

Работа с событиями

В данной статье описана работа с событиями: как просматривать и фильтровать события, а также сохранять запросы фильтрации.

Раздел **События** позволяет формировать запрос на выборку Событий. Для перехода в раздел «События» нажмите на **События** в левом боковом меню на главной странице.

События (**≥78**)

ИQL SQL

() Конструктор запроса Начальная дата > Конечная дата

Q SELECT `timestamp`, `msgid`, `action`, `event\_src\_title`, `event\_src\_vendor`, `event\_src\_hostname`,

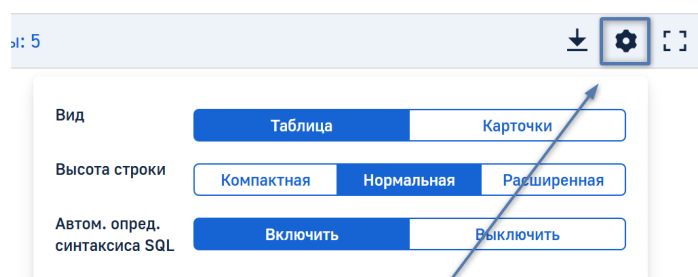
Колонки Фильтры Группировка

timestamp	msgid	action	event_src_title	event_src_vendor	event
01.01.24, 13:51:12	52024	-	-	-	-
02.01.24, 02:21:26	2898	-	-	-	-
02.01.24, 07:20:08	2405	-	-	-	-
02.01.24, 08:46:13	1188	-	-	-	-
02.01.24, 13:40:23	24978	-	-	-	-
02.01.24, 15:26:50	37013	-	-	-	-
02.01.24, 18:41:13	32004	-	-	-	-
03.01.24, 02:07:17	52956	-	-	-	-
03.01.24, 14:43:37	32160	-	-	-	-
04.01.24, 16:06:17	55450	-	-	-	-
04.01.24, 17:58:03	56337	-	-	-	-
06.01.24, 01:24:33	28055	-	-	-	-
06.01.24, 04:13:18	25271	-	-	-	-
06.01.24, 06:54:20	27554	-	-	-	-

На данной странице отображаются все зарегистрированные в Системе события. Здесь вы можете просмотреть список событий, отфильтровать и экспортировать события.

Конфигурация отображения таблицы

Вы можете сконфигурировать отображение таблицы событий. Для этого нажмите на иконку шестеренки в правом верхнем углу таблицы:



В выпадающем меню вы можете настроить следующие параметры:

- **Вид** — формат отображения таблицы событий. Доступные значения: **Таблица** и **Карточки**;
- **Высота строки** — высота строк в таблице событий. Доступные значения: **Компактная**, **Нормальная** и **Расширенная**;
- **Автоматическое определение синтаксиса SQL** — данная строка активирует/деактивирует автоматическое определение синтаксиса SQL в содержимом событий.

Также вы можете развернуть таблицу в режим полноэкранного отображения. Для этого нажмите на иконку рамок в правом верхнем углу таблиц:



Просмотр событий

Все события отображаются в виде списка в таблице. Для того, чтобы просмотреть подробную информацию о событии, нажмите на событие. Дополнительная информация откроется в правом сайдбаре.

События (≥238)

3

() Конструктор запроса

Начальная дата > Конечная дата

Q SELECT `timestamp`, `msgid`, `action`, `event\_src\_title`

Колонки Фильтры Группировка

timestamp	msgid	action
17.03.24, 08:42:04	60657	-
17.03.24, 22:26:32	9180	-
18.03.24, 09:32:21	11317	-
18.03.24, 17:38:37	32058	-
19.03.24, 02:02:06	38478	-
19.03.24, 05:26:36	55268	-
19.03.24, 09:33:13	54163	-
19.03.24, 16:48:43	5482	-
20.03.24, 10:53:26	26944	-
20.03.24, 17:29:27	11735	-
20.03.24, 17:57:11	52165	-
20.03.24, 18:56:28	14577	-
20.03.24, 22:30:43	8150	-
21.03.24, 03:49:44	32669	-

