002.11.6

Kaspersky Endpoint Security and Management

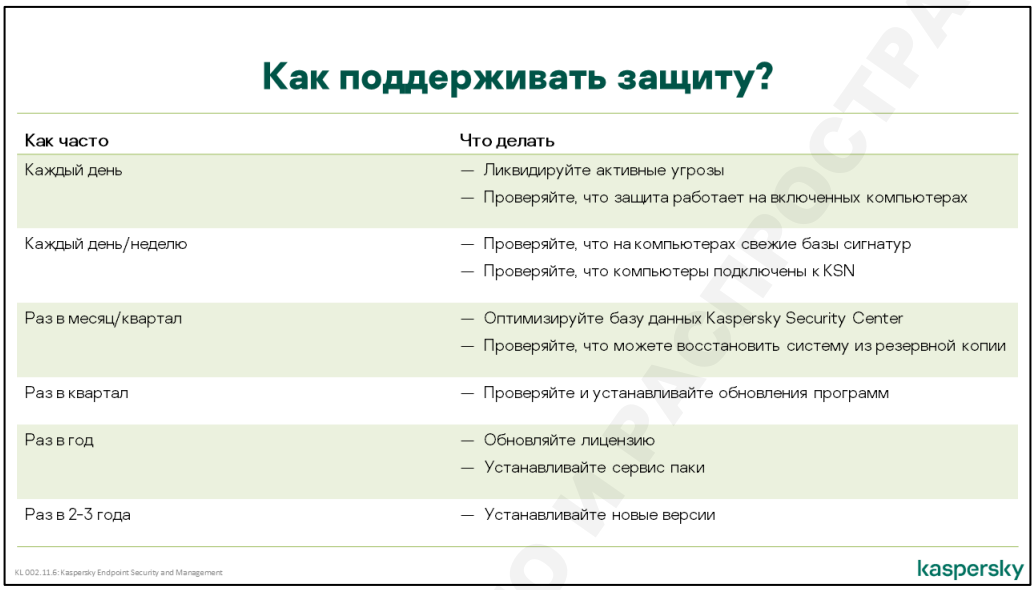
Часть IV. Обслуживание

kaspersky

Учебный курс

Содержание

1. Как поддерживать защиту



Когда вы установили на компьютеры Kaspersky Endpoint Security и Агент администрирования, создали необходимые политики и задачи, и настроили их, как считаете нужным, остается следить за тем, что защита работает, и реагировать инциденты.

Чтобы защита работала, необходимо делать разные вещи, какие-то из них чаще, а какие-то реже. Большинство мер не требуют пояснений, но мы их все равно приведем, на всякий случай.

Что делать каждый день

Проверяйте самое важное.

Что проверять	Почему так часто
На компьютерах нет необработанных угроз	Именно чтобы не было угроз, вы и устанавливаете защиту. Большинство угроз Kaspersky Endpoint Security блокирует автоматически. Но если защита не справилась, вам нужно немедленно об этом узнать и обезвредить угрозу самостоятельно. Чем дольше угроза активна, тем больший ущерб она нанесет. Это все достаточно очевидно.
Защита на компьютерах установлена и работает	Если защита не работает, вы не знаете, есть ли на компьютере вредоносные программы. И чем дольше защита не работает, тем больше шансов у вредоносных программ заразить компьютер.

Что делать раз в неделю

Устраняйте проблемы, которые ухудшают защиту. Если есть время, делайте это каждый день, но даже если времени нет, выделите один день в неделю на то, чтобы решать проблемы второго порядка.

Что проверять	Почему так часто
На компьютерах свежие базы сигнатур	Почти все компоненты защиты используют сигнатуры, чтобы обнаруживать вредоносные программы. Если сигнатуры старые, Kaspersky Endpoint Security не сможет обнаруживать новые вирусы. Чем более старые сигнатуры, тем больше риск. Поэтому если сигнатуры устарели на 2 дня, это плохо, но не критично. А если они устарели на 2 месяца, это почти так же опасно, как если бы защита не была запущена совсем
Защита использует Kaspersky Security Network	Kaspersky Security Network сообщает об известных вредоносных файлах и помогает их обнаруживать, даже если сигнатуры устарели. Более того, Kaspersky Security Network сообщает о новых вредоносных файлах раньше, чем для них появляются сигнатуры. Поэтому без Kaspersky Security Network защита работает не так хорошо. Но все же работает и защищает от большинства угроз.

Что делать раз в месяц

Выполняйте профилактические работы на Сервере администрирования.

Что проверять	Почему так часто
Проверяйте, что можете восстановить Сервер из резервной копии	Чтобы установить защиту вы потратили немало времени. Если вы потеряете Сервер администрирования из-за сбоя оборудования, вам придется потратить почти столько же времени, чтобы установить и настроить защиту заново. От этого защищает резервное копирование. А самое важное в резервном копировании не сделать копию, а проверить, что вы сможете ее восстановить. Потратьте полчаса в месяц на профилактику, чтобы в критический момент не оказалось, что что-то было неправильно настроено, вы об этом не знали, но теперь восстановить данные из копии нельзя.
Оптимизируйте базу данных Сервера администрирования	Если базу не оптимизировать, со временем она увеличивается в размерах и фрагментируется. Из-за этого у вас будет уходить больше времени на то, чтобы получить отчеты или отобразить выборку компьютеров. Особенно это проявляется в больших сетях или если у Сервера администрирования (вернее, сервера баз данных, но часто это один и тот же компьютер) недостаточно ресурсов.

Что делать раз в квартал

Устанавливайте промежуточные обновления и исправления.

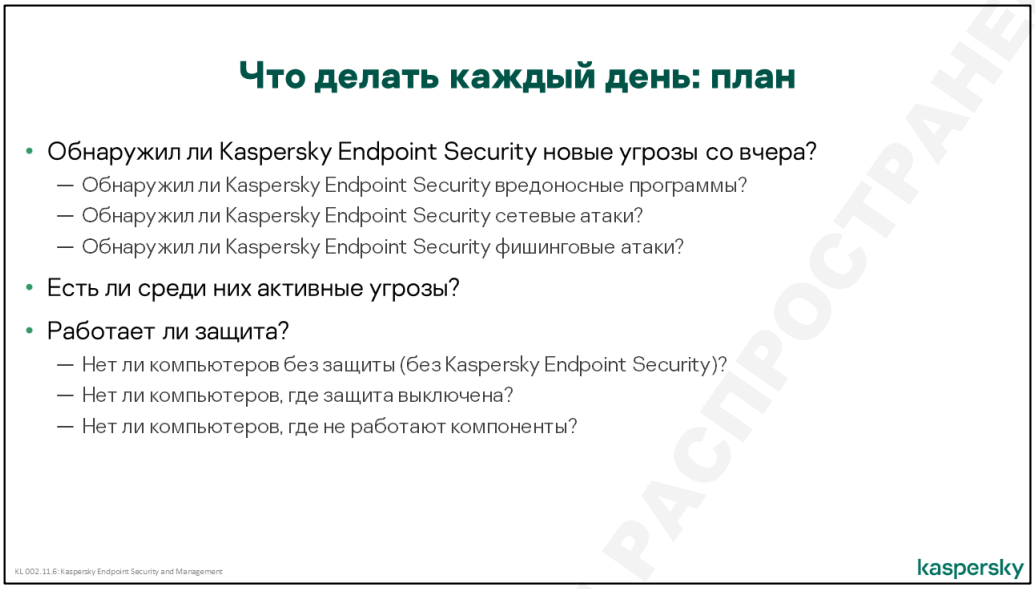
Что проверять	Почему так часто
Нет ли обновлений или исправлений к продуктам Лаборатории Касперского	Патчи Kaspersky Security Center и пакеты обновлений (maintenance release) Kaspersky Endpoint Security выходят примерно раз в 1-2 квартала. Они исправляют ошибки, улучшают производительность и, иногда, добавляют новые функции, важные для защиты. Чтобы установить патчи, много усилий не нужно, но не забывайте тестировать их перед установкой.

Что делать раз в год

Продлевайте лицензию и устанавливайте новые версии.

Что проверять	Почему так часто
Лицензия не истекла и не превысила ограничение по узлам	Коммерческие лицензии, как правило, продаются на 1 год. Без лицензии защита продолжает работать, но задача обновления перестает загружать сигнатуры и Kaspersky Endpoint Security перестает использовать KSN. Поэтому со временем защита становится хуже.
Нет ли новых версий продуктов Лаборатории Касперского	Новые версии или большие пакеты обновлений (service pack) выходят раз в 1-2 года. Они исправляют ошибки, улучшают производительность, но также меняют настройки и работу продуктов. Новые технологии, компоненты, способы перехвата и т.п. появляются именно в новых версиях или сервис паках. Если старую версию долго не обновлять, то даже с новыми сигнатурами и при помощи KSN она не сможет блокировать новые угрозы. К тому же спустя несколько лет после выхода старые версии снимаются с поддержки.

2. Что делать каждый день



Во время ежедневного осмотра:

1. Выясните, какие угрозы Kaspersky Endpoint Security обнаружил с прошлого осмотра. Если вы проводите осмотр каждый день, значит вас интересуют угрозы за последние сутки.

2. Разберитесь, все ли угрозы Kaspersky Endpoint Security обезвредил. Если есть необработанные угрозы, займитесь ими немедленно

3. Посмотрите, на всех ли компьютерах работает защита. Если защита не запущена или не установлена, запустите или установите ее. Выясните, почему так произошло.

Чтобы не тратить на осмотр много времени, подготовьте инструменты в консоли, чтобы быстро узнавать все, что нужно об угрозах и защите.

2.1 Как собрать быстрый дэшборд

Как ответить на все вопросы одним взглядом

Информацию в консоли Kaspersky Security Center можно найти во множестве разных мест:

— Отчетах
— Событиях
— Статусах компьютеров
— Свойствах компьютеров
— Статистике установленных программ в свойствах компьютеров
— Хранилищах вредоносных объектов
— Журналах задач

Но они или недостаточно наглядны, как списки событий, или их нельзя осмотреть все сразу, как отчеты.

Чтобы быстро получить общее представление о состоянии защиты, можно открыть Веб-консоль администрирования на вкладке **Мониторинг и отчеты | Панель мониторинга**. На ней администратор сам выбирает, какие графики показывать, какие формы графиков использовать и как их расположить друг относительно друга.

Чтобы сократить время ежедневного осмотра, сделайте свою панель мониторинга и поместите на нее веб-виджеты с графиками о:

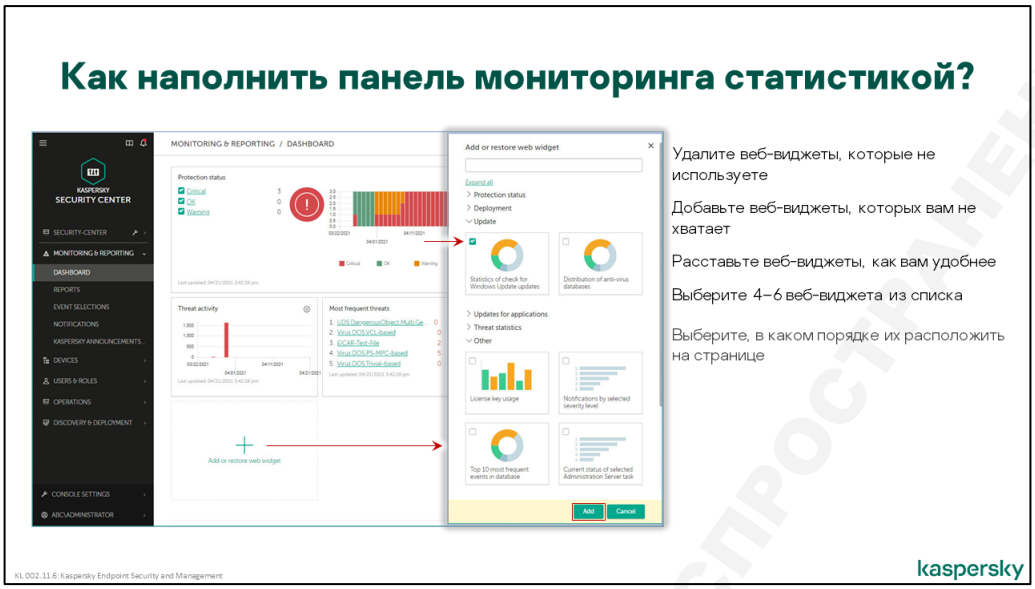
- Состояние защиты
- Типы обнаруженных вирусов и результаты лечения
- Новые устройства
- Сетевых атаках
- История сетевых атак
- Типы обнаруженных вирусов и результаты лечения
- И других важных событиях на свое усмотрение, например, о версиях сигнатур

Типы веб-виджетов фиксированы, но их достаточно много и для большинства вопросов есть веб-виджет, который отвечает на этот вопрос.

Как наполнить панель мониторинга статистикой

По умолчанию вкладка **Панель мониторинга** включает 7 веб-виджетов, посвященных различным аспектам состояния сети: *Состояние защиты*, *Новые устройства*, *Активность угроз*, *Наиболее распространенные угрозы*, *Наиболее зараженные устройства*, *Обнаружение угроз компонентами программы*.

Обычно веб-виджет представляет собой график или диаграмму с легендой. По умолчанию они строятся на основе событий со всех управляемых компьютеров и по данным за последний день, если это распределение во времени. Администратор может ограничить диапазон компьютеров, или ввести другой период — окно настройки открывается кнопкой ⚙. Панель мониторинга состоит из нескольких веб-виджетов.

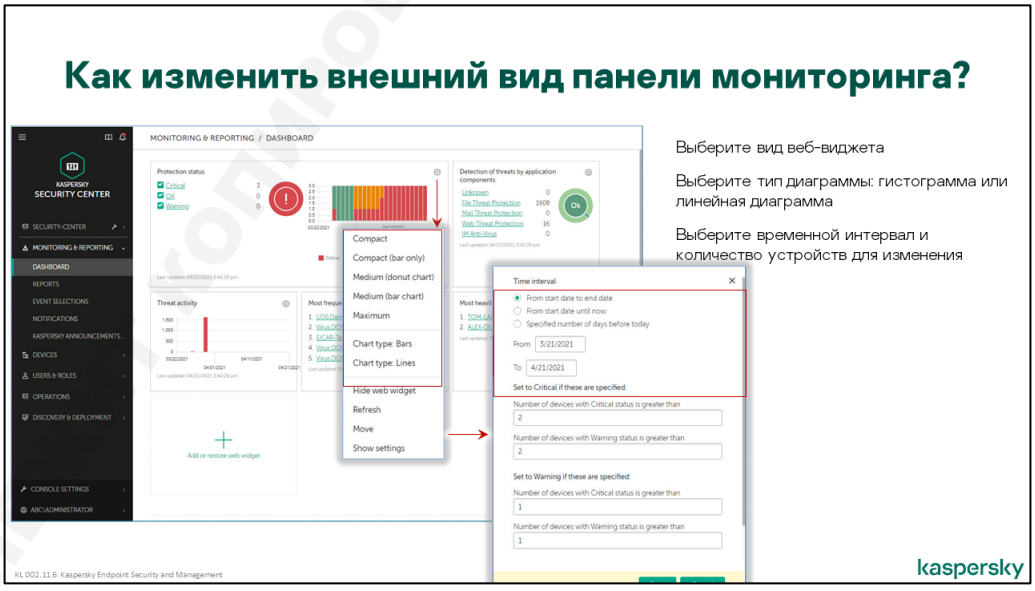


Администратор может добавлять, удалять и перемещать веб-виджеты на панели мониторинга, а также может менять настройки и внешний вид веб-виджетов.

Всего доступно более 25 видов веб-виджетов, сгруппированных в 6 категорий. Администратор может свободно комбинировать различные веб-виджеты на панели мониторинга, как ему удобнее.

Чтобы изменить наполнение панели мониторинга нужно использовать веб-виджет *Добавить или восстановить веб-виджет*.

В настройках веб-виджета, в зависимости от его типа, можно изменить временной интервал для отображаемых данных и компьютеры, с которых собираются данные. Для компьютеров есть всего два варианта — либо группа администрирования, либо компьютеры из указанной выборки.

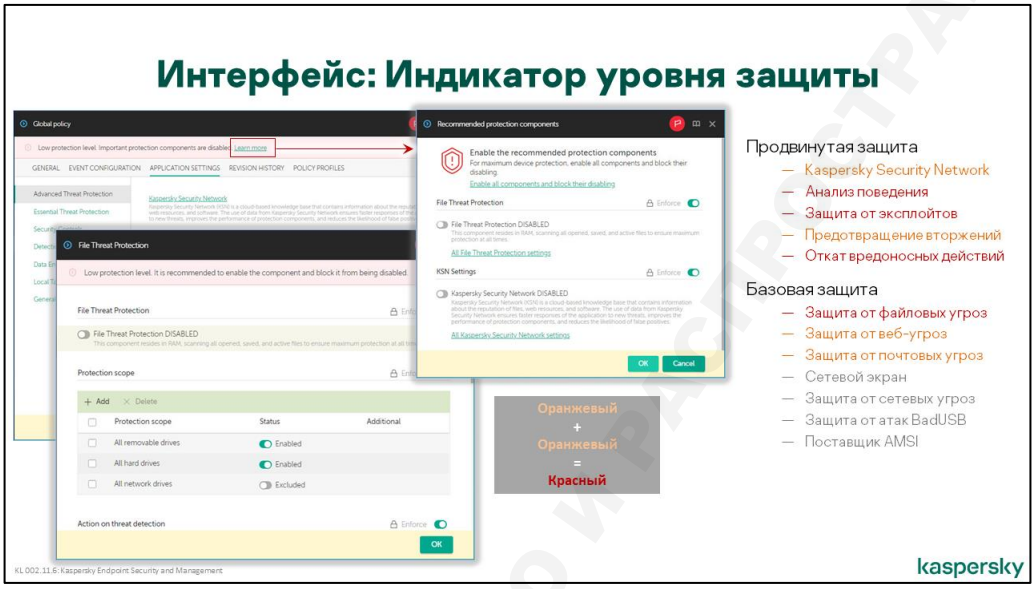


В настройках внешнего вида веб-виджета можно изменить тип и выбрать вид диаграммы.

Одной из возможностей веб-виджетов является вывод истории изменения определенного показателя за период. Например, сколько вирусов было обнаружено за каждый час прошедших

суток. Эти данные могут помочь выбрать порог для события *Вирусная атака*. И такой возможности нет в отчетах.

Как понять, что в политике выключены важные компоненты защиты



В интерфейсе свойств политики, начиная с версии Kaspersky Endpoint Security 11, появился **Индикатор уровня защиты**, который помогает администратору оценить уровень противодействия угрозам, и подсказывает, какие компоненты необходимо включить, чтобы уровень защиты соответствовал максимальному.

Например, администратор в политике включил все компоненты Базовой защиты и Продвинутой защиты, но по ошибке или целенаправленно, отключил критически важный компонент **Анализ поведения**, который обнаруживает угрозы на основе анализа поведения программ, в частности, детектирует сложные угрозы такие как программы-вымогатели. Как только компонент **Анализ поведения** будет выключен, **Индикатор уровня защиты** сразу изменит цвет на красный и надпись на индикаторе будет соответствовать статусу *Уровень защиты низкий*. Дополнительно, после применения настроек политики, справа от индикатора, появится надпись *Выключены важные компоненты защиты* и ссылка *Узнать больше*, кликнув по которой, отроется окно *Рекомендованные компоненты защиты*, в котором можно включить необходимые компоненты для максимального противодействия угрозам. Если администратор игнорирует предупреждение и нажмёт кнопку *Сохранить* в окне политики, Kaspersky Security Center покажет информационное окно и предложит исправить ситуацию.

Индикатор уровня защиты может принимать одно из следующих значений:

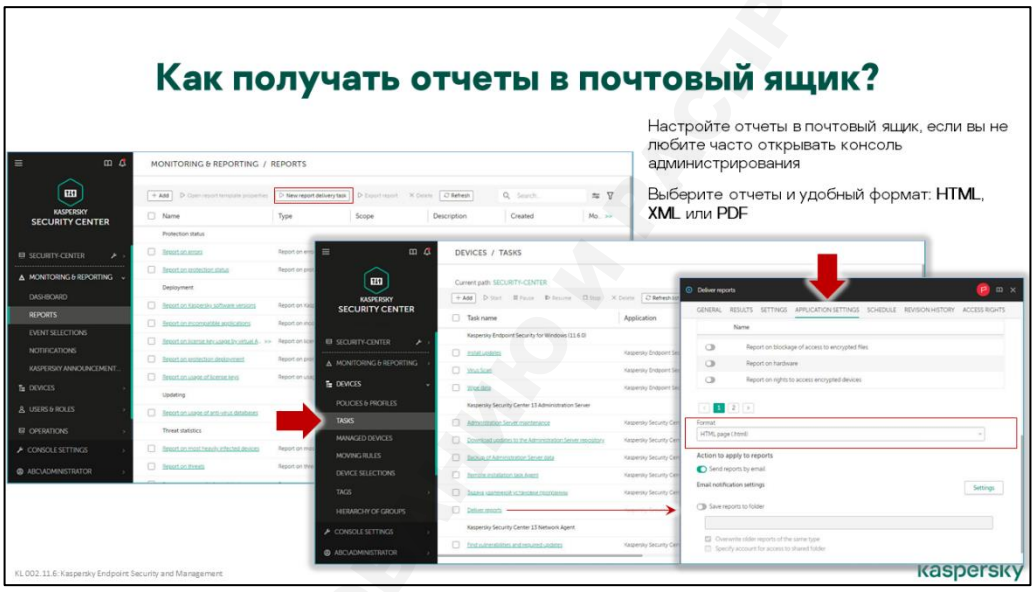
- **Уровень защиты высокий**. Цвет индикатора изменяется на зеленый, если включены все компоненты, относящиеся к следующим категориям:
  - Критические:
    - Защита от файловых угроз;
    - Анализ поведения;
    - Защита от эксплойтов;
    - Откат вредоносных действий.
  - Важные:
    - Kaspersky Security Network;
    - Защита от веб-угроз;

— Защита от почтовых угроз;
— Предотвращение вторжений.

— **Уровень защиты средний**. Цвет индикатора изменяется на желтый, если отключен один важный компонент.
— **Уровень защиты низкий**. Цвет индикатора изменяется на красный в одном из следующих случаев:

— отключены один или несколько критических компонентов;
— отключены два или более важных компонента.

2.2 Как получать отчеты в почтовый ящик



Некоторые администраторы предпочитают открывать Консоль, только когда уже нужно что-то выяснять или настраивать, а узнавать о проблемах предпочитают по почте. Так они используют один инструмент — почтовый ящик — чтобы узнавать о проблемах разных подсистем, вместо того, чтобы открывать десяток разных консолей.

Kaspersky Security Center может доставлять уведомления и отчеты по почте. Для ежедневного осмотра лучше подходят отчеты, которые показывают, что происходит во всей сети. Уведомлениями сообщайте о конкретных угрозах, которыми нужно заняться немедленно.

Чтобы получать отчеты по почте, используйте соответствующую задачу:

1. Выберите вкладку **Отчеты** в разделе **Мониторинг и отчеты** и нажмите **Новая задача рассылки отчетов**

2. Если задача такого типа уже есть, веб-консоль сообщит об этом. Чтобы отредактировать параметры, откройте окно свойств задачи **Рассылка отчета** и перейдите на вкладку **Параметры программы.**

3. Если задачи такого типа еще нет, веб-консоль запустит мастер создания задачи рассылки отчетов

4. Выберите типы отчетов, которые хотите получать. Задача показывает все шаблоны отчетов, которые есть на вкладке **Отчеты**. Но это не все типы отчетов, которые умеет

создавать Kaspersky Security Center. Если каких-то отчетов не хватает, создайте их предварительно на вкладке **Отчеты** в разделе **Мониторинг и отчеты**.

5. Выберите формат. Поддерживаются html, xls и pdf.

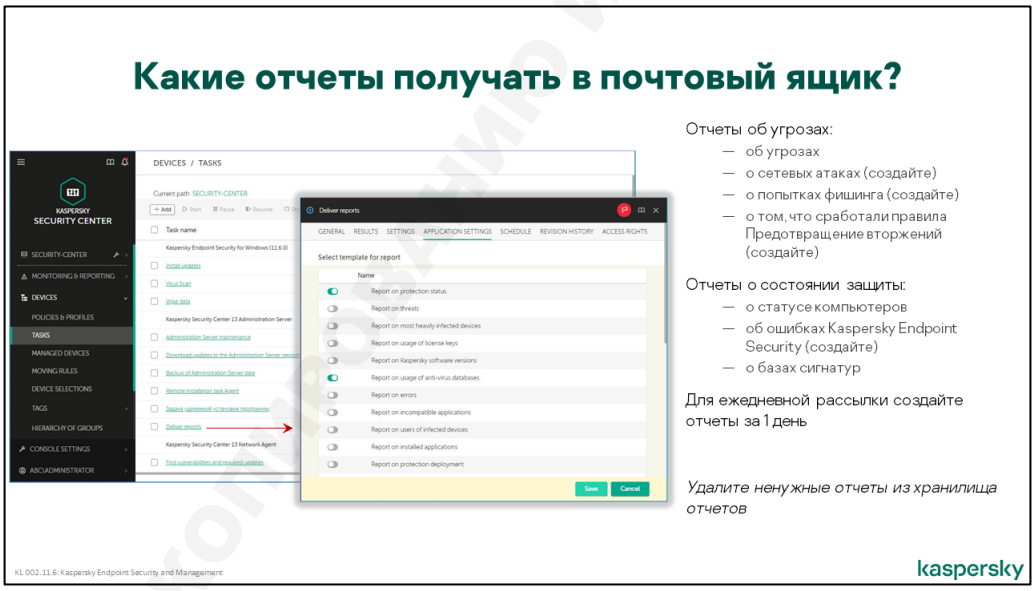
6. Выберите действия с отчетами. Отчеты можно пересылать по почте и/или сохранять в папке.

