?????????? ??????? KSMG ??????? ?? ?????????, ?????????? ? ?????????

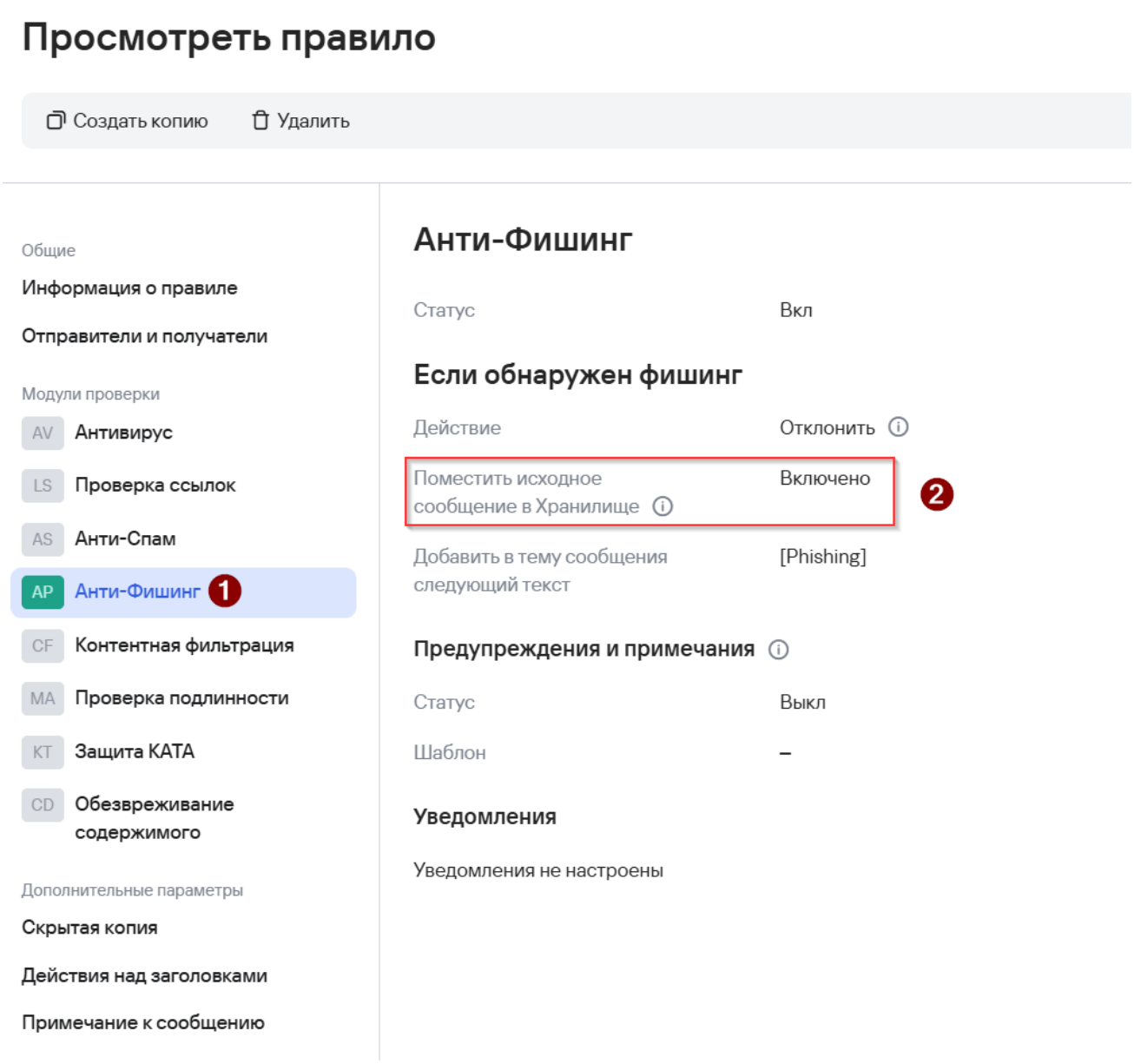
> Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

> Для нормализации событий KSMG в KUMA применяется нормализатор [OOTB] KSMG 2.1+ syslog CEF

????????? ????????? KSMG

Хранилище предназначено для хранения поступающих почтовых сообщений перед их обработкой модулями KSMG. В случае если почтовое сообщение будет отклонено или удалено в результате работы одного из модулей KSMG, аналитик может получить доступ к оригинальному почтовому сообщению в Хранилище.

