Реагирование на алерты и инциденты

> Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

Одним из шагов расследования алерта или инцидента является реагирование, направленное на сдерживание (Containment) угрозы/злоумышленника или устранение (Eradication) угрозы.

Сдерживание (Containment)

Цель: Ограничить распространение угрозы/злоумышленника и минимизировать ущерб.

Примеры возможных действий:

- Изоляция зараженных систем/сетевых сегментов/хостов.
- Блокировка вредоносных IP-адресов или доменов.
- Временное отключение сервисов, если это необходимо.

Устранение (Eradication)

Цель: Полностью устранить причину инцидента.

Примеры возможных действий:

- Удаление вредоносного ПО или вредоносных скриптов.
- Закрытие уязвимостей, которые были использованы злоумышленниками.
- Обновление систем и приложений до актуальных версий.
- Смена скомпрометированных учетных данных (паролей, ключей).

За счет интеграции с другими решениями KUMA позволяет производить действия по реагированию:

- Реагирование через Kaspersky Security Center:
  - Запуск обновления антивирусных баз и модулей Kaspersky Endpoint Security для Windows или Linux;
  - Запуск задачи поиска вредоносного ПО.
- Реагирование через KEDR:

    - Управление сетевой изоляцией активов.
    - Управление правилами запрета (по хеш-сумме файла).
    - Запуск программы.
- Реагирование через KICS for Networks:
    - Изменение статуса устройства на Разрешенное
    - Изменение статуса устройства на Неразрешенное
- Реагирование через Active Directory:
    - Добавление учетной записи в группу.
    - Удаление учетной записи из группы.
    - Сброс пароля учетной записи.
    - Блокировка учетной записи.
- Выполнение произвольного скрипта на сервере коррелятора KUMA.

Действия по реагированию могут запускаться вручную из веб-интерфейса KUMA или автоматически с помощью правил реагирования.

> Статья онлайн-справки «Интеграция с другими решениями»
> https://support.kaspersky.ru/kuma/4.0/217927

> Статья KUMA Community «Реагирование» (доступны «кастомные» интеграции со сторонними решениями):
> https://kb.kuma-community.ru/books/integracii/chapter/reagirovanie

Ниже рассмотрен пример ручного реагирования средствами Kaspersky Security Center.

Создание задач в Kaspersky Security Center

Предварительно выполните шаги по настройке интеграции с Kaspersky Security Center, описанные в Статье Интеграция с Kaspersky Security Center.

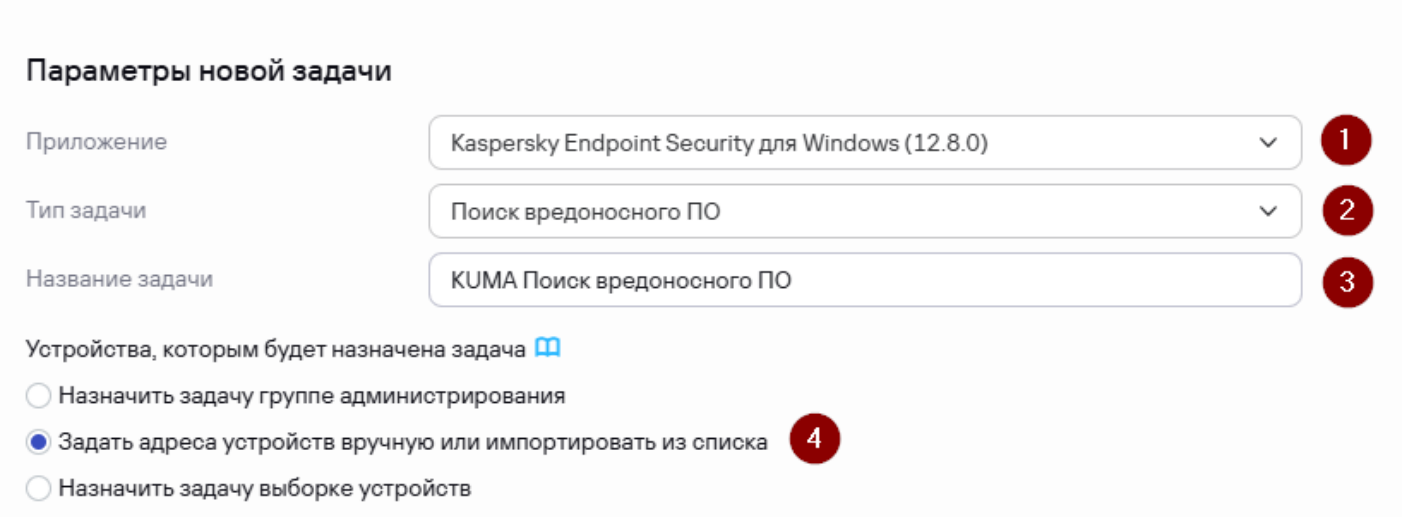
Вы можете вручную или автоматически запускать на активах Kaspersky Security Center, импортированных в KUMA, задачу обновления антивирусных баз и модулей программы и задачу поиска вредоносного ПО. На активах должны быть установлены программы Kaspersky Endpoint Security для Windows или Linux.

Предварительно на стороне Kaspersky Security Center необходимо создать задачи обновления антивирусных баз и поиска вредоносного ПО.

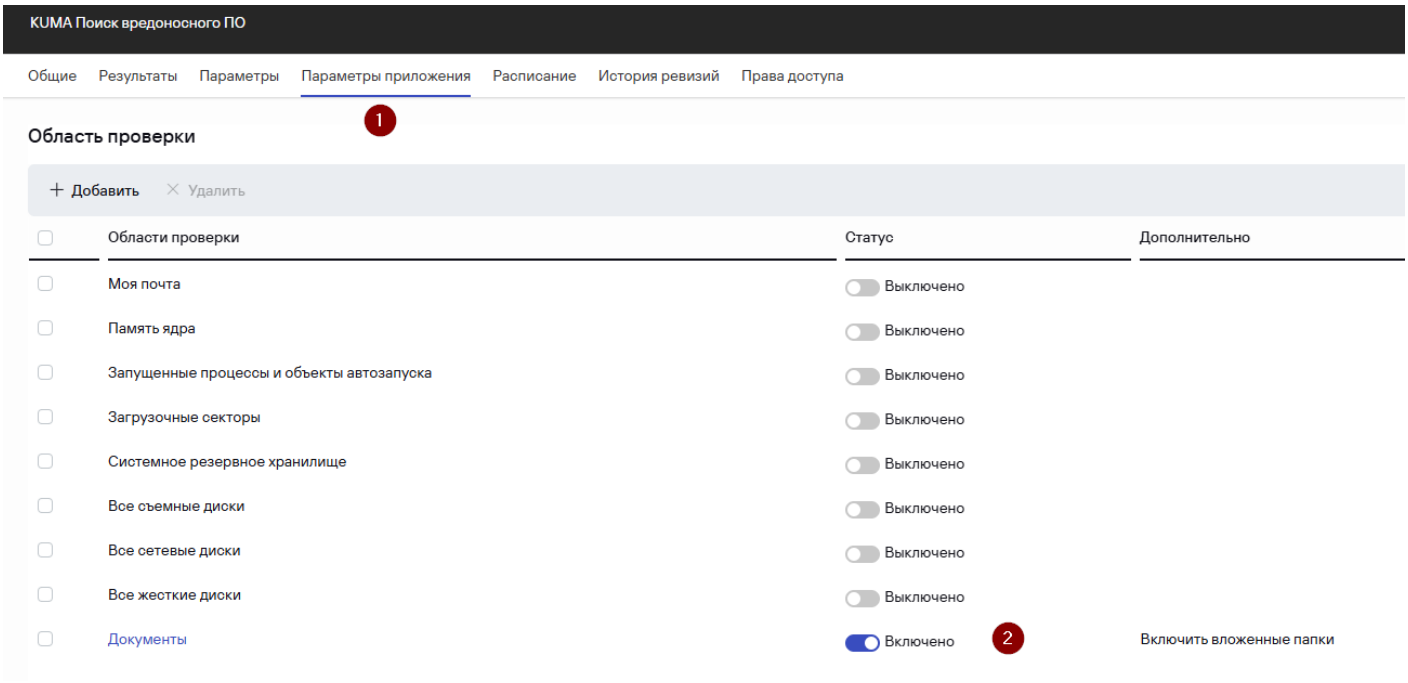
Kaspersky Security Center Web Console

Чтобы создать задачу поиска вредоносного ПО:

