# Работа с событиями

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

> Официальная документация по данному разделу приведена в онлайн-справке на продукт: https://support.kaspersky.ru/kuma/4.0/228267

После подключения источников событий вы можете просматривать полученные KUMA события в разделе **События** веб-интерфейса KUMA.

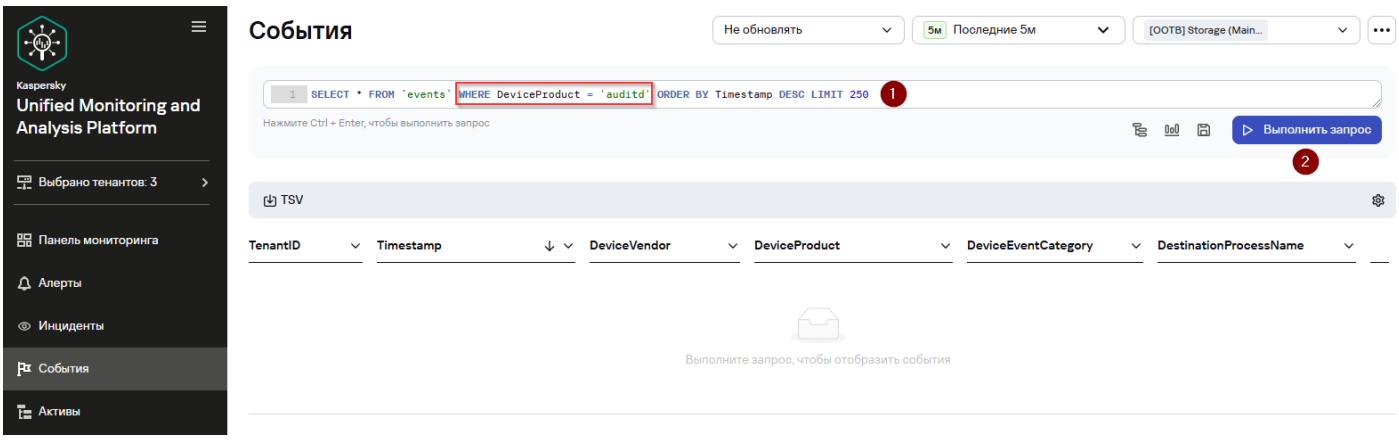
> Видео «Работа с событиями»:
> https://rutube.ru/video/61eaf7b9ba77f32ed778ed174a9693a9/?playlist=540937

# Формирование SQL-запроса

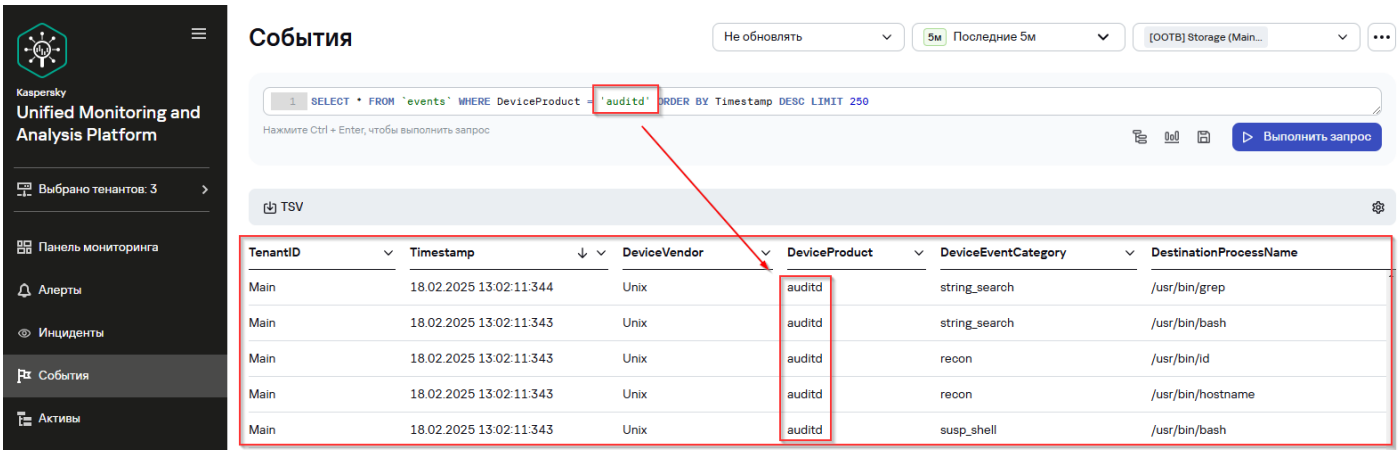
По умолчанию в разделе **События** данные не отображаются. Для просмотра событий в поле поиска нужно задать SQL-запрос и нажать на кнопку **Выполнить запрос**. SQL-запрос можно ввести вручную или сформировать с помощью **конструктора запросов.**

Для создания SQL-запроса вручную:

- Введите SQL-запрос в поле ввода. Используйте одинарные кавычки в запросах.
- Нажмите на кнопку **Выполнить запрос**.