> Для сохранения оригинала сообщения в Хранилище в параметрах модуля KSMG должен быть активирован параметр **Поместить исходное сообщение в Хранилище.** Сообщения помещаются в Хранилище вместе с вложениями.



???????? ??????? ??????????? ? KUMA

Чтобы настроить обогащение событий KSMG ссылкой на почтовое сообщение, помещенное в Хранилище KSMG, создайте правило обогащения:

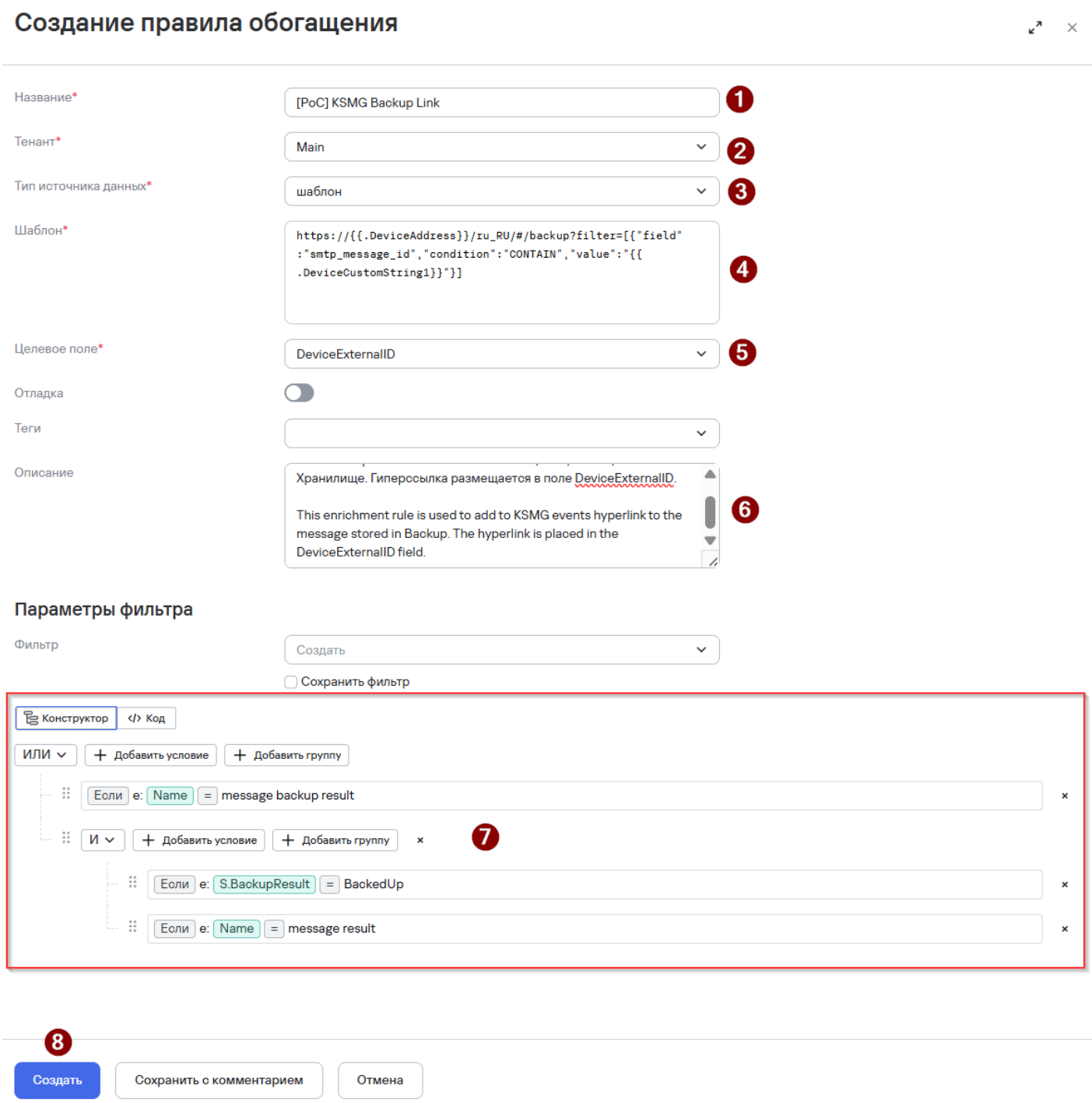
- В веб-интерфейсе KUMA перейдите в раздел **Ресурсы** ? **Правила обогащения**.
- Нажмите на кнопку **Создать**.
- В появившемся окне **Создание правила обогащения**:
  - В поле **Название** введите уникальное имя правила.
  - В раскрывающемся списке **Тенант** выберите, к какому тенанту относится этот ресурс.
  - В раскрывающемся списке **Тип источника данных** выберите шаблон.
  - В поле **Шаблон** укажите следующий шаблон ссылки:

```
https://{{.DeviceAddress}}/ru_RU/#/backup?filter=[{"field":"smtp_message_id","condition":"CONT
AIN","value":"{{.DeviceCustomString1}}"}]
```

