

**Руководство по миграции
с Kaspersky Security для
виртуальных сред 6.1
Защита без агента
на Kaspersky Security для
виртуальных сред 6.4
Легкий агент**

Уважаемый пользователь!

Спасибо, что доверяете нам. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.

Внимание! Права на этот документ являются собственностью АО «Лаборатория Касперского» (далее также «Лаборатория Касперского») и защищены законодательством Российской Федерации об авторском праве и международными договорами. За незаконное копирование и распространение документа и его отдельных частей нарушитель несет гражданскую, административную или уголовную ответственность в соответствии с применимым законодательством.

Копирование в любой форме, распространение, в том числе в переводе, любых материалов возможны только с письменного разрешения «Лаборатории Касперского».

Документ и связанные с ним графические изображения могут быть использованы только в информационных, некоммерческих или личных целях.

Документ может быть изменен без предварительного уведомления.

За содержание, качество, актуальность и достоверность используемых в документе материалов, права на которые принадлежат другим правообладателям, а также за возможный ущерб, связанный с использованием этих материалов, «Лаборатория Касперского» ответственности не несет.

В этом документе используются зарегистрированные товарные знаки и знаки обслуживания, которые являются собственностью соответствующих правообладателей.

© 2026 АО «Лаборатория Касперского»

<https://www.kaspersky.ru>
<https://help.kaspersky.com/ru>
<https://support.kaspersky.ru>

О «Лаборатории Касперского» <https://www.kaspersky.ru/about/company>

Содержание

О решениях Kaspersky Security для виртуальных сред	4
Архитектура решений	4
Функции решений.....	5
Комплект поставки решения Kaspersky Security для виртуальных сред 6.4 Легкий агент	7
Подготовка к миграции	8
Программные и аппаратные требования	8
О лицензировании	8
Ознакомление с особенностями установки Агентского решения	9
Процедура миграции	10
Источники информации	13

О решениях Kaspersky Security для виртуальных сред

Это руководство содержит инструкцию по миграции с Kaspersky Security для виртуальных сред 6.1 Защита без агента на Kaspersky Security для виртуальных сред 6.4 Легкий агент.

Kaspersky Security для виртуальных сред 6.1 Защита без агента (далее также «Безагентское решение») представляет собой интегрированное решение, обеспечивающее защиту виртуальных машин на платформе VMware vSphere от вирусов и других вредоносных программ, а также от сетевых угроз. Подробную информацию о решении Kaspersky Security для виртуальных сред 6.1 Защита без агента см. в [справке решения](#).

Kaspersky Security для виртуальных сред 6.4 Легкий агент (далее также «Агентское решение») представляет собой интегрированное решение, обеспечивающее комплексную защиту виртуальных машин с гостевыми операционными системами Linux и с гостевыми операционными системами Windows от различных видов информационных угроз, сетевых и мошеннических атак. Подробную информацию о решении Kaspersky Security для виртуальных сред 6.4 Легкий агент см. в [справке решения](#).

Архитектура решений

Перед миграцией с Безагентского решения на Агентское решение рекомендуется ознакомиться с архитектурой решения Kaspersky Security для виртуальных сред 6.4 Легкий агент (см. подробнее «[Архитектура решения](#)»).

Основные отличия в архитектуре решений:

Безагентское решение	Агентское решение
В составе решения две SVM (secure virtual machine, виртуальная машина защиты): • SVM с компонентом Защита от файловых угроз; • SVM с компонентом Защита от сетевых угроз.	В составе решения одна SVM: SVM с компонентом Сервер защиты.
Требуется только развертывание SVM на гипервизорах в виртуальной инфраструктуре.	Требуется как развертывание SVM на гипервизорах в виртуальной инфраструктуре, так и установка специального приложения (далее также «Легкий агент») на каждой виртуальной машине, которую требуется защищать.
Защитой виртуальных машин занимаются только SVM.	Функции защиты и контроля виртуальных машин обеспечиваются функциональными компонентами и задачами Легкого агента.

Архитектура Агентского решения по сравнению с Безагентским решением обеспечивает больший объем дополнительного функционала защиты виртуальных машин. Этот функционал использует передовые методы обнаружения угроз и защиты виртуальных машин. Также появляется возможность защиты популярных виртуальных сред, отличных от VMware vSphere.