< 1 ... 8 9 10 11 12 > Перейти к

Детали события

UUID: 68f91abe-c8dc-4260-8d0f-a943ba0baed8

Q Название поля или значение

message
vforeeiqkhjxxcmpfnixnwsxfbqplsewiymyspoeekfykajafgvzermglpxbvfxlouvrooxnp
zedqz

Колонка

Значение

timestamp17.03.24, 22:26:32

msgid9180

Пустые события

Экспорт события

Для быстрого переключения между событиями нажмите на иконки стрелочек в правом верхнем углу сайдбара. Переключатель **Пустые события** активирует/деактивирует отображение колонок с пустыми значениями.

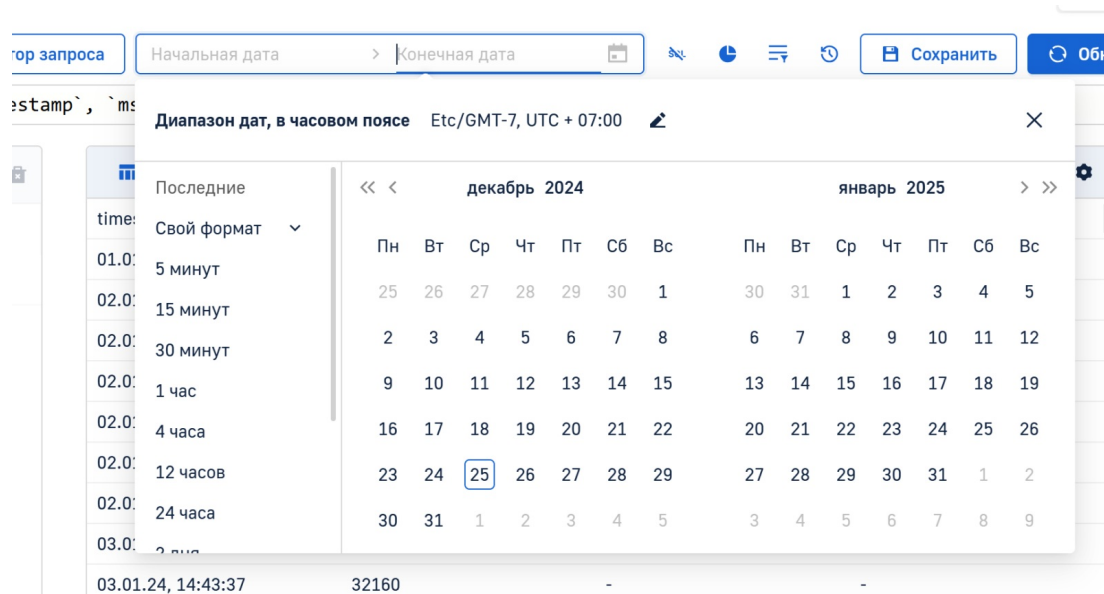
Фильтрация событий

Для того, чтобы отфильтровать события, можно использовать следующие инструменты:

- Определение временных рамок;
- Фильтры;
- Поле ввода SQL-запроса;
- Дополнение фильтра из события;
- [Конструктор запроса](#).

