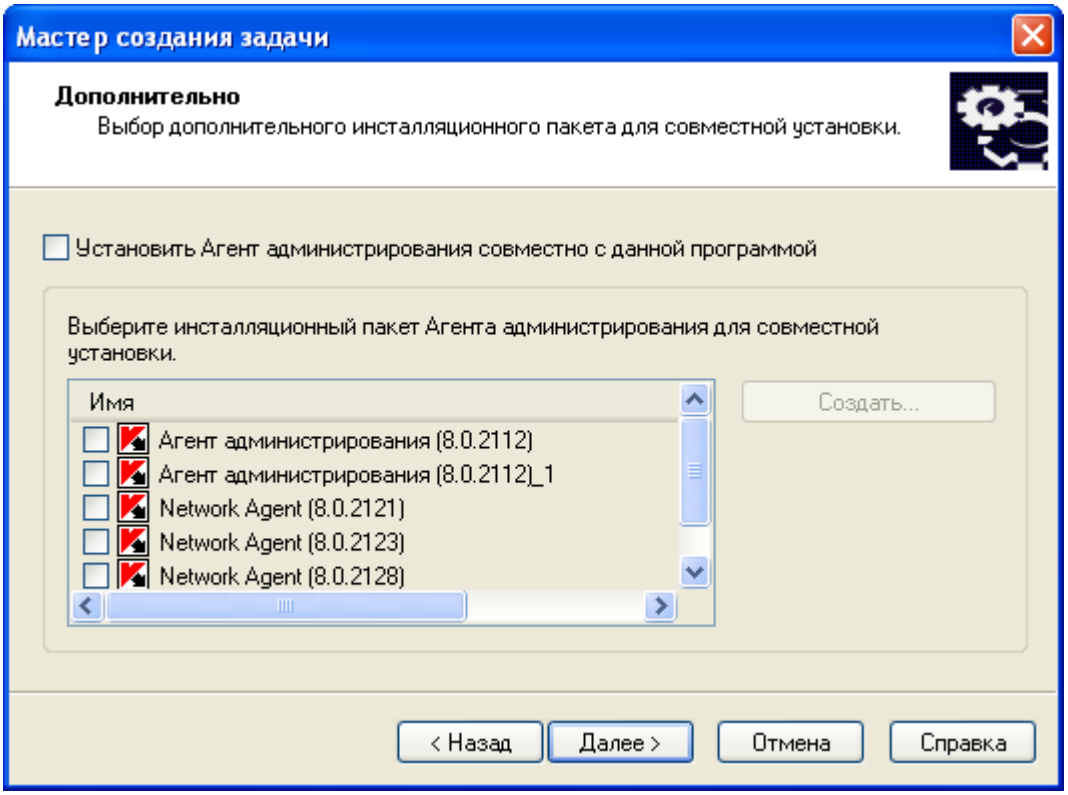


Рисунок 8. Создание задачи. Выбор дополнительного инсталляционного пакета для совместной установки

10. Выберите действие, которое нужно выполнить, если после завершения установки программы требуется перезагрузка компьютера (см. рисунок ниже):

    - **Не перезагружать компьютер**.
    - **Перезагрузить компьютер**.
    - **Спросить у пользователя** (выбрано по умолчанию).

Установите флажок **Принудительно закрывать программы в заблокированных сеансах**, если для перезагрузки операционной системы может понадобиться принудительное завершение работающих программ в заблокированных сеансах.

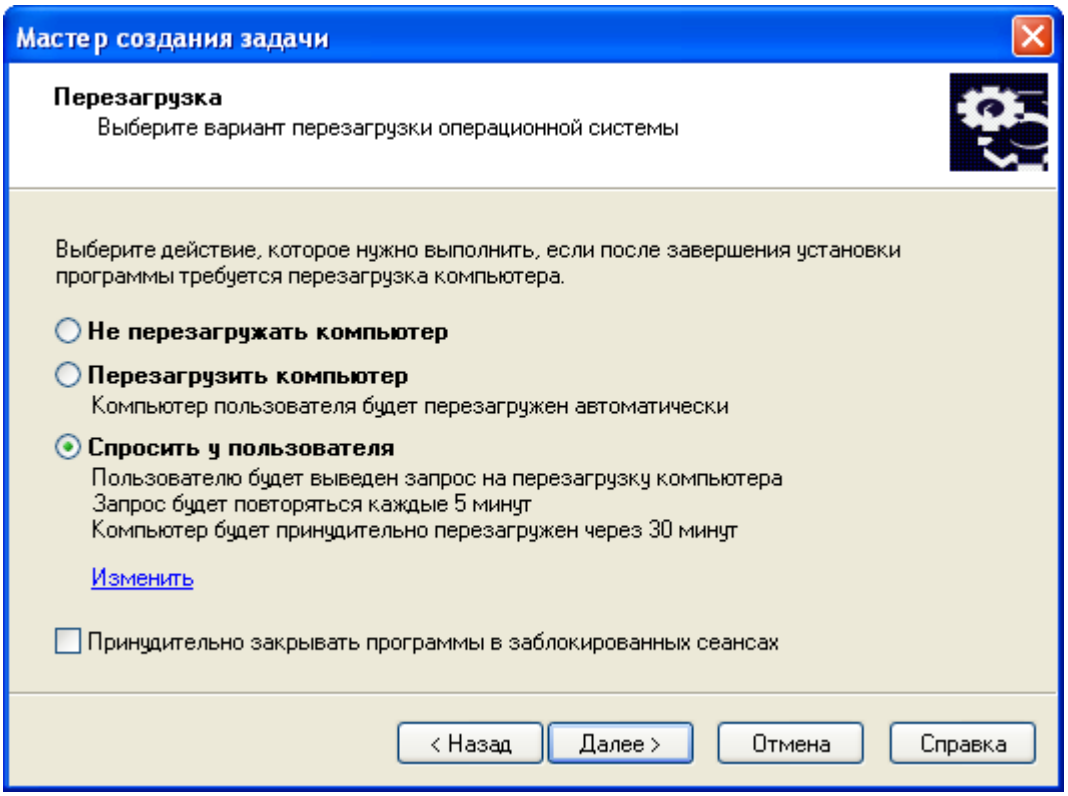


Рисунок 9. Создание задачи. Выбор варианта перезагрузки системы

11. Сформируйте список учетных записей пользователей, под которыми будет запускаться задача удаленной установки на компьютерах (см. рисунок ниже).

    Для добавления учетной записи в список нажмите на кнопку **Добавить** и в открывшемся окне укажите имя пользователя и пароль.

Учетная запись должна обладать правами администратора на всех компьютерах, где планируется провести удаленную установку программного обеспечения. При установке программного обеспечения на компьютеры, входящие в состав различных доменов, необходимо наличие доверительных отношений между этими доменами и доменом, в котором работает Сервер администрирования.

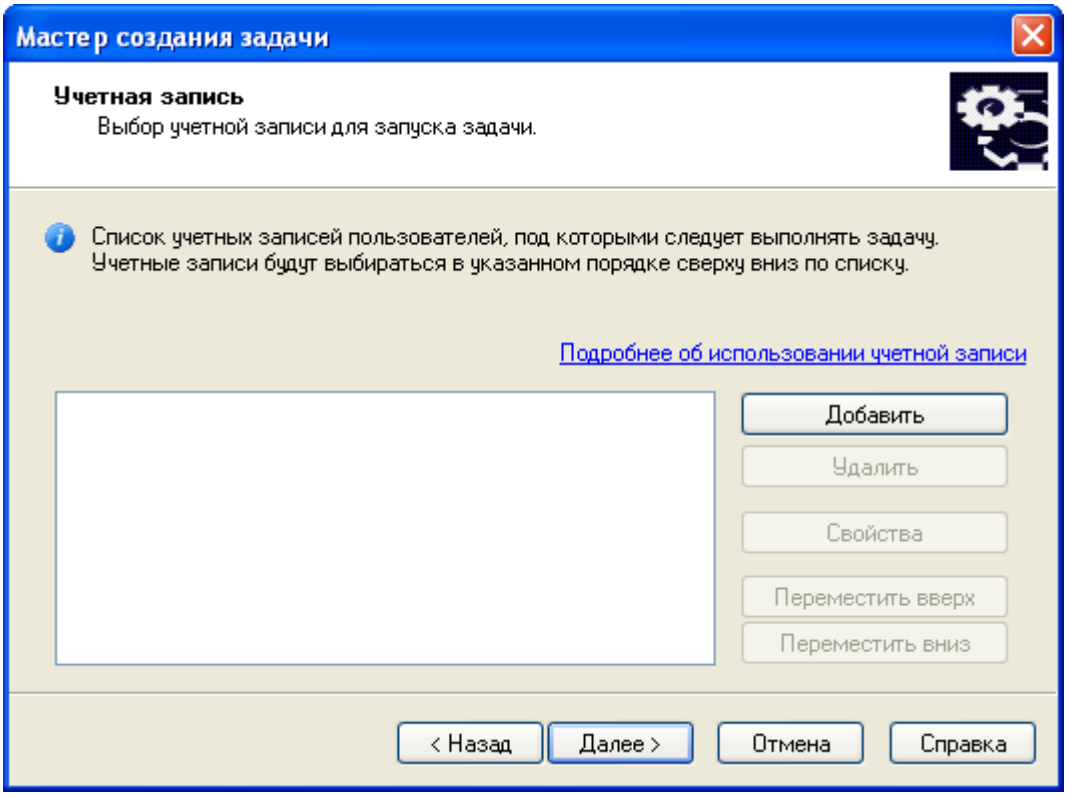


Рисунок 10. Создание задачи. Выбор учетных записей

12. Выполните настройку расписания запуска задачи (см. рисунок ниже):

- В раскрывающемся списке **Запуск по расписанию** выберите нужный режим запуска задачи:
  - **Вручную**.
  - **Каждый N час**.
  - **Ежедневно**.
  - **Еженедельно**.
  - **Ежемесячно**.
  - **Один раз** (в этом случае запуск задачи удаленной установки на компьютерах будет осуществлен только один раз независимо от того, с каким результатом закончится ее выполнение).

- **Немедленно** (сразу после создания задачи, по завершении работы мастера).
- **По завершении другой задачи** (в этом случае задача удаленной установки будет запускаться только после завершения работы указанной задачи).

- В группе полей, соответствующих выбранному режиму, настройте параметры расписания (подробнее см. в Справочном руководстве для Kaspersky Administration Kit).

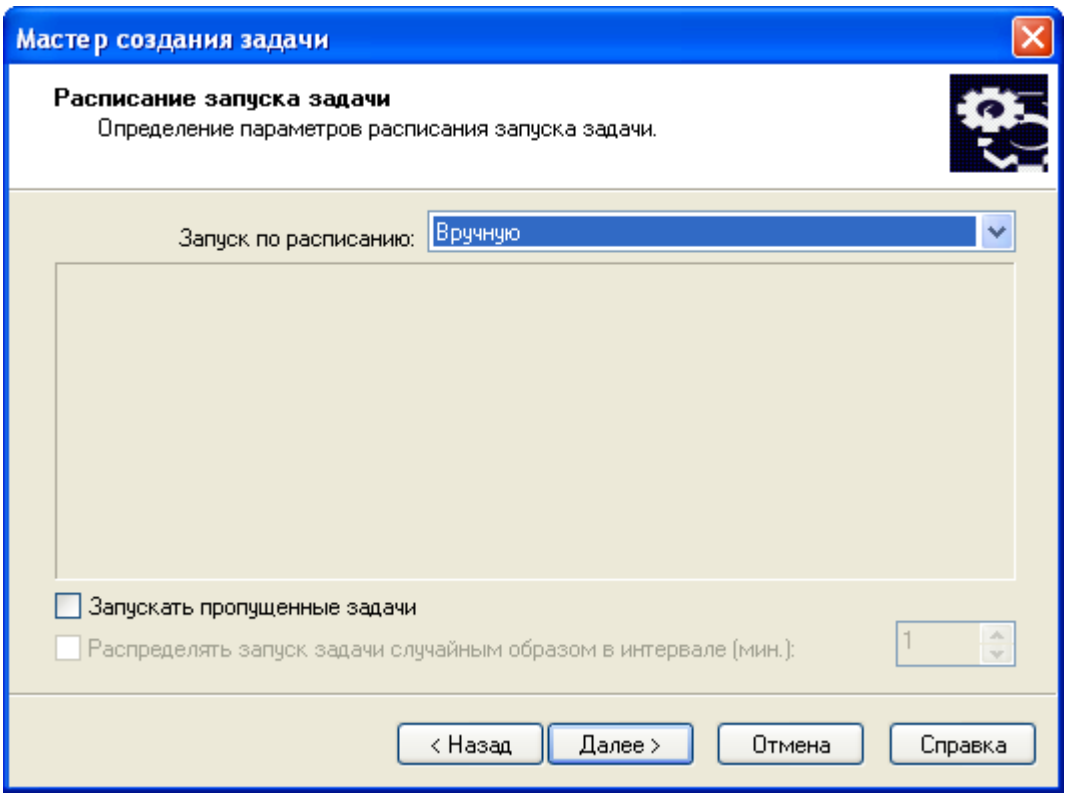


Рисунок 11. Создание задачи. Настройка расписания запуска задачи

По окончании работы мастера задача будет добавлена в папку **Групповые задачи** соответствующей группы и представлена в дереве консоли. Задача будет запущена в соответствии со своим расписанием, однако вы можете запустить задачу и вручную.

Чтобы вручную запустить задачу удаленной установки,

выберите пункт **Свойства** в контекстном меню задачи удаленной установки. В открывшемся окне на закладке **Общие** нажмите на кнопку **Запустить** (см. рисунок ниже).

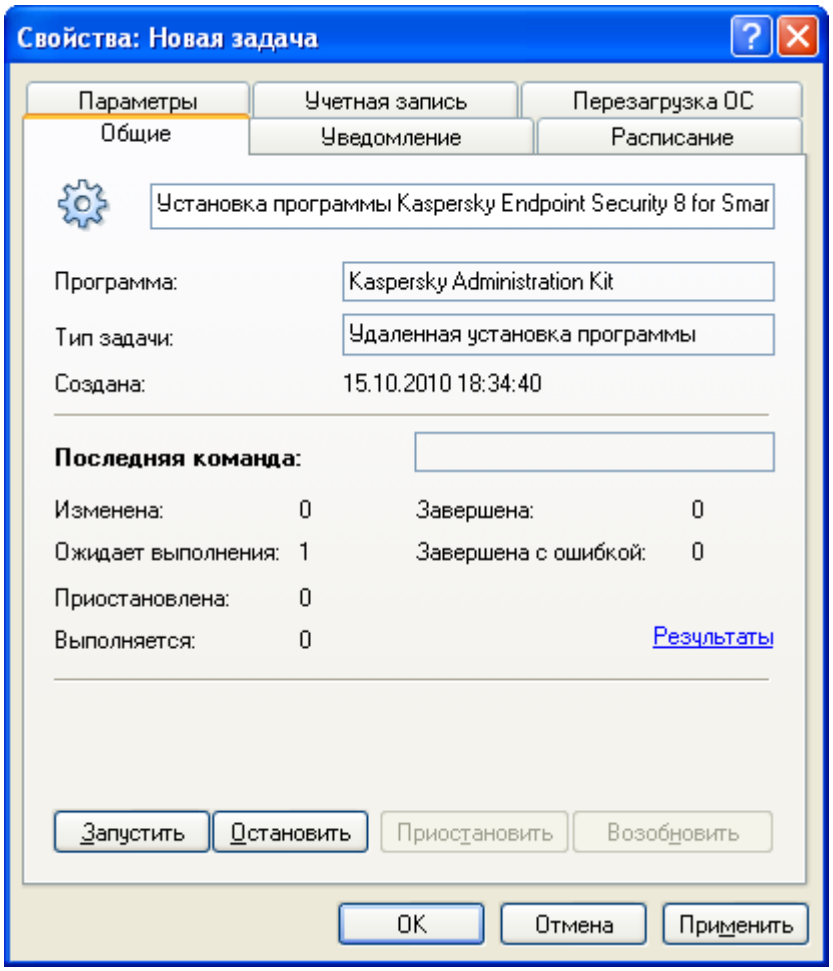


Рисунок 12. Запуск установки программы

ДОСТАВКА ДИСТРИБУТИВА ПРОГРАММЫ НА МОБИЛЬНОЕ УСТРОЙСТВО ЧЕРЕЗ РАБОЧУЮ СТАНЦИЮ

Доставку дистрибутива программы Kaspersky Endpoint Security 8 for Smartphone на мобильное устройство выполняет утилита kmlisten.exe, установленная на рабочей станции в результате выполнения задачи удаленной установки. При подключении устройства к компьютеру утилита предложит пользователю установить Kaspersky Endpoint Security 8 for Smartphone на подключенное мобильное устройство.

Чтобы скопировать дистрибутив программы Kaspersky Endpoint Security 8 for Smartphone с рабочей станции на мобильное устройство, пользователь должен выполнить следующие действия:

1. Подключить устройство к рабочей станции. Если устройство удовлетворяет системным требованиям для установки программы, автоматически откроется окно **KES 8** (см. рисунок ниже).

Рисунок 13. Окно утилиты kmlisten.exe

2. В списке обнаруженных устройств выбрать одно или несколько устройств, на которые следует установить программу.

3. Нажать на кнопку **Установить**. Утилита доставит дистрибутив программы на выбранные устройства. В результате на выбранных мобильных устройствах автоматически запустится установка программы.

В окне **KES 8** будет указан статус доставки инсталляционного пакета программы на устройства.

Окно **KES 8** открывается при каждом подключении мобильного устройства к компьютеру.

Чтобы при каждом подключении устройства к рабочему компьютеру утилита kmlisten.exe не предлагала установить программу, пользователь должен выполнить следующее действие:

в окне **KES 8** установить флажок **Прекратить автоматический запуск программы для установки Kaspersky Endpoint Security 8 for Smartphone**.

Установка программы на мобильном устройстве через рабочую станцию

После завершения загрузки инсталляционного пакета на мобильное устройство программа автоматически устанавливается на устройство без участия пользователя. Статус установки программы на экране устройства при этом не отображается.

Для Symbian OS пользователю потребуется выполнить дополнительные действия во время установки программы. Подробнее об этом читайте в Руководстве пользователя для Symbian OS.

УСТАНОВКА ПРОГРАММЫ ЧЕРЕЗ РАССЫЛКУ ПО ЭЛЕКТРОННОЙ ПОЧТЕ

В случае если установку программы невозможно выполнить через рабочие станции пользователей, администратор может по электронной почте отправить пользователям письмо с инструкцией по скачиванию дистрибутива программы и подключению к Серверу администрирования.

Письмо должно содержать следующую информацию:

- ссылку на дистрибутив программы или вложение с дистрибутивом программы;
- информацию о параметрах подключения программы к Серверу администрирования, если эти параметры не входят в состав предоставленного администратору дистрибутива Kaspersky Endpoint Security 8 for Smartphone.

В ЭТОМ РАЗДЕЛЕ

СОЗДАНИЕ ПИСЬМА С ДИСТРИБУТИВОМ ПРОГРАММЫ

Чтобы создать письмо с дистрибутивом программы, выполните следующие действия:

1. Сформируйте письмо для всех пользователей, на мобильные устройства которых вы планируете установить Kaspersky Endpoint Security 8 for Smartphone.
2. В теме письма введите текст «Дистрибутив программы Kaspersky Endpoint Security 8 for Smartphone для установки на мобильное устройство».
3. В тело письма вставьте следующий шаблон:

Уважаемый пользователь мобильного устройства!

Это письмо содержит дистрибутив Kaspersky Endpoint Security 8 for Smartphone, а также информацию о параметрах подключения программы к системе удаленного администрирования.

Для установки Kaspersky Endpoint Security 8 for Smartphone Вам следует загрузить установочный файл <имя файла> на свое мобильное устройство. (Установочный файл программы приложен к письму. / Установочный файл программы расположен по ссылке: <ссылка на установочный файл>.)

Если Вы получили это письмо на мобильное устройство, то загрузите установочный файл, (приложенный к письму, / используя ссылку, указанную в теле письма) и сохраните его на вашем устройстве. Если Вы получили письмо на свой рабочий компьютер, то загрузите установочный файл на устройство с помощью программы для обмена данными между мобильным устройством и компьютером. Затем запустите загруженный установочный файл и выполните установку программы, следуя указаниям мастера установки.

Во время установки мастер предложит Вам указать значения следующих параметров:

Сервер – введите в поле адрес <адрес Сервера администрирования>.

Порт – укажите в поле порт <номер порта Сервера администрирования>.

Группа – укажите в поле группу <имя группы>.

Ваш адрес эл. почты – введите ваш корпоративный адрес электронной почты.

Адрес электронной почты используется для регистрации устройства в системе удаленного администрирования. Помните, что невозможно изменить адрес, заданный при установке программы.

Если в процессе установки программы возникли ошибки, обратитесь к администратору.

Текст, заключенный в круглые скобки и разделенный косой чертой, означает, что вы должны выбрать один из двух способов загрузки установочного файла: из приложения к письму или по ссылке – и указать соответствующие инструкции в письме.

4. Вместо текста в угловых скобках укажите конкретные значения следующих параметров:

   - <имя файла> – имя установочного файла для операционной системы, которая установлена на устройстве пользователя. Например, если на устройстве пользователя установлена операционная система Microsoft Windows Mobile, то следует указать установочный файл с расширением CAB.

   - <ссылка на установочный файл> – ссылка на установочный файл для операционной системы, которая установлена на устройстве пользователя. Установочный файл должен быть предварительно размещен на FTP- / HTTP-сервере, к которому разрешен доступ через интернет. Если по каким-либо причинам размещение установочного файла на FTP- / HTTP-сервере невозможно, то вы можете приложить установочный файл к письму.

   - <адрес Сервера администрирования> – IP-адрес или DNS-имя Сервера администрирования, к которому будут подключены мобильные устройства. Адрес сервера должен быть указан в том формате, в каком он указан в свойствах Сервера администрирования на закладке **Общие** в поле **Адрес**. То есть если в свойствах Сервера администрирования указан IP-адрес, то и в письме укажите тот же IP-адрес. Если же в свойствах Сервера администрирования указано DNS-имя, то в письме укажите то же DNS-имя.

   - <номер порта Сервера администрирования> – номер порта, открытый на Сервере администрирования для подключения мобильных устройств. По умолчанию используется порт 13292.

   - <имя группы> – имя группы, в которую будут автоматически добавлены мобильные устройства после первой синхронизации с Сервером администрирования. По умолчанию устройства добавляются в группу с именем KES8.

Если параметры подключения мобильных устройств к Серверу администрирования входят в состав предоставленного вам дистрибутива Kaspersky Endpoint Security 8 for Smartphone, то в тексте письма следует запросить только адрес электронной почты пользователей. Параметры подключения к Серверу администрирования указывать не нужно.

5. Приложите установочный файл к письму, если установочный файл программы по каким-либо причинам не может быть размещен на FTP- / HTTP-сервере.

6. Отправьте письмо. После отправки письма следует убедиться, что оно было получено всеми адресатами.

Установка программы на мобильном устройстве после получения сообщения по электронной почте

После получения от администратора письма с дистрибутивом программы пользователь загружает дистрибутив на свое устройство одним из доступных ему способов. Дистрибутив программы содержит установочный файл для операционной системы, установленной на устройстве пользователя. Пользователь открывает установочный файл, в результате на устройстве автоматически запускается мастер установки программы.

В процессе установки мастер предложит пользователю задать секретный код программы и параметры подключения программы к системе удаленного администрирования, если они не входят в состав дистрибутива Kaspersky Endpoint Security 8 for Smartphone. После ввода необходимых значений параметров установка программы завершается автоматически. Подробно об установке программы читайте в Руководстве пользователя Kaspersky Endpoint Security 8 for Smartphone.

УСТАНОВКА ЛИЦЕНЗИИ ЧЕРЕЗ KASPERSKY ADMINISTRATION KIT

Особенность установки лицензии для программы Kaspersky Endpoint Security 8 for Smartphone состоит в том, что лицензия доставляется на мобильное устройство вместе с политикой при синхронизации устройства с Сервером администрирования. В течение трех дней после установки программы устройство автоматически выходит на связь с Сервером администрирования каждые три часа. После применения политики устройство синхронизируется с Сервером администрирования с периодичностью, которая была указана в параметрах сети при создании политики (см. раздел «Создание политики» на стр. 52). По умолчанию установлена периодичность – каждые 6 часов.

Для того чтобы выполнить активацию программы, администратор должен создать политику для группы, в которую входит устройство, и включить в состав этой политики лицензию. Когда мобильное устройство в очередной раз установит соединение с Сервером администрирования, лицензия будет загружена на устройство вместе с политикой и программа, установленная на устройстве, будет активирована.

При переходе в режим работы с ограниченной функциональностью программа прекращает выполнять автоматическую синхронизацию с Сервером администрирования. Поэтому если по каким-то причинам активация программы не была выполнена в течение трех дней с момента установки, то пользователь должен будет выполнить синхронизацию с Сервером администрирования вручную (подробнее см. в Руководстве пользователя Kaspersky Endpoint Security 8 for Smartphone).

Обязательно выполните активацию программы в течение трех дней с момента установки Kaspersky Endpoint Security 8 for Smartphone на мобильные устройства. Если активация не будет выполнена, то программа автоматически переключится в режим работы с ограниченной функциональностью. В этом режиме работы большинство компонентов Kaspersky Endpoint Security 8 for Smartphone отключены.

РАБОТА С ПОЛИТИКАМИ

Все параметры работы программы, включая лицензию, расписание обновления баз программы, расписание проверки устройства, определяются через политику или локальные параметры программы. При помощи политик могут быть установлены одинаковые значения параметров работы программы для всех мобильных устройств, входящих в состав группы. Подробно о политиках и группах администрирования см. в Руководстве администратора для Kaspersky Administration Kit.

Каждый параметр, представленный в политике, имеет атрибут – «замок», который показывает, наложен ли запрет на изменение параметра в политиках вложенного уровня иерархии (для вложенных групп и подчиненных Серверов администрирования) и локальных параметрах программы.

Если в политике для параметра установлен «замок», то в дальнейшем после применения политики на мобильных устройствах будут использоваться значения, заданные политикой. При этом пользователь мобильного устройства не сможет изменить эти значения. Для параметров, которые не были зафиксированы «замком», будут использоваться локальные значения, установленные по умолчанию или самим пользователем мобильного устройства.

Информация о параметрах программы, заданных в политиках, сохраняется на Сервере администрирования и распространяется на мобильные устройства в ходе синхронизации. При этом в данные Сервера администрирования, в свою очередь, вносятся локальные изменения, проведенные на мобильных устройствах и разрешенные политикой.

Вы можете изменять параметры работы программы на конкретном мобильном устройстве с помощью локальных параметров программы (см. раздел «Настройка локальных параметров программы» на стр. 66), если на изменение этих параметров не наложен запрет в действующей политике.

В ЭТОМ РАЗДЕЛЕ

Создание политики

Чтобы создать политику, выполните следующие действия:

1. Подключитесь к Серверу администрирования.
2. Выберите в дереве консоли группу, для которой вы будете создавать политику.
3. Выберите вложенную папку **Политики**, входящую в состав группы.
4. Откройте контекстное меню и выберите пункт **Создать** → **Политику** или воспользуйтесь ссылкой **Создать новую политику** в панели задач. В результате запускается мастер. Следуйте его указаниям.
5. Укажите имя политики и в качестве программы, для которой она создается, выберите **Kaspersky Endpoint Security 8 for Smartphone**.

   Ввод имени производится стандартным способом. Если вы укажете имя уже существующей политики, к нему автоматически будет добавлено окончание **(1)**.

   Программы выбираются из раскрывающегося списка (см. рисунок ниже). В нем перечислены все программы компании, для которых на рабочее место администратора установлены плагины управления.

Создать политику для программы Kaspersky Endpoint Security 8 for Smartphone вы сможете, только если на рабочем месте администратора установлен плагин управления этой программой. Если плагин не установлен, то имя программы будет отсутствовать в списке программ.

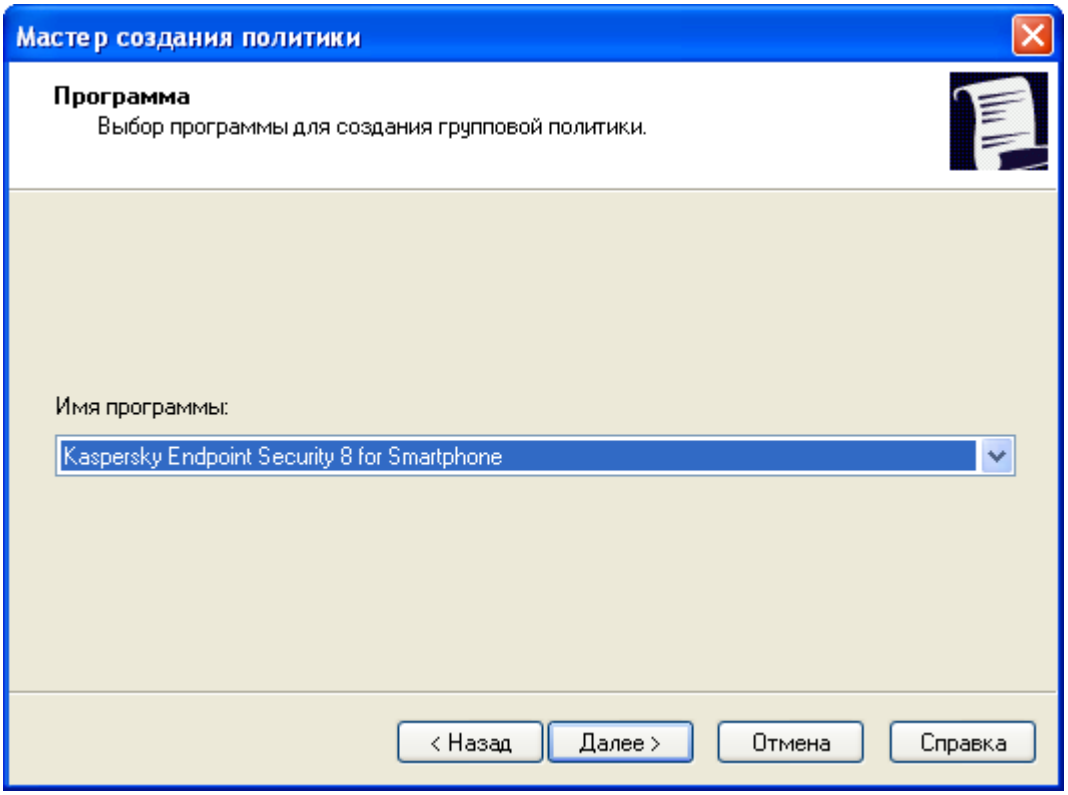


Рисунок 14. Выбор программы для создания политики

6. Укажите статус политики (см. рисунок ниже). Для этого выберите один из вариантов:

   - **Активная политика**. В этом случае созданная политика сохраняется на Сервере администрирования и будет использоваться в качестве действующей для программы.

   - **Неактивная политика**. В этом случае созданная политика сохраняется на Сервере администрирования как резервная политика и может быть активирована по событию. При необходимости неактивную политику можно сделать действующей (подробно о статусах политик см. в Справочном руководстве Kaspersky Administration Kit).

Для одной программы в группе можно создать несколько политик, но активной может быть только одна из них. При создании новой активной политики предыдущая активная политика автоматически становится неактивной.

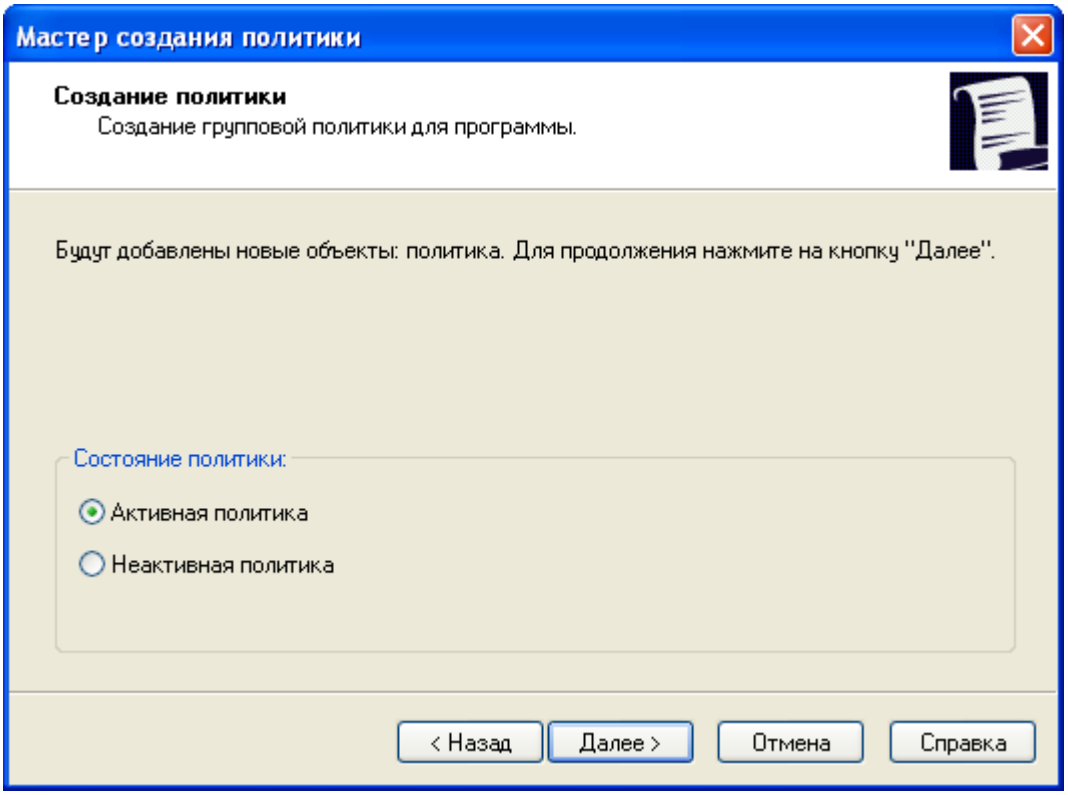


Рисунок 15. Активирование политики

7. Определите параметры проверки по требованию (см. раздел «Проверка по требованию» на стр. 17). При создании политики вы можете настроить следующие параметры (см. рисунок ниже):

   - включить / отключить проверку исполняемых файлов;
   - включить / отключить проверку архивов;
   - включить / отключить лечение зараженных объектов;
   - сформировать расписание, согласно которому программа будет запускать полную проверку файловой системы устройства.

По умолчанию Kaspersky Endpoint Security 8 for Smartphone проверяет все файлы, сохраненные на устройстве и карте расширения памяти. При обнаружении зараженного объекта программа пытается вылечить его. Если объект вылечить невозможно, то программа помещает его на карантин. Описание параметров см. в разделе «Параметры функции Проверка по требованию» (см. раздел «Параметры функции Проверка по требованию» на стр. 68).

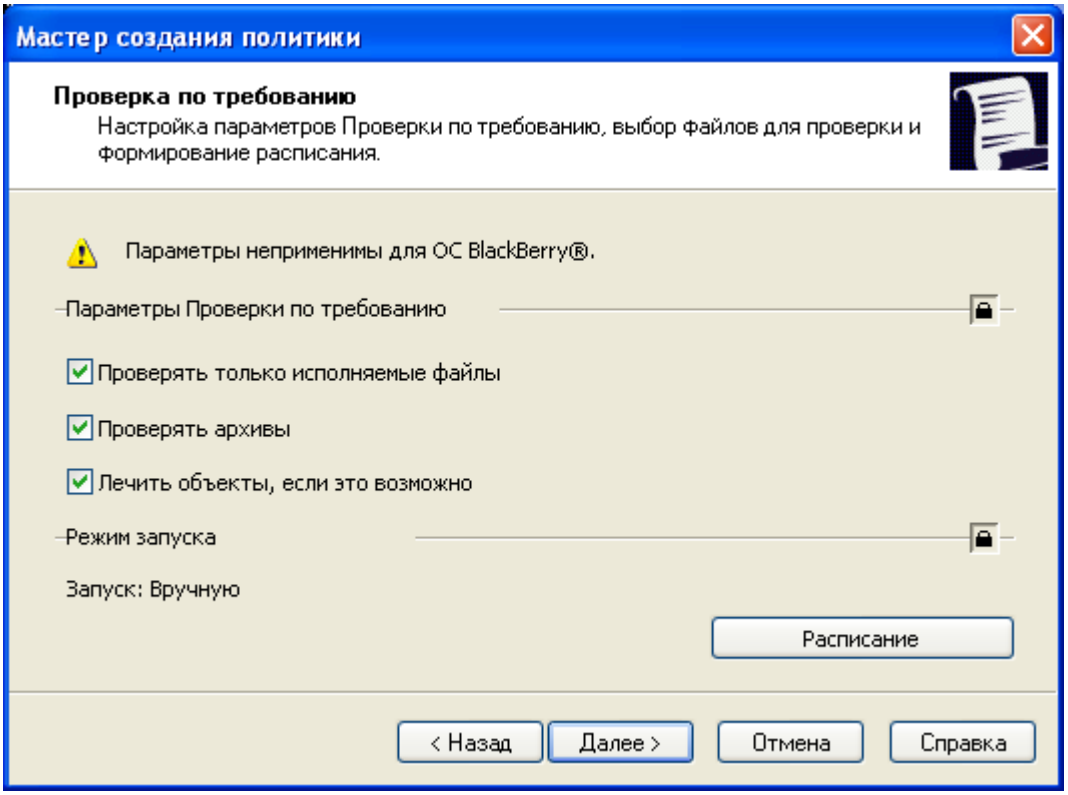


Рисунок 16. Настройка параметров компонента Проверка по требованию

8. Определите параметры компонента Защита (на стр. 17). При создании политики вы можете настроить следующие параметры (см. рисунок ниже):

   - включить / отключить работу компонента Защита на мобильных устройствах пользователей;
   - включить / отключить проверку исполняемых файлов;
   - выбрать действие над зараженными объектами.

По умолчанию компонент Защита включен и проверяет все типы файлов, к которым пользователь устройства пытается получить доступ. При обнаружении зараженного объекта программа пытается вылечить его. Если объект вылечить невозможно, то программа помещает его в карантинный каталог. Описание параметров см. в разделе «Параметры функции Защита» (см. раздел «Параметры функции Защита» на стр. 70).

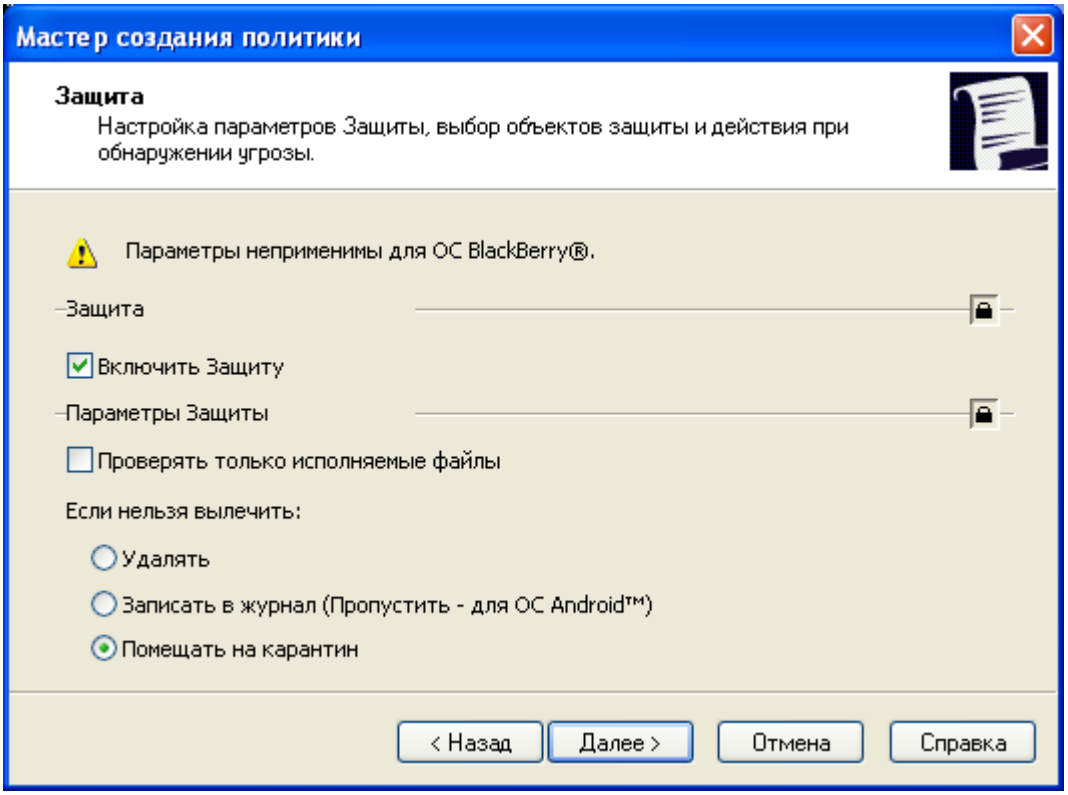


Рисунок 17. Настройка параметров компонента Защита

9. Настройте параметры обновления баз программы: выберите источник обновлений и установите расписание, согласно которому будут проходить обновления (см. рисунок ниже). Укажите, будет ли выполняться обновление, если устройства пользователей находятся в зоне роуминга. По умолчанию в качестве источника обновлений используются серверы обновлений «Лаборатории Касперского». Запуск обновлений выполняется вручную пользователем мобильного устройства. Обновление в роуминге не выполняется. Описание параметров см. в разделе «Параметры функции Обновление» (см. раздел «Параметры функции Обновление» на стр. 72).

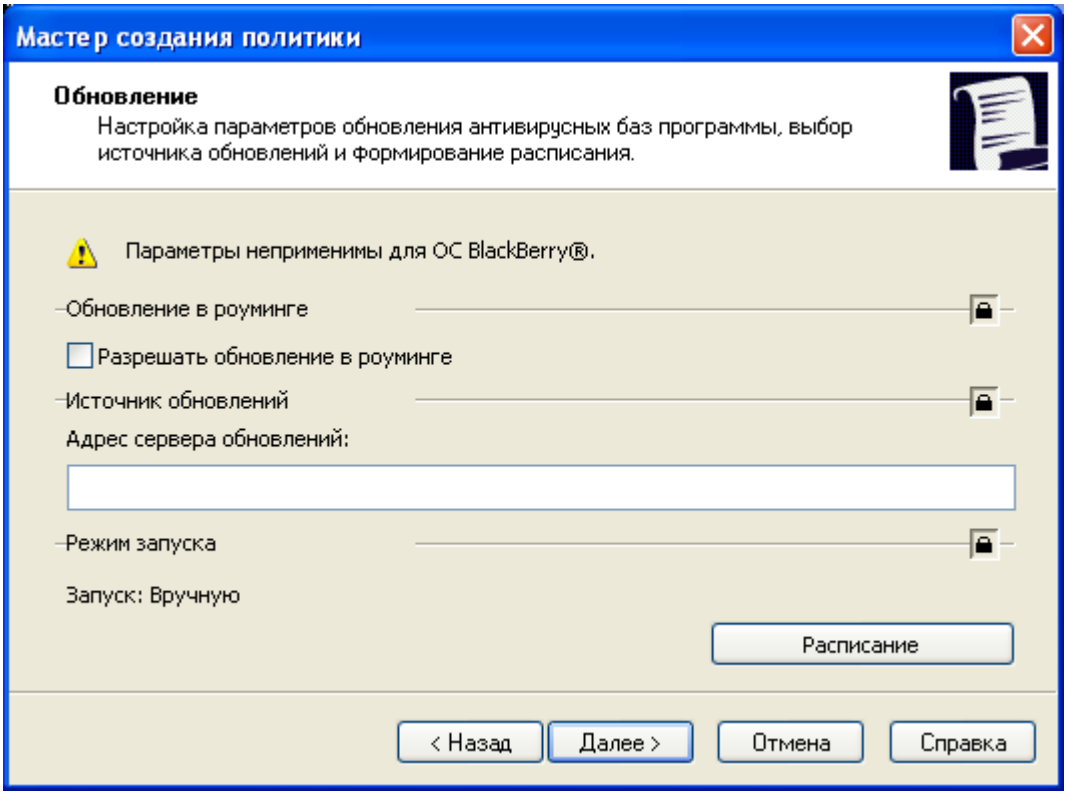


Рисунок 18. Выбор источника обновлений

10. Определите параметры компонента Анти-Вор (на стр. 19). Укажите, какие функции компонента будут доступны на устройствах пользователей, и настройте параметры выбранных функций (см. рисунок ниже). По умолчанию все функции компонента Анти-Вор отключены. Описание параметров см. в разделе «Параметры компонента Анти-Вор» (см. раздел «Параметры компонента Анти-Вор» на стр. 73).

