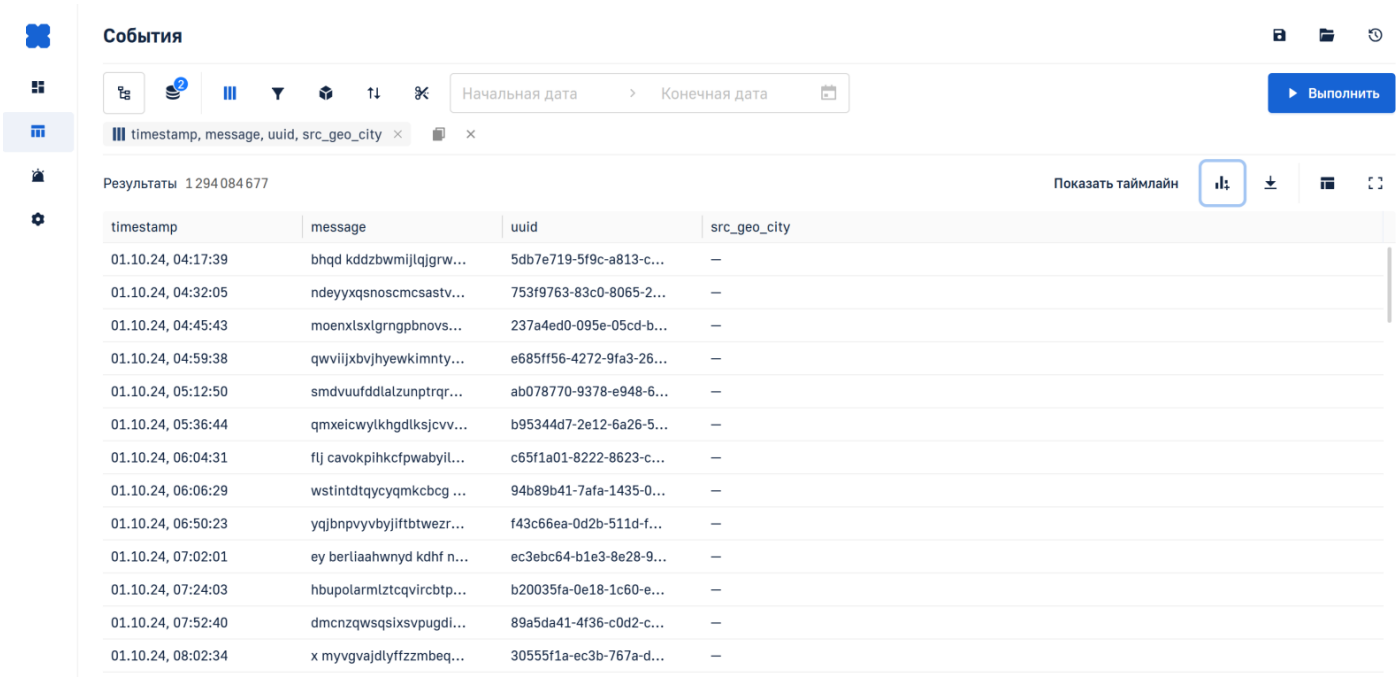
Работа с событиями

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.



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

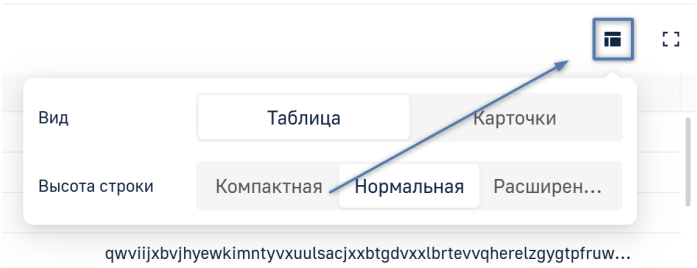
Управление таблицей

По умолчанию на странице отображается 100 записей, однако вы можете выбрать отображение 20, 50, 100 и 500 записей на странице. Для этого нажмите на поле  в правом верхнем углу списка и выберите в выпадающем списке необходимое количество для отображения.