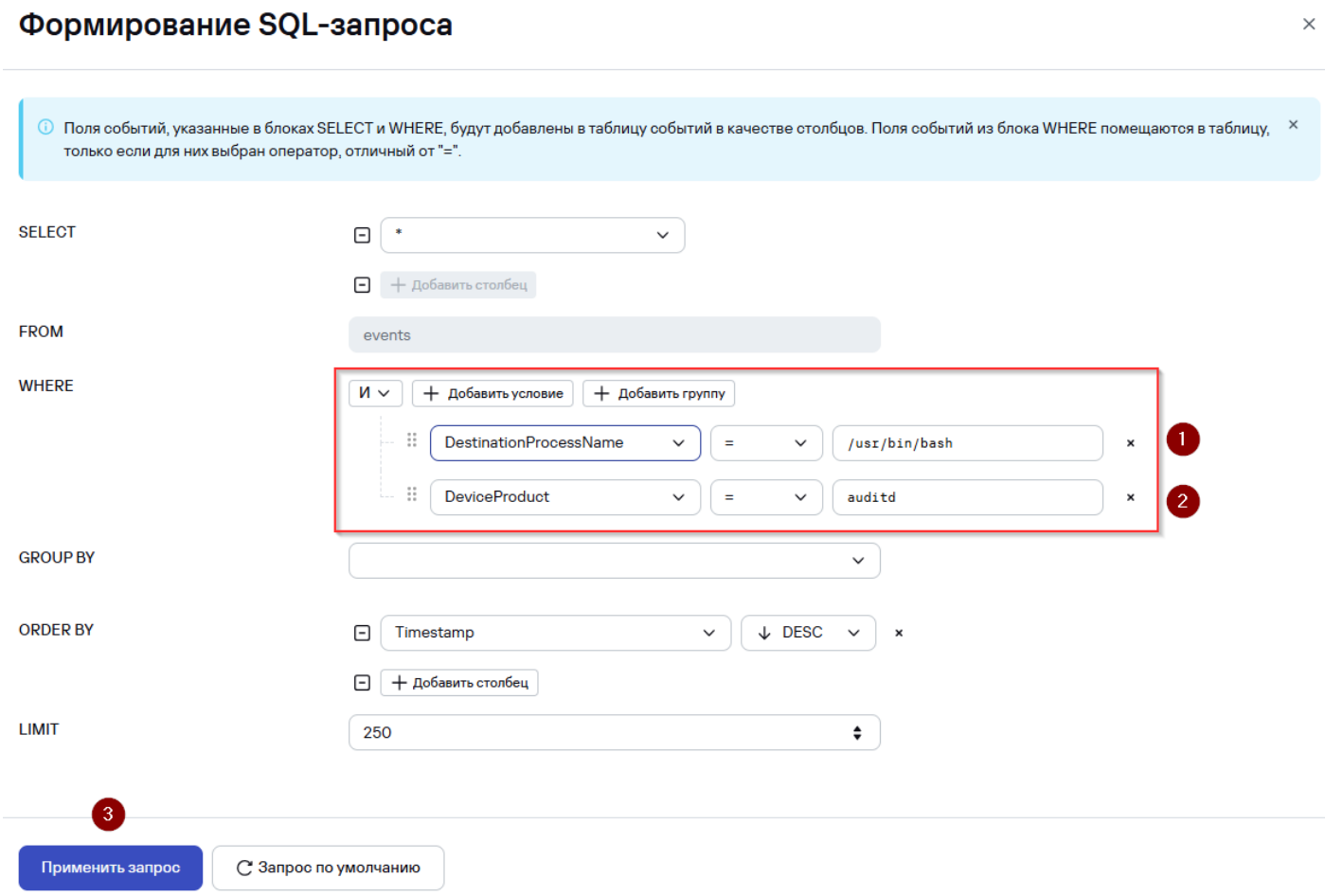



- Отобразится таблица событий, соответствующих условиям вашего запроса.

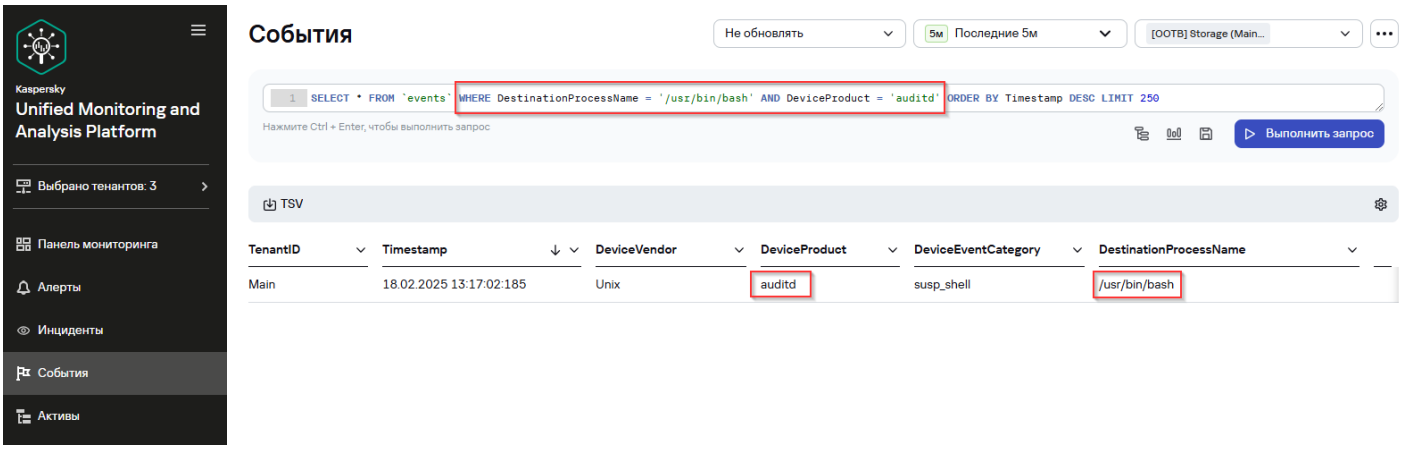



Для создания SQL-запроса с помощью конструктора:

- Нажмите на кнопку ..
- В появившемся окне конструктора запросов сформулируйте поисковый запрос.
- Нажмите на кнопку **Применить запрос.**




- Текущий SQL-запрос будет перезаписан. В поле поиска отобразится сформированный SQL-запрос.
- Для отображения данных в таблице нажмите на кнопку **Выполнить запрос**.
- Отобразится таблица событий, соответствующих условиям вашего запроса.




# Примеры запросов

```
SELECT * FROM `events` WHERE Type IN ('Base', 'Audit') ORDER BY Timestamp DESC LIMIT 250
```

Все события таблицы events с типом Base и Audit, отсортированные по столбцу Timestamp в порядке убывания. Количество отображаемых в таблице строк – 250.

```
SELECT * FROM `events` WHERE BytesIn BETWEEN 1000 AND 2000 ORDER BY Timestamp ASC LIMIT 250
```

Все события таблицы events, для которых в поле BytesIn значение полученного трафика находится в диапазоне от 1000 до 2000 байт, отсортированные по столбцу Timestamp в порядке возрастания. Количество отображаемых в таблице строк – 250.

```
SELECT * FROM `events` WHERE Message LIKE '%ssh:%' ORDER BY Timestamp DESC LIMIT 250
```

Все события таблицы events, которые в поле Message содержат данные, соответствующие заданному шаблону %ssh:% в нижнем регистре, и отсортированы по столбцу Timestamp в порядке убывания. Количество отображаемых в таблице строк – 250.

```
SELECT * FROM `events` WHERE inSubnet(DeviceAddress, '00.0.0.0/00') ORDER BY Timestamp DESC
LIMIT 250
```

Все события таблицы events для хостов, которые входят в подсеть 00.0.0.0/00, отсортированные по столбцу Timestamp в порядке убывания. Количество отображаемых в таблице строк – 250.

```
SELECT * FROM `events` WHERE match(Message, 'ssh.*') ORDER BY Timestamp DESC LIMIT 250
```

Все события таблицы events, которые в поле Message содержат текст, соответствующий шаблону ssh.*, и отсортированы по столбцу Timestamp в порядке убывания. Количество отображаемых в таблице строк – 250.

```
SELECT max(BytesOut) / 1024 FROM `events`
```

Максимальный размер исходящего трафика (КБ) за выбранный период времени.

```
SELECT count(ID) AS "Count", SourcePort AS "Port" FROM `events` GROUP BY SourcePort ORDER BY Port ASC LIMIT 250
```

Количество событий и номер порта. События сгруппированы по номеру порта и отсортированы по столбцу Port в порядке возрастания. Количество отображаемых в таблице строк – 250. Столбцу ID в таблице событий присвоено имя Count, столбцу SourcePort присвоено имя Port.