7. Перейдите на вкладку **Расписание** и выберите, когда получать отчеты.

Чтобы выбрать, куда посылать отчеты, выберите в свойствах задачи вкладку **Параметры программы** в области **Действие с отчетами** включите параметр **Посылать отчеты по электронной почте** и нажмите кнопку **Параметры**. Здесь выберите адрес получателя и тему письма. Адрес отправителя и параметры почтового сервера проверьте в свойствах Сервера администрирования.

Примечание: мастер первоначальной настройки веб-консоли, если в нем задать параметры почтового сервера, в отличие от мастера первоначальной настройки MMC-консоли не создает автоматически задачу рассылки отчетов.

Какие отчеты получать в почтовый ящик



Для ежедневного осмотра понадобятся отчеты, которые показывают угрозы, и отчеты, которые показывают состояние защиты:

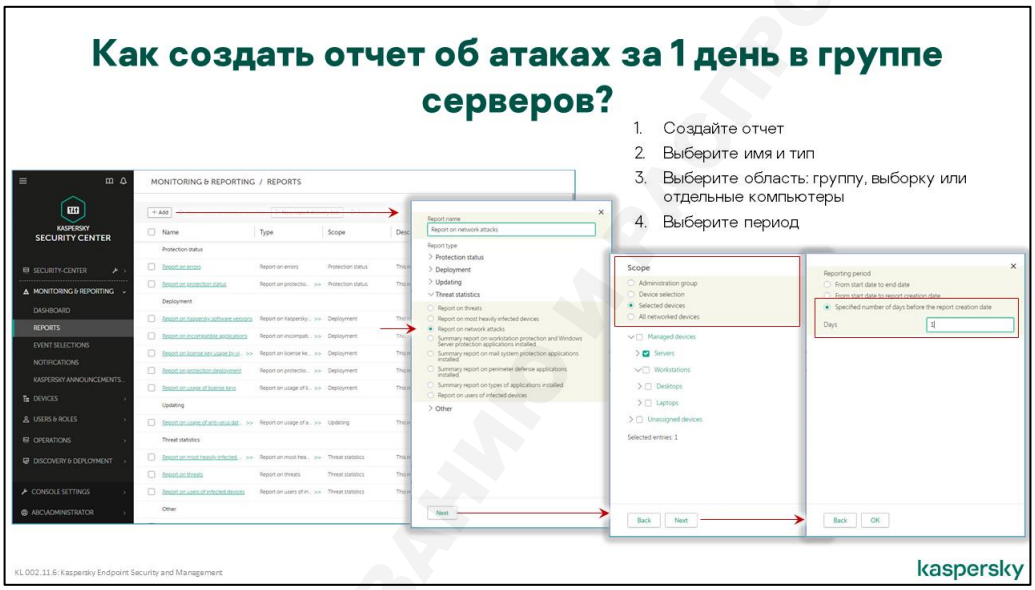
- Угрозы:
  - О вирусах (за день)
  - О сетевых атаках (за день)
  - О попытках фишинга (за день)
  - О правилах предотвращения вторжений (за день)
- Защита
  - О состоянии защиты
  - Об используемых базах
  - Отчет об ошибках (за день)

Все отчеты, которые есть в разделе **Отчеты** по умолчанию или не имеют периода, или показывают события за последние 30 дней. Использовать отчеты за 30 дней для ежедневного осмотра неудобно. По ним сложно понять, что изменилось сегодня, по сравнению с вчера.

Поэтому отчеты с периодом за день создайте отдельно. Заодно удалите все отчеты, которые не собираетесь использовать. Например, отчеты об ошибках шифрования, если у вас нет лицензии на шифрование.

Как создать свой отчет

Как создать отчет за период



Формально в разделе **Отчеты** находятся не сами отчеты, а *шаблоны отчетов*, которые описывают тип и параметры отчета. Отчеты Сервер администрирования генерирует из шаблонов, когда администратор нажимает на ссылку с именем отчета, или когда нужно отправить отчеты по почте.

Чтобы создать отчет (шаблон отчета):

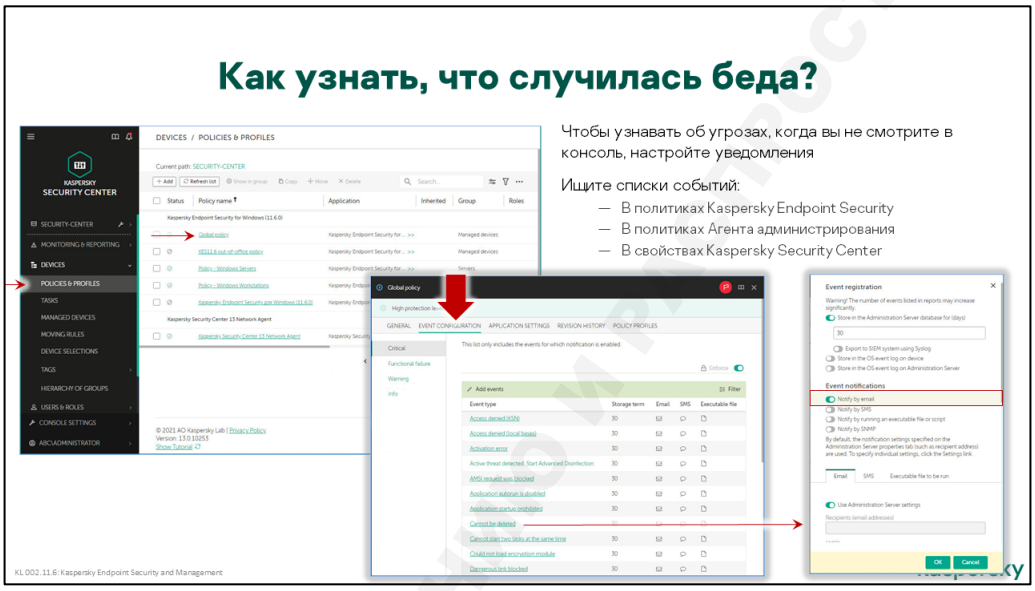
1. В разделе **Отчеты** нажмите кнопку **Добавить**
2. Дайте ему понятное имя, например, *Отчет об угрозах* за 1 день
3. Выберите тип отчета. В Kaspersky Security Center более 50 типов отчетов
4. Выберите область действия отчета. Отчет может быть для группы, для отдельных компьютеров (списка) и для *выборки компьютеров*. Большинство отчетов нужны для всей сети сразу, для этого выбирайте область действия отчета **Все устройства в сети.**
5. Выберите период. Для отчетов в ежедневную рассылку укажите период 1 день

В настройках шаблона задается также перечень информационных полей, которые составляют таблицы отчета. Некоторые поля не несут важной информации и их вполне можно удалить, чтобы

не загромождать отчет. Например, поле *Виртуальный сервер* нет смысла включать в отчет, если в сети не используются виртуальные сервера администрирования[1].

2.3 Как получать уведомления в почтовый ящик

Где включить уведомления



Параметры хранения событий по их типам задаются в политиках Kaspersky Endpoint Security и Агента администрирования, а также в свойствах Сервера администрирования — на вкладке **Настройка событий**. События разбиты на 4 уровня важности — *Критическое*, *Отказ функционирования*, *Предупреждение*, *Информационное сообщение*. Уровень важности является постоянным атрибутом события, изменить его нельзя. У каждой программы свои события со своими настройками по умолчанию.

У любого события есть три настройки хранения:

— **На Сервере администрирования** — т.е. в базе данных Сервера

Этот способ хранения включен для большинства критических событий и ошибок, многих предупреждений и некоторых информационных сообщений. У Kaspersky Endpoint Security и Агента администрирования время хранения по умолчанию равно 30 дням для любых событий, кроме тех, хранение которых отключено.

У Сервера администрирования время хранения событий по умолчанию одинаковое для всех уровней важности – 30 дней.

Дополнительно можно настроить экспорт в SIEM-систему событий, произошедших на Сервере администрирования и в других программах "Лаборатории Касперского", установленных на управляемых устройствах. Для этого отметьте флаг **Экспортировать в SIEM-систему по протоколу Syslog** (стандарт RFC 5424).

[1] Здесь «виртуальный Сервер администрирования» или «Виртуальный сервер», как написано в отчете, не нужно путать с Сервером администрирования, запущенным на виртуальной машине. Слово виртуальный в отчете используется в другом, гораздо более специальном смысле. В терминах Kaspersky Security Center Сервер администрирования на виртуальной машине, это не виртуальный, а обычный Сервер администрирования. Виртуальные сервера Kaspersky Security Center описаны в курсе 302

— **В журнале событий ОС на устройстве** — имеет смысл только для событий Агента администрирования. Для Kaspersky Endpoint Security аналогичная возможность есть в настройках локальной обработки событий.

— **В журнале событий ОС на Сервере администрирования** — смысл тот же, что и для локальных событий Kaspersky Endpoint Security. Если вдруг Сервер администрирования окажется недоступен, администратор сможет почерпнуть информацию из журнала Windows.

По истечении указанного времени хранения событий в базе данных Сервера администрирования они автоматически удаляются (но остаются в журналах Windows, у которых свои параметры хранения). Чем дольше срок хранения, тем больше событий в среднем находится в базе в каждый конкретный момент, и тем медленнее буду выполняться операции, связанные с обработкой событий. С другой стороны, уменьшая время хранения событий, администратор уменьшает и максимальный период, который могут отражать отчеты.

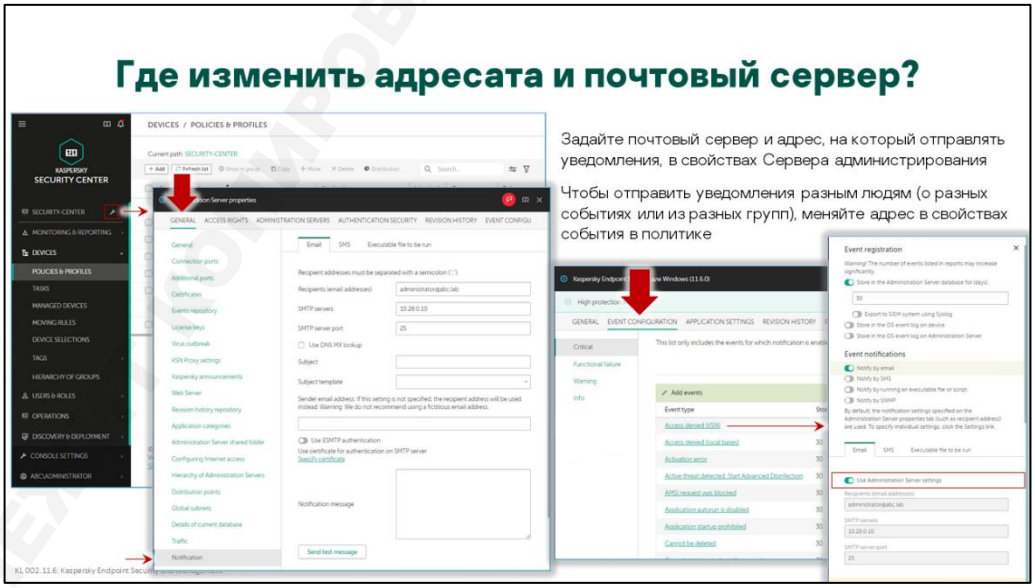
Чтобы узнавать о важных событиях, настройте уведомления. Настройки расположены в том же окне свойств события и одинаковы для всех событий. Kaspersky Security Center поддерживает 4 канала доставки уведомлений:

— Электронная почта
— SMS
— Запуск исполняемого файла или скрипта
— SNMP

Уведомления призваны привлечь внимание администратора к наиболее важным событиям.

По умолчанию никакие уведомления не отсылаются. Чтобы начать получать уведомления, откройте свойства события и отметьте методы доставки.

Как изменить адресата и почтовый сервер



По умолчанию все события доставляются с одинаковыми параметрами, заданными в свойствах Сервера администрирования. Чтобы отправлять разные уведомления на разные адреса или с разным шаблоном текста, откройте свойства события и отключите параметр **Использовать параметры Сервера администрирования**. После этого измените адреса получателей, шаблон текста и другие параметры уведомления.

Изначально, параметры доставки почтовых уведомлений задаются в ходе выполнения мастера первоначальной настройки. Впоследствии их можно изменить в разделе Уведомление на вкладке **Общие** в окне свойств Сервера администрирования.

Параметры доставки почтовых уведомлений состоят из:

- Получатели — почтовые адреса через точку с запятой
- SMTP-сервер — имя или IP-адрес
- Порт SMTP-сервера
- Использовать DNS и MX поиск
- Текста уведомления

Этих параметров достаточно, если для отправки уведомлений через выбранный SMTP-сервер не нужна авторизация. Адрес получателя используется и как адреса отправителя, а тема отправляемых уведомлений формируется из уровня важности события и его типа, например, *Критическое событие: Обнаружен вредоносный объект*

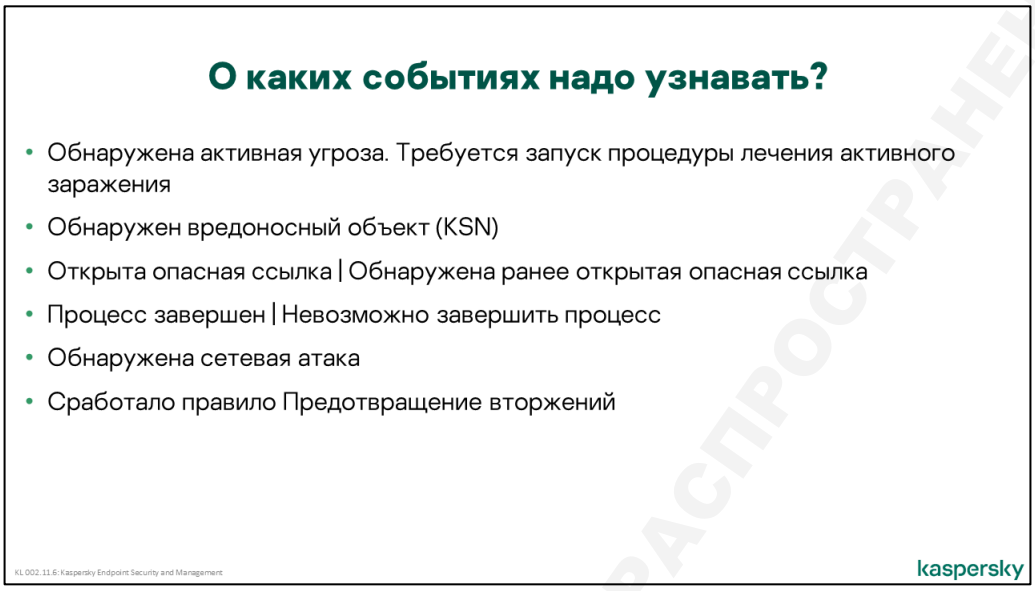
Дополнительно можно настроить следующее:

- Тему шаблона сообщения
- Имя пользователя и пароль для авторизации
- Адрес отправителя
- Задать сертификат для аутентификации на SMTP-сервере

При настройке темы и текста уведомления можно использовать макросы, которые при составлении уведомления будут заменены соответствующими атрибутами события:

- %SEVERITY% — Уровень важности события
- %COMPUTER% — Устройство-отправитель
- %DOMAIN% — Windows-домен
- %EVENT% — Событие
- %DESCR% — Описание события
- %RISE_TIME% — Время возникновения
- %KLCSAK_EVENT_TASK_DISPLAY_NAME% — Название задачи
- %KL_PRODUCT% — Программа
- %KL_VERSION% — Номер версии
- %HOST_IP% — IP-адрес
- %HOST_CONN_IP% — IP-адрес соединения

О каких событиях нужно знать



О каких событиях получать уведомления, решает администратор. Но первыми кандидатами будут события об активных угрозах и потенциально успешных атаках:

Событие	О чем говорит
Обнаружена активная угроза. Требуется запуск процедуры лечения активного заражения	Вредоносный файл выполняется на компьютере, но Kaspersky Endpoint Security не может его выгрузить. Чтобы начать лечение активного заражения, нужно подтверждение пользователя или администратора
Обнаружен вредоносный объект (KSN)	Вредоносный объект обнаружен не сигнатурами, а по запросу в KSN. Это значит, что это новая угроза, и администратору нужно внимательно следить, за тем, что происходит в сети. Может быть даже перейти на политику с повышенными настройками защиты
Обнаружена ранее открытая опасная ссылка	Информация о том, что ссылка является опасной, появилась уже после того, как пользователь ее открыл (данные о прошлых действиях хранит кэш KSN и журналы Мониторинга системы). Пользователь мог загрузить и запустить еще неизвестную вредоносную программу.
Процесс завершен	Вредоносная программа выполнялась на компьютере. Хотя Kaspersky Endpoint Security ее завершил, она могла успеть нанести ущерб
Обнаружена сетевая атака	Если атакующий компьютер находится внутри сети, это может значить, что он заражен неизвестной вредоносной программой, или что на нем не работает защита
Сработало правило Предотвращения вторжений	Если вы настроили Предотвращение вторжений защищать документы от программ-вымогателей, эти события сообщат, когда неизвестные программы пытаются менять или удалять документы пользователей

Все эти события относятся к Kaspersky Endpoint Security. Ищите их в политике Kaspersky Endpoint Security на вкладке **Настройка событий**. Последнее событие является *Информационным сообщением*. Все остальные — это *Критические события*.

Некоторые, в том числе и важные события могут случаться слишком часто, чтобы отправлять уведомления о каждом из них. Например, событие **Обнаружен вредоносный объект** в ходе вирусной атаки может породить десятки и сотни уведомлений.

Чтобы каждое уведомление привлекало внимание, включите ограничение на количество уведомлений. Для этого в свойствах Сервера администрирования откройте раздел **Уведомление** и нажмите ссылку *Настроить ограничение количества уведомлений*.

Установите лимит в виде максимального количества уведомлений за определенный период времени. По достижении лимита уведомления прекращаются до конца указанного периода. Если после этого приходят новые события, ограничение отсчитывается заново. Ограничение одинаковое для всех видов уведомлений, но применяется отдельно к каждому типу события. Например, если достигнут лимит для уведомлений о событиях **Обнаружена угроза**, уведомления о других событиях не пострадают.

3. Что делать, если что-то случилось

3.1 Что делать с вредоносными программами

Если за день на компьютерах не появилось новых событий об угрозах, ничего делать не надо. Но что делать, если события есть?

В первую очередь разберитесь, что произошло с угрозами. Если Kaspersky Endpoint Security удалил, вылечил или заблокировал угрозу, ничего делать не нужно. Просто обнулите счетчик вирусов на компьютере, чтобы видеть, когда появятся новые угрозы.

Если вредоносная программа не вылечена и не удалена, действуйте по плану. План подготовьте заранее.

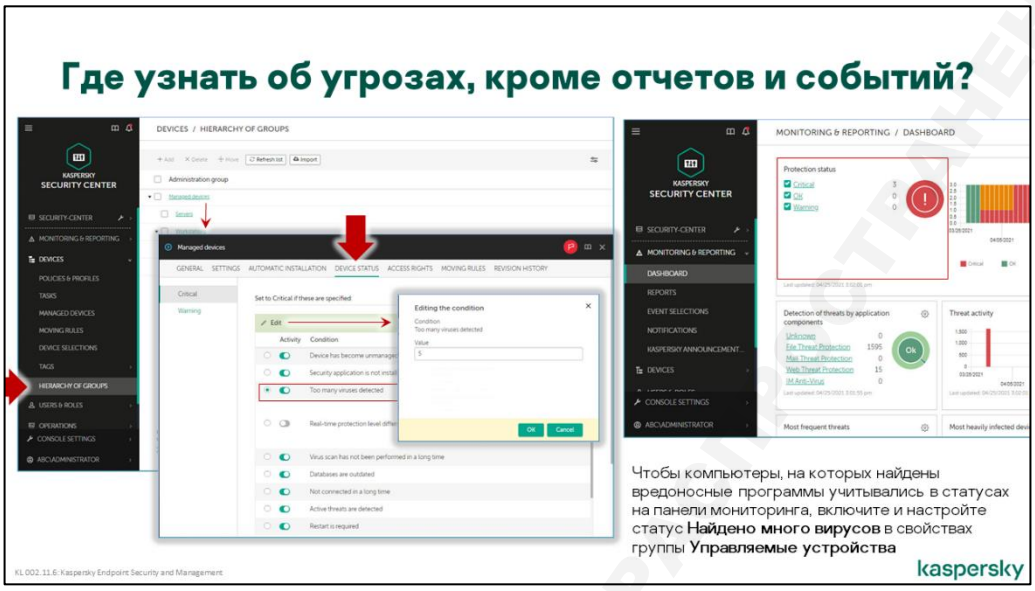
Типичный план может включать такие шаги:

1. Запустите проверку критических областей, чтобы понять, заражен ли компьютер
2. Если компьютер заражен или вы подозреваете, что он может быть заражен неизвестной вредоносной программой:
   2.1. Изолируйте компьютер от остальных компьютеров в сети
   2.2. С помощью пароля выйдите из-под политики
   2.3. Увеличьте уровень эвристики и включите лечение активного заражения
   2.4. Проверьте целостность Kaspersky Endpoint Security локальной задачей
   2.5. Выполните полную проверку компьютера

Если все это не помогает, восстановите компьютер из образа. Если в компании все компьютеры установлены из образа, а данные пользователей хранятся не на компьютерах, а в сети, восстановить из образа может быть первым шагом плана, чтобы не терять время.

Если в ходе расследования вы нашли подозрительные файлы, отправьте их для анализа в Лабораторию Касперского через кабинет на портале *companyaccount.kaspersky.com* , или задействуйте внутренние или внешние ресурсы для расследования инцидента, если есть подозрение на целенаправленную атаку против вашей организации.

Где узнать об угрозах



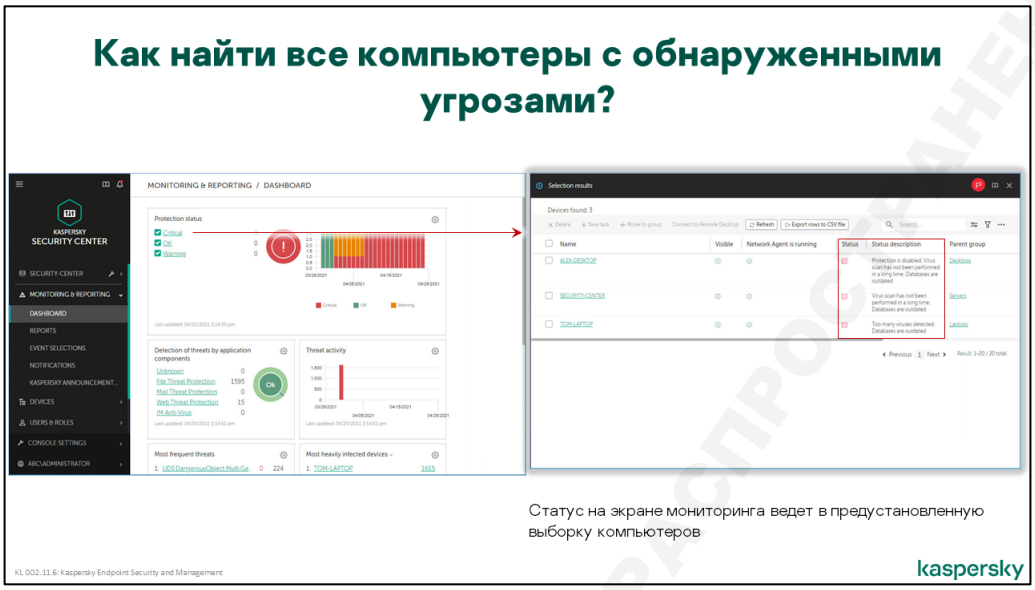
О том, что найдены вирусы можно узнать из событий, отчетов, статистики и статусов компьютеров. Не считая статистики, статусы первыми обращают на себя внимание.

Обнаружение и результаты обработки угроз влияют на статус компьютера в Консоли администрирования — **OK**, **Предупреждение** или **Критический**. Это позволяет администратору легко выделять проблемные компьютеры при просмотре группы.

О том, что на компьютерах были вирусы, говорит статус **Найдено много вирусов**. Этот статус связан с таким параметром как счетчик вирусов. Каждый раз, когда на компьютере фиксируется обнаружение вредоносной программы, счетчик увеличивается на 1. Значение счетчика передается на Сервер администрирования во время синхронизации. Статус становится активным, если счетчик вирусов превышает указанное пороговое значение. По умолчанию статус **Найдено много вирусов** отключен.

Чтобы включить статус и видеть компьютеры, на которых найдено много вредоносных программ, перейдите в раздел **Иерархия групп,** откройте свойства узла **Управляемые устройства**. Перейдите на вкладку **Статус устройства** и активируйте статус **Найдено много вирусов**. Чтобы компьютеры получали статус *Предупреждение* и становились желтыми, активируйте статус в разделе **Установить статус ‘Предупреждение’ если:**. Чтобы компьютеры становились красными, активируйте статус в разделе **Установить статус ‘Критический’ если:**. Чтобы компьютеры становились желтыми, когда на них просто есть вирусы, и красными, когда событий о вирусах было больше 5, настройте разные пороговые значения для статуса **Найдено много вирусов** (выберите статус и нажмите кнопку **Изменить**).