Легкие агенты в составе Агентского решения оптимизированы для работы в виртуальной среде. SVM обеспечивают комплексную защиту виртуальной инфраструктуры и экономию ресурсов виртуальной среды, используя функции защиты и управления, такие как:

- активация решения;
- управление обновлением баз и программных модулей решения;
- функции защиты и контроля.

Для оптимизации работы Агентского решения применяются такие механизмы:

- SharedCache. При каждом обращении к файлу на виртуальной машине Легкий агент проверяет в общем кеше на SVM, был ли ранее проверен этот файл. Если в кеше есть результат проверки файла, он передается на виртуальную машину, с которой пришел запрос, без дополнительных циклов проверки. Файл проверяется повторно только в случае его изменения.

- Распределение выполнения задач обновления баз и программных модулей. Сервер защиты управляет запуском задач обновления баз и программных модулей, а также осуществляет откат обновления баз и программных модулей с целью оптимизации потребления ресурсов гипервизора, которые необходимы для обновления.
- Очередь проверки. В случае большого количества запросов на проверку Сервер защиты может приостанавливать задачи проверки, а также возобновлять выполнение задач и управлять задачами проверки группы виртуальных машин с целью оптимизации потребления ресурсов гипервизора.

Функции решений

В качестве компонента Легкий агент в Агентском решении используются следующие приложения:

- Kaspersky Endpoint Security для Windows 12.12 обеспечивает защиту и контроль виртуальных машин с операционными системами Windows (далее также «Легкий агент для Windows»).
- Kaspersky Endpoint Security для Linux 12.4 обеспечивает защиту и контроль виртуальных машин с операционными системами Linux (далее также «Легкий агент для Linux»).

Решение может поддерживать новые версии приложений Kaspersky Endpoint Security и не требовать обновления версии решения в целом. Актуальный список поддерживаемых версий приложений в режиме Легкого агента см. в [справке Kaspersky Security для виртуальных сред 6.4 Легкий агент](#).

Приложения Kaspersky Endpoint Security обеспечивают комплексную защиту и контроль виртуальных машин, предоставляя не только защиту от файловых и сетевых угроз, но также следующую функциональность:

- Защита от атак BadUSB.
- Защита от удаленного вредоносного шифрования.
- Защита от почтовых угроз.
- Сетевой экран.
- Защита от эксплойтов.
- Анализ поведения.
- Веб-Контроль.
- Контроль устройств.
- Контроль приложений.
- Контроль целостности системы.
- Расширенные возможности использования Kaspersky Security Network.
- Возможности использования передовых решений Kaspersky Detection and Response.

Для виртуальных машин с операционными системами Windows также доступна функциональность AMSI-защиты.

Подробнее о функциональности приложения Kaspersky Endpoint Security для Windows см. в [справке Kaspersky Endpoint Security для Windows 12.12](#).

Подробнее о функциональности приложения Kaspersky Endpoint Security для Linux 12.4 см. в [справке Kaspersky Endpoint Security для Linux 12.4](#).

Обратите внимание на возможные ограничения функциональности приложений в режиме Легкого агента. См. подробнее в справках Kaspersky Endpoint Security для Windows (раздел «[Особенности работы приложения в режиме Легкого агента](#)») и Kaspersky Endpoint Security для Linux (раздел «[Использование приложения в режиме Легкого агента](#)»).

Агентское решение имеет следующие функциональные особенности:

- Защиту виртуальных машин от файловых угроз осуществляют соответствующие функциональные компоненты Легкого агента для Windows и Легкого агента для Linux.
- Проверку виртуальных машин обеспечивают задачи проверки Легкого агента для Windows и Легкого агента для Linux.
- Защиту виртуальных машин от сетевых угроз осуществляют соответствующие функциональные компоненты Легкого агента для Windows и Легкого агента для Linux.
- В Агентском решении доступен функционал тегов безопасности VMware для контроля состояния защиты виртуальной машины (см. подробнее «[О тегах безопасности \(Security Tags\)](#)»). При этом использование VMware NSX Manager не обязательно для функционирования Агентского решения.
- Функционал проверки выключенной виртуальной машины отсутствует в Агентском решении, так как проверка инициируется на виртуальной машине Легким агентом.
- В Агентском решении, как и в Безагентском, доступен режим мультитенантности (см. подробнее «[Использование Kaspersky Security для виртуальных сред 6.3 Легкий агент в режиме мультитенантности](#)»). При этом не требуется дополнительных плагинов управления Kaspersky Security для клиентов, не выдвигаются дополнительные программные и аппаратные требования к виртуальной инфраструктуре, а также не требуется наличие связи между структурой виртуальной среды и структурой тенантов.
- В Агентском решении, как и в Безагентском, поддерживается SNMP-мониторинг состояния SVM, но может потребоваться перенастройка в соответствии со справкой Агентского решения (см. подробнее «[SNMP-мониторинг состояния SVM](#)»).