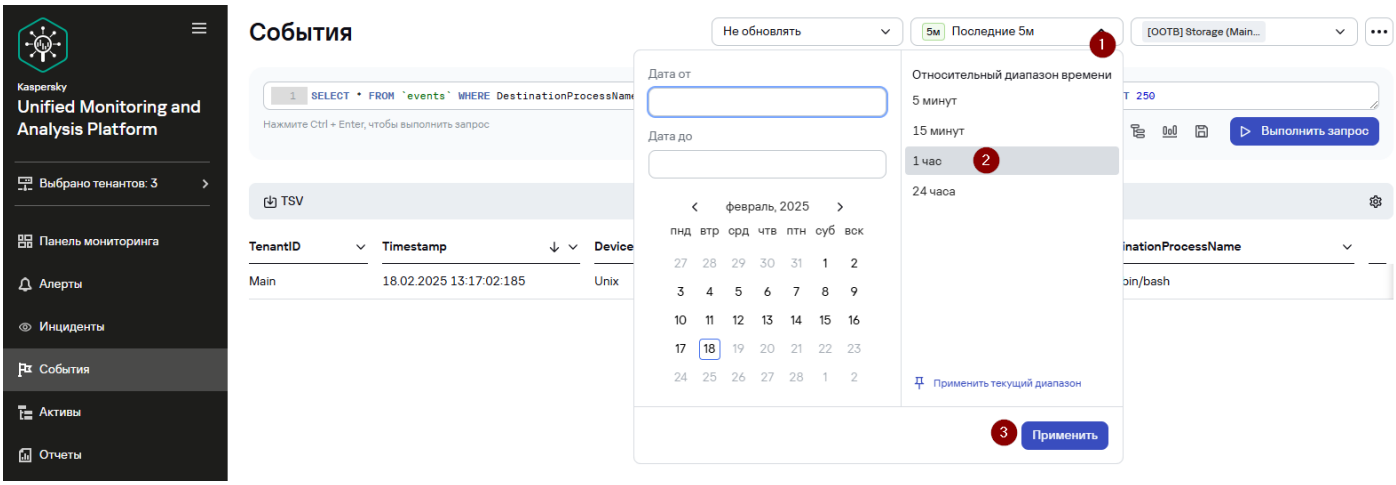
---

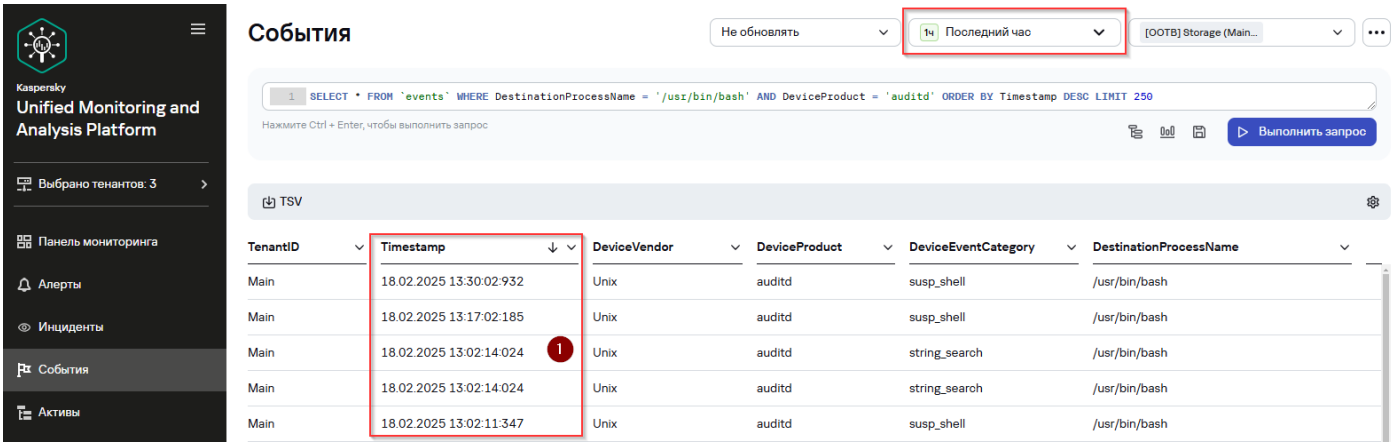
# Фильтрация событий по периоду

В KUMA вы можете настроить отображение событий, относящихся к определенному временному периоду. В предыдущих примерах поиск событий выполнялся за последние 5 минут (диапазон по умолчанию).

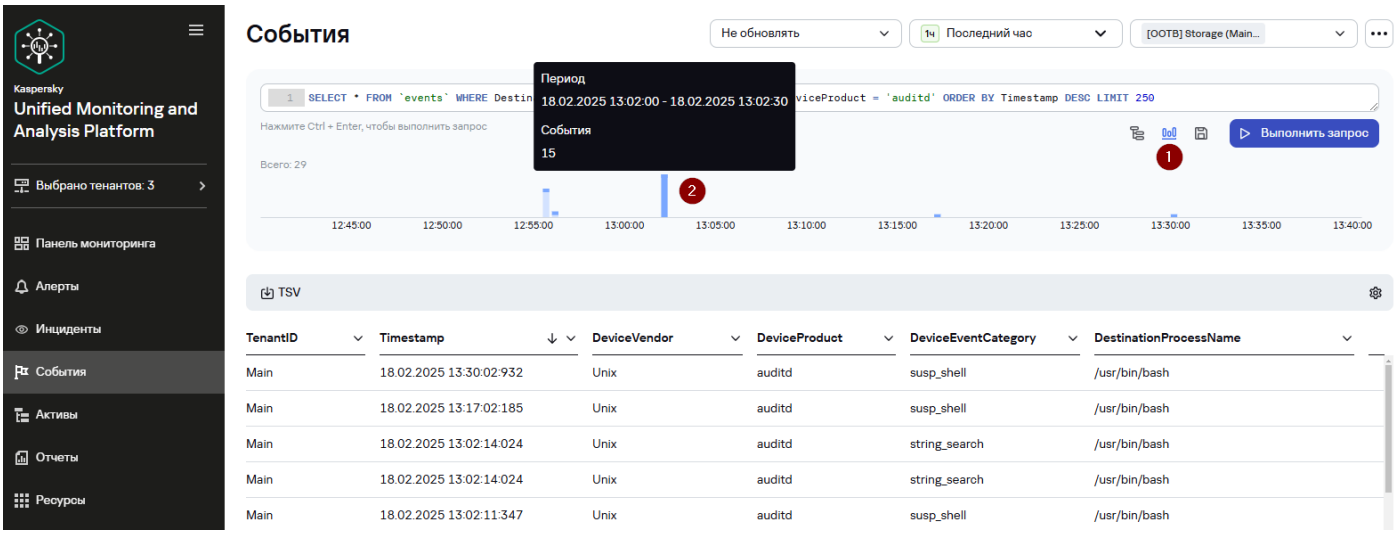
Чтобы отфильтровать события по периоду:

- В разделе **События** веб-интерфейса KUMA в верхней части окна откройте раскрывающийся список временного периода.
- Выполните одно из следующих действий, чтобы выбрать временной период:
  - Если вы хотите выполнить фильтрацию по относительному временному периоду, выберите один из доступных временных периодов в блоке **Относительный диапазон времени** справа. Например, вы можете выбрать временной период 5 минут, 15 минут, 1 час, 24 часа.
  - Если вы хотите выполнить фильтрацию по конкретному временному периоду, в календаре слева выберите дату начала и окончания периода и нажмите на кнопку **Применить**. Формат даты и времени зависит от настроек вашей операционной системы. При необходимости вы также можете указать значения даты вручную в полях **Дата от** и **Дата до**.
- Нажмите на кнопку **Выполнить запрос**.