Для переключения между страницами используйте блок в левом нижнем углу списка, или введите конкретную страницу и нажмите клавишу **Enter**:

Конфигурация отображения таблицы

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



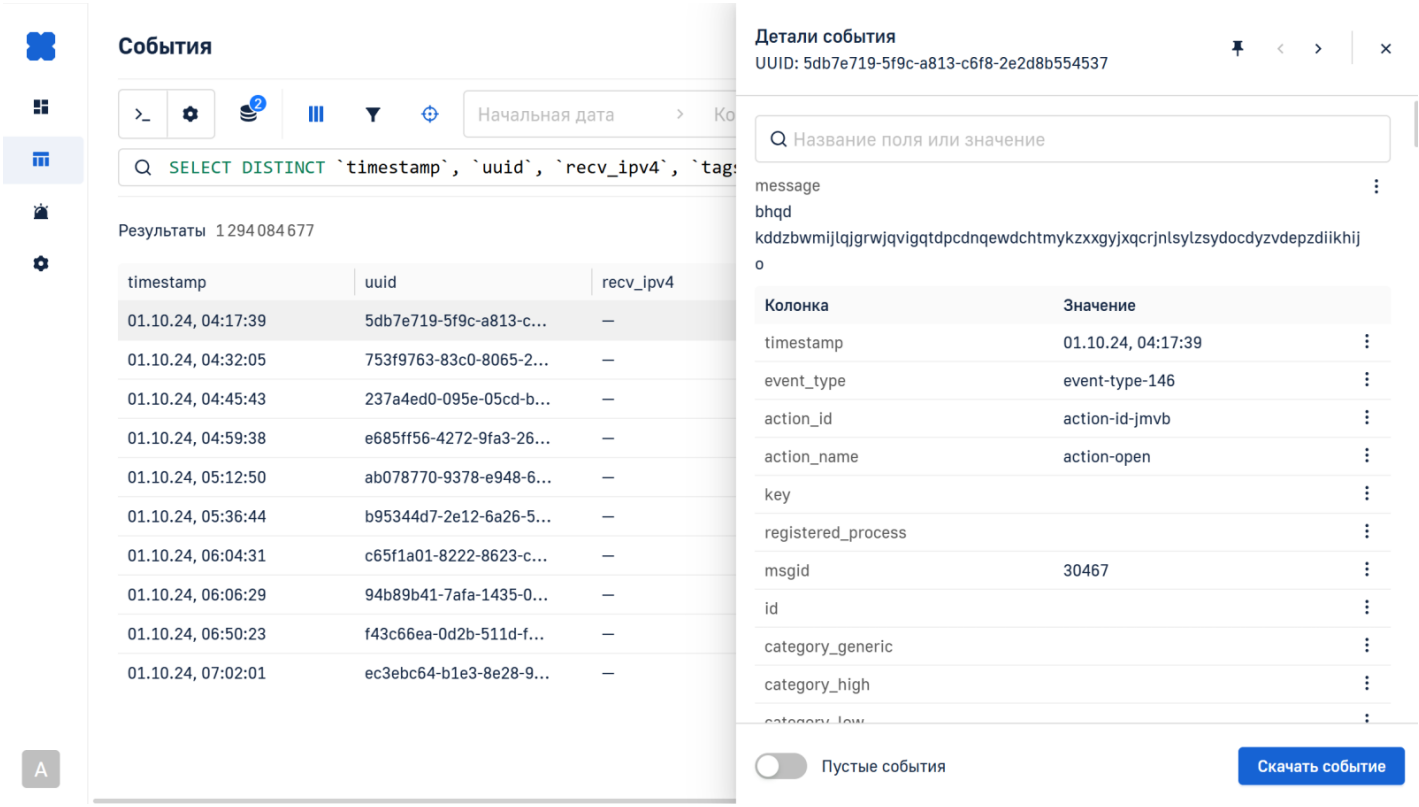
В выпадающем меню вы можете настроить следующие параметры:

- **Вид** — формат отображения таблицы событий. Доступные значения: **Таблица** и **Карточки**;
- **Высота строки** — высота строк в таблице событий. Доступные значения: **Компактная**, **Нормальная** и **Расширенная**.