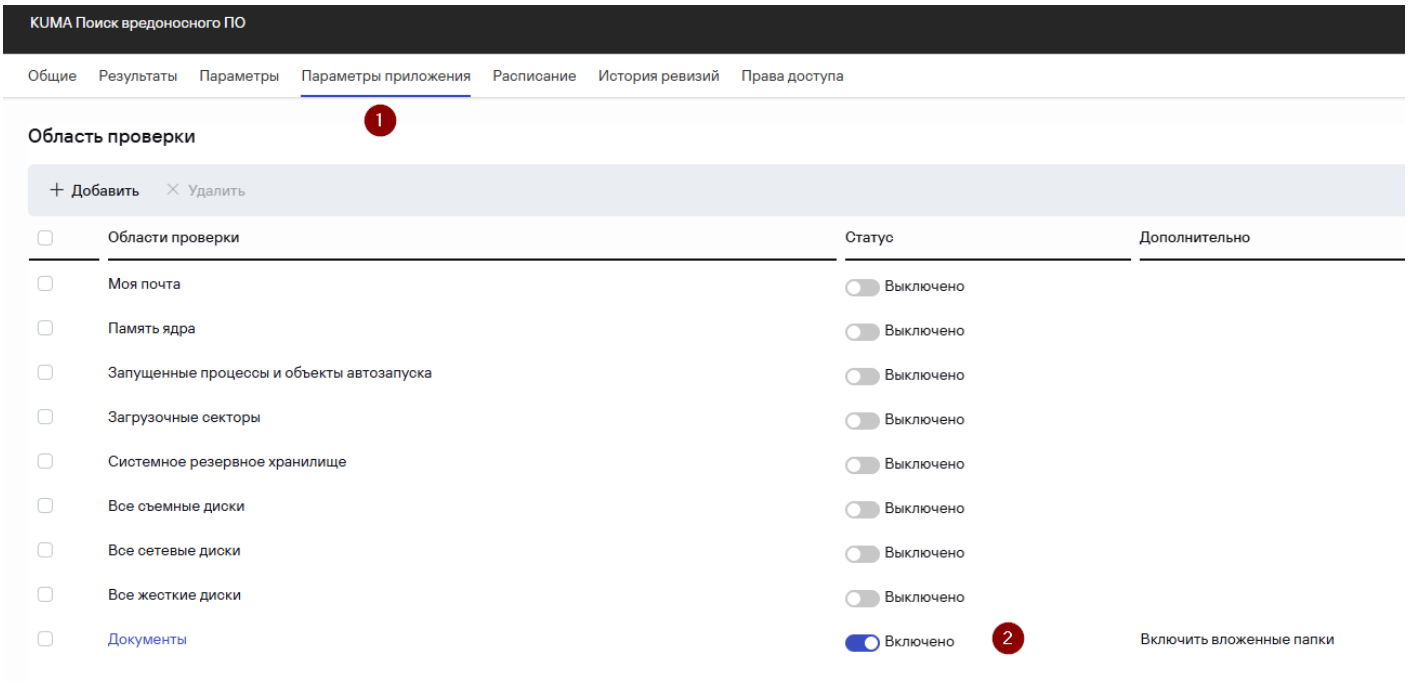
- Выберите **Активы (Устройства)** → **Задачи**.
- В Списке задач нажмите на кнопку **Добавить**.
- Запустится мастер создания задачи.
- Настройте параметры задачи:
  - В раскрывающемся списке **Приложение** выберите используемое приложение Kaspersky Endpoint Security для Windows (в нашем примере 12.8.0).
  - В раскрывающемся списке **Тип задачи** выберите **Поиск вредоносного ПО.**
  - В поле **Название задачи** введите название создаваемой задачи. Важно в названии задачи указать префикс «**KUMA**». Задачи для Kaspersky Endpoint Security с данным префиксом в дальнейшем будут доступны в интерфейсе KUMA.
  - В блоке **Устройства**, **которым будет назначена задача** выберите **Задать адреса устройств вручную или импортировать из списка.**



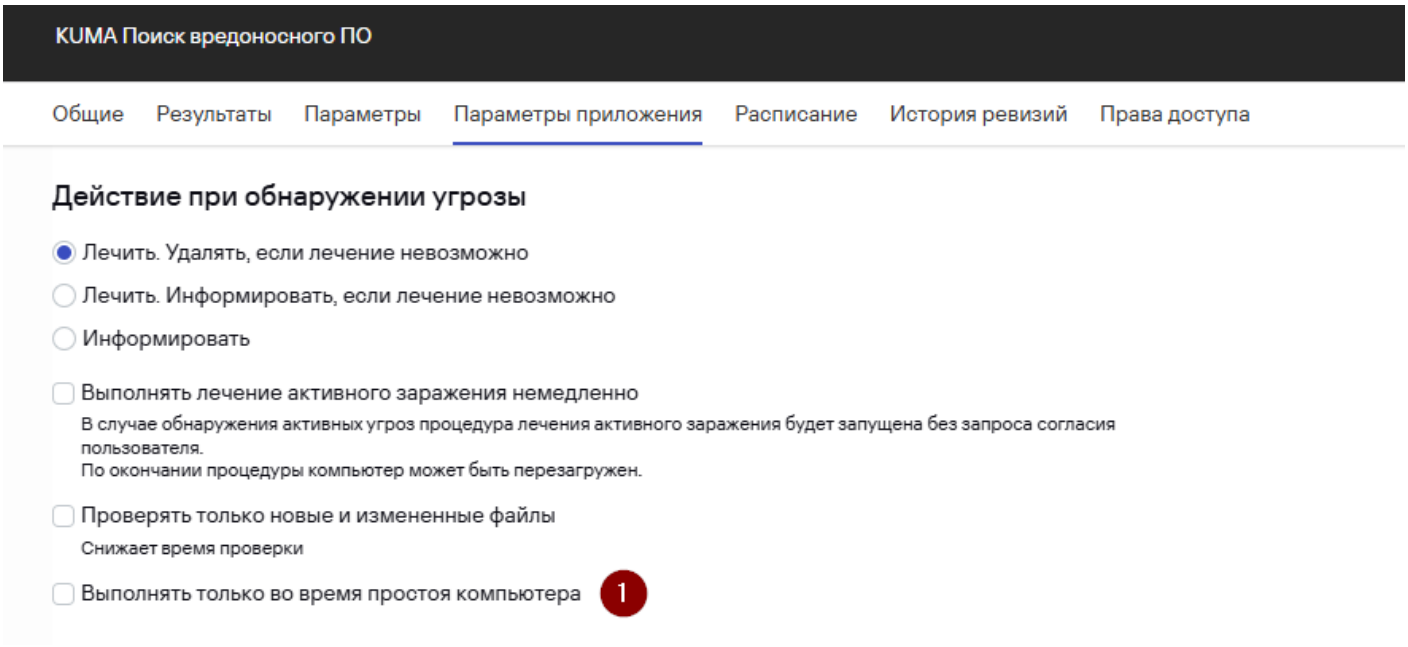
- Нажмите на кнопку **Далее**.
- В окне **Область действия задачи** нажмите **Добавить устройства**. В окне справа **Добавить устройства** выберите **Выбрать устройства, обнаруженные в сети Сервером администрирования**. Для создания задачи можно указать любое устройство. KUMA будет передавать имена устройств, на которых нужно запустить задачу поиска вредоносного ПО.