- В поле **Целевое поле** укажите **DeviceExternalID.**
- Опционально добавьте **Описание**.
- В секции **Параметры фильтра** укажите условия определения событий KSMG, в которые будет добавляться ссылка. Переключитесь на **Код** и укажите следующее условие:

```
Name = 'message backup result'
OR (
S.BackupResult = 'BackedUp'
AND
Name = 'message result'
)
```

- Нажмите **Создать**.

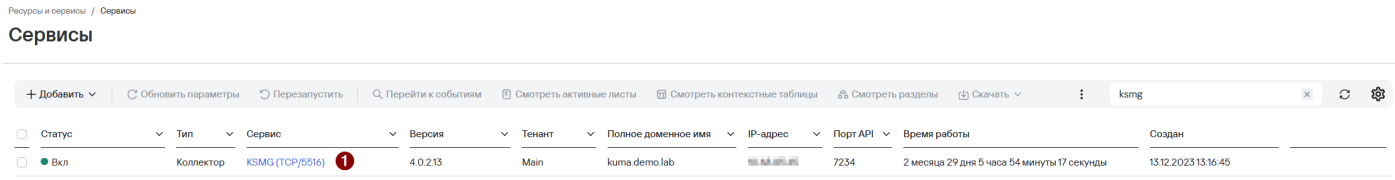


Далее созданное правило обогащения необходимо применить в Коллекторе для приема и обработки событий KSMG.

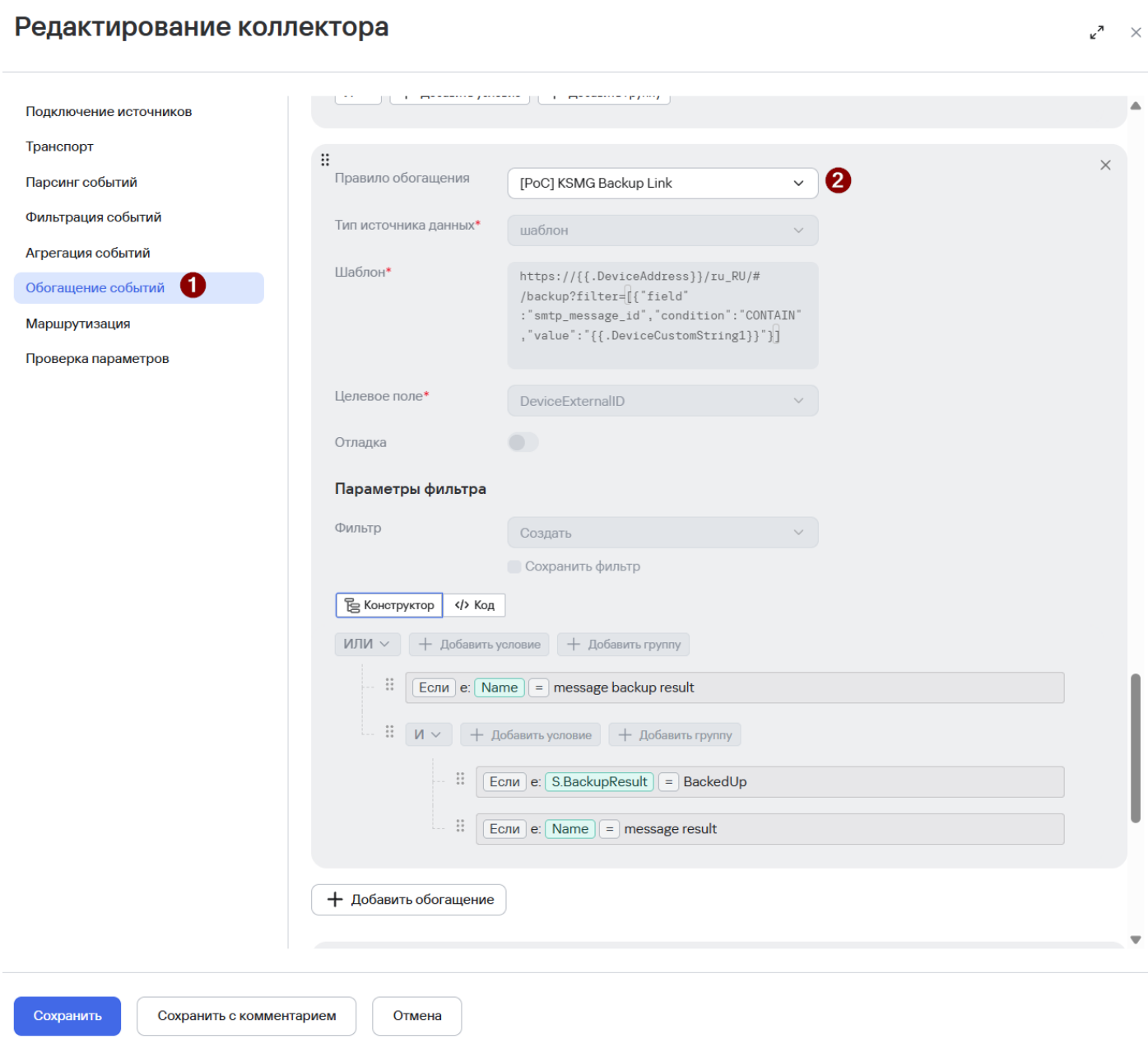
?????????? ??????? ?????????? ? ?????????? KSMG