Как найти компьютеры с угрозами



Если есть хотя бы один компьютер со статусом **Есть необработанные объекты** или **Найдено много вирусов** меняется цифра возле глобального статуса в веб-виджете **Состояние защиты** в панели мониторинга.

Статусы **OK**, **Предупреждение**, **Критический** являются ссылками. Если кликнуть по статусу **Критический**, открывается выборка устройств с соответствующим статусом. Точно так же ведут себя все статусы. В выборке можно ознакомиться с описанием причин, которые привели к присвоению устройству соответствующего статуса.

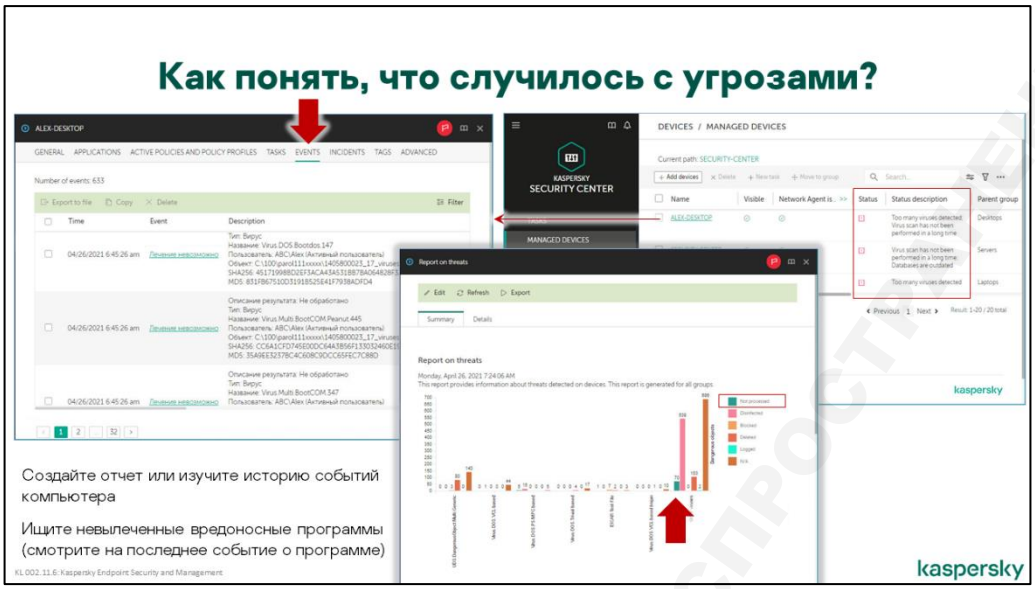
Выборка — это динамический набор компьютеров, отобранных по какому-либо признаку. На Сервере администрирования есть стандартные выборки, которые показывают компьютеры с разными статусами. Среди них есть и выборки **Есть активные угрозы** и **Найдено много вирусов**

С компьютерами, объединенными в выборку, можно выполнять групповые действия, например, запускать для них задачи обновления и поиска, перемещать в группу. Таким образом, выборки удобно использовать для исправления ситуации на компьютерах, имеющих проблемный статус.

Как понять, что случилось с угрозами

Отчет об угрозах показывает статистику результатов обработки вредоносных программ, найденных на управляемых компьютерах — сколько объектов было вылечено, сколько заблокировано (Веб-Антивирусом) сколько удалено и сколько остались необработанными. Также показывается число опасных объектов, результаты обработки которых неизвестны. Такая статистика приводится по каждому типу вредоносной программы отдельно.

Отчет об угрозах может показывать, какие вредоносные программы KES обнаружил и с помощью, какой технологии была обнаружена угроза. Чтобы увидеть это, добавьте в таблицу детализации колонку **По заключению KSN**. Можно добавить в отчёт, какая **Технология обнаружения** выявила вредоносный код и отразить **Хеш-функцию SHA-256**. Для этого в свойствах **Отчёт об угрозах** перейдите на вкладку **Графы** выберите область **Детальные данные**, кнопка **Добавить** и раскрывающемся списке **Название поля отчёта** выберите одноимённые значения поля.



Кроме отчета об угрозах, полезными могут быть *Отчет о наиболее заражаемых устройствах* и *Отчет о пользователях зараженных устройств*. Если на некоторых компьютерах частота заражения существенно (в несколько раз) выше, чем на других, имеет смысл разобраться, в чем причина такого отклонения и принять меры.

Сетевые атаки не попадают в отчет о вирусной активности. Чтобы увидеть общую картину по всем атакам, смотрите в *Отчет о сетевых атаках*. Он показывает, какие типы атак были выявлены, и что более важно, IP-адреса компьютеров, которые выполняли атаки. Зная адрес, администратору может разобраться, почему с компьютера выполнялись атаки и устранить проблему.

Отчет о сетевых атаках не входит в список стандартных отчетов. Чтобы его увидеть, создайте новый шаблон в разделе **Мониторинг и Отчеты | Отчеты**.

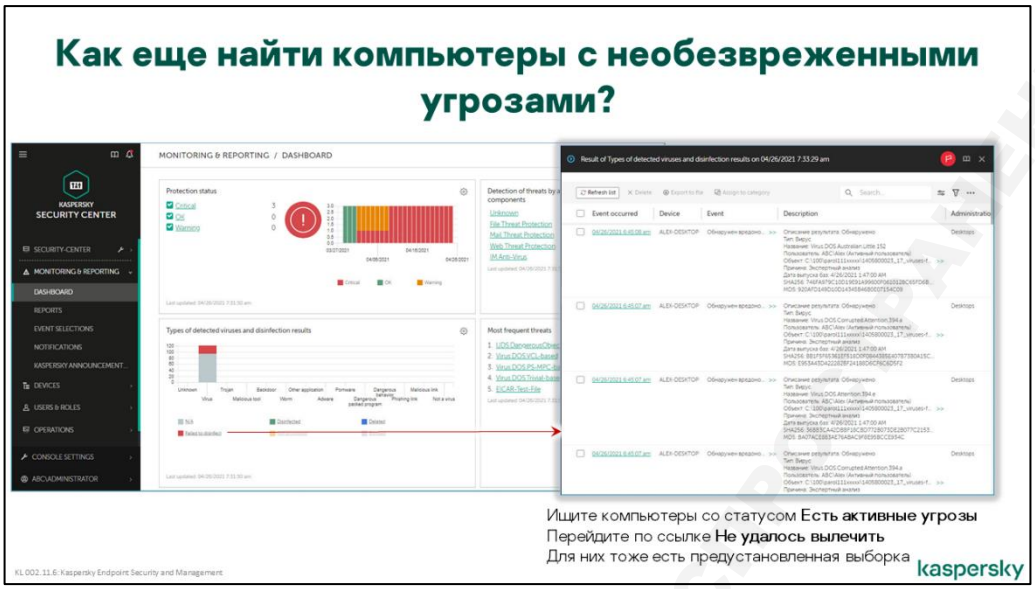
Кроме отчетов, чтобы понять, как Kaspersky Endpoint Security справился с угрозами, смотрите в события компьютера. В событиях можно заметить, что происходило одновременно с обнаружением угрозы, были ли сообщения о других угрозах или ошибках в работе компонентов. Чтобы понять, что случилось с угрозой, всегда смотрите на самое последнее событие о ней. Вполне нормально, когда Kaspersky Endpoint Security сначала сообщает, что не может вылечить файл, а через секунду пишет, что файл успешно удален.

Как найти компьютеры с необезвреженными угрозами

Не обязательно самостоятельно изучать отчеты и события, чтобы понять, что есть зараженные компьютеры.

Как правило, если Kaspersky Endpoint Security не смог обезвредить вредоносный файл, он сообщит об этом серверу статусом *Есть активные угрозы*. Этот статус включен по умолчанию, и отображается на веб-виджете **Типы обнаруженных вирусов и результаты лечения** дает компьютерам общий статус *Предупреждение,* и отображается на вкладке **Панель мониторинга.**

Статус присваивается компьютерам, на которых были обнаружены и не были обезврежены вредоносные программы.



В категорию **Активные угрозы** могут попадать очень разные по опасности объекты. Это может быть и находящийся в памяти вирус, который активно сопротивляется попыткам его удалить. А может быть, зараженный объект находится на сетевом диске, где у Kaspersky Endpoint Security нет прав записи, чтобы вылечить или удалить файл.

На серверах с общими папками бывает так, что, когда пользователь обращается к вредоносному файлу в папке, защитное решение на сервере блокирует доступ и впоследствии удаляет файл. Но защитное решение на компьютере пользователя успевает обнаружить угрозу, но не может удалить файл из папки, и сообщает, что есть необработанная угроза, хотя она и была обработана на сервере. Это все равно повод обратить внимание, потому что вредоносных файлов в общих папках быть не должно, и нужно выяснить, как он туда попал.

Чтобы вернуть статус компьютера в нормальное состояние, нужно обезвредить найденные объекты. Если обезвредить объект нельзя, как в описанной ситуации с вредоносной программой в общей папке, удалите запись о необработанном объекте из списка необработанных объектов:

1. Откройте в Веб-консоли администрирования раздел **Операции | Хранилища | Активные угрозы**

2. Найдите файл в сетевой папке и примените к нему команду Удалить

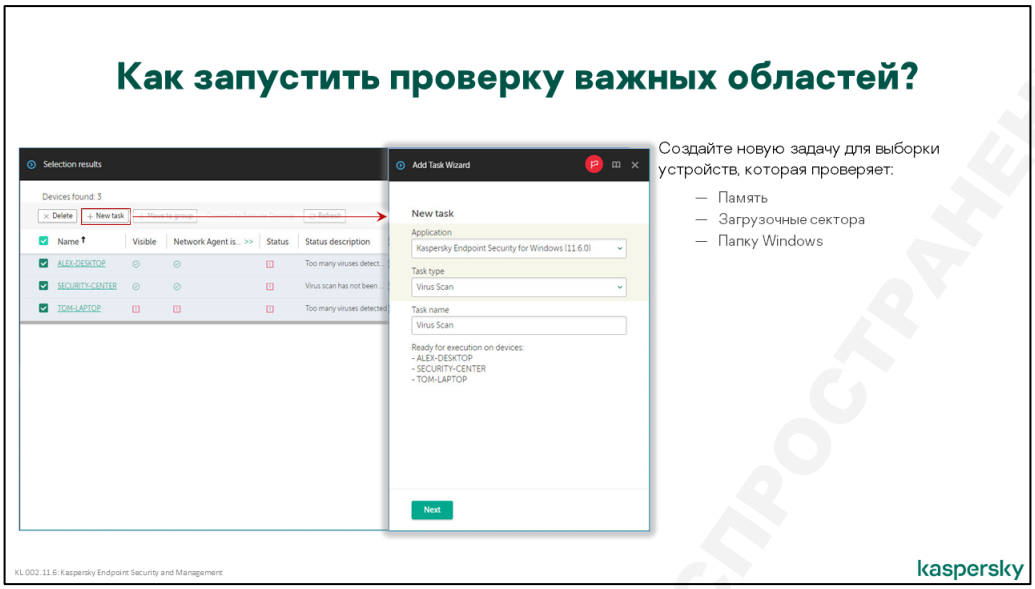
Как запустить проверку важных областей

Если на компьютере было найдено много вирусов, или обнаружена ранее открытая вредоносная ссылка, или был завершен вредоносный процесс, это значит, что компьютер все еще может быть заражен. Чтобы проверить, нет ли на компьютере известных угроз, запустите на нем проверку критических областей.

Это можно сделать по-разному. Один способ, доступный всегда, выглядит так:

1. Откройте свойства компьютера
2. Перейдите на вкладку **Задачи**
3. Найдите задачу **Проверка важных областей** и запустите ее

Проверка важных областей — это локальная задача, которая есть в каждой установке Kaspersky Endpoint Security. Локальная, значит, что ее видно только в свойствах компьютера, но не видно в группах и в узле Задачи. Из-за этого пользоваться ей неудобно. Чтобы запустить ее на нескольких компьютерах, нужно по очереди заходить в свойства каждого компьютера.



Можно использовать групповую задачу **Поиск вирусов**, ее придется создать самостоятельно. Но она запустит проверку на всех компьютерах, а зачем замедлять компьютеры, на которых нет угроз?

Чтобы быстро запускать проверку важных областей на тех компьютерах, где есть угрозы, сделайте задачу поиска вирусов для наборов компьютеров или соответствующей выборки компьютеров.

Как изолировать компьютер и лечить активное заражение

Как правило, даже если вредоносная программа выполняется, Kaspersky Endpoint Security может ее завершить. За это отвечают компоненты Предотвращение вторжений, Анализ поведения и Защита от эксплойтов. Защита от файловых угроз программы в памяти не проверяет.

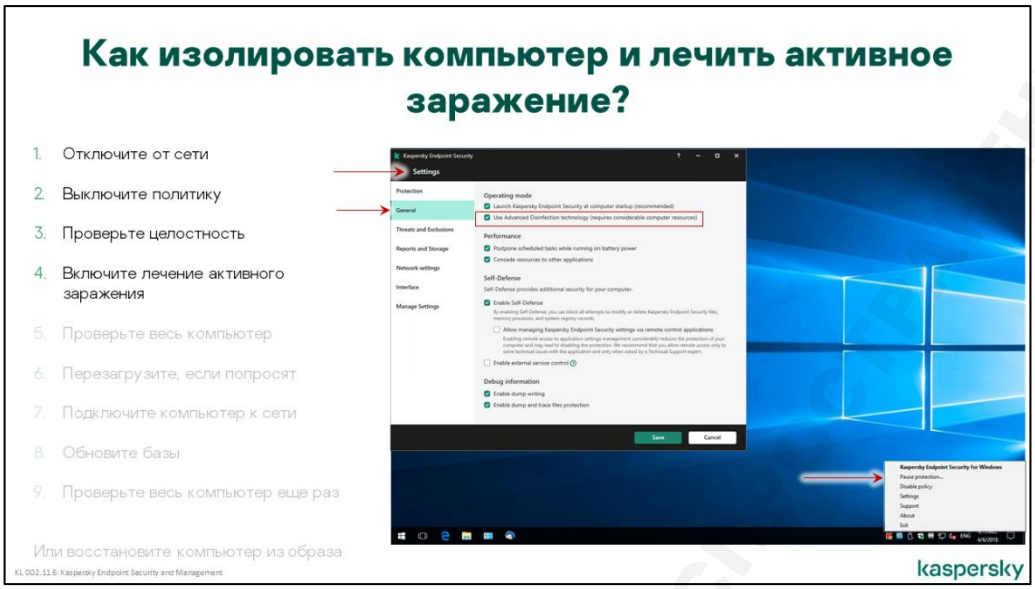
Но если компьютер заражен и Kaspersky Endpoint Security не может остановить вредоносную программу, примените технологию лечения активного заражения.

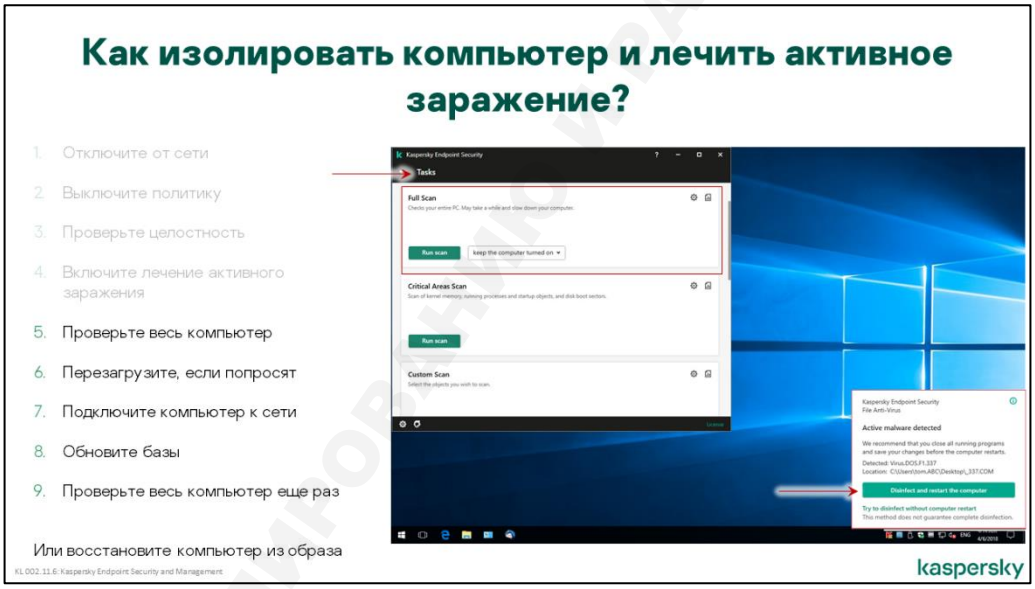
По умолчанию эта технология выключена, так как она блокирует запуск любых программ и перезагружает компьютер, что помешает пользователю компьютера. Пользователь может согласиться выполнить процедуру и рискует потерять данные, или пользователь может отказаться выполнить процедуру и компьютер останется зараженным. В любом случае лучше, если решать будет администратор, а не пользователь.

Если вы подозреваете, что компьютер заражен, лучше всего сразу переустановить его из образа. Если это неприемлемо или невозможно, попробуйте вылечить компьютер:

1. Отключите компьютер от корпоративной сети
2. Выйдите из политики командой *Выключение политики* в контекстном меню значка KES

Чтобы использовать эту команду, включите в политике Kaspersky Endpoint Security защиту паролем



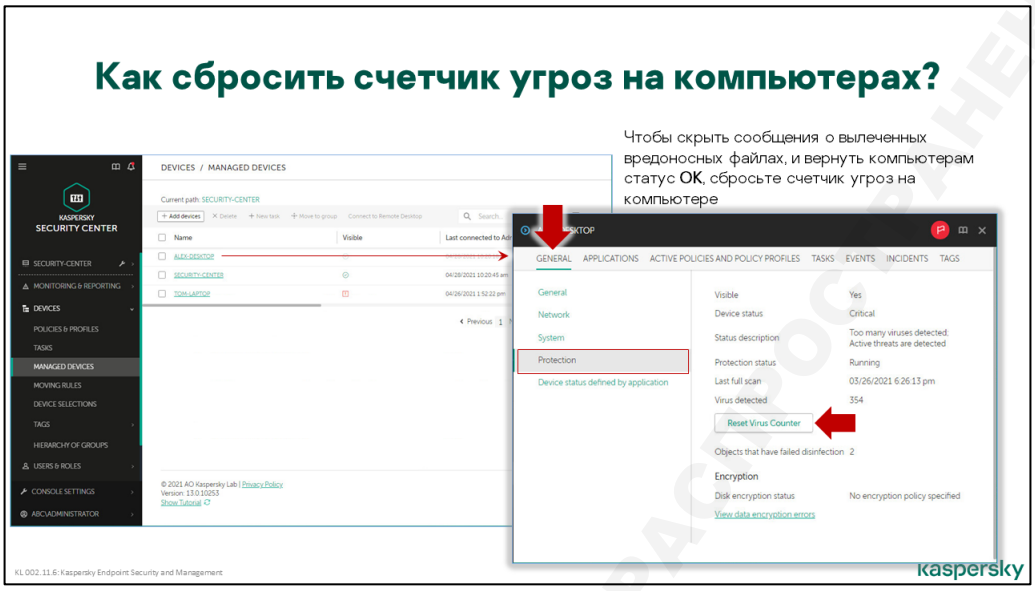


3. Откройте окно Kaspersky Endpoint Security и нажмите кнопку **Компоненты защиты**
4. Откройте раздел **Общие** и отметьте флаг *Применять технологию лечения активного заражения*
5. Запустите задачу **Поиск вирусов.** Для этого вернитесь к главному окну Kaspersky Endpoint Security, нажмите область **Задачи**
6. Если Kaspersky Endpoint Security найдет угрозу и попросит выполнить лечение активного заражения, соглашайтесь

> При лечении активного заражения Kaspersky Endpoint Security не дает запускаться новым программам, сканирует память, применяет более агрессивные методы завершения процессов, пробует удалить вредоносные файлы на перезагрузке

7. Перезагрузите компьютер, подключите его к Интернет и обновите сигнатуры
8. Проверьте весь компьютер еще раз

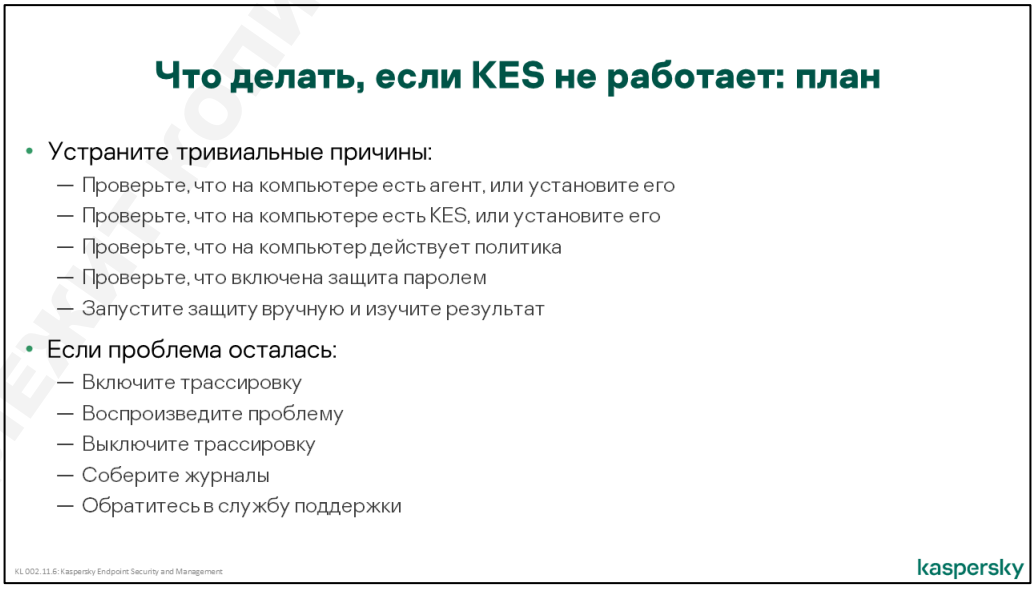
Как сбросить счетчик вирусов



В конце осмотра, когда все угрозы обезврежены, сбросьте счетчик вирусов на компьютерах.

Без внешнего вмешательства счетчик вирусов может только увеличиваться, единственный способ привести этот статус в нормальное состояние — сбросить значение счетчика вручную. Для этого откройте свойства компьютера, на вкладке **Общие** в разделе **Защита**, есть кнопка **Обнулить счетчик вирусов**.

3.2 Что делать, если Kaspersky Endpoint Security не работает

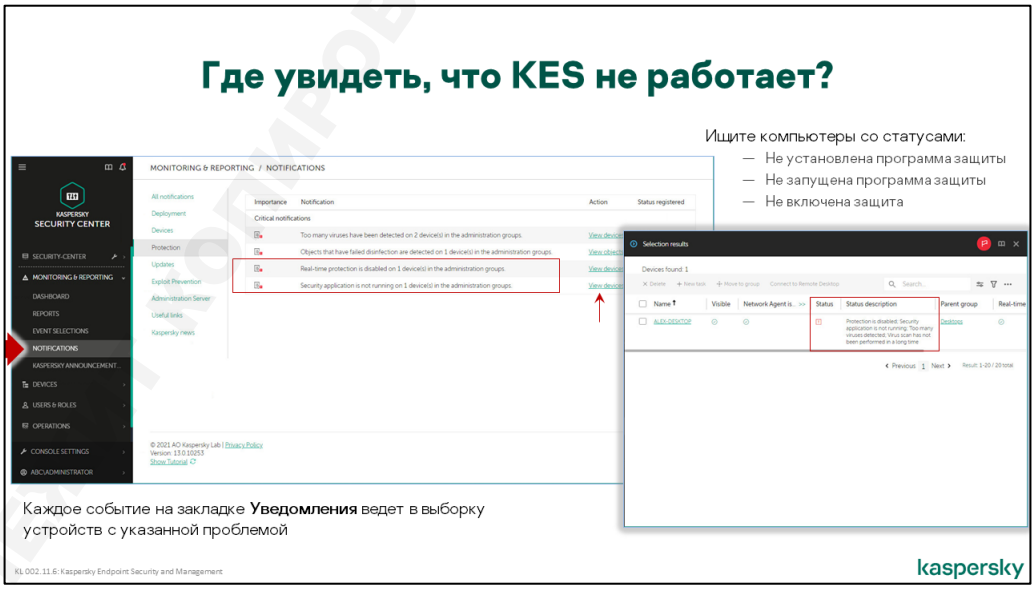


Если защита не работает, это может быть по очень разным причинам. Не торопитесь жаловаться в техническую поддержку. Сначала исключите тривиальные причины. Убедитесь, что:

На компьютере есть Агент администрирования	Пользователь мог удалить Агент администрирования и тогда Консоль показывает последние сведения, которые Агент отправил на Сервер. Установите Агент заново и защитите его от пользователя: задайте пароль на деинсталляцию
На компьютере есть Kaspersky Endpoint Security	Пользователь мог удалить Kaspersky Endpoint Security. Установите защиту заново и защитите ее от пользователя: задайте пароль
К компьютеру применяется политика	Компьютер может быть в группе без политики, или на компьютере может быть версия Kaspersky Endpoint Security, для которой на Сервере нет политики. Создайте политики во всех группах и для всех версий Kaspersky Endpoint Security
Настройки политики закрыты замком	Если замки не закрыты, пользователь может менять значения параметров и потенциально может выключить компоненты или автозапуск Kaspersky Endpoint Security. Закройте замки для всех важных параметров в политике
Включена защита паролем	Если защита паролем не включена, пользователь может выгрузить Kaspersky Endpoint Security, даже без прав администратора

После того, как вы исключили тривиальные причины, смотрите на ошибки. Если Kaspersky Endpoint Security не запускается из-за сбоев, соберите журналы диагностики и обратитесь в службу поддержки Лаборатории Касперского.

