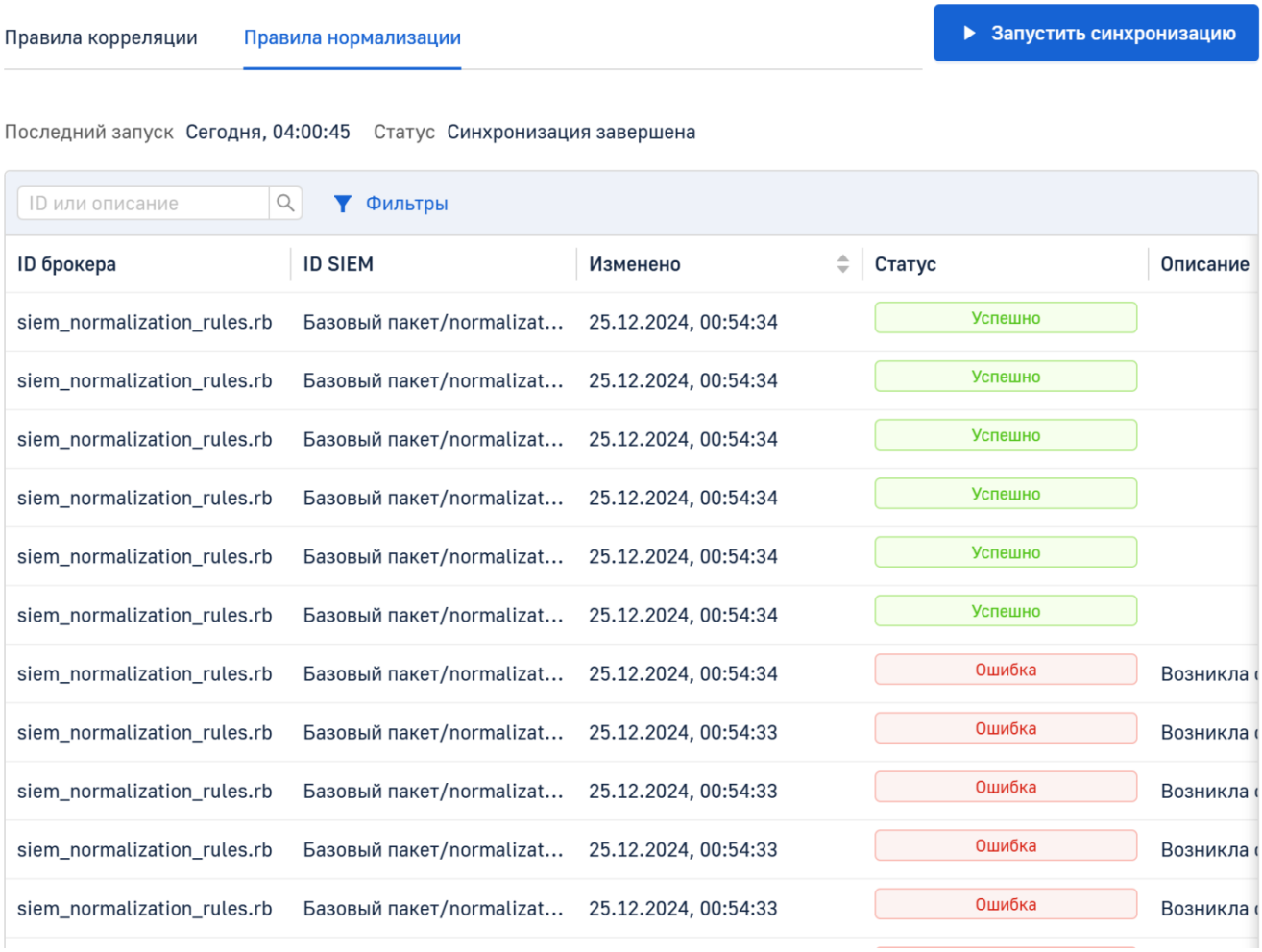
Синхронизация правил нормализации

Данные о последней успешной синхронизации правил нормализации в SIEM и правила нормализации в системе логирования отображаются на странице **Настройки → Компоненты системы → Правила нормализации** .