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

Просмотр событий

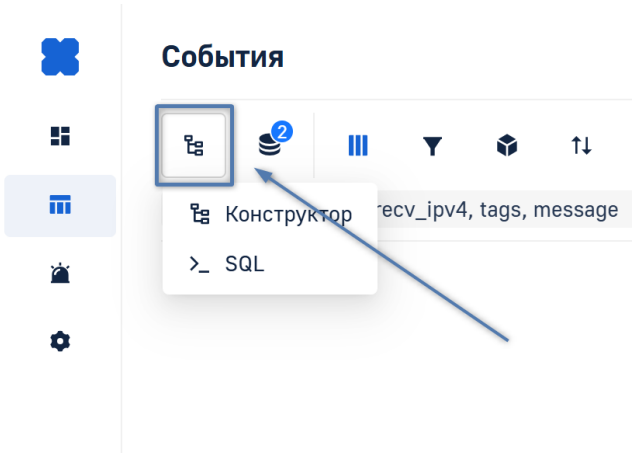
Все события отображаются в виде списка в таблице. Для того, чтобы просмотреть подробную информацию о событии, нажмите на событие. Дополнительная информация откроется в правом сайдбаре.



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

Переключение между режимами запросов

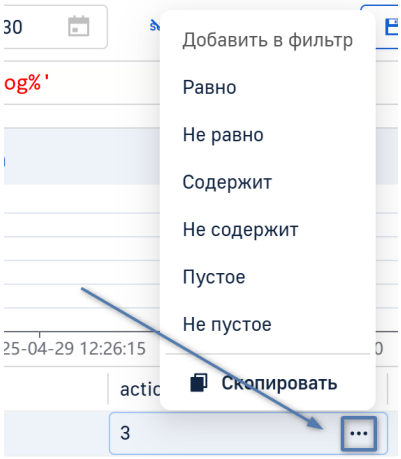
В Системе доступны два режима написания запросов — **Конструктор** и **SQL**. Для того, чтобы переключаться между режимами, нажмите на переключатель иконку режима в левом верхнем углу страницы и в выпадающем списке выберите режим, который вы хотите использовать.



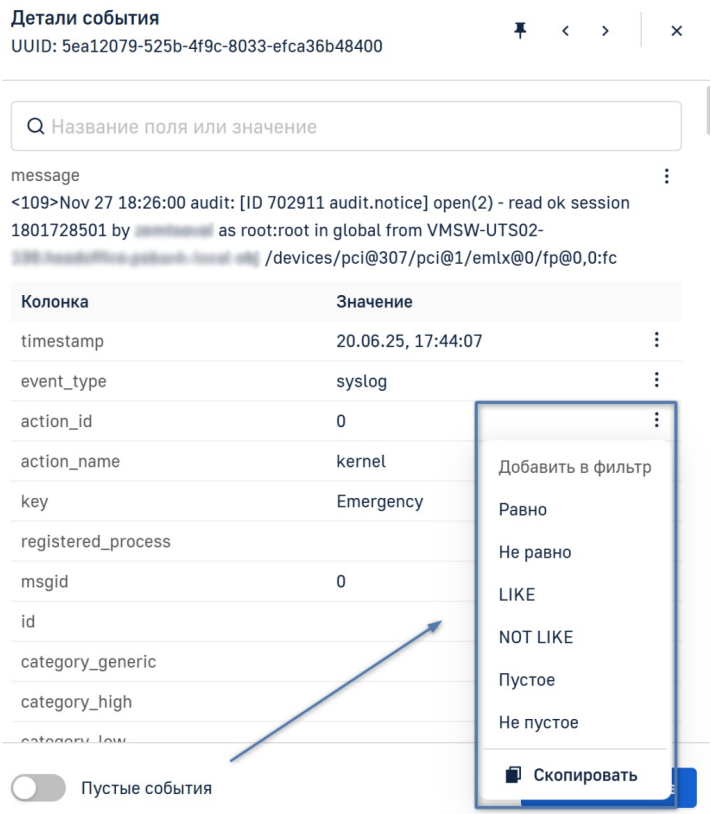
Дополнение фильтра из события

При расследовании событий безопасности может появиться необходимость дополнить фильтр новыми данными,