Где увидеть, что Kaspersky Endpoint Security не работает



О том, что защита не работает, могут говорить следующие статусы компьютера:

Не установлена программа защиты	По умолчанию включен для статусов **Предупреждение** и **Критический**
Уровень постоянной защиты отличается от установленного администратором	По умолчанию выключен. Установить можно одно из значений: — Запускается — Выполняется (максимальная скорость) — Выполняется — Остановлена — Выполняется (рекомендуемые параметры) — Выполняется (с пользовательскими параметрами) — Приостановлена — Не удалось запустить — Выполняется
Не включена защита	По умолчанию включен для статуса **Критический**
Не запущена программа защиты	По умолчанию включен для статуса **Критический**

Статус *Уровень постоянной защиты отличается от установленного администратором*, хотя и выключен по умолчанию, полезнее статуса *Не включена защита*. Статус *Не включена защита* не показывает, почему она не включена: из-за сбоя или потому, что ее выключил пользователь. Статус *Уровень постоянной защиты отличается от установленного администратором* эту разницу показывает.

Поэтому включите условие *Уровень постоянной защиты отличается от установленного администратором* для общего статуса **Критический** и выберите для него значение *Выполняется*.

Для статусов *Не включена защита* и *Не установлена программа защиты* есть стандартные выборки компьютеров. Для остальных статусов администратор может создать свои выборки.

Статус *Не запущена программа защиты* всегда сопровождается статусом *Не включена защита*. Но не наоборот. Если Kaspersky Endpoint Security работает, но все компоненты защиты выключены, у компьютера будет статус *Не включена защита* без статуса *Не запущена программа защиты*.

Защита в Kaspersky Endpoint Security считается включенной, если работает хотя бы один компонент защиты. Даже если это только Защита от почтовых угроз

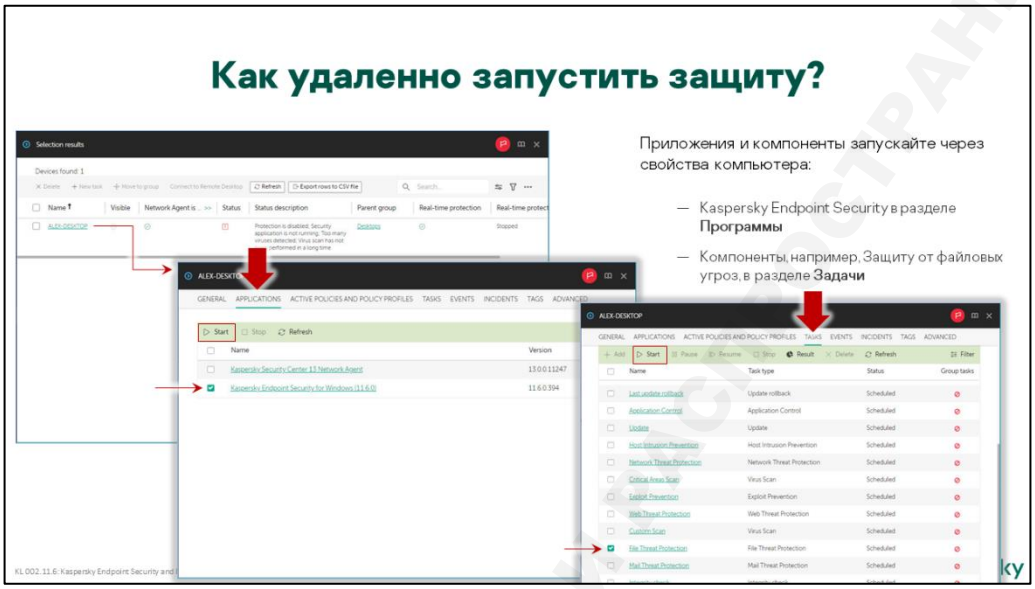
Чтобы заметить, что на компьютере из-за сбоя не запустились компоненты, смотрите в отчет об ошибках или в выборку событий. Чтобы увидеть все ошибки:

1. Откройте узел **Выборки событий** в разделе Мониторинг и отчеты
2. Перейдите по ссылке с именем выборки *Отказы функционирования*

Чтобы понять, какие компоненты работают на компьютере, откройте вкладку **Задачи** в свойствах компьютера. Компоненты перечислены среди прочих задачи и в списке видно, какие выполняются, а какие нет.

Как удаленно запустить защиту

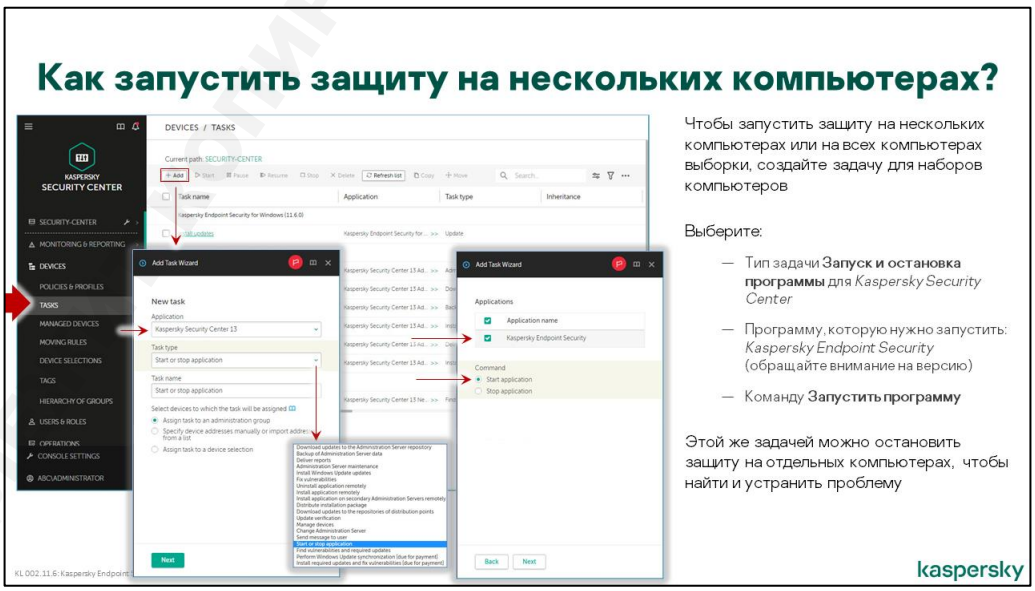
Как запустить защиту на одном компьютере



Одним из наиболее критичных статусов защиты является статус **Защита выключена**. Чтобы исправить этот статус нужно отдать команду Агенту администрирования, чтобы агент запустил Kaspersky Endpoint Security. Отдать такую команду можно в свойствах компьютера на вкладке **Программы**.

Если не запущены отдельные компоненты, их можно запустить на вкладке **Задачи**.

Как запустить защиту на нескольких компьютерах



Второй способ запустить Kaspersky Endpoint Security — с помощью задачи **Запуск и остановка программы**. Эта задача относится к дополнительным задачам Kaspersky Security Center и может быть как групповой, так и для наборов компьютеров.

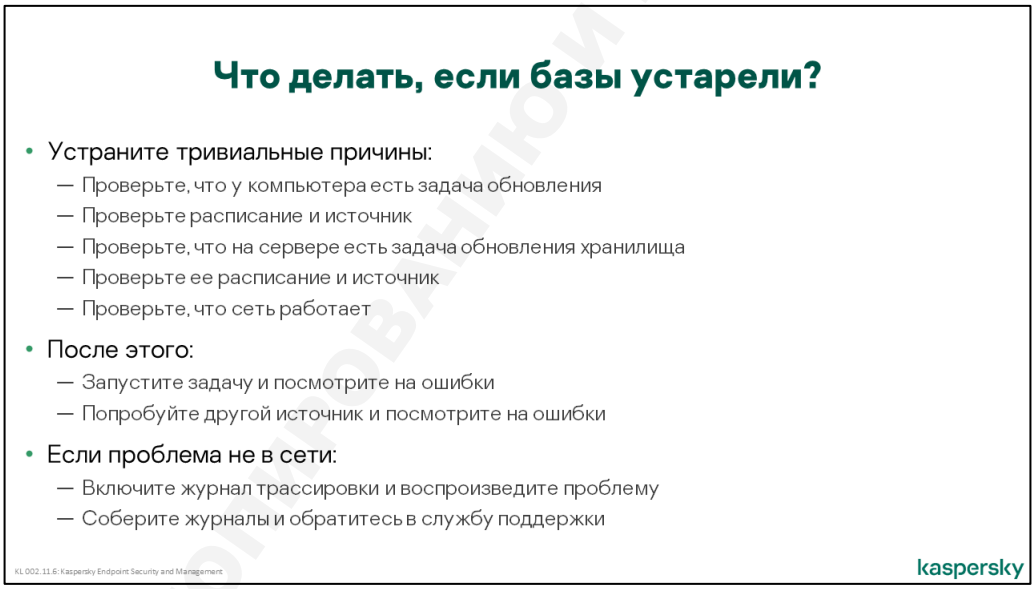
Групповую задачу удобно использовать при регистрации события **Вирусная атака** — с ее помощью можно запустить защиту на всех компьютерах сети, на случай если защита где-нибудь остановлена.

Задача для наборов компьютеров лучше подходит для исправления статуса *Защита выключена*.

Чтобы создать задачу, которая запускает Kaspersky Endpoint Security:

1. Запустите мастер создания задачи в разделе **Устройства | Задачи**
2. Выберите программу *Kaspersky Security Center* и тип задачи *Запуск и остановка программы*
3. Выберите устройства, которым будет назначена задача – *выборка*
4. Укажите выборку компьютеров *Protection is disabled*
5. Выберите версии Kaspersky Endpoint Security, которые надо запустить и команду **Запустить программу**

3.3 Что делать, если базы устарели



Если защита не работает, это совсем плохо. Но и если она работает со старыми сигнатурами, это не намного лучше. Обращайте внимание на компьютеры со старыми сигнатурами, обновляйте их и заодно выясняйте, почему на них оказались старые сигнатуры.

Сначала устраните тривиальные причины. Проверьте:

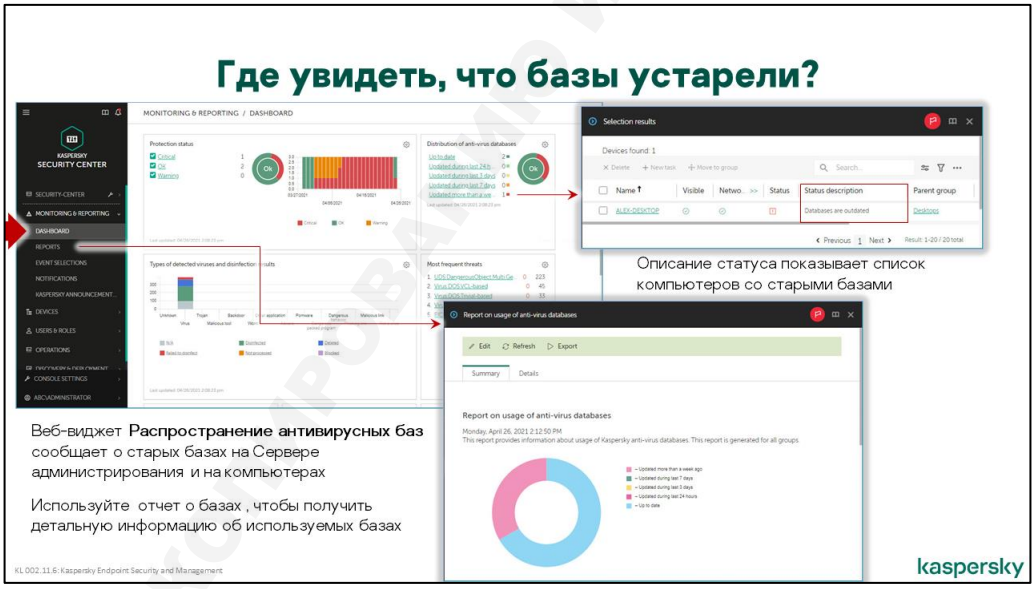
У компьютеров есть задача обновления	По умолчанию такая задача есть. Но со временем, когда групп и задач станет много, может оказаться, что у части компьютеров нет задачи обновления для нужной версии Kaspersky Endpoint Security
Расписание задачи	Если администратор создавал задачи обновления вручную, он мог ошибиться и не выбрать расписание
Источник задачи	Источником внутри сети должен быть Kaspersky Security Center

У сервера администрирования есть задача загрузки обновлений в хранилище	По умолчанию такая задача есть, но кто-то мог ее по ошибке удалить
Расписание и источник задачи загрузки обновлений в хранилище	По умолчанию такая задача есть, но кто-то мог ее по ошибке удалить или расписание задано неверно
У Сервера администрирования есть доступ в Интернет или к выбранному источнику	Возможно, для доступа в Интернет требуется использовать прокси-сервер, но адрес и логин/пароль для аутентификации на прокси-сервере не заданы или их нужно обновить

После этого смотрите на ошибки задач обновления. Если ошибки вызваны сбоями в Kaspersky Endpoint Security, соберите журналы и обратитесь в техническую поддержку.

Отдельно подумайте, нужны ли вам Точки распространений. В небольшой сети они не приносят много пользы, но усложняют диагностику. По умолчанию Сервер администрирования автоматически назначает Точки распространений. Вы можете это отключить.

Где увидеть, что базы устарели



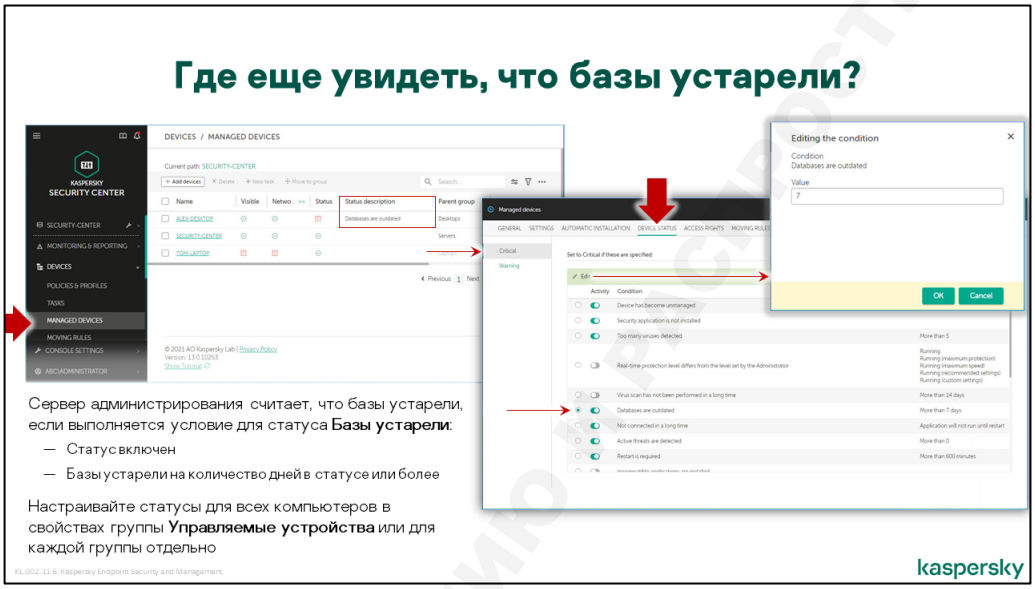
Информация об используемых базах доступна администратору в веб-виджете **Распространение антивирусных баз** в разделе **Панель мониторинга.** Если все нормально, в веб-виджете будет показана зеленая круговая диаграмма и время последней загрузки новых баз в серверное хранилище. Если есть проблема, часть круговой диаграммы поменяет цвет на желтый или красный и увеличится счетчик рядом с соответствующим статусом баз.

Статусы баз в веб-виджете представлены ссылками, которые открывают выборки устройств:

- Устройства с актуальными базами
- Устройства с базами, которые обновлены в последние 24 часа
- Устройства с базами, которые обновлены в последние 3 дня
- Устройства с базами, которые обновлены в последние 7 дней
- Устройства с базами, которые не обновлялись более 7 дней

Более подробную информацию об используемых базах и проблемных компьютерах администратор может в отчетах. Отчет об используемых базах показывает у какого количества компьютеров базы устарели на одни сутки, трое суток, семь суток и более 7 суток.

Если базы на компьютере устарели не потому, что он был выключен, а из-за постоянных сбоев задачи обновления, для выяснения подробностей администратору потребуются события задачи обновления. Событий, поступающих на Сервер администрирования, часто недостаточно для полноценной оценки ситуации. В локальном отчете обновления Kaspersky Endpoint Security, как правило, содержится больше событий.

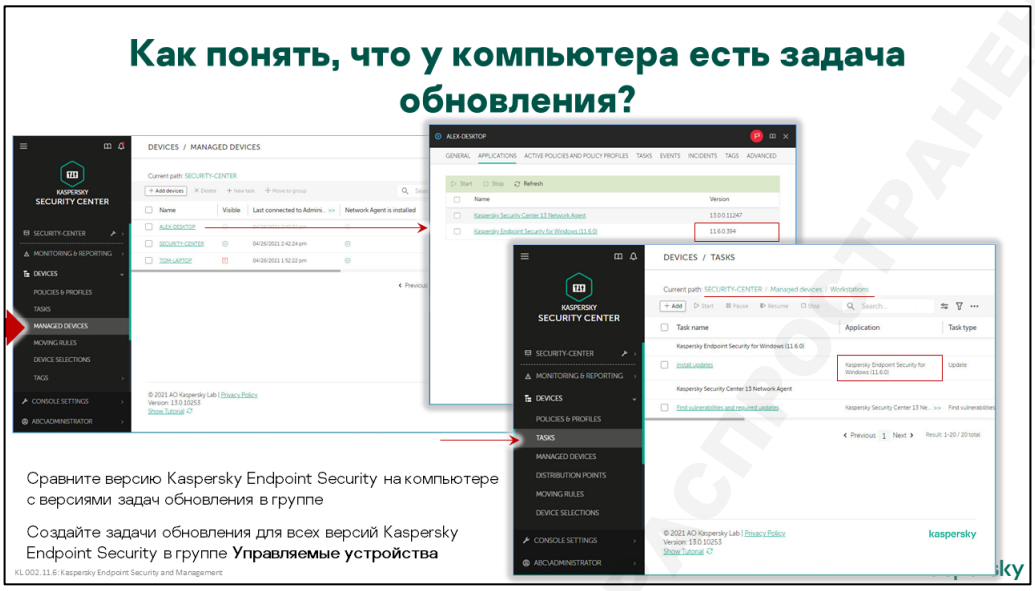


О старых базах сигнатур сообщают статусы компьютеров.

Компьютеры со старыми базами получают статус **Предупреждение** или **Критический**, в зависимости от того, насколько старые базы на них установлены. Критерии присвоения статусов настраиваются в свойствах групп. По умолчанию для статуса **Предупреждение** базы должны устареть на 7 дней, а для статуса **Критический** — на 14 дней.

Понять, что статус компьютера отличается от **OK** именно из-за старых баз, можно по описанию статуса в свойствах компьютера в разделе **Защита**, или на вкладке **Управляемые устройства** в графе **Описание статуса**. Более подробная информация о сигнатурах и, в частности, дата последнего обновления доступны через свойства программы Kaspersky Endpoint Security, которая в свою очередь доступна на вкладке **Программы** в свойствах компьютера.

Как узнать, есть ли у компьютера задача обновления



Раздача обновлений из серверного хранилища клиентским компьютерам осуществляется групповыми задачами обновления.

Чтобы гарантированно охватить все управляемые компьютеры, задача обновления должна быть групповой и относиться к группе **Управляемые устройства**. Именно такую задачу создает мастер первоначальной настройки — **Установка обновлений**. Если компьютеры организованы в группы и оптимальный порядок обновления в разных группах отличается, можно создать свои задачи обновления в каждой группе.

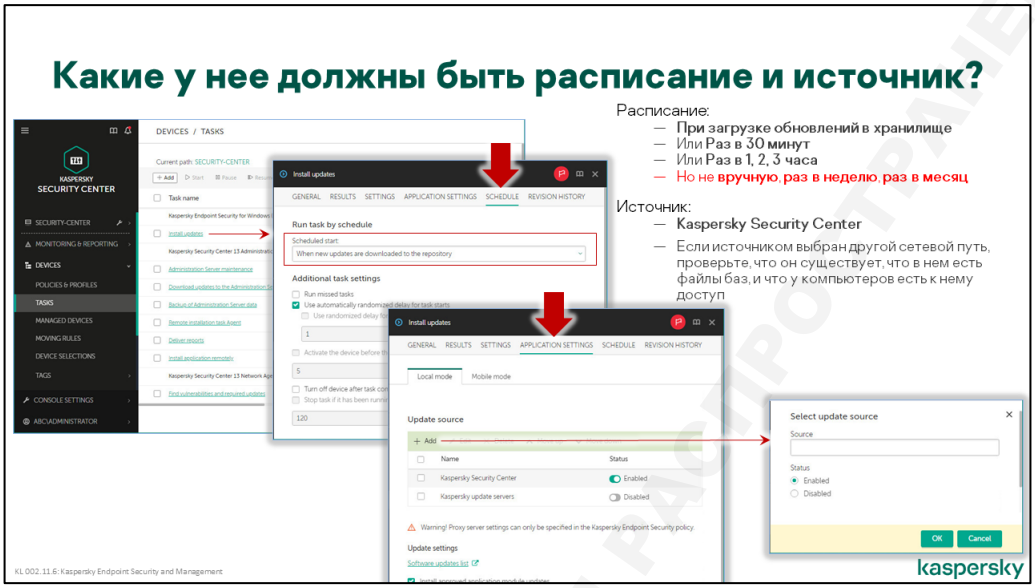
Если однотипные задачи имеются в родительской и дочерней группе, на компьютерах дочерней группы будут запускаться обе задачи. Это, скорее всего, приведет к ошибкам, т.к. если Kaspersky Endpoint Security выполняет задачу обновления, он не может запустить еще одну. Чтобы этого избежать, в родительской группе задачу можно удалить, перевести в ручной режим запуска или исключить из нее подгруппы, где есть своя задача обновлений.

Примечание: если на управляемых компьютерах используются другие или более ранние версии Kaspersky Endpoint Security, например, Kaspersky Endpoint Security для Mac или Kaspersky Security для Windows Servers, для них нужны будут отдельные задачи обновления

Если в Веб-консоли много групп, а на компьютерах есть разные версии Kaspersky Endpoint Security, с первого взгляда тяжело оценить, у всех ли компьютеров есть задача обновления. Если на компьютере старые сигнатуры, чтобы понять, есть ли у него задача обновления:

1. Откройте свойства компьютера и перейдите на вкладку Программы
2. Запомните полное название Kaspersky Endpoint Security с версией Service Pack
3. Перейдите в группу компьютера
4. Откройте вкладку **Задачи**
5. Ищите задачу с типом **Обновление** и версией Kaspersky Endpoint Security такой, как в свойствах компьютера

Если такой задачи нет, создайте ее в этой группе или одной из вышестоящих групп. Старайтесь использовать поменьше задач. Часто достаточно одной задачи обновления для каждой версии Kaspersky Endpoint Security в корневой группе **Управляемые устройства**.



Расписание

Задачи обновления клиентских компьютеров характеризуются расписанием, и параметрами обновления, которые включают:

- Список источников обновления
- Параметры обновлений
- Параметры копирования обновлений во внешнюю папку
- Список подгрупп, на компьютерах которых задача выполняться не будет

Стандартное расписание задач обновления Kaspersky Endpoint Security — **При загрузке обновлений в хранилище**. В отличие от периодического расписания, когда время запуска определяет Kaspersky Endpoint Security и запускает задачу независимо от того, есть связь с Сервером администрирования или нет, расписание **При загрузке обновлений в хранилище** означает, что задача всегда запускается по команде от Сервера администрирования.

Чтобы отправить команду запуска, Сервер администрирования посылает сигнал на клиентский компьютер на UDP-порт 15000. Этот порт слушает Агент администрирования и, получив на него сигнал, связывается с Сервером администрирования. В результате соединения с Сервером Агент получает команду запуска задачи и передает ее на выполнение Kaspersky Endpoint Security. Если сигнал Сервера до клиентского компьютера не дошел, Агент получит команду запуска задачи при следующей плановой синхронизации (по умолчанию раз в 15 минут). То же самое происходит, когда администратор пытается вручную запустить задачу через Консоль администрирования.

Расписание **При загрузке обновлений в хранилище** гарантирует, что клиентские компьютеры будут получать обновления своевременно и без ненужных обращений к Серверу. Альтернативно можно использовать простое периодическое расписание запуска — например, раз в час.

Чтобы клиентские компьютеры в момент запуска задачи не создавали большой пиковой нагрузки на источник обновлений и на сеть, используется случайный разброс времени запуска в некотором интервале. Скажем, если выбран интервал 5 минут, компьютер начнет обновление не ровно в назначенное время, а после случайной задержки от 0 до 5 минут.

По умолчанию Сервер администрирования автоматически определяет интервал разброса в зависимости от количества компьютеров в задаче. Администратор может отключить опцию

Автоматически определять период задержки запуска задачи в параметрах расписания и установить период на свое усмотрение.