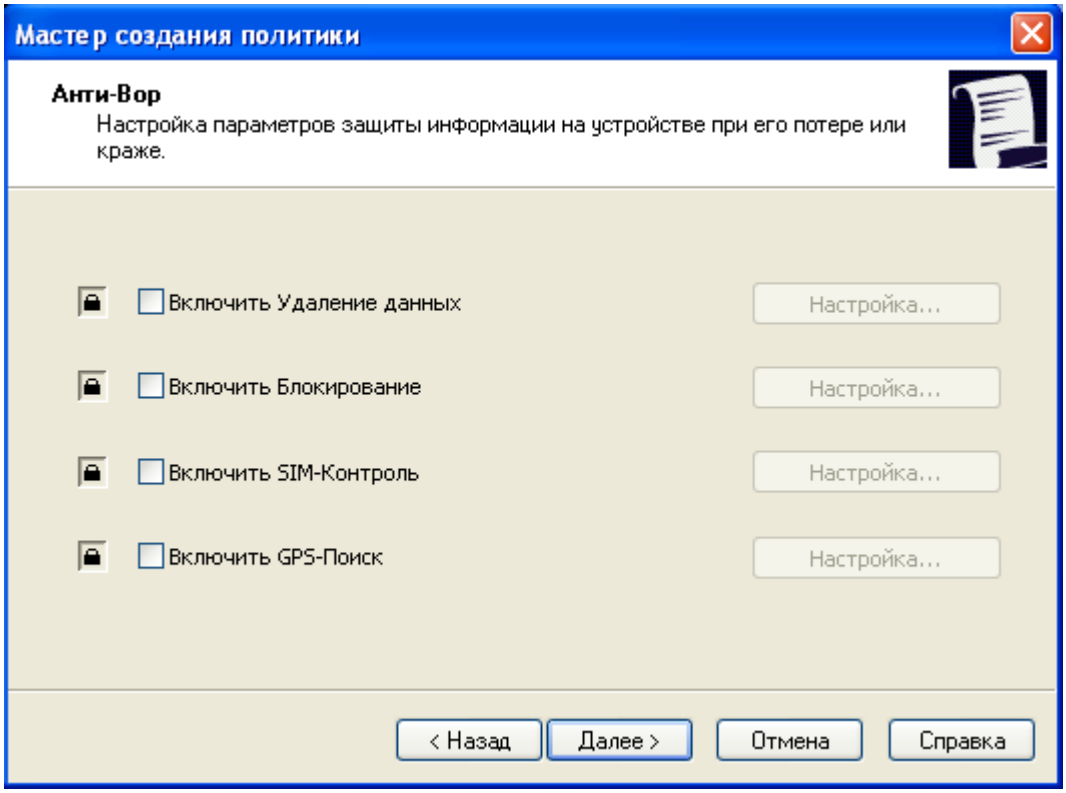


Рисунок 19. Настройка параметров компонента Анти-Вор

11. Определите параметры синхронизации мобильных устройств с Сервером администрирования (см. рисунок ниже) и режим работы компонента Сетевой экран (на стр. 21). По умолчанию мобильное устройство инициирует попытку подключения к Серверу администрирования каждые 6 часов. Сетевой экран по умолчанию отключен. Описание параметров см. в разделе «Параметры компонента Сетевой экран» (см. раздел «Параметры компонента Сетевой экран» на стр. 79).

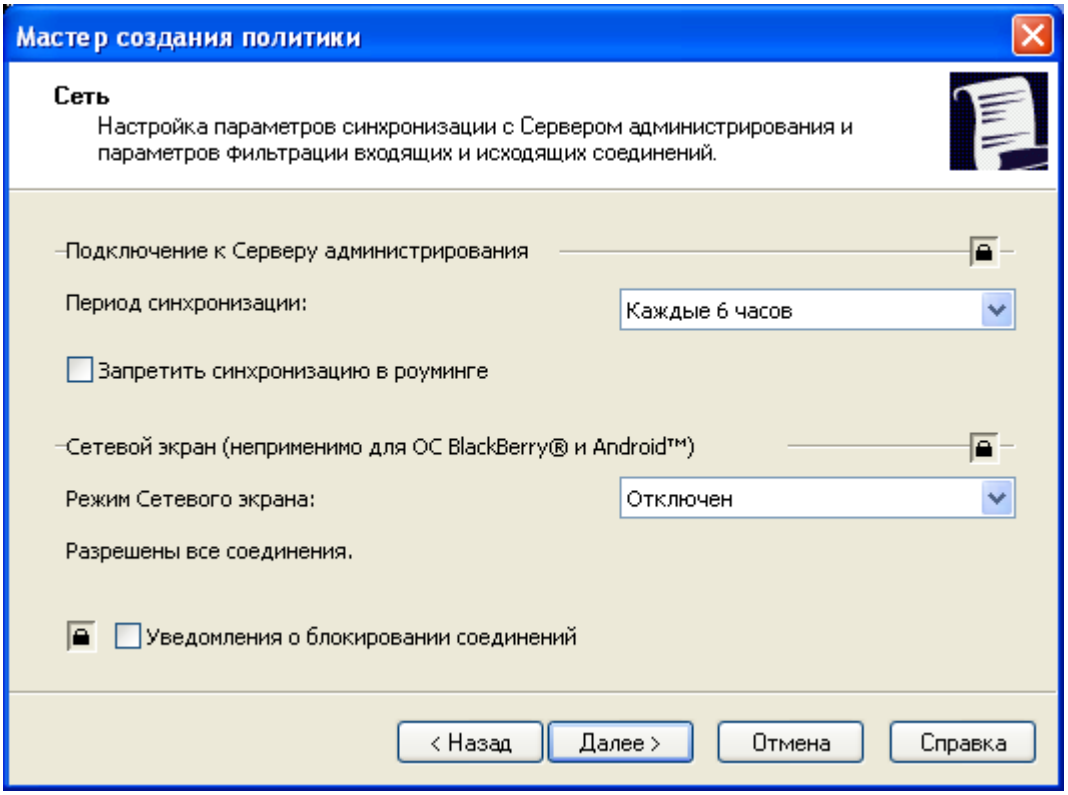


Рисунок 20. Настройка сети

12. Определите параметры компонентов Анти-Спам (на стр. 20), Личные контакты (на стр. 20) и Шифрование (на стр. 21). Укажите, какие компоненты будут доступны для использования на устройствах пользователей, и настройте параметры компонента Шифрование (см. рисунок ниже). По умолчанию использование компонентов Анти-Спам и Личные контакты разрешено пользователю. Параметры компонентов Анти-Спам и Личные контакты пользователи настраивают на устройствах самостоятельно. Описание параметров см. в разделах «Параметры компонентов Анти-Спам и Личные контакты» (см. раздел «Параметры компонентов Анти-Спам и Личные контакты» на стр. 81), «Параметры компонента Шифрование» (см. раздел «Параметры компонента Шифрование» на стр. 82).

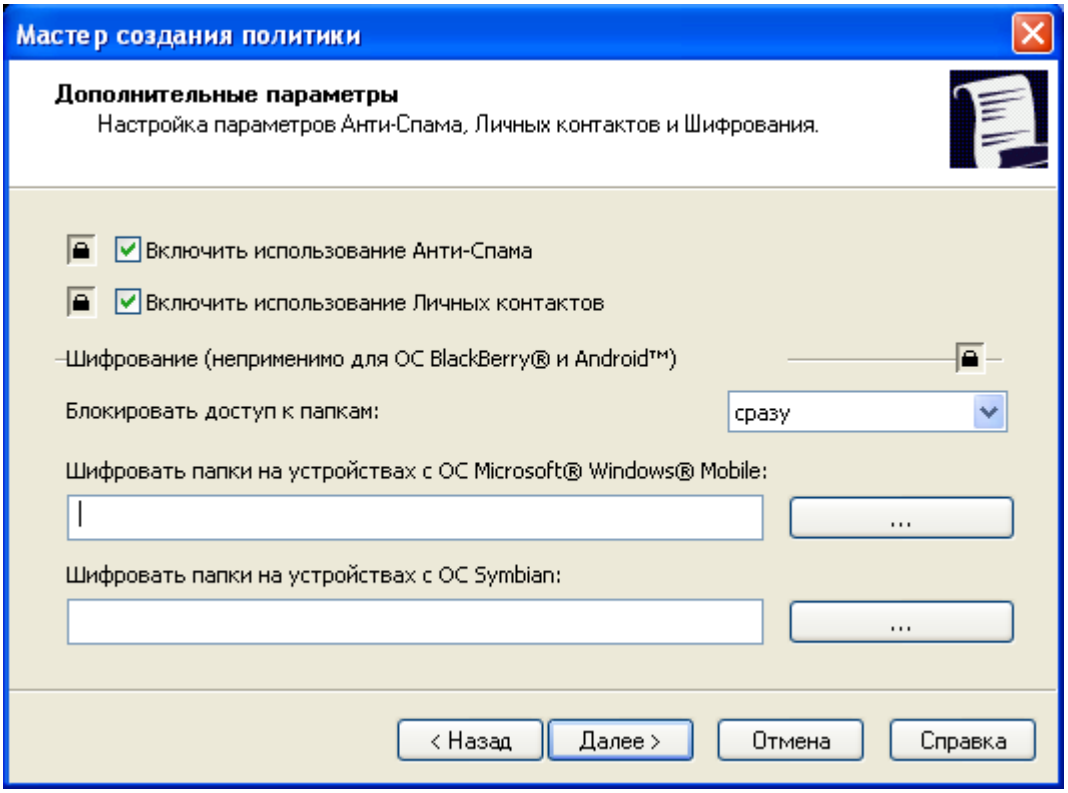


Рисунок 21. Настройка дополнительных параметров

13. Укажите лицензию, которая будет установлена на мобильные устройства для активации программы (см. рисунок ниже).

Обязательно выполните активацию программы в течение трех дней с момента установки Kaspersky Endpoint Security 8 for Smartphone на мобильные устройства. Если активация программы не будет выполнена, то программа автоматически переключится в режим работы с ограниченной функциональностью. В этом режиме работы большинство компонентов Kaspersky Endpoint Security 8 for Smartphone отключены.

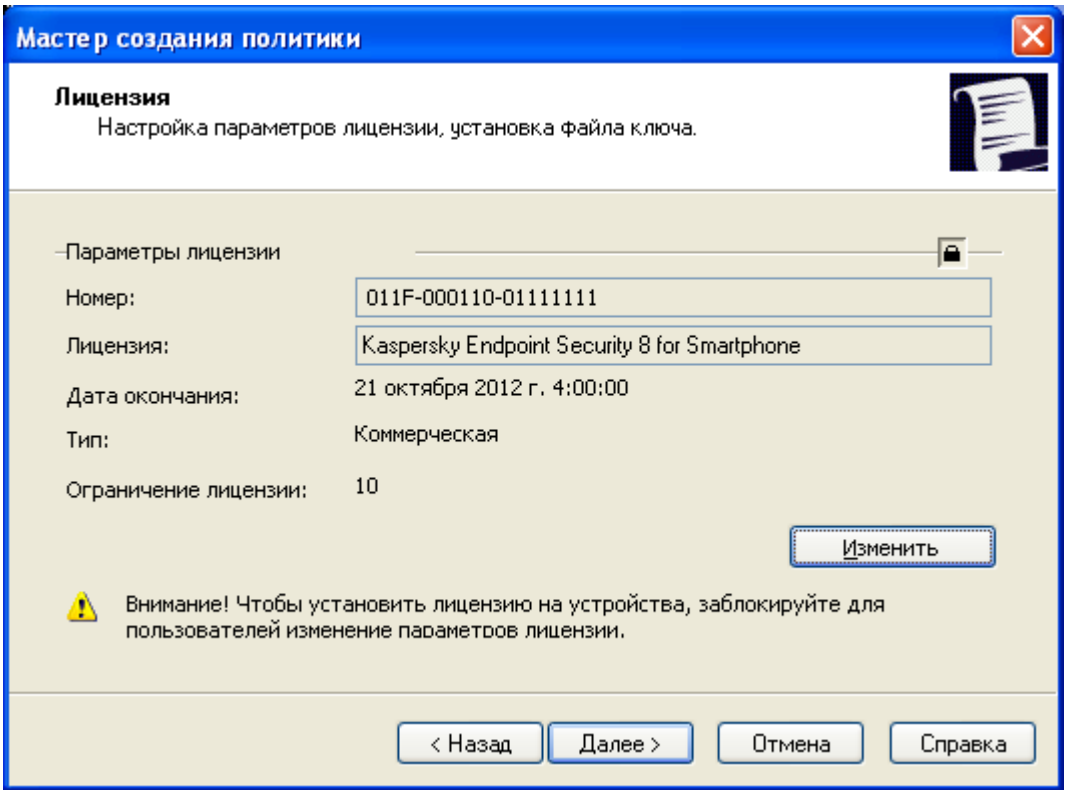


Рисунок 22. Выбор файла ключа для активации лицензии

Нажмите на кнопку **Изменить** и в открывшемся окне выберите файл ключа для установки лицензии. После этого в окне мастера отображается информация о лицензии:

- номер лицензии;
- название лицензии;
- дата окончания срока действия лицензии;
- тип установленной лицензии, например: коммерческая, пробная;
- ограничения, заданные в лицензии.

Убедитесь, что на кнопке в правом верхнем углу изображен закрытый «замок» – . Если «замок» открыт, то установка лицензии на мобильных устройствах выполнена не будет.

14. Нажмите на кнопку **Готово** для завершения работы мастера создания политики.

По окончании работы мастера политика для Kaspersky Endpoint Security 8 for Smartphone будет добавлена в папку **Политики** соответствующей группы администрирования и представлена в панели результатов.

Распространение политики на мобильные устройства будет осуществлено при синхронизации устройств с Сервером администрирования сразу после добавления мобильного устройства в группу администрирования узла **Управляемые компьютеры** (см. раздел «**Перемещение устройств в группу Управляемые компьютеры**» на стр. 62).

Настройка параметров политики

После создания политики вы можете редактировать параметры программы через свойства политики. При редактировании параметров политики вы можете использовать кнопку для того, чтобы разрешить / запретить изменение параметров на мобильном устройстве.

Чтобы внести изменения в политику, выполните следующие действия:

1. Подключитесь к Серверу администрирования.
2. Выберите в дереве консоли в папке **Управляемые компьютеры** группу администрирования, в состав которой входят мобильные устройства.
3. Выберите входящую в состав данной группы папку **Политики**. В панели результатов будут отображены все политики, созданные для группы.
4. Выберите в списке политик политику для Kaspersky Endpoint Security 8 for Smartphone, параметры которой вы планируете изменить.
5. Выберите в контекстном меню политики пункт **Свойства**. Откроется окно настройки параметров политики, содержащее несколько закладок.
6. Установите нужные значения параметров для компонентов программы на закладках **Проверка** (см. раздел «**Параметры функции Проверка по требованию**» на стр. 68), **Защита** (см. раздел «**Параметры функции Защита**» на стр. 70), **Обновление** (см. раздел «**Параметры функции Обновление**» на стр. 72), **Анти-Вор** (см. раздел «**Параметры компонента Анти-Вор**» на стр. 73), **Сеть** (см. раздел «**Параметры синхронизации устройств с Сервером администрирования**» на стр. 80), **Дополнительно** и **Лицензия**. Закладки **Общие** и **События** являются стандартными для программы Kaspersky Administration Kit (подробнее см. в Руководстве администратора Kaspersky Administration Kit). Остальные закладки содержат параметры программы Kaspersky Endpoint Security 8 for Smartphone.
7. Нажмите на кнопку **Применить** или на кнопку **ОК**.

Применение политики

При синхронизации мобильных устройств с Сервером администрирования параметры программы, заданные в политике, передаются на все устройства, входящие в группу. Вместе с параметрами программы на мобильные устройства копируется лицензия для активации программы.

Если в политике для параметра установлен «замок», то пользователь не сможет изменить значение этого параметра на мобильном устройстве. Все остальные параметры работы программы пользователь может переопределить по своему усмотрению.

Параметры, измененные пользователем, передаются на Сервер администрирования при следующей синхронизации и сохраняются на Сервере администрирования в локальных параметрах программы (см. раздел «Настройка локальных параметров программы» на стр. 66).

Перемещение устройств в группу Управляемые компьютеры

При первой синхронизации мобильных устройств с Сервером администрирования устройства автоматически попадают в группу узла **Нераспределенные компьютеры** (по умолчанию эта группа называется KES8). Пока устройства находятся в этой группе, централизованное управление параметрами программ Kaspersky Endpoint Security 8 for Smartphone, установленными на этих устройствах, невозможно.

Чтобы получить возможность управлять программами Kaspersky Endpoint Security 8 for Smartphone, установленными на мобильных устройствах, с помощью политик, администратор должен переместить устройства из группы узла **Нераспределенные компьютеры** в созданную ранее группу узла **Управляемые компьютеры** (см. раздел «**Создание групп**» на стр. 34).

Администратор может переместить мобильные устройства в группу узла **Управляемые компьютеры** вручную или настроить автоматическое перемещение устройств в заданную группу.

В ЭТОМ РАЗДЕЛЕ

ПЕРЕМЕЩЕНИЕ УСТРОЙСТВА В ГРУППУ ВРУЧНУЮ

*Чтобы вручную переместить мобильные устройства в группу узла **Управляемые компьютеры**, выполните следующие действия:*

1. Подключитесь к Серверу администрирования.
2. Выберите в дереве консоли узел **Нераспределенные компьютеры**.
3. Выберите группу, в которую были автоматически добавлены мобильные устройства при синхронизации с Сервером администрирования (по умолчанию KES8).
4. Выберите в группе устройство, которое необходимо переместить в группу узла **Управляемые компьютеры**.
5. Откройте контекстное меню и выберите пункт **Переместить в группу**. Откроется окно **Выберите группу** (см. рисунок ниже).

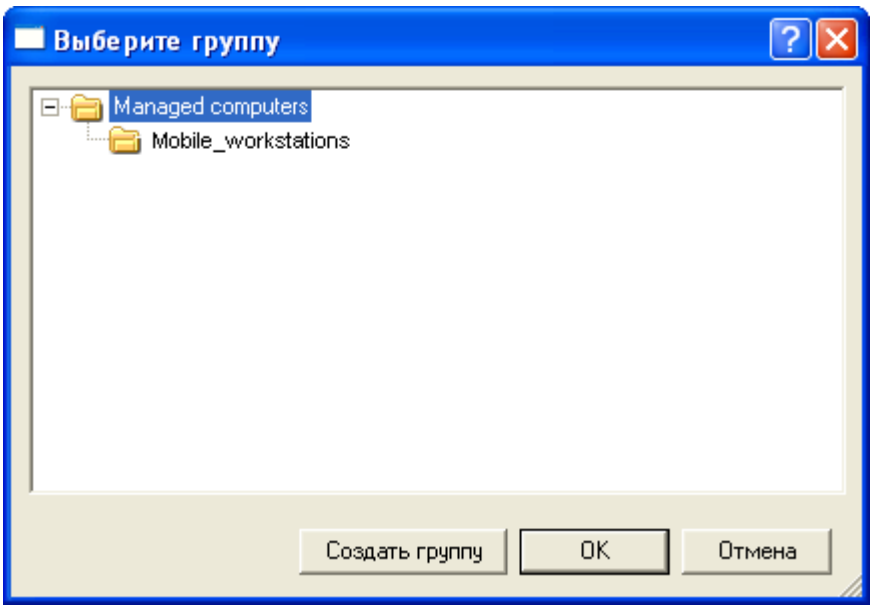


Рисунок 23. Выбор группы

6. Откройте узел **Управляемые компьютеры**, выберите группу, в которую должно быть перемещено устройство. Вы можете выбрать группу, которую создали ранее на этапе подготовки к установке (см. раздел «Создание групп» на стр. 34), или создать новую группу.

   Чтобы создать новую группу, выберите в узле **Управляемые компьютеры** группу, внутри которой будет создана группа, и нажмите на кнопку **Создать группу**. После этого введите имя созданной группы.

7. Нажмите на кнопку **ОК**. Мобильное устройство перемещается в выбранную группу.

Настройка автоматического перемещения устройств в группу

*Чтобы настроить автоматическое перемещение устройств в группу узла **Управляемые компьютеры**, выполните следующие действия:*

1. Выберите в дереве консоли Сервер администрирования, к которому подключены мобильные устройства.

2. Откройте контекстное меню сервера и выберите пункт **Свойства**. Откроется окно настройки параметров Сервера администрирования.

3. Откройте закладку **Перемещение компьютеров** (см. рисунок ниже).

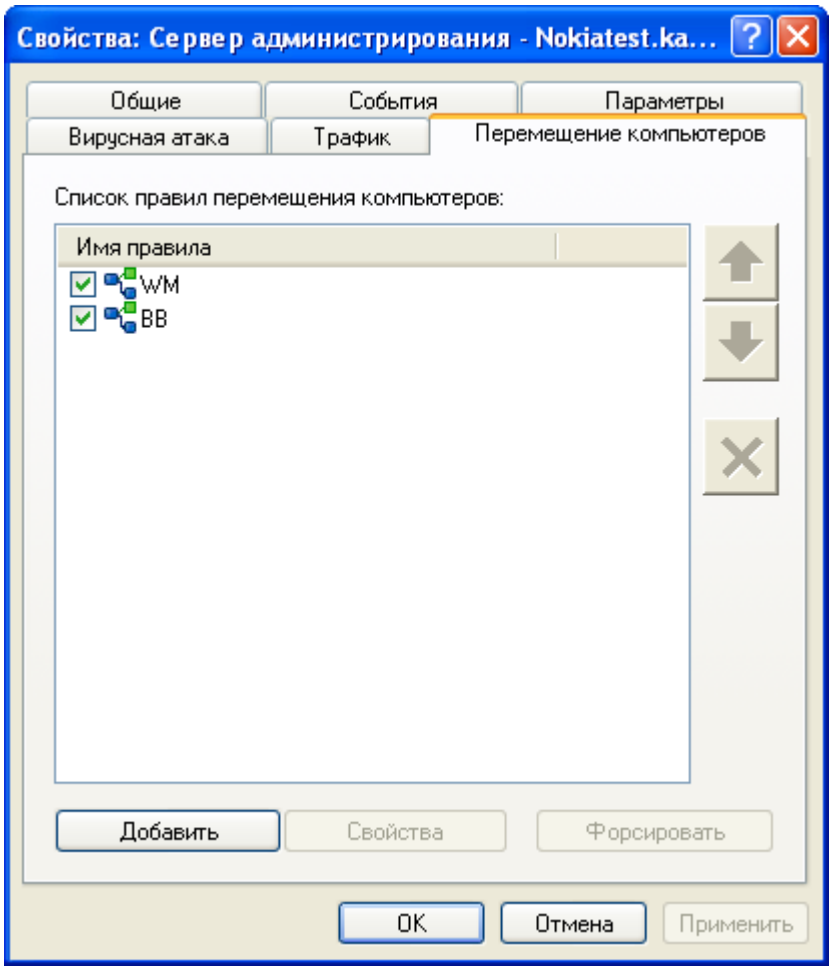


Рисунок 24. Окно настройки параметров Сервера администрирования

4. Создайте правило перемещения мобильных устройств в группу. Для этого нажмите на кнопку **Добавить**. Откроется окно **Новое правило** (см. рисунок ниже).

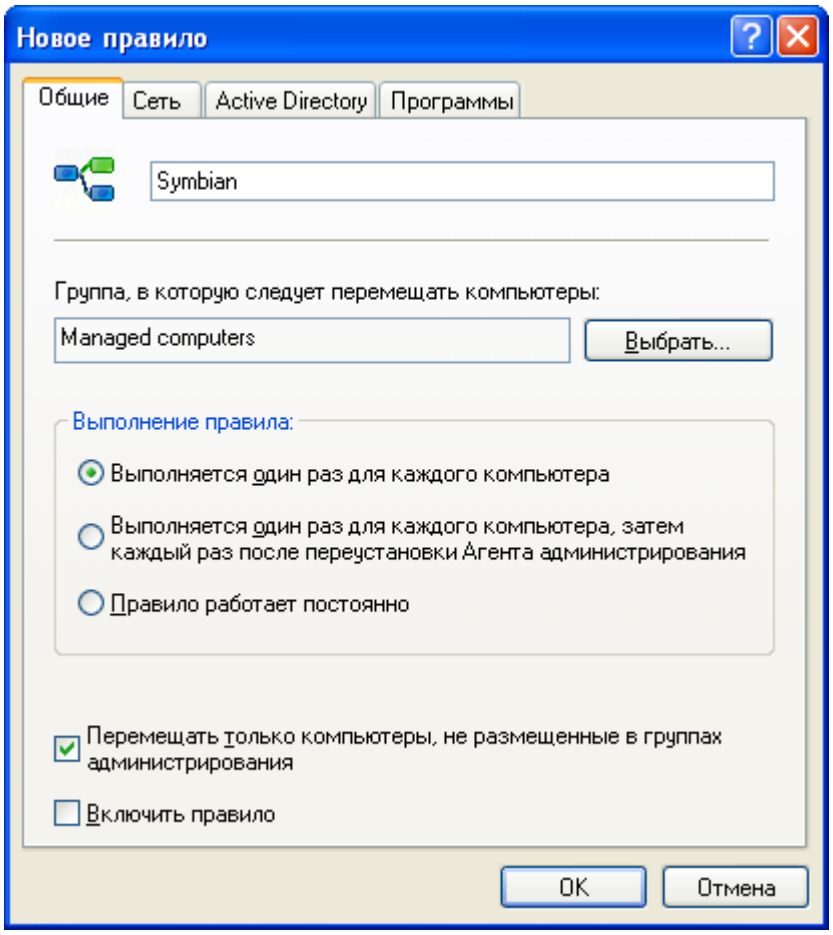


Рисунок 25. Общие параметры перемещения устройств в группу

5. Откройте закладку **Общие** и выполните следующие действия:

   - Введите имя правила.
   - Укажите группу, в которую должны быть перемещены мобильные устройства. Для этого нажмите на кнопку **Выбрать** справа от поля **Группа, в которую следует перемещать компьютеры** и в открывшемся окне выберите группу.
   - В блоке **Выполнение правила** выберите **Выполняется один раз для каждого компьютера**.
   - Установите флажок **Перемещать только компьютеры, не размещенные в группах администрирования**, если устройства, уже входящие в какие-либо группы администрирования, не должны перемещаться в другую группу в результате применения правила.
   - Установите флажок **Включить правило**, чтобы правило применялось.

6. Откройте закладку **Программы** (см. рисунок ниже) и выберите тип операционной системы устройств, которые будут перемещаться в указанную группу: Windows Mobile, Symbian, BlackBerry или Android.

Если вы хотите поместить все устройства в одну группу, независимо от того, какая операционная система на них установлена, сформируйте несколько правил, указав в каждом из них одну и ту же группу для размещения устройств.

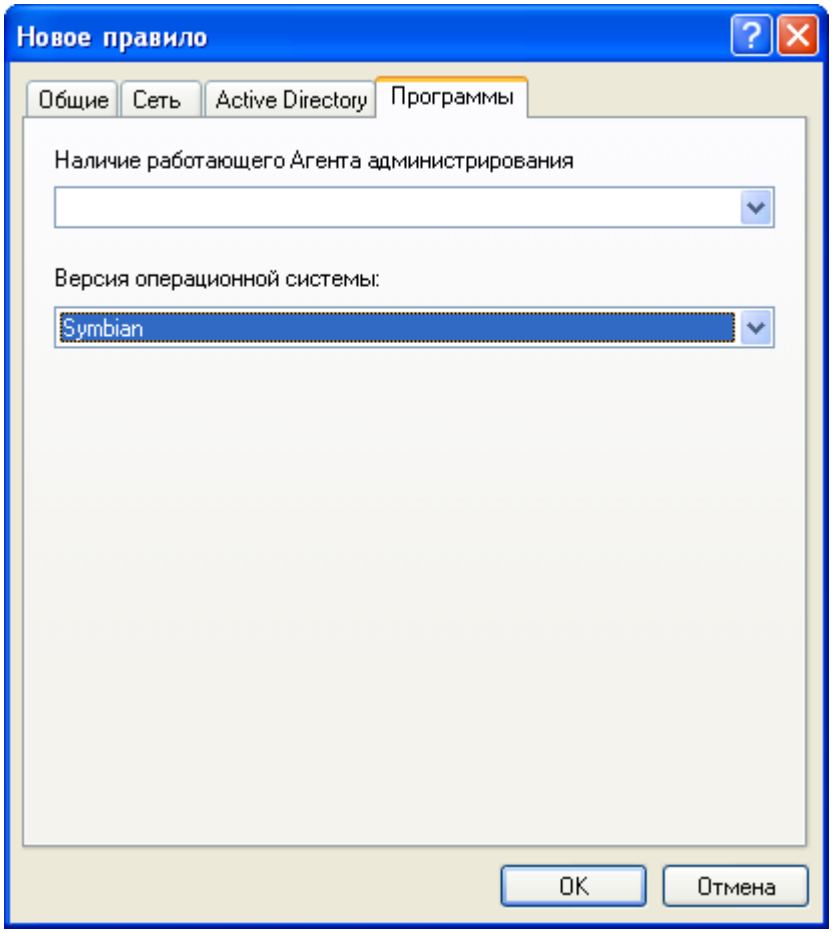


Рисунок 26. Выбор операционной системы устройств

7. Нажмите на кнопку **ОК**. Правило добавляется в список правил перемещения компьютеров (см. закладку **Перемещение компьютеров** в окне настройки параметров Сервера администрирования).

В результате выполнения правила все еще не перемещенные устройства будут перенесены из группы **Нераспределенные компьютеры** в указанную вами группу.

Настройка локальных параметров программы

Система администрирования Kaspersky Administration Kit предоставляет возможность удаленного управления локальными параметрами программы Kaspersky Endpoint Security 8 for Smartphone на мобильных устройствах через Консоль администрирования. С помощью локальных параметров программы можно установить на устройстве индивидуальные значения параметров, отличные от значений параметров, установленных в политике. Если в политике была установлена лицензия, которая рассчитана на меньшее количество устройств, чем содержит группа, то через локальные параметры программы на устройства, для которых не хватило лицензии, можно установить другую лицензию.

Если для параметра в политике был установлен «замок», то заданное в политике значение параметра не может быть изменено ни в локальных параметрах программы, ни на мобильном устройстве. Значение этого параметра может быть изменено только через политику.

Если для параметра в политике «замок» снят, то программа будет использовать одно из следующих значений:

- значение по умолчанию, если другое значение параметра не было указано администратором в локальных параметрах программы или пользователем на мобильном устройстве;
- локальное значение параметра, которое было задано администратором в локальных параметрах программы;
- значение, заданное пользователем на своем мобильном устройстве.

Значения параметров, заданные администратором через консоль в локальных параметрах программы, передаются на мобильное устройство во время синхронизации устройства с Сервером администрирования и сохраняются на устройстве в качестве действующих параметров программы. Если пользователь установит на своем устройстве другие значения параметров, то при очередной синхронизации устройства с Сервером администрирования новые значения параметров будут переданы на сервер и сохранены в локальных параметрах программы вместо значений, которые были установлены ранее администратором.

Чтобы настроить локальные параметры программы, выполните следующие действия:

1. Подключитесь к Серверу администрирования.
2. Выберите в дереве консоли узел **Управляемые компьютеры** и откройте группу с мобильными устройствами, на которых установлена программа Kaspersky Endpoint Security 8 for Smartphone.
3. Выберите мобильное устройство, для которого вы будете менять локальные параметры программы.
4. Откройте контекстное меню устройства и выберите пункт **Свойства**. В результате откроется окно **Свойства: <имя устройства>**, состоящее из нескольких закладок.
5. Выберите закладку **Программы**. На ней в виде таблицы представлен список программ «Лаборатории Касперского», установленных на мобильном устройстве, а также отображена краткая информация о каждой из них.
6. Выберите программу Kaspersky Endpoint Security 8 for Smartphone и нажмите на кнопку **Свойства**. В результате откроется окно **Параметры программы Kaspersky Endpoint Security 8 for Smartphone**.
7. Установите нужные значения параметров программы на закладках **Проверка**, **Защита**, **Обновление**, **Анти-Вор**, **Сеть**, **Дополнительно**, **Лицензия** (см. раздел «**Описание параметров программы Kaspersky Endpoint Security 8 for Smartphone**» на стр. 67).
8. Нажмите на кнопку **ОК**. В результате значения локальных параметров программы сохраняются на Сервере администрирования и передаются на мобильное устройство при очередной синхронизации Сервера администрирования с устройством.

ОПИСАНИЕ ПАРАМЕТРОВ ПРОГРАММЫ KASPERSKY ENDPOINT SECURITY 8 FOR SMARTPHONE

Через свойства политики или свойства мобильного устройства, выбранного в Консоли администрирования, администратор может выполнять удаленную настройку параметров работы Kaspersky Endpoint Security 8 for Smartphone для компонентов Проверка, Защита, Анти-Вор, Сетевой экран, Анти-Спам, Личные контакты и Шифрование.

Кроме этого, администратор обязательно должен настроить параметры подключения устройств к Серверу администрирования и обновления баз программы, а также выполнить установку лицензии. В противном случае программы, установленные на мобильных устройствах, не смогут обмениваться данными с Сервером администрирования и будут работать в режиме ограниченной функциональности.

Если в локальных параметрах программы параметр недоступен для редактирования, то в политике на изменение параметра наложен запрет (параметр сопровождается значком ).

Далее приводится подробное описание закладок окна **Свойства** и элементов интерфейса, с помощью которых администратор может задать параметры работы программы.

В этом разделе

Параметры функции Проверка по требованию

Проверка по требованию помогает выявить и нейтрализовать вредоносные объекты (см. раздел «Проверка по требованию» на стр. 17).

Параметры, заданные администратором, используются как при полной, так и при частичной проверке устройства на присутствие вредоносных объектов. В параметрах проверки по требованию (см. рисунок ниже) администратор может указать типы файлов, которые будут проверяться, выбрать действие, которое будет выполняться при обнаружении зараженного объекта, а также задать расписание, согласно которому программа будет запускать полную проверку файловой системы устройства. Настройка запуска частичной проверки по расписанию через систему удаленного управления не предусмотрена. Частичная проверка устройства по расписанию может быть настроена пользователем непосредственно из программы, установленной на мобильном устройстве.

Проверка по требованию не используется на устройствах с BlackBerry OS.

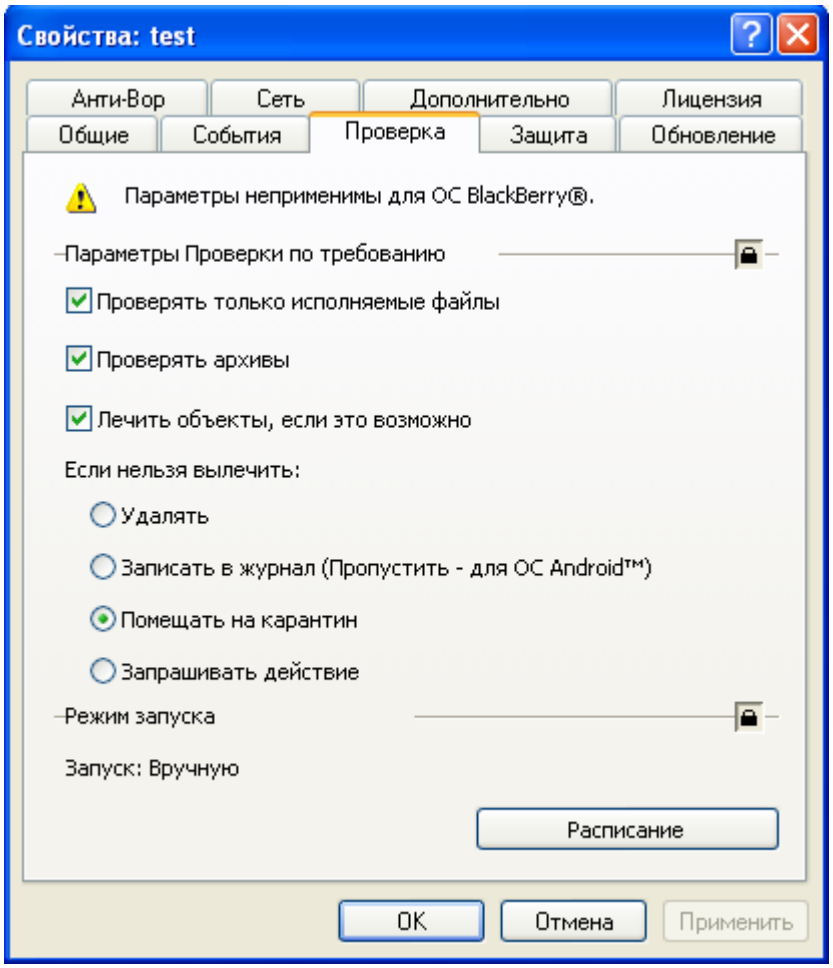


Рисунок 27. Настройка параметров функции Проверка по требованию

Флажок **Проверять только исполняемые файлы**. Если флажок установлен, программа будет проверять только исполняемые файлы следующих форматов: EXE, DLL, MDL, APP, RDL, PRT, PXT, LDD, PDD, CLASS, SO, ELF.

Флажок **Проверять архивы**. Если флажок установлен, программа будет проверять все файлы, включая содержимое архивов. В зависимости от операционной системы программа позволяет проверять архивы следующих форматов:

- для Microsoft Windows Mobile – ZIP, JAR, JAD и CAB;
- для Symbian OS – ZIP, JAR, JAD, SIS и SISX;
- для Android OS – ZIP, JAR, JAD, SIS, SISX, CAB и APK.

Если флажки **Проверять только исполняемые файлы** и **Проверять архивы** не установлены, то программа будет проверять все файлы, кроме файлов в архивах.

Флажок **Лечить объекты, если это возможно**. Если флажок установлен, программа будет лечить излечимые вредоносные объекты. Если лечение невозможно, к объекту будет применяться действие, заданное для зараженных объектов в списке **Если нельзя вылечить**. Если флажок не установлен, то при обнаружении вредоносного объекта будет выполняться действие, заданное в списке **Действие при обнаружении угрозы**.

Список **Если нельзя вылечить** / **Действие при обнаружении угрозы** позволяет выбрать действие, которое будет выполняться при обнаружении вредоносного объекта или при невозможности его лечения:

- **Удалять**. Физически удалять вредоносные объекты без уведомления пользователя.
- **Записать в журнал (Пропустить – для ОС Android)**. Пропускать вредоносные объекты, при этом записывая информацию об их обнаружении в журнал программы; блокировать объект при попытке к нему обратиться (например, скопировать или открыть).

  Для устройств с Android OS программа будет выполнять действие **Пропустить** – пропускать вредоносные объекты, не удалять их с устройства.
- **Помещать на карантин**. Блокировать объект, переместить вредоносный объект в специальную папку – карантин.
- **Запрашивать действие**. При обнаружении вредоносного объекта уведомить пользователя и предложить выбрать действие над обнаруженным объектом.

Выбрать действия при обнаружении угрозы вы можете только при настройке параметров политики (см. раздел «Настройка параметров политики» на стр. 62) и локальных параметров программы (см. раздел «Настройка локальных параметров программы» на стр. 66). Настройка этого параметра не предусмотрена при создании политики (см. раздел «Создание политики» на стр. 52).

Кнопка **Расписание**. Открывает окно, в котором задается расписание полной проверки файловой системы устройства. Вы можете выбрать один из следующих вариантов:

- **Вручную.** Проверка будет запускаться пользователем вручную.
- **Ежедневно**. Проверка будет автоматически запускаться каждый день. В группе полей **Время запуска** укажите время запуска проверки. Время указывается в 24-часовом формате ЧЧ:ММ.
- **Еженедельно.** Проверка будет автоматически запускаться один раз в неделю в определенный день. В раскрывающемся списке выберите день недели, когда проверка будет запускаться, и в группе полей **Время запуска** укажите время запуска проверки. Время указывается в 24-часовом формате ЧЧ:ММ.

Параметры функции Защита

Защита помогает избежать заражения файловой системы мобильного устройства (см. раздел «Защита» на стр. 17). В параметрах защиты администратор может указать типы файлов, которые будут проверяться, выбрать действие, которое будет выполняться при обнаружении зараженного объекта (см. рисунок ниже).

По умолчанию Защита запускается при старте операционной системы устройства – постоянно находится в оперативной памяти устройства и проверяет все открываемые, сохраняемые и запускаемые файлы.

Защита не используется на устройствах с BlackBerry OS.

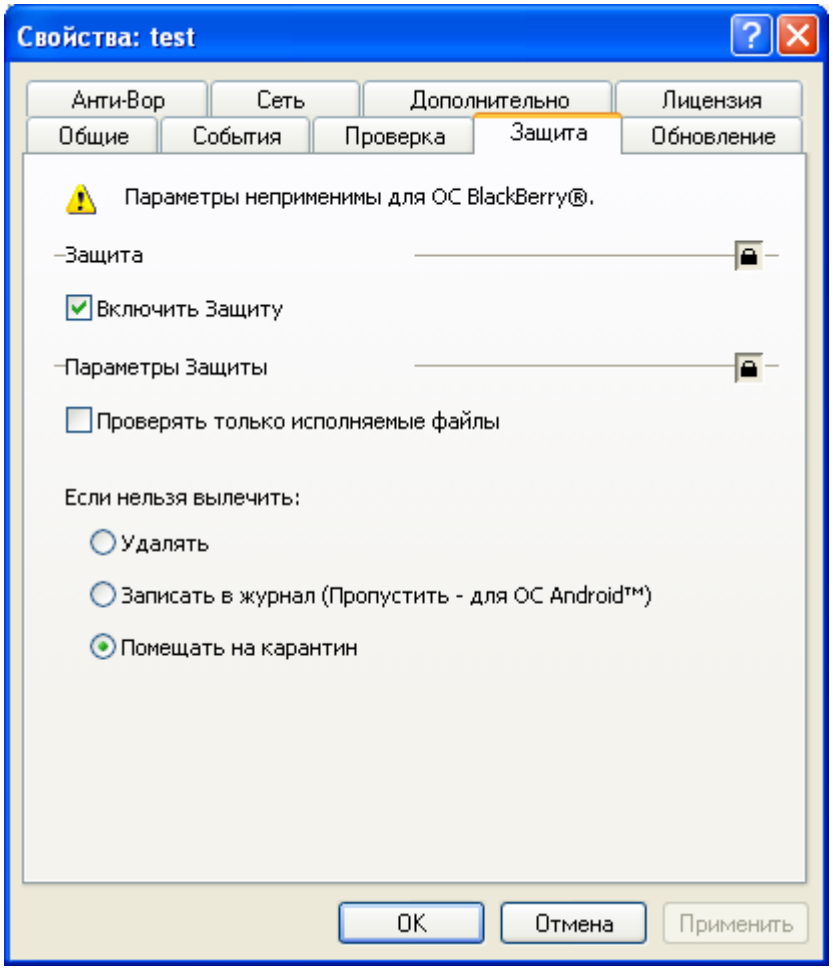


Рисунок 28. Настройка параметров функции Защита

Флажок **Включить Защиту**. Если флажок установлен, программа проверяет все открываемые, запускаемые и сохраняемые файлы. Если флажок снят, Защита отключена. По умолчанию Защита включена.

Блок **Параметры Защиты** позволяет указать типы файлов, которые будут проверяться, и выбрать действие, которое будет выполняться при обнаружении зараженного объекта.

Флажок **Проверять только исполняемые файлы**. Если флажок установлен, программа будет проверять только исполняемые файлы следующих форматов: EXE, MDL, APP, DLL, RDL, PRT, PXT, LDD, PDD, CLASS, SO, ELF. Если флажок снят, программа проверяет файлы всех типов.

Список **Если нельзя вылечить** позволяет выбрать действие, которое будет выполняться при обнаружении зараженного объекта:

- **Удалять**. Физически удалять вредоносные объекты без уведомления пользователя.
- **Записать в журнал (Пропустить – для ОС Android)**. Пропускать вредоносные объекты, при этом записывая информацию об их обнаружении в журнал программы; блокировать объект при попытке к нему обратиться (например, скопировать или открыть).

  Для устройств с Android OS программа будет выполнять действие **Пропустить** – пропускать вредоносные объекты, не удалять их с устройства.
- **Помещать на карантин**. Помещать вредоносные объекты на карантин.

Параметры функции Обновление

Обновление антивирусных баз обеспечивает надежность системы антивирусной защиты мобильных устройств (см. раздел «Обновление» на стр. 18).

Администратор может указать источник обновлений и задать расписание, согласно которому программа будет запускать автоматическое обновление.

По умолчанию в качестве источника обновлений используются серверы обновлений «Лаборатории Касперского». Запуск обновления выполняется вручную пользователем мобильного устройства (см. рисунок ниже).

Обновление антивирусных баз не используется на устройствах с BlackBerry OS.

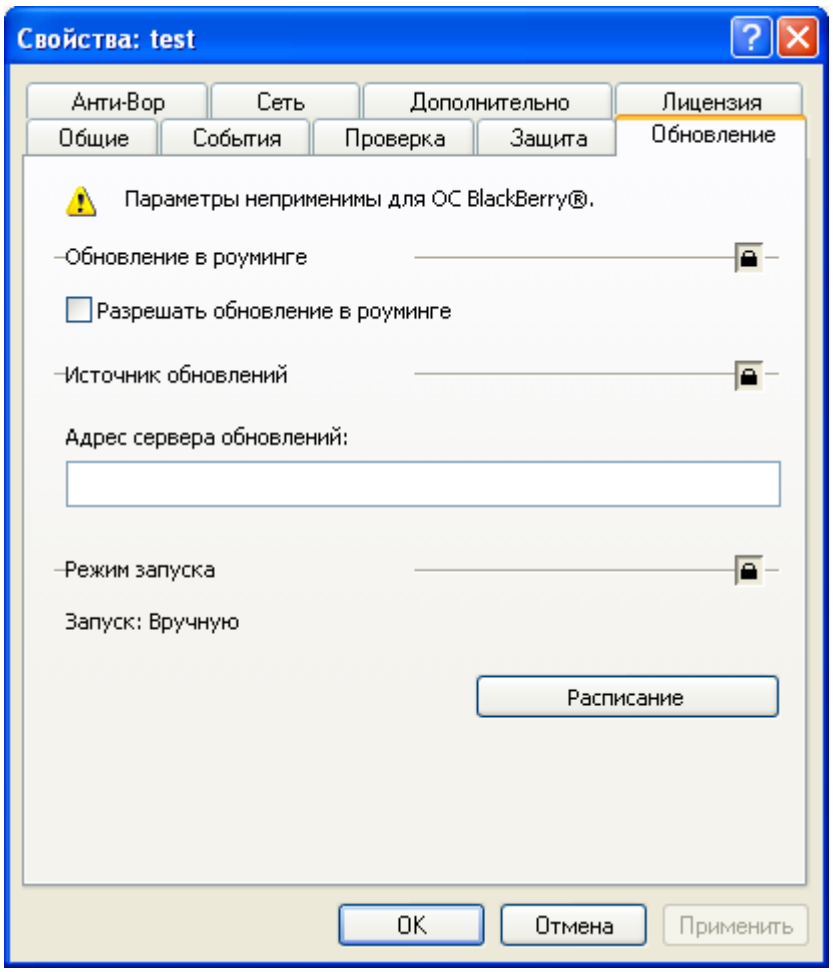


Рисунок 29. Настройка параметров функции Обновление

Флажок **Разрешить обновление в роуминге**. Если флажок установлен, обновление баз программы по расписанию будет также выполняться, когда устройство находится в зоне роуминга. При любом значении параметра пользователь может вручную запустить обновление антивирусных баз. По умолчанию флажок снят.