Комплект поставки решения Kaspersky Security для виртуальных сред 6.4 Легкий агент

В комплект поставки Агентского решения входят следующие файлы:

- Мастер установки компонентов Kaspersky Security и Сервер интеграции на базе Windows.
- Сервер интеграции на базе Linux.
- Образы SVM (архивы для установки Сервера защиты в виртуальных инфраструктурах разных типов). Развернутая в инфраструктуре SVM выполняет полный набор функций защиты, не требуется разворачивать отдельную SVM для защиты от файловых угроз и отдельную SVM для защиты от сетевых угроз.
- Легкий агент для Linux.
- Легкий агент для Windows.
- Kaspersky Security Center и Агент администрирования Kaspersky Security Center.
- MMC-плагины управления.
- Веб-плагины управления.
- Файлы с текстами Лицензионного соглашения и Политики конфиденциальности.
- MIB-файл, который вы можете использовать для получения сведений о состоянии SVM с помощью системы SNMP-мониторинга.

См. подробнее в справке решения (раздел «[Комплект поставки](#)»).

Подготовка к миграции

Перед миграцией с Безагентского решения на Агентское решение рекомендуется:

- Проверить вашу инфраструктуру на соответствие программным и аппаратным требованиям Агентского решения и выполнить необходимые обновления.
- Ознакомиться с особенностями лицензирования и особенностями установки Агентского решения.
- Ознакомиться с разделами «Что нового» и «Основные известные ограничения и ошибки» используемых компонентов Агентского решения.

Программные и аппаратные требования

Убедитесь, что инфраструктура соответствует программным и аппаратным требованиям Агентского решения («[Аппаратные и программные требования](#)»):

В зависимости от вашей инфраструктуры вам может потребоваться:

- обновить виртуальные машины, где будут установлены Легкие агенты для Windows и Легкие агенты для Linux;
- обновить решение Kaspersky Security Center;
- обновить Microsoft .NET Framework на устройстве, где будет установлен Сервер интеграции на базе Windows и Консоль Сервера интеграции;
- обновить виртуальную машину, где будет установлен Сервер интеграции;
- изменить выделенные ресурсы для виртуальной машины с установленным Сервером интеграции;
- изменить выделенные ресурсы для группы SVM;
- обновить гипервизор VMware ESXi;
- обновить VMware NSX Manager (в случае использования функционала тэгов безопасности NSX для контроля состояния защиты виртуальной машины).

Для защиты виртуальных машин с помощью Агентского решения не нужен установленный компонент Guest Introspection Thin Agent. Перед установкой Легких агентов в составе Агентского решения вам нужно:

- 1) На виртуальных машинах с операционными системами Windows удалить NSX File Introspection Driver, который выполняет роль компонента Guest Introspection Thin Agent.
- 2) На виртуальных машинах с операционными системами Linux удалить специальные пакеты, которые предусмотрены для установки компонента Guest Introspection Thin Agent.
- 3) Перезагрузить виртуальные машины.
- 4) Для работоспособности Легких агентов в составе Агентского решения установить на виртуальные машины пакеты guests tools, см. подробнее в справке Агентского решения («Требования к виртуальной машине для установки Легкого агента»).

О лицензировании

Перед миграцией убедитесь, что приобретенная лицензия удовлетворяет требованиям к лицензированию Агентского решения (см. подробнее «[О лицензиях](#)»).

В Агентском решении, в отличие от Безагентского решения, отсутствует ограничение на использование только ключей для серверов или только ключей с ограничением по ядрам или процессорам для защиты виртуальных машин с гостевыми операционными системами Linux. Во время установки Легкого агента для Linux на виртуальную машину, которую вы хотите защищать, вы выбираете роль виртуальной машины в виртуальной инфраструктуре: сервер или рабочая станция (см. подробнее «[Использование приложения в режиме Легкого агента](#)»).