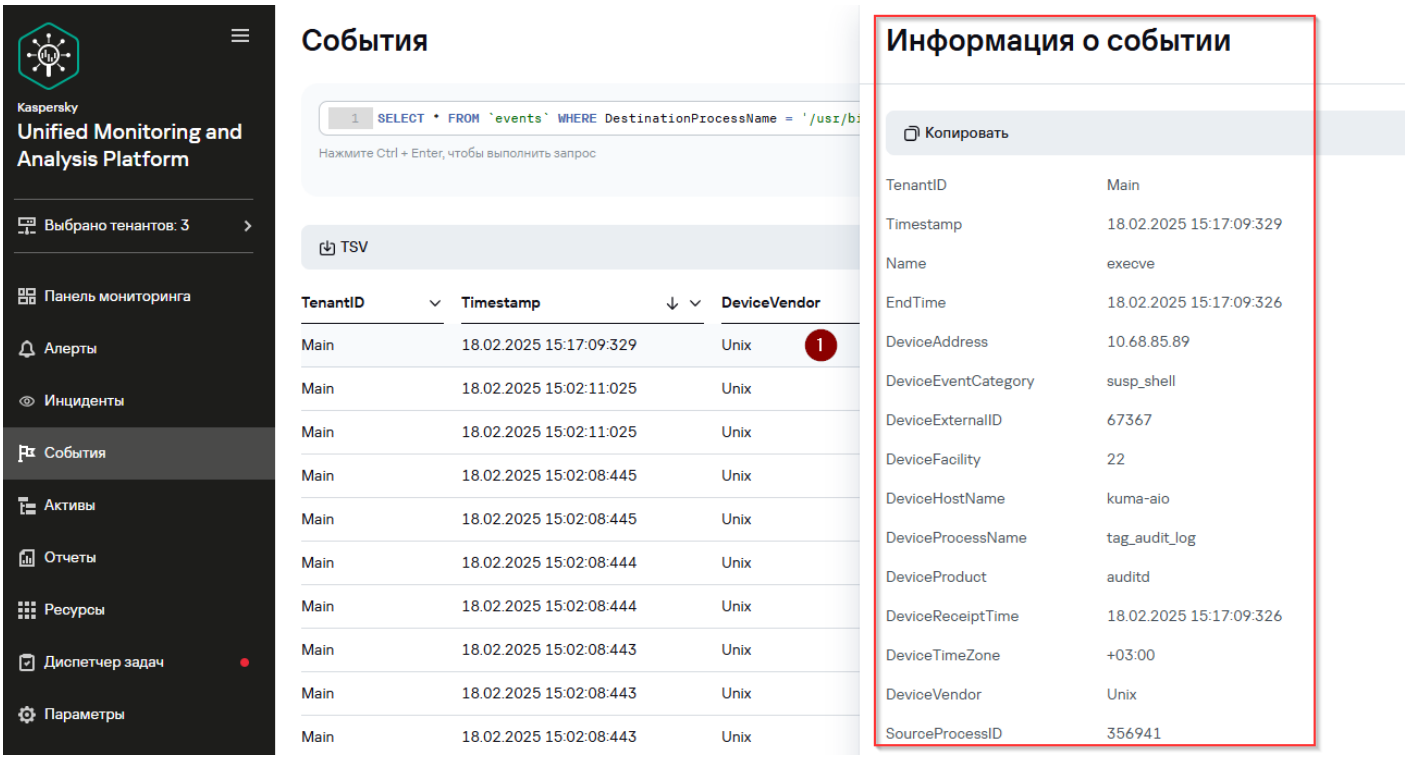

Вы также можете настроить отображение событий с помощью **гистограммы событий**, которая отображается при нажатии на кнопку  в верхней части раздела **События**. События отобразятся, если нажать на нужный столбец данных или выделить требуемый период времени и нажать на кнопку **Показать события**.




# Просмотр информации о событии

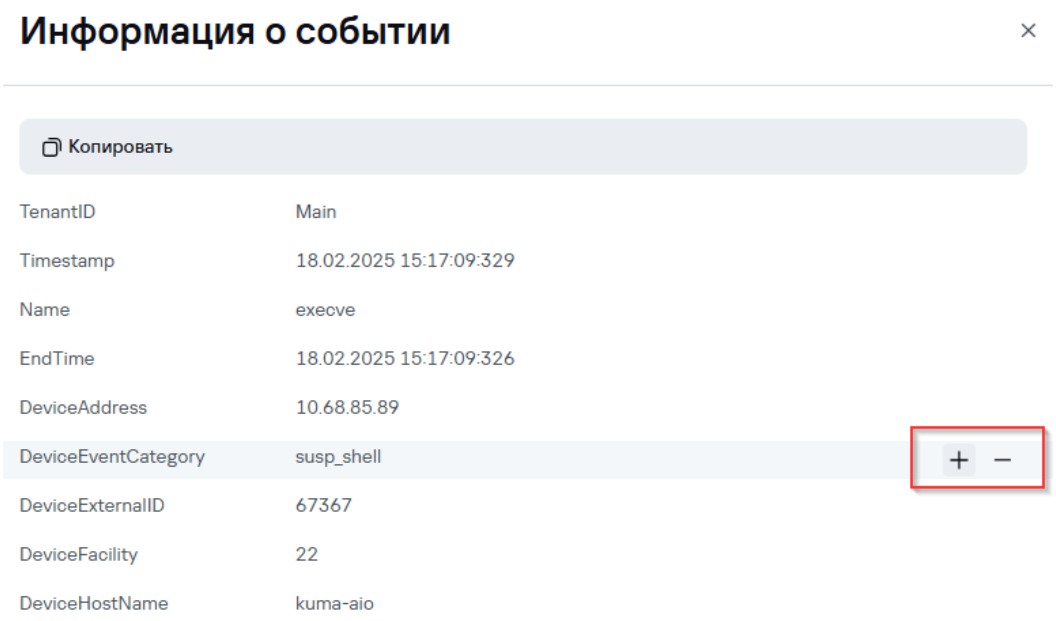
Чтобы просмотреть информацию о событии (карточку события):

- В таблице событий выберите событие, информацию о котором вы хотите просмотреть.
- Откроется окно **Информация о событии** со списком полей события и их значений.

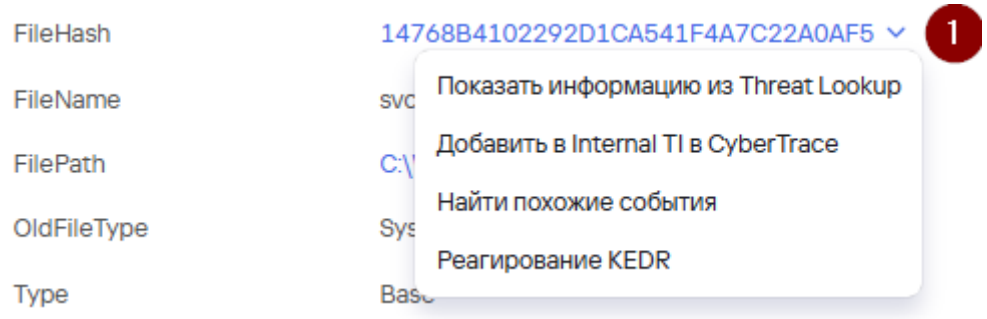



В окне **Информация о событии** доступны следующие действия:

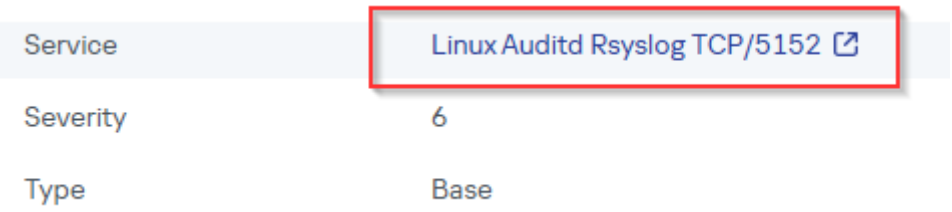
- Включить выбранное поле в поиск или исключить его из поиска, нажав на `+` или `−` рядом со значением поля.



- По хешу файла в полях **FileHash** или **OldFileHash** раскрыть список, в котором можно выбрать одно из следующих действий:
  - Показать информацию о файле из Threat Lookup (доступно при интеграции с Kaspersky Threat Intelligence Portal. См. Статью Интеграция с Kaspersky Threat Intelligence Portal).
  - Добавить в Internal TI CyberTrace (доступно при интеграции с Kaspersky CyberTrace. См. Статью Интеграция с Kaspersky CyberTrace).




  - Найти похожие события (в строку поиска будет добавлено условие вида FileHash = '<значение хэш-суммы>' OR OldFileHash = '<значение хэш-суммы>')
- Открыть окно со сведениями об активе, если событие обогащено информацией об активе (см. Статью Интеграция с Kaspersky Security Center).
- Просмотреть параметры сервиса, обработавшего событие, перейдя по ссылке с именем коллектора в поле Service.