Возможность разрешать обновление в роуминге не поддерживается для устройств с Android OS.

В блоке **Источник обновлений** указывается адрес сервера, с которого будут копироваться обновления. Для того чтобы обновления производились с серверов обновлений «Лаборатории Касперского», в поле **Адрес сервера обновлений** введите `KLServers`.

При использовании для обновления баз программы какого-либо другого сервера обновлений в блоке **Источник обновлений** указывается HTTP-сервер, локальная или сетевая папка. Например, http://domain.com/index/.

Структура папок в источнике обновлений должна совпадать с аналогичной структурой на серверах обновлений «Лаборатории Касперского».

Кнопка **Расписание**. Открывает окно, в котором задается расписание обновления баз программы. Вы можете выбрать один из следующих вариантов:

- **Вручную**. Обновление баз программы будет запускаться пользователем вручную.
- **Ежедневно**. Обновление баз программы будет автоматически запускаться каждый день. В группе полей **Время запуска** укажите время запуска обновления.
- **Еженедельно**. Обновление баз программы будет автоматически запускаться один раз в неделю в определенный день. В раскрывающемся списке выберите день недели, когда будет запускаться обновление, и в группе полей **Время запуска** укажите время запуска обновления.

Независимо от того, сформировал администратор расписание автоматического обновления баз или нет, пользователь всегда может запустить обновление вручную.

ПАРАМЕТРЫ КОМПОНЕНТА АНТИ-ВОР

Компонент Анти-Вор обеспечивает защиту информации, хранящейся на мобильных устройствах пользователей, от несанкционированного доступа (см. раздел «Анти-Вор» на стр. 19). Администратор может включить или отключить использование функций компонента Анти-Вор на мобильных устройствах пользователей и настроить параметры этих функций (см. рисунок ниже).

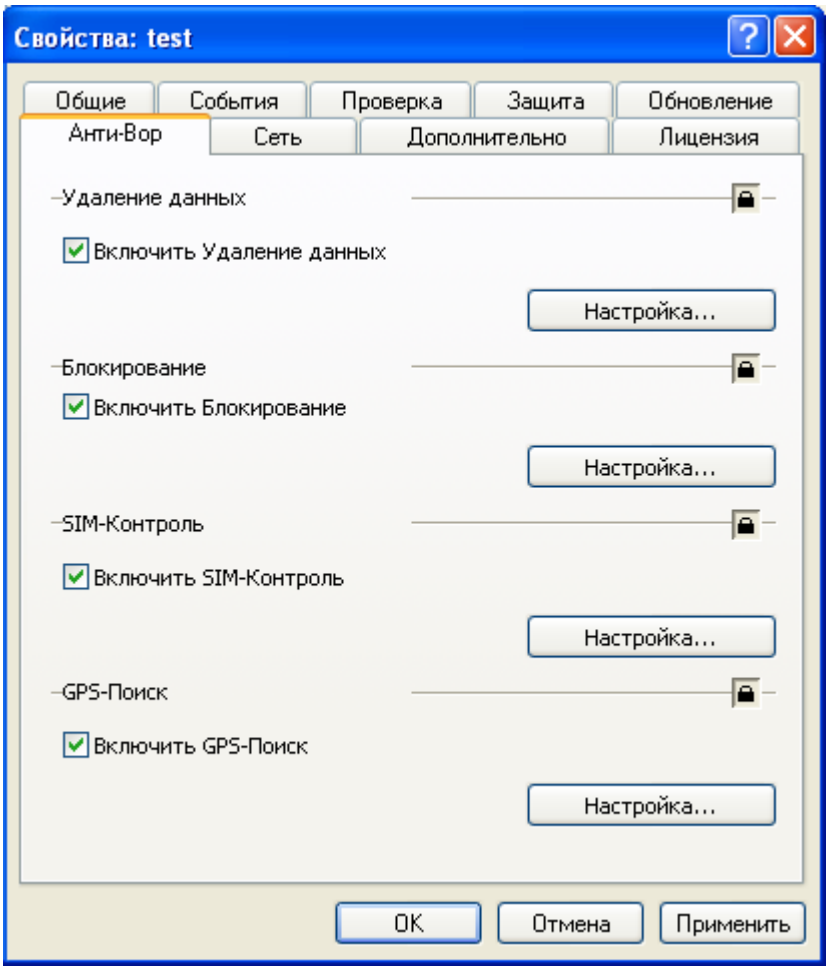


Рисунок 30. Настройка параметров компонента Анти-Вор

Флажок **Включить Удаление данных**. Если флажок установлен, то будет включена возможность дистанционно удалять данные, а также выбрать данные, которые будут удалены. По умолчанию функция Удаление данных отключена. Кнопка **Настройка** справа от флажка открывает окно **Параметры Удаления данных**, в котором вы можете настроить параметры функции (см. раздел «Параметры функции Удаление данных» на стр. 75).

Флажок **Включить Блокирование**. Если флажок установлен, то будет включена возможность дистанционно заблокировать доступ к устройству и данным, хранящимся на нем. По умолчанию функция Блокирование отключена. Кнопка **Настройка** справа от флажка открывает окно, в котором вы можете настроить параметры функции (см. раздел «Параметры функции Блокирование» на стр. 77).

Для работы функции Блокирование на устройстве с Android OS версии 2.2 и выше требуется, чтобы программа Kaspersky Endpoint Security 8 for Smartphone была установлена главным экраном по умолчанию.

Если на устройстве с Android OS версии 2.2 и выше программа не установлена главным экраном по умолчанию, то Kaspersky Endpoint Security 8 for Smartphone выполнит действия в зависимости от следующих условий:

- Если параметры программы заблокированы, то после их передачи на устройство функция Блокирование включится. При этом защиту устройства при срабатывании функции гарантировать будет невозможно. При синхронизации с Kaspersky Administration Kit программа отправит событие **Устройство не может быть заблокировано**. При каждом запуске программы или синхронизации устройства с Kaspersky Administration Kit программа будет предлагать пользователю установить Kaspersky Endpoint Security 8 for Smartphone главным экраном по умолчанию.

  Когда пользователь установит программу главным экраном по умолчанию, при следующей синхронизации устройства с Kaspersky Administration Kit программа отправит событие **Блокирование включено**.

- Если параметры программы разрешены для изменения, то после их передачи на устройство функция Блокирование не включится. При синхронизации устройства с Kaspersky Administration Kit программа отправит событие **Блокирование отключено**.

Флажок **Включить SIM-Контроль**. Если флажок установлен, Kaspersky Endpoint Security 8 for Smartphone блокирует мобильное устройство в случае смены SIM-карты или при включении без нее. Пользователь может задать телефонный номер и (или) адрес электронной почты, на которые будет отправлен новый номер телефона, а также включить блокирование устройства при смене SIM-карты. Для настройки этой функции необходимо задать номер телефона и (или) адрес электронной почты, на которые в случае смены SIM-карты на устройстве будет отправлен текущий номер телефона. По умолчанию функция SIM-Контроль отключена. Кнопка **Настройка** справа от флажка открывает окно **Параметры SIM-Контроля**, в котором вы можете настроить параметры функции (см. раздел «Параметры функции SIM-Контроль» на стр. 77).

Флажок **Включить GPS-Поиск**. Если флажок установлен, Kaspersky Endpoint Security 8 for Smartphone позволяет определить географические координаты устройства и позволяет пользователю получить их с помощью SMS на запрашивающее устройство или на определенный адрес электронной почты. Для настройки этой функции необходимо задать адрес электронной почты, на который программа при получении SMS-команды будет отправлять географические координаты устройства. По умолчанию программа отправляет координаты устройства в SMS на номер телефона, с которого отправлена специальная SMS-команда. По умолчанию функция GPS-Поиск отключена. Кнопка **Настройка** справа от флажка открывает окно, в котором вы можете настроить параметры функции GPS-Поиск.

ПАРАМЕТРЫ ФУНКЦИИ УДАЛЕНИЕ ДАННЫХ

Настройка параметров функции Удаление данных выполняется в окне **Параметры Удаления данных** (см. рисунок ниже).

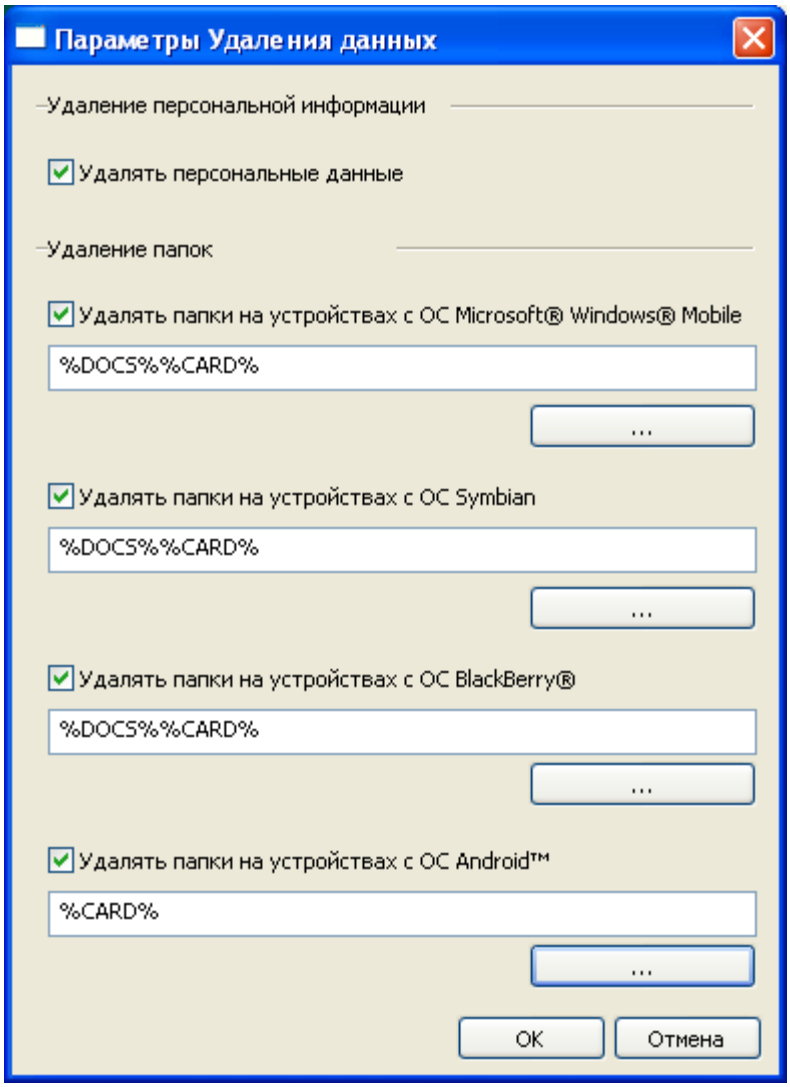


Рисунок 31. Настройка параметров функции Удаление данных

Флажок **Удалять персональные данные**. Для устройств с операционной системой Microsoft Windows Mobile и Symbian программа позволяет удалить следующую информацию: записи в Контактах и на SIM-карте, SMS, галерею, календарь, параметры подключения к интернету. Для устройств с операционной системой BlackBerry программа удаляет следующую персональную информацию: записи в Контактах, календарь, сообщения электронной почты, журнал вызовов. Для устройств с операционной системой Android программа удаляет следующие персональные данные пользователя: записи в Контактах и на SIM-карте, SMS, журнал вызовов, календарь, параметры подключения к интернету, учетные записи пользователя, кроме учетной записи Google™. Функция активизируется, когда на устройстве получена специальная SMS-команда.

Если флажок установлен, после получения специальной SMS-команды персональные данные будут удалены. Если флажок снят, после получения специальной SMS-команды персональные данные не будут удалены.

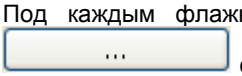
По умолчанию флажок **Удалять персональные данные** установлен.

Блок **Удаление папок** (см. рисунок выше). Программа позволяет настроить удаление папок на мобильном устройстве в случае получения мобильным устройством специальной SMS-команды.

При настройке параметров политики параметры удаления папок определяются для каждой операционной системы отдельно, и блок **Удаление папок** содержит следующие флажки:

- **Удалять папки на устройствах с ОС Microsoft Windows Mobile**. Удаление заданных администратором и пользователем папок на устройствах с операционной системой Microsoft Windows Mobile.
- **Удалять папки на устройствах с ОС Symbian**. Удаление заданных администратором и пользователем папок на устройствах с операционной системой Symbian.
- **Удалять папки на устройствах с ОС BlackBerry**. Удаление заданных администратором и пользователем папок на устройствах с операционной системой BlackBerry.
- **Удалять папки на устройствах с ОС Android**. Удаление заданных администратором и пользователем папок на устройствах с операционной системой Android.

Если флажок установлен, после получения специальной SMS-команды на мобильном устройстве будут удалены папки, заданные администратором, и папки, заданные пользователем. Если флажок снят, папки удаляться не будут.

Под каждым флажком расположено поле для формирования списка папок для удаления. Кнопка 

справа от поля открывает окно, в котором администратор может сформировать список папок для удаления. При этом могут быть указаны папки, расположенные в памяти устройства либо на карте памяти. По умолчанию список папок для удаления пуст.

При формировании списка папок администратор может использовать следующие макросы:

- Для устройств с операционной системой Microsoft Windows Mobile:
  - %DOCS% – папка **Мои документы** (точное название зависит от локализации устройства);
  - %CARD% – все доступные карты памяти в системе.
- Для устройств с операционной системой Symbian:
  - %DOCS% – папка **C:\Data**;
  - %CARD% – все доступные карты памяти в системе.
- Для устройств с операционной системой BlackBerry:
  - %DOCS% – папка **\store\home\user\documents**;
  - %CARD% – карта расширения памяти (**\SDCard**).
- Для устройств с операционной системой Android макрос %CARD% – карта расширения памяти (**\SDCard**).

При настройке локальных параметров программы через Консоль администрирования в окне **Параметры Удаления данных** представлены параметры, определяющие удаление данных на отдельном устройстве, поэтому блок **Удаление папок** представлен только одним флажком **Удалять папки** и полем ввода списка папок для удаления (см. рисунок выше). При этом список папок для удаления доступен только для просмотра. Изменить список папок для удаления администратор может только в параметрах политики.

Внимание! Чтобы отменить удаление ранее заданных папок, администратор должен удалить всю информацию, расположенную в поле ввода под флажком **Удалять папки на устройствах с ОС Microsoft Windows Mobile** / **Удалять папки на устройствах с ОС Symbian** / **Удалять папки на устройствах с ОС BlackBerry** / **Удалять папки на устройствах с ОС Android**, и обеспечить передачу параметров на мобильные устройства пользователей. Для этого в окне настройки параметров политики на закладке **Анти-Вор** в блоке **Удаление данных** должен быть установлен «замок».

ПАРАМЕТРЫ ФУНКЦИИ БЛОКИРОВАНИЕ

Настройка параметров функции Блокирование выполняется в окне **Параметры Блокирования** (см. рисунок ниже).

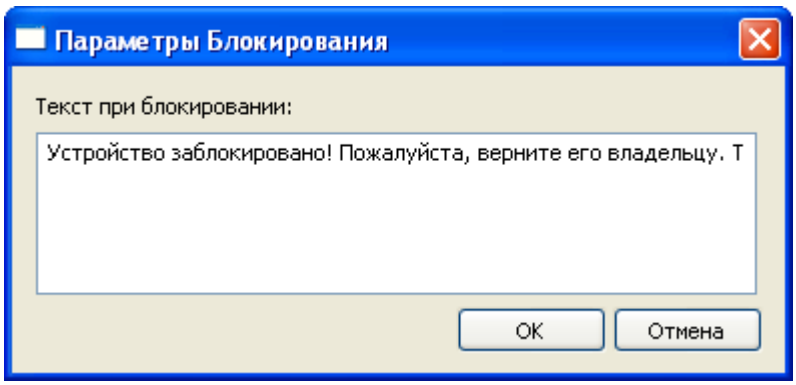


Рисунок 32. Настройка параметров функции Блокирование

Текст при блокировании. Текст сообщения, которое будет отображаться на экране заблокированного устройства. По умолчанию введен стандартный текст.

ПАРАМЕТРЫ ФУНКЦИИ SIM-КОНТРОЛЬ

Настройка параметров функции SIM-Контроль выполняется в окне **Параметры SIM-Контроля** (см. рисунок ниже).

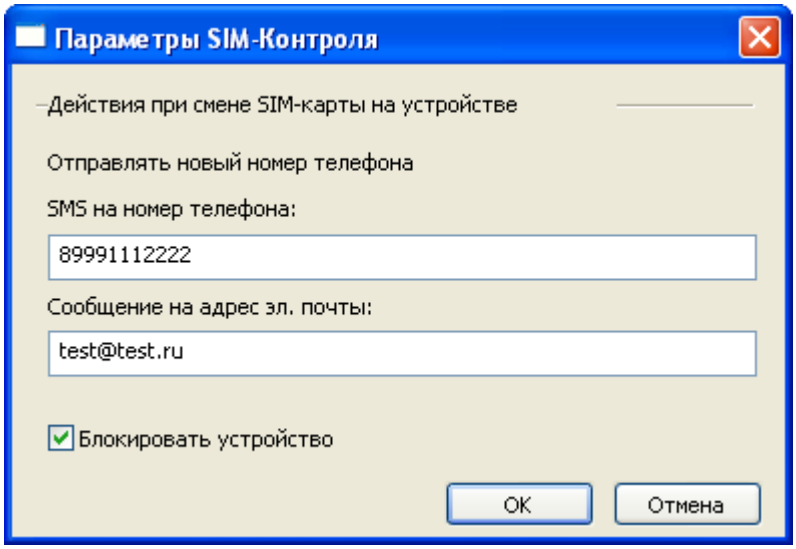


Рисунок 33. Настройка параметров функции SIM-Контроль

SMS на номер телефона. В поле указывается номер, на который при смене SIM-карты программа отправляет SMS с новым номером телефона. Номер может начинаться с цифры или со знака «+» и должен содержать только цифры. Рекомендуется указывать номер в формате, который использует ваш оператор сотовой связи.

Сообщение на адрес эл. почты. В поле указывается адрес электронной почты, на который при смене SIM-карты программа отправляет сообщение с новым номером телефона.

Блокировать устройство. Блокирование устройства при смене SIM-карты или при включении без нее. Если флажок установлен, SIM-Контроль будет блокировать устройство при смене SIM-карты. Чтобы разблокировать устройство, пользователю устройства потребуется ввести секретный код программы. Если флажок снят, SIM-Контроль не будет блокировать устройство при смене SIM-карты. Вы можете также указать текст, который будет отображаться на экране устройства в заблокированном состоянии. По умолчанию введен стандартный текст.

Параметры функции GPS-Поиск

Настройка параметров функции GPS-Поиск выполняется в окне GPS-Поиск (см. рисунок ниже).

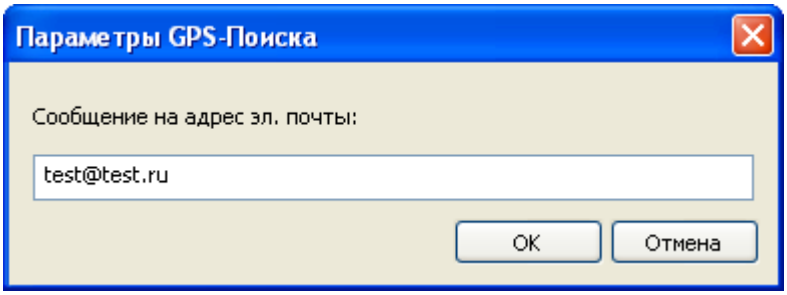


Рисунок 34. Настройка параметров функции GPS-Поиск

Сообщение на адрес эл. почты. Адрес электронной почты, на который программа при получении SMS-команды будет отправлять географические координаты устройства. По умолчанию программа отправляет координаты устройства в SMS на номер телефона, с которого отправлена специальная SMS-команда.

ПАРАМЕТРЫ КОМПОНЕНТА СЕТЕВОЙ ЭКРАН

Сетевой экран контролирует сетевые соединения на мобильных устройствах пользователей (см. раздел «Сетевой экран» на стр. 21). Администратор может задать для компонента Сетевой экран уровень защиты, который будет установлен на мобильных устройствах пользователей. Параметры компонента Сетевой экран представлены на закладке **Сеть** (см. рисунок ниже).

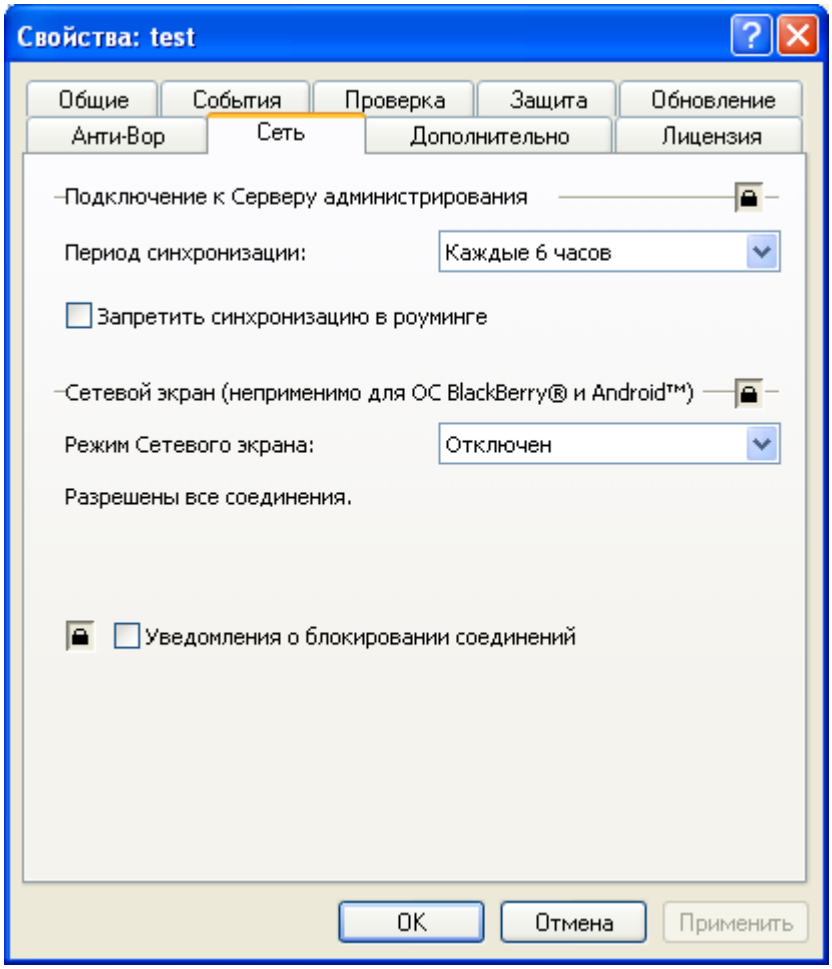


Рисунок 35. Настройка параметров компонента Сетевой экран и параметров синхронизации с Сервером администрирования

Компонент Сетевой экран не используется на устройствах с BlackBerry OS и Android OS.

Блок **Сетевой экран (неприменимо для ОС BlackBerry и Android)** позволяет настроить параметры компонента Сетевой экран:

- Раскрывающийся список **Режим Сетевого экрана** позволяет выбрать один из следующих режимов:
  - **Отключен** – разрешение любой сетевой активности. Сетевой экран отключен.
  - **Минимальная защита** – блокирование только входящих соединений. Исходящие соединения разрешены.

- **Максимальная защита** – блокирование всех входящих соединений. Пользователю доступны проверка почты, просмотр веб-сайтов, скачивание файлов. Исходящие соединения могут осуществляться только по портам SSH, HTTP, HTTPS, IMAP, SMTP, POP3.

- **Блокировать все** – блокирование любой сетевой активности, кроме обновления антивирусных баз и подключения к Серверу администрирования.

По умолчанию Сетевой экран не используется, для параметра **Режим Сетевого экрана** установлено значение **Отключен**.

- Флажок **Уведомления о блокировании соединений**. Если флажок установлен, программа уведомляет пользователя о блокировании соединения. Если флажок снят, программа согласно выбранному режиму блокирует соединение без уведомления пользователя.

  По умолчанию уведомления Сетевого экрана отключены.

Параметры синхронизации устройств с Сервером администрирования

Синхронизация мобильных устройств с Сервером администрирования обеспечивает управление мобильными устройствами через Kaspersky Administration Kit (см. раздел «Концепция управления программой через Kaspersky Administration Kit» на стр. 27). Администратор может установить параметры синхронизации устройств с Сервером администрирования на закладке **Сеть** (см. рисунок ниже).

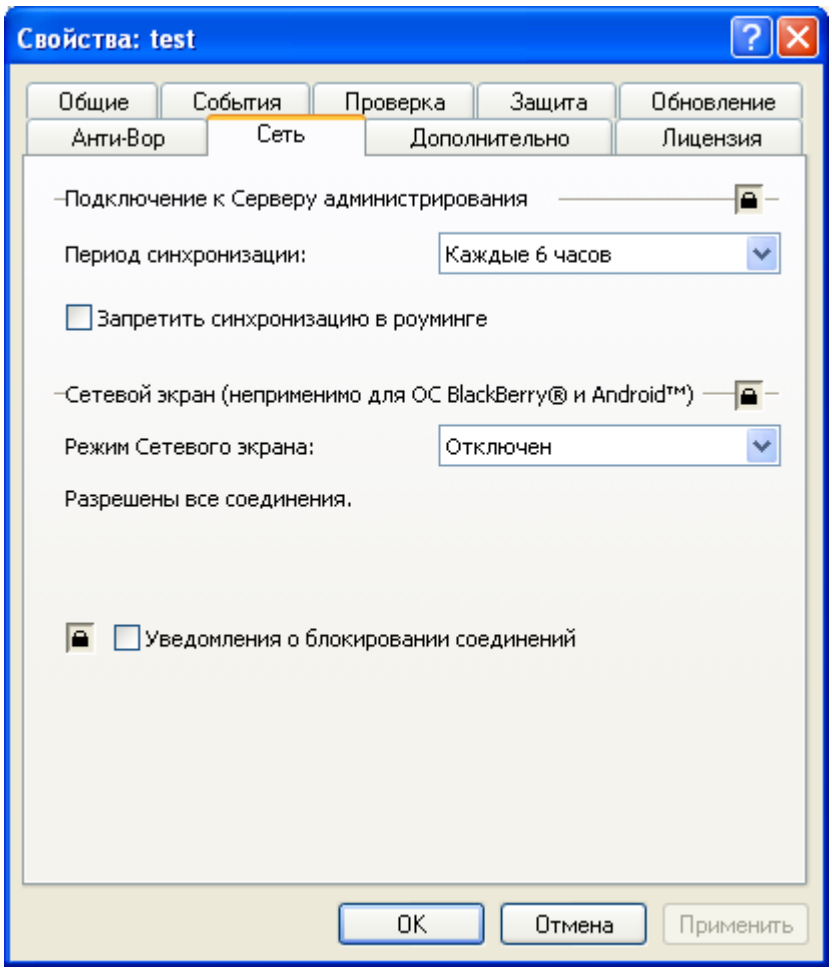


Рисунок 36. Настройка параметров компонента Сетевой экран и параметров синхронизации с Сервером администрирования

Блок **Подключение к Серверу администрирования** позволяет настроить следующие параметры синхронизации:

- **Период синхронизации**. В поле указывается, с какой периодичностью должна выполняться синхронизация мобильных устройств с Сервером администрирования.

  По умолчанию синхронизация выполняется каждые 6 часов.

- Флажок **Запретить синхронизацию в роуминге**. Если флажок установлен, то будет запрещена автоматическая синхронизация с Сервером администрирования, когда устройство находится в зоне роуминга. При этом пользователь может выполнять синхронизацию вручную.

  По умолчанию автоматическая синхронизация мобильных устройств с Сервером администрирования в роуминге разрешена, флажок снят.

  Запрет синхронизации в роуминге не поддерживается для устройств с Android OS.

ПАРАМЕТРЫ КОМПОНЕНТОВ АНТИ-СПАМ И ЛИЧНЫЕ КОНТАКТЫ

Компонент Анти-Спам предотвращает доставку нежелательных вызовов и SMS на основе сформированных пользователем «черного» и «белого» списков (см. раздел «Анти-Спам» на стр. 20). Компонент Личные контакты скрывает конфиденциальную информацию пользователя: записи в Контактах, входящие, исходящие, переданные SMS и записи в журнале вызовов (см. раздел «Личные контакты» на стр. 20).

Администратор может определить доступность компонентов Анти-Спам и Личные контакты пользователям мобильных устройств на закладке **Дополнительно** (см. рисунок ниже). Если использование компонентов разрешено, настройку параметров для этих компонентов пользователь выполняет самостоятельно.

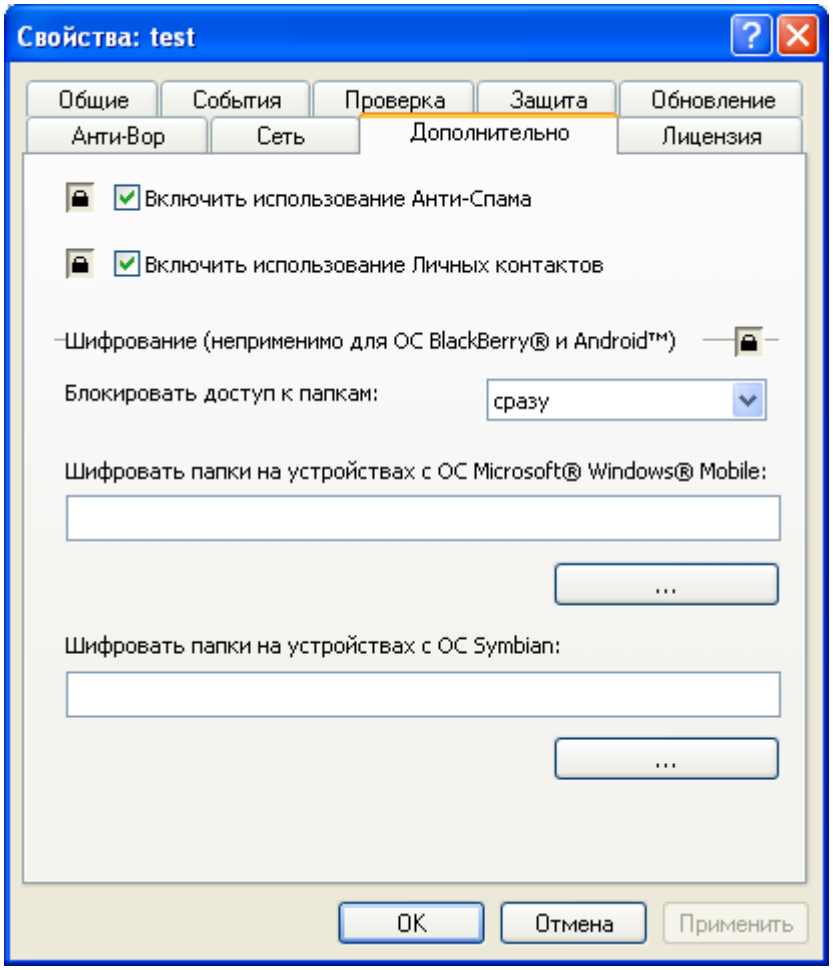


Рисунок 37. Настройка параметров компонентов Анти-Спам, Личные контакты и Шифрование

Параметры компонентов Анти-Спам и Личные контакты представлены на закладке **Дополнительно**:

- Флажок **Включить использование Анти-Спама**. Если флажок установлен, то пользователю будет разрешено использовать на своем мобильном устройстве компонент Анти-Спам и настраивать его параметры. Если использование Анти-Спама запрещено, компонент на устройстве недоступен пользователю.

  По умолчанию использование компонента Анти-Спам разрешено.

- Флажок **Включить использование Личных контактов**. Если флажок установлен, то пользователю будет разрешено использовать на своем мобильном устройстве компонент Личные контакты и настраивать его параметры. Если использование Личных контактов запрещено, компонент на устройстве недоступен пользователю.

  По умолчанию использование компонента Личные контакты разрешено.

  Компонент Личные контакты не поддерживается на устройствах с BlackBerry OS.

ПАРАМЕТРЫ КОМПОНЕНТА ШИФРОВАНИЕ

Компонент Шифрование шифрует информацию из заданного списка папок для шифрования (см. раздел «Шифрование» на стр. 21).

Администратор может задать время, через которое после перехода устройства в режим энергосбережения доступ к зашифрованным папкам будет запрещен, и определить, какие папки будут при этом шифроваться. Настройка параметров шифрования выполняется на закладке **Дополнительно** (см. рисунок ниже).

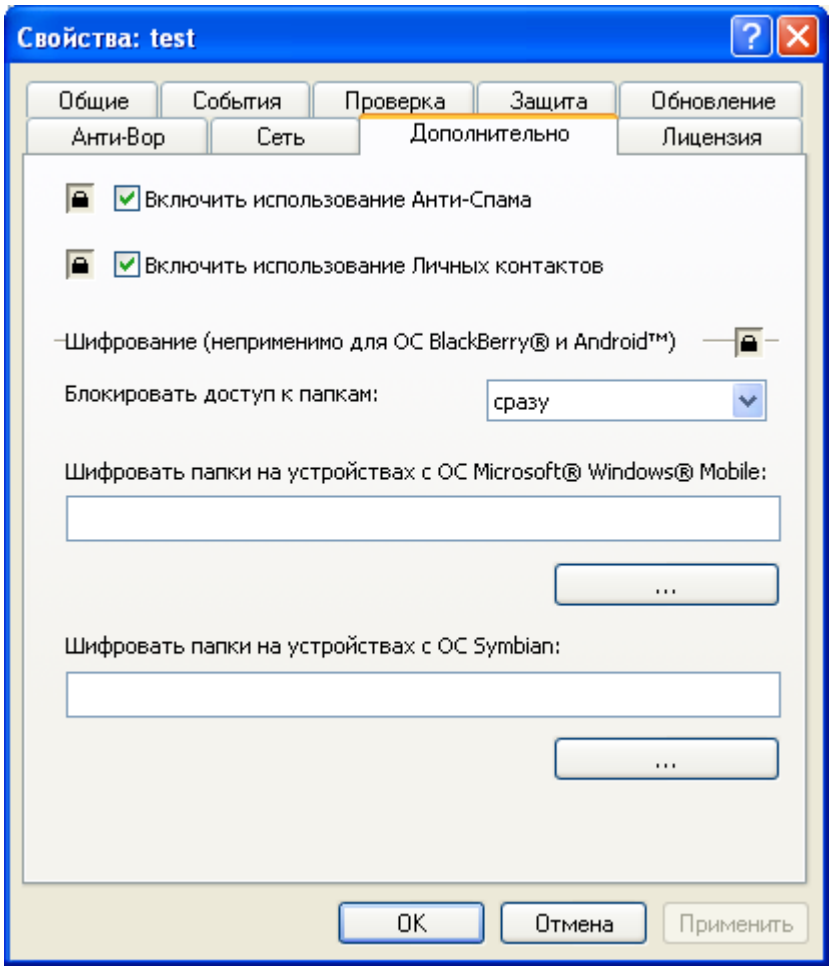


Рисунок 38. Настройка параметров компонентов Анти-Спам, Личные контакты и Шифрование

Компонент Шифрование не поддерживается на устройствах с операционной системой BlackBerry и Android.

Блок **Шифрование (неприменимо для ОС BlackBerry и Android)** позволяет настроить параметры компонента Шифрование:

- **Блокировать доступ к папкам**. В списке выбирается период времени, через который доступ к используемым зашифрованным папкам будет запрещен. Функция активизируется при переходе устройства в режим энергосбережения.

  По умолчанию доступ к используемым зашифрованным папкам блокируется сразу после перехода устройства в режим энергосбережения. Для параметра **Блокировать доступ к папкам** выбрано значение **сразу**.

- **Шифровать папки на устройствах с ОС Microsoft Windows Mobile**. Поле содержит список папок, выбранных администратором для шифрования на устройствах с операционной системой Microsoft Windows Mobile. Кнопка  справа от поля открывает окно, в котором администратор может сформировать список папок для шифрования.

- **Шифровать папки на устройствах с ОС Symbian**. Поле содержит список папок, выбранных администратором для шифрования на устройствах с операционной системой Symbian. Кнопка  справа от поля открывает окно, в котором администратор может сформировать список папок для шифрования.

При формировании списка папок администратор может использовать следующие макросы:

- Для устройств с операционной системой Microsoft Windows Mobile:
  - %DOCS% – папка **Мои документы** (точное название зависит от локализации устройства);
  - %CARD% – все доступные карты памяти в системе.
- Для устройств с операционной системой Symbian:
  - %DOCS% – папка **C:\Data**;
  - %CARD% – все доступные карты памяти в системе.

Пользователь не может отменить шифрование папок, заданных администратором, но может дополнительно указать папки для шифрования на своем мобильном устройстве через локальный интерфейс программы. Если администратор не задал папки для шифрования, то будут шифроваться только папки, заданные пользователем.

При редактировании локальных параметров программы через Консоль администрирования список папок для шифрования доступен только для просмотра. Изменить список папок для шифрования администратор может только в параметрах политики.

Чтобы отменить шифрование ранее заданных папок, администратор должен удалить всю информацию, расположенную в поле ввода под флажком **Шифровать папки на устройствах с ОС Microsoft Windows Mobile / Шифровать папки на устройствах с ОС Symbian**, и обеспечить передачу параметров на мобильные устройства пользователей. Для этого в окне настройки параметров политики на закладке **Дополнительно** в блоке **Шифрование (неприменимо для ОС BlackBerry и Android)** должен быть установлен «замок».

Удаление программы

Удаление программы выполняется пользователем вручную на мобильном устройстве.

Для операционных систем Microsoft Windows Mobile и Symbian перед удалением программы на устройстве автоматически будет отключено скрытие конфиденциальной информации и расшифрована вся ранее зашифрованная информация. Для операционных систем BlackBerry и Android перед удалением программы на устройстве пользователь должен вручную отключить скрытие конфиденциальной информации.

Подробно об удалении программы см. в Руководстве пользователя Kaspersky Endpoint Security 8 for Smartphone.

РАЗВЕРТЫВАНИЕ ПРОГРАММЫ ЧЕРЕЗ MS SCMDM

В этом разделе рассмотрен процесс развертывания Kaspersky Endpoint Security 8 for Smartphone через Mobile Device Manager.

В ЭТОМ РАЗДЕЛЕ

Концепция управления программой через MDM

Управление параметрами Kaspersky Endpoint Security 8 for Smartphone через сервер MDM обеспечивает файл административного шаблона endpoint8_ru.adm. Он включен в дистрибутив программы (см. раздел «Схема развертывания программы через MDM» на стр. 86). Для каждого компонента программы (см. раздел «О компонентах Kaspersky Endpoint Security 8 for Smartphone» на стр. 16) в состав административного шаблона входит набор политик, обеспечивающих настройку параметров этого компонента. По умолчанию после установки шаблона управления ни одна политика не задана и пользователь может самостоятельно настраивать параметры программы.

Для компонента Антивирус (см. раздел «Файловый Антивирус» на стр. 16) представлены следующие политики:

- **Защита**. Политика обеспечивает настройку защиты мобильных устройств от вредоносных объектов (см. раздел «Защита» на стр. 17).
- **Проверка по требованию**. Политика обеспечивает настройку проверки мобильных устройств на наличие вредоносных объектов (см. раздел «Проверка по требованию» на стр. 17).
- **Проверка по расписанию**. Политика обеспечивает запуск проверки мобильных устройств по заданному расписанию.
- **Обновление по расписанию**. Политика обеспечивает запуск автоматического обновления баз программы по заданному расписанию (см. раздел «Обновление» на стр. 18).
- **Запрет обновления в роуминге**. Политика позволяет запретить запуск автоматического обновления баз программы, когда мобильные устройства пользователей находятся в зоне роуминга.
- **Источник обновления**. Политика позволяет указать источник обновлений, с которого будет загружаться пакет обновлений на мобильные устройства.

Для компонента Анти-Вор (на стр. 19) представлены следующие политики:

- **Блокирование**. Политика обеспечивает настройку функции Блокирование (на стр. 19).
- **Отображение текста при блокировании устройства**. Политика позволяет указать текст, который будет отображаться на экране заблокированных мобильных устройств.

- **Удаление данных**. Политика обеспечивает настройку функции Удаление данных (на стр. 19).
- **Список папок для удаления**. Политика позволяет сформировать список папок для дистанционного удаления с мобильных устройств.
- **GPS-Поиск**. Политика обеспечивает настройку функции GPS-Поиск (на стр. 20).
- **SIM-Контроль**. Политика обеспечивает настройку функции SIM-Контроль (на стр. 20).

Для компонента Анти-Спам (на стр. 20) представлена политика **Запрет использования Анти-Спама**, с помощью которой можно запретить или разрешить пользователям использовать этот компонент. Если использование Анти-Спама разрешено, пользователь самостоятельно настраивает параметры работы этого компонента на мобильном устройстве.

Для компонента Личные контакты (на стр. 20) представлена политика **Запрет использования Личных контактов**, с помощью которой можно запретить или разрешить пользователям использовать этот компонент. Если использование Личных контактов разрешено, пользователь самостоятельно настраивает параметры работы этого компонента на мобильном устройстве.

Для компонента Шифрование (на стр. 21) представлены следующие политики:

- **Запрет доступа к зашифрованным данным**. Политика позволяет заблокировать доступ к зашифрованным данным.
- **Список папок для шифрования**. Политика позволяет сформировать список папок для шифрования.

Для компонента Сетевой экран (на стр. 21) представлены следующие политики:

- **Режим Сетевого экрана**. Политика обеспечивает настройку уровня безопасности Сетевого экрана.
- **Уведомления Сетевого экрана**. Политика позволяет включить или отключить информирование пользователя о блокировке запрещенных соединений.

Установка лицензии на мобильные устройства пользователей выполняется через административный шаблон с помощью политики **Лицензия**.

С помощью политик администратор настраивает параметры Kaspersky Endpoint Security 8 for Smartphone перед установкой программы и может изменять значения параметров после установки программы.

Обратите внимание, что период синхронизации мобильных устройств с сервером MDM может быть не равен периоду применения политик!

Схема развертывания программы через MDM

В состав дистрибутива Kaspersky Endpoint Security 8 for Smartphone входит самораспаковывающийся архив KES8_forMicrosoftMDM_ru.exe, который содержит следующие файлы, необходимые для установки программы на мобильных устройствах:

- endpoint_MDM_Afaria_8_0_x_xx_ru.cab – установочный файл программы для операционной системы Microsoft Windows Mobile;
- endpoint8_ru.adm – файл административного шаблона управления политиками, содержащий их параметры;
- endpoint8_ca.cer – файл сертификата центра сертификации;
- endpoint8_cert.cer – файл сертификата, которым подписан установочный файл программы;

- kes2mdm.exe – утилита для преобразования файла ключа программы;
- kl.pbv, licensing.dll, oper.pbv – набор файлов, обеспечивающий работу утилиты kes2mdm.exe.

Развертывание Kaspersky Endpoint Security 8 for Smartphone выполняется по стандартной схеме развертывания программного обеспечения через Mobile Device Manager. Вначале необходимо создать объект групповой политики для хранения параметров программы и управления мобильными устройствами. Объект политики создается для группы зарегистрированных устройств Active Directory®, на которые требуется установить программу. Затем выполняется установка административного шаблона в созданном объекте политики. После установки шаблона настраиваются все необходимые параметры программы и устанавливается лицензия. Для распространения программы на мобильные устройства пользователей в консоли Mobile Device Manager Software Distribution создается инсталляционный пакет. Инсталляционный пакет копируется на мобильное устройство при его синхронизации с сервером MDM. После завершения копирования запускается автоматическая установка программы на мобильных устройствах, не требующая вмешательства пользователя.

Таким образом, установка Kaspersky Endpoint Security 8 for Smartphone через Mobile Device Manager состоит из следующих этапов:

1. Установка административного шаблона управления в объекте групповой политики.
2. Настройка параметров программы.
3. Установка лицензии с помощью утилиты преобразования файла ключа.
4. Создание инсталляционного пакета программы и распространение его на мобильные устройства пользователей.
5. Установка программы на мобильных устройствах.

Подготовка к развертыванию программы через MDM

Перед развертыванием Kaspersky Endpoint Security 8 for Smartphone через Mobile Device Manager администратор должен убедиться, что выполнены следующие условия:

1. В сети развернут и настроен Microsoft System Center Mobile Device Manager.
2. Все мобильные устройства пользователей входят в состав сети и зарегистрированы в домене.
3. На сервере MDM установлен и настроен Windows Server Update Services 3.0 SP1.

В этом разделе

О шаблоне управления

Административный шаблон управления Kaspersky Endpoint Security 8 for Smartphone позволяет настроить политики для управления программой. Он представляет собой текстовый файл, в котором хранятся все необходимые параметры программы. Этот файл endpoint8_ru.adm входит в состав дистрибутива программы.

При развертывании Kaspersky Endpoint Security 8 for Smartphone через Mobile Device Manager шаблон управления программой должен быть добавлен в объект групповой политики, созданный в консоли управления. Установка шаблона производится на рабочее место администратора, имеющего права на управление политиками в доменном контроллере.

Язык шаблона управления должен совпадать с языком операционной системы, установленной на рабочем месте администратора!

Вы можете настроить параметры политик для всех компонентов программы (см. раздел «Настройка шаблона управления» на стр. 89).

Установка шаблона управления

- *Чтобы установить шаблон управления Kaspersky Endpoint Security 8 for Smartphone, выполните следующие действия:*

1. В консоли управления (MMC) создайте объект групповой политики.
2. В дереве консоли в узле созданного объекта политики выберите узел **Конфигурация компьютера**, затем группу **Административные шаблоны**.
3. В контекстном меню выберите пункт **Добавление и удаление шаблонов**.
4. В открывшемся окне **Добавление и удаление шаблонов** нажмите на кнопку **Добавить**.
5. В открывшемся окне выберите файл шаблона endpoint8_ru.adm, сохраненный на рабочем месте администратора.
6. В окне **Добавление и удаление шаблонов** нажмите на кнопку **Закрыть**.