Ознакомление с особенностями установки Агентского решения

Перед миграцией рекомендуется ознакомиться с процедурой «чистой» (без миграции) установки Kaspersky Security для виртуальных сред 6.4 Легкий агент (см. подробнее [«Подготовка к установке решения»](#) и [«Установка решения Kaspersky Security»](#)). Процедура установки Агентского решения отличается от процедуры установки Безагентского решения ([«Приложение. Краткая инструкция по установке программы»](#)).

Некоторые различия:

- Установка Агентского решения не зависит от структуры виртуальной среды.
- Использование VMware NSX Manager не требуется для Агентского решения.
- Использование VMware Cloud Director не требуется для работы Агентского решения.
- Концепция управления политиками Kaspersky Security Center в случае Агентского решения не содержит дополнительных ограничений и особенностей.

Процедура миграции

Миграция с Безагентского решения на Агентское решение выполняется в ручном режиме. Это связано с существенными отличиями в архитектуре решений.

Миграция с Безагентского решения на Агентское решение состоит из следующих этапов:

1. Подготовка инфраструктуры

а. Подготовительные действия.

Выполните действия, описанные в этом руководстве в разделе «Подготовка к миграции».

б. Настройка использования безопасных криптографических алгоритмов, шифров и протоколов.

Убедитесь в том, что на устройствах, где будут установлены компоненты решения и объекты виртуальной инфраструктуры, к которым подключается Сервер интеграции Агентского решения, используются только безопасные криптографические алгоритмы, наборы шифров и протоколы (см. подробнее «[Настройка использования безопасных криптографических алгоритмов, шифров и протоколов](#)»).

в. Настройка используемых портов.

Убедитесь в том, что в настройках сетевого оборудования или программного обеспечения, обеспечивающего контроль трафика между виртуальными машинами, разрешено прохождение сетевого трафика через порты, используемые при установке и работе Агентского решения (см. подробнее «[Настройка используемых портов](#)»).

г. Настройка учетных записей.

Убедитесь в том, что настроены параметры учетных записей, которые требуются для установки и работы Агентского решения (см. подробнее «[Учетные записи для установки и работы решения](#)»).

2. Установка Сервера интеграции

а. Установка Сервера интеграции и консоли управления.

Установите ту версию Сервера интеграции, которую вы планируете использовать:

- Сервер интеграции на базе Linux. Для управления Сервером интеграции на базе Linux вы можете использовать Веб-консоль Сервера интеграции. Также вы можете использовать REST API Сервера интеграции. Сервер интеграции на базе Linux поддерживает отправку событий аудита в Kaspersky Security Center.
- Сервер интеграции на базе Windows. Для управления Сервером интеграции на базе Windows вы можете использовать Консоль Сервера интеграции или Веб-консоль Сервера интеграции. Также вы можете использовать REST API Сервера интеграции.

Если вы устанавливаете новый Сервер интеграции на устройство, где установлен Сервер интеграции Безагентского решения, при установке Сервера интеграции Агентского решения необходимо изменить порт по умолчанию (см. подробнее «[Установка Сервера интеграции на базе Windows](#)»).

б. Подключение Сервера интеграции к виртуальной инфраструктуре.

Настройте параметры подключения Сервера интеграции Агентского решения к виртуальной инфраструктуре. Если требуется, на этом этапе также настройте подключение к VMware NSX Manager, чтобы обеспечить работоспособность тегов безопасности (см. подробнее «[О теге безопасности \(Security Tags\)](#)»).

3. Установка и настройка Серверов защиты

а. Установка элементов управления Сервером защиты Агентского решения в Kaspersky Security Center.

Установите MMC- и/или веб-плагин Сервера защиты.

b. Скачивание образа SVM.

Скачайте образ SVM, соответствующий вашей виртуальной инфраструктуре, и файл описания образов SVM (см. подробнее [«Файлы, необходимые для установки решения»](#)).

c. Подготовка дистрибутива Агента администрирования.

Подготовьте дистрибутив Агента администрирования для установки на SVM Агентского решения (см. подробнее [«Подготовка дистрибутива Агента администрирования для SVM»](#)).

d. Развертывание SVM.