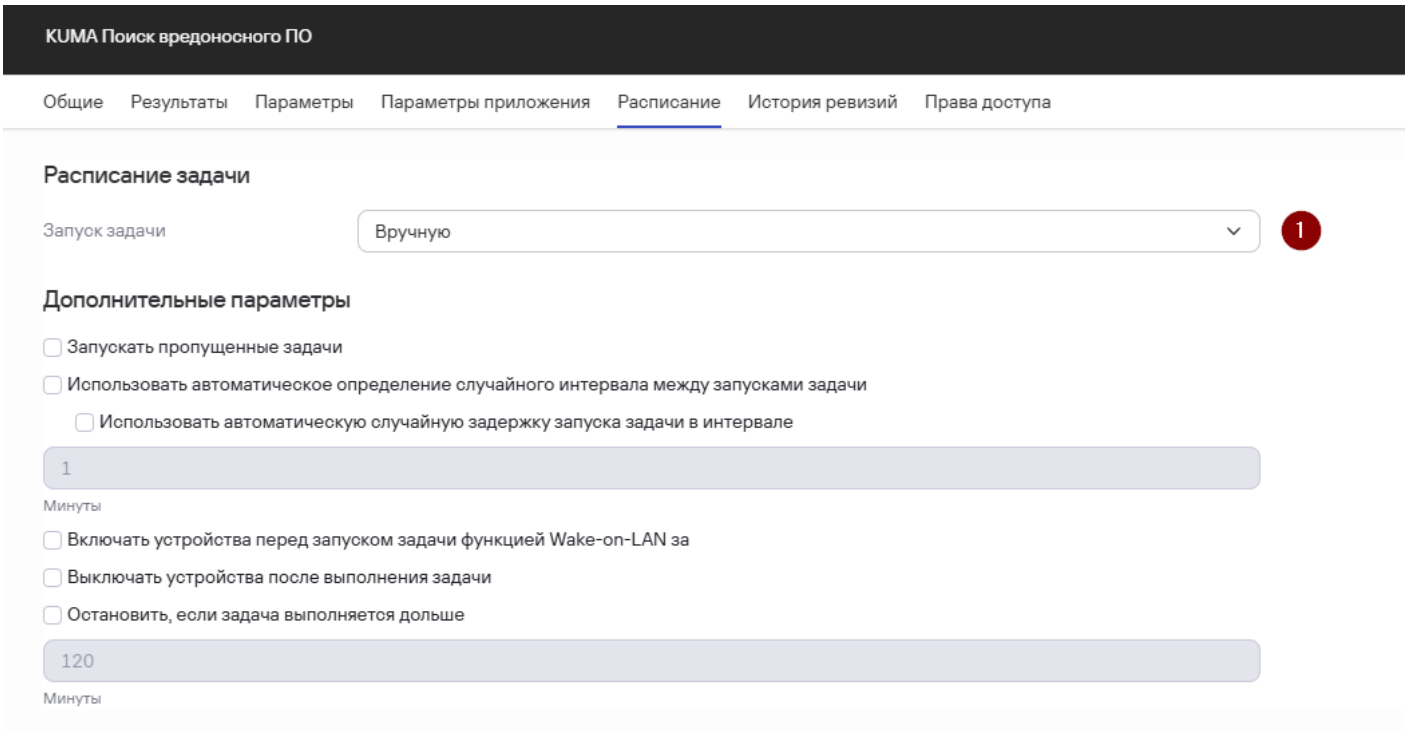
- Нажмите **Добавить** и затем **Далее**.
- В окне **Выбор учетной записи для запуска задачи** укажите **Учетная запись по умолчанию**. Нажмите **Далее**.
- Завершите работу мастера, нажав кнопку **Готово**.
- В открывшемся окне свойств задачи перейдите на вкладку **Параметры приложения** и укажите **Области проверки**. В рамках тестирования можно уменьшить область проверки. В дальнейшем эту настройку можно изменить.



- В секции **Действие при обнаружении угрозы** снимите флажок **Выполнять только во время простоя компьютера**.



- Перейдите на вкладку **Расписание** и убедитесь, что для параметра **Запуск задачи** указано **Вручную**.



- Нажмите **Сохранить**.

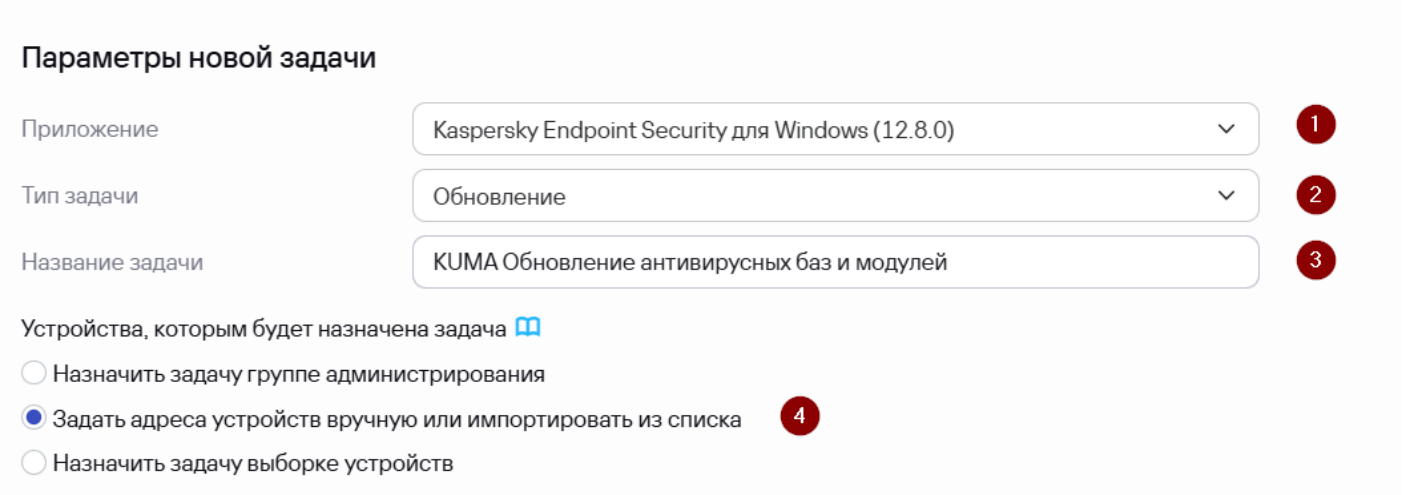
Задача поиска вредоносного ПО создана.

Далее создадим задачу обновления антивирусных баз и модулей.