В результате в группу **Административные шаблоны** будет добавлена группа **Параметры Kaspersky Endpoint Security 8 for Smartphone**, содержащая группы параметров для каждого компонента программы (см. рисунок ниже).

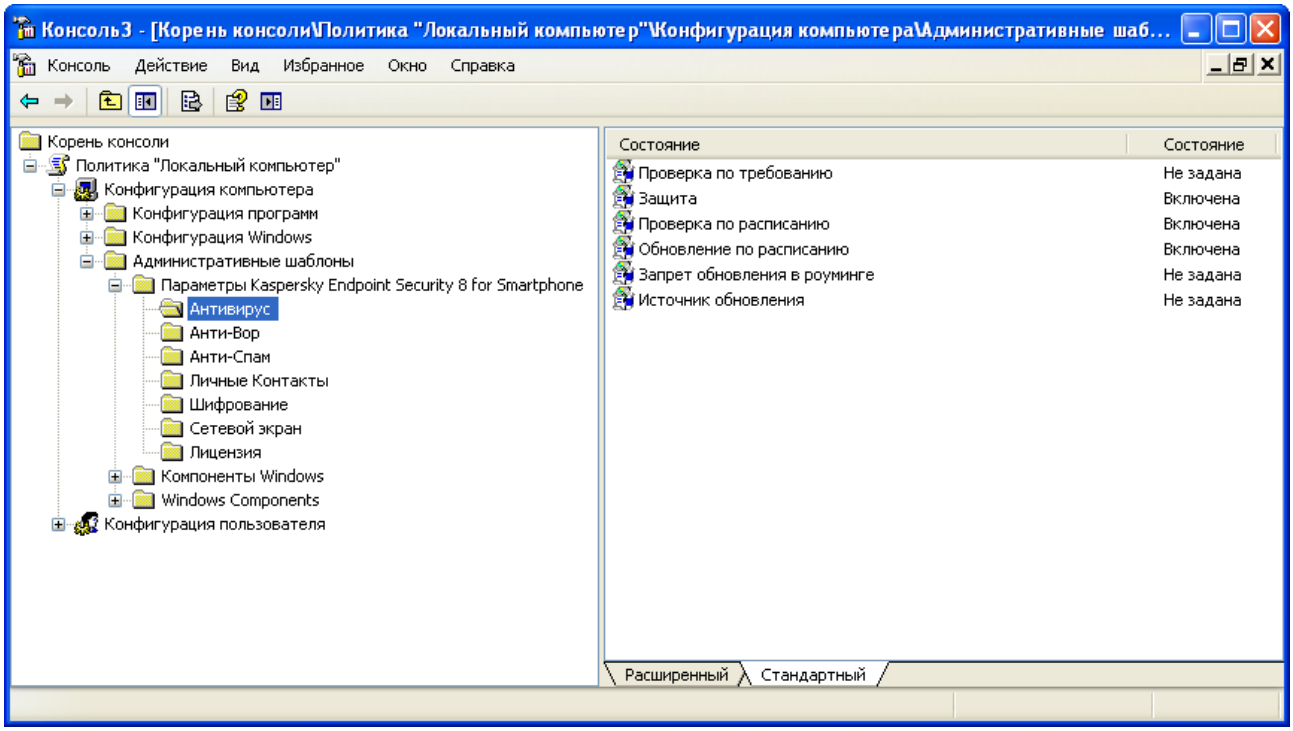


Рисунок 39. Административный шаблон управления

НАСТРОЙКА ШАБЛОНА УПРАВЛЕНИЯ

Все параметры работы Kaspersky Endpoint Security 8 for Smartphone, включая активацию лицензии, определяются через политики. Информация о параметрах программы, заданных в политиках, сохраняется на сервере MDM и распространяется на мобильные устройства в ходе синхронизации.

Чтобы настроить шаблон управления, выполните следующие действия:

1. В дереве консоли управления выберите объект групповой политики, для которого вы хотите настроить параметры Kaspersky Endpoint Security 8 for Smartphone.

2. Выберите узел **Конфигурация компьютера**.

3. Выберите папку **Административные шаблоны**, в ней папку **Параметры Kaspersky Endpoint Security 8 for Smartphone**.

4. Выберите папку с названием компонента программы, параметры которого вы хотите настроить (см. раздел «О компонентах Kaspersky Endpoint Security 8 for Smartphone» на стр. 16).

   В результате в правой части окна консоли управления будут представлены политики, обеспечивающие настройку выбранного компонента (см. раздел «Концепция управления программой через MDM» на стр. 85).

В следующих разделах приведены более подробные процедуры настройки политик для каждого компонента программы.

В этом разделе

Настройка политики Защита

Чтобы настроить политику Защита, выполните следующие действия:

1. В дереве консоли управления выберите папку **Антивирус**.
2. В правой части окна консоли управления выберите политику **Защита**.
3. В контекстном меню политики выберите пункт **Свойства**.

В результате откроется окно **Свойства: Защита** (см. рисунок ниже).

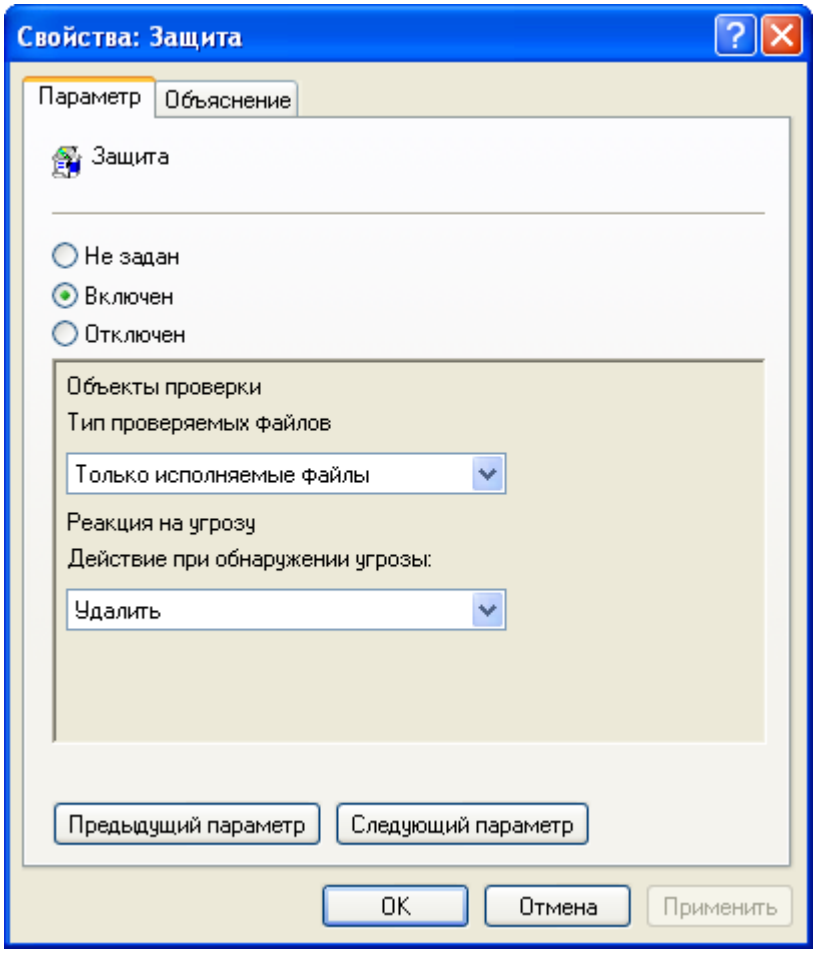


*Рисунок 40. Окно **Свойства: Защита***

4. На закладке **Параметр** выберите один из следующих вариантов:

   - **Не задан**. Компонент / функция включены на мобильном устройстве пользователя. Параметры, определяемые политикой, доступны для редактирования пользователем на мобильном устройстве.

     При этом компонент / функция будет работать с параметрами, заданными пользователем.

   - **Включен**. Компонент / функция включены на мобильном устройстве пользователя. Параметры, определяемые политикой, недоступны для редактирования пользователем на мобильном устройстве. При этом на экране мобильного устройства в левом верхнем углу отображается «замок».

     Компонент / функция будет работать с параметрами, заданными политикой. При выборе этого варианта вы можете настроить параметры политики.

   - **Отключен**. Компонент / функция, определяемые политикой, отключены на мобильном устройстве пользователя. Изменение параметров недоступно. При этом на экране мобильного устройства в левом верхнем углу отображается «замок».

5. В раскрывающемся списке **Тип проверяемых файлов** выберите тип файлов, которые будут проверяться Kaspersky Endpoint Security 8 for Smartphone. Возможные значения:

   - **Все файлы**. Проверяются файлы всех типов.

   - **Только исполняемые файлы**. Проверяются только исполняемые файлы следующих форматов: EXE, DLL, SIS, MDL, APP, RDL, PRT, PXT, LDD, PDD, CLASS.

6. В раскрывающемся списке **Действие при обнаружении угрозы** выберите действие, выполняемое при обнаружении вредоносного объекта. Возможные значения:

   - **Удалить**. Вредоносные объекты удаляются без уведомления пользователя.
   - **Записать в журнал**. Вредоносные объекты остаются без изменений, при этом информация об их обнаружении записывается в журнал программы. При попытке обращения к объекту (например, попытке скопировать или открыть его) доступ к объекту блокируется.
   - **Помещать на карантин**. Обнаруженные зараженные объекты помещаются на карантин.

Настройка политики Проверка по требованию

Чтобы настроить политику Проверка по требованию, выполните следующие действия:

1. В дереве консоли управления выберите папку **Антивирус**.
2. В правой части окна консоли управления выберите политику **Проверка по требованию**.
3. В контекстном меню политики выберите пункт **Свойства**.

   В результате откроется окно **Свойства: Проверка по требованию** (см. рисунок ниже).

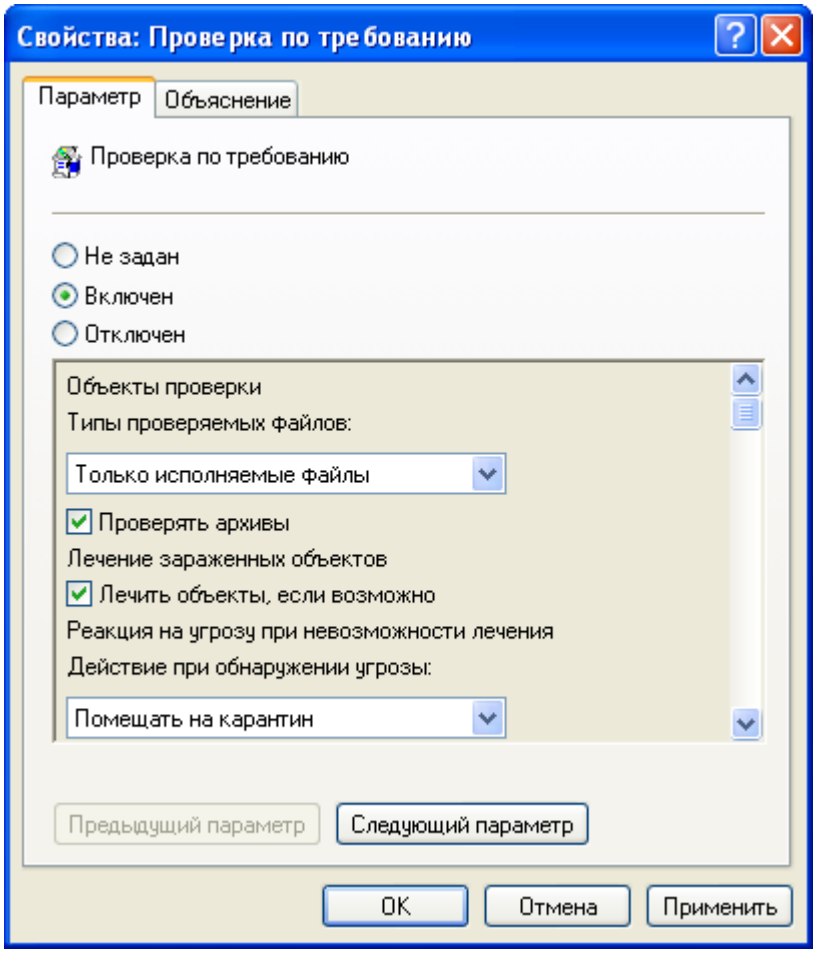


*Рисунок 41. Окно **Свойства: Проверка по требованию***

4. На закладке **Параметр** выберите один из следующих вариантов:

   - **Не задан**. Компонент / функция включены на мобильном устройстве пользователя. Параметры, определяемые политикой, доступны для редактирования пользователем на мобильном устройстве.

     При этом компонент / функция будет работать с параметрами, заданными пользователем.

   - **Включен**. Компонент / функция включены на мобильном устройстве пользователя. Параметры, определяемые политикой, недоступны для редактирования пользователем на мобильном устройстве. При этом на экране мобильного устройства в левом верхнем углу отображается «замок».

     Компонент / функция будет работать с параметрами, заданными политикой. При выборе этого варианта вы можете настроить параметры политики.

   - **Отключен**. Компонент / функция, определяемые политикой, отключены на мобильном устройстве пользователя. Изменение параметров недоступно. При этом на экране мобильного устройства в левом верхнем углу отображается «замок».

5. В раскрывающемся списке **Типы проверяемых файлов** выберите тип файлов, которые будут проверяться Kaspersky Endpoint Security 8 for Smartphone. Возможные значения:

   - **Все файлы**. Проверяются файлы всех типов.

   - **Только исполняемые файлы**. Проверяются только исполняемые файлы следующих форматов: EXE, DLL, SIS, MDL, APP, RDL, PRT, PXT, LDD, PDD, CLASS. При этом архивы не распаковываются и не проверяются.

6. Установите флажок **Проверять архивы**, если вы хотите, чтобы Kaspersky Endpoint Security 8 for Smartphone проверял файлы, запакованные в архив. Проверяются архивы следующих форматов: ZIP, JAR, JAD и CAB.

   Если флажок **Проверять архивы** не установлен и в раскрывающемся списке **Типы проверяемых файлов** выбран вариант **Все файлы**, то программа будет проверять все файлы, кроме файлов, запакованных в архив.

7. Установите флажок **Лечить объекты, если возможно**, чтобы программа лечила вредоносные объекты. Если лечение невозможно, программа выполняет действие, выбранное в раскрывающемся списке **Действие при обнаружении угрозы**.

8. В раскрывающемся списке **Действие при обнаружении угрозы** выберите действие, выполняемое при обнаружении вредоносного объекта. Возможные значения:

   - **Удалять**. Вредоносные объекты удаляются без уведомления пользователя.

   - **Записать в журнал**. Вредоносные объекты остаются без изменений, при этом информация об их обнаружении записывается в журнал программы. При попытке обращения к объекту (например, скопировать или открыть) доступ к нему блокируется.

- **Помещать на карантин**. Обнаруженные зараженные объекты помещаются на карантин. По умолчанию выбрано это действие.
- **Запрашивать действие**. При обнаружении вредоносного объекта выводится уведомление, в котором предлагается выбрать одно из следующих действий:
  - **Пропустить**.
  - **Помещать на карантин**.
  - **Удалить**.
  - **Пытаться лечить**.

Настройка политики Проверка по расписанию

Чтобы настроить политику Проверка по расписанию, выполните следующие действия:

1. В дереве консоли управления выберите папку **Антивирус**.
2. В правой части окна консоли управления выберите политику **Проверка по расписанию**.
3. В контекстном меню политики выберите пункт **Свойства**.

   В результате откроется окно **Свойства: Проверка по расписанию** (см. рисунок ниже).

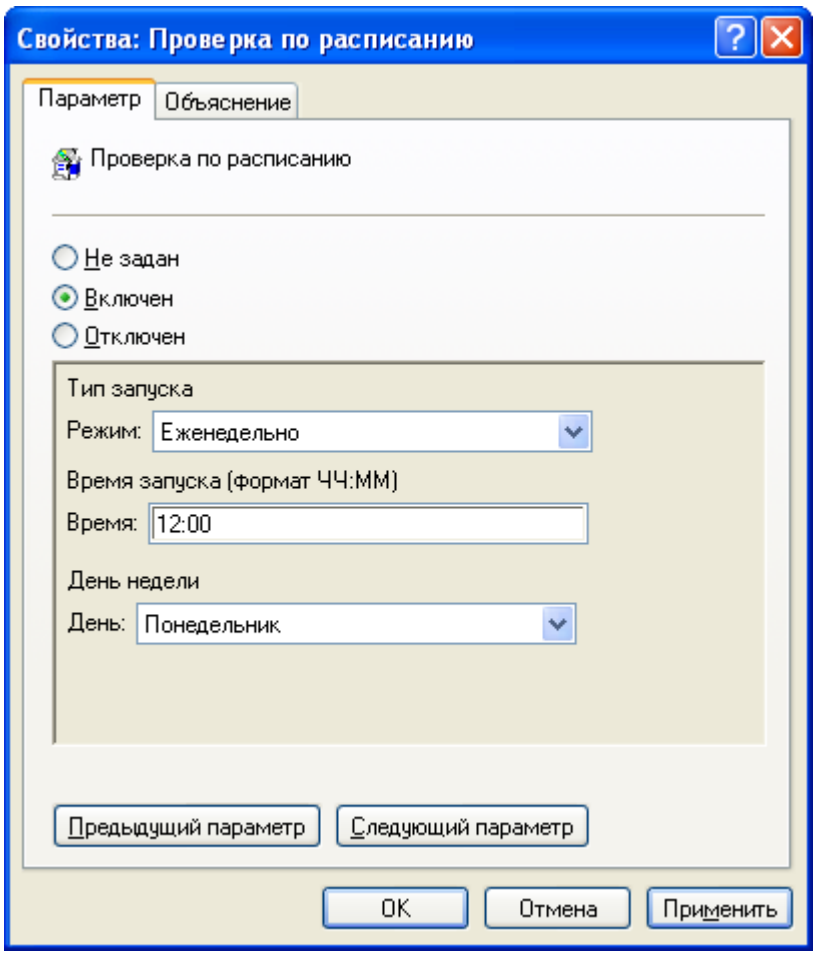


*Рисунок 42. Окно **Свойства: Проверка по расписанию***

4. На закладке **Параметр** выберите один из следующих вариантов:

   - **Не задан**. Компонент / функция включены на мобильном устройстве пользователя. Параметры, определяемые политикой, доступны для редактирования пользователем на мобильном устройстве.

     При этом компонент / функция будет работать с параметрами, заданными пользователем.

   - **Включен**. Компонент / функция включены на мобильном устройстве пользователя. Параметры, определяемые политикой, недоступны для редактирования пользователем на мобильном устройстве. При этом на экране мобильного устройства в левом верхнем углу отображается «замок».

     Компонент / функция будет работать с параметрами, заданными политикой. При выборе этого варианта вы можете настроить параметры политики.

   - **Отключен**. Компонент / функция, определяемые политикой, отключены на мобильном устройстве пользователя. Изменение параметров недоступно. При этом на экране мобильного устройства в левом верхнем углу отображается «замок».

5. В раскрывающемся списке **Режим** выберите режим запуска проверки по требованию. Возможные значения:

   - **Вручную**. Проверка может запускаться пользователем вручную в удобное для него время.

   - **Ежедневно**. Проверка выполняется каждый день в заданное время. Ниже в поле **Время** укажите время запуска в формате ЧЧ:ММ.

   - **Еженедельно**. Проверка выполняется один раз в неделю в указанный день и заданное время. Ниже в раскрывающемся списке **День** выберите день недели, а в поле **Время** – время запуска в формате ЧЧ:ММ.

НАСТРОЙКА ПОЛИТИКИ ОБНОВЛЕНИЕ ПО РАСПИСАНИЮ

Чтобы настроить политику Обновление по расписанию, выполните следующие действия:

1. В дереве консоли управления выберите папку **Антивирус**.

2. В правой части окна консоли управления выберите политику **Обновление по расписанию**.

3. В контекстном меню политики выберите пункт **Свойства**.

В результате откроется окно **Свойства: Обновление по расписанию** (см. рисунок ниже).

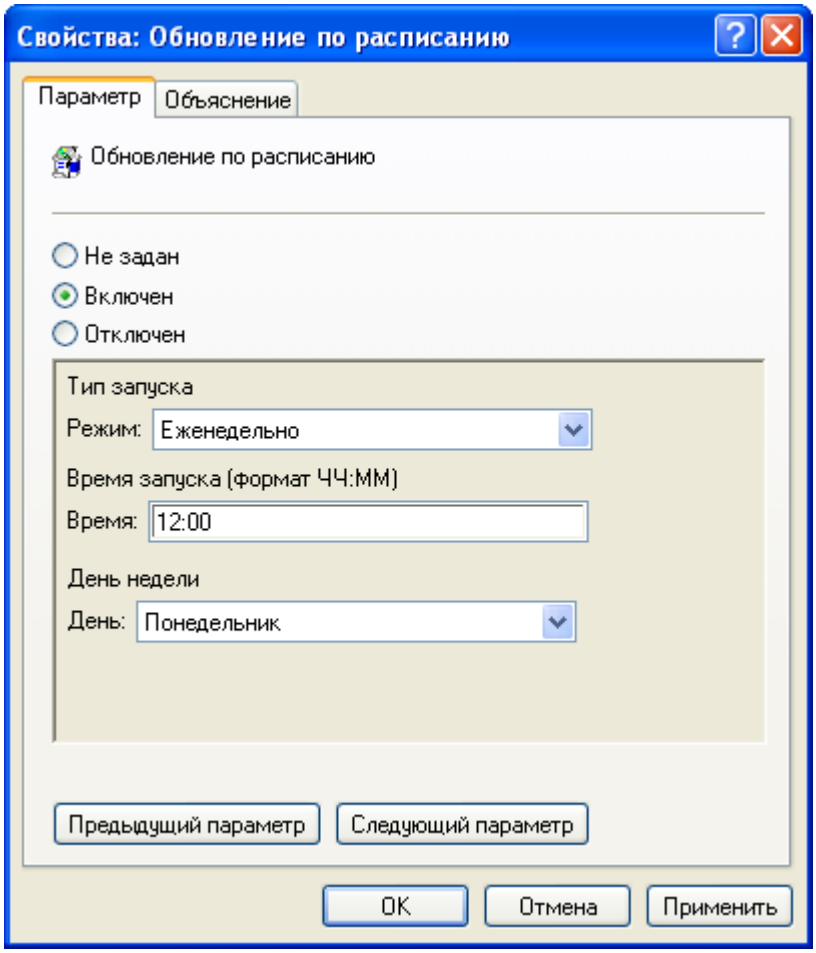


*Рисунок 43. Окно **Свойства: Обновление по расписанию***

4. На закладке **Параметр** выберите один из следующих вариантов:

   - **Не задан**. Компонент / функция включены на мобильном устройстве пользователя. Параметры, определяемые политикой, доступны для редактирования пользователем на мобильном устройстве.

     При этом компонент / функция будет работать с параметрами, заданными пользователем.

   - **Включен**. Компонент / функция включены на мобильном устройстве пользователя. Параметры, определяемые политикой, недоступны для редактирования пользователем на мобильном устройстве. При этом на экране мобильного устройства в левом верхнем углу отображается «замок».

     Компонент / функция будет работать с параметрами, заданными политикой. При выборе этого варианта вы можете настроить параметры политики.

   - **Отключен**. Компонент / функция, определяемые политикой, отключены на мобильном устройстве пользователя. Изменение параметров недоступно. При этом на экране мобильного устройства в левом верхнем углу отображается «замок».

5. В раскрывающемся списке **Режим** выберите режим запуска обновления баз программы. Возможные значения:

   - **Вручную**. Обновление баз может запускаться пользователем вручную в удобное для него время.
   - **Ежедневно**. Обновление баз программы выполняется каждый день в заданное время. Ниже в поле **Время** укажите время запуска в 24-часовом формате (ЧЧ:ММ).
   - **Еженедельно**. Обновление баз программы выполняется один раз в неделю в указанный день и заданное время. Ниже в раскрывающемся списке **День** выберите день недели, а в поле **Время** – время запуска в 24-часовом формате (ЧЧ:ММ).

НАСТРОЙКА ПОЛИТИКИ ЗАПРЕТ ОБНОВЛЕНИЯ В РОУМИНГЕ

Чтобы настроить политику Запрет обновления в роуминге, выполните следующие действия:

1. В дереве консоли управления выберите папку **Антивирус**.
2. В правой части окна консоли управления выберите политику **Запрет обновления в роуминге**.
3. В контекстном меню политики выберите пункт **Свойства**.

   В результате откроется окно **Свойства: Запрет обновления в роуминге** (см. рисунок ниже).

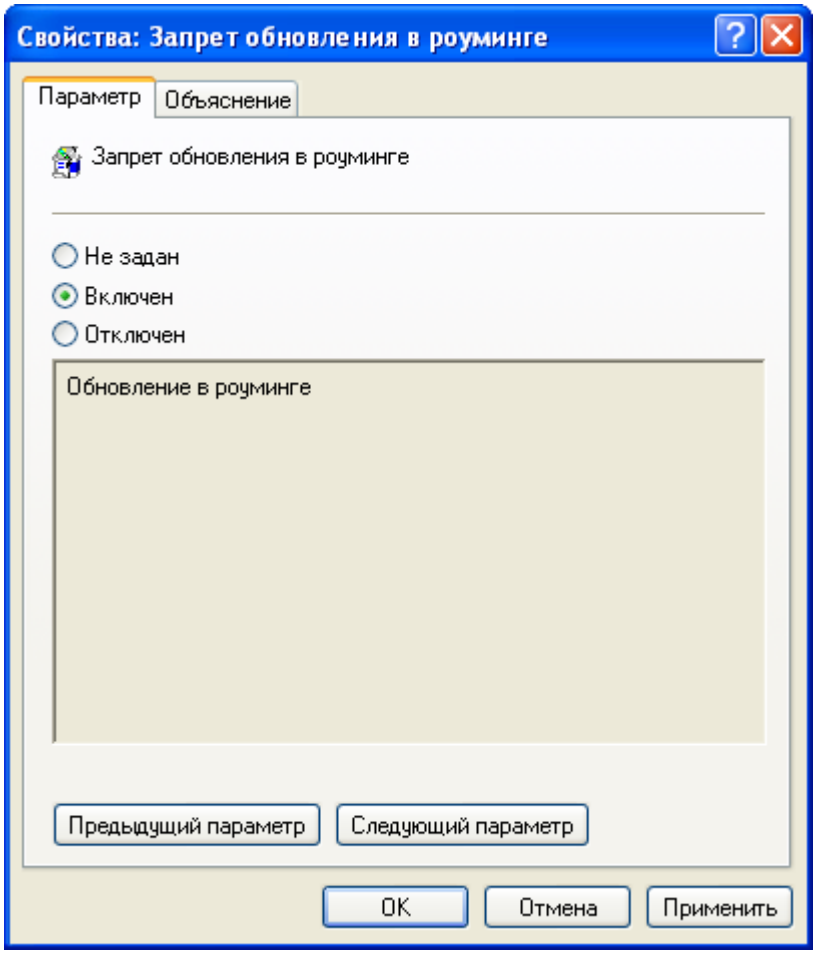


*Рисунок 44. Окно **Свойства: Запрет обновления в роуминге***

Если вы хотите запретить автоматическое обновление баз программы, когда мобильное устройство пользователя работает в зоне роуминга, на закладке **Параметр** выберите вариант **Включен**.

Если вы хотите разрешить автоматическое обновление баз программы, когда мобильное устройство пользователя работает в зоне роуминга, на закладке **Параметр** выберите вариант **Отключен**.

Если вы хотите, чтобы пользователь самостоятельно настроил запрет обновления в роуминге, на закладке **Параметр** выберите вариант **Не задан**.

Настройка политики Источник обновлений

Чтобы настроить политику Источник обновления, выполните следующие действия:

1. В дереве консоли управления выберите папку **Антивирус**.
2. В правой части окна консоли управления выберите политику **Источник обновления**.
3. В контекстном меню политики выберите пункт **Свойства**.

   В результате откроется окно **Свойства: Источник обновления** (см. рисунок ниже).

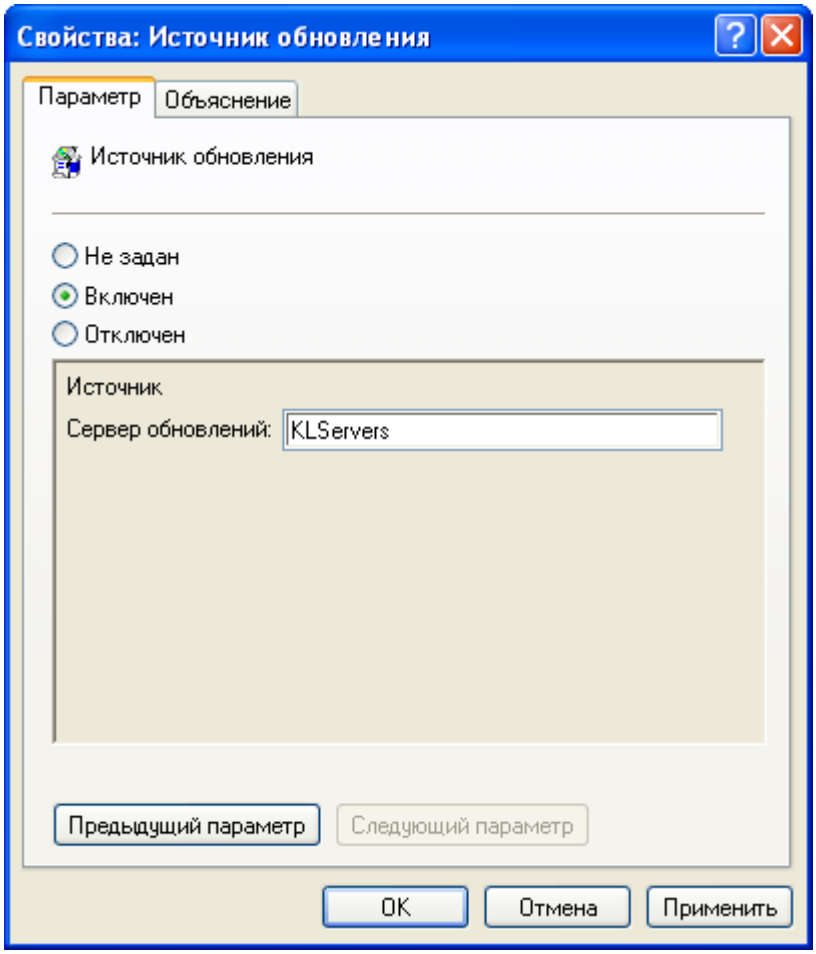


*Рисунок 45. Окно **Свойства: Источник обновления***

4. На закладке **Параметр** выберите один из следующих вариантов:

   - **Не задан**. Компонент / функция включены на мобильном устройстве пользователя. Параметры, определяемые политикой, доступны для редактирования пользователем на мобильном устройстве.

     При этом компонент / функция будет работать с параметрами, заданными пользователем.

   - **Включен**. Компонент / функция включены на мобильном устройстве пользователя. Параметры, определяемые политикой, недоступны для редактирования пользователем на мобильном устройстве. При этом на экране мобильного устройства в левом верхнем углу отображается «замок».

     Компонент / функция будет работать с параметрами, заданными политикой. При выборе этого варианта вы можете настроить параметры политики.

   - **Отключен**. Компонент / функция, определяемые политикой, отключены на мобильном устройстве пользователя. Изменение параметров недоступно. При этом на экране мобильного устройства в левом верхнем углу отображается «замок».

5. В поле **Сервер обновлений** укажите адрес источника обновлений баз программы, с которого обновления будут загружаться на мобильные устройства.

   Если вы хотите, чтобы обновления баз программы загружались с серверов обновлений «Лаборатории Касперского», в этом поле должен быть указан следующий адрес: KL Servers.

   Если вы хотите, чтобы обновления баз программы загружались с какого-либо другого сервера обновлений, укажите HTTP-сервер, локальный или сетевой каталог. Например, http://domain.com/index/.

   Структура папок в источнике обновлений должна повторять структуру на серверах обновлений «Лаборатории Касперского».

НАСТРОЙКА ПОЛИТИКИ БЛОКИРОВАНИЕ

Чтобы настроить политику Блокирование, выполните следующие действия:

1. В дереве консоли управления выберите папку **Анти-Вор**.
2. В правой части окна консоли управления выберите политику **Блокирование**.
3. В контекстном меню политики выберите пункт **Свойства**.

В результате откроется окно **Свойства: Блокирование** (см. рисунок ниже).

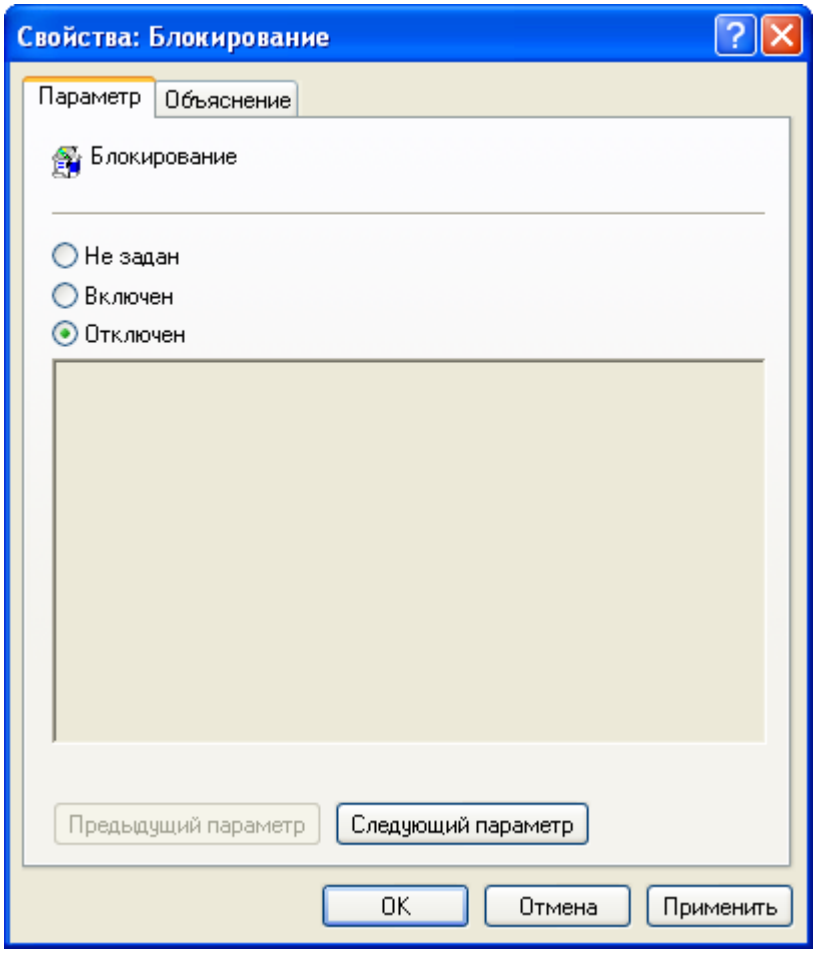


*Рисунок 46. Окно **Свойства: Блокирование***

4. Если вы хотите включить возможность дистанционного блокирования мобильного устройства пользователя, на закладке **Параметр** выберите вариант **Включен**.

   Если вы хотите отключить функцию Блокирование, на закладке **Параметр** выберите вариант **Отключен**.

   Если вы хотите, чтобы пользователь самостоятельно включил или отключил функцию Блокирование, на закладке **Параметр** выберите вариант **Не задан**.

Настройка политики Отображение текста при блокировании устройства

Чтобы настроить политику Отображение текста при блокировании устройства, выполните следующие действия:

1. В дереве консоли управления выберите папку **Анти-Вор**.

2. В правой части окна консоли управления выберите политику **Отображение текста при блокировании устройства**.

3. В контекстном меню политики выберите пункт **Свойства**.

   В результате откроется окно **Свойства: Отображение текста при блокировании устройства** (см. рисунок ниже).

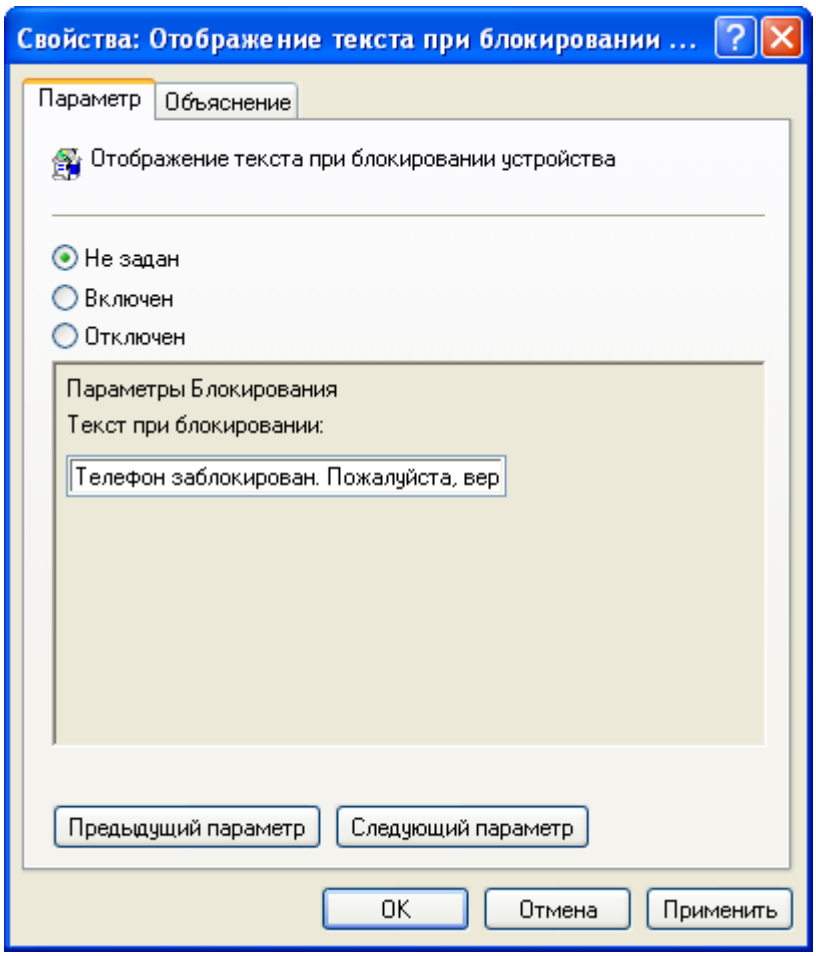


*Рисунок 47. Окно **Свойства: Отображение текста при блокировании устройства***

4. На закладке **Параметр** выберите один из следующих вариантов:

   - **Не задан**. Компонент / функция включены на мобильном устройстве пользователя. Параметры, определяемые политикой, доступны для редактирования пользователем на мобильном устройстве.

     При этом компонент / функция будет работать с параметрами, заданными пользователем.

   - **Включен**. Компонент / функция включены на мобильном устройстве пользователя. Параметры, определяемые политикой, недоступны для редактирования пользователем на мобильном устройстве. При этом на экране мобильного устройства в левом верхнем углу отображается «замок».

     Компонент / функция будет работать с параметрами, заданными политикой. При выборе этого варианта вы можете настроить параметры политики.

   - **Отключен**. Компонент / функция, определяемые политикой, отключены на мобильном устройстве пользователя. Изменение параметров недоступно. При этом на экране мобильного устройства в левом верхнем углу отображается «замок».

5. В поле **Текст при блокировании** введите текст, который будет отображаться на экране заблокированного устройства пользователя.

Настройка политики Удаление данных

Чтобы настроить политику Удаление данных, выполните следующие действия:

1. В дереве консоли управления выберите папку **Анти-Вор**.
2. В правой части окна консоли управления выберите политику **Удаление данных**.
3. В контекстном меню политики выберите пункт **Свойства**.

   В результате откроется окно **Свойства: Удаление данных** (см. рисунок ниже).

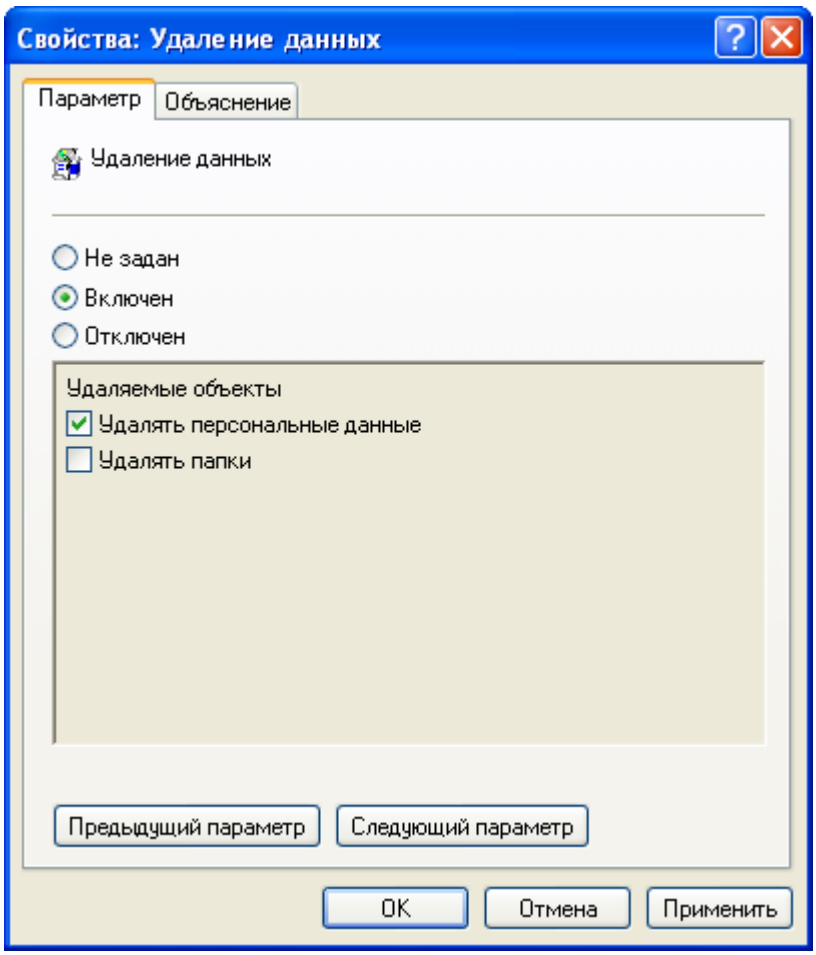


*Рисунок 48. Окно **Свойства: Удаление данных***

4. На закладке **Параметр** выберите один из следующих вариантов:

   - **Не задан**. Компонент / функция включены на мобильном устройстве пользователя. Параметры, определяемые политикой, доступны для редактирования пользователем на мобильном устройстве.

     При этом компонент / функция будет работать с параметрами, заданными пользователем.

   - **Включен**. Компонент / функция включены на мобильном устройстве пользователя. Параметры, определяемые политикой, недоступны для редактирования пользователем на мобильном устройстве. При этом на экране мобильного устройства в левом верхнем углу отображается «замок».

     Компонент / функция будет работать с параметрами, заданными политикой. При выборе этого варианта вы можете настроить параметры политики.

- **Отключен**. Компонент / функция, определяемые политикой, отключены на мобильном устройстве пользователя. Изменение параметров недоступно. При этом на экране мобильного устройства в левом верхнем углу отображается «замок».

При включении политики Удаление данных следует указать хотя бы один из ее параметров!

5. Установите флажок **Удалять персональные данные**, если вы хотите, чтобы Kaspersky Endpoint Security 8 for Smartphone удалял все персональные данные (например, контакты, сообщения, галерею изображений) с мобильного устройства по команде пользователя.

6. Установите флажок **Удалять папки**, если вы хотите, чтобы Kaspersky Endpoint Security 8 for Smartphone удалял указанные папки с мобильного устройства пользователя.

НАСТРОЙКА ПОЛИТИКИ СПИСОК ПАПОК ДЛЯ УДАЛЕНИЯ

Чтобы настроить политику Список папок для удаления, выполните следующие действия:

1. В дереве консоли управления выберите папку **Анти-Вор**.

2. В правой части окна консоли управления выберите политику **Список папок для удаления**.

3. В контекстном меню политики выберите пункт **Свойства**.

   В результате откроется окно **Свойства: Список папок для удаления** (см. рисунок ниже).

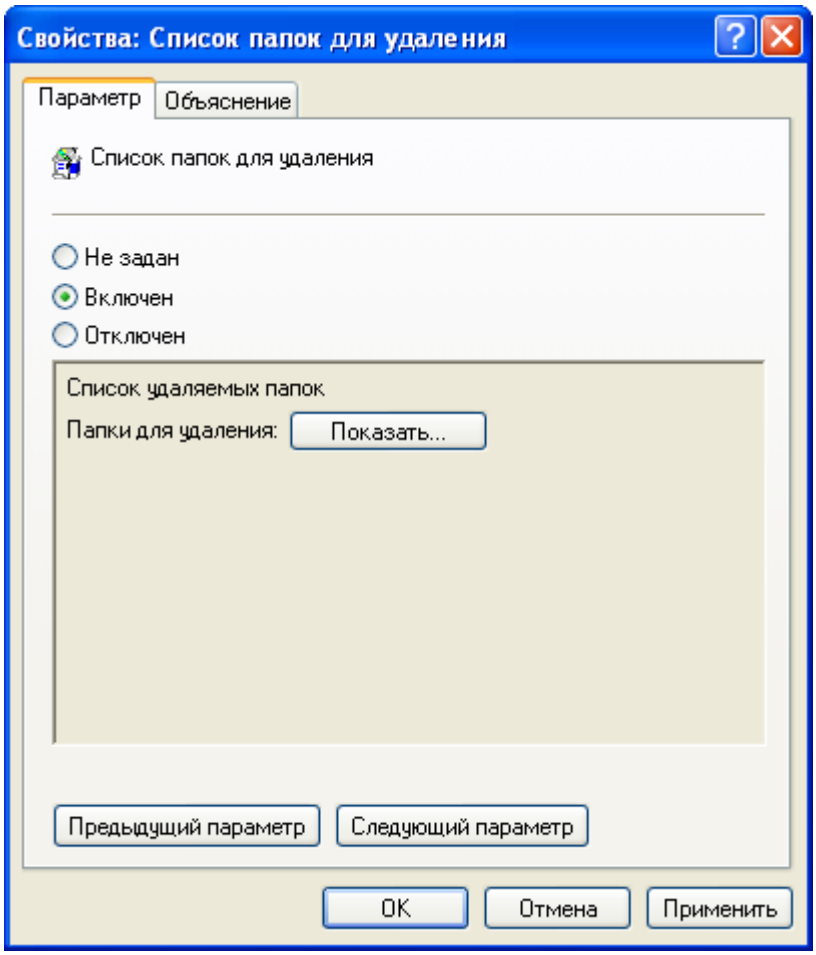


*Рисунок 49. Окно **Свойства: Список папок для удаления***

4. На закладке **Параметр** выберите один из следующих вариантов:

   - **Не задан**. Список папок для удаления пользователь формирует самостоятельно на мобильном устройстве.