Если на компьютерах старые версии сигнатур, проверьте расписание в задаче обновления. Если расписание *Вручную*, *Раз в неделю* или *Раз в месяц*, измените его на *При загрузке обновлений в хранилище* или *Раз в N часов*

Источник

Чтобы задать список источников нужно открыть свойства задачи и перейти на вкладку **Параметры программы | Локальный режим** . Источниками обновления могут выступать:

- **Kaspersky Security Center** — рекомендуемый источник для всех управляемых компьютеров. Более того, наиболее естественный источник для расписания **При загрузке обновлений в хранилище**
- **Серверы обновления «Лаборатории Касперского»** — рекомендуемый источник для компьютеров за пределами корпоративной сети или резервный источник, когда Сервер администрирования недоступен. Впрочем, нередко администраторы предпочитают, чтобы компьютеры ждали возобновления связи с Сервером администрирования, а не создавали лишний внешний трафик
- **Локальная или сетевая папка** — еще один вариант настройки резервных источников обновлений. В качестве сетевой папки можно указать HTTP- или FTP-адрес. Например, если в сети несколько Серверов администрирования (что является темой курса KL 302), можно в качестве резервных источников использовать HTTP-адреса папок с обновлениями на других Серверах

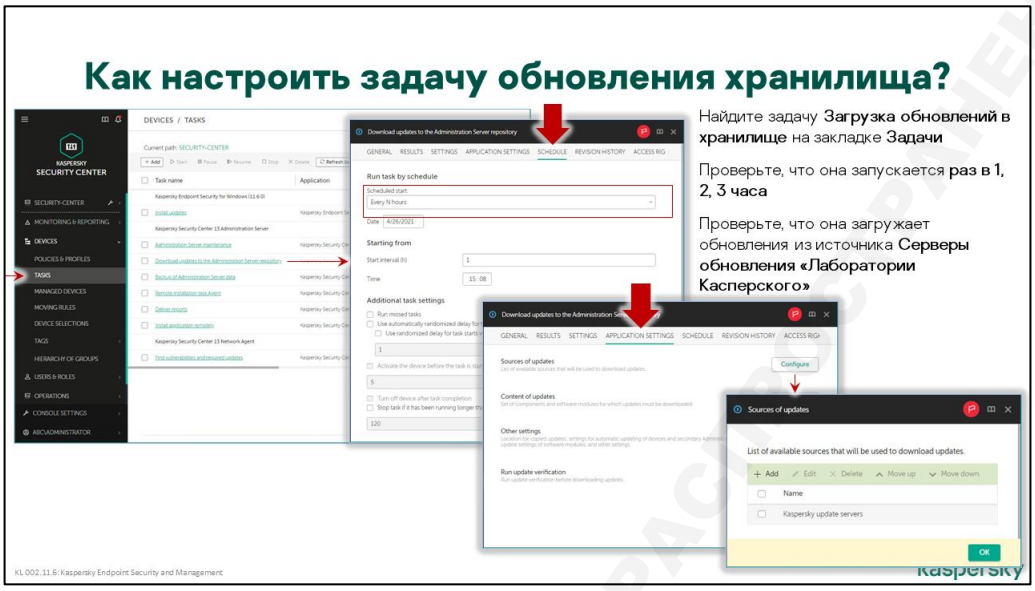
Задаче обновления клиентских компьютеров можно назначить не один, а несколько источников. Если первый источник окажется недоступен, задача попробует обновиться из следующего по списку.

Загрузка обновлений с Сервера администрирования осуществляется Агентами администрирования. Загрузка обновлений с серверов обновлений Лаборатории Касперского или с других FTP- или HTTP-серверов осуществляется самой программой Kaspersky Endpoint Security без помощи агента.

Если на компьютерах старые версии сигнатур, проверьте источник в задаче обновления. Установите источник Kaspersky Security Center. Если вы хотите использовать папку или FTP-сервер, проверьте, что по этому адресу есть обновления, и что у компьютеров есть доступ к файлам

В задаче обновления можно включить копирование обновлений в отдельную папку. Этот режим может использоваться для создания источника обновлений в малых сетях или подсетях без Сервера администрирования. В больших сетях для создания промежуточных источников обновления используются Точки распространения. Сервер администрирования автоматически назначает Агент обновлений (подробнее см. в курсе 302 Масштабирование).

Как узнать, есть ли Сервера задача обновления



Задача обновления серверного хранилища так и называется — **Загрузка обновлений в хранилище**. Она создается автоматически мастером первоначальной настройки и существует в единственном экземпляре. В консоли она находится в разделе **Устройства | Задачи** группы “Имя сервера администрирования”.

Если у компьютеров старые базы, проверьте, есть ли у Сервера администрирования задача обновления. Перейдите в раздел **Устройства | Задачи** сервера администрирования и ищите задачу с типом *Загрузка обновлений в хранилище*

Задача такого типа может быть только одна. Если она уже есть, мастер создания задачи не позволяет создать еще одну. Однако в порядке диагностики проблем можно удалить созданную автоматически задачу **Загрузка обновлений в хранилище** и создать новую.

К настройкам этой задачи относятся расписание, источник обновления, параметры подключения к источнику, состав загружаемых обновлений и ряд дополнительных параметров.

Поскольку задача существует в единственном экземпляре, единственным разумным расписанием для нее является периодическое, с небольшим интервалом от 15—20 минут до нескольких часов. Исходное значение интервала — 1 час.

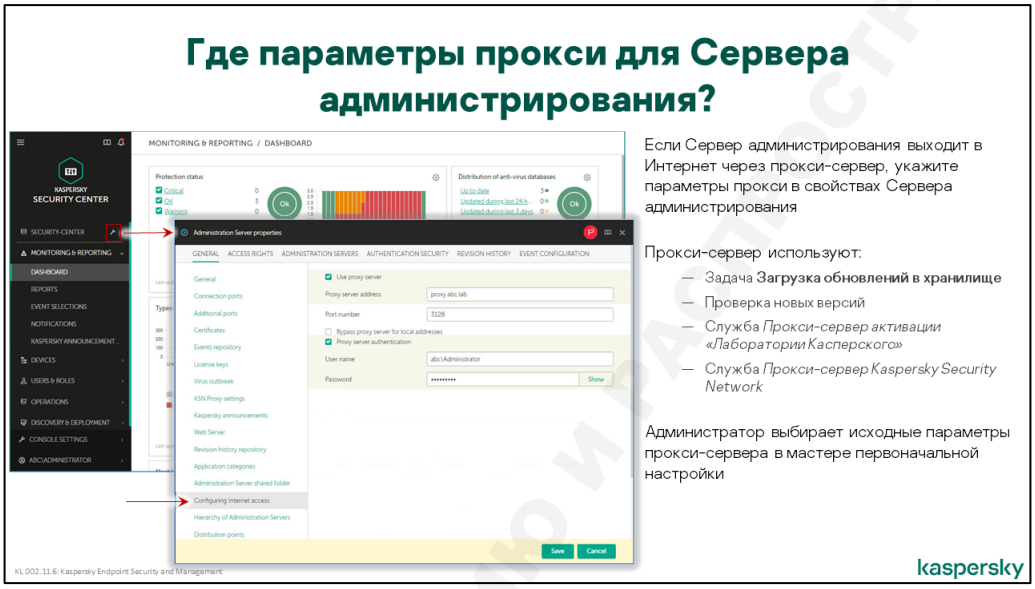
Источник обновлений может быть одного из трех типов:

- **Серверы обновлений «Лаборатории Касперского»** — список FTP- и HTTP-серверов, официально поддерживаемых Лабораторией Касперского. Такие Сервера расположены в разных странах по всему миру, что обеспечивает высокую надежность обновления. Если задача не может подключиться к одному серверу, она пробует следующий по списку. Список серверов загружается вместе с другими обновлениями
- **Главный Сервер администрирования** — используется, если есть несколько серверов Kaspersky Security Center, и они объединены в иерархию (рассматривается в курсе KL 302. Kaspersky Endpoint Security and Management. Масштабирование)
- **Локальная или сетевая папка** — используется для обновления из источников, созданных администратором. В качестве сетевой папки можно указать, в том числе, FTP- или HTTP-адрес

Задаче загрузки обновлений в хранилище можно назначить не один, а несколько источников. Если первый источник окажется недоступен[2], задача попробует обновиться из следующего по списку.

Где задать параметры прокси-сервера

Где задать параметры прокси-сервера для Сервера администрирования



Для доступа к источнику обновлений Серверу администрирования может потребоваться указать параметры прокси-сервера. Эти параметры общие для всех источников. Если для каких-то источников прокси-сервер не нужен, это можно отметить в их свойствах, выключив опцию **Использовать прокси-сервер**.

По умолчанию прокси-сервер не задан. Параметры прокси-сервера спрашивает мастер первоначально настройки. Позже, чтобы использовать прокси-сервер:

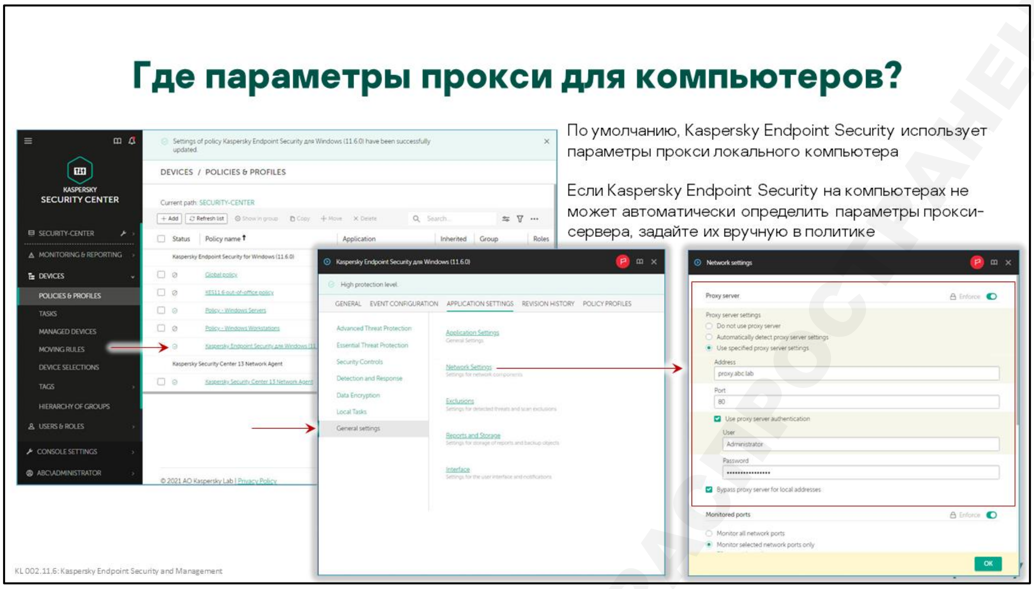
1. В свойствах Сервера администрирования откройте вкладку **Общие** раздел **Параметры доступа к сети Интернет**

2. Задайте адрес прокси-сервера, порт и параметры аутентификации: имя и пароль пользователя

Эти настройки будут использоваться как при получении обновлений, так и, в частности, для обращений к серверам KSN.

[2] Источник **Серверы обновлений Лаборатории Касперского** считается недоступным, если недоступны все известные сервера

Где задать параметры прокси-сервера для компьютеров



Если в задаче обновления компьютеров выбран адрес FTP- или HTTP-сервера и для доступа к нему нужен прокси-сервер, задайте параметры прокси-сервера в политике Kaspersky Endpoint Security. Откройте свойства политики на вкладке **Параметры программы** выберите раздел **Общие параметры** и перейдите по ссылке *Параметры сети*.

По умолчанию используется автоматически определяемый прокси-сервер. Это значит, что Kaspersky Endpoint Security возьмет настройки прокси-сервера из настроек Интернет в панели управления Windows. Администратор может явно указать адрес, порт и учетную запись для аутентификации.

Как не назначать Точки распространения автоматически

Точки распространения — это дополнительные источники обновлений в сети. Точкой распространения может быть любой компьютер с Агентом администрирования. Какие компьютеры являются Точками распространения, Сервер администрирования выбирает автоматически. Администратор может выключить автоматическое назначение и назначить Точки распространения вручную.

Автоматически выбранные Точки распространения рассылают файлы обновлений с помощью многоадресных рассылок (multicast) и это нельзя отключить. Администраторы сети часто не любят, когда в сети есть трафик, который они не контролируют. К тому же в небольшой сети на несколько сотен машин один Сервер администрирования вполне справляется с обновлениями и сам без дополнительных Точек распространения.

Чтобы выключить автоматическое назначение Точек распространения:

1. Откройте раздел **Точки распространения** в свойствах Сервера администрирования
2. Выберите **Вручную назначать точки распространения**

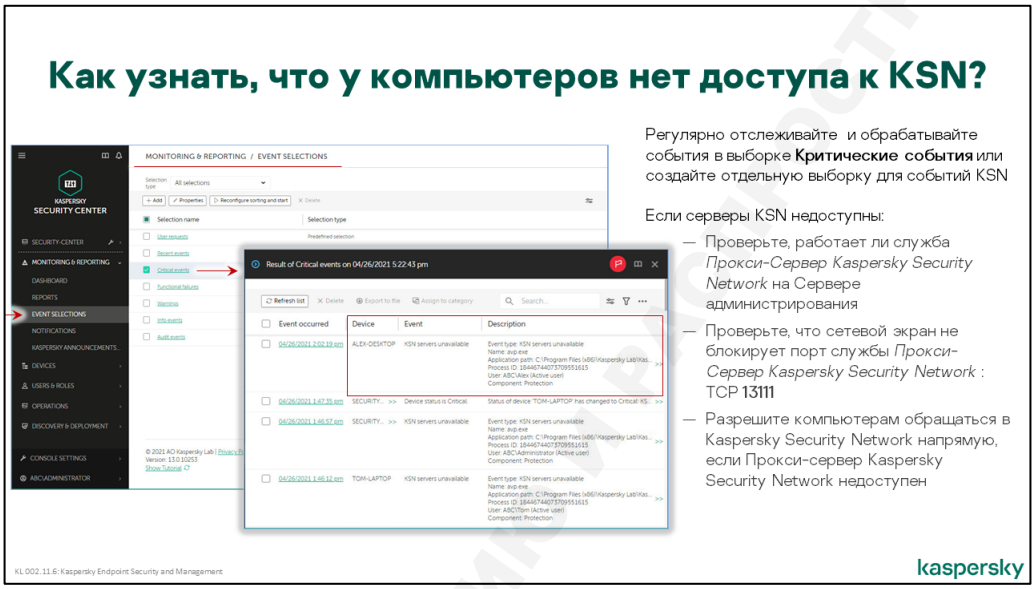
Когда выбран параметр **Вручную назначать точки распространения**, администратор может сам выбрать компьютеры, которые будут Точками распространения.

Подробнее о том, как работают Точки распространения, рассказывает курс KL 302. Масштабирование.

Как проверить, используется ли KSN

Kaspersky Security Network сообщает о новых вредоносных файлах быстрее, чем задачи обновления. Если у компьютеров нет доступа к KSN, у злоумышленников выше шансы их заразить.

Как узнать, что у компьютеров нет доступа к KSN



Если у Kaspersky Endpoint Security нет доступа к KSN, он сообщает об этом на Сервер администрирования событием *Серверы KSN недоступны*. Чтобы быстро находить все компьютеры, на которых нет доступа к KSN, создайте свою выборку компьютеров.

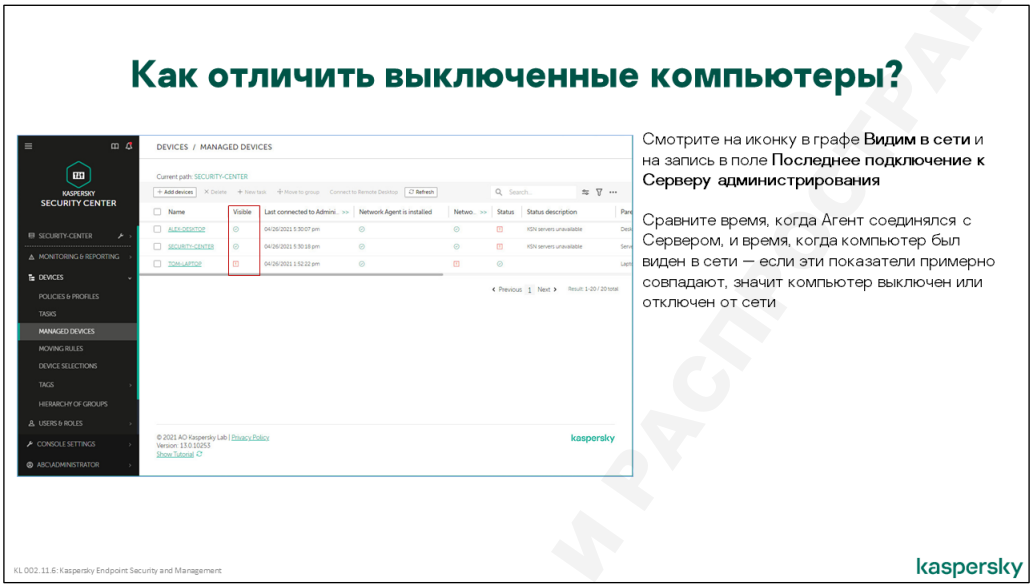
По умолчанию Kaspersky Endpoint Security обращаются в KSN через службу Сервера администрирования: *Прокси-сервер Kaspersky Security Network*. Служба принимает соединения на TCP-порт 13111. Если у компьютеров нет доступа к KSN, убедитесь, что:

— Запущена служба *Прокси-сервер Kaspersky Security Network* на Сервере администрирования

— Порт 13111 не закрыт сетевым экраном

3.4 Как проверить связь компьютера с Сервером

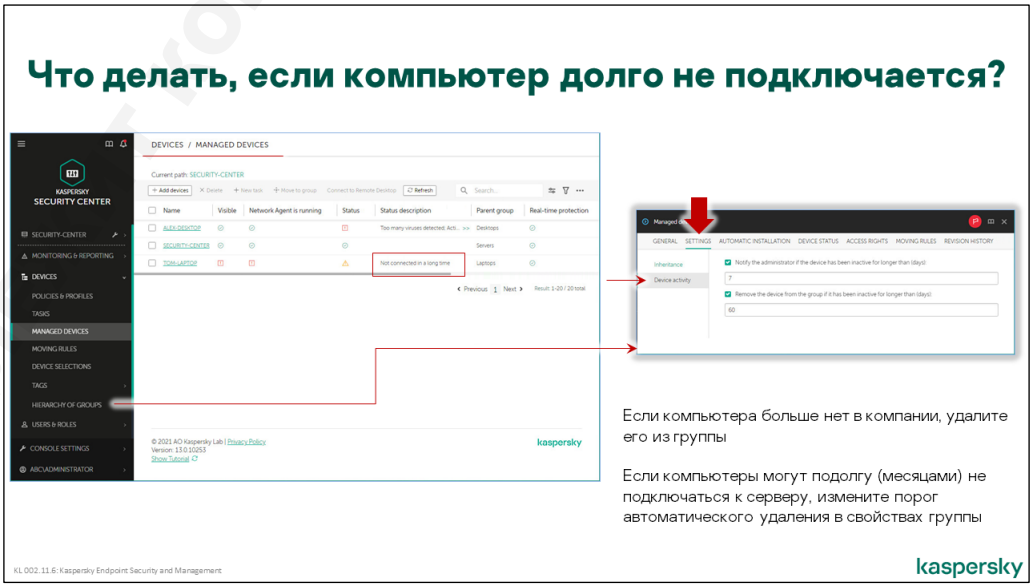
Как отличить выключенные компьютеры

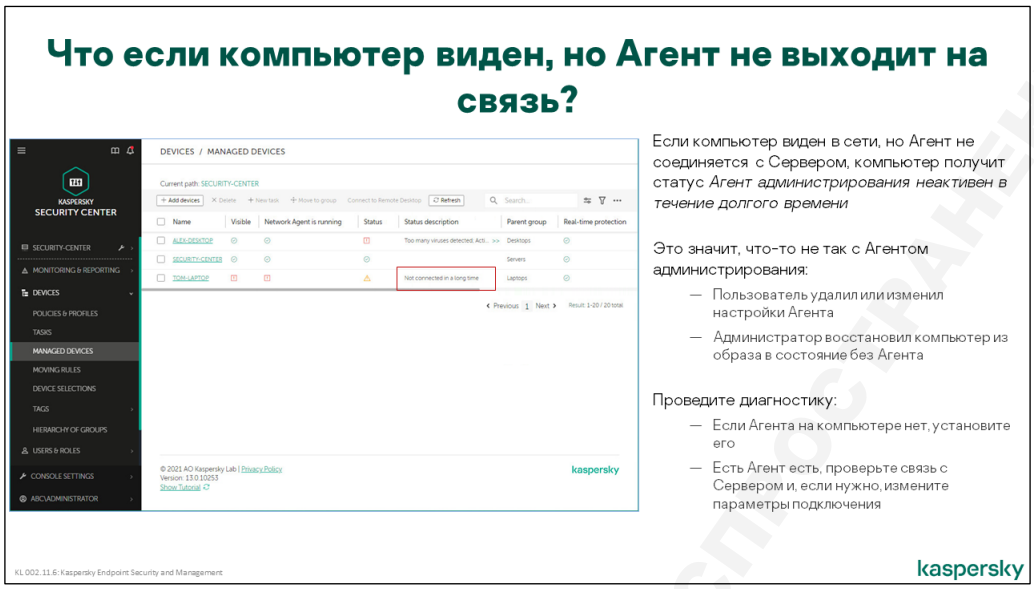


В большой сети все компьютеры почти никогда не бывают включены. Какие-то обязательно выключены.

В консоли их легко отличить по значку: у выключенных компьютеров в графе **Видим в сети** появится значок красного треугольника с восклицательным знаком. Смотрите также на статусы и записи в графах *Агент администрирования установлен, Агент администрирования запущен* и *Последнее подключение к Серверу администрирования*. Если Агент не работает, а последнее соединение было давно, не обращайте внимания на статусы защиты компьютера, они может быть неточным.

Что делать, если компьютер долго не подключается





Если компьютер остается выключенным слишком долго, Сервер администрирования назначает ему один из двух статусов:

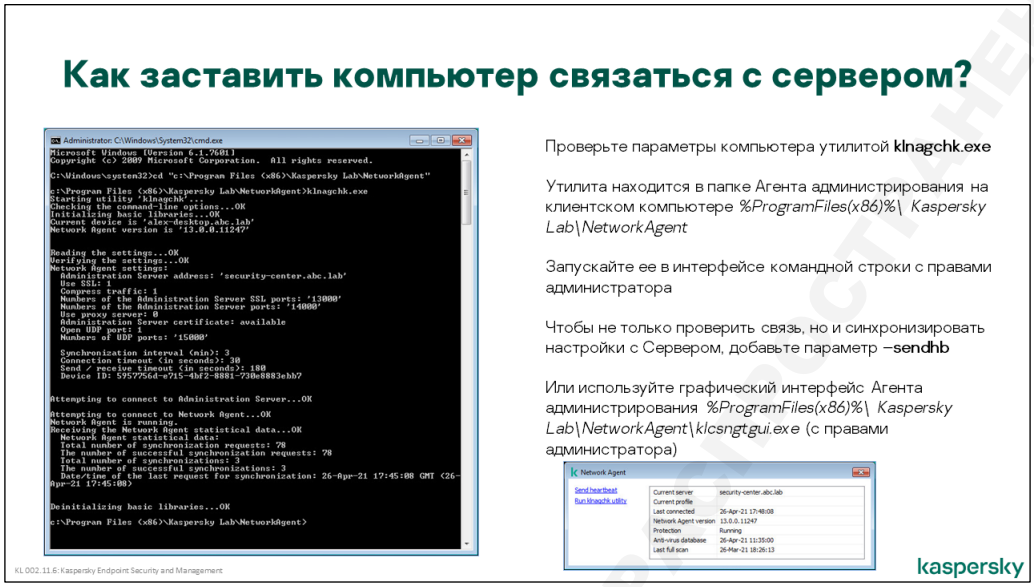
Агент администрирования неактивен в течение долгого времени	По умолчанию компьютеры получают этот статус через 14 дней. Меняйте дату в настройках статуса в свойствах узла Управляемые устройства Статус означает, что все это время Агент администрирования не связывался с Сервером, и Сервер не мог соединиться с компьютером во время полного опроса сети
Контроль над устройством потерян	Этот статус означает, что Агент не соединяется с Сервером, но Сервер соединялся с компьютером во время полного опроса сети

Если у компьютера статус Агент администрирования неактивен в течение долгого времени, выясните, что случилось с компьютером. Если этого компьютера больше нет, удалите его из группы и затем еще раз из списка **Обнаружение устройств и развертывание | Нераспределенные устройства**. Если сотрудник болеет или в отпуске, ничего не делайте.

Если сотрудники подолгу (месяцами) не бывают в сети, увеличьте период, после которого Сервер администрирования автоматически удаляет компьютеры из группы. По умолчанию это 60 дней. Откройте свойства группы **Управляемые устройства**, перейдите на вкладку **Параметры** выберите раздел **Активность устройств** и измените значение параметра **Удалять устройство из группы, если оно неактивно больше (сут)**. Или отключите этот параметр совсем, если сотрудники могут работать вне офиса неограниченно долго.

Чтобы сотрудники вне офиса могли подключаться к Серверу администрирования, получать настройки и сообщать об угрозах, организуйте доступ к портам Сервера администрирования из Интернет. Несколько вариантов того, как это сделать, описано в курсе KL 302 Масштабирование

Как заставить компьютер связаться с сервером



Если у компьютера статус *Давно не подключался*, проверьте, что:

- Агент администрирования установлен
- Агент администрирования запущен

Если пользователь удалил Агент администрирования, включите защиту паролем в политике Агента.