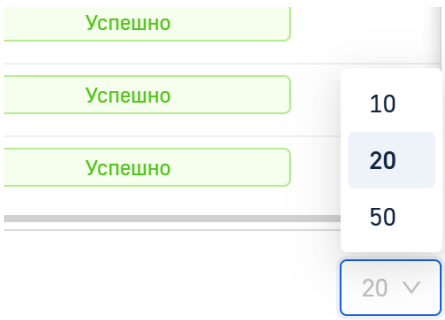
Выполнение синхронизации правил нормализации происходит автоматически раз в сутки, однако администратор может запустить синхронизацию в ручном режиме.

Для ручного запуска синхронизации необходимо нажать на кнопку **Запустить синхронизацию**. Поле **Последний запуск** обновится и будет отображаться таблица результатов процесса синхронизации.

Таблица содержит следующие поля:

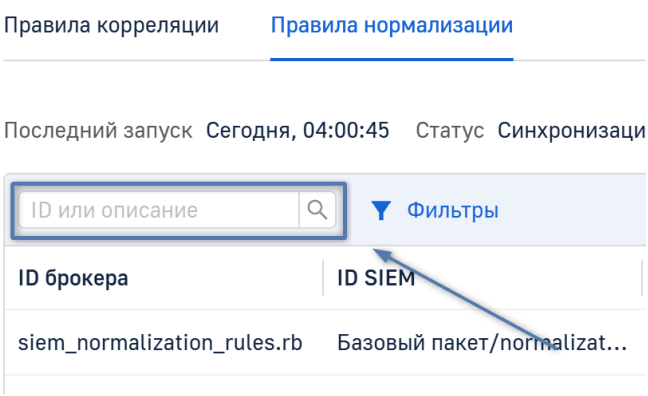
- **ID брокера** — идентификатор брокера, в котором хранится правило;
- **ID SIEM** — имя события, которому соответствует правило в SIEM;
- **Изменено** — дата последнего изменения правила;
- **Статус** — статус правила нормализации. Может принимать следующие значения:
  - **Успешно** — правило нормализации успешно загружено;
  - **Ошибка** — не удалось загрузить правило нормализации.
- **Описание** — описание ошибки из-за которой не удалось загрузить правило нормализации.

По умолчанию, на странице отображается до 20 записей. Для того, чтобы увеличить число отображаемых записей на странице, нажмите на количество записей в правом нижнем углу страницы и выберите одно из значений:



Поиск и фильтрация правил

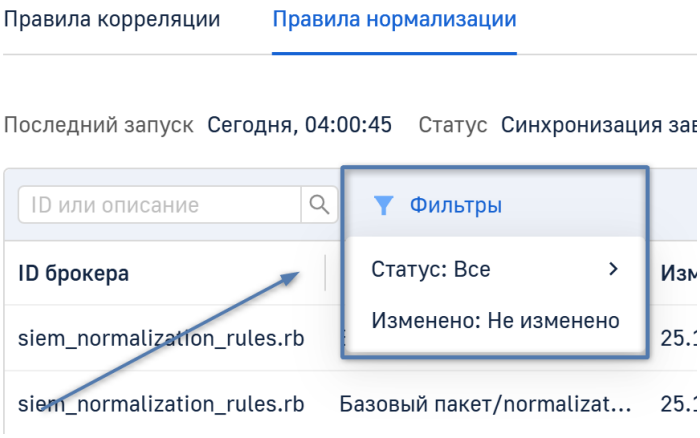
Для того, чтобы найти определенное правило в списке, нажмите на форму поиска в левом верхнем углу таблицы и введите ключевое слово.



В качестве ключевых слов для поиска могут быть использованы:

- ID брокера;
- ID SIEM;
- Описание ошибки.

Вы также можете отфильтровать список правил по их статусу и дате изменения. Для этого нажмите на иконку фильтра и выберите параметр для фильтрации списка.



ID статьи: 1383
Последнее обновление: 29 апр., 2025
Обновлено от: Егоров В.
Ревизия: 1
База знаний LogIQ -> Документация -> Система хранения и обработки данных «LogIQ». Версия 2.6.0 -> LogIQ. Руководство администратора -> Синхронизация компонентов системы -> Синхронизация правил нормализации
https://docs.axel.pro/entry/1383/