   - **Включен**. Список папок для удаления может быть сформирован как пользователем самостоятельно на мобильном устройстве, так и администратором. При этом список папок для удаления, добавленный администратором, пользователь не может редактировать или удалить.

   - **Отключен**. Компонент / функция, определяемые политикой, отключены на мобильном устройстве пользователя. Изменение параметров недоступно. При этом на экране мобильного устройства в левом верхнем углу отображается «замок».

5. Нажмите на кнопку **Показать** и в открывшемся окне сформируйте список папок для удаления с помощью кнопок **Добавить** и **Удалить**.

Настройка политики GPS-Поиск

Чтобы настроить политику GPS-Поиск, выполните следующие действия:

1. В дереве консоли управления выберите папку **Анти-Вор**.

2. В правой части окна консоли управления выберите политику **GPS-Поиск**.

3. В контекстном меню политики выберите пункт **Свойства**.

   В результате откроется окно **Свойства: GPS-Поиск** (см. рисунок ниже).

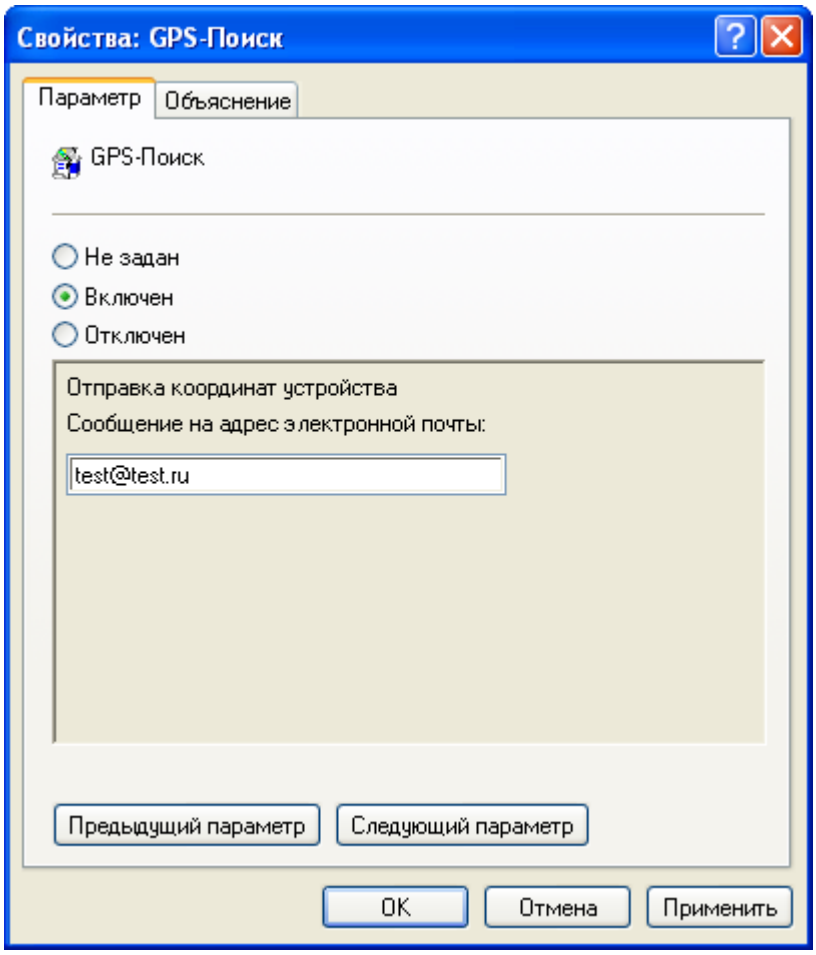


*Рисунок 50. Окно **Свойства: GPS-Поиск***

4. На закладке **Параметр** выберите один из следующих вариантов:

   - **Не задан**. Компонент / функция включены на мобильном устройстве пользователя. Параметры, определяемые политикой, доступны для редактирования пользователем на мобильном устройстве.

     При этом компонент / функция будет работать с параметрами, заданными пользователем.

   - **Включен**. Компонент / функция включены на мобильном устройстве пользователя. Параметры, определяемые политикой, недоступны для редактирования пользователем на мобильном устройстве. При этом на экране мобильного устройства в левом верхнем углу отображается «замок».

     Компонент / функция будет работать с параметрами, заданными политикой. При выборе этого варианта вы можете настроить параметры политики.

   - **Отключен**. Компонент / функция, определяемые политикой, отключены на мобильном устройстве пользователя. Изменение параметров недоступно. При этом на экране мобильного устройства в левом верхнем углу отображается «замок».

5. В поле **Сообщение на адрес электронной почты** укажите адрес электронной почты, на который будет отправлено письмо, содержащее географические координаты мобильного устройства пользователя.

НАСТРОЙКА ПОЛИТИКИ SIM-КОНТРОЛЬ

Чтобы настроить политику SIM-Контроль, выполните следующие действия:

1. В дереве консоли управления выберите папку **Анти-Вор**.

2. В правой части окна консоли управления выберите политику **SIM-Контроль**.

3. В контекстном меню политики выберите пункт **Свойства**.

   В результате откроется окно **Свойства: SIM-Контроль** (см. рисунок ниже).

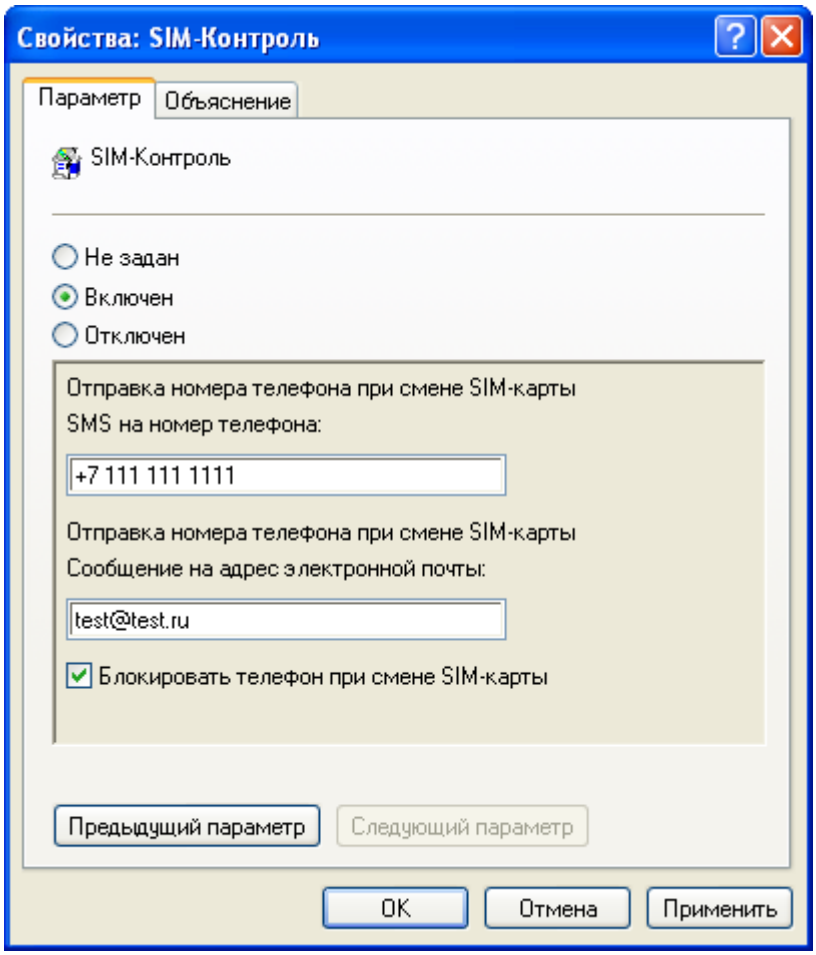


*Рисунок 51. Окно **Свойства: SIM-Контроль***

4. На закладке **Параметр** выберите один из следующих вариантов:

   - **Не задан**. Компонент / функция включены на мобильном устройстве пользователя. Параметры, определяемые политикой, доступны для редактирования пользователем на мобильном устройстве.

     При этом компонент / функция будет работать с параметрами, заданными пользователем.

   - **Включен**. Компонент / функция включены на мобильном устройстве пользователя. Параметры, определяемые политикой, недоступны для редактирования пользователем на мобильном устройстве. При этом на экране мобильного устройства в левом верхнем углу отображается «замок».

     Компонент / функция будет работать с параметрами, заданными политикой. При выборе этого варианта вы можете настроить параметры политики.

   - **Отключен**. Компонент / функция, определяемые политикой, отключены на мобильном устройстве пользователя. Изменение параметров недоступно. При этом на экране мобильного устройства в левом верхнем углу отображается «замок».

   При включении политики SIM-Контроль следует указать хотя бы один из ее параметров!

5. В поле **SMS на номер телефона** укажите номер телефона, на который при смене SIM-карты будет отправлено SMS с новым телефонным номером, соответствующим вставленной SIM-карте. Номер может начинаться с цифры или со знака «+» и должен содержать только цифры.

6. В поле **Сообщение на адрес электронной почты** укажите адрес электронной почты, на который необходимо отправить письмо, содержащее новый телефонный номер, соответствующий вставленной SIM-карте.

7. Установите флажок **Блокировать телефон при смене SIM-карты**, если вы хотите чтобы программа блокировала мобильное устройство пользователя при смене SIM-карты или при включении без нее. Разблокировать устройство можно путем ввода секретного кода.

НАСТРОЙКА ПОЛИТИКИ ЗАПРЕТ ИСПОЛЬЗОВАНИЯ АНТИ-СПАМА

Чтобы настроить политику Запрет использования Анти-Спама, выполните следующие действия:

1. В дереве консоли управления выберите папку **Анти-Спам**

2. В правой части окна консоли управления выберите политику **Запрет использования Анти-Спама**.

3. В контекстном меню политики выберите пункт **Свойства**.

   В результате откроется окно **Свойства: Запрет использования Анти-Спама** (см. рисунок ниже).

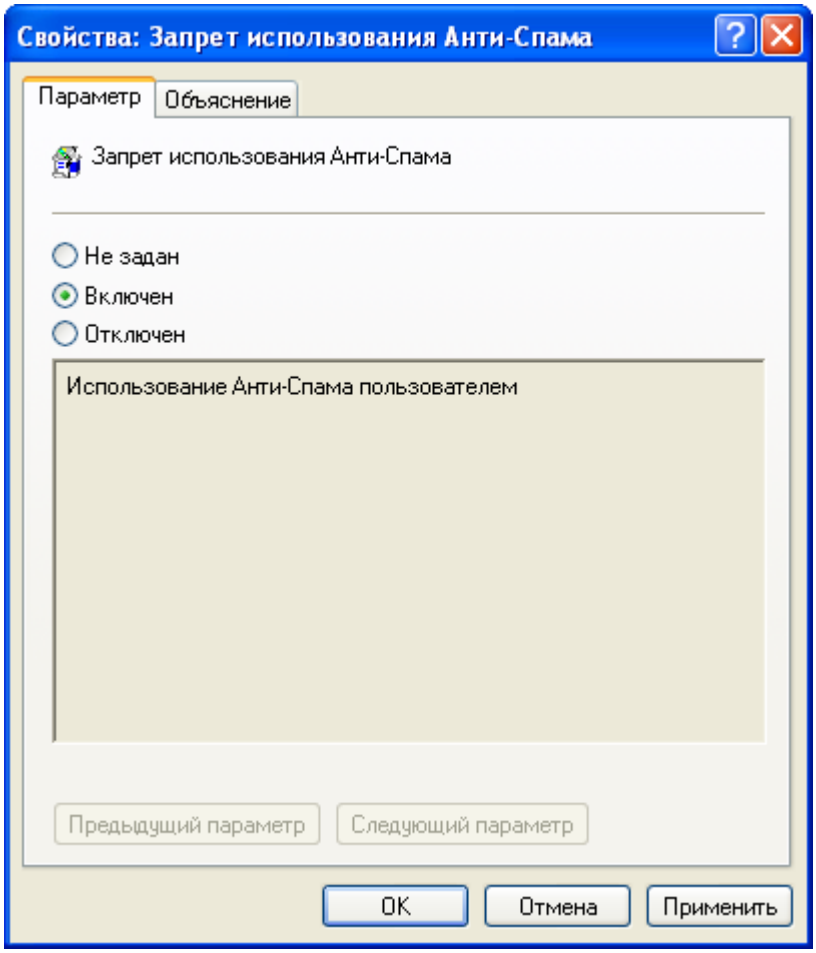


*Рисунок 52. Окно **Свойства: Запрет использования Анти-Спама***

4. Если вы хотите запретить пользователю редактирование параметров Анти-Спама и просмотр журнала этого компонента, на закладке **Параметр** выберите вариант **Включен**.

   Если вы хотите разрешить пользователю использовать компонент Анти-Спам, на закладке **Параметр** выберите вариант **Отключен** или **Не задан**.

Настройка политики Запрет использования Личных контактов

Чтобы настроить политику Запрет использования Личных контактов, выполните следующие действия:

1. В дереве консоли управления выберите папку **Личные контакты**.

2. В правой части окна консоли управления выберите политику **Запрет использования Личных контактов**.

3. В контекстном меню политики выберите пункт **Свойства**.

   В результате откроется окно **Свойства: Запрет использования Личных контактов** (см. рисунок ниже).

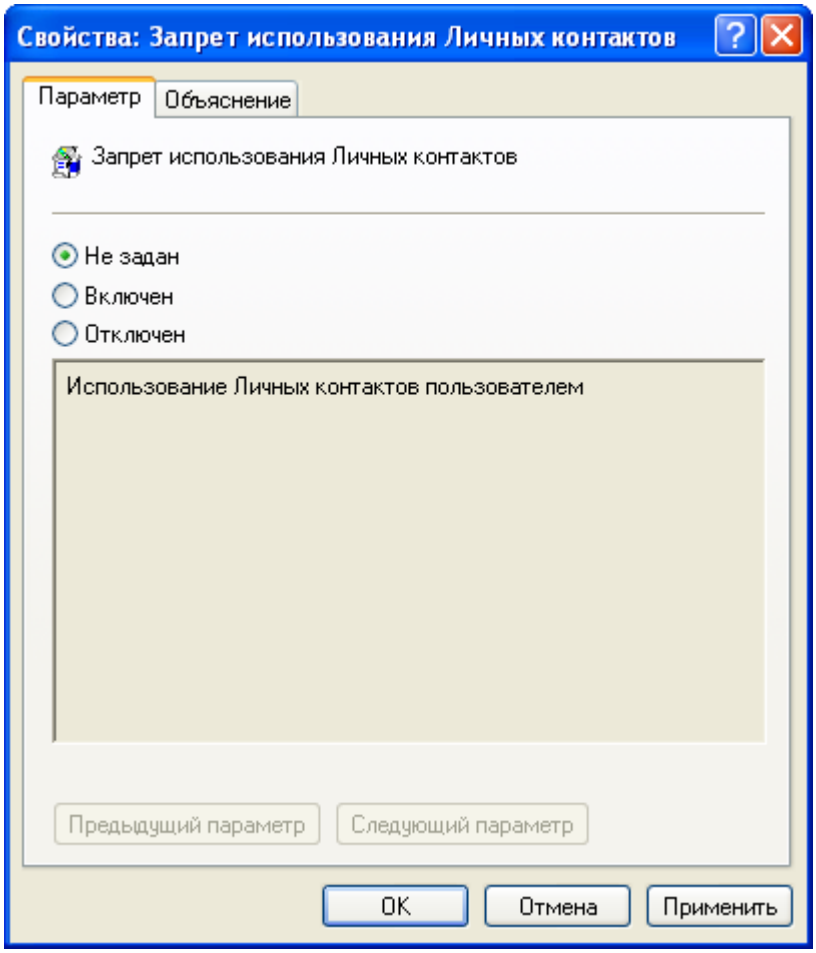


*Рисунок 53. Окно **Свойства: Запрет использования Личных контактов***

4. Если вы хотите запретить пользователю редактирование параметров Личных контактов и просмотр журнала этого компонента, на закладке **Параметр** выберите вариант **Включен**.

   Если вы хотите разрешить пользователю использовать компонент Личные контакты, на закладке **Параметр** выберите вариант **Отключен** или **Не задан**.

НАСТРОЙКА ПОЛИТИКИ ЗАПРЕТ ДОСТУПА К ЗАШИФРОВАННЫМ ДАННЫМ

Чтобы настроить политику Автоматическое шифрование данных, выполните следующие действия:

1. В дереве консоли управления выберите папку **Шифрование**.

2. В правой части окна консоли управления выберите политику **Запрет доступа к зашифрованным данным**.

3. В контекстном меню политики выберите пункт **Свойства**.

   В результате откроется окно **Свойства: Запрет доступа к зашифрованным данным** (см. рисунок ниже).

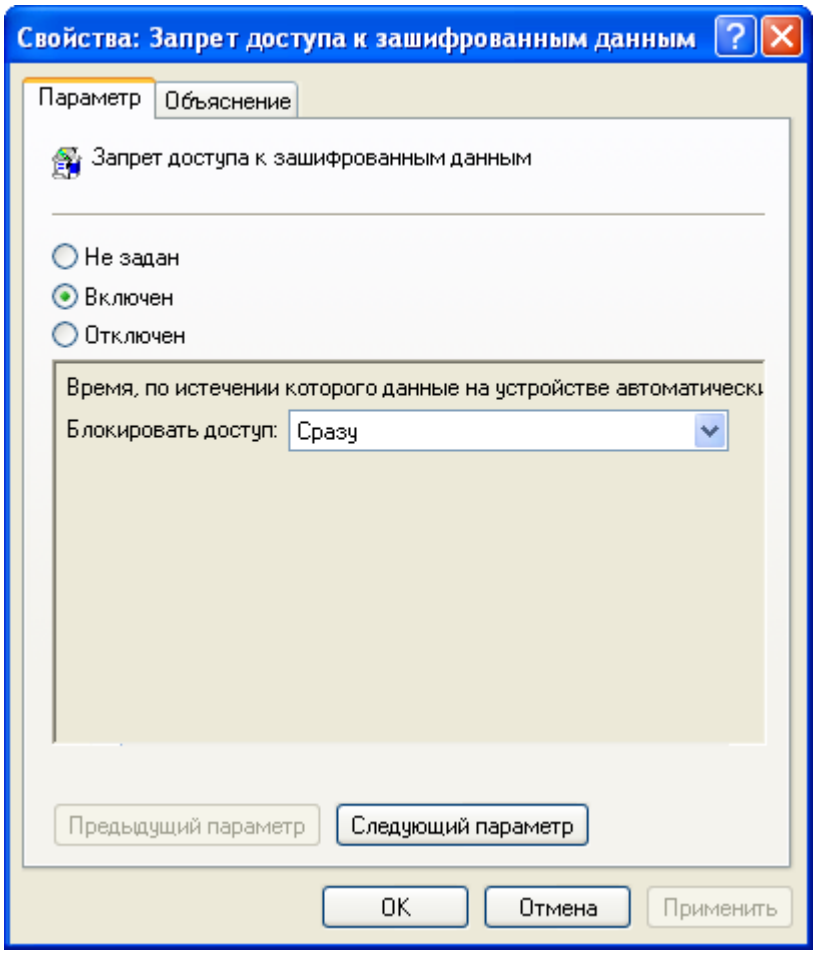


*Рисунок 54. Окно **Свойства: Автоматическое шифрование данных***

4. На закладке **Параметр** выберите один из следующих вариантов:

   - **Не задан**. Пользователю разрешено редактировать параметры программы на мобильном устройстве. При этом программа будет работать с параметрами, заданными пользователем.

   - **Включен**. Политика включена. Пользователю запрещено редактировать параметры программы на мобильном устройстве. При этом на экране мобильного устройства в левом верхнем углу отображается «замок».

     Программа будет работать с параметрами, заданными политикой. При выборе этого варианта вы можете настроить параметры политики.

- **Отключен**. Компонент / функция, определяемые политикой, отключены на мобильном устройстве пользователя. Изменение параметров недоступно. При этом на экране мобильного устройства в левом верхнем углу отображается «замок».

5. В раскрывающемся списке **Блокировать доступ** выберите временной интервал, по истечении которого доступ к зашифрованным данным автоматически заблокируется. Функция активизируется после перехода мобильного устройства в режим энергосбережения.

Настройка политики Список папок для шифрования

Чтобы настроить политику Список папок для шифрования, выполните следующие действия:

1. В дереве консоли управления выберите папку **Шифрование**.
2. В правой части окна консоли управления выберите политику **Список папок для шифрования**.
3. В контекстном меню политики выберите пункт **Свойства**.

   В результате откроется окно **Свойства: Список папок для шифрования** (см. рисунок ниже).

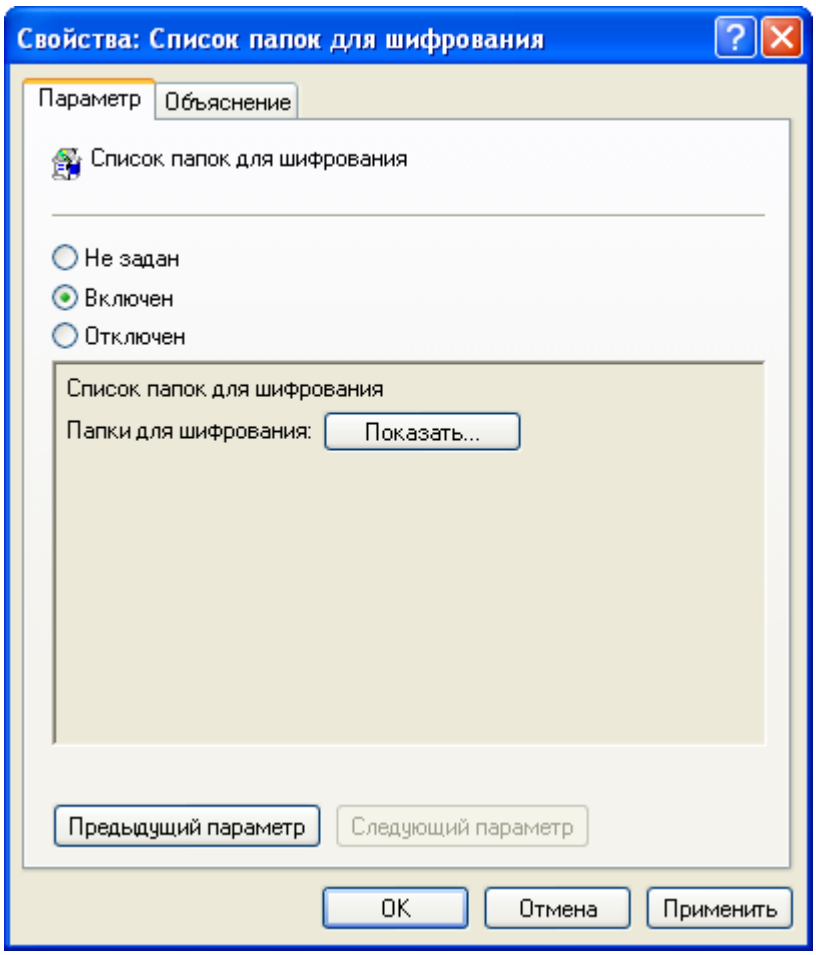


*Рисунок 55. Окно **Свойства: Список папок для шифрования***

4. На закладке **Параметр** выберите один из следующих вариантов:

   - **Не задан**. Список папок для шифрования пользователь формирует самостоятельно на мобильном устройстве.

   - **Включен**. Список папок для шифрования может быть сформирован как пользователем самостоятельно на мобильном устройстве, так и администратором. При этом список папок для шифрования, добавленный администратором, пользователь не может редактировать или удалить.

   - **Отключен**. Компонент / функция, определяемые политикой, отключены на мобильном устройстве пользователя. Изменение параметров недоступно. При этом на экране мобильного устройства в левом верхнем углу отображается «замок».

5. Нажмите на кнопку **Показать** и в открывшемся окне сформируйте список папок для шифрования с помощью кнопок **Добавить** и **Удалить**.

НАСТРОЙКА ПОЛИТИКИ РЕЖИМ СЕТЕВОГО ЭКРАНА

Чтобы настроить политику Режим Сетевого экрана, выполните следующие действия:

1. В дереве консоли управления выберите папку **Сетевой экран**.

2. В правой части окна консоли управления выберите политику **Режим Сетевого экрана**.

3. В контекстном меню политики выберите пункт **Свойства**.

   В результате откроется окно **Свойства: Режим Сетевого экрана** (см. рисунок ниже).

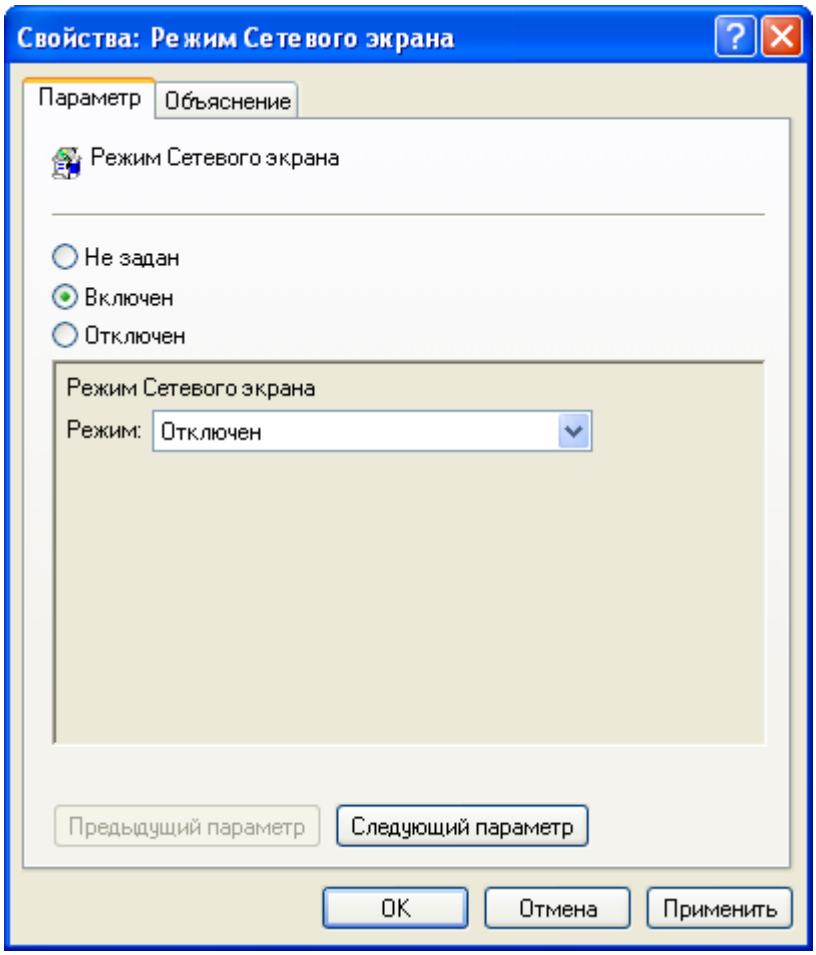


*Рисунок 56. Окно **Свойства: Режим Сетевого экрана***

4. На закладке **Параметр** выберите один из следующих вариантов:

   - **Не задан**. Компонент / функция включены на мобильном устройстве пользователя. Параметры, определяемые политикой, доступны для редактирования пользователем на мобильном устройстве.

     При этом компонент / функция будет работать с параметрами, заданными пользователем.

   - **Включен**. Компонент / функция включены на мобильном устройстве пользователя. Параметры, определяемые политикой, недоступны для редактирования пользователем на мобильном устройстве. При этом на экране мобильного устройства в левом верхнем углу отображается «замок».

     Компонент / функция будет работать с параметрами, заданными политикой. При выборе этого варианта вы можете настроить параметры политики.

   - **Отключен**. Компонент / функция, определяемые политикой, отключены на мобильном устройстве пользователя. Изменение параметров недоступно. При этом на экране мобильного устройства в левом верхнем углу отображается «замок».

5. В раскрывающемся списке **Режим** выберите уровень безопасности Сетевого экрана. Возможные значения:

   - **Отключен**. Сетевой экран отключен. Разрешена любая сетевая активность.
   - **Минимальная защит**а. Сетевой экран блокирует все входящие соединения. Любые исходящие соединения разрешены.
   - **Максимальная защита**. Сетевой экран блокирует все входящие соединения. Исходящие соединения разрешены по протоколам SSH / HTTP / HTTPS / IMAP / SMTP / POP3.
   - **Блокировать все**. Сетевой экран блокирует любую сетевую активность, кроме обновления баз программы и работы Mobile Device Manager.

НАСТРОЙКА ПОЛИТИКИ УВЕДОМЛЕНИЯ СЕТЕВОГО ЭКРАНА

Чтобы настроить политику Уведомления Сетевого экрана, выполните следующие действия:

1. В дереве консоли управления выберите папку **Сетевой экран**.
2. В правой части окна консоли управления выберите политику **Уведомления Сетевого экрана**.
3. В контекстном меню политики выберите пункт **Свойства**.

   В результате откроется окно **Свойства: Уведомления Сетевого экрана** (см. рисунок ниже).

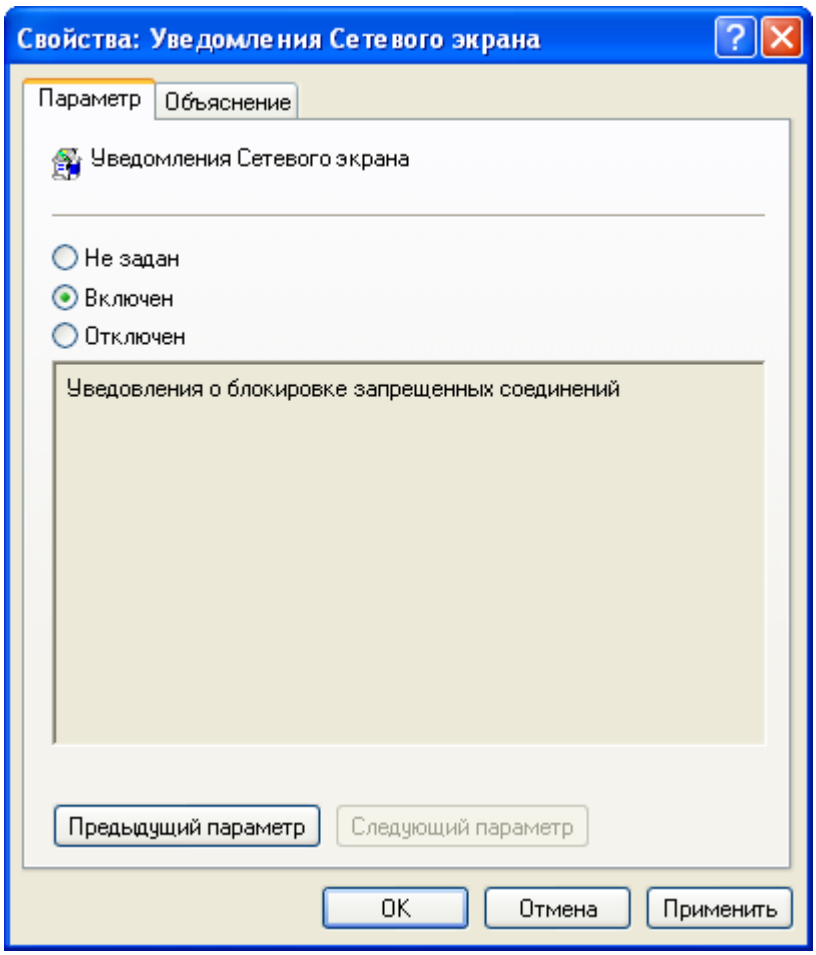


*Рисунок 57. Окно **Свойства: Уведомления Сетевого экрана***

4. Если вы хотите, чтобы пользователь получал уведомления о попытке соединения, запрещенного на выбранном уровне безопасности, на закладке **Параметр** выберите вариант **Включен**.

   Если вы хотите, чтобы Сетевой экран не информировал пользователя о блокировке запрещенных соединений на мобильном устройстве, на закладке **Параметр** выберите вариант **Отключен**.

   Если вы хотите, чтобы пользователь самостоятельно включал или отключал использование уведомлений Сетевого экрана, на закладке **Параметр** выберите вариант **Не задан**.

Настройка политики Лицензия

Чтобы настроить политику Лицензия, выполните следующие действия:

1. Сохраните файл ключа, присланный вам по электронной почте, на сервере MDM.

2. Откройте папку с дистрибутивом программы и запустите утилиту kes2mdm.exe.

   В командной строке консоли сервера введите команду, имеющую следующий синтаксис:

   ```
   kes2mdm.exe <полный путь к файлу ключа>\<имя файла ключа>
   ```

   В результате работы утилиты в папку с дистрибутивом программы будет добавлен файл kes8key.txt, содержащий текстовую строку.

   Если файл kes8key.txt не добавился в папку с дистрибутивом программы, из командной строки консоли сервера скопируйте расшифровку ошибки и отправьте ее в Службу технической поддержки «Лаборатории Касперского».

3. Откройте файл kes8key.txt и скопируйте текстовую строку в буфер обмена.

4. Откройте консоль управления.

5. В дереве консоли управления выберите объект групповой политики, для которого вы хотите установить лицензию Kaspersky Endpoint Security 8 for Smartphone.

6. В узле **Конфигурация компьютера** выберите папку **Административные шаблоны**, в ней папку **Параметры Kaspersky Endpoint Security 8 for Smartphone**.

7. Выберите папку **Лицензия**.

8. Откройте окно **Свойства: Лицензия** (см. рисунок ниже).

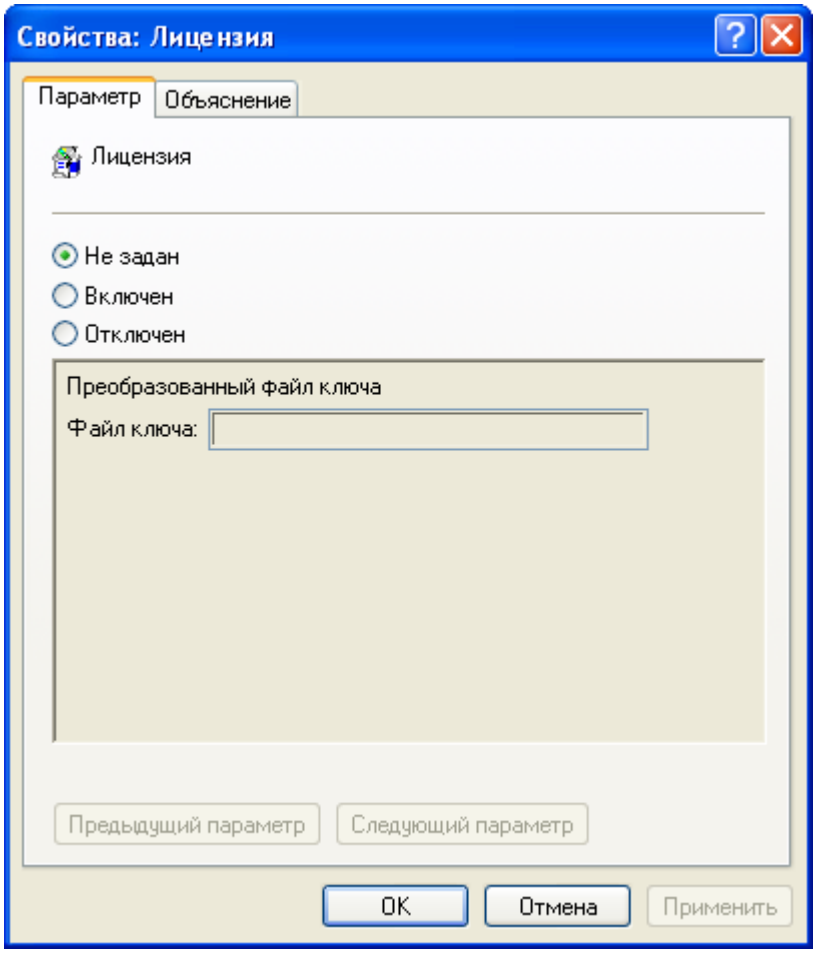


*Рисунок 58. Окно **Свойства: Лицензия***

9. На закладке **Параметр** выберите вариант **Включен**, чтобы настроить политику.

10. В поле **Файл ключа** вставьте текстовую строку из буфера обмена.

    При следующей синхронизации политик лицензия Kaspersky Endpoint Security 8 for Smartphone будет установлена на мобильные устройства пользователей.

АКТИВАЦИЯ ПРОГРАММЫ

Для того чтобы установить лицензию для программы Kaspersky Endpoint Security 8 for Smartphone на мобильные устройства, администратор должен настроить политику Лицензия в административном шаблоне управления программой. Когда политика будет передана на устройства пользователей, лицензия будет установлена и программа будет активирована.

После установки на мобильное устройство программа Kaspersky Endpoint Security 8 for Smartphone работает три дня без активации в режиме полной функциональности. Если по истечении трех дней установка лицензии не будет выполнена, то программа автоматически переключится в режим работы с ограниченной функциональностью.

Если вы не приобрели лицензию до установки программы, вы можете добавить ее в состав политики позже.

По умолчанию лицензия не включена в состав политики.

Установка и удаление программы на мобильных устройствах

Mobile Device Manager позволяет дистанционно устанавливать и удалять Kaspersky Endpoint Security 8 for Smartphone на мобильных устройствах пользователей.

Для этого необходимо в консоли System Center Mobile Device Manager Software Distribution создать инсталляционный пакет для установки программы (см. раздел «Создание инсталляционного пакета» на стр. 116) и распространить его на группу мобильных устройств, зарегистрированных в домене.

Рекомендуется перед созданием и распространением инсталляционного пакета настроить параметры политик управления программой (см. раздел «Настройка шаблона управления» на стр. 89), так как периодичность синхронизации мобильных устройств с сервером MDM отличается от периода применения политик. Это действие позволит одновременно установить программу и применить политики на мобильных устройствах пользователей.

В результате при следующей синхронизации мобильных устройств с сервером MDM программа автоматически установится на эти устройства. При этом статус установки программы не отображается и пользователь не принимает в ней никакого участия.

В дальнейшем после установки программы на мобильные устройства вы можете изменять параметры ее работы с помощью политик. После применения политик при синхронизации мобильных устройств с сервером MDM программа будет работать уже с измененными параметрами.

Чтобы выполнить дистанционное удаление программы с мобильных устройств пользователей, необходимо в консоли System Center Mobile Device Manager Software Distribution созданный инсталляционный пакет отметить на удаление. При следующей синхронизации мобильных устройств с сервером MDM программа автоматически удалится с них.

При создании инсталляционного пакета вы можете разрешить пользователям самостоятельно удалить программу с мобильных устройств путем стандартной процедуры «Удаление программ».

В этом разделе

Создание инсталляционного пакета

Для распространения Kaspersky Endpoint Security 8 for Smartphone на мобильные устройства пользователей, зарегистрированных в домене, следует создать инсталляционный пакет программы. В состав созданного пакета будет входить инсталляционный файл, который при получении мобильными устройствами запустится автоматически.

Перед созданием инсталляционного пакета убедитесь, что сертификат, которым подписан инсталляционный файл Kaspersky Endpoint Security 8 for Smartphone, и сертификат центра сертификации установлены на сервере MDM. Сертификат программы добавлен в список доверенных издателей Trusted Publishers, а сертификат центра сертификации – в список доверенных корневых центров сертификации Trusted Root Certification Authorities.

Чтобы создать инсталляционный пакет для установки Kaspersky Endpoint Security 8 for Smartphone на мобильные устройства пользователей, выполните следующие действия:

1. Откройте консоль System Center Mobile Device Manager Software Distribution.

2. Откройте мастер создания инсталляционного пакета по ссылке **Create** (см. рисунок ниже).

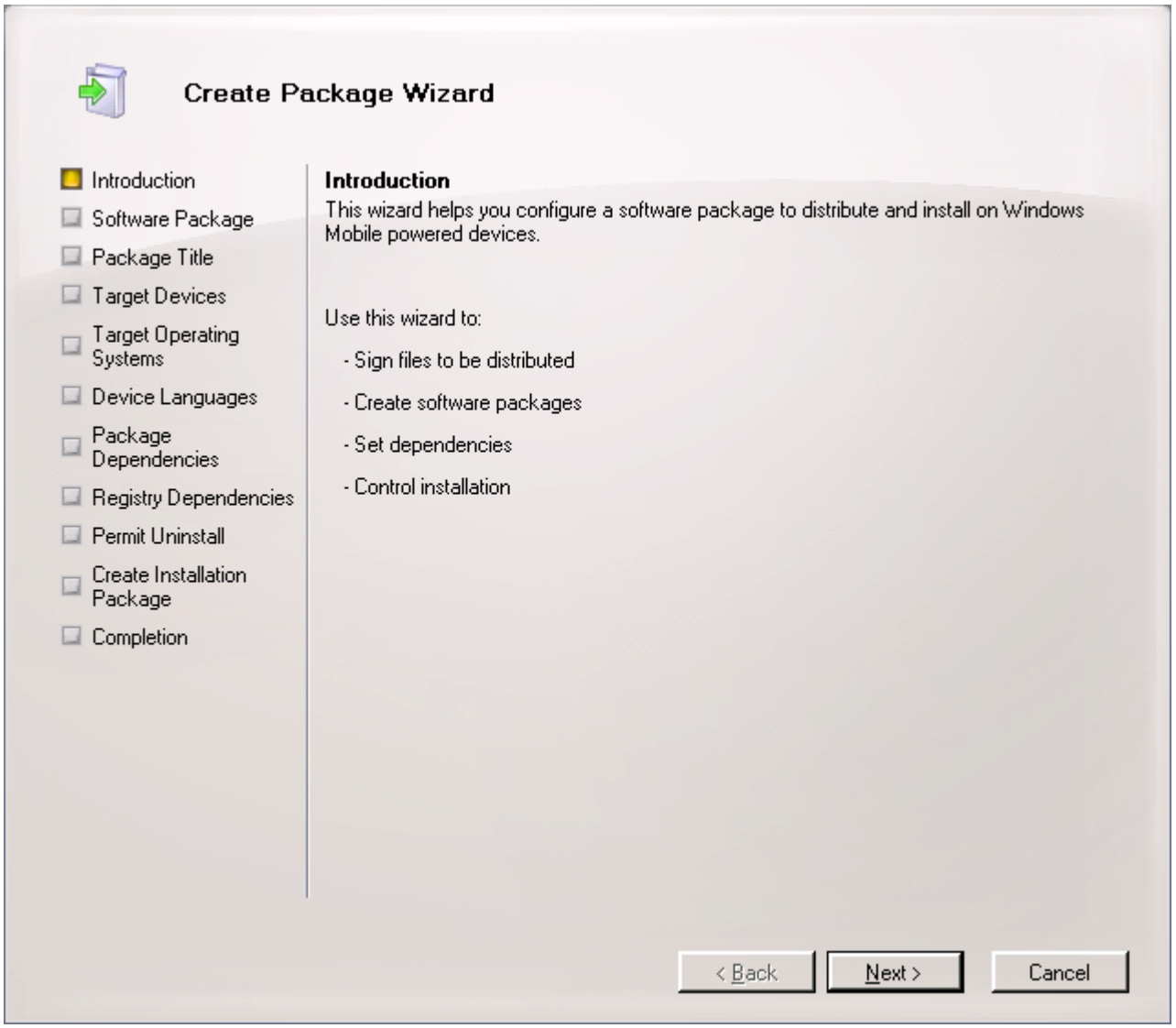


*Рисунок 59. Окно **Create Package Wizard***

3. На закладке **Software Package** в поле **Cabinet file** с помощью кнопки **Browse** откройте папку с дистрибутивом программы и выберите инсталляционный файл endpoint_for_MDM_Afaria_en_8.0.0.15.cab, сохраненный на сервере MDM (см. рисунок ниже).