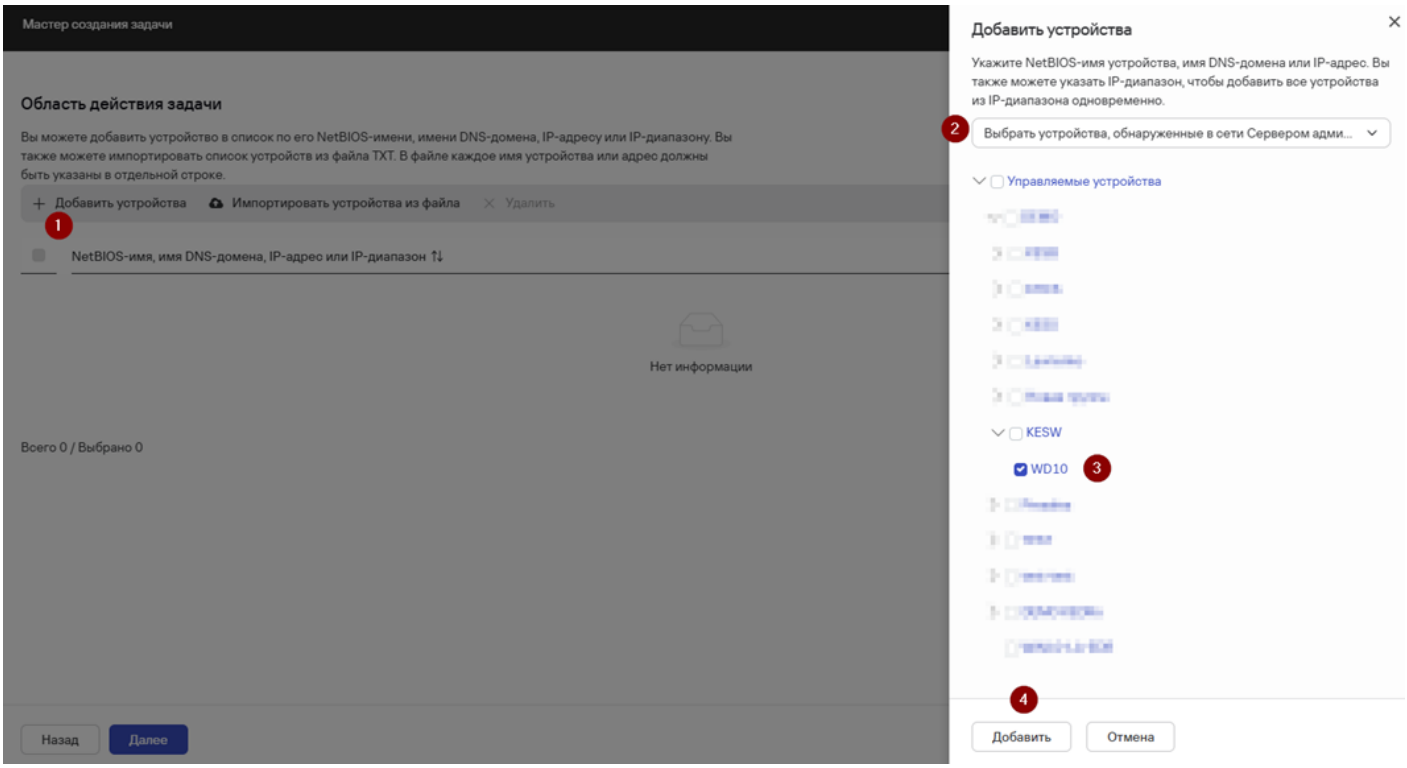
Чтобы создать задачу обновления антивирусных баз и модулей:

- Выберите **Активы (Устройства)** → **Задачи**.
- В **Списке задач** нажмите на кнопку **Добавить**

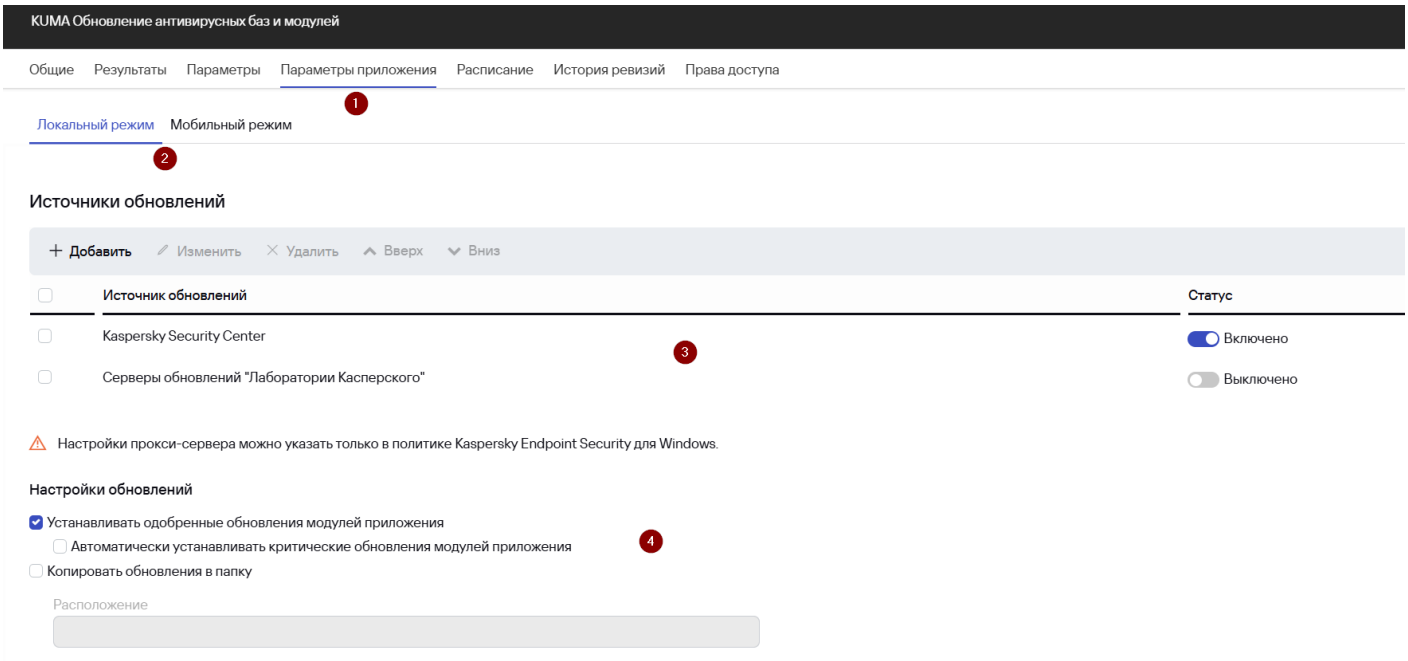
- Запустится мастер создания задачи.
- Настройте параметры задачи:
  - В раскрывающемся списке **Приложение** выберите используемое приложение Kaspersky Endpoint Security для Windows (в нашем примере 12.8.0).
  - В раскрывающемся списке **Тип задачи** выберите **Обновление**.
  - В поле **Название задачи** введите название создаваемой задачи. Важно в названии задачи указать префикс «**KUMA**». Задачи для Kaspersky Endpoint Security с данным префиксом в дальнейшем будут доступны в интерфейсе KUMA.
  - В блоке **Устройства, которым будет назначена задача** выберите **Задать адреса устройств вручную или импортировать из списка**.