Если Агент установлен и запущен, проверьте его настройки. Используйте утилиту **klnagchk.exe** из папки Агента администрирования *%ProgramFiles(x86)%\Kaspersky Lab\NetworkAgent*:

- Запустите интерфейс командной строки (cmd.exe) с правами администратора
- Зайдите в папку Агента администрирования
- Запустите утилиту **klnagchk.exe**

Без параметров утилита выводит настройки Агента администрирования, пробует подключиться к Серверу администрирования с этими настройками, публикует результат, и в конце выводит статистику подключений.

Во время тестового подключения Агент не проверяет, есть ли на Сервере новые настройки и не посылает на Сервер свои данные.

Чтобы заставить Агент синхронизироваться с Сервером, выполните команду **klnagchck.exe –sendhb**

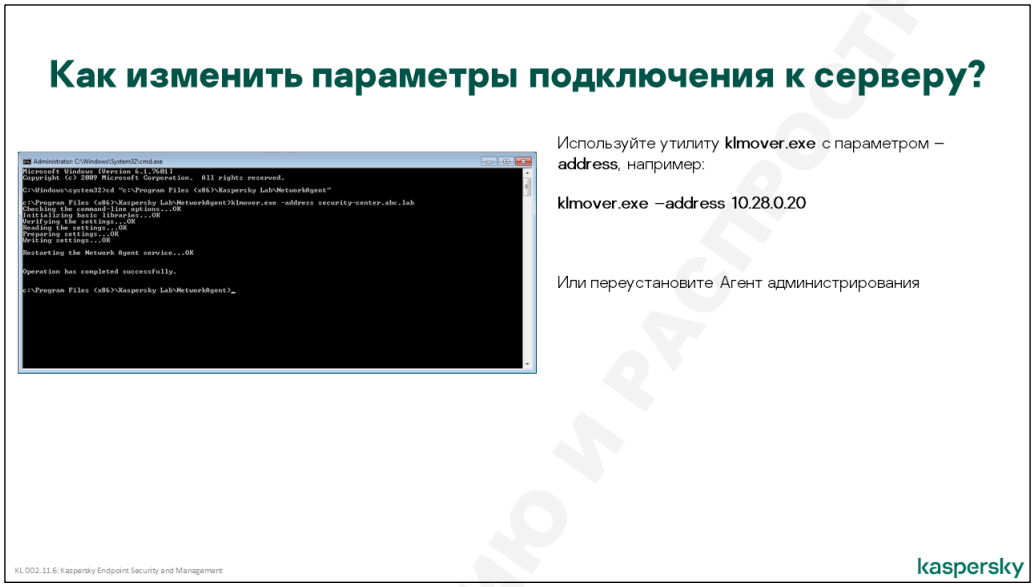
Эту команду нужно выполнять локально на клиентском компьютере.

В веб-консоли администрирования тоже есть команды, чтобы проверить связь с компьютером:

Проверить доступность устройства (Команда доступна только в MMC-консоли администрирования)	Проверяет статус компьютера *Видим в сети* по базе Сервера администрирования. Связываться с компьютером не пытается, поэтому ничего не добавляется к тому, что и так показывает иконка компьютера

Синхронизировать принудительно (Свойства устройства вкладка Общие, **раздел** Общие**)**	Посылает сигнал на порт UDP 15000 компьютера.

Как переподключить компьютер к серверу



Если у Агента администрирования неправильные параметры подключения к Серверу, исправьте их утилитой **klmover.exe** из той же папки Агента администрирования:

- Запустите интерфейс командной строки (**cmd.exe**) с правами администратора
- Зайдите в папку Агента администрирования
- Запустите утилиту **klmover.exe** с параметром **–address** и адресом Сервера:

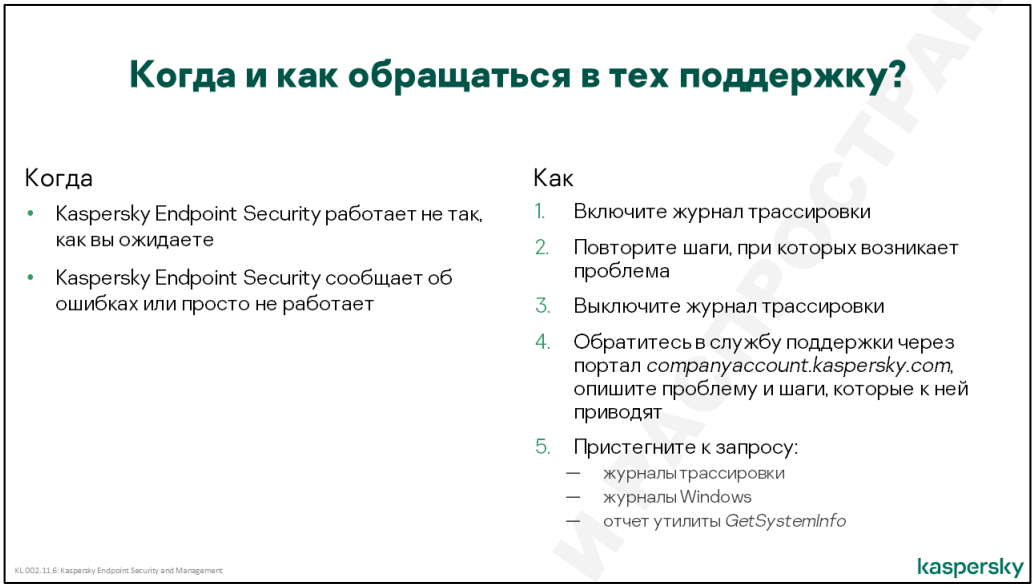
```
klmover.exe –address 10.28.0.20
```

Если у Сервера нестандартный порт, добавьте параметр **–ps** и номер порта.

Чтобы исправить неправильные параметры подключения удаленное, переустановите Агент администрирования. Перед этим проверьте настройки пакета Агента администрирования. Если у установленного Агента неправильные параметры, не исключено, что они были неправильными в пакете.

3.5 Как обратиться в поддержку

Как и когда обращаться в техническую поддержку



Если Kaspersky Endpoint Security не работает или работает не так, как настроит администратор, а простые меры не решают проблему, обращайтесь в техподдержку.

Чтобы быстрее получить ответ, сразу соберите журналы:

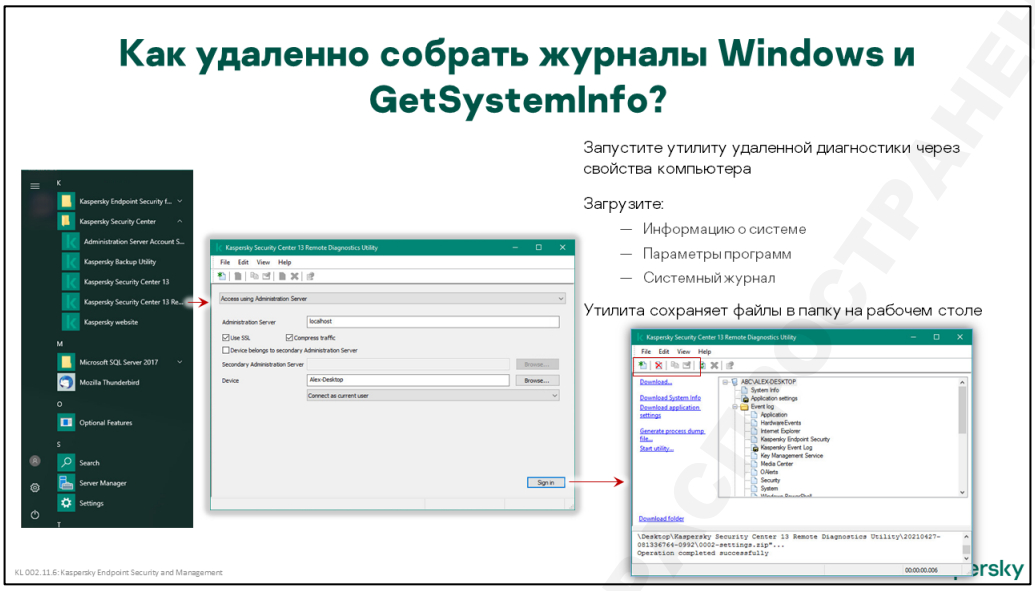
- Журналы Kaspersky Endpoint Security
- Журналы трассировки Kaspersky Endpoint Security вокруг момента, когда возникает проблема
- Журналы Windows
- Журнал GetSystemInfo — информация о компьютере

Чтобы обратиться в техническую поддержку:

1. Создайте запрос на портале *companyaccount.kaspersky.com*
2. Выберите продукт и область функциональности
3. Опишите шаги, которые приводят к проблеме
4. Приложите журналы

Журналы можно собирать локально прямо на компьютере, удаленно с помощью утилиты удаленной диагностики Kaspersky Security Center или через MMC-консоль Kaspersky Security Center.

Как удаленно собрать журналы Windows и GetSystemInfo



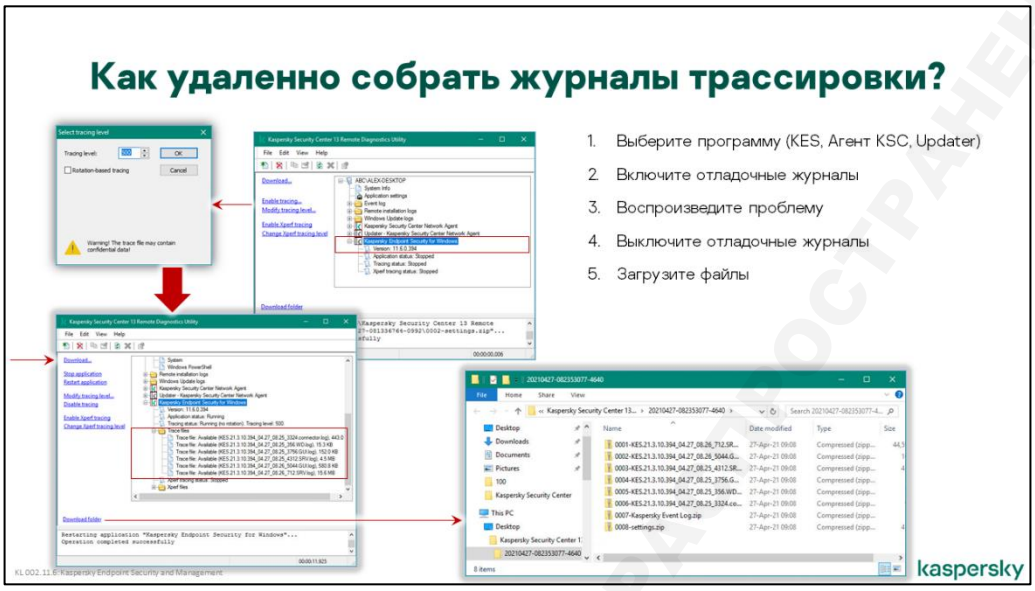
Чтобы собрать журналы удаленно, подключитесь к компьютеру утилитой удаленной диагностики:

1. Запустите утилиту из папки Kaspersky Security Center в меню *Пуск*
2. Выберите **Имя компьютера** и **Адрес сервера администрирования**
3. Нажмите кнопку **Войти**
4. Чтобы получить информацию о компьютере, нажмите ссылку *Загрузить информацию о системе* в левом верхнем углу
5. Чтобы получить журналы Windows, выберите журнал и нажмите ссылку *Загрузить журнал…* в левом верхнем углу

> Загрузите журнал Kaspersky Event Log и любые другие журналы, в которых есть события о проблеме

Утилита диагностики сохраняет файлы в папку на рабочем столе. Откройте ее по ссылку *Папка загрузки* в левом нижнем углу.

Как удаленно собрать журналы трассировки



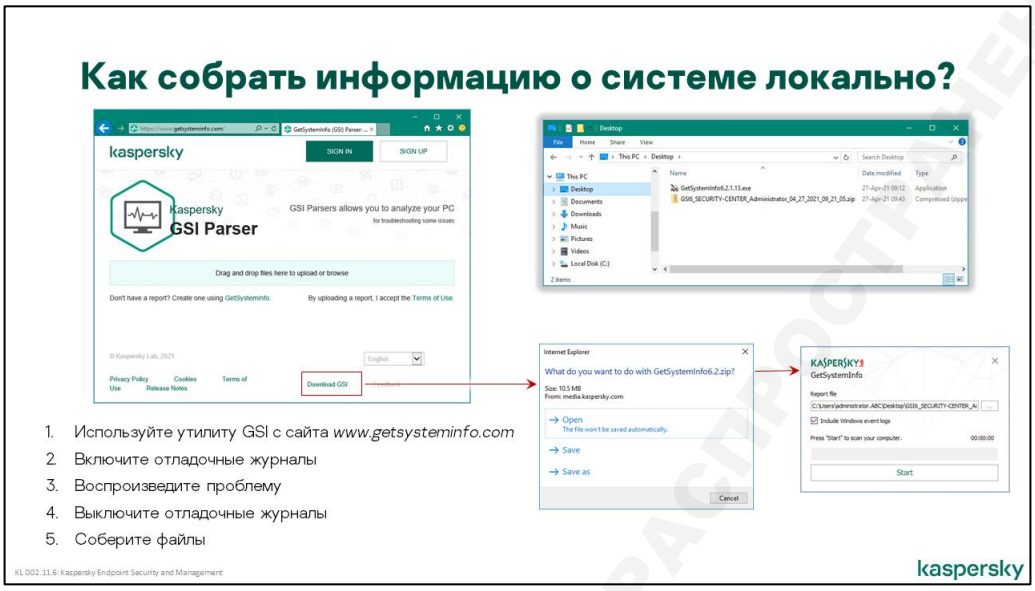
Чтобы собрать журналы трассировки через утилиту диагностики:

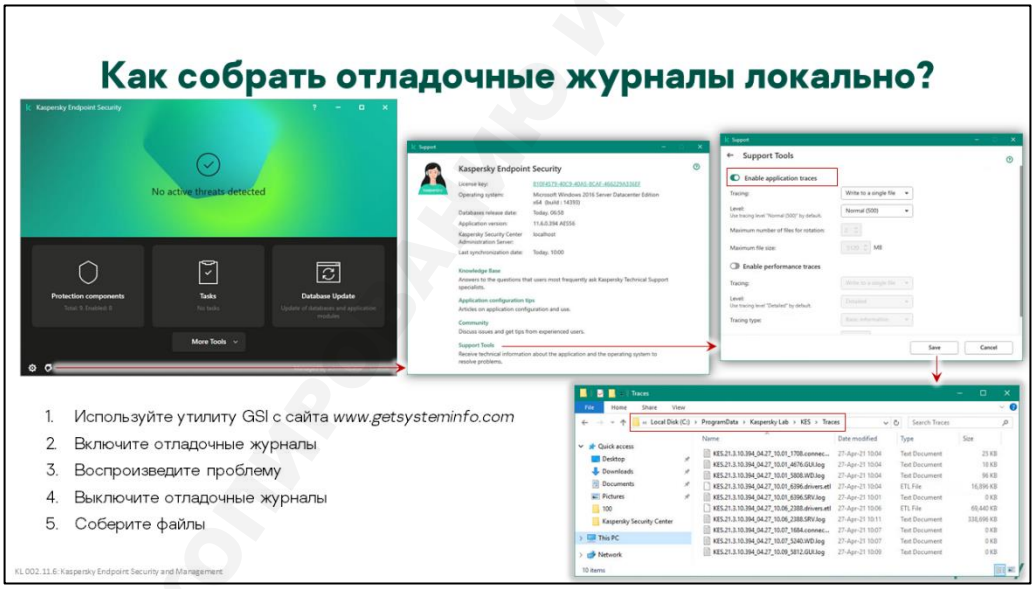
1. Выберите в дереве объектов Kaspersky Endpoint Security
2. Нажмите ссылку *Включить трассировку* слева, не меняйте уровень трассировки, и нажмите **OK**
3. Повторите шаги, которые демонстрируют проблему
4. Нажмите ссылку *Выключить трассировку* в утилите диагностики
5. Раскройте папку **Файлы трассировки** под Kaspersky Endpoint Security
6. По одному выберите файлы и загрузите их ссылкой *Скачать файл* слева

Если проблема не в Kaspersky Endpoint Security или не только в нем, точно так же соберите журналы трассировки Агента администрирования, Сервера администрирования, компонента Updater.

Когда закроете утилиту диагностики, она спросит, не удалить ли папку загрузки. Не удаляйте папку, пока не отправите журналы в техническую поддержку.

Как собрать журналы локально





Иногда проблему удобнее воспроизводить локально на компьютере. В таком случае и журналы удобнее собирать локально.

Чтобы собрать сведения о системе, загрузите утилиту GetSystemInfo с сайта *getsysteminfo.com* Запустите ее и сохраните журнал в папку. Утилита собирает сразу и информацию о системе и журналы Windows, поэтому отдельно собирать журналы Windows не нужно.

Чтобы собрать журналы трассировки:

1. В окне Kaspersky Endpoint Security нажмите кнопку **Поддержка**
2. В окне **Поддержка** нажмите ссылку *Мониторинг проблем*

3. Выберите **Включить трассировку программы**, в списке выберите уровень *Обычный (500)* и нажмите **OK**

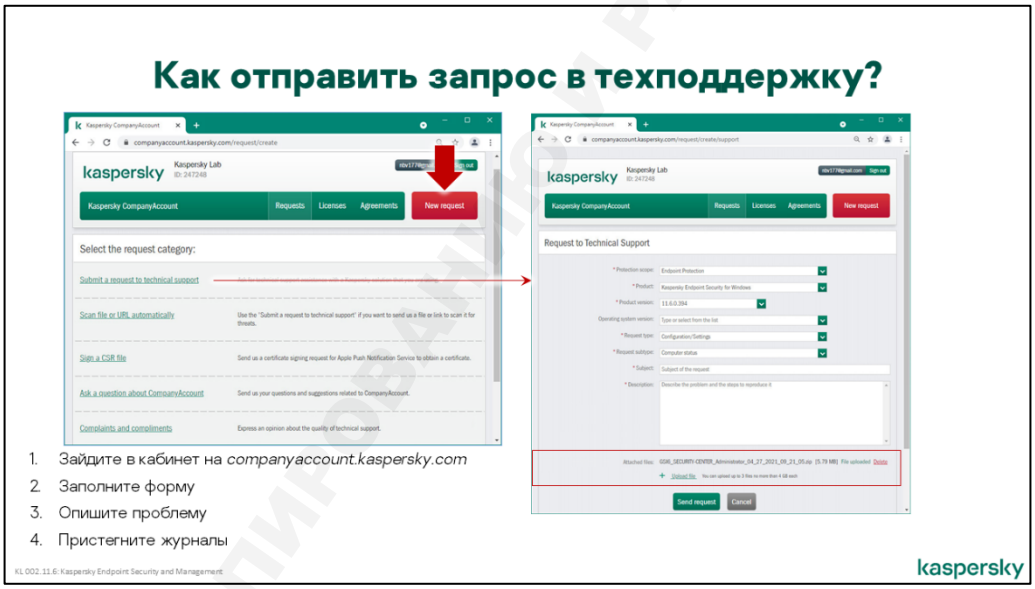
> Можно выбрать трассировку **С ротацией**. В этом случае появится возможность ограничить максимальное количество файлов трассировки и максимальный размер каждого из файлов трассировки. Если количество файлов трассировки достигло предела, самый старый файл удаляется, чтобы можно было писать новый.

4. Воспроизведите проблему
5. Выключите трассировку
6. Заберите журналы трассировки из папки *%ProgramData%\Kaspersky Lab*

> В имени файла указана дата и время создания, выбирайте последние по времени журналы

Как локально включить журналы трассировки компонентов Kaspersky Security Center, читайте в статье *http://support.kaspersky.com/9323*

Как отправить запрос в техническую поддержку



Когда у вас есть все журналы, обращайтесь в техническую поддержку:

1. Войдите на веб-сайт *companyaccount.kaspersky.com*

> Если у вас нет учетной записи, зарегистрируйтесь: укажите ваш почтовый ящик и лицензию на продукты Лаборатории Касперского (код активации или ключевой файл)

2. Создайте кнопку **Создать запрос** и выберите *Запрос в Службу Технической поддержки*
3. Выберите область защиты, продукт, версию, операционную систему, тип и подтип запроса
4. Введите тему запроса: кратко сформулируйте проблему
5. Заполните описание проблемы: опишите шаги, которые к ней приводят, укажите, какой результат вы ожидаете в результате этих шагов, и какой получаете вместо этого
6. Прикрепите архив со всеми журналами

4. Что делать не каждый день

4.1 Как устанавливать обновления программ

Какие бывают обновления программ

Какие бывают обновления программ?

Обновления Kaspersky Endpoint Security	Как часто появляются	Как устанавливать
Новые версии	Раз в 2-4 года	Задачей установки
Service Packs	Раз в 1-2 года	Задачей установки
Maintenance Release	Раз в квартал/Раз в полгода	Задачей обновления
Private Fix	По запросу	Задачей установки сторонних программ

Обновления Kaspersky Security Center	Как часто появляются	Как устанавливать
Новые версии	Раз в 2-4 года	Переустановкой
Service Packs	Раз в 1-2 года	Переустановкой
Maintenance Release	Иногда	Переустановкой
Patch	Раз в квартал	Автоматически
Private Fix	По запросу	Задачей установки сторонних программ

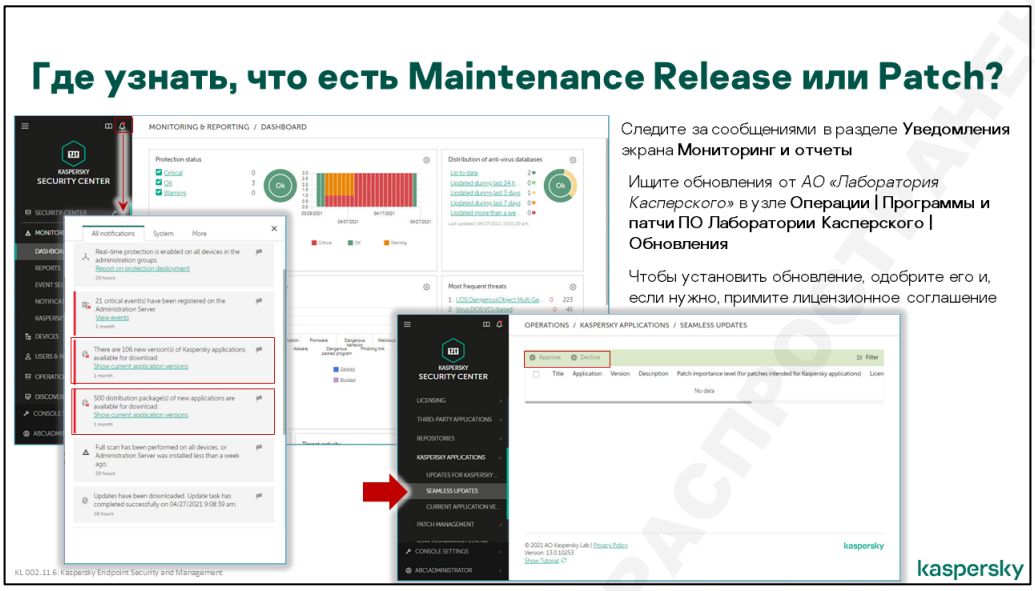
KL 002.11.6: Kaspersky Endpoint Security and Management

kaspersky

Кроме обновлений сигнатур, которые выходят практически постоянно, есть обновления самих программ, которые выходят гораздо реже:

Новые версии	Появляются раз в несколько лет, приносят новые возможности, компоненты, настройки т.д. Устанавливаются задачей установки Kaspersky Endpoint Security и мастером установки Kaspersky Security Center
Service Pack	Появляются примерно раз в год, иногда реже. Обновляют версии компонентов и драйверов, могут приносить новые настройки и возможности, но изменения не такие большие как в новых версиях Устанавливаются задачей установки Kaspersky Endpoint Security и мастером установки Kaspersky Security Center
Maintenance Release	В Kaspersky Endpoint Security выпускаются раз в 1–2 квартала, исправляют ошибки, вносят незначительные изменения в настройки, устанавливаются задачей обновления В Kaspersky Security Center это практически то же самое, что и Service Pack: выпускаются через год после новой версии или Service Pack, устанавливаются мастером установки Kaspersky Security Center
Patch	В Kaspersky Endpoint Security не выпускаются, в Kaspersky Security Center выпускаются раз в квартал, исправляют ошибки, вносят небольшие изменения в работу, на Агенты администрирования устанавливаются автоматически
Private fix	Выпускаются по запросу, исправляют отдельные проблемы для отдельных клиентов. Как правило, для клиентов с Maintenance Service Agreement

Где узнать, что вышло исправление



Узнать, что вышло минорное обновление — Maintenance Release для Kaspersky Endpoint Security или патч для Kaspersky Security Center — можно в разделе **Операции | Программы «Лаборатории Касперского» | Обновления**. Следите за сообщениями в разделе **Мониторинг и отчеты | Уведомления** на вкладке **Обновления**.

Минорные обновления устанавливаются автоматически, но только после того, как их одобрит администратор. Как правило, чтобы установить обновление, нужно принять лицензионное соглашение. Об этом говорит статус **Требуется принять Лицензионные соглашения для обновления**.

Чтобы устанавливать обновления сторонних производителей нужна лицензия на Управление системами, например, лицензия KESB Расширенный. Читайте об этом в курсе KL 009 Управление системами. Веб-консоль в текущей версии не поддерживает функционал управления системами.