полученными из других событий. Для того, чтобы это сделать, наведите указатель на поле, по которому вы хотели бы добавить фильтр, нажмите на три точки в правой части ячейки и выберите оператор.



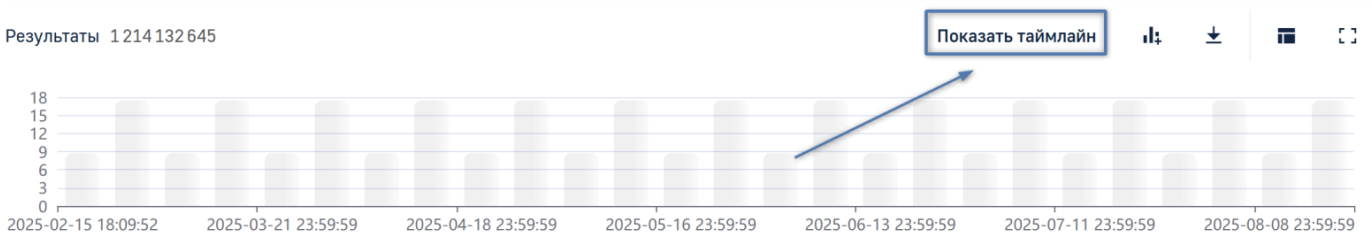
Также вы можете дополнить фильтр данными из события, открыв само событие событие. Нажмите на три точки справа от колонки и значения которые вы хотите добавить в фильтр и выберите оператор.



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

Просмотр таймлайна событий

Функционал системы позволяет просмотреть распределение событий по временной шкале. Для просмотра, нажмите **Показать таймлайн** в левом верхнем углу таблицы.



Для того, чтобы увеличить масштаб временной шкалы нажмите и удерживайте левую кнопку мыши и выделить отрезок, который необходимо отобразить более детально. Чтобы вернуться к общему виду нажмите **Предыдущий период**.

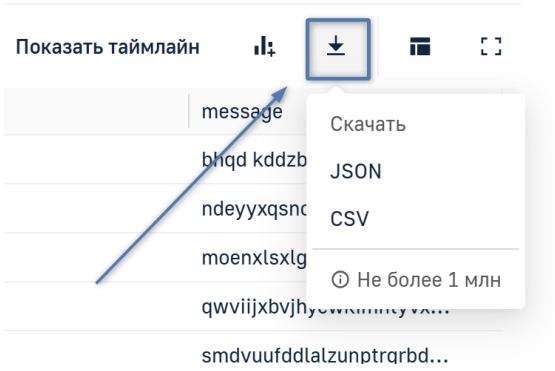
Также вы можете выбрать тип отображения таймлайна — линейный или логарифмический. Для этого воспользуйтесь

иконками графиков в правом верхнем углу таймлайна.

На данный момент функционал таймлайна доступен только для режима конструктора запросов.

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:

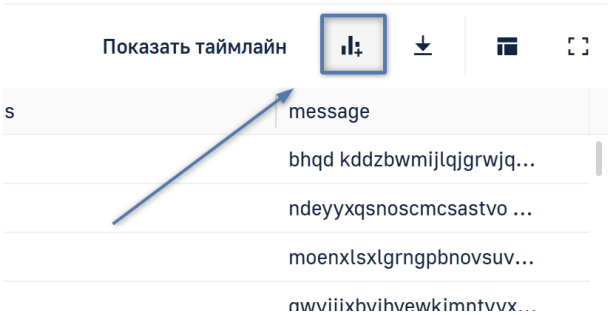


Вы можете экспортировать не более 1 миллиона событий за раз.