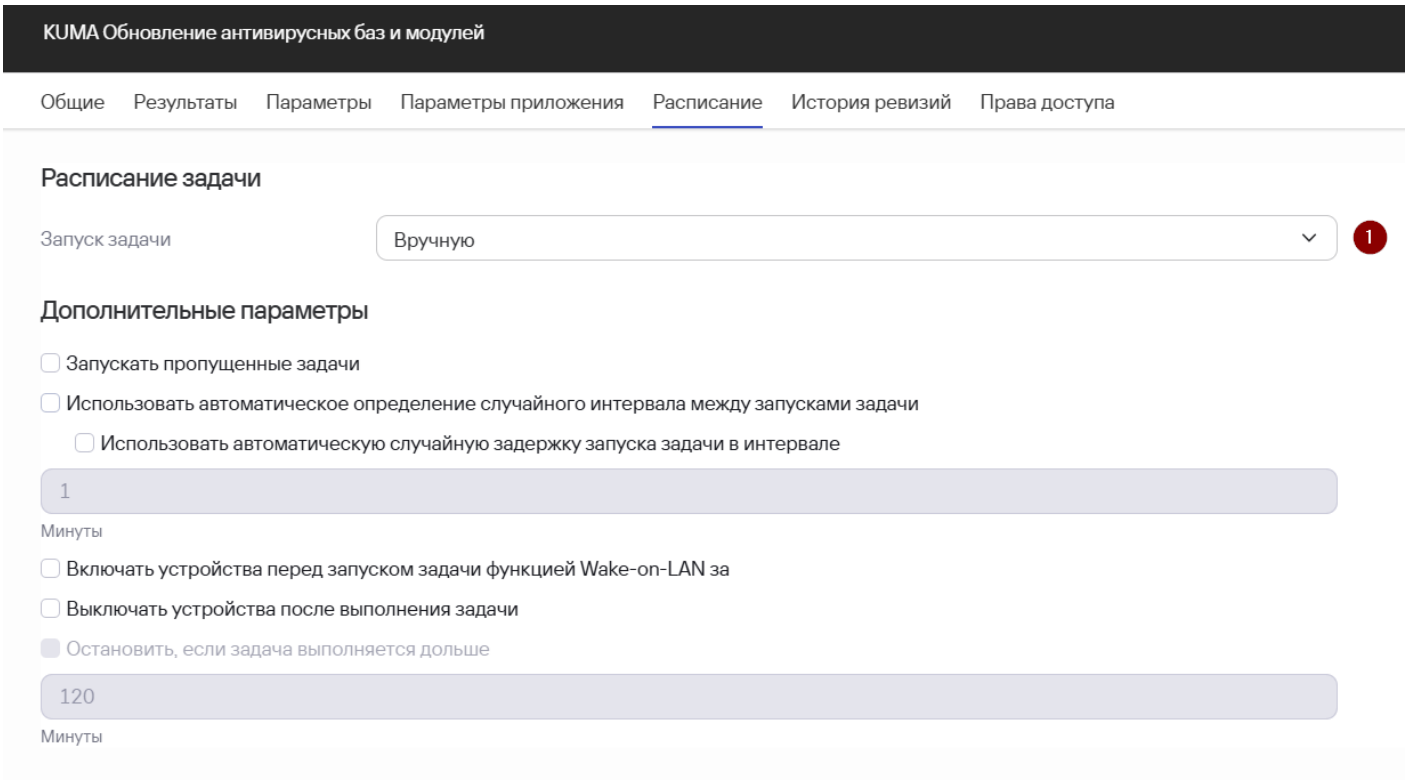
- Нажмите на кнопку **Далее**.
- В окне **Область действия задачи** нажмите **Добавить устройства**. В окне справа **Добавить устройства** выберите **Выбрать устройства, обнаруженные в сети Сервером администрирования**. Для создания задачи можно указать любое устройство. KUMA будет передавать имена устройств, на которых нужно запустить задачу обновления антивирусных баз.



- Нажмите **Добавить** и затем **Далее**.
- В окне **Выбор учетной записи для запуска задачи** укажите **Учетная запись по умолчанию**. Нажмите **Далее**.
- Завершите работу мастера, нажав кнопку **Готово**.
- В открывшемся окне свойств задачи перейдите на вкладку **Параметры приложения** и при необходимости отредактируйте **Источники обновлений** и **Настройки обновлений.**



- Перейдите на вкладку **Расписание** и убедитесь, что для параметра **Запуск задачи** указано **Вручную**.



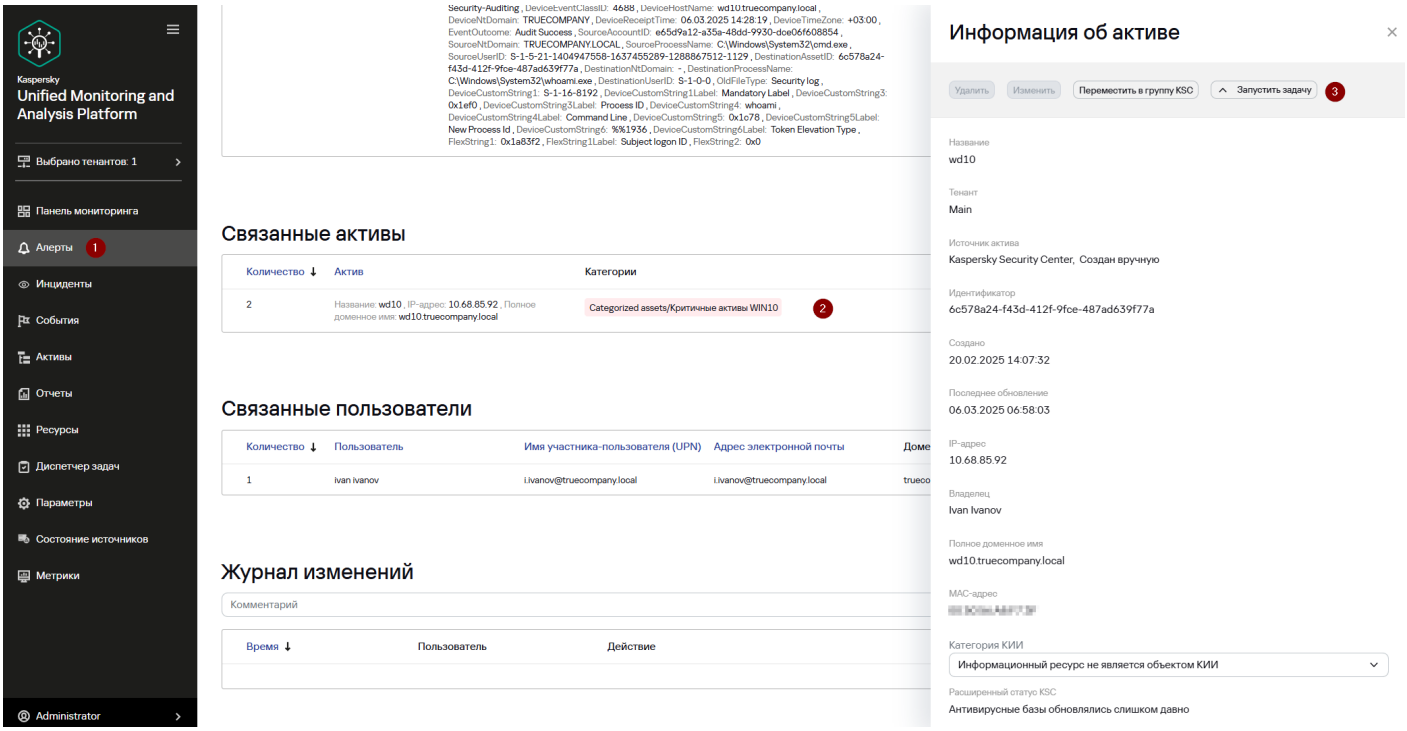
- Нажмите **Сохранить**.

Задача обновления антивирусных баз и модулей создана.

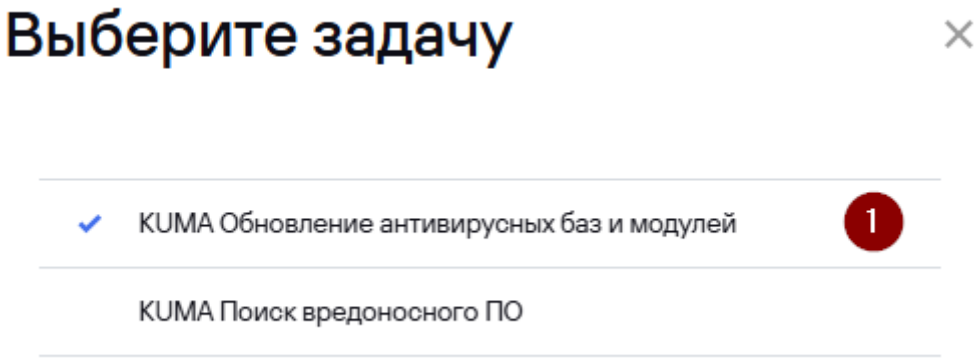
Реагирование вручную средствами Kaspersky Security Center

Чтобы запустить реагирование средствами Kaspersky Security Center вручную:

- Перейдите в **Алерты** и выберите алерт, в рамках которого необходимо запустить действие по реагированию. В нашем примере это алерт **R220_Сбор информации об учетных записях** (см. статью Работа с алертами)
- В карточке алерта в разделе **Связанные активы** выберите актив для запуска задачи.
- В появившемся окне **Информация об активе** нажмите **Запустить задачу**.