Как устанавливать только одобренные обновления

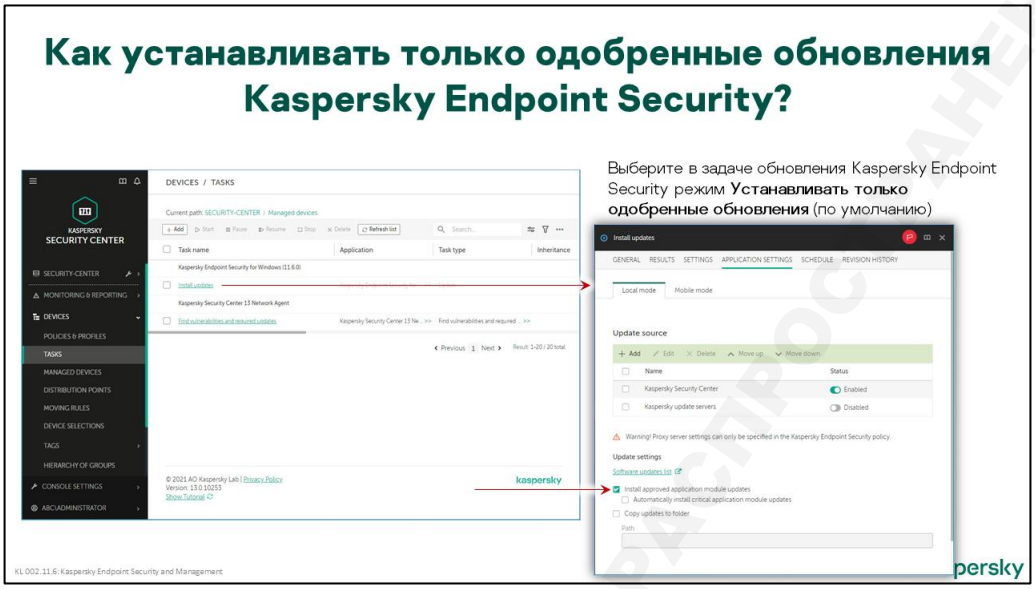
Как устанавливать только одобренные обновления KES

Kaspersky Endpoint Security может обойтись без обновлений программы. Если нет никаких критических проблем, мешающих работе, можно использовать Kaspersky Endpoint Security, до тех пор, пока не выйдет новая версия или Service Pack.

И все же, обновления модулей могут быть полезны. Они могут улучшать показатели производительности компьютера, улучшать защиту и добавлять новые возможности продукту. Часто преимущества весомее рисков. К тому же риски можно контролировать тестированием обновлений и распространением только одобренных. В отношении обновлений модулей, у администратора есть такие возможности выбора в задаче обновления Kaspersky Endpoint Security:

- **Устанавливать одобренные обновления модулей программы** — включено по умолчанию. Можно отключить в группах, где компьютеры исключительно чувствительны к изменениям, например, в группах с важными серверами
- **Автоматически устанавливать критические обновления модулей программы** — устанавливает обновления, одобренные администратором, и отмеченные критическими в

Лаборатории Касперского. Установка непроверенных обновлений несет с риски возникновения непредвиденных проблем



Чтобы одобрить обновление:

1. Выберите обновление на вкладке **Операции** | **Программы «Лаборатории Касперского»** | **Обновления и патчи ПО «Лаборатории Касперского»**
2. Нажмите кнопку **Одобрить** над списком обновлений
3. Если в обновлении есть лицензионное соглашение, появится окно с ним. Примите соглашение

Если вы по ошибке одобрили не то обновление, откройте его свойства и измените значение поля **Одобрение обновления** на *Не определено* или *Отклонено*.

Перед тем, как одобрить обновление, установите его на тестовые компьютеры и проследите, что оно не вызывает проблем.

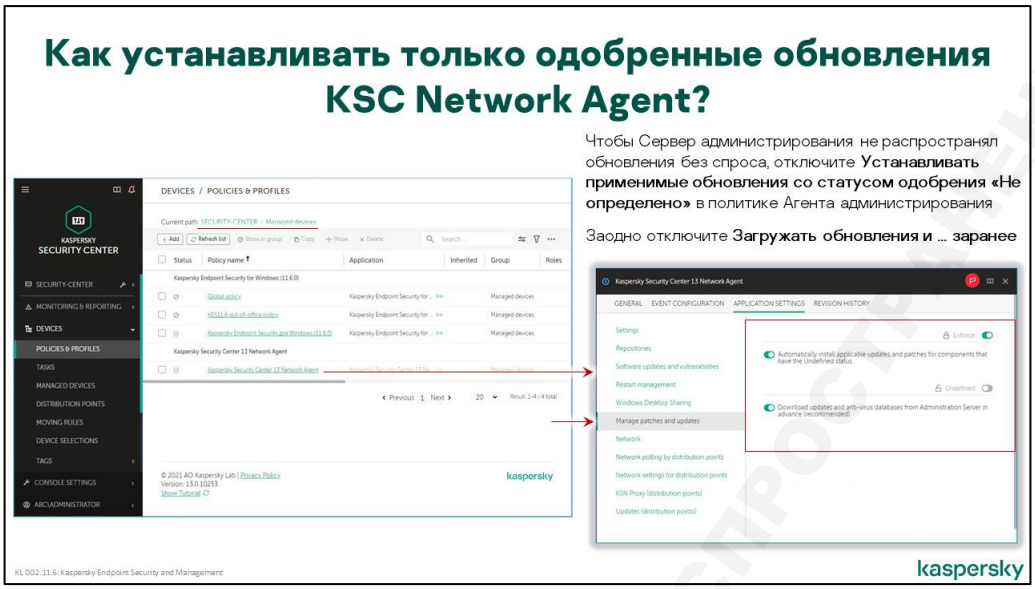
После установки обновления программы может потребоваться перезагрузка.

Как устанавливать только одобренные обновления Агента администрирования

Одобренные обновления Агента администрирования устанавливаются автоматически без помощи задач. После того как администратор одобрил обновление, Агенты начнут загружать его во время плановых синхронизаций и устанавливать локально.

По умолчанию Сервер администрирования устанавливает все обновления Агента администрирования, а не только одобренные. Чтобы устанавливать только одобренные обновления:

1. Откройте политику *Агента администрирования* на вкладке **Устройства | Политики и профили политик**
2. Перейдите на вкладку **Параметры программы** в раздел **Управления патчами и обновлениями**
3. Снимите флаг **Установить применимые обновления и патчи для компонентов со статусом «Не определено»**



Чтобы тестировать обновления Агента администрирования создайте группу для тестовых компьютеров и включите устанавливать неодобренные обновления в политике этой группы

Администратор всегда может не устанавливать какое-то обновление, даже если в политике настроено автоматическое обновление. Для этого нужно открыть свойства обновления и выбрать для параметра **Одобрение обновления** значение **Отклонено**.

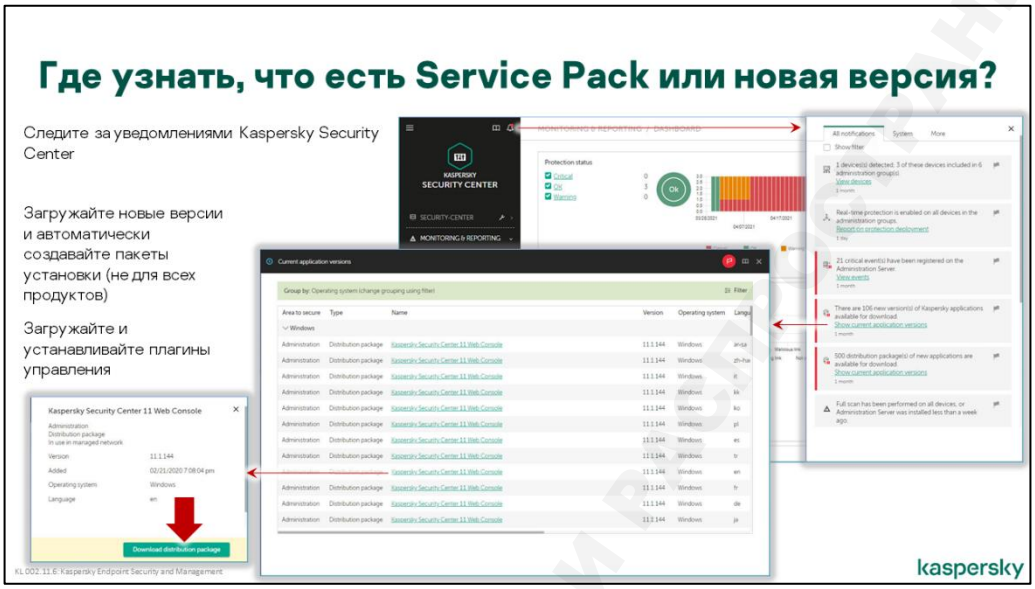
Чтобы не распространять обновления Агентов администрирования более старых версий (до версии 10 SP1 включительно), отключите параметр в задаче **Загрузка обновлений в хранилище**:

1. Откройте свойства задачи **Загрузка обновлений в хранилище** на вкладке Устройства | **Задачи**
2. Перейдите на вкладку **Параметры программ** и нажмите ссылку *Настроить…* в секции **Прочие параметры**
3. Снимите флаг **Обновлять модули Агентов администрирования (для агентов администрирования версии ниже 10 Service Pack 2)**

Поскольку задача существует в единственном экземпляре, обновления Агентов администрирования (до версии 10 SP1 включительно) будут устанавливаться или не устанавливаться одновременно во всей сети. Включить установку этих обновлений в одних группах и выключить в других не получится.

Как узнать, что вышла новая версия

Где искать новые версии



О том, что есть новые мажорные версии продуктов — Service Pack и новые версии — тоже сообщают события в разделе **Мониторинг и отчеты | Уведомления | Обновления**. Следите за сообщениями:

- Есть обновления компонентов Kaspersky Security Center
- Есть обновления программ «Лаборатории Касперского»
- Для загрузки доступно новых версий программ «Лаборатории Касперского»

Все они ведут в окно **Инсталляционные пакеты**.

Чтобы открыть это окно не из сообщения о новых версиях, зайдите в раздел **Операции | Программы «Лаборатории Касперского» | Текущие версии программ**

Окно показывает список доступных версий продуктов «Лаборатории Касперского», которыми может управлять Kaspersky Security Center. Их загрузить с серверов Лаборатории Касперского прямо в этом окне.

Среди версий программ есть:

- Дистрибутивы, которые можно загрузить на Сервер администрирования
- Дистрибутивы, из которых нельзя сделать пакет, но можно просто загрузить
- Плагины управления, которые можно загрузить и отдельно установить в Консоль

Как найти нужный продукт, версию и язык

В списке много разных программ, несколько версий каждой программы и несколько локализаций каждой версии, и поэтому легко потеряться.

Чтобы найти то, что нужно, например, последнюю версию Kaspersky Endpoint Security на русском языке, настройте фильтр:

— Тип программы:

Инструменты управления	Дистрибутивы и патчи компонентов Kaspersky Security Center и Агентов администрирования для разных платформ
Рабочие станции	Kaspersky Endpoint Security для разных платформ (Windows, Mac)
Файловые серверы и системы хранения данных	Дистрибутивы и плагины Антивируса Касперского для Windows File Servers, Антивируса Касперского для Windows Servers и Kaspersky Security для Windows Servers
Виртуальные среды	Дистрибутивы и плагины Kaspersky Security for Virtualization Light Agent
Мобильные устройства	Дистрибутивы и плагины Kaspersky Security for Mobile (Android)
Банкоматы и POS-системы	Дистрибутивы и плагины Kaspersky Embedded Systems Security

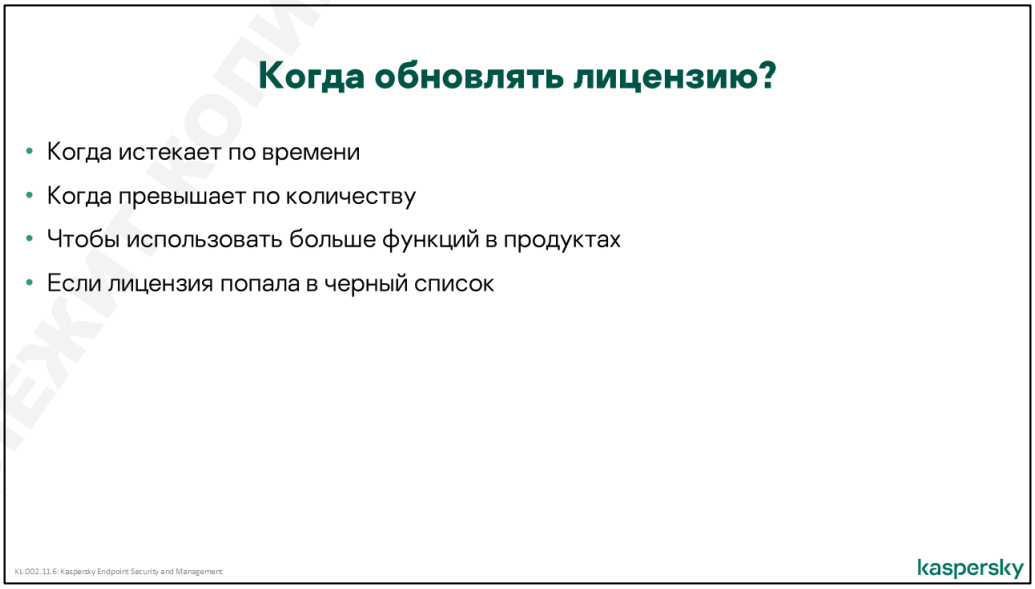
— Тип обновления: полный дистрибутив, плагин, веб-плагин или патч

— Какие обновления ПО показывать — укажите требуемую версию программы

— Язык – укажите требуемый язык интерфейса программы

4.2 Как обновить лицензию

Когда обновлять лицензию



Первоначальная лицензия приобретается вместе с продуктом для получения права его использования. В дальнейшем вопрос о приобретении лицензии возникает при необходимости преодолеть какое-либо из ограничений лицензии:

— Продление срока действия — наиболее типичная ситуация, когда компанию все устраивает и нужно продлить лицензию, чтобы продолжить пользоваться продуктом

— Увеличение количества компьютеров — если компания растет, и количество компьютеров грозит превысить лицензионное ограничение

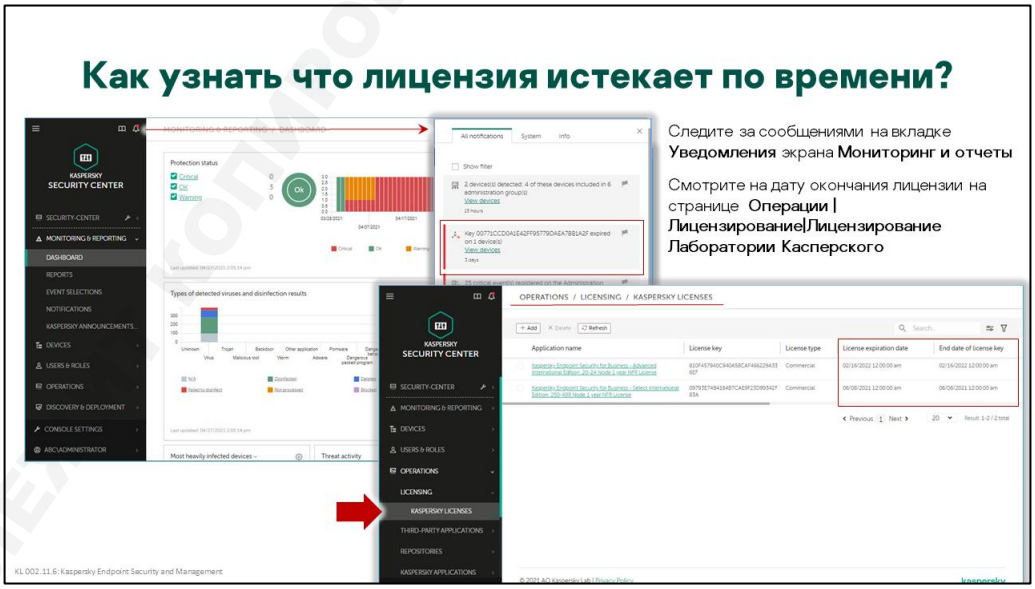
— Расширение функциональности — если в компании назрела необходимость в использовании ранее невостребованных функций продукта, например, шифрования или автоматической установки обновлений Windows

Кроме этого, лицензия может попасть в черный список, если окажется в свободном доступе в Интернете. Лаборатория Касперского блокирует эти лицензии, и они перестают работать. Черный список лицензий продукты получают вместе с обновлениями сигнатур.

Без лицензии Kaspersky Endpoint Security работает, но с ограничениями:

До первой установки лицензии	Работают Защита от файловых угроз и Сетевой экран.
Если истекла коммерческая лицензия	Все компоненты работают, но задача обновления не запускается и сервера KSN недоступны. Уровень защиты из-за этого постепенно падает.
Если истекла пробная лицензия или коммерческая лицензия попала в черный список	Продолжат работать только Защита от файловых угроз и Сетевой экран. Защита будет возобновлена после активации продукта годной коммерческой лицензией.

Как узнать, что лицензия истекает по времени



Если лицензия на компьютере заканчивается или закончилась, это повод для администратора обратить внимание.

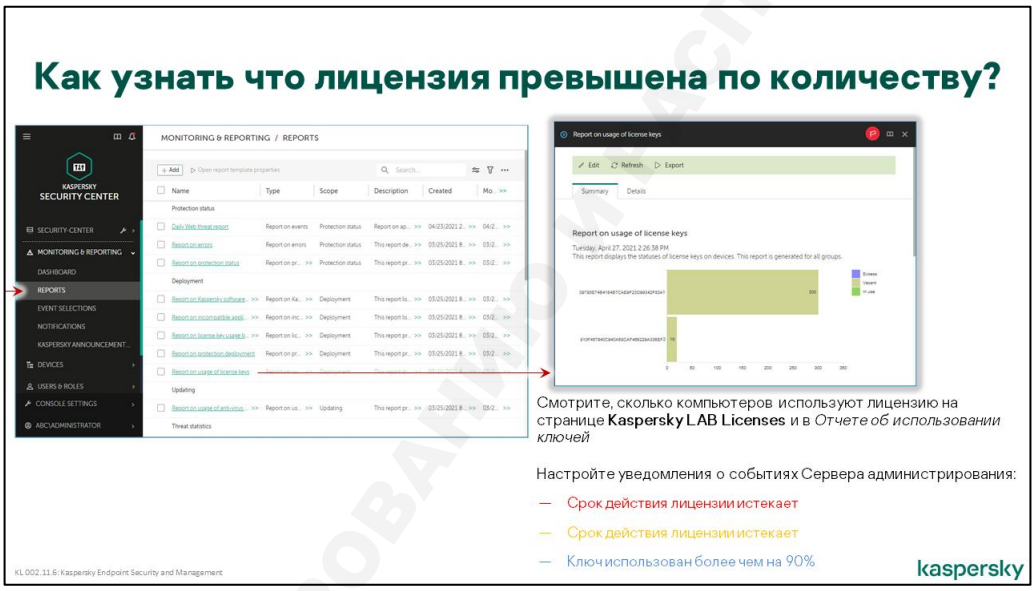
Дату окончания лицензии можно увидеть в свойствах лицензий в разделе **Операции | Лицензирование | Лицензии Лаборатрии Касперского**.

Также внимание администратора могут привлекать статусы компьютеров, настраиваемые в свойствах групп администрирования. К лицензиям имеют отношение два условия присвоения статуса:

— **Срок действия лицензии истек** — придает компьютеру статус *Критический*. Может срабатывать не сразу, а спустя заданное количество дней после истечения лицензии — чтобы дать возможность отработать механизмам автоматического обновления лицензии и не беспокоить администратора понапрасну. По умолчанию все же условие срабатывает через 0 дней, т.е. сразу после истечения лицензии

— **Срок действия лицензии скоро истечет** — придает компьютеру статус *Предупреждение*. По умолчанию начинает отображаться за 7 дней до срока истечения, но этот параметр можно изменить в любую сторону.

Как узнать, что лицензия истекает по количеству



Практически вся информация о ключах, которая может понадобиться администратору, доступна на вкладке **Операции | Лицензирование | Лицензии Лаборатории Касперского**. В том числе, какое у лицензии ограничение по узлам, и сколько компьютеров уже использует лицензию.

Сервер администрирования показывает, сколько управляемых компьютеров использует лицензию. Он не получает данные от серверов активации Лаборатории Касперского, у которых может быть другая статистика, если лицензию используют компьютеры без Агента администрирования

События Сервера администрирования сообщают о превышении ограничения по узлам:

— **Лицензионное ограничение превышено** — есть два события с таким именем, одно из которых является *критическим*, а второе — *предупреждением*. *Критическое событие* генерируется при превышении 110% от заданного в лицензии ограничения по узлам. *Предупреждение* сообщает о превышении 100% от заданного ограничения

— **Ключ использован более чем на 90%** — *информационное сообщение*, смысл которого полностью передается названием

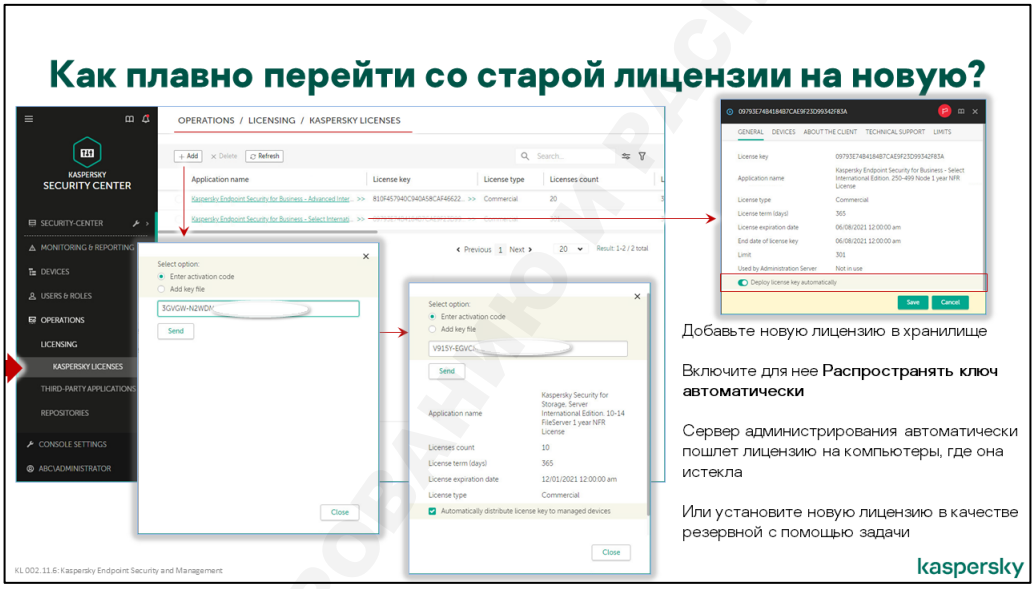
Никаких технических ограничений в связи с превышением 100% или 110% от лицензионного ограничения, Сервер администрирования не вводит. Если для активации используются ключи, а не коды, администратор может беспрепятственно распространить их задачей установки ключа на неограниченное количество компьютеров. С точки зрения лицензионного соглашения, лицензия

дает вам право использовать программное обеспечение на том количестве устройств, которое приобретено и обозначено в лицензионном сертификате. Если в свойствах ключа включить параметр *Распространять ключ автоматически*, Сервер администрирования будет не только распространять его на компьютеры, но и отзывать с «лишних» компьютеров.

При использовании кодов активации технические ограничения могут вводить сервера активации Лаборатории Касперского. Каждому экземпляру Kaspersky Endpoint Security который приходит за активацией Сервера активации выдают разрешение (ticket) на использование продукта. Если одновременно выданных разрешений намного больше, чем ограничение лицензии (в полтора-два раза), Сервера активации прекращает их выдавать.

Как перейти со старой лицензии на новую

Как продлить лицензию на компьютерах



Когда приближается срок истечения лицензии, компания приобретает новую. Возникает вопрос, как переключиться с одной лицензии на другую без временного разрыва, но и не уменьшая эффективный срок использования ни одной из лицензий. С одной стороны, не хотелось бы заменять старую лицензию пока у нее еще есть несколько дней до истечения. Но и новую лицензию нужно активировать до того, как старая окончательно перестанет работать.

Чтобы не терять лицензионный период ни старой, ни новой лицензии, используйте один из двух подходов:

1. Заранее распространите новый ключ на компьютеры задачей установки ключа. В настройках задачи укажите, что это дополнительный (резервный) ключ

   Резервные ключи и коды можно добавлять практически во всех продуктах Лаборатории Касперского. Как только лицензия, указанная в активном ключе, перестает действовать, продукт автоматически активируется с использованием резервного ключа или кода.

2. Добавьте новую лицензию на Сервер администрирования и включите в ее свойствах параметр *Распространять ключ автоматически*

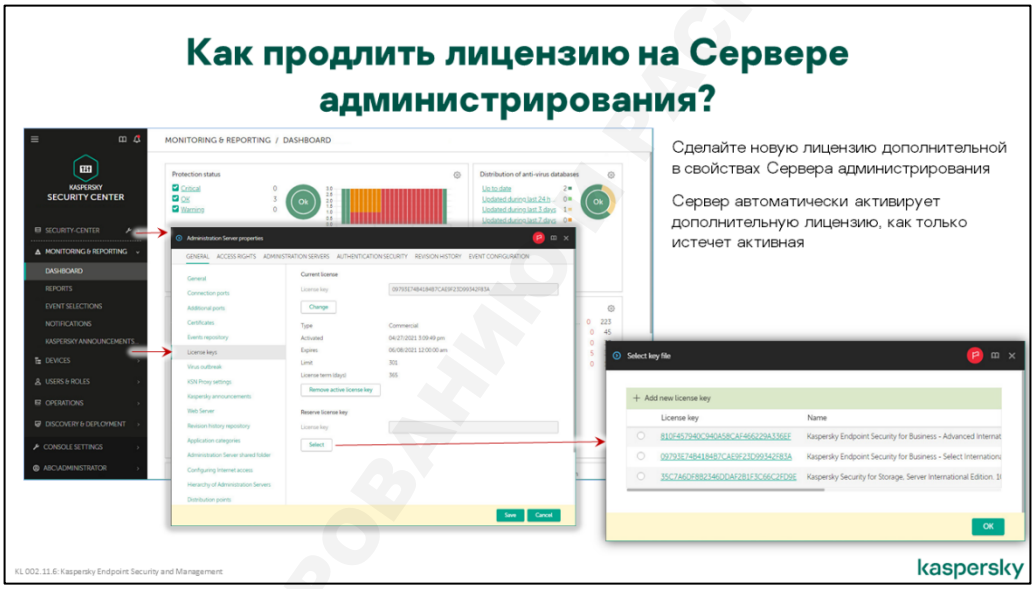
   Когда на компьютерах истечет предыдущий ключ, они получат от Сервера администрирования новый ключ с установленным флагом автоматического распространения.