Разверните необходимое количество SVM Агентского решения (см. подробнее [«Установка решения Kaspersky Security»](#)), также см. [«Концепция управления решением»](#)).

e. Создание политики.

Используя элементы управления Сервером защиты Агентского решения, создайте в Kaspersky Security Center политику для Сервера защиты (см. подробнее [«Создание политики для Сервера защиты»](#)). В политике настройте параметры подключения SVM к Серверу интеграции.

f. Активация.

Создайте и выполните задачу «Активация решения» (см. подробнее [«Об активации решения Kaspersky Security для виртуальных сред 6.4 Легкий агент»](#)).

g. Обновление баз.

- a. Выполните задачу «Загрузка обновлений в хранилище Сервера администрирования». Если задача загрузки обновлений в хранилище отсутствует в списке задач для Сервера администрирования, вам нужно создать ее.
 - b. Убедитесь, что в политике Сервера защиты верно указаны версии Легких агентов, для которых Сервер защиты будет получать обновления. Если требуется, с помощью флажков настройте список версий Легких агентов и примените политику.
 - c. Создайте и выполните задачу для Сервера защиты типа «Обновление баз».
- См. подробнее [«Обновление баз и программных модулей Kaspersky Security»](#).

4. Установка Легких агентов на защищаемые виртуальные машины

a. Установка элементов управления Легкими агентами в Kaspersky Security Center.

- Если вы планируете использовать Агентское решение для защиты виртуальных машин с операционными системами Windows, установите MMC- и веб-плагины Легкого агента для Windows (плагины управления приложением Kaspersky Endpoint Security для Windows 12.12).
- Если вы планируете использовать Агентское решение для защиты виртуальных машин с операционными системами Linux, установите MMC- и веб-плагины Легкого агента для Linux (плагины управления приложением Kaspersky Endpoint Security для Linux 12.4).

Обратите внимание, что в Kaspersky Security Center Web Console оптимизирована структура разделов политик приложений Kaspersky Endpoint Security, чтобы быстрее находить нужные функции. Также выполнена унификация разделов политик Kaspersky Endpoint Security для Windows и Kaspersky Endpoint Security для Linux, что позволяет идентично настраивать параметры приложений в режиме Легкого агента.

b. Создание политик для Легких агентов в Kaspersky Security Center.

Используя установленные элементы управления Легкими агентами, создайте в Kaspersky Security Center необходимые политики для Легких агентов. Рекомендуется учесть:

- Вы можете перенести значения параметров раздела «Защита виртуальных машин от файловых угроз» в идентичные параметры в разделах «Защита от файловых угроз» и «Общие настройки → Настройки приложения» (см. подробнее для Легкого агента для Linux: [«Защита от файловых угроз»](#), см. подробнее для Легкого агента для Windows: [«Защита от файловых угроз»](#)).
- Вы можете настроить исключения для «Защиты от файловых угроз» в политиках Легкого агента в разделе «Доверенная зона».

- Вы можете перенести значения параметров раздела «Защита от сетевых угроз» в идентичные параметры в разделе «Защита от сетевых угроз» (см. подробнее для Легкого агента для Linux: [«Защита от сетевых угроз»](#), см. подробнее для Легкого агента для Windows: [«Защита от сетевых угроз»](#)).
- Вы можете настроить исключения для «Защиты от сетевых угроз» в политиках Легкого агента в разделе «Защита от сетевых угроз» (если вы используете Консоль администрирования KSC) или в разделе «Доверенная зона» (если вы используете Web Console KSC).

c. Создание задач для Легких агентов в Kaspersky Security Center.

Используя установленные элементы управления Легкими агентами, создайте в Kaspersky Security Center необходимые задачи проверки. Рекомендуется учесть:

- Вы можете перенести значения параметров задачи «Полная проверка», настроенной для Безагентского решения, в идентичные параметры задач «Поиск вредоносного ПО» Легкого агента для Linux (см. подробнее [«Поиск вредоносного ПО»](#)) и Легкого агента для Windows (подробнее см. подробнее [«Поиск вредоносного ПО»](#)).
- Для Легкого агента для Windows вы можете настроить исключения для задачи проверки в политике Легкого агента в разделе «Доверенная зона» (см. подробнее [«Создание исключения из проверки»](#)).
- Для Легкого агента для Linux вы можете настроить исключения для задачи проверки в параметрах самой задачи.

d. Подготовка к установке Легких агентов на виртуальные машины.