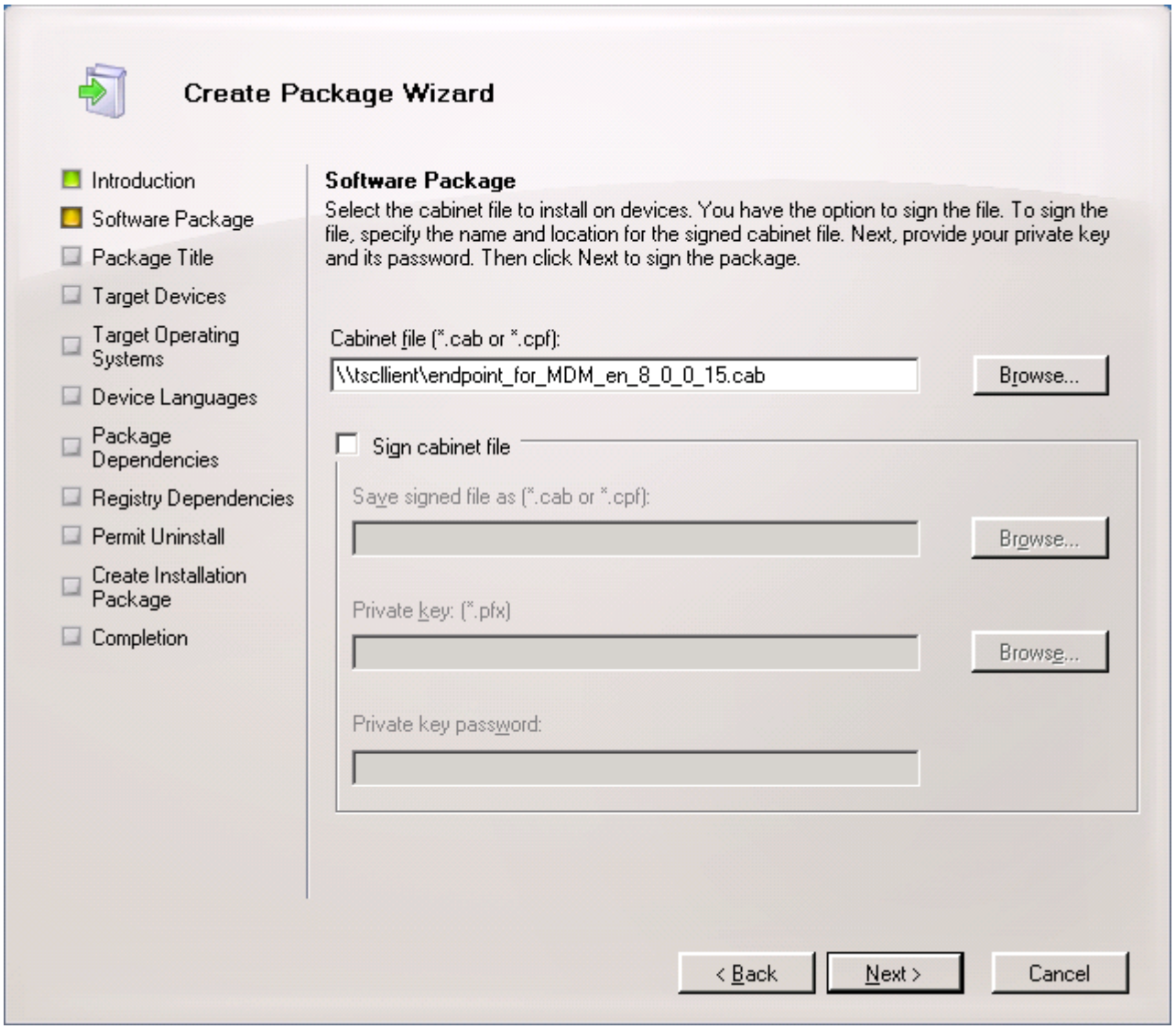


*Рисунок 60. Закладка **Software Package***

4. На закладке **Package Title** в поле **Package title** укажите имя создаваемого инсталляционного пакета, а в поле **Package description** введите его описание (см. рисунок ниже).

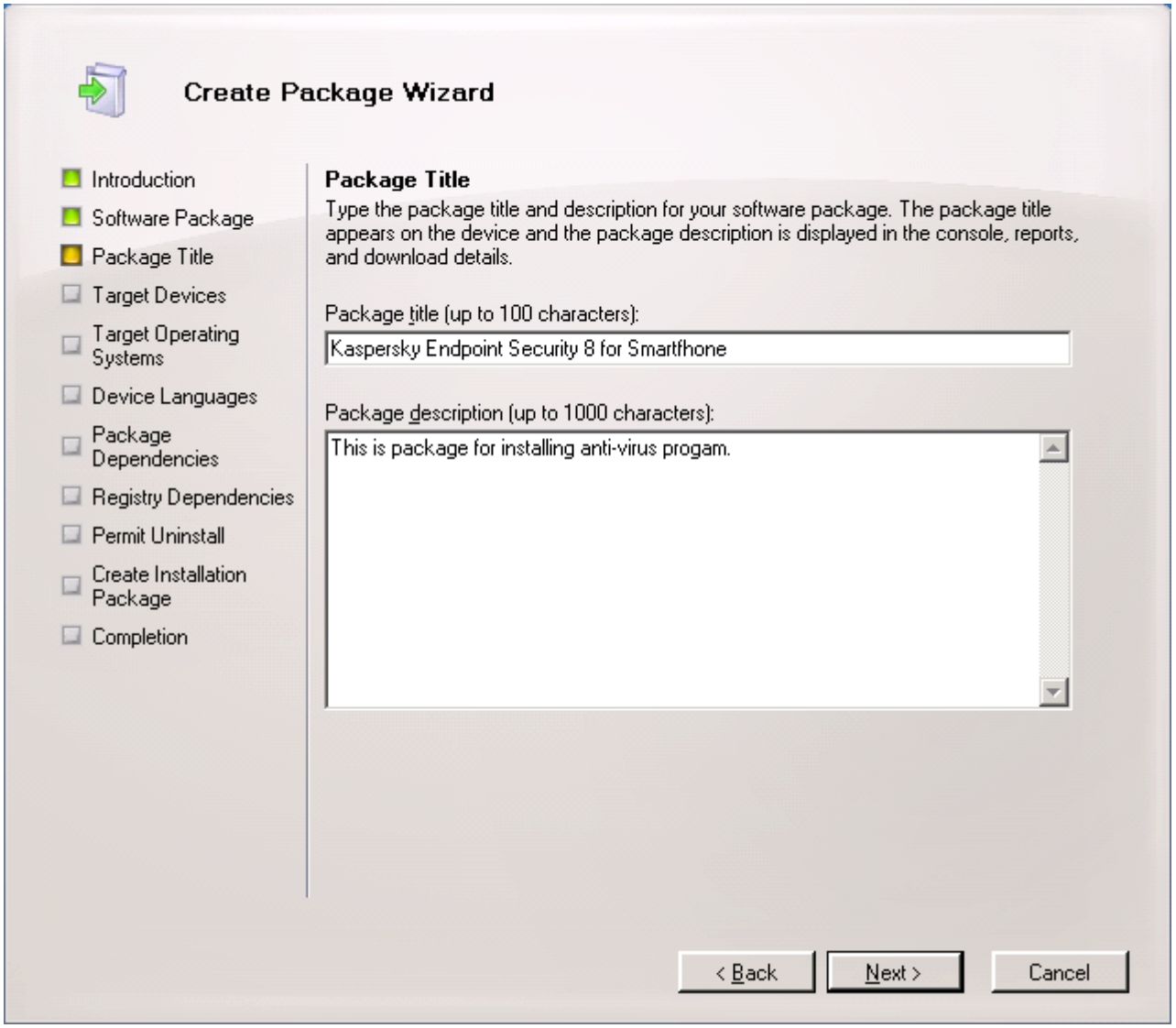


*Рисунок 61. Закладка **Package Title***

5. На закладке **Target Devices** (см. рисунок ниже) выберите тип операционной системы мобильных устройств, на которые требуется установить Kaspersky Endpoint Security 8 for Smartphone.

   Если вы хотите установить программу на мобильные устройства с любой операционной системой выберите вариант **All**. Рекомендуется выбрать это значение.

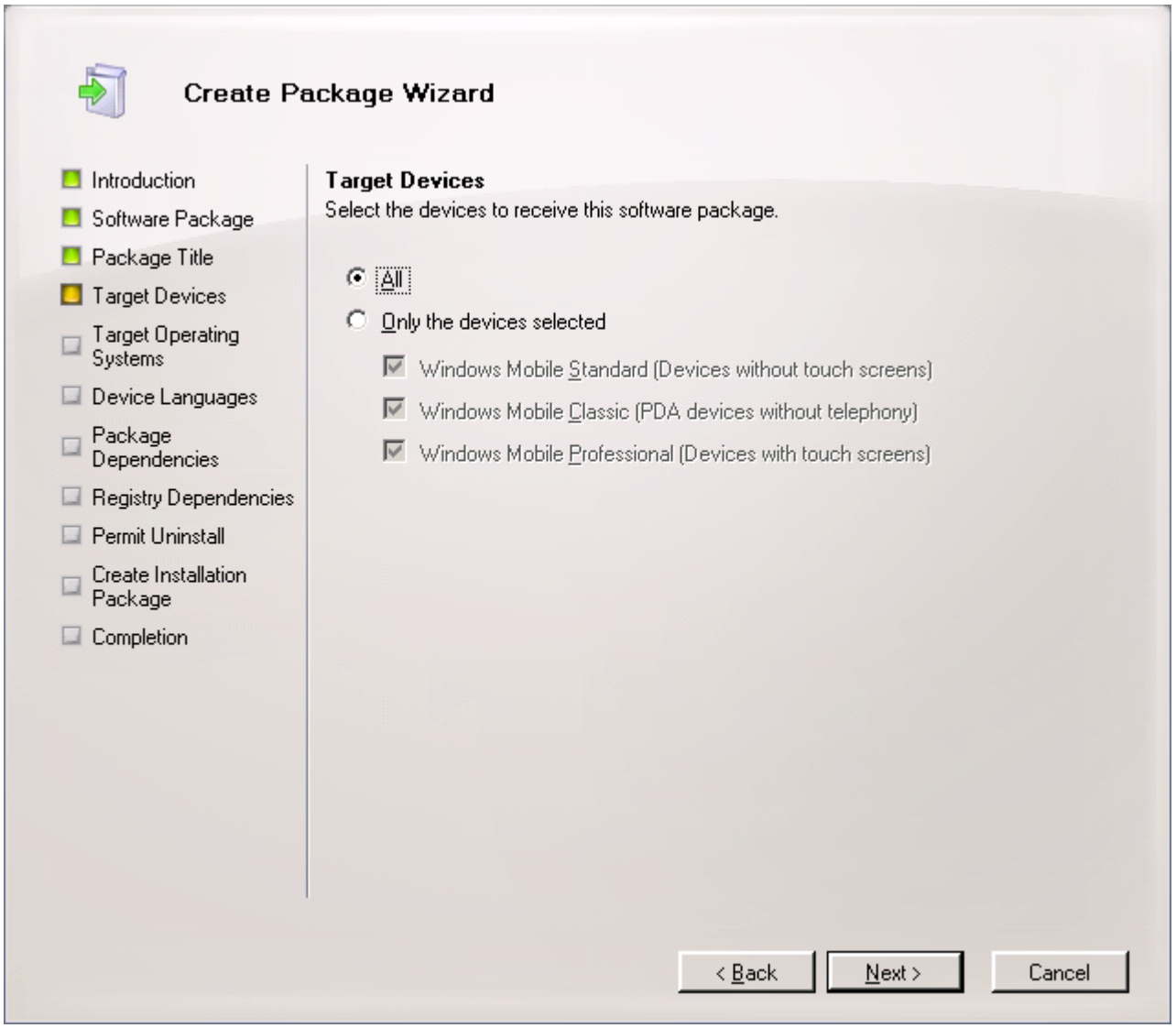


*Рисунок 62. Закладка **Target Devices***

6. На закладке **Target Operating Systems** (см. рисунок ниже) укажите диапазон версий операционной системы мобильных устройств, на которые требуется установить Kaspersky Endpoint Security 8 for Smartphone.

   Если вы хотите установить программу на мобильные устройства с любой версией операционной системы, выберите вариант **All**. Рекомендуется выбрать это значение.

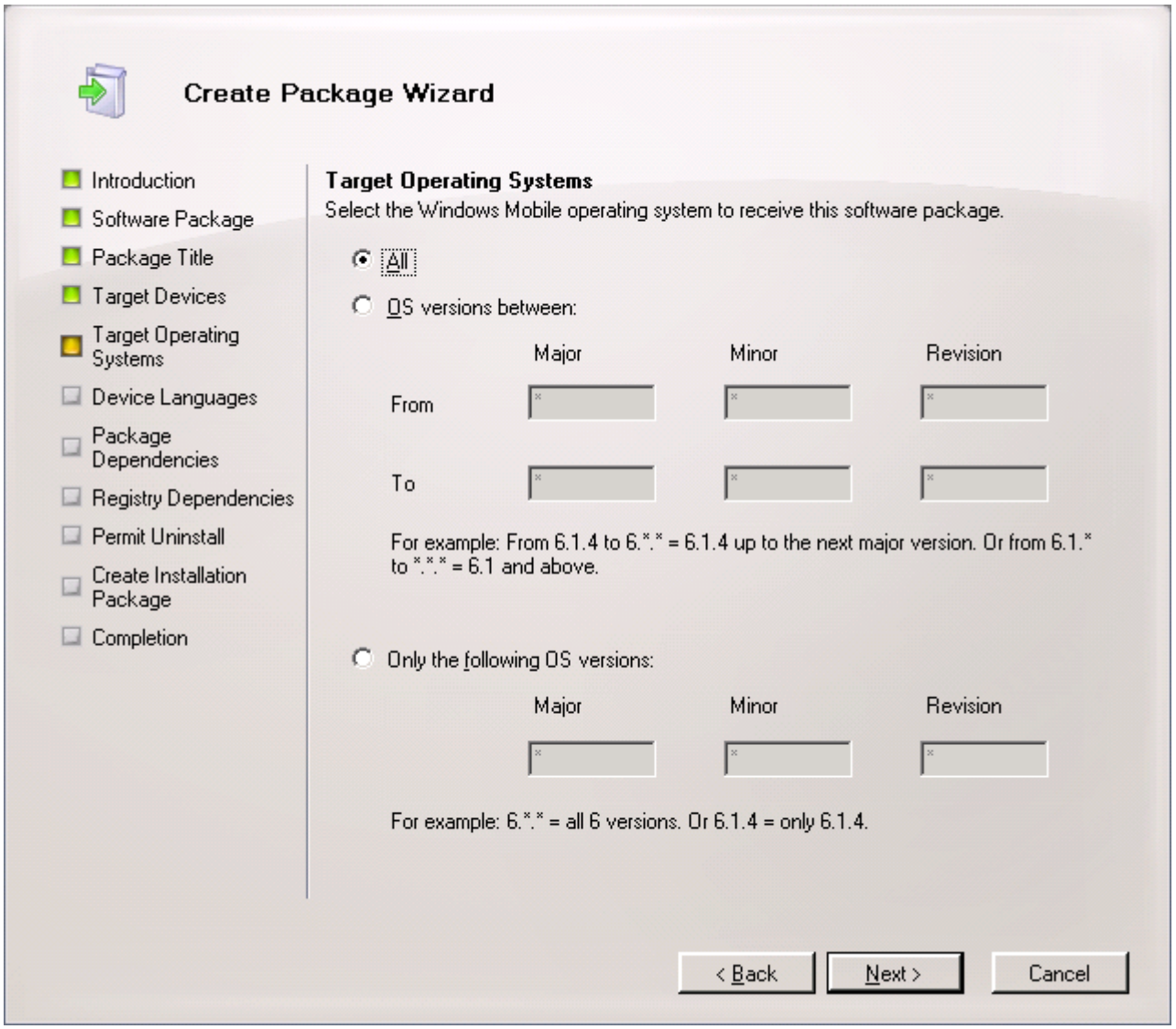


*Рисунок 63. Закладка **Target Operating Systems***

7. На закладке **Device Languages** (см. рисунок ниже) выберите язык интерфейса мобильных устройств, на которые требуется установить Kaspersky Endpoint Security 8 for Smartphone.

   Если вы хотите установить программу на мобильные устройства с любым языком интерфейса, выберите вариант **All**.

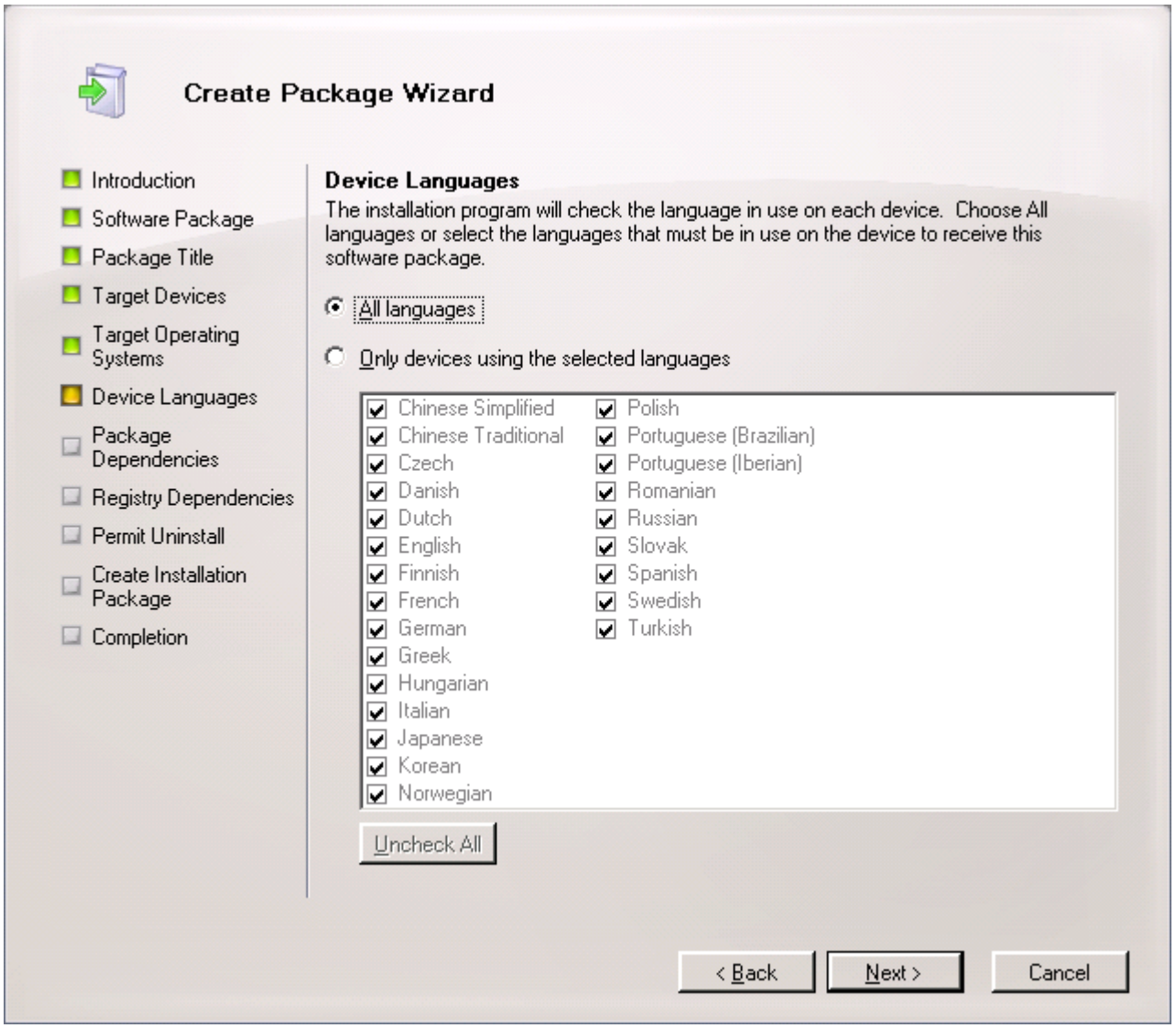


*Рисунок 64. Закладка **Device Languages***

8. На закладке **Package Dependencies** (см. рисунок ниже) укажите зависимости создаваемого пакета от других инсталляционных пакетов.

   Если таких зависимостей нет, выберите вариант **No dependencies**. Рекомендуется выбрать это значение.

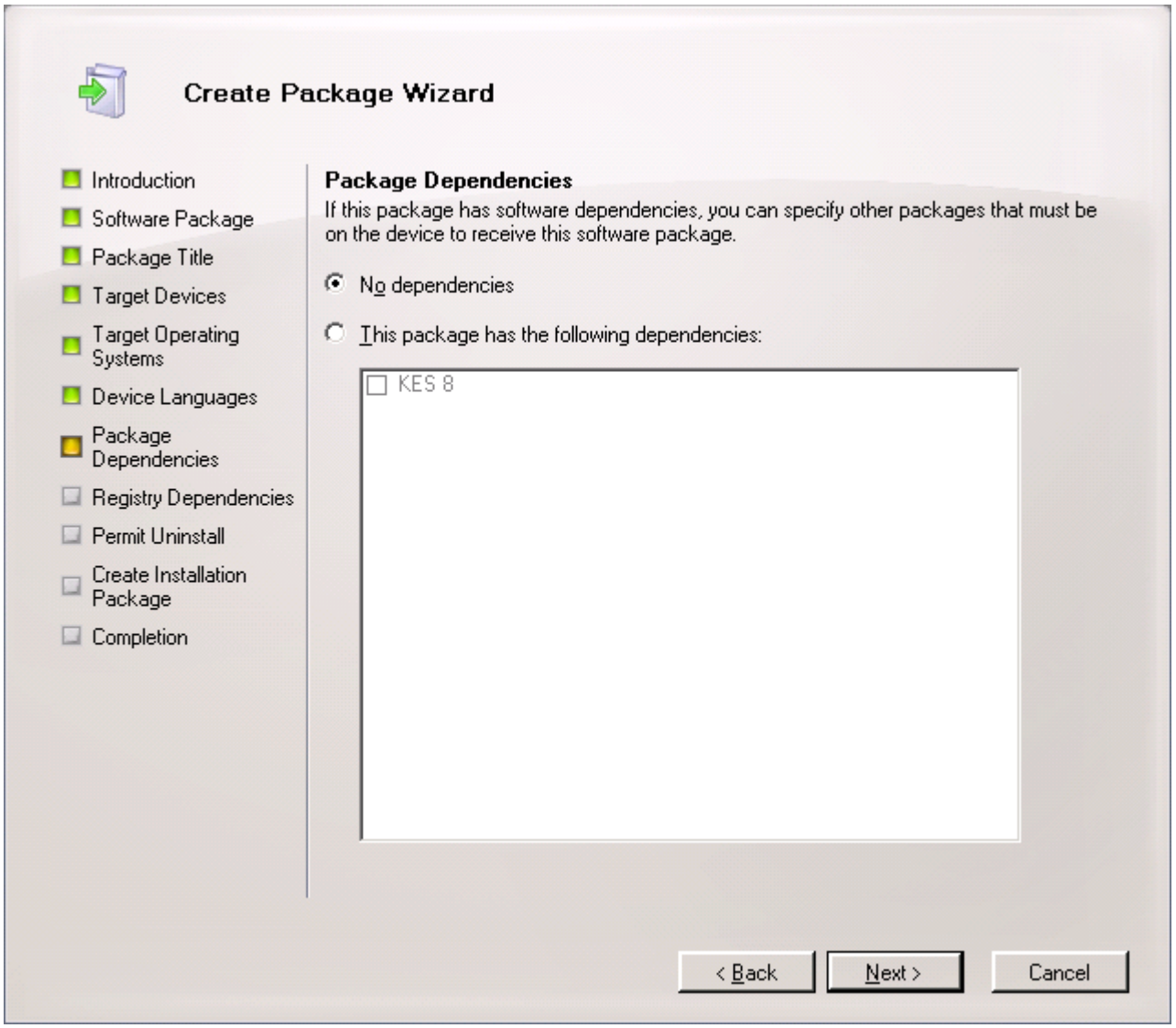


*Рисунок 65. Закладка **Package Dependencies***

9. На закладке **Registry Dependencies** (см. рисунок ниже) укажите зависимости создаваемого пакета от наличия нужных ключей в реестре.

   Если таких зависимостей нет, выберите вариант **No registry dependencies**. Рекомендуется выбрать это значение.

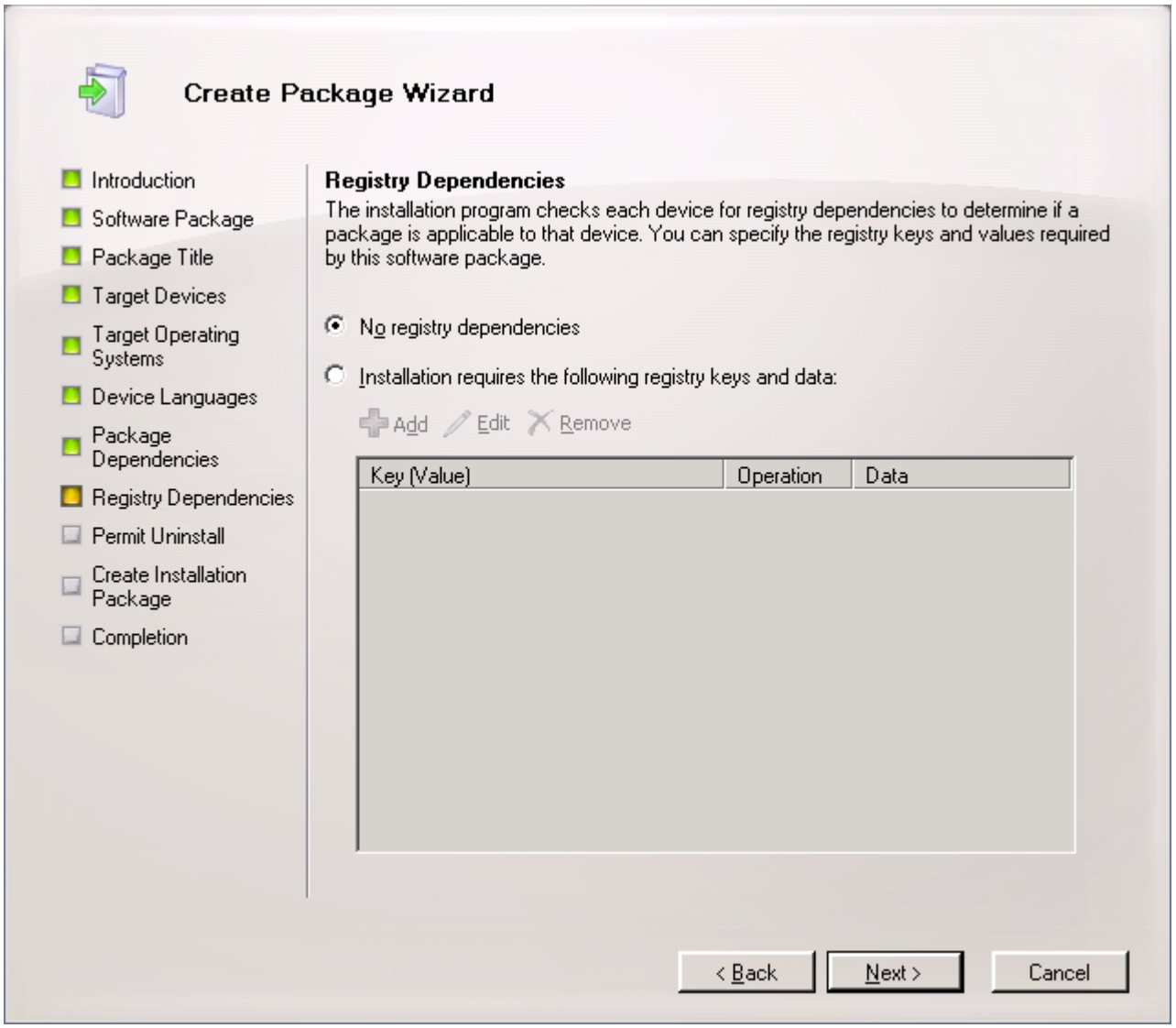


*Рисунок 66. Закладка **Registry Dependencies***

10. Если вы хотите, чтобы пользователь мог самостоятельно удалить программу с мобильного устройства, на закладке **Permit Uninstall** выберите вариант **Yes** (см. рисунок ниже).

    Если вы хотите, чтобы пользователь не мог самостоятельно удалить программу с мобильного устройства, на закладке **Permit Uninstall** выберите вариант **No**.

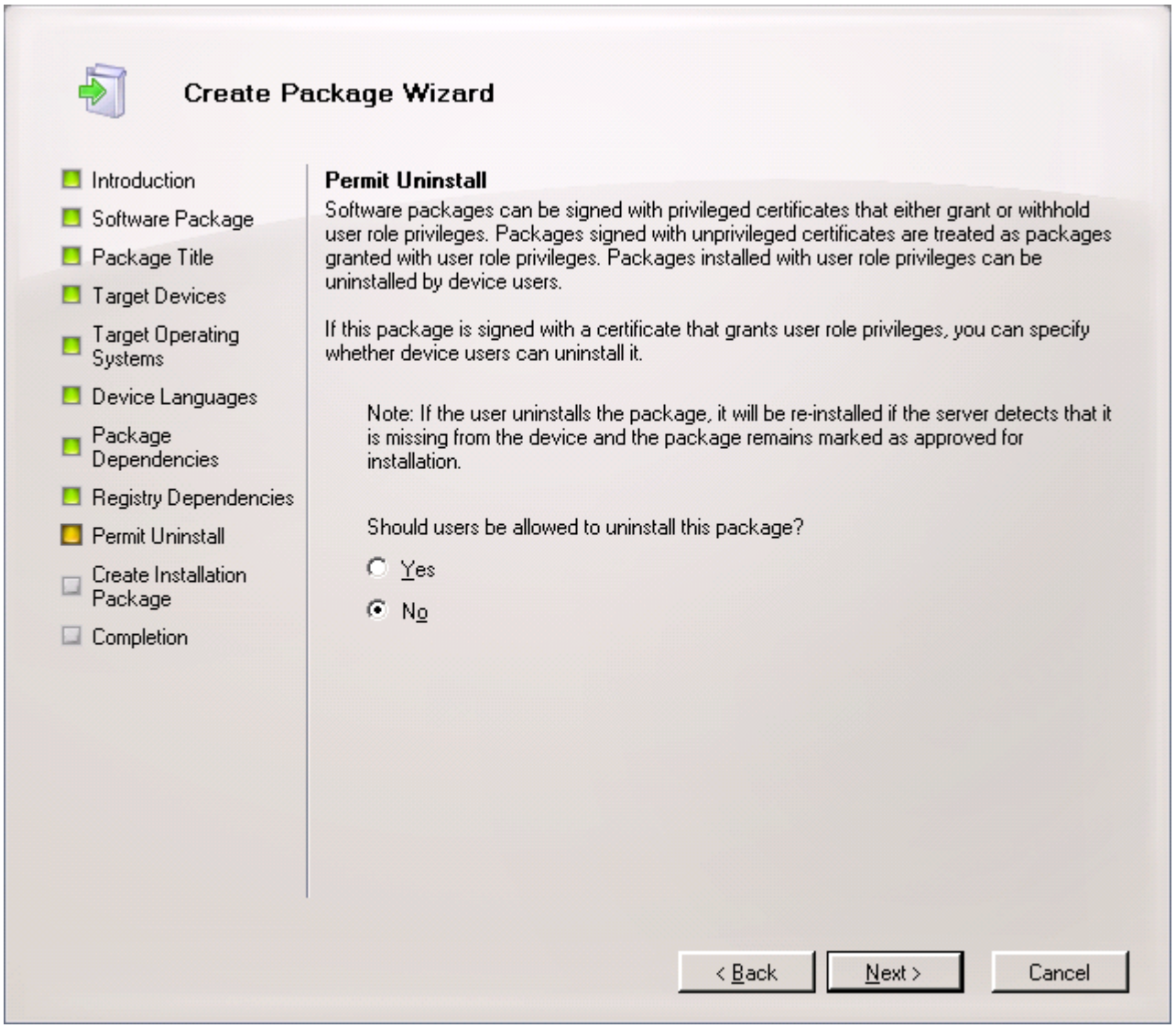


*Рисунок 67. Закладка **Permit Uninstall***

11. Нажмите на кнопку **Next**, чтобы продолжить работу мастера (см. рисунок ниже).

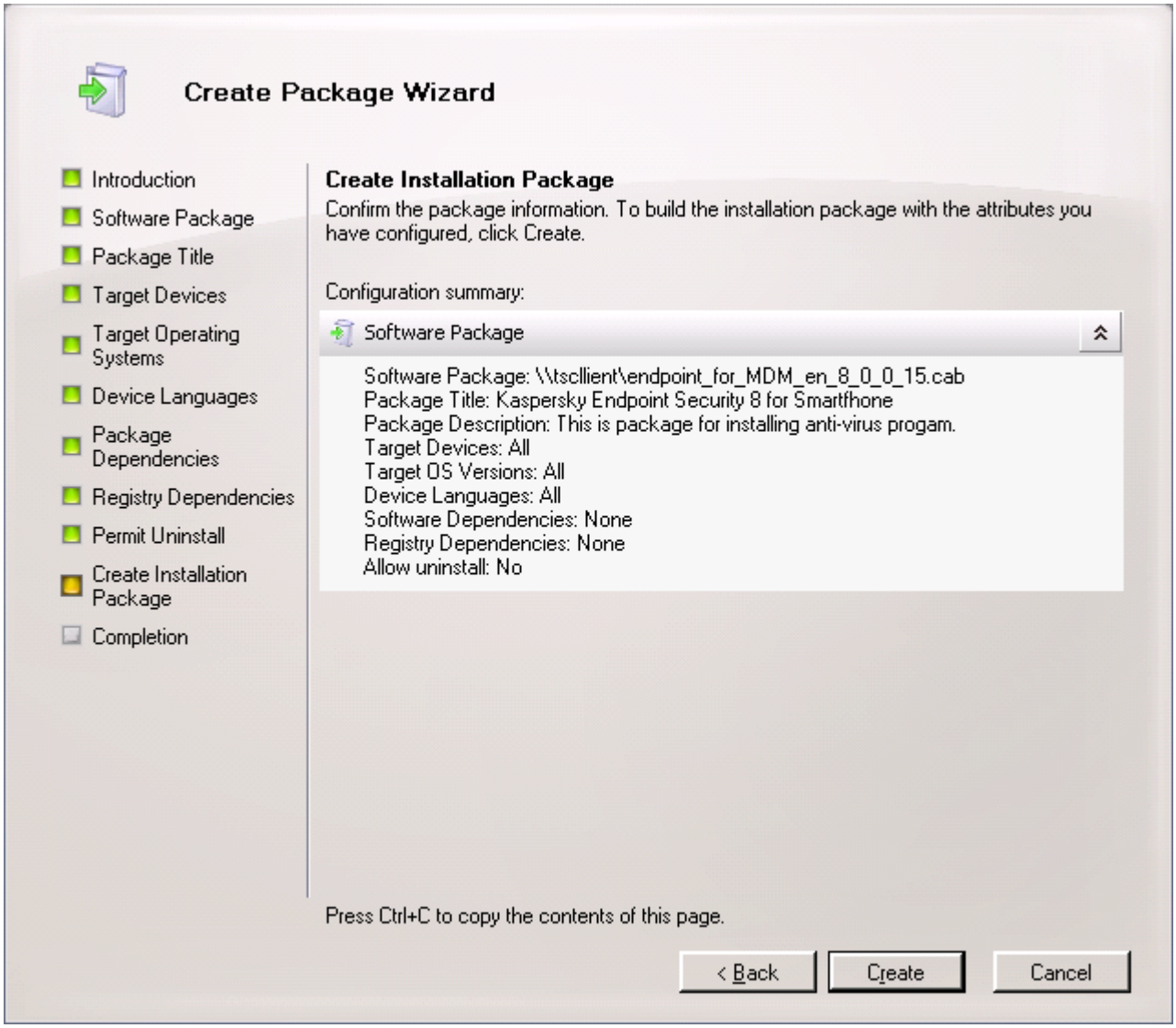


*Рисунок 68. Закладка **Create Installation Package***

12. Нажмите на кнопку **Create**. Мастер перейдет на закладку **Completion**, где отображается информация о создании инсталляционного пакета (см. рисунок ниже).

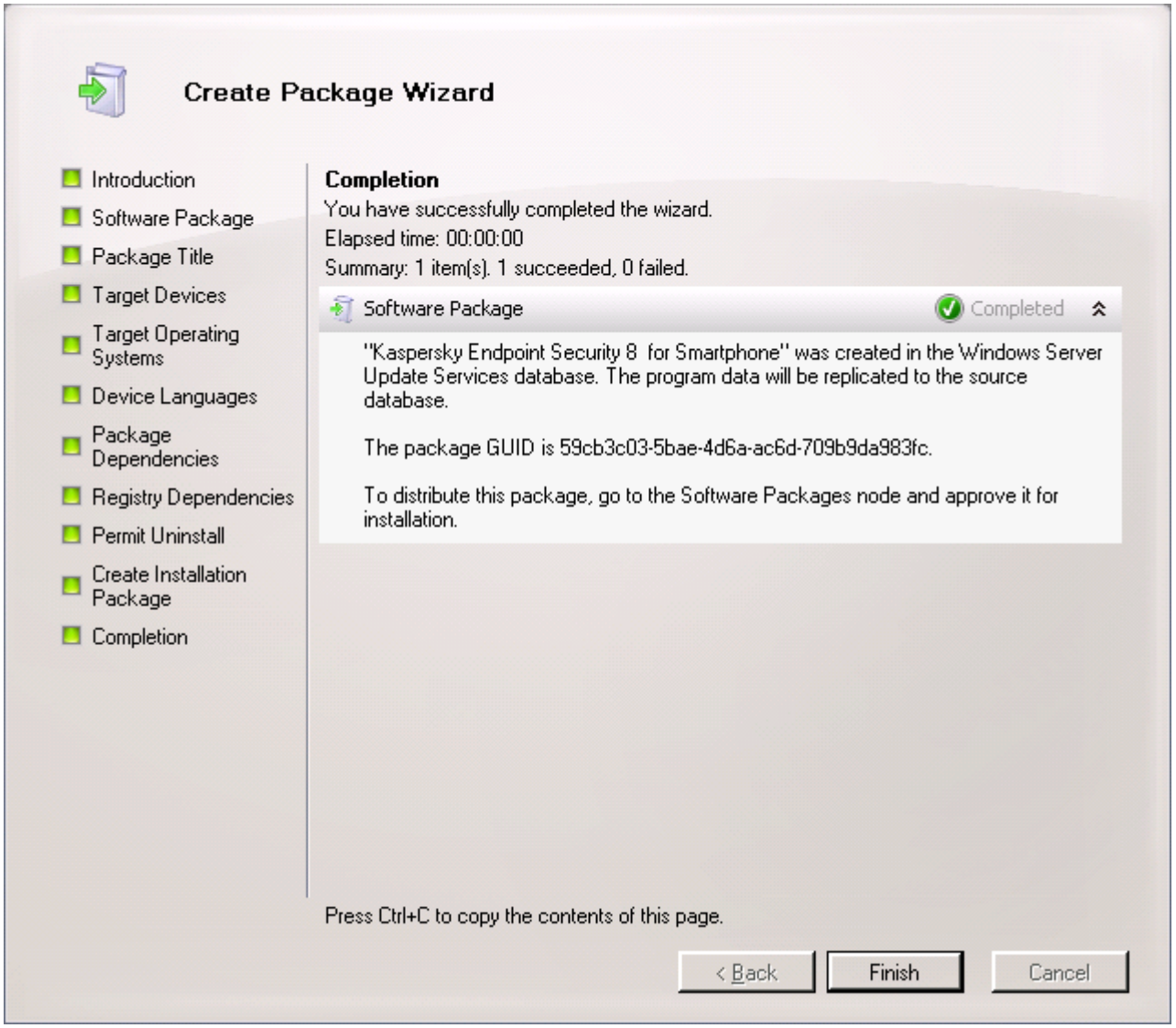


*Рисунок 69. Закладка **Completion***

После завершения работы мастера сформированный пакет будет добавлен в хранилище созданных пакетов в группу Software Packages и представлен в списке инсталляционных пакетов консоли System Center Mobile Device Manager Software Distribution. В дальнейшем вы можете использовать этот пакет для установки программы на мобильные устройства пользователей.

УСТАНОВКА ПРОГРАММЫ НА МОБИЛЬНЫЕ УСТРОЙСТВА

Вы можете дистанционно устанавливать Kaspersky Endpoint Security 8 for Smartphone на мобильные устройства пользователей, зарегистрированные в домене.

Чтобы установить Kaspersky Endpoint Security 8 for Smartphone на мобильные устройства пользователей, выполните следующие действия:

1. Откройте консоль System Center Mobile Device Manager Software Distribution.
2. В хранилище инсталляционных пакетов выберите инсталляционный пакет программы.
3. Откройте контекстное меню и выберите пункт **Approve**.

4. В открывшемся окне **Approve Packages** выберите группу мобильных устройств, на которые требуется установить программу.

5. Откройте контекстное меню и выберите пункт **Approved for Install**.

   В результате при следующей синхронизации мобильных устройств с сервером MDM Kaspersky Endpoint Security 8 for Smartphone установится на них.

Удаление программы с мобильных устройств

Вы можете дистанционно удалить Kaspersky Endpoint Security 8 for Smartphone с мобильных устройств пользователей, зарегистрированных в домене.

Чтобы удалить Kaspersky Endpoint Security 8 for Smartphone с мобильных устройств пользователей, выполните следующие действия:

1. Откройте консоль System Center Mobile Device Manager Software Distribution.

2. В хранилище инсталляционных пакетов выберите инсталляционный пакет программы.

3. Откройте контекстное меню и выберите пункт **Approve**.

4. В открывшемся окне **Approve Packages** выберите группу мобильных устройств, с которых требуется удалить программу.

5. Откройте контекстное меню и выберите пункт **Approved for Removal**.

   В результате при следующей синхронизации мобильных устройств с сервером MDM Kaspersky Endpoint Security 8 for Smartphone будет удален на них.

РАЗВЕРТЫВАНИЕ ПРОГРАММЫ ЧЕРЕЗ SYBASE AFARIA

В этом разделе рассмотрен процесс развертывания Kaspersky Endpoint Security 8 for Smartphone через Sybase Afaria.

В ЭТОМ РАЗДЕЛЕ

КОНЦЕПЦИЯ УПРАВЛЕНИЯ ПРОГРАММОЙ ЧЕРЕЗ SYBASE AFARIA

Все параметры работы программы, включая лицензию, определяются через политику Kaspersky Endpoint Security 8 for Smartphone. При помощи политики могут быть установлены одинаковые значения параметров работы программы для целевых групп устройств.

Создание и редактирование политик для Kaspersky Endpoint Security 8 for Smartphone выполняется с помощью утилиты управления политиками KES2Afaria.exe, входящей в состав дистрибутива программы. С помощью утилиты администратор настраивает параметры программы и сохраняет их в файл политики с расширением kes (см. раздел «Создание политики. Настройка параметров Kaspersky Endpoint Security 8 for Smartphone» на стр. 132).

Утилита может быть установлена на рабочем месте администратора либо на сервере Sybase Afaria (см. раздел «Установка утилиты управления политикой» на стр. 132).

Файл политики должен размещаться на сервере Sybase Afaria. Если утилита установлена на другом компьютере, то после настройки параметров администратор должен копировать файл политики на сервер Sybase Afaria.

После создания файла политики администратор создает канал, который копирует файл политики на мобильные устройства. В дальнейшем администратор должен обеспечить доставку канала на мобильные устройства. Доставка осуществляется стандартными средствами Sybase Afaria.

Для операционных систем Microsoft Windows Mobile и Symbian рекомендуется использовать два отдельных канала для копирования файла политики и установки программы. Это позволяет избежать повторной установки программы при обновлении политики. Для операционных систем BlackBerry рекомендуется использовать один канал, в котором задана последовательность установки программы.

Администратор может создать несколько файлов политик. При копировании файла политики на устройства он должен называться policy.kes. Программа не распознает файлы политик с другим именем.

После доставки канала с файлом политики на устройства файл политики будет сохранен в выбранную администратором папку. Для операционных систем Microsoft Windows Mobile администратор должен указать папку **\Temp**, для операционных систем Symbian – папку **C:\Data**. Для операционной системы BlackBerry файл политики автоматически сохраняется в папку **store\home\user**.

В случае изменения файла политики на сервере изменения параметров будут доставлены на устройства в ходе очередной синхронизации устройств с Sybase Afaria. Синхронизация мобильных устройств с Sybase Afaria выполняется с периодичностью, заданной администратором в мониторе.

При удалении файла политики с устройства примененные значения параметров в программе останутся. Когда администратор обновит файл политики на сервере, при синхронизации устройств с Sybase Afaria файл политики будет снова скопирован на устройства.

Каждый параметр, представленный в политике, имеет атрибут – «замок», с помощью которого администратор может управлять изменением параметров программы на мобильных устройствах.

Если в политике для параметра установлен «замок», то в дальнейшем после применения политики на мобильных устройствах будут использоваться значения, заданные политикой. При этом пользователь мобильного устройства не сможет изменить эти значения. Для параметров, которые не были зафиксированы «замком», будут использоваться локальные значения, установленные по умолчанию или самим пользователем мобильного устройства.

После установки программы пользователь должен задать секретный код программы. После этого пользователь может настроить параметры работы Анти-Спама и Личных контактов и других компонентов, если администратор не наложил запрет на их изменение.

Схема развертывания программы через Sybase Afaria

В состав дистрибутива для Sybase Afaria входит самораспаковывающийся архив KES8_forSybaseAfaria_ru.exe, который содержит следующие файлы, необходимые для установки программы на мобильных устройствах:

- endpoint_MDM_Afaria_8_0_x_xx_ru.cab – установочный файл программы для операционной системы Microsoft Windows Mobile;
- endpoint8_mobile_8_x_xx_eu4.sisx – установочный файл программы для операционной системы Symbian;
- Endpoint8_Mobile_Installer.cod – файл установки программы для операционной системы BlackBerry;
- KES2Afaria.exe – утилита управления политикой программы Kaspersky Endpoint Security 8 for Smartphone;
- kl.pbv, licensing.dll, oper.pbv – набор файлов, входящий в состав утилиты KES2Afaria.exe и необходимый для ее работы.

Установка выполняется по стандартной схеме установки программ через Sybase Afaria.

Администратор устанавливает утилиту управления политиками KES2Afaria.exe либо на рабочей станции, либо непосредственно на сервере Sybase Afaria. После установки утилиты администратор создает политику, включает в нее лицензию и сохраняет настроенные параметры программы в файл политики. Если лицензии нет, администратор может добавить ее позже.

После этого администратор создает канал для применения политики и для установки программы на устройства. Для операционных систем Microsoft Windows Mobile и Symbian рекомендуется использовать два канала Software Manager Channel для копирования файла политики и дистрибутива программы на устройства.

Для операционной системы BlackBerry следует использовать один канал Session Manager Channel. В нем администратор создает рабочий список (worklist), в котором создает скрипт с последовательностью установки программы.

Администратор должен выполнять установку программы в строгой последовательности: сначала передавать на устройства файл политики, после этого дистрибутив программы. При выполнении установки программы на устройства в другой последовательности программа не будет работать.

Публикация и доставка каналов выполняется стандартными методами Sybase Afaria. При синхронизации Sybase Afaria с мобильными устройствами каналы доставляются на устройства, после чего на них копируется файл политики и запускается автоматическая установка программы. После установки применяются настроенные администратором параметры программы.