Автоматически распространяемые ключи поступают на все компьютеры. Если у компьютера нет активной лицензии, автоматически распространяемый ключ станет активным. Если активная лицензия уже есть, автоматически распространяемый ключ станет резервным. Если есть и активная, и резервная лицензии, автоматически распространяемый ключ не установится.

Ключ или код для распространения можно добавить в мастере первоначальной настройки. Впоследствии добавлять ключи проще на вкладке **Операции | Лицензирование | Лицензии Лаборатории Касперского** используя кнопку **Добавить**.

Зарегистрированные ключи и коды можно экспортировать из хранилища в виде файлов ключей и текстовых файлов с кодом, функционал доступен только в MMC-консоли администрирования. Экспортированные файлы можно использовать для локальной активации или как резервную копию лицензии.

Как продлить лицензию на Сервере администрирования



Сервер администрирования Kaspersky Security Center нужно активировать только для использования расширенных функций системы администрирования, доступных по лицензиям KESB Стандартный и KESB Расширенный.

Для операций, описанных в этом курсе, активировать Сервер администрирования не нужно

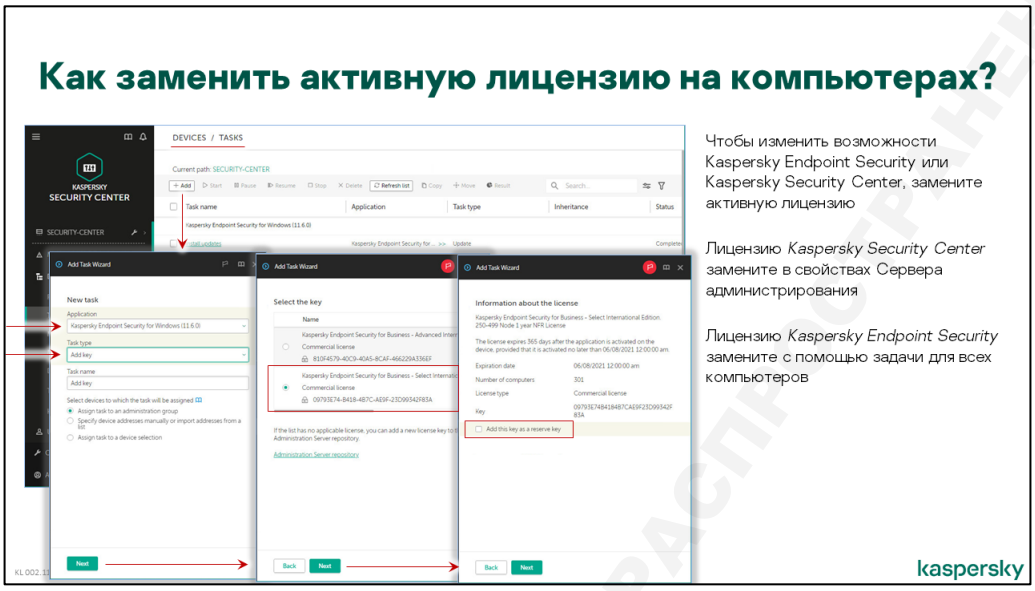
Чтобы заменить активный или добавить резервный ключ на Сервер администрирования, откройте раздел **Ключи** в окне свойства Сервера. В этом разделе можно указать основную и резервную лицензии. При необходимости ключ можно заменить или удалить.

Лицензию для Сервера администрирования можно выбрать из лицензий, добавленных в хранилище **Лицензии Лаборатории Касперского**.

Чтобы добавить на Сервер администрирования ключ, нужно выбрать именно ключ для Kaspersky Security Center. Смотрите, что написано в таблице ключей в графе **Название программы**. Там обычно есть описание: *Security Center* или *Kaspersky Security for WS and FS*, который указывает на назначение ключа.

Если вы добавляете код, в его название можно не смотреть, один и тот же код активирует все продукты, которые входят в лицензию: и Kaspersky Endpoint Security и Kaspersky Security Center.

Как заменить активную лицензию



Иногда бывает нужно установить конкретный ключ на конкретный компьютер или группу компьютеров. Автоматическое распространение для этого плохо подходит. Вместо этого можно создать задачу *Добавление ключа*.

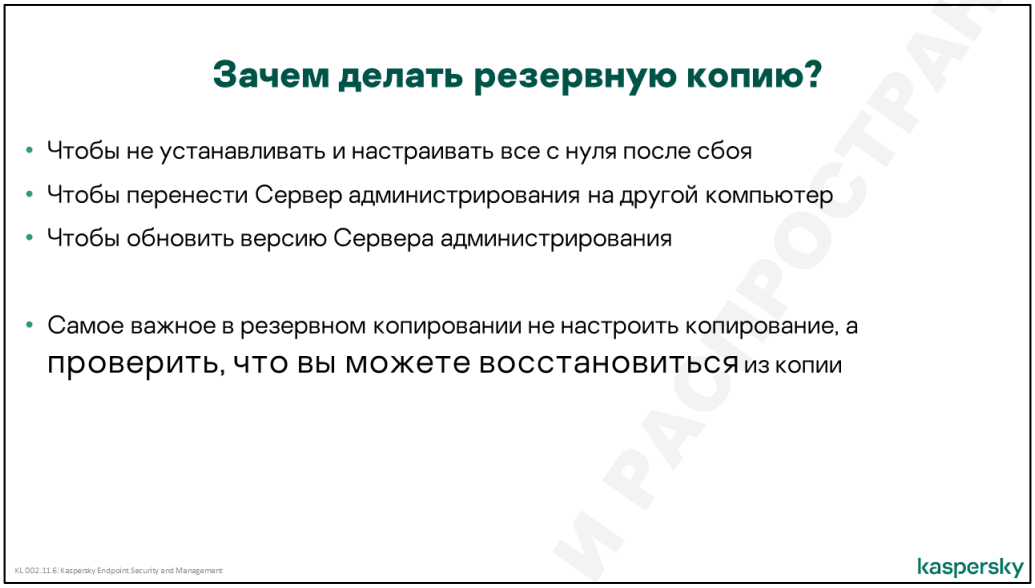
Эту задачу можно создать с помощью обычного мастера создания задачи на вкладке **Задачи**.

Если два продукта используют разные плагины управления в Консоли администрирования, им потребуются и разные задачи *Добавить ключ*. Например, у Kaspersky Endpoint Security 10 Service Pack 2 для Windows и Kaspersky Endpoint Security 10 Service Pack 1 для Windows разные плагины. Следовательно, задача добавления ключа для Kaspersky Endpoint Security 10 Service Pack 2 для Windows не будет выполнена Kaspersky Endpoint Security 10 Service Pack 1 для Windows и наоборот.

В мастере создания задачи и позже в ее свойствах лицензию можно выбрать из списка зарегистрированных ключей и кодов (на вкладке **Операции | Лицензирование | Лицензии Лаборатории Касперского**). Выбранный ключ или код можно установить в качестве дополнительного с помощью опции в свойствах задачи. Эта опция включена по умолчанию, поскольку считается, что для установки основной лицензии используется механизм автоматической установки (опция в свойствах кода или ключа).

4.3 Как организовать резервное копирование

Зачем делать резервные копии



Резервное копирование — универсальная защита от любых проблем. Что бы ни случилось с Сервером администрирования или сервером с базой данных Kaspersky Security Center, если у администратора в надежном месте есть резервная копия конфигурации, он сможет восстановить управление системой в течение часа.

Резервная копия данных Kaspersky Security Center включает практически все видимые и невидимые объекты управления и настройки: всю базу данных, структуру групп администрирования, все задачи и политики, шаблоны отчетов, инсталляционные пакеты[3], созданные выборки событий и компьютеров, сертификат Сервера администрирования и т. д. Не резервируются только обновления в серверном хранилище, поскольку к моменту восстановления из резервной копии они все равно успеют устареть.

С появлением в Kaspersky Endpoint Security функций шифрования, важность резервного копирования еще более возросла. Частью конфигурации Сервера администрирования является хранилище ключей шифрования, которое содержит мастер-ключи всех компьютеров, на которых используется шифрование. Эти ключи необходимы для восстановления доступа к зашифрованным данным в случае любых сбоев. Если мастер-ключи на Сервере администрирования окажутся утеряны, возникает риск безвозвратной потери зашифрованных данных. Подробнее о шифровании и связанных с ним рисках рассказывается в курсе 008. Шифрование.

Даже без учета шифрования потеря данных Сервера администрирования может означать много часов или даже дней или недель на восстановление системы. В большой сети даже создание структуры групп не является тривиальной задачей и может требовать заметных временных затрат. При переустановке Сервера также меняется его сертификат, а это значит, что Агенты администрирования, даже используя правильный адрес, не смогут устанавливать соединение с Сервером. В общем случае для восстановления связи с компьютерами все Агенты придется переустановить.

[3] В том числе автономные, но не включая пакеты с образом операционной системы (об этих пакетах рассказывается в курсе 009)

Наличие резервной копии спасает администраторов от всех перечисленных проблем, т.к. копия включает и сертификат Сервера, и все настройки, и хранилище ключей шифрования.

Резервное копирование может использоваться и как альтернативный способ обновления версии Kaspersky Security Center. Стандартный вариант обновления версии — установка новой версии поверх старой. Инсталлятор обнаруживает установленную старую версию и выполняет обновление компонентов, по возможности сохраняя или конвертируя настройки. Вместо этого можно создать резервную копию старой системы, деинсталлировать ее, установить новую версию Сервера администрирования и восстановить конфигурацию из резервной копии. При таком подходе можно параллельно обновить не только программные компоненты сервера, но и аппаратную конфигурацию.

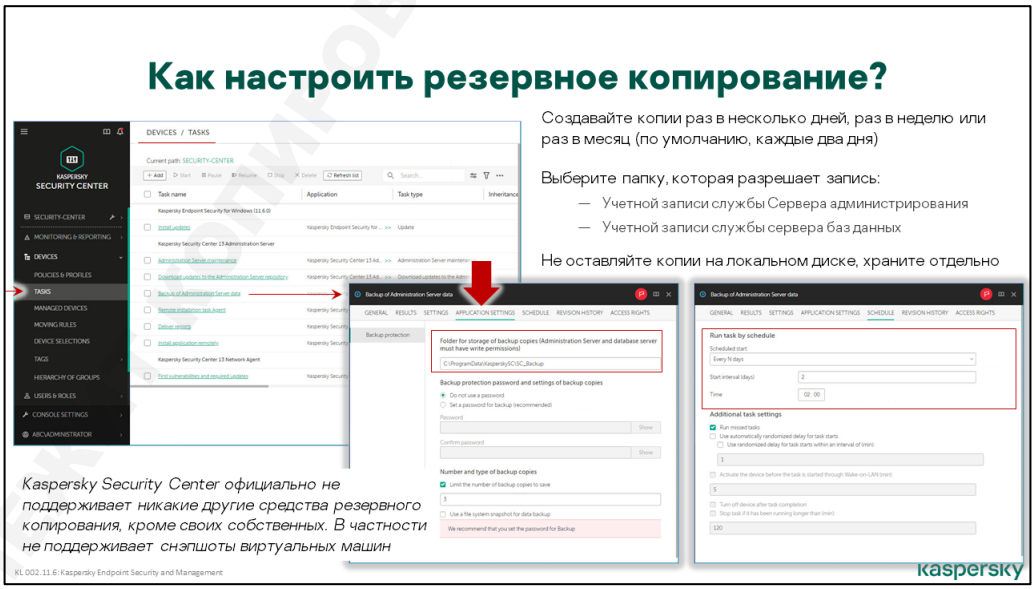
Аналогично через резервную копию можно переносить Сервер администрирования на другой компьютер. Сначала создается копия, потом Сервер администрирования устанавливается на новом месте и восстанавливается из копии. При этом важно, чтобы старый и новый Серверы администрирования использовали однотипный SQL-сервер: оба Microsoft SQL или оба MySQL.

Если при переносе меняется имя Сервера, используемое для подключения к нему клиентских компьютеров, необходимо будет предварительно выполнить задачу смены Сервера администрирования. Подробнее эта задача рассматривается в курсе 302. Kaspersky Endpoint Security and Management. Масштабирование.

Самое важное в резервном копировании, регулярно проверять, что вы можете восстановить систему из резервной копии

Потратьте полчаса времени раз в месяц или хотя бы раз в квартал, чтобы восстановить данные Сервера администрирования на тестовом компьютере. Так вы проверите, что резервные копии не повреждены и заодно отточите навыки и в случае настоящего сбоя, сможете восстановить системы быстро и спокойно

Как настроить резервное копирование



Для создания резервных копий в Kaspersky Security Center предусмотрена специальная задача, которая так и называется — *Резервное копирование данных Сервера администрирования*. Она создается Мастером первоначальной настройки и может существовать только в единственном экземпляре. При необходимости ее можно удалить и создать заново.

Задача, фактически, является надстройкой над утилитой резервного копирования **klbackup.exe**, которую можно найти в каталоге программных файлов Сервера администрирования. При запуске задача просто запускает утилиту с нужными параметрами, а уже утилита выполняет всю работу.

С версии Kaspersky Security Center 10 SP3 в ходе резервного копирования утилита **klbackup.exe** не останавливает службу, копирует все данные и настройки Сервера, после чего посылает на SQL-сервер команду создать резервную копию базы событий.

Для создания резервной копии нужно указать только один параметр — папку назначения. В заданной папке для каждой резервной копии создается подпапка, имя которой содержит дату и время создания. По умолчанию используется папка **SC_Backup** в каталоге данных Сервера администрирования *(%ProgramData%***KasperskySC\SC_Backup**).

Недостаток хранения копий на том же диске, что и сам Сервер администрирования в том, что аппаратный сбой может повредить сразу и работающую систему, и резервную копию. Безопаснее хранить резервные копии отдельно. Администратор может либо сразу указать сетевую папку назначения, либо настроить перенос резервных копий внешними средствами.

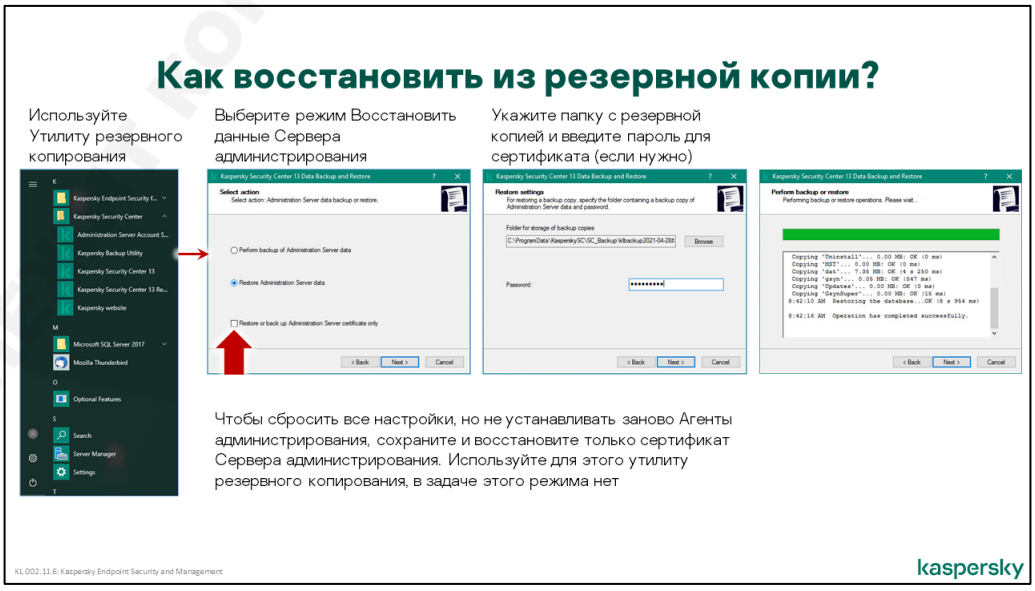
Важно понимать, что копирование данных и настроек Сервера выполняется с правами Сервера администрирования, а копирование базы данных — справами Сервера баз данных. Если в качестве папки для резервных копий указан сетевой путь, нужно обеспечить доступ к этой сетевой папке и Серверу администрирования, и SQL-серверу. Естественно, на указанном диске должно быть достаточно свободного места.

Поскольку резервная копия может занимать до нескольких гигабайт, в зависимости от размера сети и параметров хранения событий, имеет смысл ограничить количество хранимых резервных копий. По умолчанию в параметрах задачи установлено ограничение в 3 резервные копии.

Сертификат Сервера администрирования при сохранении шифруется. Это делается из соображений безопасности, чтобы злоумышленник не смог использовать его для перехвата управления клиентскими компьютерами. Для шифрования нужно указать пароль. По умолчанию он пустой.

Стандартное расписание у задачи резервного копирования — каждые два дня в 2 часа ночи — следовательно, по умолчанию будут храниться резервные копии только за шесть последних дней.

Как восстановить данные из резервной копии



Для восстановления из резервной копии специальной задачи нет. Это продуманное решение, принятое, чтобы избежать случайных запусков восстановления, которые могут привести к потере данных и настроек, сделанных после создания резервной копии.

Для восстановления Сервера администрирования используется уже упомянутая утилита **klbackup.exe**, которую можно открыть через меню *Пуск*. При запуске без параметров она выполняется в режиме пошагового мастера, который запрашивает путь к резервной копии и пароль для расшифровки сертификата. Путь к резервной копии для восстановления отличатся от пути для создания резервных копий на имя подкаталога с конкретной резервной копией. Например, если путь для создания резервной копии был **c:\backups**, путь для восстановления будет наподобие *c:\backups\klbackup2018-12-27#02-00-02*

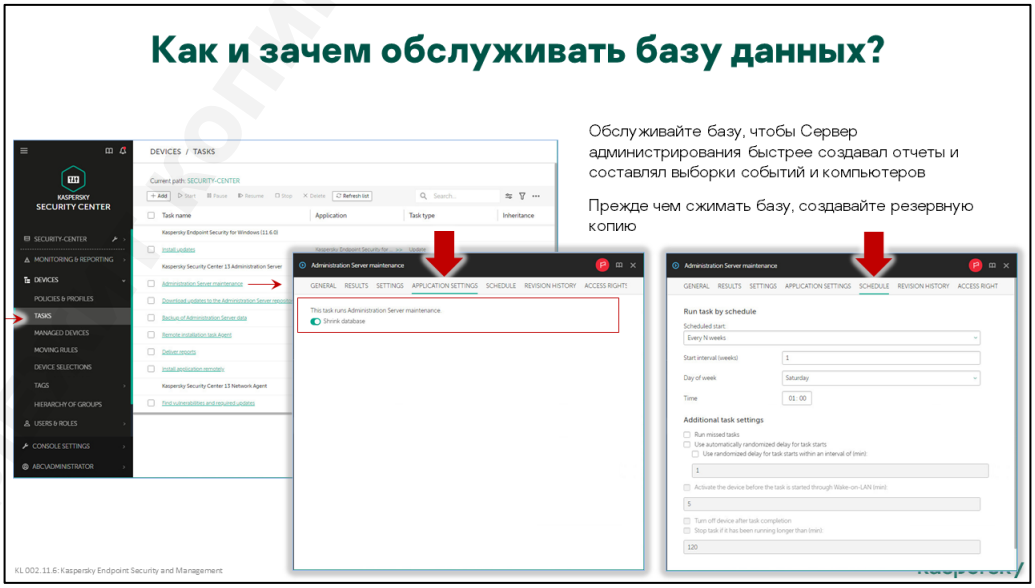
Утилита резервного копирования может использоваться не только для восстановления, но и для создания резервных копий. Для этого на шаге **Выберите действие** нужно выбрать **Выполнить резервное копирование данных Сервера администрирования**.

На этом же шаге можно включить режим, когда сохраняться и восстанавливаться будет только сертификат Сервера администрирования. Этот режим можно использовать, например, чтобы восстановить только связь между Агентами и Сервером, а структуру и настройки создать с нуля. В задаче этот режим недоступен.

Утилиту **klbackup.exe** можно запускать из командной строки с параметрами:

- **–path** — параметр для задания пути к резервной копии
- –**restore** — параметр, указывающий на то, что нужно выполнить восстановление, без него утилита выполнит создание копии
- –**use_ts** — с этим параметром утилита будет создавать копию в подкаталоге со временем и датой создания копии (как в режиме мастера или в режиме задачи), без него — непосредственно в указанном каталоге
- –**password** — параметр для задания пароля, используемого для шифрования сертификата

Как и зачем обслуживать базу данных



Со временем база сервера администрирования может начать «тормозить». В частности, консоль долго создает отчеты, а списки событий или компьютеров показывает после заметной паузы.

Чтобы ускорить работу консоли с событиями в базе, базу нужно оптимизировать. До Kaspersky Security Center 10 SP2 оптимизировать базу нужно было средствами сервера баз данных. В Kaspersky Security Center 10 SP2 появилась специальная задача **Обслуживание базы данных**, которая оптимизирует базу Сервера администрирования на сервере Microsoft SQL. Базу на сервере MySQL задача не поддерживает. Если у вас MySQL, оптимизируйте базу средствами сервера баз данных.

Чтобы база Сервера администрирования работала быстрее, задача **Обслуживание базы данных**:

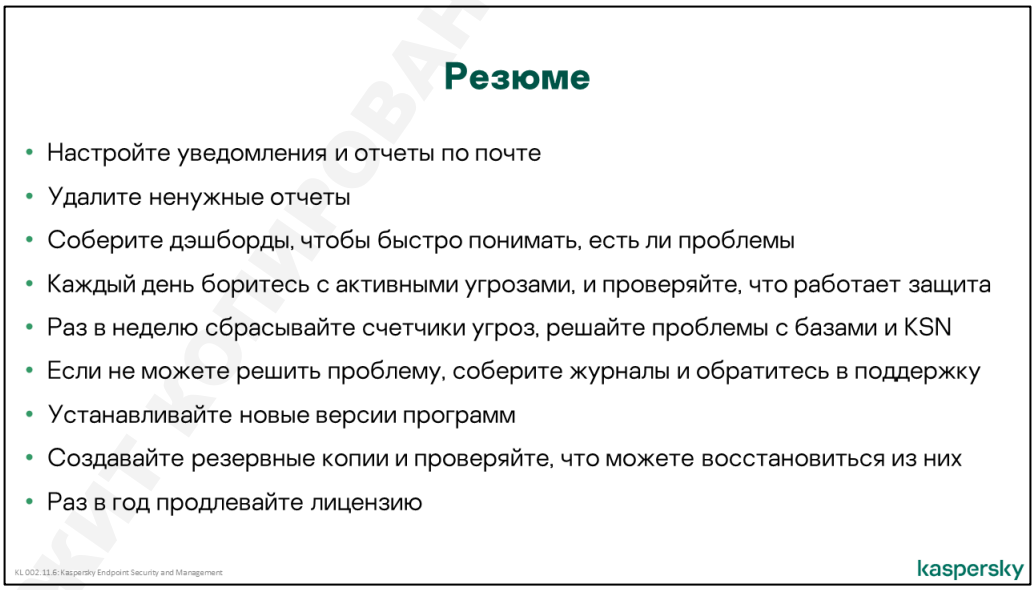
- Ищет и устраняет ошибки в базе
- Перестраивает индексы
- Обновляет статистику базы
- Опционально уменьшает размер базы

Параметров у задачи почти нет. Кроме расписания, есть единственная опция **Сжать базу данных**, которая уменьшает размер базы. Рекомендуется оптимизировать базу раз в неделю.

Если Сервер администрирования работает медленно, потому что у него мало ресурсов, задача **Обслуживание базы данных** ничем не поможет

Задача **Обслуживание базы данных** может быть только одна. Ее создает мастер первоначальной настройки. По умолчанию задача запускается по субботам в час ночи.

4.4 Сопровождение: резюме



Чтобы защита работала и защищала компьютеры, следите за важными событиями:

- Настройте уведомления о возможно зараженных компьютерах
- Настройте отчеты себе в почтовый ящик
- Организуйте ежедневный осмотр состояния защиты: подготовьте панель мониторинга

Серьезные инциденты, такие как заражение, разбирайте немедленно. Менее важные проблемы устраняйте раз в неделю. Не давайте им накапливаться, иначе среди них будет сложно заметить важное.

Если проблема не решается, обращайтесь в техническую поддержку. Чтобы получить ответ раньше и более точный, соберите журналы и приложите их к запросу.

Устанавливайте обновления и новые версии. Они исправляют ошибки, улучшают производительность и улучшают защиту.

Делайте резервные копии данных Сервера администрирования. Регулярно проверяйте, что можете восстановить данные из копии.

Не забывайте продлевать лицензию. Настройте статусы и уведомления, чтобы заранее знать, когда она закончится.