На данный момент функционал доступен только для режима конструктора запросов.

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.

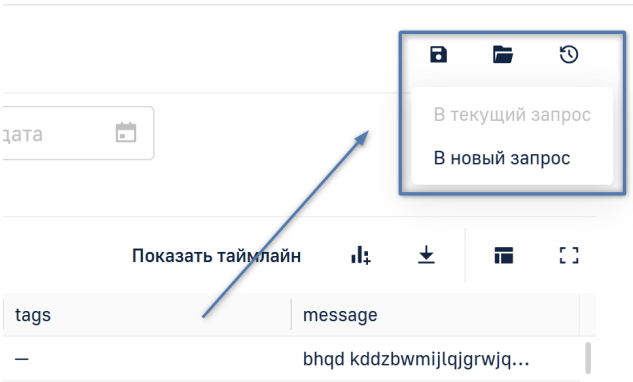


На данный момент функционал доступен только для режима конструктора запросов.

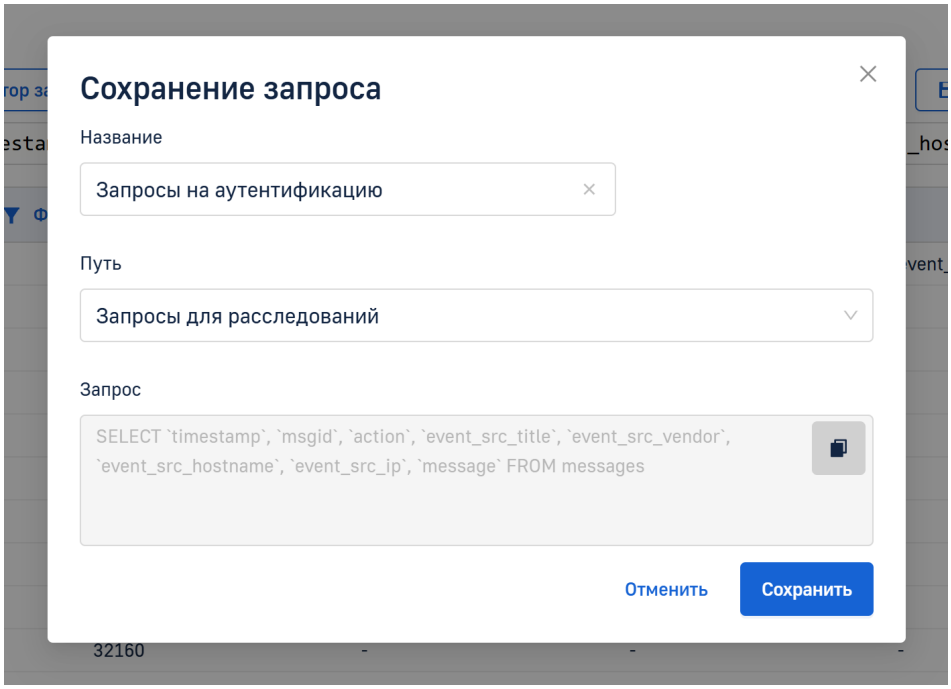
Сохраненные запросы

Сохранение запросов

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

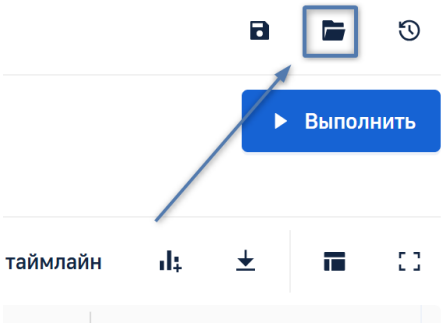


Если вы выбрали **В новый запрос**, откроется новое окно, в котором вы сможете задать имя запроса и указать путь для его сохранения. Для сохранения запроса нажмите **Сохранить**.