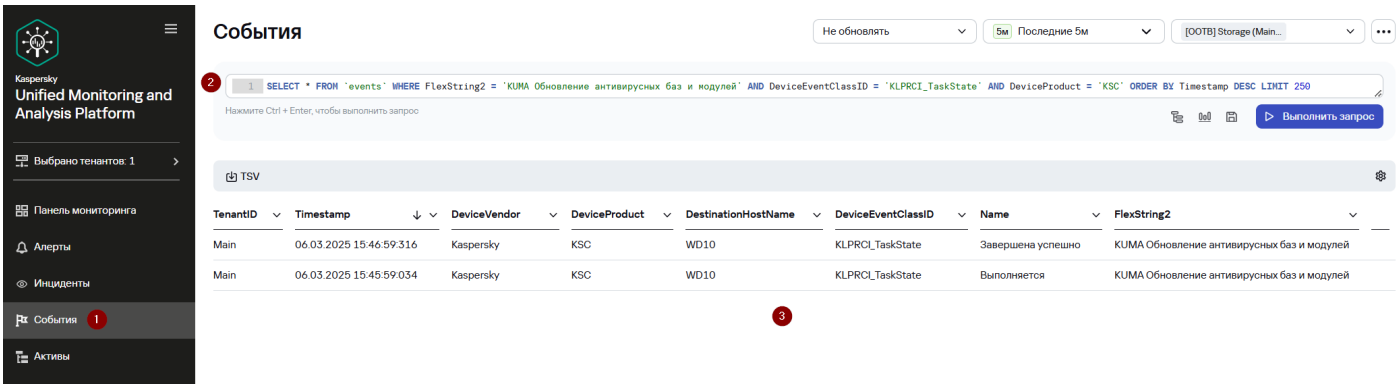
- В раскрывающемся списке выберите **Реагирование KSC** и далее ранее созданную задачу **KUMA Обновление антивирусных баз и модулей** (перед запуском задачи KUMA **Поиск вредоносного ПО** выполним задачу обновления для получения наиболее актуальных сигнатур вредоносного ПО).



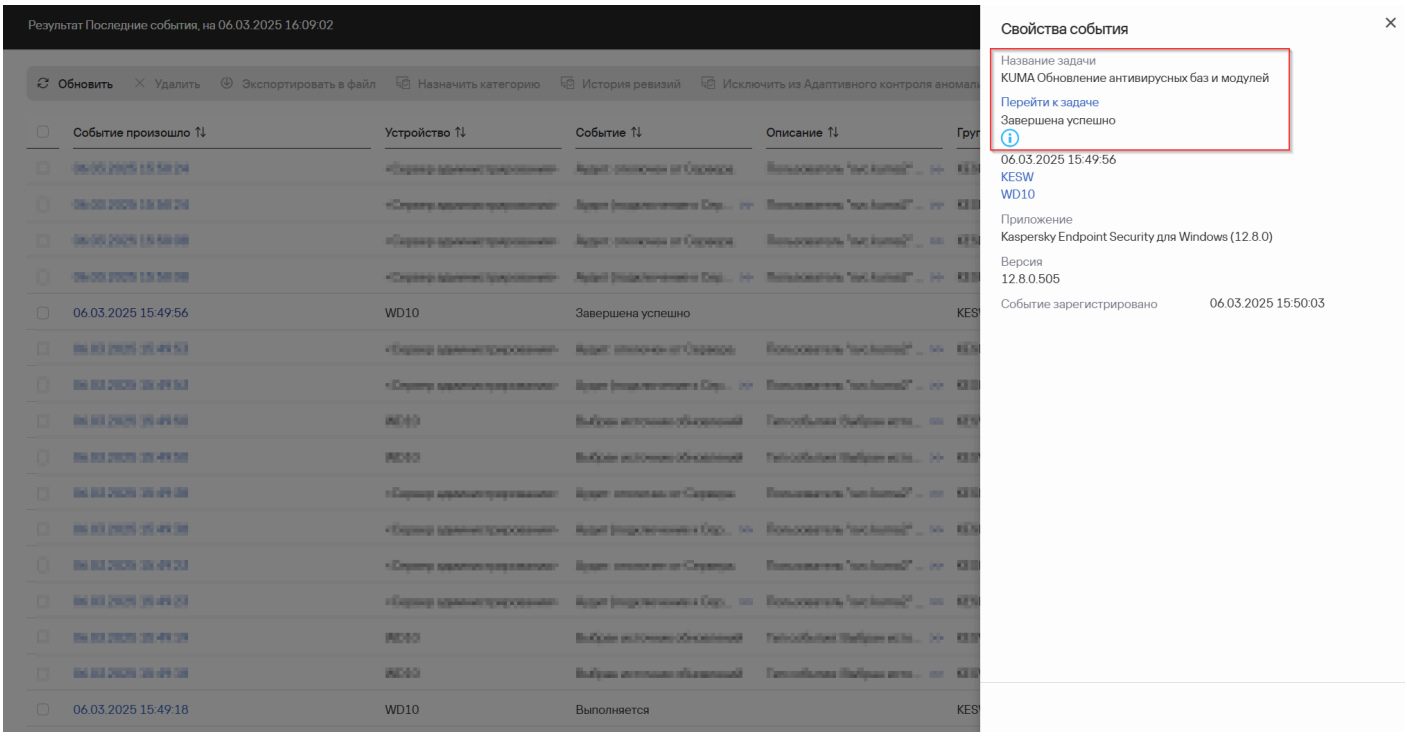
- Нажмите **Запустить**.

Задача обновления на выбранном активе запущена.
Чтобы убедиться, что задача была запущена и завершена успешно перейдите в раздел **События** и выполните следующий поисковый запрос:

```
SELECT * FROM `events` WHERE FlexString2 = 'KUMA Обновление антивирусных баз и модулей' AND DeviceEventClassID = 'KLPRCI_TaskState' AND DeviceProduct = 'KSC' ORDER BY Timestamp DESC LIMIT 250
```