Если администратор добавил в состав политики лицензию, то при применении политики лицензия будет установлена и программа будет активирована.

При первом запуске программы пользователь должен задать секретный код. После этого пользователь может установить параметры компонентов Анти-Спам и Личные контакты и других компонентов, если администратор не наложил запрет на их изменение.

В дальнейшем администратор может менять параметры политики. Когда администратор обновит файл политики на сервере, при следующей синхронизации устройств с Sybase Afaria файл политики обновится на устройстве, и параметры программы будут изменены.

Таким образом, развертывание программы состоит из следующих этапов:

1. Установка утилиты (см. раздел «Установка утилиты управления политикой» на стр. 132).
2. Создание политики, настройка параметров программы и добавление лицензии программы.
3. Создание канала / объединения каналов для установки программы на устройства и применения политики (см. раздел «Установка программы» на стр. 151).
4. Распространение канала / объединения каналов на устройства. Это действие выполняется стандартными средствами Sybase Afaria.
5. Установка программы на мобильных устройствах (см. раздел «Установка программы на мобильные устройства» на стр. 157).

ПОДГОТОВКА К РАЗВЕРТЫВАНИЮ KASPERSKY ENDPOINT SECURITY 8 FOR SMARTPHONE

Перед развертыванием Kaspersky Endpoint Security 8 for Smartphone через Sybase Afaria администратор должен убедиться, что выполнены следующие условия:

1. В сети развернут и настроен Sybase Afaria.
2. Устройства соответствуют программным и системным требованиям для установки программы.
3. Созданы группы устройств (Groups) на сервере Sybase Afaria.
4. Созданы профили устройств (Profiles) на сервере Sybase Afaria.
5. Настроена синхронизация устройств с сервером Sybase Afaria: на устройствах установлена программа **Client Afaria**.

Установка утилиты управления политикой

Утилита KES2Afaria.exe используется для создания и изменения политик Kaspersky Endpoint Security 8 for Smartphone.

Утилита входит в состав дистрибутива KES8_forSybaseAfaria_ru.exe и может быть установлена на рабочем месте администратора или на сервере Sybase Afaria.

Для работы утилиты необходимы файлы kl.pbv, licensing.dll, oper.pbv. Они также входят в состав дистрибутива программы и должны храниться в одной папке с утилитой.

Чтобы установить утилиту,

из дистрибутива программы скопируйте файлы KES2Afaria.exe, kl.pbv, licensing.dll, oper.pbv в одну папку на рабочую станции или на сервер Sybase Afaria.

Создание политики. Настройка параметров Kaspersky Endpoint Security 8 for Smartphone

После установки утилиты KES2Afaria.exe вам необходимо создать политику Kaspersky Endpoint Security 8 for Smartphone.

Вы можете создать новую политику или изменить параметры программы в существующей политике (см. раздел «Редактирование политики» на стр. 151).

При редактировании параметров политики вы можете использовать кнопку для того, чтобы разрешить / запретить изменение параметров на мобильном устройстве.

В следующих разделах приведены более подробные процедуры настройки параметров каждого компонента программы.

Чтобы создать политику Kaspersky Endpoint Security 8 for Smartphone, выполните следующие действия:

1. Запустите утилиту **KES2Afaria.exe**.

   Откроется окно **Kaspersky Endpoint Security 8 for Smartphone** с параметрами компонентов программы.

2. Настройте параметры каждого компонента программы.

3. Сохраните полученный файл политики, выбрав меню **Файл** → **Сохранить как**.

Если вы установили утилиту на рабочей станции, после настройки параметров скопируйте полученный файл политики на сервер.

В ЭТОМ РАЗДЕЛЕ

Настройка параметров функции Защита

Чтобы настроить параметры функции Защита, выполните следующие действия:

1. Откройте закладку **Защита** в окне **Kaspersky Endpoint Security 8 for Smartphone** (см. рисунок ниже).

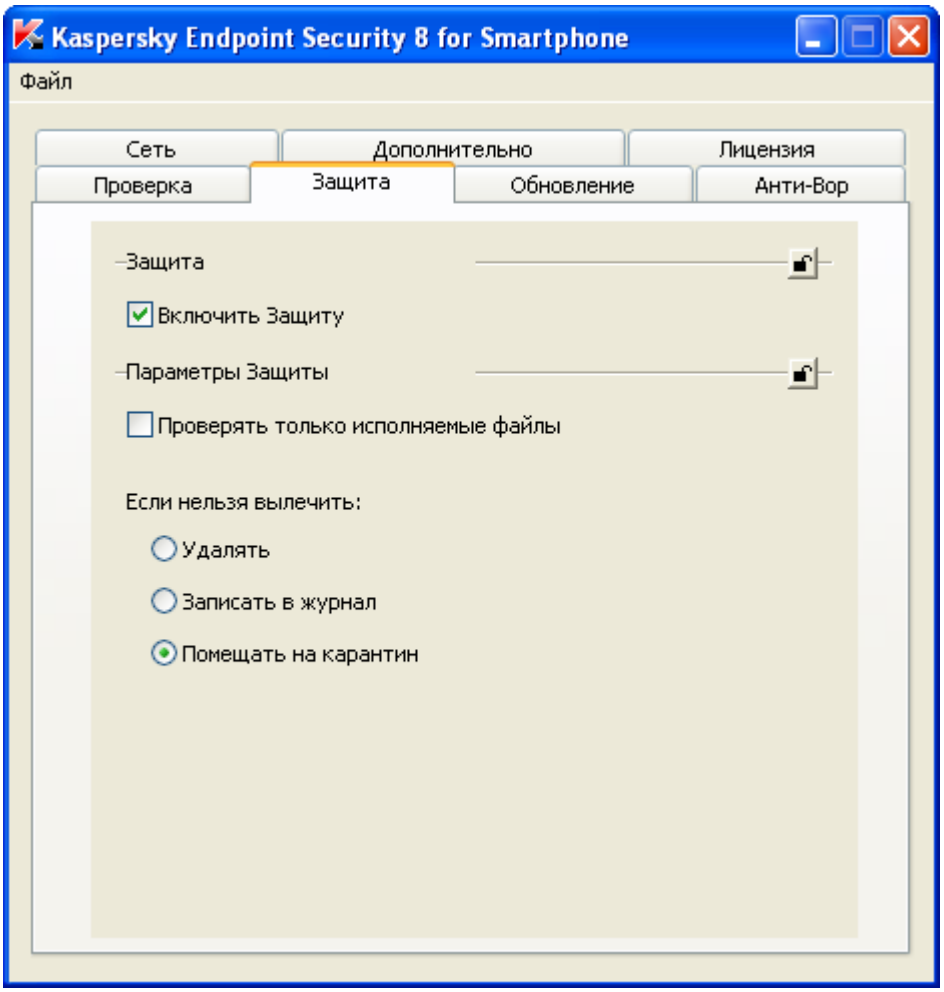


*Рисунок 70. Закладка **Защита***

2. Включите / отключите использование Защиты на устройстве. Для этого в блоке **Защита** установите / снимите флажок **Включить Защиту**.

   По умолчанию Защита включена, флажок **Включить Защиту** установлен.

3. Выберите тип файлов, которые проверяет Kaspersky Endpoint Security 8 for Smartphone.

   Чтобы программа проверяла только исполняемые файлы, в блоке **Параметры Защиты** установите флажок **Проверять только исполняемые файлы**.

   Чтобы программа проверяла файлы всех типов, снимите флажок **Проверять только исполняемые файлы**.

   По умолчанию программа проверяет все типы файлов, флажок **Проверять только исполняемые файлы** снят.

4. Выберите действие, которое выполняет Kaspersky Endpoint Security 8 for Smartphone при обнаружении угрозы. Для этого в блоке **Параметры Защиты** выберите одно из предложенных значений для параметра **Если нельзя вылечить**:

   - **Удалять** – физически удалять вредоносные объекты без уведомления пользователя.
   - **Записать в журнал** – пропускать вредоносные объекты, при этом записывая информацию об их обнаружении в журнал программы; блокировать объект при попытке к нему обратиться (например, скопировать или открыть его).
   - **Помещать на карантин** – помещать вредоносные объекты на карантин.

   По умолчанию программа помещает обнаруженные вредоносные объекты на карантин, выбрано значение **Помещать на карантин**.

НАСТРОЙКА ПАРАМЕТРОВ ФУНКЦИИ ПРОВЕРКА ПО ТРЕБОВАНИЮ

Чтобы настроить параметры Проверки по требованию, выполните следующие действия:

1. Откройте закладку **Проверка** в окне **Kaspersky Endpoint Security 8 for Smartphone** (см. рисунок ниже).

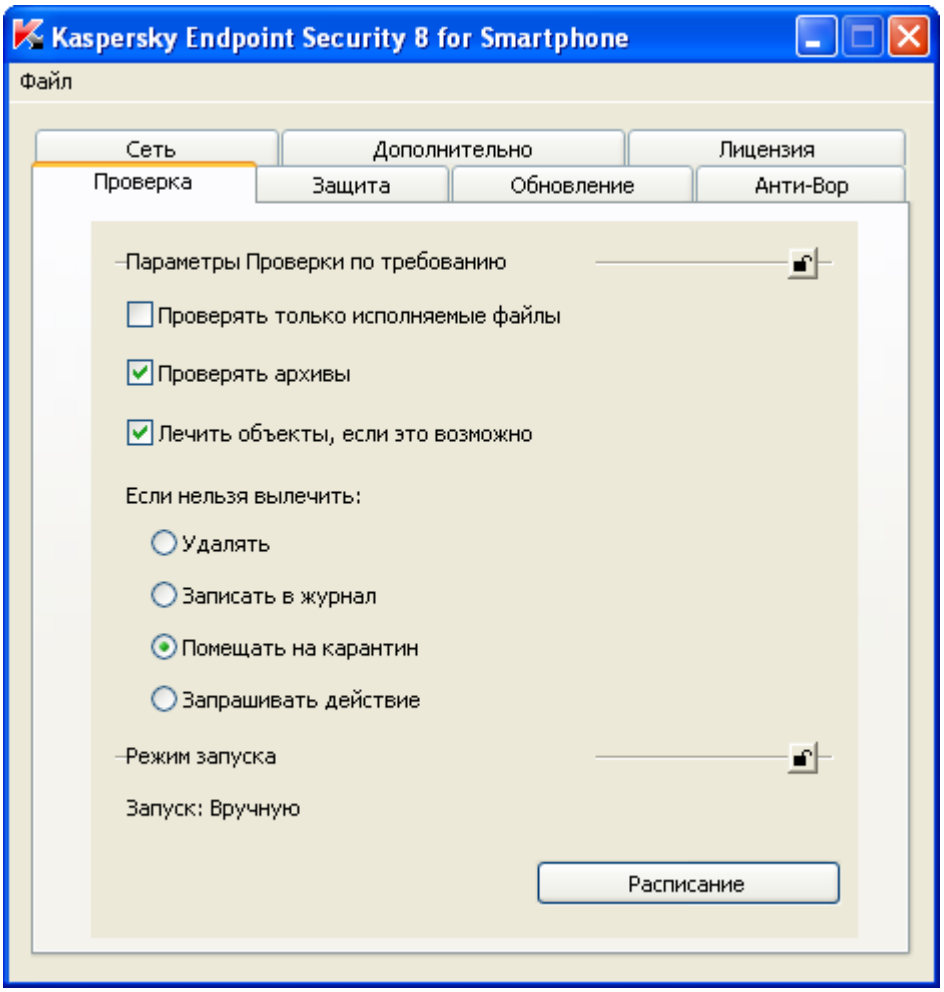


*Рисунок 71. Закладка **Проверка***

2. Выберите тип файлов, которые проверяет Kaspersky Endpoint Security 8 for Smartphone.

   Чтобы программа проверяла только исполняемые файлы, в блоке **Параметры Проверки по требованию** установите флажок **Проверять только исполняемые файлы**. Поддерживается проверка исполняемых файлов программ следующих форматов: EXE, DLL, MDL, APP, RDL, PRT, PXT, LDD, PDD, CLASS.

   Чтобы программа проверяла файлы всех типов, в блоке **Параметры Проверки** по требованию снимите флажок **Проверять только исполняемые файлы**.

   По умолчанию программа проверяет файлы всех типов, флажок **Проверять только исполняемые файлы** снят.

3. Включите / отключите проверку архивов на устройствах. Для этого в блоке **Параметры проверки по требованию** установите / снимите флажок **Проверять архивы**.

   Для Microsoft Windows Mobile программа проверяет архивы следующих форматов: ZIP, JAR, JAD и CAB. Для Symbian OS программа позволяет проверять архивы следующих форматов: ZIP, JAR, JAD, SIS и SISX.

   Если флажок **Проверять архивы** не установлен и флажок **Проверять только исполняемые типы файлов** снят, то программа будет проверять все файлы, кроме файлов, запакованных в архив.

   По умолчанию программа распаковывает и проверяет архивы, флажок **Проверять архивы** установлен.

4. Включите / отключите попытку программы лечить обнаруженные объекты при их обнаружении. Для этого в блоке **Параметры Проверки по требованию** установите / снимите флажок **Лечить объекты, если это возможно**.

   По умолчанию программа пытается вылечить обнаруженный вредоносный объект, флажок **Лечить объекты, если это возможно** установлен.

5. Выберите действие, которое выполняет программа при обнаружении вредоносных объектов. Для этого в блоке **Параметры Проверки по требованию** выберите одно из предложенных значений для параметра **Если нельзя вылечить**:

   - **Удалять** – физически удалять вредоносные объекты без уведомления пользователя.
   - **Записать в журнал** – пропускать вредоносные объекты, при этом записывая информацию об их обнаружении в журнал программы.
   - **Помещать на карантин** – блокировать объект, переместить вредоносный объект в специальную папку – карантин.
   - **Запрашивать действие** – при обнаружении вредоносного объекта уведомить пользователя и предложить выбрать действие над обнаруженным объектом.

6. Выберите режим запуска Проверки по требованию на устройстве. Для этого в блоке **Режим запуска** нажмите на кнопку **Расписание** и в открывшемся окне **Расписание** выберите один из следующих типов запуска:

   - **Вручную** – отключить проверку по расписанию. Пользователь запускает проверку в любое удобное для него время.

- **Ежедневно** – производить проверку каждый день. В поле **Время запуска** укажите время запуска. Время указывается в 24 часовом формате ЧЧ:ММ.

- **Еженедельно** – производить проверку раз в неделю. Задайте время и день запуска проверки. Для этого в раскрывающемся списке выберите день запуска и в поле **Время запуска** укажите время запуска. Время указывается в 24 часовом формате ЧЧ:ММ.

По умолчанию Проверка по требованию запускается пользователем вручную, для параметра **Тип запуска** выбрано значение **Вручную**.

НАСТРОЙКА ПАРАМЕТРОВ ОБНОВЛЕНИЯ АНТИВИРУСНЫХ БАЗ

Чтобы настроить параметры обновления антивирусных баз, выполните следующие действия:

1. Откройте закладку **Обновление** в окне **Kaspersky Endpoint Security 8 for Smartphone** (см. рисунок ниже).

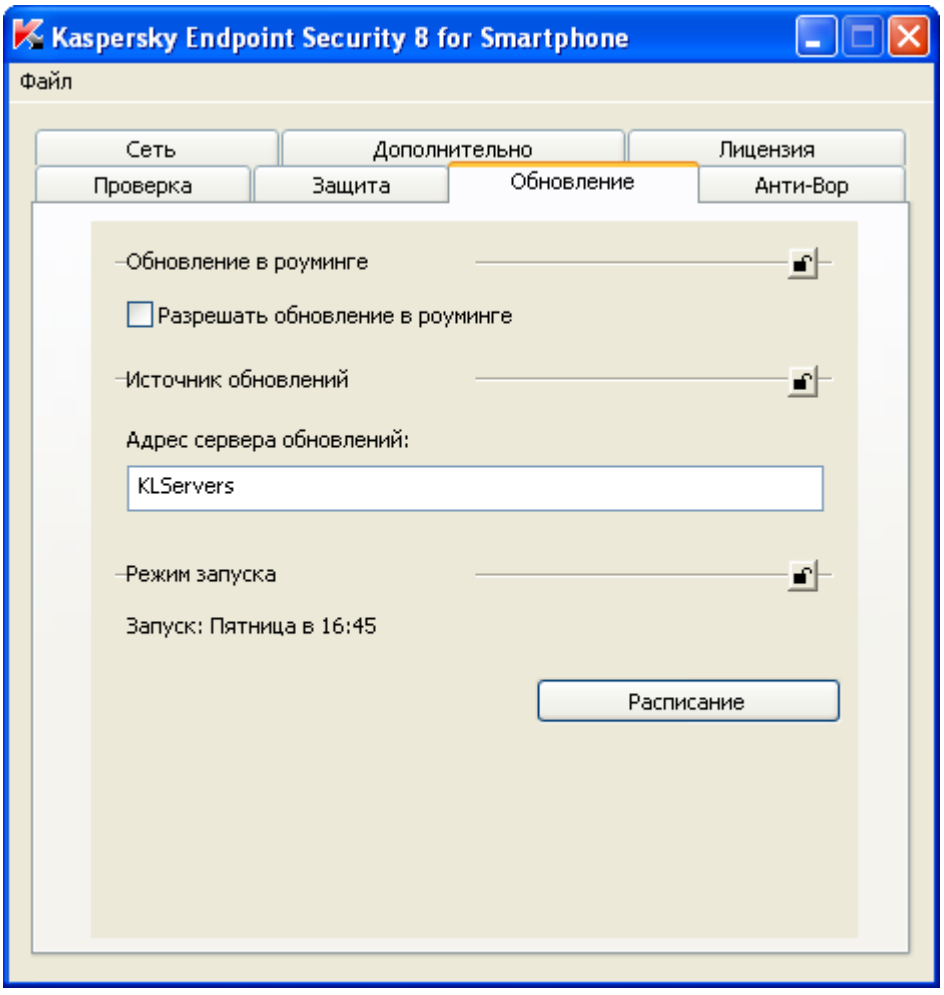


*Рисунок 72. Закладка **Обновление***

2. Разрешите / запретите автоматическое обновление антивирусных баз по расписанию, когда устройство находится в зоне роуминга. Для этого в блоке **Обновление в роуминге** установите / снимите флажок **Разрешать обновление в роуминге**.

   По умолчанию автоматическое обновление в роуминге запрещено, флажок **Разрешать обновление в роуминге** снят.

3. Задайте адрес источника, с которого программа будет загружать обновления антивирусных баз. Вы можете указать HTTP-сервер, локальную или сетевую папку (например, http://domain.com/index/). Для этого в блоке **Источник обновлений** заполните поле **Адрес сервера обновлений**.

   Структура папок в источнике обновлений должна повторять структуру на серверах обновлений «Лаборатории Касперского».

   По умолчанию введен адрес серверов обновлений «Лаборатории Касперского» **KLServers**.

4. Выберите режим запуска обновления. Для этого в блоке **Режим запуска** нажмите на кнопку **Расписание** и в открывшемся окне **Расписание** выберите один из следующих типов запуска:

   - **Вручную** – отключить обновление по расписанию. Пользователь запускает обновление антивирусных баз программы в любое удобное для него время.
   - **Ежедневно** – производить обновление каждый день. В поле **Время запуска** укажите время запуска. Время указывается в 24 часовом формате ЧЧ:ММ.
   - **Еженедельно** – производить обновление раз в неделю. Задайте время и день запуска обновления. Для этого в раскрывающемся списке выберите день запуска и в поле **Время запуска** укажите время запуска. Время указывается в 24 часовом формате ЧЧ:ММ.

   По умолчанию обновление запускается еженедельно, для параметра **Тип запуска** выбрано значение **Еженедельно**. Для дня запуска указан текущий день. Для времени запуска указано время запуска утилиты +1 минута.

Настройка параметров компонента Анти-Вор

Настройка параметров компонента Анти-Вор состоит из настройки следующих функций:

- Удаление данных (см. раздел «Настройка параметров функции Удаление данных» на стр. 138).
- Блокирование (см. раздел «Настройка параметров функции Блокирование» на стр. 141).
- SIM-Контроль (см. раздел «Настройка параметров функции SIM-Контроль» на стр. 142).
- GPS-Поиск (см. раздел «Настройка параметров функции GPS-Поиск» на стр. 143).

В этом разделе

НАСТРОЙКА ПАРАМЕТРОВ ФУНКЦИИ УДАЛЕНИЕ ДАННЫХ

Чтобы настроить параметры функции Удаления данных, выполните следующие действия:

1. Откройте закладку **Анти-Вор** в окне **Kaspersky Endpoint Security 8 for Smartphone** (см. рисунок ниже).

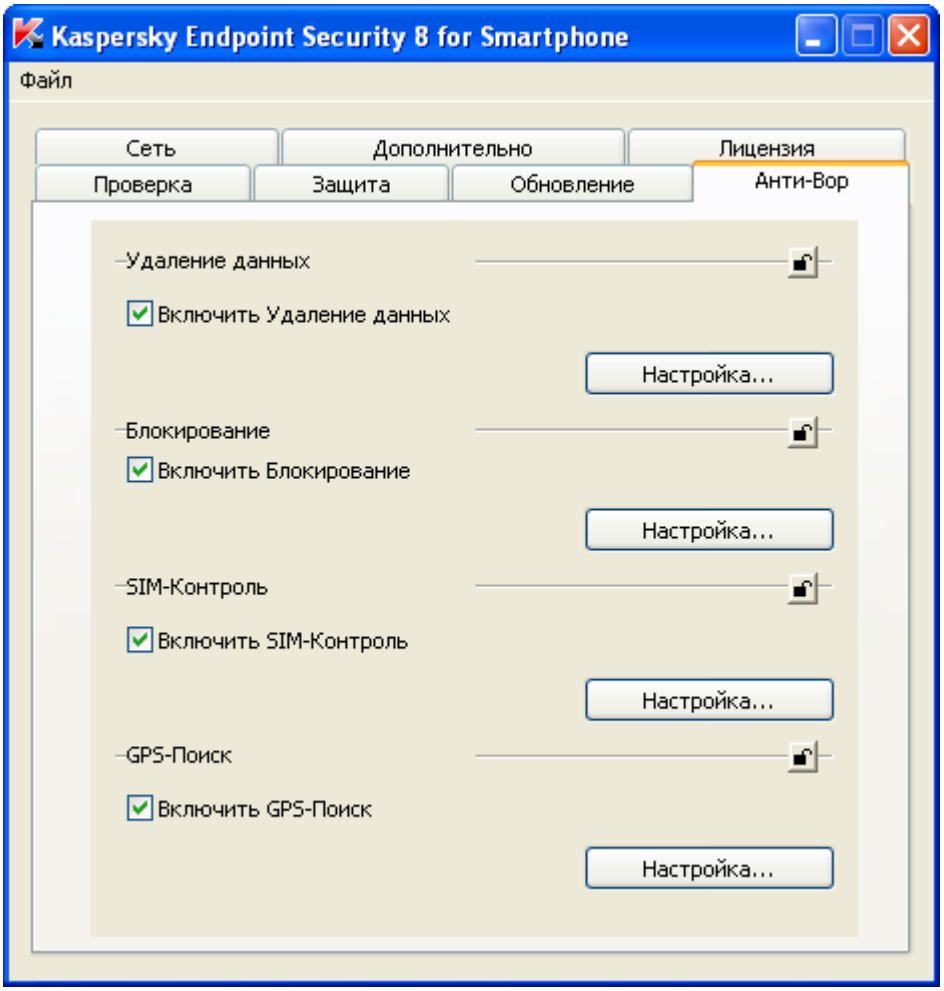


*Рисунок 73. Закладка **Анти-Вор***

2. Включите / отключите использование функции Удаление данных на устройстве. Для этого в блоке **Удаление данных** установите / снимите флажок **Включить Удаление данных**.

   По умолчанию функция Удаление данных отключена.

3. Если вы включили использование функции Удаление данных, выберите информацию, которую программа будет удалять с устройства при получении SMS-команды. Для этого в блоке **Удаление данных** нажмите на кнопку **Настройка** и в открывшемся окне **Параметры Удаления данных** (см. рисунок ниже) выполните действия в зависимости от следующих условий:

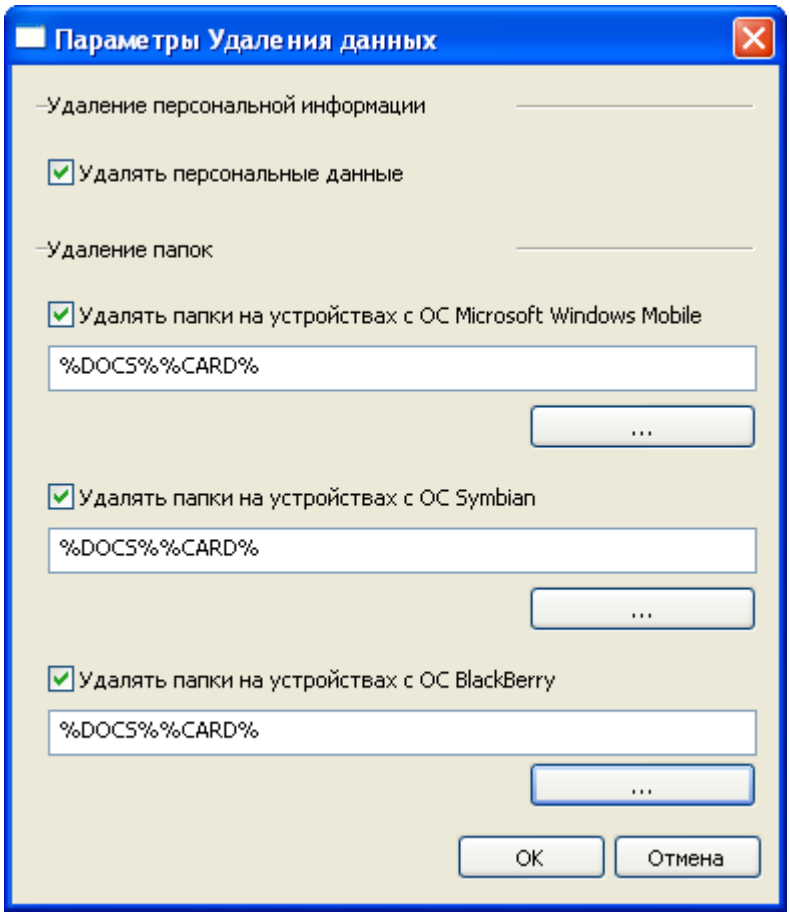


Рисунок 74. Параметры функции Удаление данных

- Чтобы программа удаляла персональные данные с устройства по команде пользователя, в блоке **Удаление персональной информации** установите флажок **Удалять персональные данные**.

  Для устройств с операционными системами Microsoft Windows Mobile и Symbian программа позволяет удалить следующую информацию: записи в Контактах и на SIM-карте, SMS, галерею, календарь, параметры подключения к интернету. Для устройств с операционной системой BlackBerry программа удаляет следующую персональную информацию: записи в Контактах, календарь, сообщения электронной почты, журнал вызовов. Пользователь не сможет восстановить эти данные! Функция активизируется, когда на устройстве получена специальная SMS-команда.

  По умолчанию флажок **Удалять персональные данные** установлен.

- Чтобы программа по команде пользователя удаляла файлы с устройства из сформированного списка папок для удаления, в блоке **Удаление папок** установите флажок **Удалять папки на устройствах с ОС <название_операционной_системы>**, нажмите на кнопку ... и в открывшемся окне **Выбор папок для удаления** перечислите папки для удаления.

  Список папок для удаления состоит из папок, добавленных администратором, и из папок, добавленных вручную пользователем на устройстве. Папки, добавленные в список администратором, пользователь не может удалить из списка.

  При формировании списка папок вы можете использовать макросы папок. Чтобы использовать макрос для удаления содержимого папки **Мои документы**, в окне **Выбор папок для удаления** нажмите на кнопку **Мои документы**. Будет добавлен макрос **%DOCS%**. Чтобы использовать макрос для удаления содержимого карты памяти, в окне **Выбор папок для удаления** нажмите на кнопку **Карта памяти**. Будет добавлен макрос **%CARD%**.

Для операционной системы Microsoft Windows Mobile при использовании **%DOCS%** программа удалит папку **Мои документы** (точное название зависит от локализации устройства), при использовании **%CARD%** программа удалит папки на всех доступных картах памяти на устройстве.

Для операционной системы Symbian при использовании **%DOCS%** программа удалит папку **C:\Data**, при использовании **%CARD%** программа удалит папки на всех доступных картах памяти на устройстве.

Для операционной системы BlackBerry при использовании **%DOCS%** программа удалит папку **\store\home\user\documents**, при использовании **%CARD%** программа удалит папку **\SDCard**.

По умолчанию список папок для удаления пуст.

НАСТРОЙКА ПАРАМЕТРОВ ФУНКЦИИ БЛОКИРОВАНИЕ

Чтобы настроить параметры Блокирования, выполните следующие действия:

1. Откройте закладку **Анти-Вор** в окне **Kaspersky Endpoint Security 8 for Smartphone** (см. рисунок ниже).

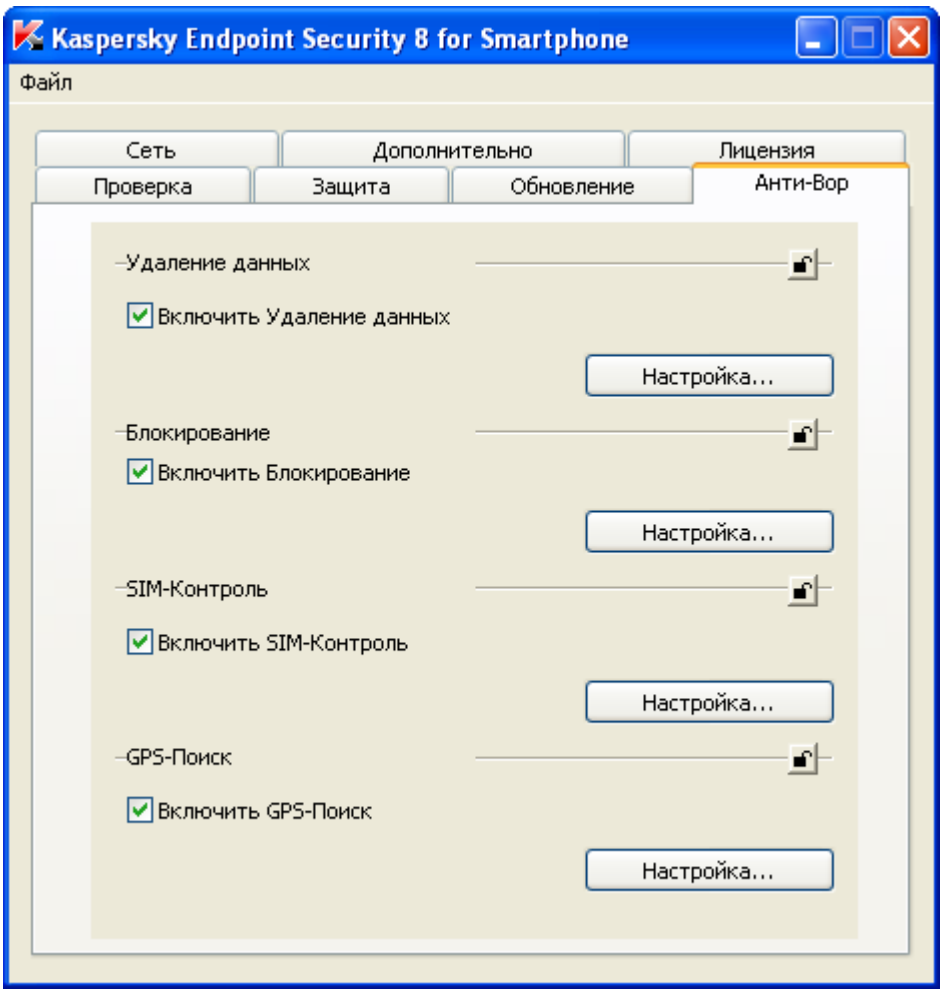


*Рисунок 75. Закладка **Анти-Вор***

2. Включите / отключите использование функции Блокирование на устройстве. Для этого в блоке **Блокирование** установите / снимите флажок **Включить Блокирование**.

   По умолчанию функция Блокирование отключена.

   Чтобы на экране заблокированного устройства отображался текст, в блоке **Блокирование** нажмите на кнопку **Настройка** и в открывшемся окне **Параметры Блокирования** заполните поле **Текст при блокировании**. По умолчанию текст не введен.

Настройка параметров функции SIM-Контроль

Чтобы настроить параметры Анти-Вора, выполните следующие действия:

1. Откройте закладку **Анти-Вор** в окне **Kaspersky Endpoint Security 8 for Smartphone** (см. рисунок ниже).

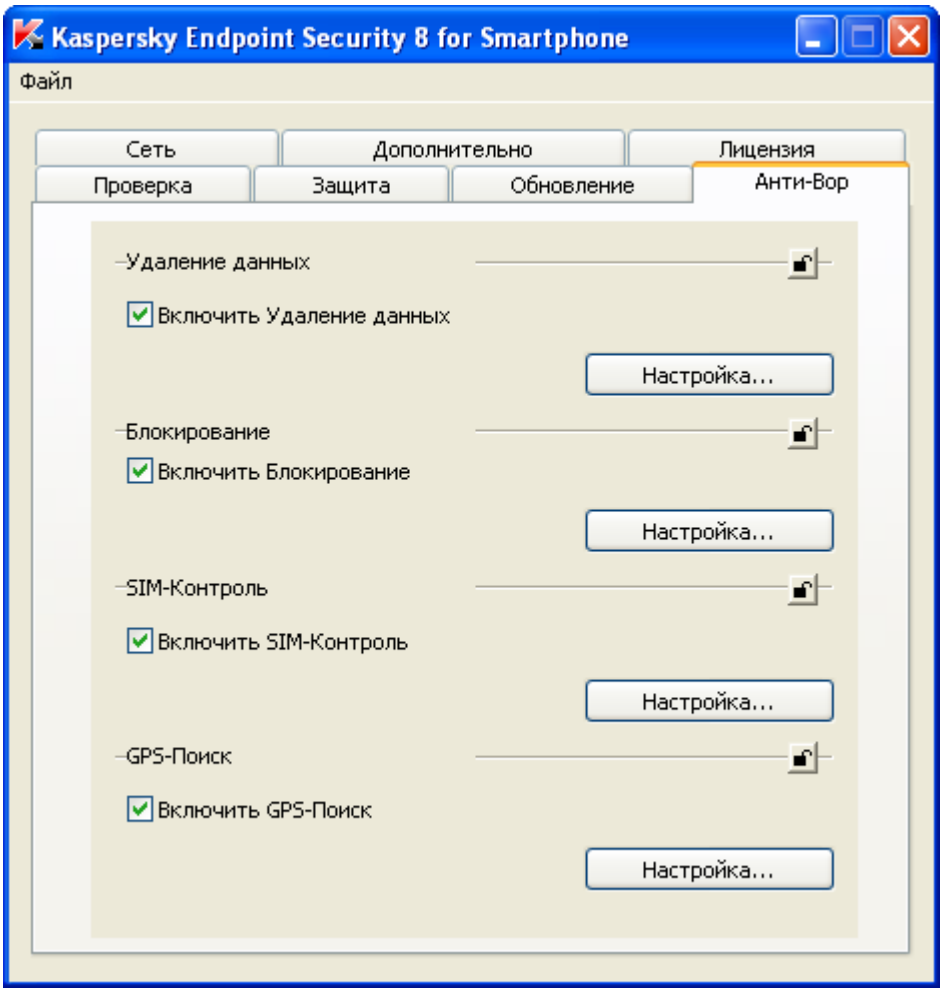


*Рисунок 76. Закладка **Анти-Вор***

2. Включите / отключите использование функции SIM-Контроль на устройстве. Для этого в блоке **SIM-Контроль** установите / снимите флажок **Включить SIM-Контроль**.

   По умолчанию функция SIM-Контроль отключена.

3. Укажите действия, которые выполнит программа при смене SIM-карты на устройстве.

   Чтобы при смене SIM-карты на устройстве программа отправляла новый номер телефона, в блоке **SIM-Контроль** нажмите **Настройка** и в открывшемся окне **Параметры SIM-Контроля** (см. рисунок ниже) выполните действия в зависимости от следующих условий:

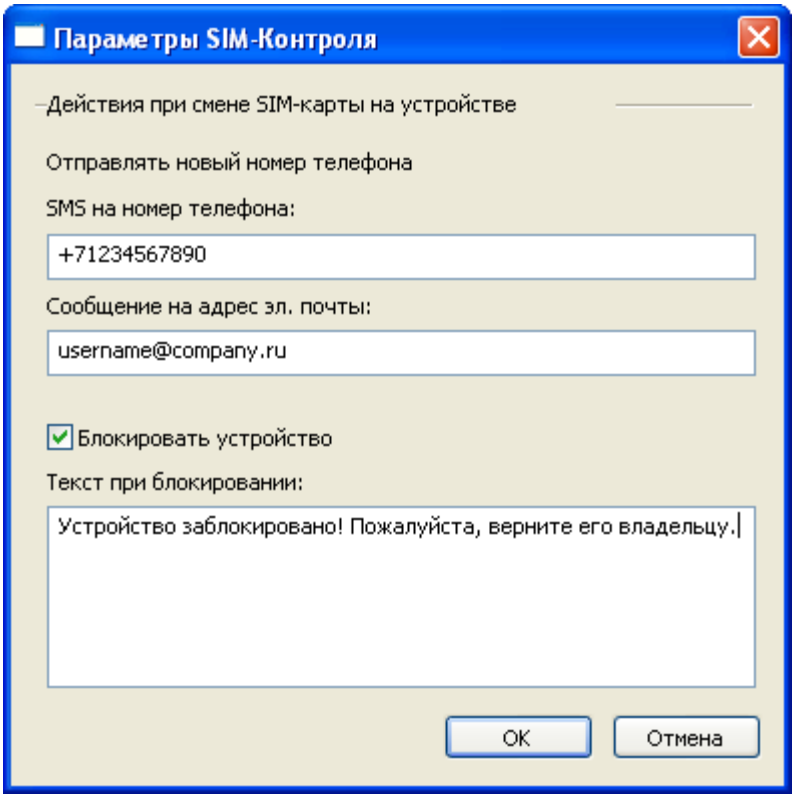


Рисунок 77. Параметры функции SIM-Контроль

- Чтобы программа отправляла новый номер в SMS на указанный номер телефона, введите его в поле **SMS на номер телефона**. Номер может начинаться с цифры или со знака «+» и должен содержать только цифры. Рекомендуется указывать номер в формате, который использует ваш оператор сотовой связи.

- Чтобы программа отправляла новый номер на адрес электронной почты, введите его в поле **Сообщение на адрес эл. почты**.

Чтобы при смене SIM-карты программа блокировала устройство, в блоке **SIM-Контроль** нажмите **Настройка**, в открывшемся окне **Параметры SIM-Контроля** установите флажок **Блокировать устройство** и в поле **Текст при блокировании** введите текст, который будет отображаться на экране заблокированного устройства.

Настройка параметров функции GPS-Поиск

Чтобы настроить параметры Анти-Вора, выполните следующие действия:

1. Откройте закладку **Анти-Вор** в окне **Kaspersky Endpoint Security 8 for Smartphone** (см. рисунок ниже).

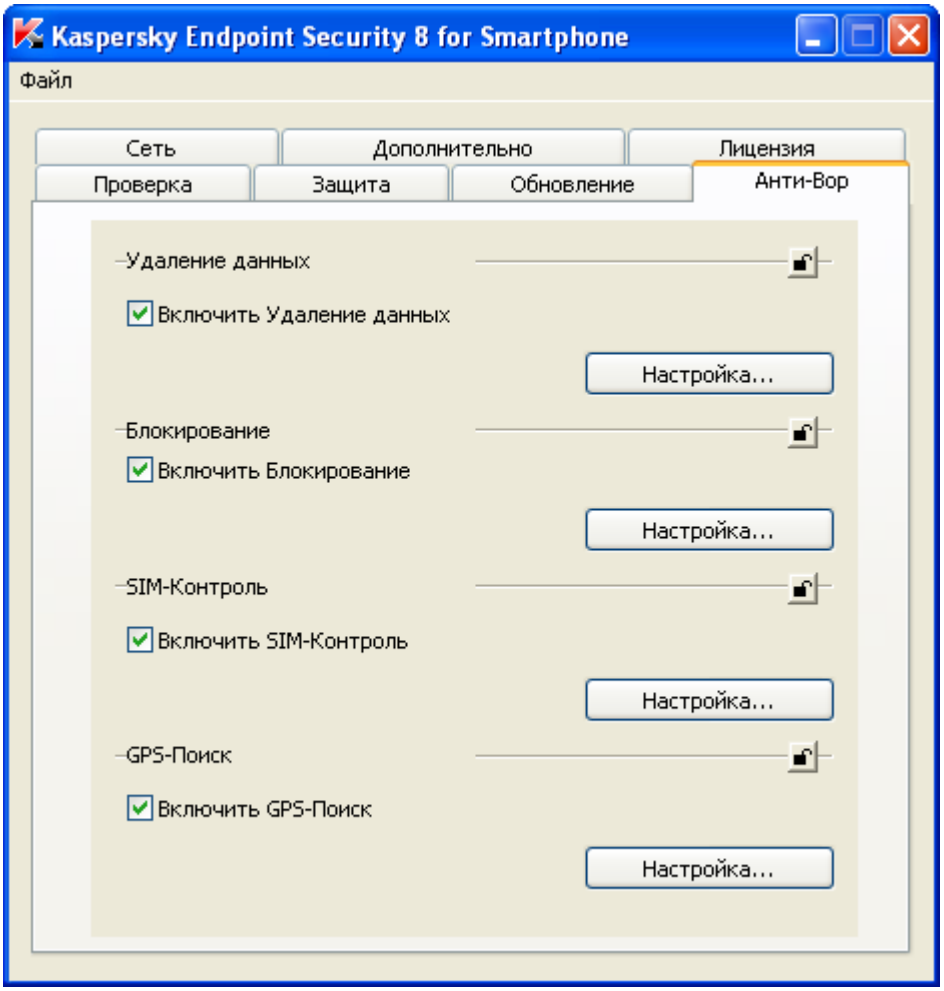


*Рисунок 78. Закладка **Анти-Вор***

2. Включите / отключите использование функции GPS-Поиск на устройстве. Для этого в блоке **GPS-Поиск** установите / снимите флажок **Включить GPS-Поиск**.

   По умолчанию программа отправляет координаты только в SMS на устройство, с которого отправлена SMS-команда. По умолчанию функция GPS-Поиск отключена.

   Чтобы по команде пользователя программа также отправляла координаты устройства на указанный адрес электронной почты, в блоке **GPS-Поиск** нажмите на кнопку **Настройка** и в открывшемся окне введите его в поле **Сообщение на адрес эл. почты**.

НАСТРОЙКА ПАРАМЕТРОВ КОМПОНЕНТА СЕТЕВОЙ ЭКРАН

Чтобы настроить параметры компонента Сетевой экран, выполните следующие действия:

1. Откройте закладку **Сеть** (см. рисунок ниже).

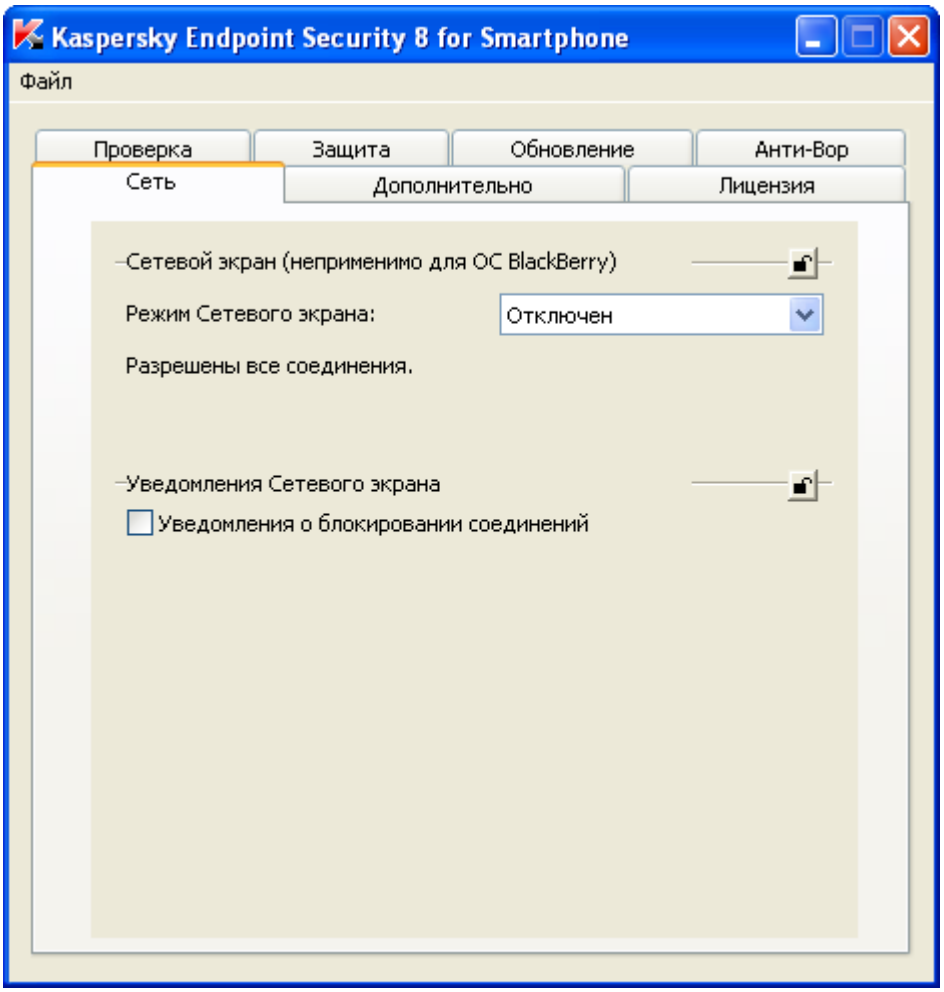


*Рисунок 79. Закладка **Сеть***

2. Выберите режим, в соответствии с которым Сетевой экран будет определять запрещенные и разрешенные соединения на устройстве. Для этого из раскрывающегося списка **Режим Сетевого экрана** выберите одно из следующих значений:

   - **Отключен** – разрешение любой сетевой активности. Сетевой экран отключен.
   - **Минимальная защита** – блокирование только входящих соединений. Исходящие соединения разрешены.
   - **Максимальная защита** – блокирование всех входящих соединений. Пользователю доступны проверка почты, просмотр веб-сайтов, скачивание файлов. Исходящие соединения могут осуществляться только по портам SSH, HTTP, HTTPS, IMAP, SMTP, POP3.
   - **Блокировать все** – блокирование любой сетевой активности, кроме обновления антивирусных баз и подключения к Серверу администрирования.