Определение временных рамок

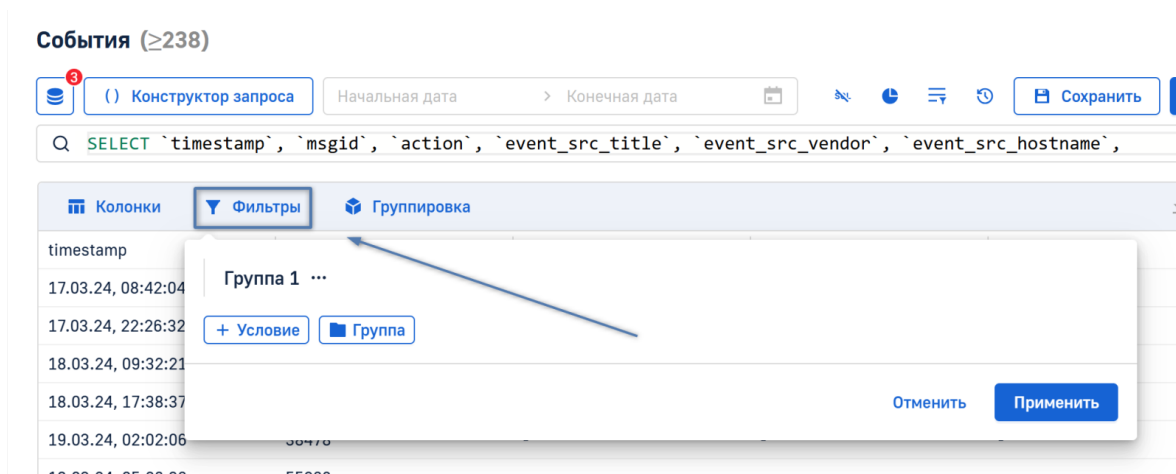
Для того, чтобы отфильтровать список событий по времени их регистрации, нажмите **Выберите диапазон** справа от конструктора SQL. Во всплывающем окне вы можете ввести диапазон дат и времени вручную, либо выбрать одно из предустановленных значений.



После того как вы выбрали временной диапазон, нажмите **Обновить**, чтобы обновить список событий.

Фильтры

Для работы с условиями можно использовать функционал фильтров таблицы. Для этого нажмите **Фильтры** в левом верхнем углу таблицы.



После этого откроется список всех примененных к таблице фильтров. Для того, чтобы добавить условие, нажмите **+ Условие** и заполните всю необходимую информацию:

- **Поле** — поле в базе данных, по которому будет выполняться фильтрация;
- **Оператор** — выбор оператор для фильтрации. Возможные значения **И** и **ИЛИ**;
- **Значение** — значение, по которому будет выполняться фильтрация.

Нажмите **Применить** для сохранения фильтра, затем обновите список событий, нажав **Обновить**.

Групповые фильтры

Вы также можете добавить группу для условий. Для этого в окне выбора фильтров нажмите **Группа**.

Группа 1 ...

Подгруппа 1.1 ...

message ▼ Равно ▼ REJECT ✕

И

uuid ▼ Не равно ▼ 0 ✕

ИЛИ

Подгруппа 1.2 ...

message ▼ Равно ▼ ACCEPT ✕

И

uuid ▼ Не равно ▼ 0 ✕

И

action_name ▼ Содержит ▼ %login% ✕

+ Условие + Группа

Отменить Применить

Условия, сформированные в группы, можно использовать для построения сложных выборок с использованием операторов **И** и **ИЛИ**.



Чтобы изменить конфигурацию группы или подгруппы фильтров, наведите курсор на три точки справа от ее имени и нажмите на одну из иконок:

- **Иконка карандаша** — отредактировать имя группы/подгруппы;
- **+** — добавить условие;
- **Иконка ветки** — добавить подгруппу;
- **Иконка корзины** — удалить группу/подгруппу.

Нажмите **Применить** для сохранения фильтра, затем обновите список событий, нажав **Обновить**.

Поле ввода SQL-запроса

При необходимости, вы можете ввести SQL-запрос вручную. Для этого нажмите на поле ввода SQL-запроса и отредактируйте его содержимое под свои нужды.