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.

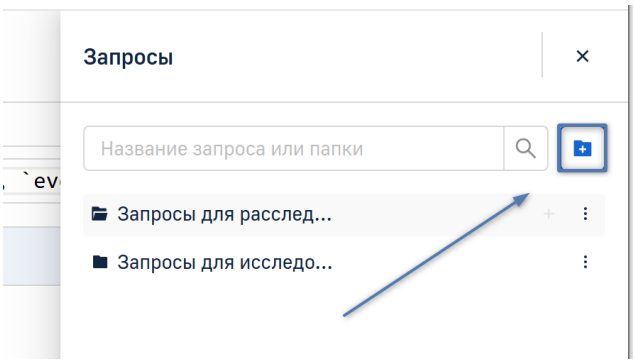


Управление хранилищем сохраненных запросов

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.

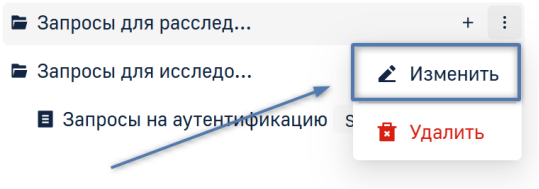


Введите имя для новой папки и нажмите **Создать**.

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

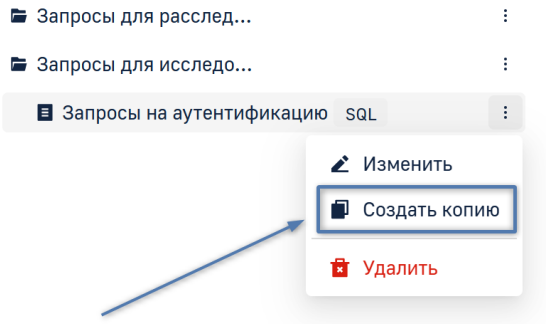
Для того, чтобы отредактировать сохраненный запрос или папку, нажмите на три точки справа от имени и в выпадающем списке выберите **Изменить**.



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

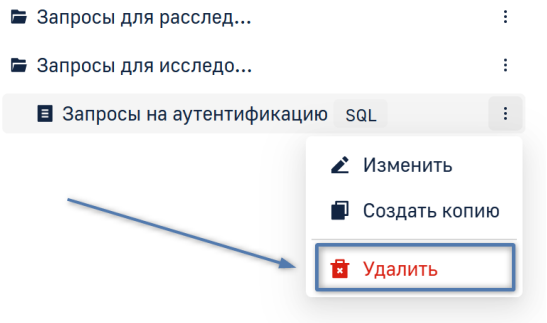
Для того, чтобы создать копию сохраненного запроса, нажмите на три точки справа от имени и в выпадающем списке выберите **Создать копию**.



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

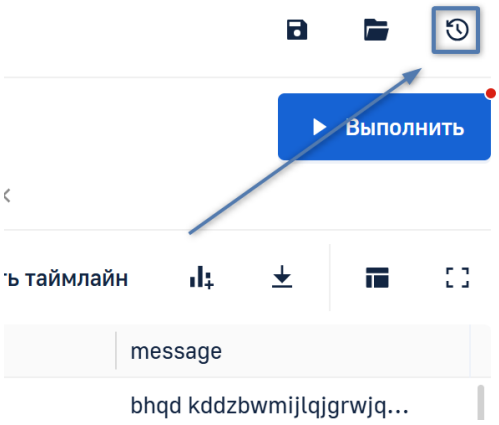
Удаление содержимого

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.

ID статьи: 1394
Последнее обновление: 20 нояб., 2025
Обновлено от: Егоров В.
Ревизия: 5
База знаний LogIQ -> Документация -> Система хранения и обработки данных «LogIQ». Версия 2.6.0 -> LogIQ. Руководство пользователя -> Раздел «События» -> Работа с событиями
https://docs.axel.pro/entry/1394/