   По умолчанию Сетевой экран не используется, для параметра **Режим Сетевого экрана** установлено значение **Отключен**.

3. Включите / отключите уведомления пользователя о блокировании соединения. Для этого в блоке **Уведомления Сетевого экрана** установите / снимите флажок **Уведомления о блокировании соединений**.

   По умолчанию уведомления Сетевого экрана отключены.

Настройка параметров компонента Шифрование

Чтобы настроить параметры компонента Шифрование, выполните следующие действия:

1. Откройте закладку **Дополнительно** (см. рисунок ниже).

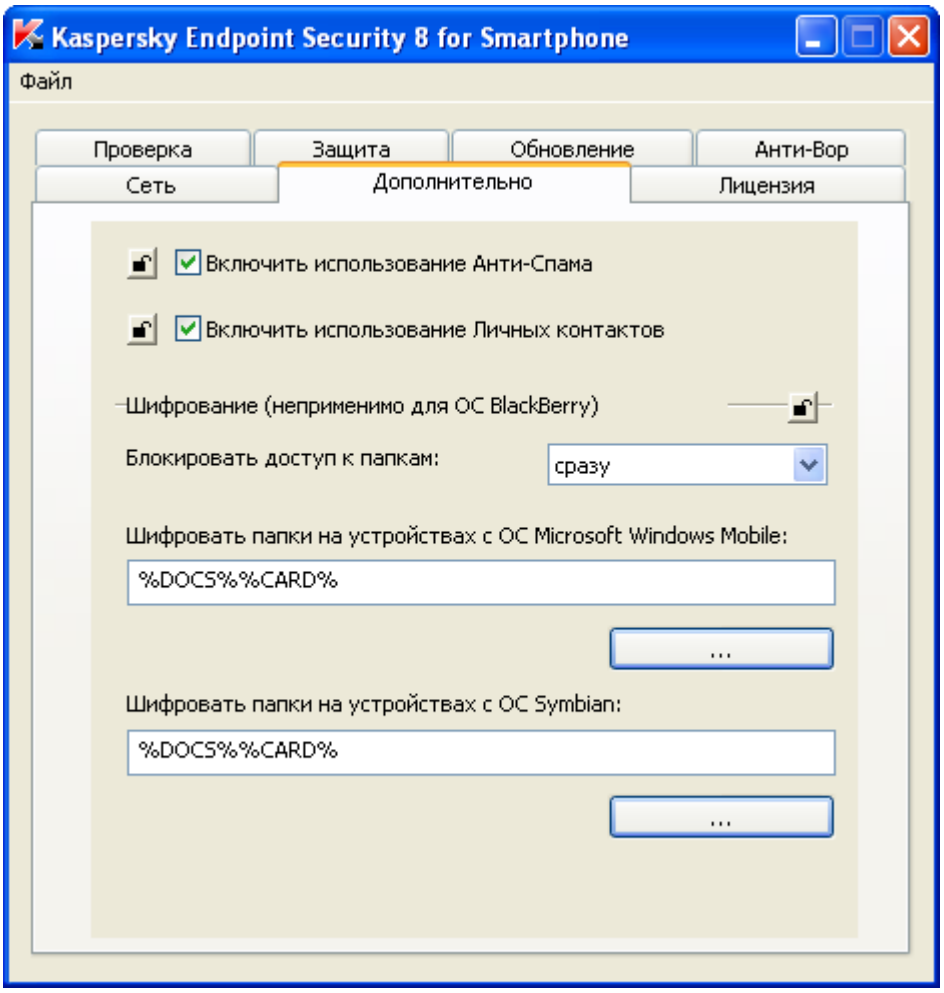


*Рисунок 80. Закладка **Дополнительно***

2. Укажите время, спустя которое после перехода устройства в режим энергосбережения доступ к используемым зашифрованным данным заблокируется. Для этого выберите значение из раскрывающегося списка **Блокировать доступ**.

   По умолчанию доступ к используемым зашифрованным папкам блокируется сразу после перехода устройства в режим энергосбережения. Для параметра **Блокировать доступ** выбрано значение **сразу**.

3. Сформируйте список зашифрованных на устройствах папок для выбранной операционной системы. Для доступа к ним пользователю потребуется ввести секретный код программы. Список состоит из папок, добавленных администратором, и из папок, добавленных вручную пользователем на устройстве. Папки, зашифрованные администратором, пользователь не может расшифровать и удалить из списка папок для шифрования.

Для формирования списка зашифрованных папок перечислите их в полях **Шифровать папки на устройствах с ОС <название_операционной_системы>** или нажмите на кнопку ... рядом с полем для требуемой операционной системы. В открывшемся окне **Выбор папок для шифрования** задайте папки, которые будут зашифрованы на устройстве.

При формировании списка папок вы можете использовать макросы папок. Чтобы использовать макрос для шифрования содержимого папки **Мои документы**, в окне **Выбор папок для шифрования** нажмите на кнопку **Мои документы**. Будет добавлен макрос **%DOCS%**. Чтобы использовать макрос для шифрования содержимого карты памяти, в окне **Выбор папки для шифрования** нажмите на кнопку **Карта памяти**. Будет добавлен макрос **%CARD%**.

Для операционной системы Microsoft Windows Mobile при использовании макроса **%DOCS%** программа зашифрует папку **Мои документы** (точное название зависит от локализации устройства), при использовании макроса **%CARD%** программа зашифрует папки на всех доступных картах памяти на устройстве.

Для операционной системы Symbian при использовании макроса **%DOCS%** программа зашифрует папку **C:\Data**, при использовании макроса **%CARD%** программа зашифрует папки на всех доступных картах памяти на устройстве.

По умолчанию список папок для шифрования пуст.

НАСТРОЙКА ПАРАМЕТРОВ КОМПОНЕНТА АНТИ-СПАМ

Чтобы настроить параметры компонента Анти-Спам, выполните следующие действия:

1. Откройте закладку **Дополнительно** (см. рисунок ниже).

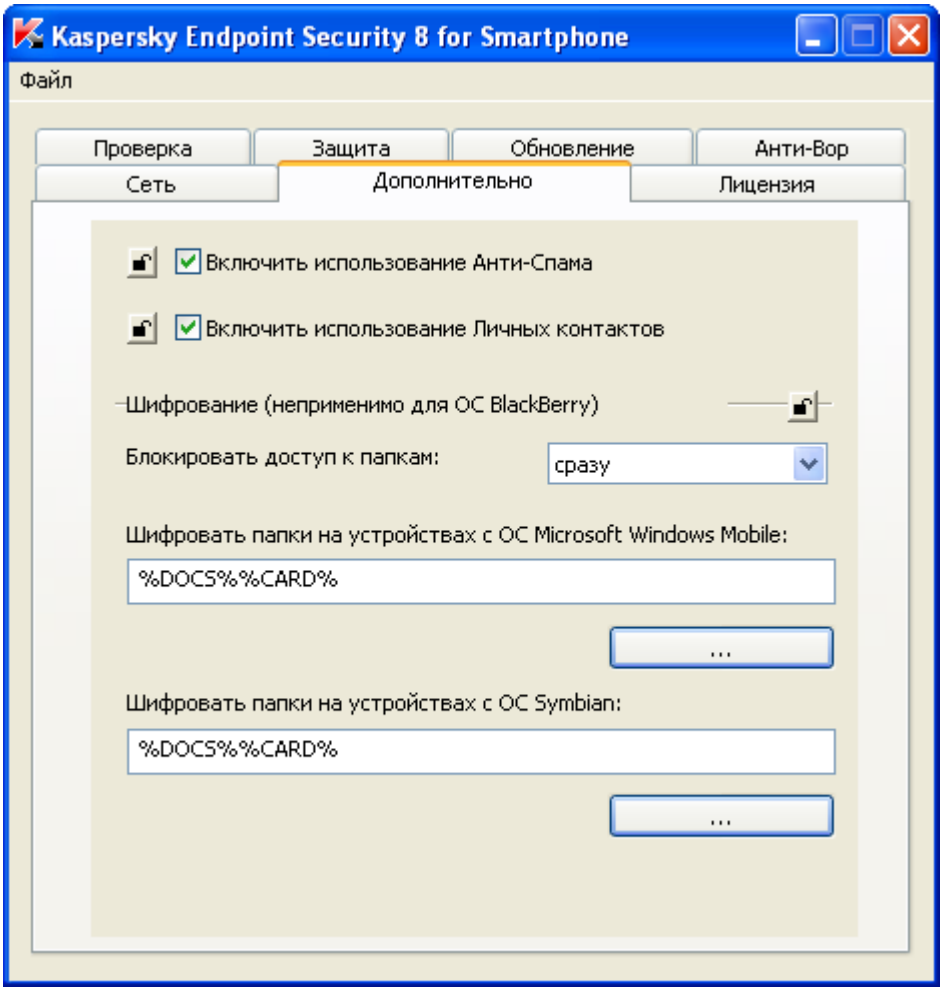


*Рисунок 81. Закладка **Дополнительно***

2. Разрешите / запретите использование Анти-Спама и изменение его параметров на устройстве. Для этого установите / снимите флажок **Включить использование Анти-Спама**.

   Если использование Анти-Спама разрешено, все параметры компонента настраиваются пользователем на устройстве. Если использование Анти-Спама запрещено, компонент на устройстве недоступен пользователю.

   По умолчанию использование Анти-Спама и изменение его параметров на устройстве разрешено.

НАСТРОЙКА ПАРАМЕТРОВ КОМПОНЕНТА ЛИЧНЫЕ КОНТАКТЫ

Чтобы настроить параметры компонента Личные контакты, выполните следующие действия:

1. Откройте закладку **Дополнительно** (см. рисунок ниже).

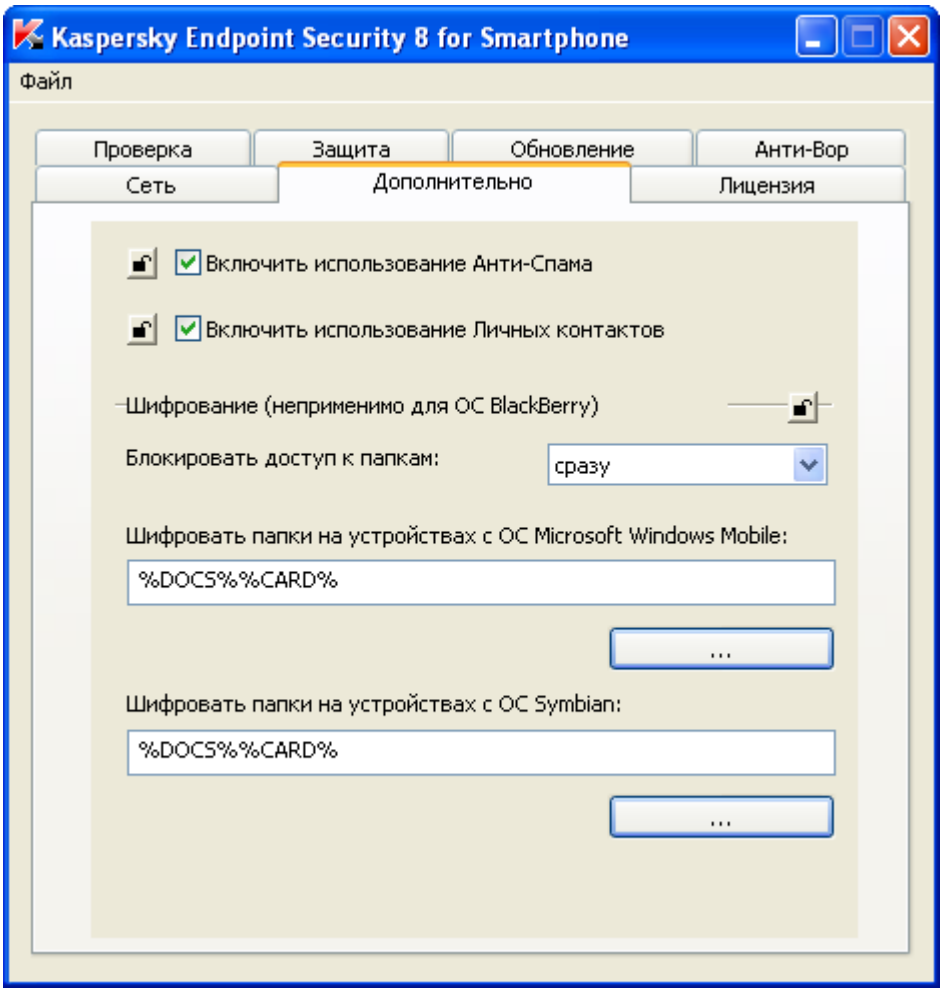


*Рисунок 82. Закладка **Дополнительно***

2. Разрешите / запретите использование Личных контактов и изменение параметров компонента на устройстве. Для этого установите / снимите флажок **Включить использование Личных контактов**.

   Если использование Личных контактов разрешено, все параметры компонента настраиваются пользователем на устройстве. Если использование Личных контактов запрещено, компонент на устройстве недоступен пользователю.

   По умолчанию использование Личных контактов и изменение их параметров на устройстве разрешено.

Настройка параметров лицензии

Чтобы включить лицензию в состав политики, выполните следующие действия:

1. Откройте закладку **Лицензия** (см. рисунок ниже).

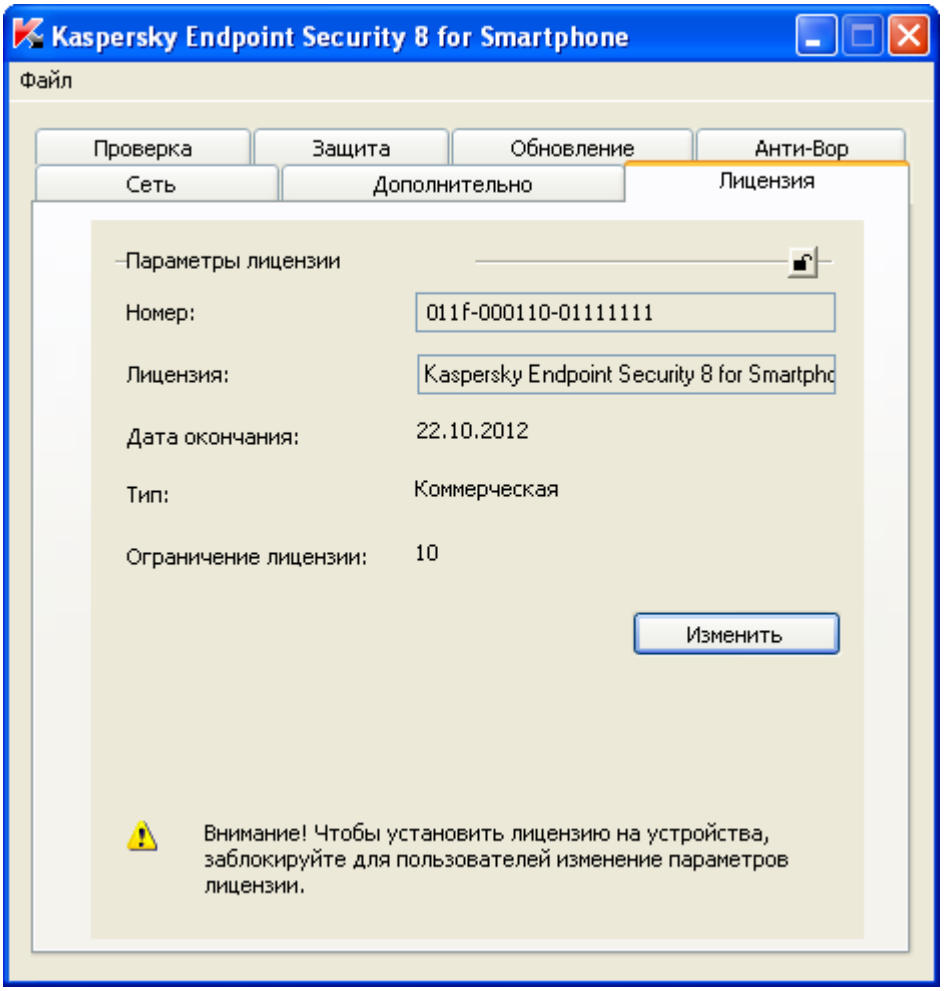


*Рисунок 83. Закладка **Лицензия***

2. Нажмите на кнопку **Изменить** и в открывшемся окне выберите файл ключа, полученный при покупке программы.

   После загрузки файла ключа информация о лицензии отобразится на закладке.

3. Сохраните файл политики.

Добавление лицензии через Sybase Afaria

Для того чтобы установить лицензию на мобильные устройства, администратор должен создать политику Kaspersky Endpoint Security 8 for Smartphone и включить в состав этой политики лицензию (см. раздел «Настройка параметров лицензии» на стр. 149). После этого администратор должен обеспечить доставку созданной политики на устройства выбранного профиля (см. раздел «Установка программы» на стр. 151). В результате при синхронизации мобильных устройств с Sybase Afaria политика программы с входящей в нее лицензией будет передана и применена на устройствах, после чего программа будет активирована.

Если лицензия не установлена на устройствах, то программа работает без лицензии в режиме полной функциональности в течение трех дней после установки программы на устройства.

Если в течение трех дней лицензия не была установлена, программа переходит в режим ограниченной функциональности.

Если вы не приобрели лицензию до установки программы, вы можете добавить ее в состав политики позже.

По умолчанию лицензия не включена в состав политики.

РЕДАКТИРОВАНИЕ ПОЛИТИКИ

- *Чтобы изменить параметры программы в существующей политике Kaspersky Endpoint Security 8 for Smartphone, выполните следующие действия:*

1. Запустите утилиту **KES2Afaria.exe**.

   Откроется окно **Kaspersky Endpoint Security 8 for Smartphone** с несколькими закладками.

2. Выберите в меню **Файл** → **Открыть** и укажите файл политики, в котором следует изменить параметры программы.

3. Внесите необходимые изменения и сохраните полученный файл политики, выбрав в меню **Файл** → **Сохранить**.

УСТАНОВКА ПРОГРАММЫ

Sybase Afaria позволяет дистанционно устанавливать Kaspersky Endpoint Security 8 for Smartphone на устройства.

Для установки программы на устройства администратор обеспечивает доставку на мобильные устройства каналов, содержащих файл политики и дистрибутив программы для каждого типа устройств.

Администратор должен обеспечить выполнение каналов на устройствах в строгой последовательности: сначала передавать на устройства файл политики, после этого дистрибутив программы. При выполнении каналов на устройствах в другой последовательности программа не будет работать.

Для установки программы на устройства с Microsoft Windows Mobile и Symbian OS администратору следует выполнить следующие действия:

1. Создать канал Software Manager Channel, содержащий файл политики программы (см. раздел «Создание канала, содержащего политику программы для устройств с Microsoft Windows Mobile и Symbian OS» на стр. 153).

2. Создать канал Software Manager Channel, содержащий дистрибутив программы (см. раздел «Создание канала, содержащего дистрибутив программы для устройств с Microsoft Windows Mobile и Symbian OS» на стр. 154).

3. Объединить каналы (channel set) (см. раздел «Объединение каналов для установки программы на устройства с Microsoft Windows Mobile и Symbian OS» на стр. 155).

4. Опубликовать каналы / объединение каналов (publish).

5. Доставить каналы на устройства с помощью монитора.

Для установки программы на устройства с BlackBerry OS администратору следует выполнить следующие действия:

1. Создать канал Session Manager Channel (см. раздел «Создание канала для устройств с BlackBerry OS» на стр. 155).
2. Создать список событий (worklist), по которому будет выполняться установка программы.
3. Опубликовать канал.
4. Доставить канал на устройства с помощью монитора.

В результате при следующей синхронизации мобильных устройств с сервером Sybase Afaria программа будет автоматически установлена, и будет применена настроенная политика.

В дальнейшем после установки программы вы можете изменять параметры программы с помощью политики. Для этого следует обновить файл политики на сервере. При следующей синхронизации файл политики будет обновлен на устройствах, и будут применены измененные параметры.

Таким образом, установка программы для Microsoft Windows Mobile и Symbian OS состоит из следующих шагов:

- Создание канала Software Manager Channel, содержащего дистрибутив программы (см. раздел «Создание канала, содержащего дистрибутив программы для устройств с Microsoft Windows Mobile и Symbian OS» на стр. 154).
- Создание канала Software Manager Channel, содержащего политику программы (см. раздел «Создание канала, содержащего политику программы для устройств с Microsoft Windows Mobile и Symbian OS» на стр. 153).
- Объединение каналов, содержащих политику и дистрибутив программы (channel set) (см. раздел «Объединение каналов для установки программы на устройства с Microsoft Windows Mobile и Symbian OS» на стр. 155).
- Публикация каналов (Publishing).
- Доставка каналов на устройства с помощью монитора (monitor).

Установка программы для BlackBerry OS состоит из следующих шагов:

- Создание канала Session Manager Channel, содержащего список событий, по которому будет выполняться установка программы (см. раздел «Создание канала для устройств с BlackBerry OS» на стр. 155).
- Публикация канала (Publishing).
- Доставка канала на устройства с помощью монитора (monitor).

В этом разделе

СОЗДАНИЕ КАНАЛА, СОДЕРЖАЩЕГО ПОЛИТИКУ ПРОГРАММЫ ДЛЯ УСТРОЙСТВ С MICROSOFT WINDOWS MOBILE И SYMBIAN OS

Для применения политики Kaspersky Endpoint Security 8 for Smartphone на устройствах используется канал Software Manager Channel.

В результате, когда канал будет доставлен на устройства, в заданную администратором папку будет передан и установлен файл политики policy.kes.

В дальнейшем после того, как файл политики будет обновлен на сервере, при следующей синхронизации он будет обновлен на устройстве, и автоматически будут применены изменения параметров.

Предварительно перед созданием канала убедитесь, что файл политики сохранен на сервере.

Чтобы создать канал, содержащий политику Kaspersky Endpoint Security 8 for Smartphone, выполните следующие действия:

1. Выберите в меню **Administration** пункт **Policies and Profiles**.
2. Выберите нужный профиль в панели **Policies and Profiles** в папке **Group Profiles**.
3. Для выбранного профиля на закладке **Allowed channels** воспользуйтесь ссылкой **Create → Software Manager Channel**.

   Откроется окно **Software Manager Channel Wizard**.
4. Введите имя и описание нового канала.
5. Выберите типы устройств из списка **Select one or more Client Types** и нажмите на кнопку **Next**.
6. Выберите папку на сервере и нажмите на кнопку **Next**.
7. Выберите файл политики policy.kes. Для этого воспользуйтесь ссылкой **Add**.
8. В открывшемся окне укажите путь к файлу политики на сервере.
9. В блоке **Destination directory for selected files** в раскрывающемся списке выберите **Let administrator specify destination**.
10. В поле **Administrator specified destination folder** укажите папку на устройстве, в которую будет скопирован выбранный файл политики.

    Для устройств с Microsoft Windows Mobile укажите папку **\Temp**.

    Для устройств с Symbian OS укажите папку **C:\Data**.
11. В блоке **Check file options** выберите вариант **Always check file**.
12. Убедитесь, что в блоке **Send file options** выбран вариант **Send file when server file is newer**, и нажмите на кнопку **OK**. После выбора файла политики в окне **Software Manager Channel Wizard** нажмите на кнопку **Next**.
13. Нажмите на кнопку **Finish**.

    Канал будет создан.

Создание канала, содержащего дистрибутив программы для устройств с Microsoft Windows Mobile и Symbian OS

Для установки программы на устройства с Microsoft Windows Mobile и Symbian OS используется канал Software Manager Channel. Канал применяется к выбранному профилю устройств.

Канал используется для копирования дистрибутива в указанную на устройстве папку и автоматического запуска установки программы.

Если в канале включена функция автоматического запуска установки, то в него не следует добавлять файл политики. Для применения политики следует использовать отдельный канал Software Manager Channel. Это действие позволяет избежать повторной установки программы при обновлении политики на устройствах. В противном случае после того, как файл политики будет обновлен на сервере, при синхронизации мобильных устройств с сервером Sybase Afaria на них обновится файл политики и повторно запустится установка программы.

Перед созданием канала предварительно сохраните на сервере установочные файлы для Microsoft Windows Mobile / Symbian OS. Установочные файлы входят в состав дистрибутива Kaspersky Endpoint Security 8 for Smartphone.

Чтобы создать канал для установки программы на устройства с Microsoft Windows Mobile / Symbian OS, выполните следующие действия:

1. Выберите в меню **Administration** пункт **Policies and Profiles**.
2. Выберите нужный профиль в панели **Policies and Profiles** в папке **Group Profiles**.
3. Для выбранного профиля на закладке **Allowed channels** нажмите **Create** → **Software Manager Channel**.

   Откроется окно **Software Manager Channel Wizard**.
4. Введите имя, описание нового канала.
5. Выберите типы устройств из списка **Select one or more Client Types** и нажмите на кнопку **Next**.
6. Выберите папку на сервере и нажмите на кнопку **Next**.
7. Выберите дистрибутив программы, который будет передан на устройства. Для этого нажмите на кнопку **Add** и в открывшемся окне укажите путь к установочному файлу программы.

   Для устройств с Microsoft Windows Mobile выберите CAB-архив, полученный при покупке программы.

   Для устройств с Symbian OS выберите SISX-архив, полученный при покупке программы.

   После выбора дистрибутива программы, который будет передан на устройства, нажмите на кнопку **Next**.
8. Укажите папку, в которую будет скопирован выбранный файл, и нажмите на кнопку **Next**.

   Для устройств с Microsoft Windows Mobile укажите папку **\Temp**.

   Для устройств с Symbian OS укажите папку **C:\Data**.
9. Установите флажок **Continue editing**, чтобы продолжить редактирование параметров канала, и нажмите на кнопку **Finish**.

   Откроется окно **Software Manager Channel Editor: <название_канала>**.

10. Установите автоматическую установку программы после того, как дистрибутив будет передан на устройство. Для этого на закладке **Install** в блоке **Installation program** установите флажок **Start installation automatically**.

Если вы включили автоматическую установку программы, то создайте для передачи файла политики отдельный канал. Это позволяет избежать повторной установки программы при обновлении файла политики на устройствах.

11. Выберите дистрибутив программы в раскрывающемся списке **File name** и по завершении нажмите на кнопку **OK**.

ОБЪЕДИНЕНИЕ КАНАЛОВ ДЛЯ УСТАНОВКИ ПРОГРАММЫ НА УСТРОЙСТВА С MICROSOFT WINDOWS MOBILE И SYMBIAN OS

Администратор должен обеспечить выполнение каналов на устройстве в строгой последовательности: сначала передавать файл политики программы, после этого передавать дистрибутив программы. Тогда при выполнении каналов на мобильных устройствах сначала будет передана политика программы, после этого запустится установка программы и сразу же будут применены настроенные параметры программы. При выполнении каналов на устройствах в другой последовательности программа не будет работать.

Для удобства управления каналами, содержащими политику программы и дистрибутив программы, рекомендуется объединить их.

Чтобы объединить каналы, выполните следующие действия:

1. Выберите в меню **Administration** пункт **Policies and Profiles**.
2. Выберите нужный профиль в панели **Policies and Profiles** в папке **Group Profiles**.
3. Для выбранного профиля на закладке **Allowed channels** нажмите **Create** → **Channel Set**.

   Откроется окно **Channel Set Wizard**.
4. Введите имя, описание объединения каналов.
5. Выберите папку на сервере и нажмите на кнопку **Next**.
6. Выберите из списка каналы, которые следует объединить, и нажмите на кнопку **Next**.
7. Укажите последовательность выполнения каналов, и нажмите на кнопку **Finish**.

СОЗДАНИЕ КАНАЛА ДЛЯ УСТРОЙСТВ С BLACKBERRY OS

Для установки Kaspersky Endpoint Security 8 for Smartphone на устройства с BlackBerry OS используется канал **Session Manager Channel**. В нем следует создать рабочий список (worklist), по которому будет выполняться установка программы на устройства.

Перед созданием канала предварительно сохраните на сервере файл Endpoint8_Mobile_Installer.cod для BlackBerry OS. Файл входит в состав дистрибутива Kaspersky Endpoint Security 8 for Smartphone.

Чтобы установить программу на устройства с BlackBerry OS, выполните следующие действия:

1. Выберите в меню **Administration** → **Policies and Profiles**.
2. Выберите нужный профиль в панели **Policies and Profiles** в папке **Group Profiles**.

3. Для выбранного профиля на закладке **Allowed channels** воспользуйтесь ссылкой **Create → Session Manager Channel**.

   Откроется окно **Software Manager Channel Wizard**.

4. Введите имя и описание канала в поля **Name**, **Description**.

5. Выберите из списка **Select one or more types BlackBerry Clients**. Нажмите на кнопку **Next**.

6. Выберите папку на сервере и нажмите на кнопку **Finish**.

   Канал будет создан. Откроется окно **Session Manager Channel Editor**.

7. Нажмите на кнопку **Create worklist**. В открывшемся окне введите название нового рабочего списка (worklist).

8. Создайте для нового рабочего списка (worklist) следующий список событий (eventlist):

```
Send <путь к файлу политики>\policy.kes TO policy.kes
Client Find File ksgui
If Previous Event FALSE
   Send <путь к дистрибутиву программы>\Endpoint8_Mobile_Installer.cod TO
   Endpoint8_Mobile_Installer.cod
End if
```

В результате выполнения этого скрипта сначала на устройства передается и применяется файл политик policy.kes. После этого выполняется проверка, установлена ли программа на устройстве. Если программа была установлена ранее, скрипт завершается. Если программа не установлена, на устройства передается файл Endpoint8_Mobile_Installer.cod, который скачивает с серверов «Лаборатории Касперского» установочные файлы программы и автоматически запускает установку программы. После этого выполнение скрипта завершается.

1. Сохраните список событий (eventlist), нажав на кнопку **Save**.

2. Опубликуйте канал (publish).

Чтобы создать список событий (eventlist), выполните следующие действия:

1. В окне **Session Manager Channel** в правой части окна из списка событий выберите **Send file to Client**.

2. В открывшемся окне **Event details: Send File to Client** укажите в поле **Source file** файл политики policy.kes, который будет отправлять на устройства. Для этого воспользуйтесь ссылкой **Browse** и укажите путь на сервере к файлу политики policy.kes.

   Поле **Target file** будет заполнено автоматически.

3. В блоке **File comparison and transfer options** в раскрывающемся списке **Transfer** выберите **Always**. Убедитесь, что установлен флажок **Use safe transfer**.

4. В блоке **Options** убедитесь, что установлены флажки **Make target path**, **Ignore hidden files**.

5. В блоке **Status** убедитесь, что выбрано значение **Enable**, и нажмите на кнопку **OK**.

6. В окне **Session Manager Channel** на панели в правой части окна выберите **Find File**.

7. В открывшемся окне **Event details: Find File** в поле **Starting path** введите **ksgui**. Будет проверяться наличие установленной программы Kaspersky Endpoint Security 8 for Smartphone на устройствах.

8. В блоке **Options** убедитесь, что установлены флажки **Ignore hidden options**, **Include subdirectories**.

9. В блоке **Execute** убедитесь, что выбрано значение **On Client**.

10. В блоке **Status** убедитесь, что выбрано значение **Enable**, и нажмите **OK**.

11. В окне **Session Manager Channel** на панели в правой части окна выберите **If**.

12. В открывшемся окне **Event details: If** выберите значение **Previous event FALSE** и нажмите на кнопку **OK**.

13. В окне **Session Manager Channel** на панели в правой части окна выберите **Send file to Client**.

14. Укажите в поле **Source file** файл Endpoint8_Mobile_Installer.cod. Для этого воспользуйтесь ссылкой **Browse** и укажите путь к файлу на сервере. Поле **Target file** будет заполнено автоматически.

15. В блоке **File comparison and transfer options** в раскрывающемся списке **Transfer** выберите **Always**. Убедитесь, что установлен флажок **Use safe transfer**.

16. В блоке **Options** убедитесь, что установлены флажки **Make target path**, **Ignore hidden files**.

17. В блоке **Status** убедитесь, что выбрано значение **Enable**, и нажмите на кнопку **OK**.

18. В окне **Session Manager Channel** на панели в правой части окна выберите **End if**.

19. Сохраните созданный список событий, нажав на кнопку **Save**.

УСТАНОВКА ПРОГРАММЫ НА МОБИЛЬНЫЕ УСТРОЙСТВА

Установка программы на мобильные устройства происходит дистанционно.

При синхронизации мобильных устройств с сервером Sybase Afaria доставляется канал / объединение каналов, содержащие файл политики и дистрибутив программы. После этого файл политики копируется в заданную администратором папку на устройстве и автоматически запускается установка программы.

Для Microsoft Windows Mobile и BlackBerry OS пользователю не нужно выполнять дополнительных действий при установке программы.

Для Symbian OS пользователю потребуется выполнить дополнительные действия во время установки программы. Подробнее об этом читайте в Руководстве пользователя для Symbian OS.

После установки автоматически применится политика, настроенная администратором. Если в состав политики администратор добавил лицензию (см. раздел «Добавление лицензии через Sybase Afaria» на стр. 150), после применения политики лицензия автоматически установится и программа активируется.

Если в состав политики администратор не включил лицензию, программа будет работать в режиме полной функциональности в течение трех дней. Если за это время администратор не добавил лицензию в состав политики, программа на устройствах переходит в режим ограниченной функциональности.

При первом запуске программы пользователь должен задать секретный код. Пользователь может изменять на устройстве только те параметры, на которые администратор не наложил запрет на изменение в политике.

Синхронизация мобильных устройств с Sybase Afaria выполняется с периодичностью, заданной администратором в мониторе. Для обновления параметров программы (см. раздел «Создание политики. Настройка параметров Kaspersky Endpoint Security 8 for Smartphone» на стр. 132) на устройстве администратор должен обновить файл политики на сервере. Тогда при очередной синхронизации файл политики будет обновлен на устройствах и автоматически будут применены измененные параметры программы.

Удаление программы

Удаление программы выполняется пользователем вручную на мобильном устройстве.

Для Microsoft Windows Mobile и Symbian OS перед удалением программы на устройстве автоматически будет отключено скрытие конфиденциальной информации и расшифрована вся ранее зашифрованная информация. Для BlackBerry OS перед удалением программы на устройстве пользователь должен вручную отключить скрытие конфиденциальной информации.

Подробно об удалении программы см. Руководство пользователя Kaspersky Endpoint Security 8 for Smartphone.

ОБРАЩЕНИЕ В СЛУЖБУ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

Если вы уже приобрели Kaspersky Endpoint Security, вы можете получить информацию об этой программе от специалистов Службы технической поддержки по телефону или через интернет.

Специалисты Службы технической поддержки ответят на ваши вопросы об установке и использовании программы. Если ваш компьютер был заражен, они помогут устранить последствия работы вредоносных программ.

Прежде чем обращаться в Службу технической поддержки, пожалуйста, ознакомьтесь с правилами поддержки (http://support.kaspersky.ru/support/rules).

Электронный запрос в Службу технической поддержки

Вы можете задать вопрос специалистам Службы технической поддержки, заполнив веб-форму системы обработки клиентских запросов Helpdesk (http://support.kaspersky.ru/helpdesk.html).

Запрос можно отправить на русском, английском, немецком, французском или испанском языках.

Чтобы отправить электронный запрос, укажите в нем **номер клиента**, полученный при регистрации на веб-сайте Службы технической поддержки, и **пароль**.

Если вы еще не являетесь зарегистрированным пользователем программ «Лаборатории Касперского», заполните регистрационную форму (https://support.kaspersky.com/ru/personalcabinet/registration/form/). При регистрации укажите *код активации* программы или *имя файла ключа*.

Вы получите ответ на свой запрос от специалиста Службы технической поддержки в своем Персональном кабинете (https://support.kaspersky.com/ru/PersonalCabinet) и по электронному адресу, который вы указали в запросе.

В веб-форме запроса как можно подробнее опишите возникшую проблему. В обязательных для заполнения полях укажите:

- **Тип запроса**. Выберите тему, наиболее точно соответствующую возникшей проблеме, например «Проблема установки / удаления продукта» или «Проблема поиска / удаления вирусов». Если вы не найдете подходящей темы, выберите «Общий вопрос».
- **Название и номер версии программы**.
- **Текст запроса**. Как можно подробнее опишите возникшую проблему.
- **Номер клиента и пароль**. Введите номер клиента и пароль, которые вы получили при регистрации на веб-сайте Службы технической поддержки.
- **Электронный адрес**. По этому адресу специалисты Службы технической поддержки перешлют ответ на ваш запрос.

Техническая поддержка по телефону

Если возникла неотложная проблема, вы всегда можете позвонить в Службу технической поддержки в вашем городе. Перед обращением к специалистам технической поддержки, пожалуйста, соберите информацию (http://support.kaspersky.ru/support/details) о своем компьютере. Это поможет нашим специалистам быстрее помочь вам.

ГЛОССАРИЙ

А

Активация программы

Перевод программы в полнофункциональный режим. Для активации программы необходима установленная лицензия.

Антивирусные базы

Базы данных, формируемые специалистами «Лаборатории Касперского» и содержащие подробное описание всех существующих на текущий момент угроз компьютерной безопасности, способов их обнаружения и обезвреживания. Базы постоянно обновляются в «Лаборатории Касперского» по мере появления новых угроз.

Архив

Файл, «содержащий» в себе один или несколько других объектов, которые в свою очередь также могут быть архивами.

Б

«Белый» список

Записи этого списка содержат следующую информацию:

- *Номер телефона*, с которого Анти-Спам доставляет вызовы и (или) SMS.
- *Тип событий*, которые Анти-Спам доставляет с этого номера. Представлены следующие типы событий: вызовы и SMS, только вызовы, только SMS.
- *Ключевая фраза*, по которой Анти-Спам определяет, что SMS является желательным (не спамом). Анти-Спам доставляет только те SMS, которые содержат эту ключевую фразу, остальные SMS Анти-Спам блокирует.

Блокирование объекта

Запрет доступа к объекту со стороны внешних программ. Заблокированный объект не может быть прочитан, выполнен, изменен или удален.

Г

Групповая политика

см. Политика

З

Зараженный объект

Объект, внутри которого содержится вредоносный код: при проверке объекта было обнаружено полное совпадение участка кода объекта с кодом известной угрозы. Специалисты «Лаборатории Касперского» не рекомендуют вам работать с такими объектами, поскольку это может привести к заражению вашего устройства.

Защита

Режим работы программы, в котором осуществляется проверка объектов на присутствие вредоносного кода в режиме реального времени.

Программа перехватывает все попытки открыть какой-либо объект на чтение, запись и исполнение и проверяет объект на наличие угроз. Незараженные объекты пропускаются пользователю, объекты, содержащие угрозы или подозреваемые на наличие угрозы, обрабатываются в соответствии с параметрами задачи (лечатся, удаляются, помещаются на карантин).

И

Инсталляционный пакет

Набор файлов, формируемый для удаленной установки программы «Лаборатории Касперского» при помощи системы удаленного администрирования. Инсталляционный пакет создается на основании специальных файлов, входящих в состав дистрибутива программы, и содержит набор параметров, необходимых для установки программы и обеспечения ее работоспособности сразу после установки. Значения параметров соответствуют значениям параметров программы по умолчанию.

К

Карантин

Определенная папка, куда помещаются все возможно зараженные объекты, обнаруженные во время проверки или в процессе функционирования постоянной защиты.

Л

Лечение объектов

Способ обработки зараженных объектов, в результате которого происходит полное или частичное восстановление данных либо принимается решение о невозможности лечения объектов. Лечение объектов выполняется на основе записей баз. В процессе лечения часть данных может быть потеряна.

О

Обновление баз

Одна из функций, выполняемых программой «Лаборатории Касперского», которая позволяет поддерживать защиту в актуальном состоянии. При этом происходит копирование антивирусных баз с серверов обновлений «Лаборатории Касперского» на устройство и автоматическое подключение их к программе.

П

Плагин управления программой

Специализированный компонент, предоставляющий интерфейс для управления работой программы через Консоль администрирования. Для каждой программы существует свой плагин управления. Он входит в состав всех программ «Лаборатории Касперского», управление которыми может осуществляться при помощи Kaspersky Endpoint Security.

Политика

Набор параметров работы программы для целевой группы устройств. Для разных групп параметры работы программы могут быть различны. Политика включает в себя параметры полной настройки всей функциональности программы.

Проверка по требованию

Режим работы программы «Лаборатории Касперского», который инициируется пользователем и направлен на проверку любых файлов.

Р

Рабочее место администратора

Компьютер, на котором установлен компонент, предоставляющий интерфейс управления программой.

С рабочего места администратора выполняются настройка и управление программой, а для Kaspersky Administration Kit – построение системы централизованной антивирусной защиты сети предприятия, сформированной на базе программ «Лаборатории Касперского», и управление ею.

С

Секретный код программы

Секретный код программы используется, чтобы предотвратить несанкционированный доступ к параметрам программы и к защищаемой на устройстве информации. Он задается пользователем при первом запуске

программы и состоит не менее чем из четырех цифр. Секретный код программы запрашивается в следующих случаях:

- для доступа к параметрам программы;
- для доступа к зашифрованным папкам;
- при отправке с другого мобильного устройства SMS-команды, чтобы дистанционно запустить следующие функции: Блокирование, Удаление данных, SIM-Контроль, GPS-Поиск, Личные контакты;
- при удалении программы.

Серверы обновлений «Лаборатории Касперского»

Список HTTP- и FTP-серверов «Лаборатории Касперского», с которых программа копирует обновление баз на мобильные устройства.

Синхронизация

Процесс, при котором устанавливается соединение между мобильным устройством и системой удаленного администрирования и выполняется передача данных между ними. В ходе синхронизации на устройство передаются параметры программы, установленные администратором. С устройства в систему удаленного администрирования передаются отчеты о работе компонентов программы.

Система удаленного администрирования

Система, которая позволяет дистанционно управлять устройствами и администрировать их в режиме реального времени.

Срок действия лицензии

Период, в течение которого вам предоставляется возможность использовать полную функциональность программы «Лаборатории Касперского». По окончании срока действия лицензии программа переходит в режим ограниченной функциональности. В этом режиме в программе доступны следующие действия:

- отключение всех компонентов;
- расшифровывание одной или нескольких папок;
- отключение скрытия конфиденциальной информации;
- отключение автоматического скрытия конфиденциальной информации;
- просмотр справочной системы программы.

У

Удаление SMS

Способ обработки SMS, содержащего признаки спама, при котором происходит его физическое удаление. Такой способ рекомендуется применять к SMS, однозначно содержащим спам.

Удаление объекта

Способ обработки объекта, при котором происходит его физическое удаление с того места, где он был обнаружен программой (жесткий диск, папка, сетевой ресурс). Такой способ обработки рекомендуется применять к опасным объектам, лечение которых по тем или иным причинам невозможно.

Ч

«Черный» список

Записи из этого списка содержат следующую информацию:

- *Номер телефона*, с которого Анти-Спам блокирует вызовы и (или) SMS.

- *Тип событий*, которые Анти-Спам блокирует с этого номера. Представлены следующие типы событий: вызовы и SMS, только вызовы, только SMS.

- *Ключевая фраза*, по которой Анти-Спам определяет, что SMS является нежелательным (спамом). Анти-Спам блокирует только те SMS, которые содержат эту ключевую фразу, остальные SMS Анти-Спам доставляет.

ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

«Лаборатория Касперского» была основана в 1997 году. 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 тысячи 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. Основной продукт 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 мировые разработчики используют в своих продуктах программное ядро Антивируса Касперского, например, такие как: Nokia ICG (США), 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 технической поддержкой на нескольких языках.

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.

Веб-сайт «Лаборатории Касперского»:	http://www.kaspersky.ru
Вирусная энциклопедия:	http://www.securelist.com/ru/
Антивирусная лаборатория:	newvirus@kaspersky.com (только для отправки подозрительных объектов в архивированном виде) http://support.kaspersky.ru/virlab/helpdesk.html (для запросов вирусным аналитикам)

ИНФОРМАЦИЯ О СТОРОННЕМ КОДЕ

Для создания программы использовался код сторонних производителей.

В ЭТОМ РАЗДЕЛЕ

РАСПРОСТРАНЯЕМЫЙ ПРОГРАММНЫЙ КОД

В составе программы распространяется независимый программный код сторонних производителей в исходном или бинарном виде без внесения изменений.

В ЭТОМ РАЗДЕЛЕ

ADB

Copyright (C) 2005-2008, The Android Open Source Project

Distributed under the terms of the Apache License, version 2.0 of the License

ADBWINAPI.DLL

Copyright (C) 2005-2008, The Android Open Source Project

Distributed under the terms of the Apache License, version 2.0 of the License

ADBWINUSBAPI.DLL

Copyright (C) 2005-2008, The Android Open Source Project

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

«License» shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

«Licensor» shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

«Legal Entity» shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, «control» means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

«You» (or «Your») shall mean an individual or Legal Entity exercising permissions granted by this License.

«Source» form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

«Object» form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

«Work» shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

«Derivative Works» shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

«Contribution» shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, «submitted» means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as «Not a Contribution.»

«Contributor» shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a «NOTICE» text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an «AS IS» BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

Другая информация

Для проверки электронной цифровой подписи в Kaspersky Endpoint Security 8 for Smartphone используется программная библиотека защиты информации (ПБЗИ) «Крипто-Си», разработанная ООО «КриптоЭкс».

Веб-сайт ООО «КриптоЭкс»: http://www.cryptoex.ru

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

Ф

Ш