События (≥78) SQL

() Конструктор запроса Начальная дата > Конечная дата 🔍 🕒 📄 🔄 Сохранить Обновить

Q `SELECT `timestamp`, `msgid`, `action`, `event_src_title`, `event_src_vendor`, `event_src_hostname`,` ✕

При вводе SQL-запроса необходимо соблюдать следующие правила:

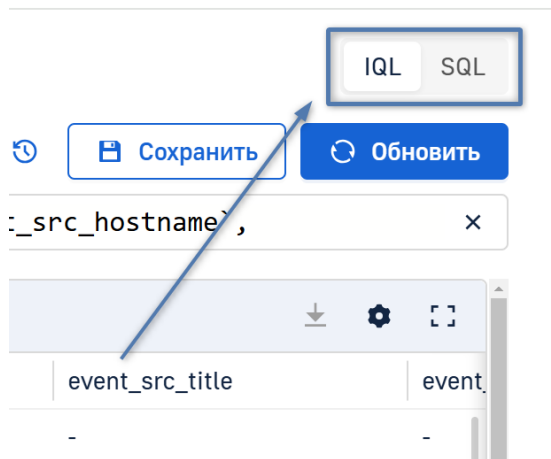
1. Следует использовать только запрос **SELECT**. Попытка обновить таблицу с любым другим запросом приведет к ошибке.
2. В запросе нельзя указывать параметр пагинации **OFFSET**.
3. Наименование полей необходимо указывать в апострофах, например ``event.type``.

Для того, чтобы скрыть/отобразить поле для ввода SQL-запроса, нажмите на иконку SQL справа от поля выбора фильтрации по дате..

Начальная дата > Конечная дата 🔍 🕒 📄 🔄

``msgid`, `action`, `event_src_title`, `event_src_vendor`, `event_src`

Вы также можете переключаться между режимами запросов: **SQL** (расширенный режим) и **SQL** (расширенный режим). Для этого нажмите на переключатель языков в правом верхнем углу страницы.

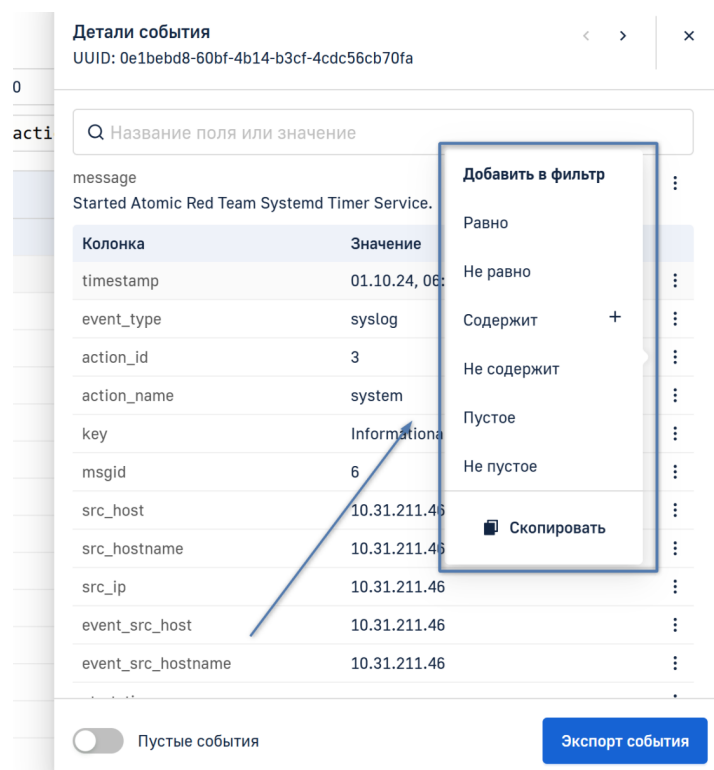


Ниже приведена сравнительная таблица функциональности режимов:

Функциональность		IQL (базовый)	SQL (Расширенный)
Выбор тенантов		+	+
Конструктор запросов		+	+
Фильтрация по дате		+	+
Сохраненные запросы		+	+
Просмотр истории запросов		+	+
Создание виджета		+	—
Поле ввода SQL-запроса		+	+
Таблица	Конфигурация колонок	+	+
	Фильтры	+	+
	Группировка событий	+	—
	Изменение вида (Карточки, Таблица)	+	+
	Высота строки	+	+
	Автоматическое определение синтаксиса запроса	—	+
	Экспорт событий	+	+
	Открытие таблицы на весь экран	+	+
	Сортировка событий	+	+
	Просмотр деталей событий	+	+

Дополнение фильтра из события

При расследовании событий безопасности может появиться необходимость дополнить фильтр новыми данными, полученными из других событий. Для того, чтобы это сделать, откройте интересующее вас событие.