Выполните подготовительные действия, описанные в следующих разделах справочника:

- Для Легкого агента для Linux: [«Подготовка к установке приложения Kaspersky Endpoint Security»](#) и [«Установка и первоначальная настройка приложения Kaspersky Endpoint Security»](#).
- Для Легкого агента для Windows: [«Установка и удаление приложения»](#).

e. Проверка виртуальных машин перед установкой Легких агентов.

Приведите виртуальные машины в соответствие с программными и аппаратными требованиями Агентского решения. Обратите особое внимание на предупреждение в разделе «Программные и аппаратные требования» этого руководства.

Если вы создаете новые виртуальные машины, не устанавливайте несовместимые драйверы и программное обеспечение.

Если вы настраиваете ранее созданные виртуальные машины, учтите, что после удаления несовместимых драйверов и программного обеспечения виртуальные машины остаются без защиты, которую обеспечивало Безагентское решение.

f. Установка Легких агентов на виртуальные машины.

Выполните установку Легких агентов. После установки поместите защищенные виртуальные машины в группы администрирования Kaspersky Security Center для распространения политик и задач.

Вам не нужно активировать Легкие агенты и выполнять обновление баз Легких агентов. Активацией решения и обновлением баз занимается Сервер защиты.

5. Проверка работоспособности решения после миграции

Убедитесь, что решение работает корректно:

- Проверьте статус защищенных виртуальных машин в консоли Kaspersky Security Center.
- Убедитесь в отсутствии ошибок в работе Легких агентов.
- Проверьте время последнего соединения Легких агентов с SVM.

6. Удаление Безагентского решения

Выполните полное удаление Kaspersky Security для виртуальных сред 6.1 Защита без агента (см. подробнее [«Удаление программы»](#)).

Источники информации

Справка на веб-сайте «Лаборатории Касперского»

В справке Kaspersky Security для виртуальных сред 6.4 Легкий агент (<https://support.kaspersky.com/help/ksvla/6.4/ru-RU/index.htm>) вы можете найти информацию об установке и использовании Агентского решения.

В справке Kaspersky Security для виртуальных сред 6.1 Защита без агента (<https://support.kaspersky.com/KSV/6.1/ru-RU/186128.htm>) вы можете найти информацию об установке и использовании Безагентского решения.

В справке Kaspersky Endpoint Security для Windows 12.12 (<https://support.kaspersky.com/KESWin/12.12/ru-RU/222859.htm>) вы можете найти информацию об установке и использовании Легкого агента для Windows.

В справке Kaspersky Endpoint Security для Linux 12.4 (<https://support.kaspersky.com/KES4Linux/12.4.0/ru-RU/287304.htm>) вы можете найти информацию об установке и использовании Легкого агента для Linux.

Страница Kaspersky Security для виртуальных сред Легкий агент на веб-сайте «Лаборатории Касперского»

На странице <http://www.kaspersky.ru/business-security/virtualization-light-agent> вы можете найти общую информацию о решении Kaspersky Security для виртуальных сред Легкий агент, его возможностях и особенностях работы.

Страница Kaspersky Security для виртуальных сред 6.4 Легкий агент в Базе знаний

База знаний – это раздел веб-сайта Службы технической поддержки.

На странице <https://support.kaspersky.ru/ksv-light-agent/6.4?page=kb> вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании решения Kaspersky Security для виртуальных сред 6.4 Легкий агент.

Статьи Базы знаний могут отвечать на вопросы, которые относятся не только к Kaspersky Security для виртуальных сред Легкий агент, но и к другим приложениям «Лаборатории Касперского». Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Обсуждение приложений «Лаборатории Касперского» на Форуме

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами «Лаборатории Касперского» и с другими пользователями на нашем Форуме (<https://forum.kaspersky.com/forum/%D1%80%D1%83%D1%81%D1%81%D0%BA%D0%BE%D1%8F%D0%B7%D1%8B%D1%87%D0%BD%D1%8B%D0%B9-%D1%84%D0%BE%D1%80%D1%83%D0%BC-162/>).

На Форуме вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.