Для просмотра остальных событий в таблице можно воспользоваться «горячими клавишами» - стрелка вниз/вверх.

---

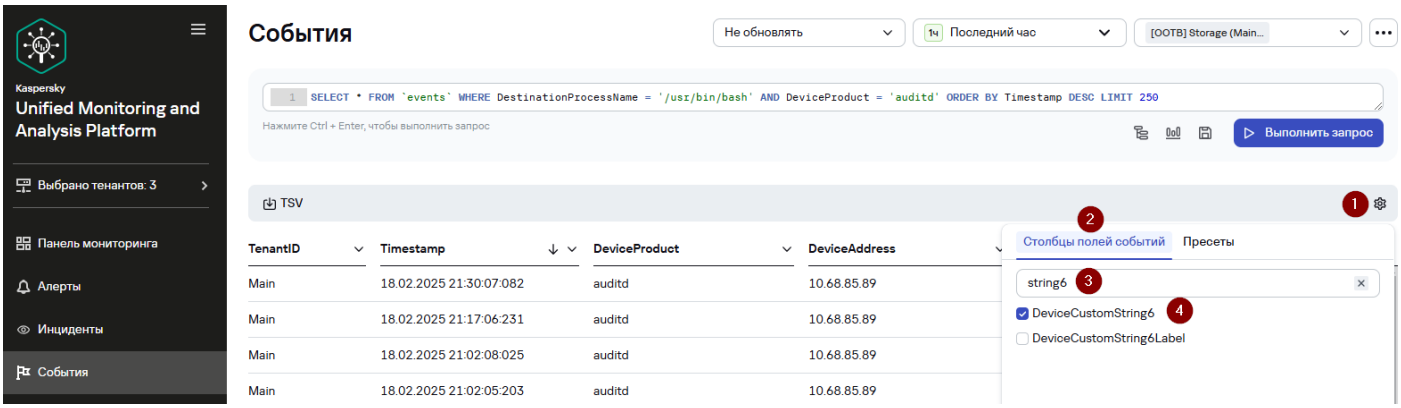
# Настройка таблицы событий

В KUMA поддерживается настройка отображаемого набора столбцов полей событий и порядок их отображения (**пресет**). Выбранную конфигурацию столбцов можно сохранить.

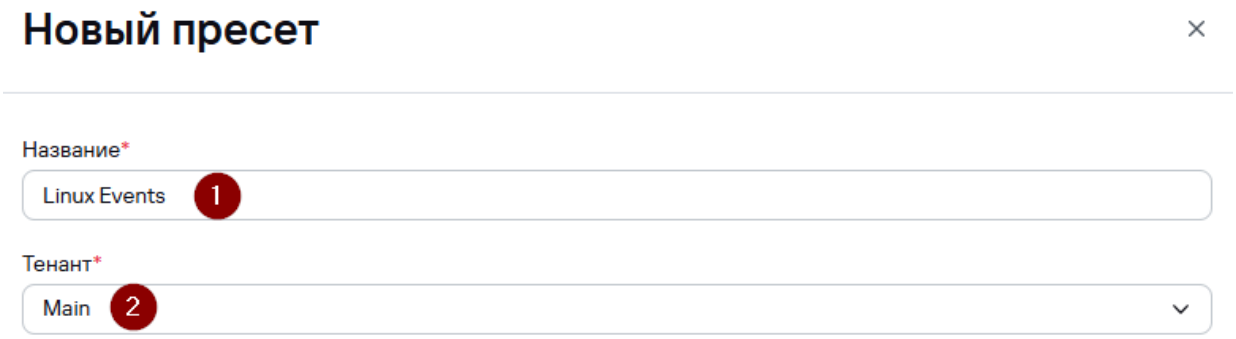
Например, необходимо, чтобы для событий Linux всегда отображались столбцы полей TenantID, Timestamp, DeviceProduct, DeviceAddress, DeviceEventCategory, DestinationProcessName и DeviceCustomString6.

Для создания пресета:

- В разделе **События** нажмите на значок .
- В открывшемся окне на вкладке **Столбцы полей событий** выберите необходимые поля (см. выше). Для упрощения поиска можно начать набирать название поля в области **Поиск**.




- Чтобы сохранить выбранные поля, нажмите **Сохранить текущий пресет.**
- В открывшемся окне **Новый пресет** укажите **Название пресета** и выберите **Тенант** в раскрывающемся списке.




- Нажмите **Сохранить**.

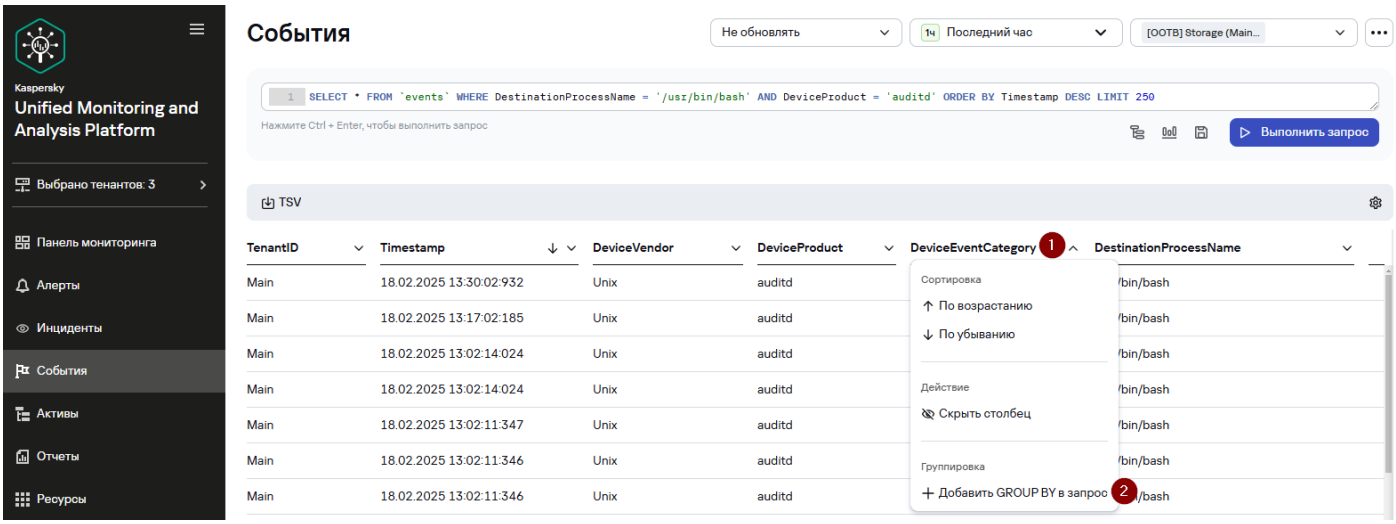
Пресет создан и сохранен. Сохраненные пресеты доступны при нажатии на значок во вкладке **Пресеты**.