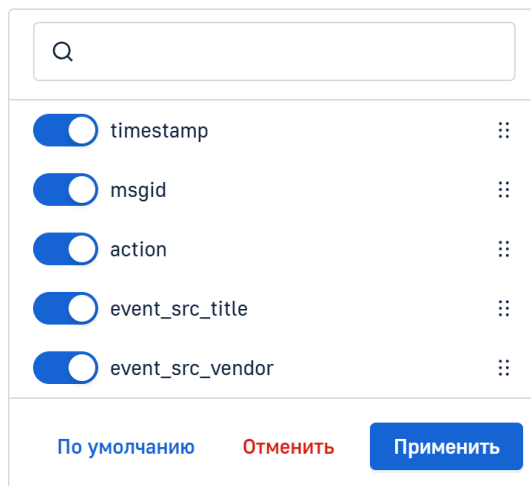
В правой части страницы откроется модальное окно с подробной информацией о событии. Нажмите на три точки справа от колонки и значения которые вы хотите добавить в фильтр и выберите оператор.

После того как вы дополнили фильтр, нажмите **Обновить**, чтобы обновить список событий.

Сортировка таблицы

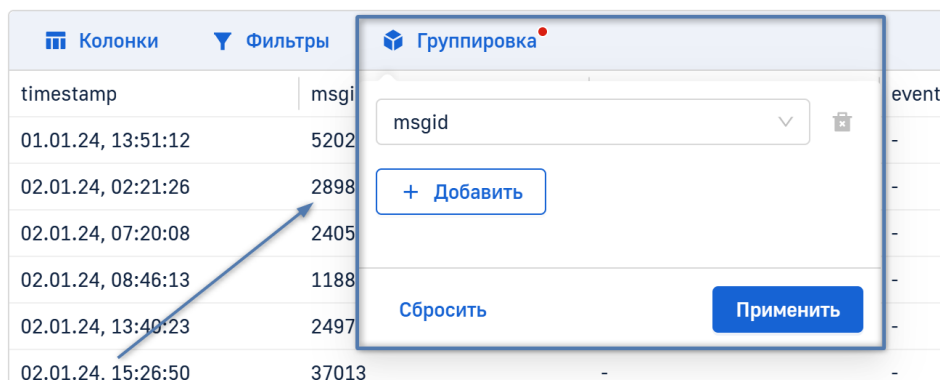
Для упрощения навигации по списку, вы можете выбрать список и порядок отображаемых колонок. Для этого нажмите **Колонки** в левом верхнем углу таблицы. Используйте переключатель слева от имени поля, для того, чтобы включить или выключить отображение колонки в таблице. По умолчанию выбраны первые 8 полей.

Для того, чтобы изменить порядок отображения колонок, наведите курсор на иконку сортировки справа от имени колонки, зажмите левую кнопку мыши и перенесите элемент в необходимое место.



Группировка событий

Для того, чтобы сгруппировать события по определенному полю, нажмите **Группировка** и выберите поле/поля для группировки. После нажатия **Применить**, сгруппированные события отобразятся в дополнительной таблице, слева от основной.



Любые изменения, которые вы вносите в любом из инструментов, будут применены в каждой из областей.