Чтобы добавить созданное правило обогащения в Коллекторе для приема и обработки событий KSMG:

- Перейдите в раздел **Ресурсы** ? **Активные сервисы.**
- Выберите **Коллектор**, который используется для приема и обработки событий KSMG.

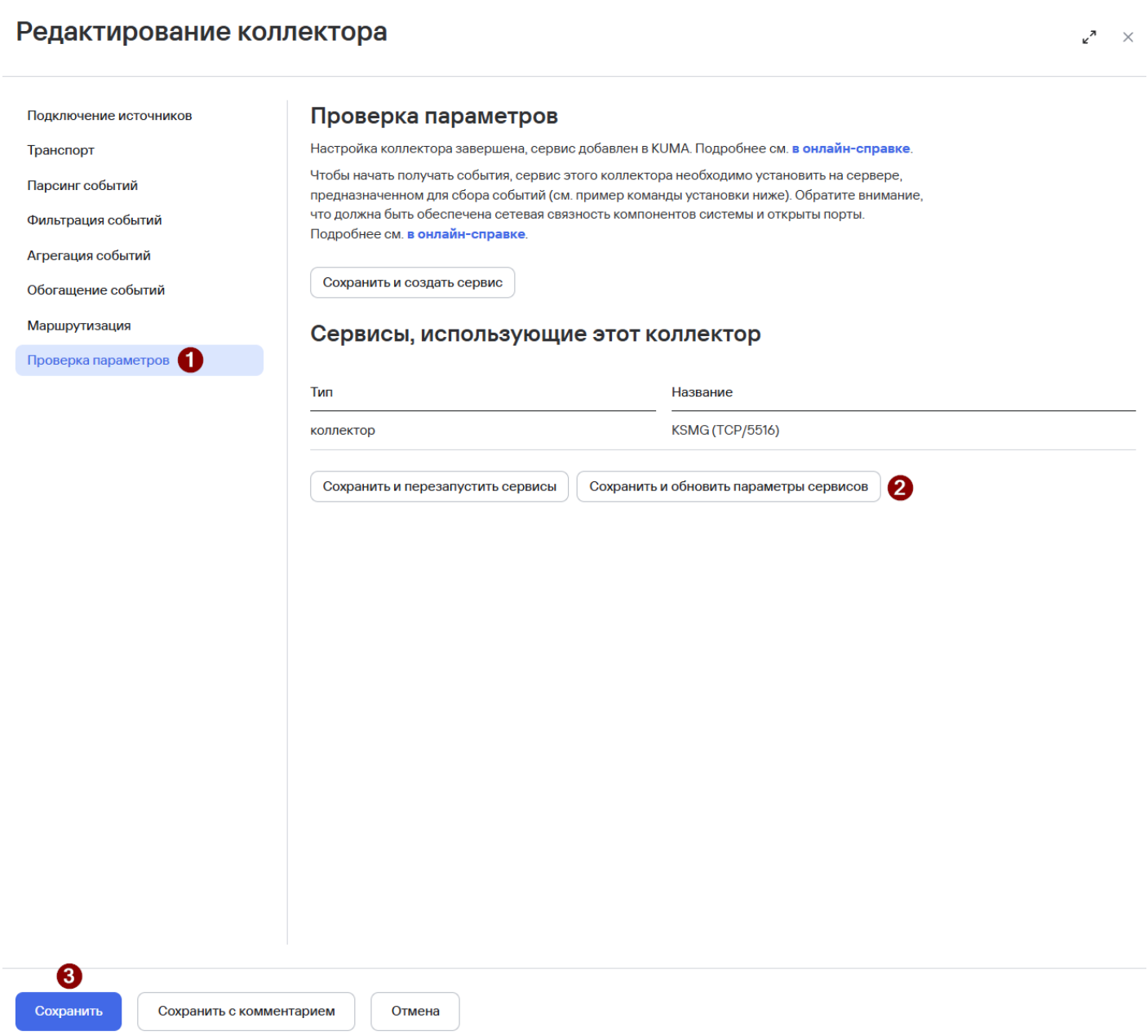


- В окне **Редактирование коллектора** перейдите на шаг **Обогащение событий** и нажмите **Добавить обогащение**.
- В поле **Правило обогащения** выберите ранее созданное правило обогащения.