# Группировка событий

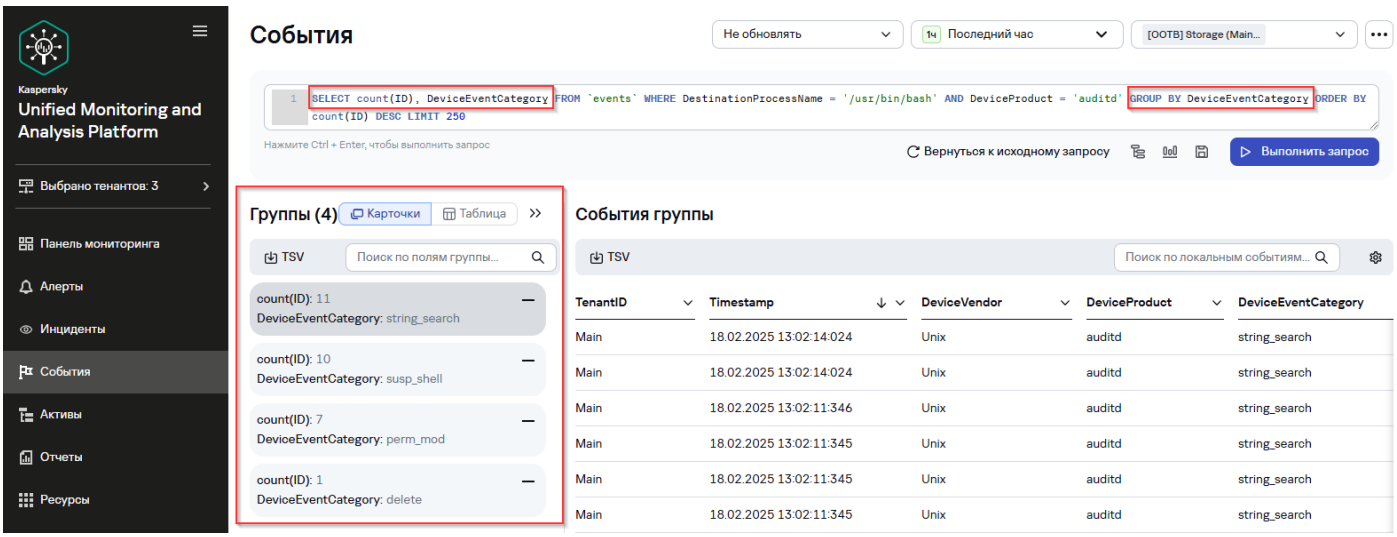
После получения списка событий часто возникает потребность разделить полученные события по группам, чтобы локализовать событие информационной безопасности. В KUMA есть возможность сгруппировать события по одному или нескольким полям для полученного списка событий.

Чтобы сгруппировать события:

- В разделе **События** нажмите на заголовок столбца, по которому необходимо выполнить группировку и в контекстном меню выберите **Добавить GROUP BY в запрос**. Вы можете выбрать последовательно несколько столбцов для группировки, поля будут автоматически добавлены в строку запроса.




- После того как вы выбрали нужные столбцы, нажмите **Выполнить запрос**. В результате будет выполнена группировка событий по заданным полям. Найденные группы будут отображаться в разделе **Группы**.



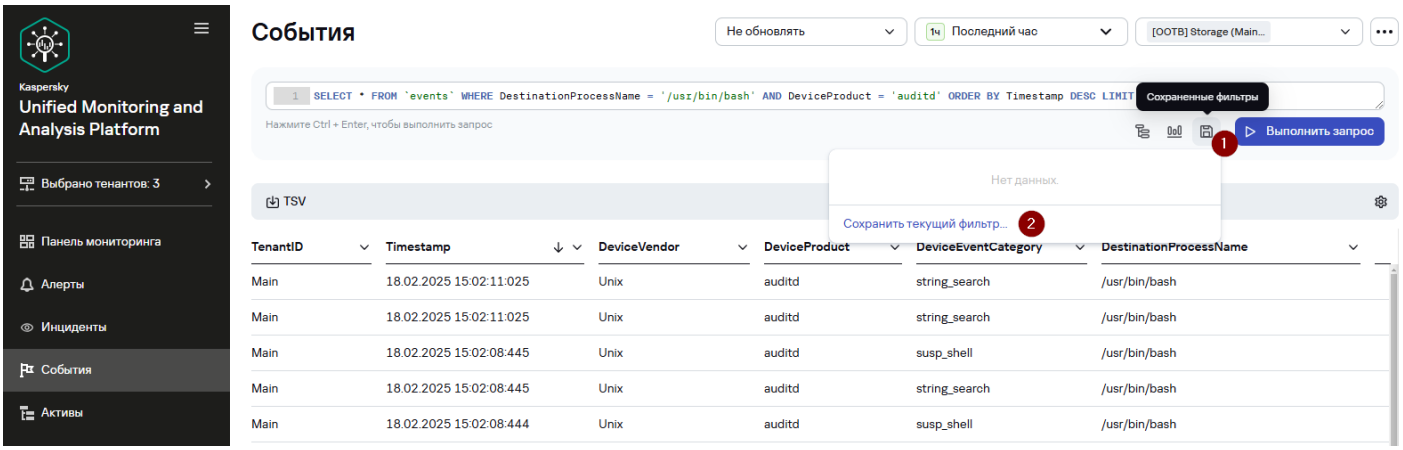

Отображение доступно в виде таблицы и в виде карточек. Вы можете переключаться между режимами отображения. Можно переходить по группам и просматривать содержимое каждой группы.

# Фильтры

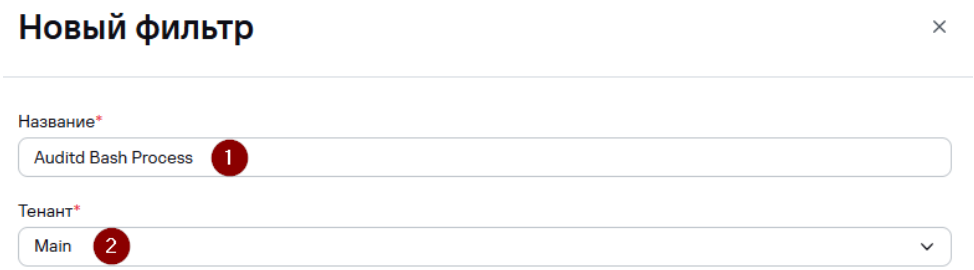
Для сохранения часто используемых поисковых запросов применяется механизм фильтров. При сохранении фильтра сохраняются также **настроенные параметры поискового запроса**: фильтр по периоду, конструктору запросов и отображаемые столбцы полей событий.

Чтобы сохранить текущие настройки фильтра, запроса и периода:

- В разделе **События** нажмите на значок  и выберите **Сохранить текущий фильтр**.




- В открывшемся окне в поле **Название** введите название фильтра.
- В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать создаваемый фильтр.
- Нажмите **Сохранить**.




Конфигурация фильтра сохранена.

Для проверки сохраненной конфигурации фильтра:

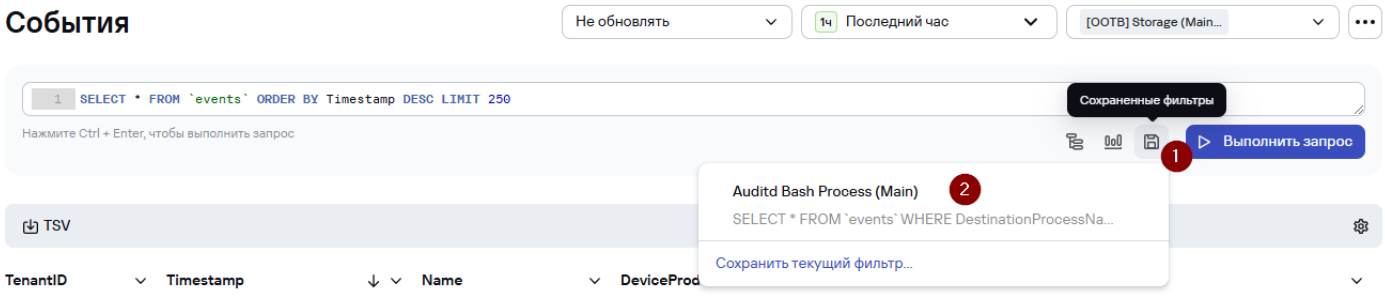
- Примените поисковый запрос по умолчанию

```
SELECT * FROM `events` ORDER BY Timestamp DESC LIMIT 250
```