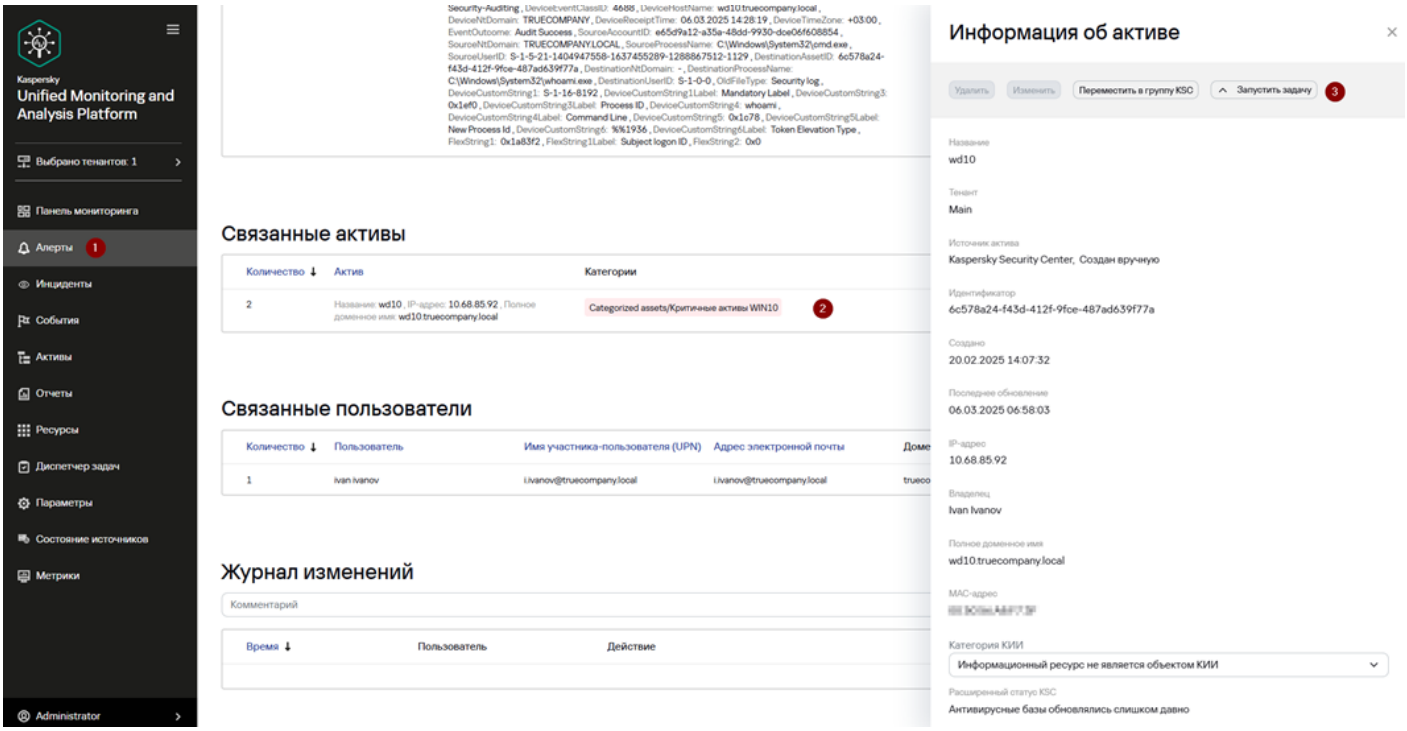


Также статус выполнения задачи можно посмотреть в консоли Kaspersky Security Center или непосредственно в интерфейсе приложения Kaspersky Endpoint Security.

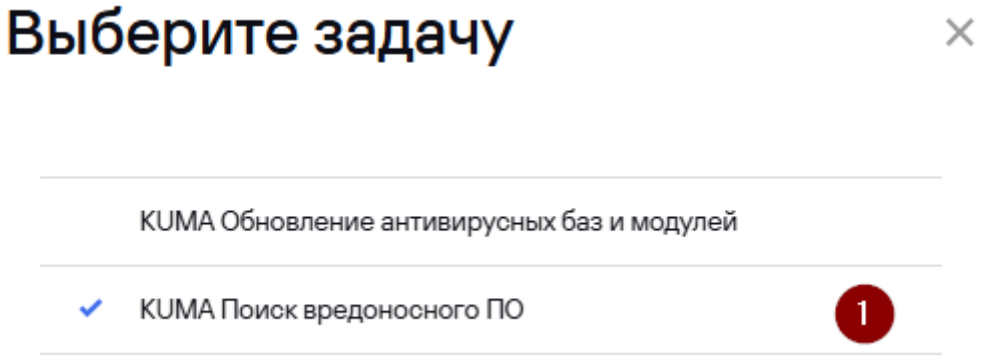


Далее запустите ранее созданную задачу KUMA Поиск вредоносного ПО:

- Перейдите в **Алерты** и выберите алерт, в рамках которого необходимо запустить действие по реагированию. В нашем примере это алерт **R220_Сбор информации об учетных записях**.
- В карточке алерта в разделе **Связанные активы** выберите актив для запуска задачи.
- В появившемся окне **Информация об активе** нажмите **Запустить задачу**.



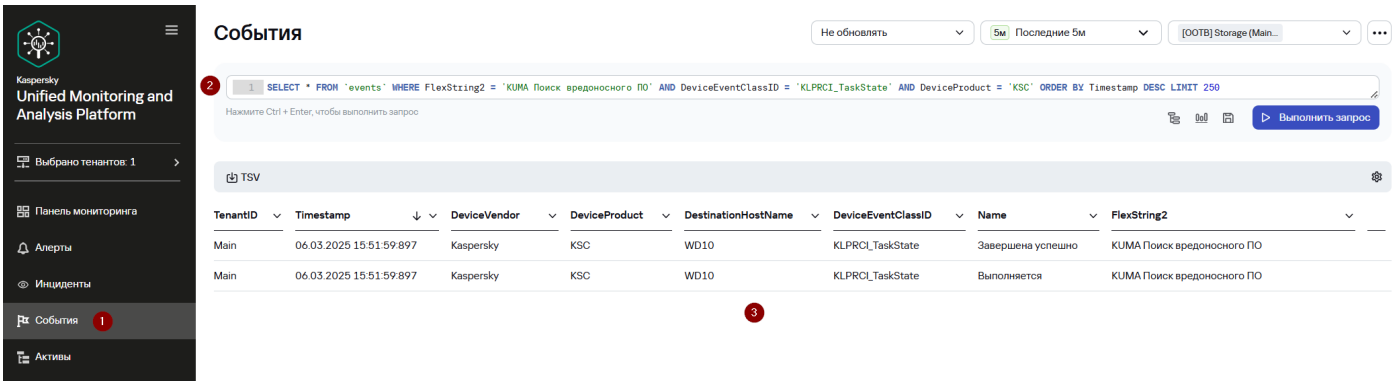
- В раскрывающемся списке выберите **Реагирование KSC** и далее ранее созданную задачу **KUMA Поиск вредоносного ПО**.
- Нажмите **Запустить.**



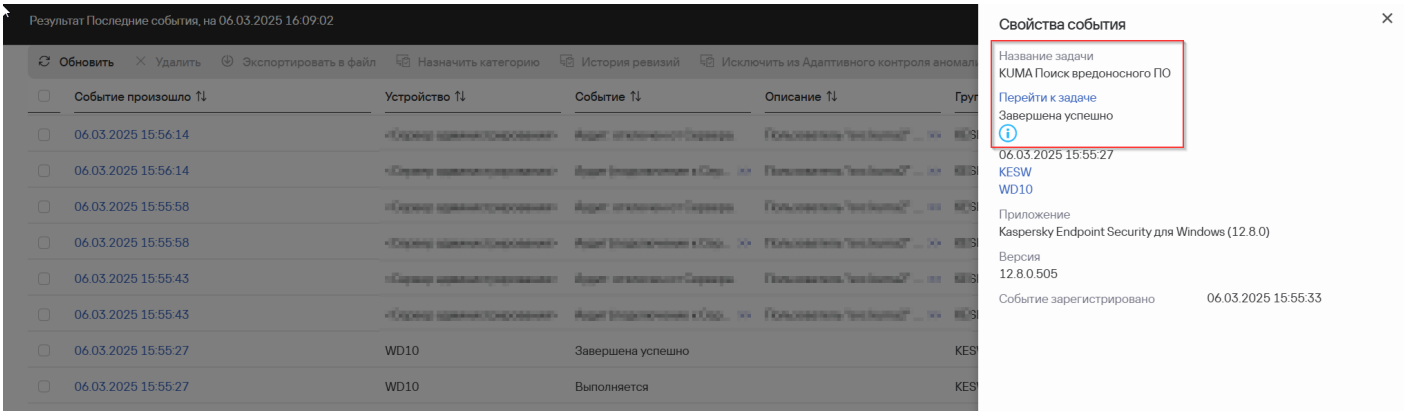
Задача поиска вредоносного ПО на выбранном активе запущена.