- Перейдите на шаг **Проверка параметров** и нажмите **Сохранить и обновить параметры сервисов**.

- Нажмите **Сохранить**.



???????? ???????? ? ????????? KSMG ?? ???????? ??????? KUMA

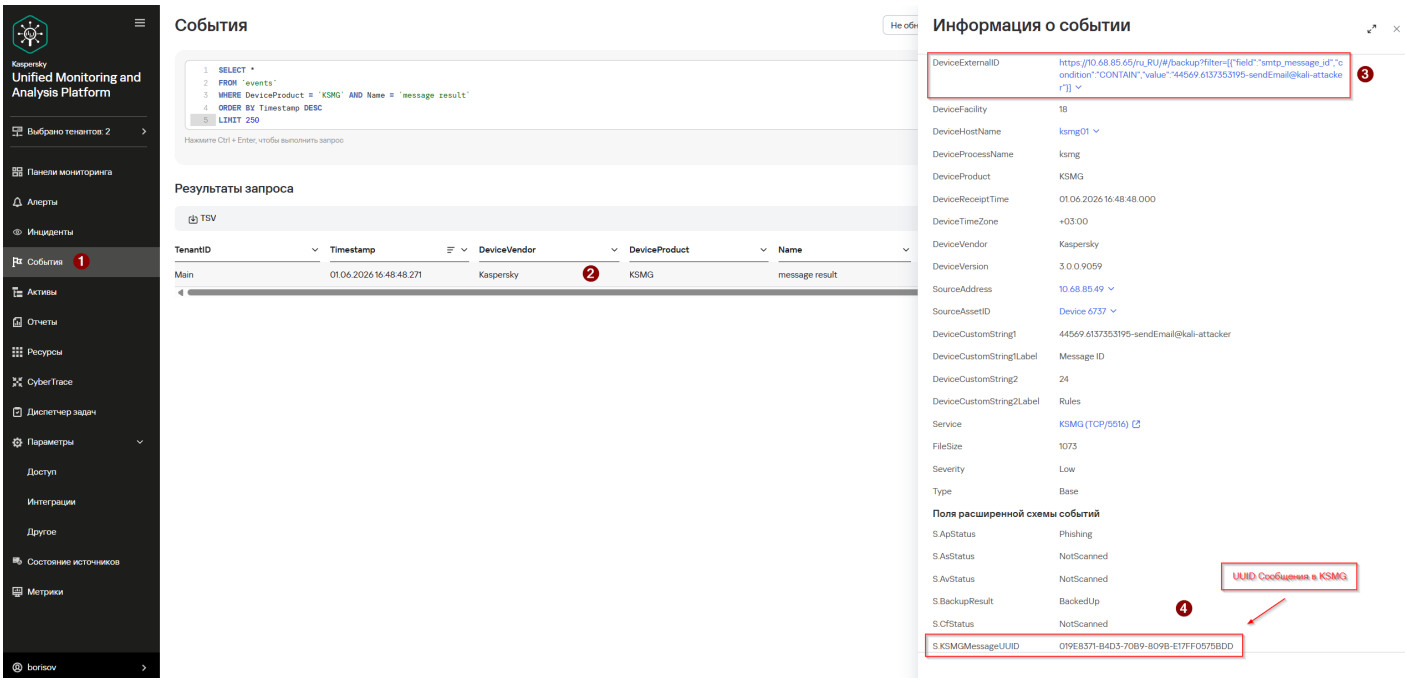
- В разделе **События** выполните поиск событий типа **message backup result** или **message result**

```
SELECT *
FROM `events`
WHERE Name = 'message backup result' AND DeviceProduct = 'KSMG'
ORDER BY Timestamp DESC
LIMIT 250
```