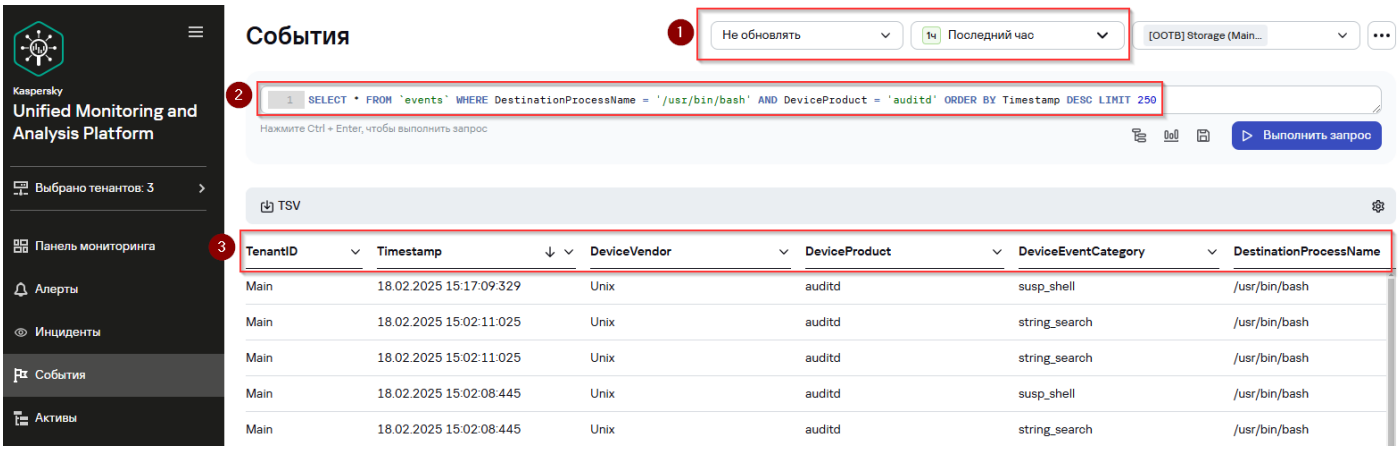
- Нажмите на значок  и перейдите во вкладку **Пресеты.**
- Нажмите на **Пресет по умолчанию.**
- Измените параметры временного диапазона на **5 минут.**
- Набор столбцов полей событий, таблица событий, временной диапазон вернутся к виду по умолчанию.

Чтобы применить ранее сохраненную конфигурацию фильтра:

- В разделе **События** нажмите на значок  и выберите нужный фильтр.




- Выбранная конфигурация фильтра станет активна: в поле поиска отобразится сохраненный поисковый запрос, в верхней части окна применятся настроенные параметры периода, частоты обновления результатов поиска.
- Для отправки поискового запроса нажмите на кнопку **Выполнить запрос**.




Обратите внимание, что набор столбцов полей событий также изменился.

Если нажать на значок  рядом с названием сохраненной конфигурации фильтра, данный фильтр станет использоваться в качестве фильтра по умолчанию.

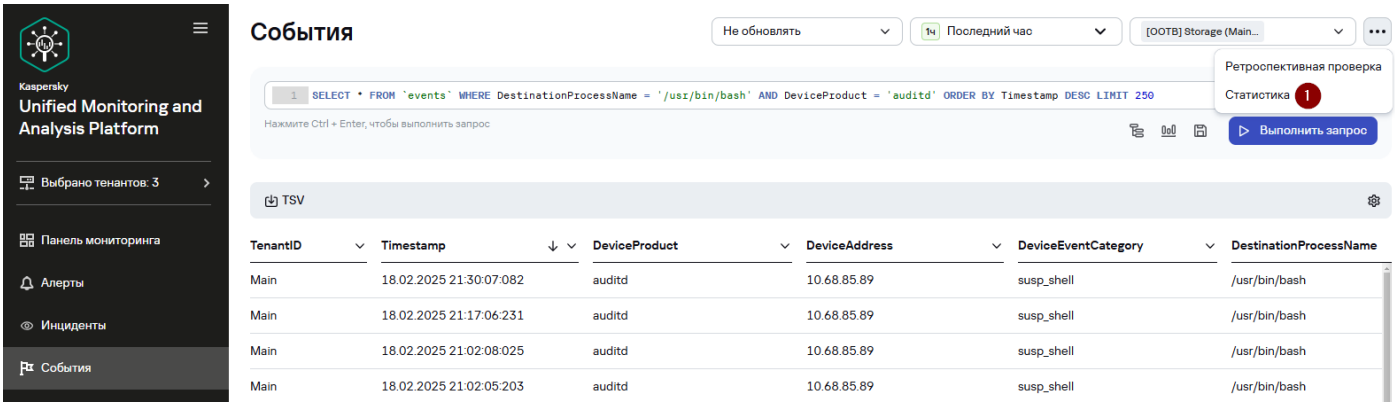
Другие пользователи KUMA также могут использовать сохраненные фильтры при условии, что у них есть соответствующие права доступа.

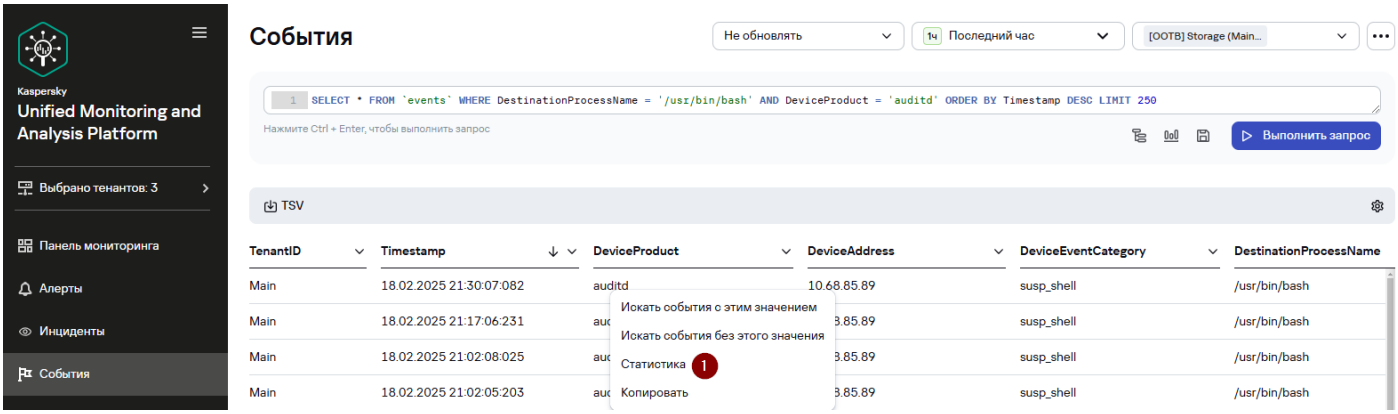
# Получение статистики по событиям в таблице

Вы можете получить статистику по текущей выборке событий, отображаемой в таблице событий.