Экспорт событий

Для того, чтобы экспортировать отфильтрованный список событий нажмите на иконку загрузки в правом верхнем углу таблицы и выберите в выпадающем меню формат файла:

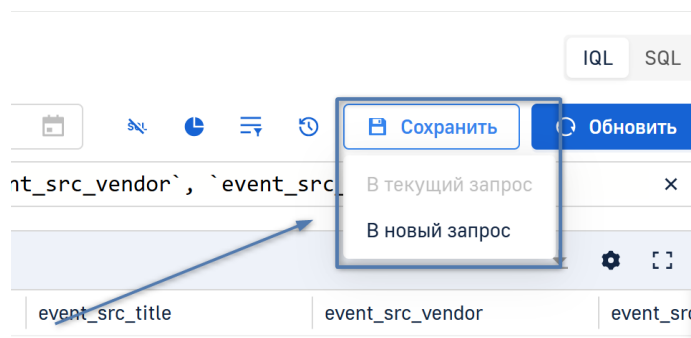


Вы можете экспортировать не более 1 миллиона событий за раз.

Сохраненные запросы

Сохранение запросов

Для удобства ежедневного использования вы можете сохранить ваши запросы и фильтры. Для этого нажмите **Сохранить** в правом верхнем углу страницы, затем в выпадающем меню выберите вариант сохранения — в текущий запрос, или в новый.



Если вы выбрали **В новый запрос**, откроется новое окно, в котором вы сможете задать имя запроса и указать путь для его сохранения. Для сохранения запроса нажмите **Сохранить**.

Сохранение запроса

Название

Запросы на аутентификацию

Путь

Запросы для расследований

Запрос

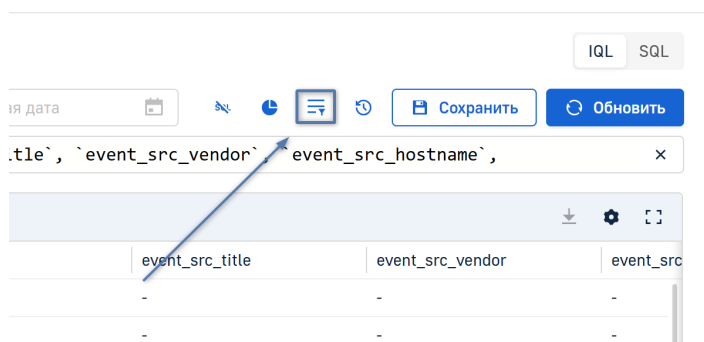
```
SELECT `timestamp`, `msgid`, `action`, `event_src_title`, `event_src_vendor`,
`event_src_hostname`, `event_src_ip`, `message` FROM messages
```

Отменить

Сохранить

Использование сохраненных запросов

Для того, чтобы отфильтровать список событий по ранее сохраненным параметрам, нажмите на иконку сохраненных запросов правом верхнем углу страницы, затем в правом сайдбаре выберите ранее сохраненный запрос.

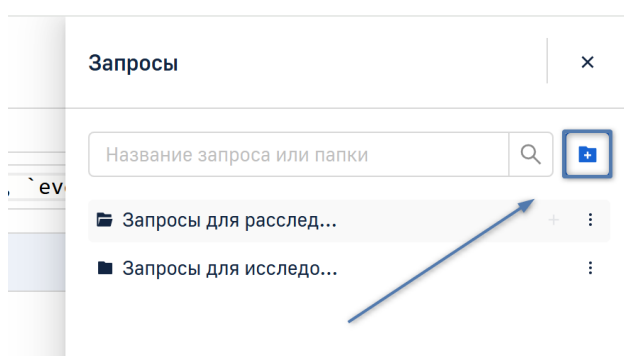


Управление хранилищем сохраненных запросов

Вы можете управлять файловой системой хранения запросов: создавать папки, а также переименовывать, перемещать и удалять папки и сохраненные запросы.

Создание новой папки

Для того, чтобы добавить новую папку, нажмите на иконку добавления в правом верхнем углу дашборда.

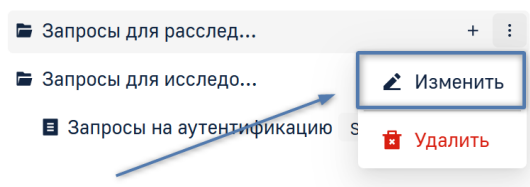


Введите имя для новой папки и нажмите **Создать**.