Чтобы убедиться, что задача завершена успешно перейдите в раздел **События** и выполните следующий поисковый запрос:

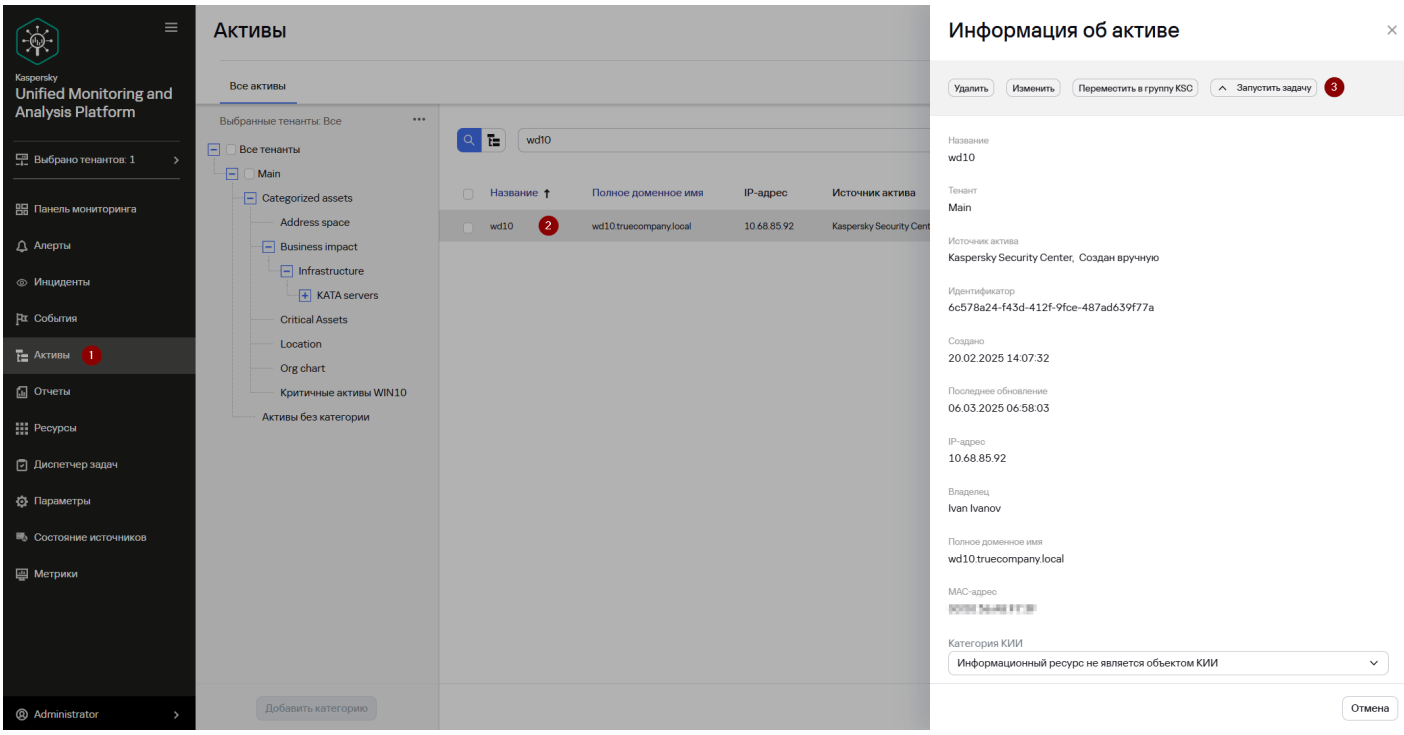
```
SELECT * FROM `events` WHERE FlexString2 = 'KUMA Поиск вредоносного ПО' AND DeviceEventClassID = 'KLPRCI_TaskState' AND DeviceProduct = 'KSC' ORDER BY Timestamp DESC LIMIT 250
```

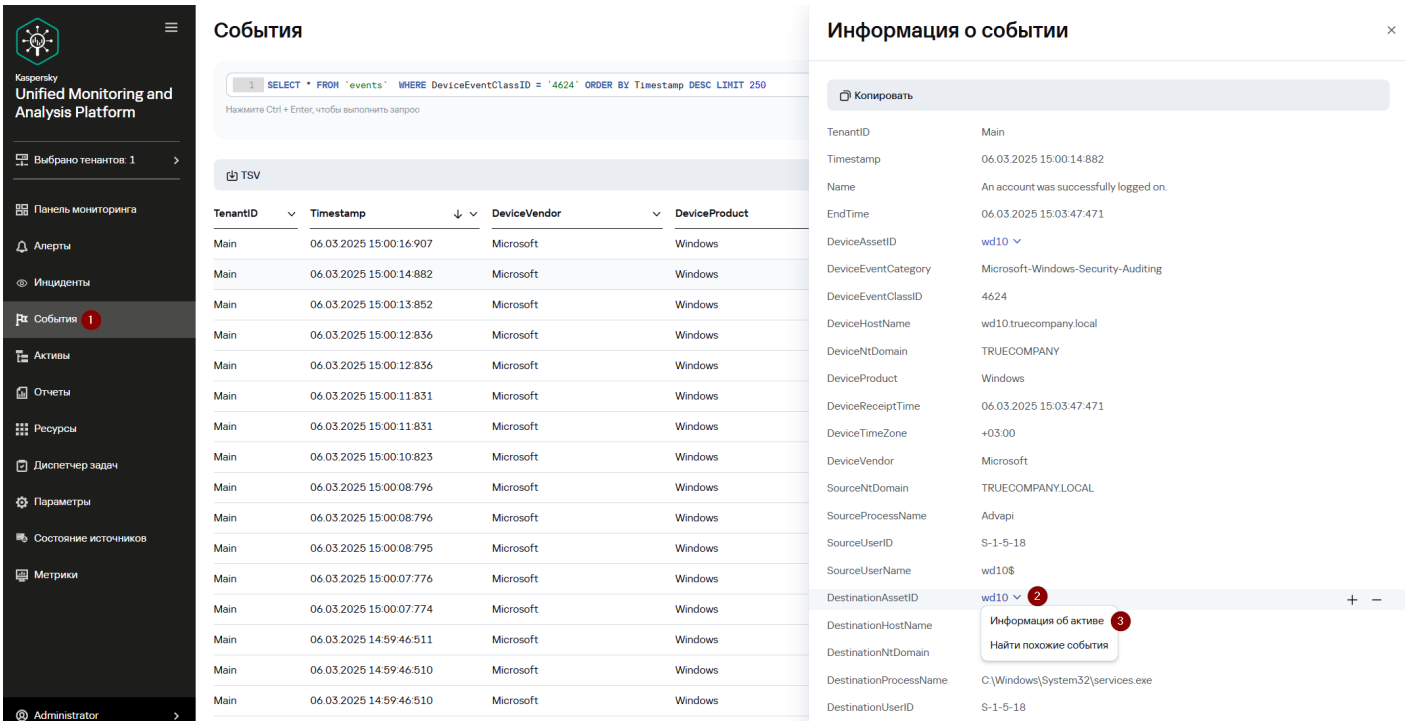


Также статус выполнения задачи можно посмотреть в консоли Kaspersky Security Center или непосредственно в интерфейсе приложения Kaspersky Endpoint Security.



Запускать вручную реагирование средствами Kaspersky Security Center также можно из раздела **Активы**, выбрав соответствующий актив из списка, или из карточки **События**, нажав на имя актива в поле ***AssetID**.





> Статья онлайн-справки «Автоматический запуск задач Kaspersky Security Center»: https://support.kaspersky.ru/kuma/4.0/218008

Revision #3
Created 2026-08-12 11:17:46 UTC by Dmitry Borisov
Updated 2026-08-12 12:56:29 UTC by Dmitry Borisov