Чтобы получить статистику:

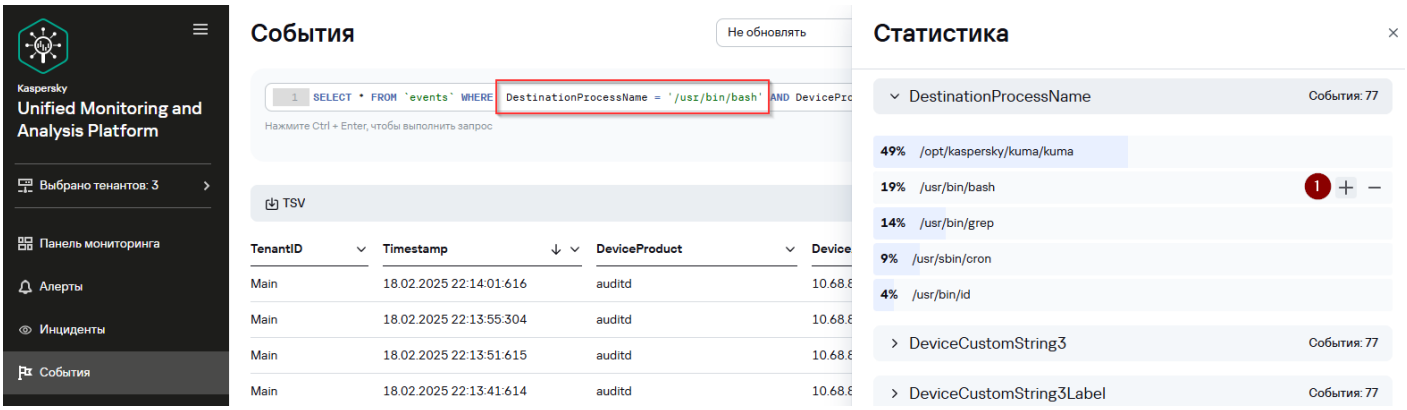
- В разделе **События** в правом верхнем углу таблицы событий в раскрывающемся списке ••• выберите **Статистика** или в таблице событий нажмите на любое значение и в открывшемся контекстном меню выберите **Статистика**




- В появившемся окне справа отобразится **статистика** со списком полей текущей выборки событий. Число возле каждого поля указывает на количество событий в выборке с данным полем. При раскрытии поля отображается пять наиболее частых значений. С помощью поля **Поиск** полей можно найти нужные поля.


При нажатии на + или − напротив значения можно добавлять значение поля в поисковый запрос в качестве условия поиска событий.

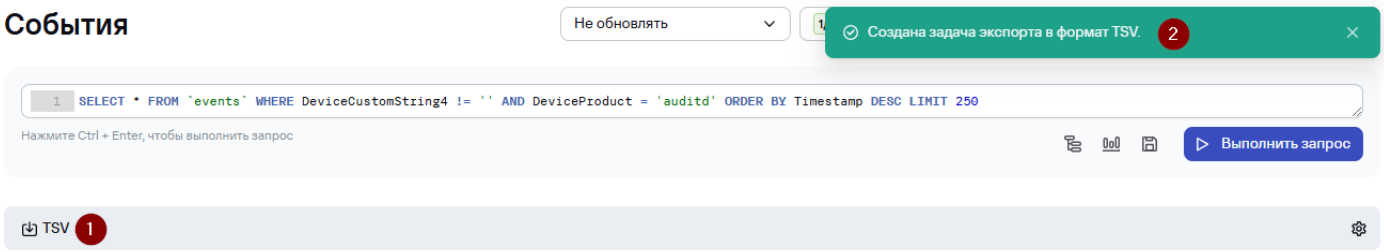



# Экспорт событий

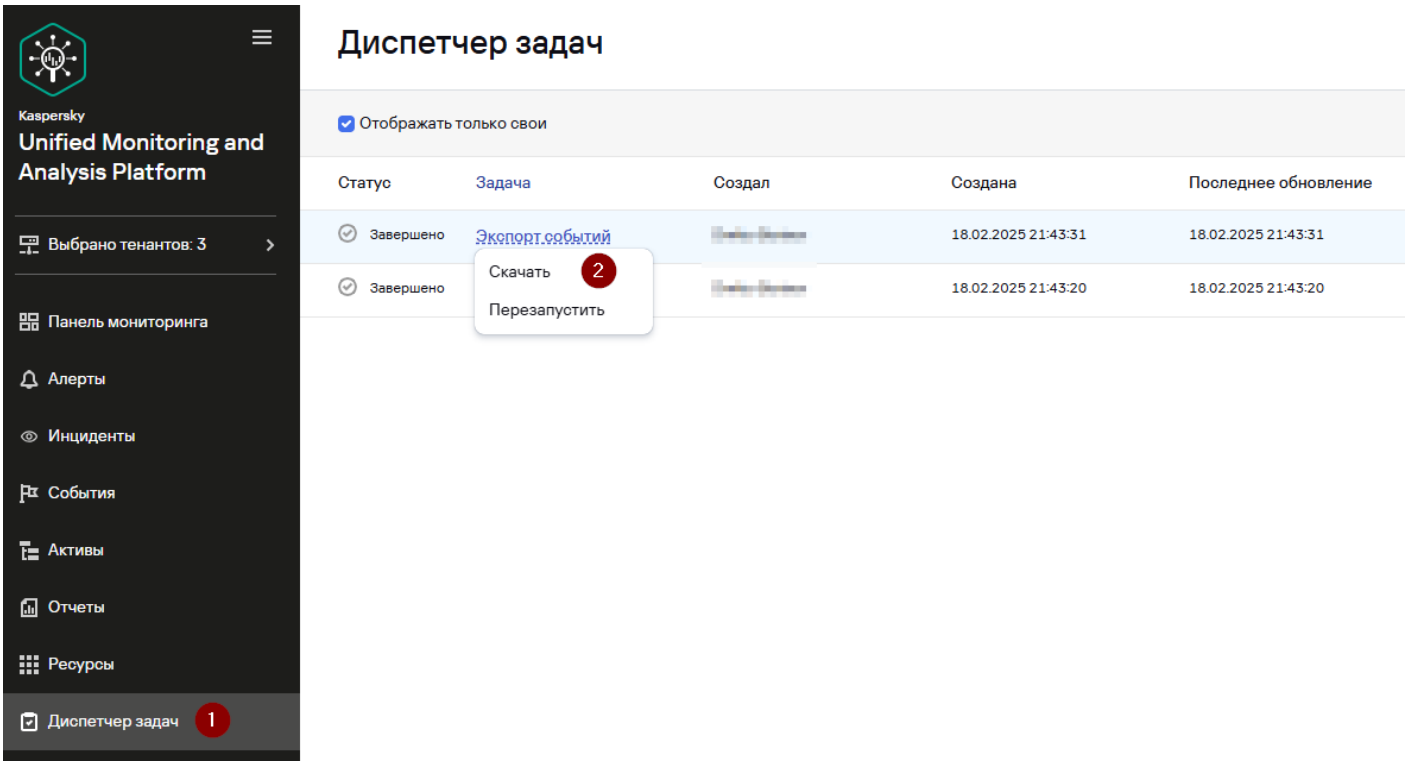
Из KUMA можно экспортировать информацию о событиях в TSV-файл. Выборка событий, которые будут экспортированы в TSV-файл, зависит от используемого поискового запроса и диапазона времени. Информация экспортируется из столбцов, которые в момент экспорта отображаются в таблице событий.

Чтобы экспортировать информацию о событиях:

- В разделе **События** нажмите на кнопку TSV .
- После этого в разделе **Диспетчере задач** будет создана новая задача экспорта TSV -файла.




- Найдите созданную задачу в разделе **Диспетчер задач**.
- Когда файл будет готов к загрузке, в строке задачи в столбце **Статус** отобразится статус **Завершено** и значок .
- Нажмите на название типа задачи и в раскрывающемся списке выберите **Загрузить**.




- TSV-файл с информацией о событиях будет загружен с использованием настроек вашего браузера. Имя файла по умолчанию: `event-export-<date>_<time>.tsv`.

---

Revision #17
Created 2026-06-11 13:00:54 UTC by lerat
Updated 2026-08-07 13:14:48 UTC by Dmitry Borisov