Если вы хотите создать папку внутри уже существующей, наведите на мышку на корневую папку и нажмите на появившуюся иконку **+**, введите имя для новой папки и нажмите **Создать**.

Редактирование содержимого

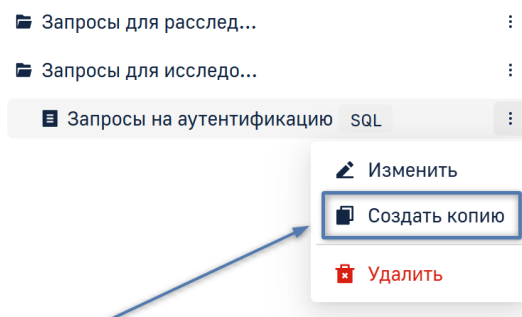
Для того, чтобы отредактировать сохраненный запрос или папку, нажмите на три точки справа от имени и в выпадающем списке выберите **Изменить**.



В открывшемся окне вы можете переименовать и изменить путь к запросу или папке, а также просмотреть содержимое сохраненного запроса. Нажмите **Сохранить** для применения изменений.

Создание копии сохраненного запроса

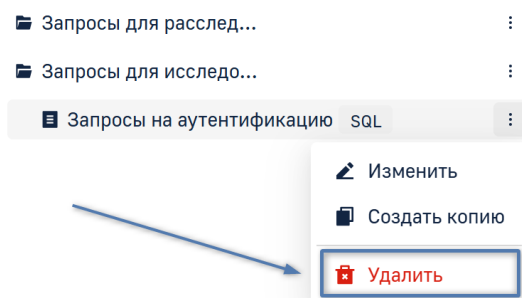
Для того, чтобы создать копию сохраненного запроса, нажмите на три точки справа от имени и в выпадающем списке выберите **Создать копию**.



Выберите путь для сохранения копии запроса и нажмите **Создать копию**.

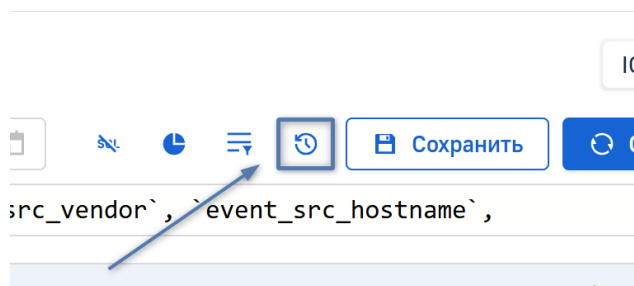
Удаление содержимого

Для того, чтобы удалить сохраненный запрос или папку, нажмите на три точки справа от имени и в выпадающем списке выберите **Удалить**.



Просмотр истории запросов

Для того, чтобы повторить один из ранее использованных запросов, вы можете воспользоваться историей запросов. Для этого нажмите на иконку истории и выберите интересующий вас запрос в правом сайдбаре.

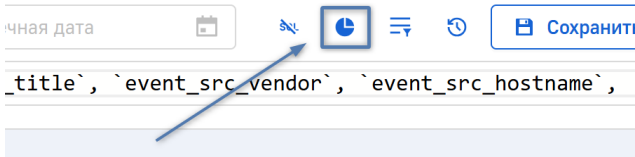


В данном сайдбаре вы можете просмотреть следующую информацию о запросах:

- Дата выполнения запроса;
- Режим выполнения запроса;
- Продолжительность выполнения запроса;
- Содержимое запроса;
- Срок хранения данного запроса в истории.

Создание виджета из событий

Вы можете создать новый виджет для отфильтрованной выборки событий. Для этого, нажмите на иконку создания виджета, выберите дашборд, куда будет добавлен виджет, укажите тип виджета и нажмите **Сохранить**. После этого откроется страница [создания виджета](#).



Выбор тенантов

Для того, чтобы просмотреть события только для определенных тенантов, нажмите на иконку базы данных в левом верхнем углу и выберите тенанты, для которых вы хотите просмотреть выборку.