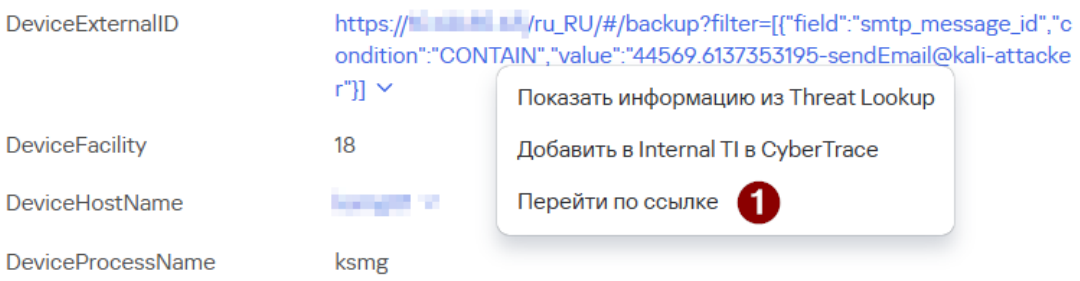
ИЛИ

```
SELECT *
FROM `events`
WHERE Name = 'message result' AND DeviceProduct = 'KSMG'
ORDER BY Timestamp DESC
LIMIT 250
```

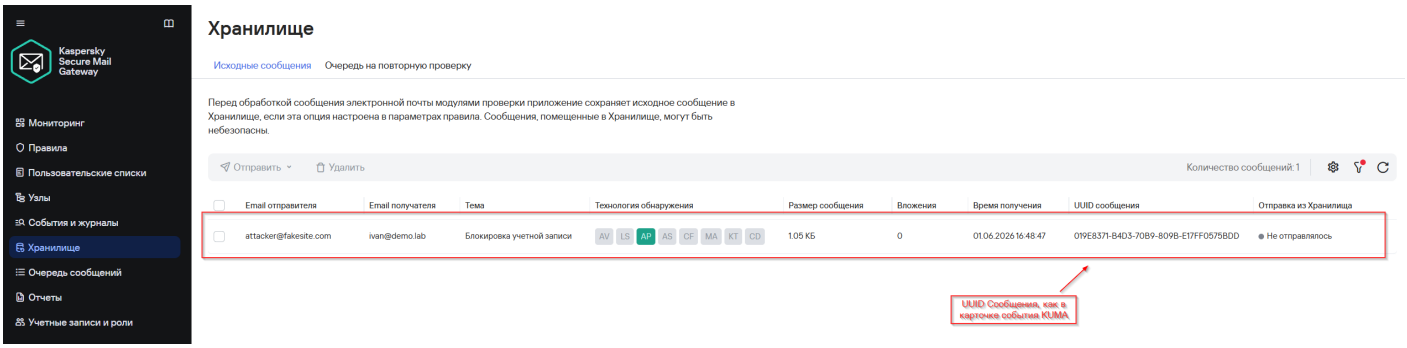
- Откройте карточку события и убедитесь, что в поле **DeviceExternalID** появилась ссылка для перехода в Хранилище KSMG.



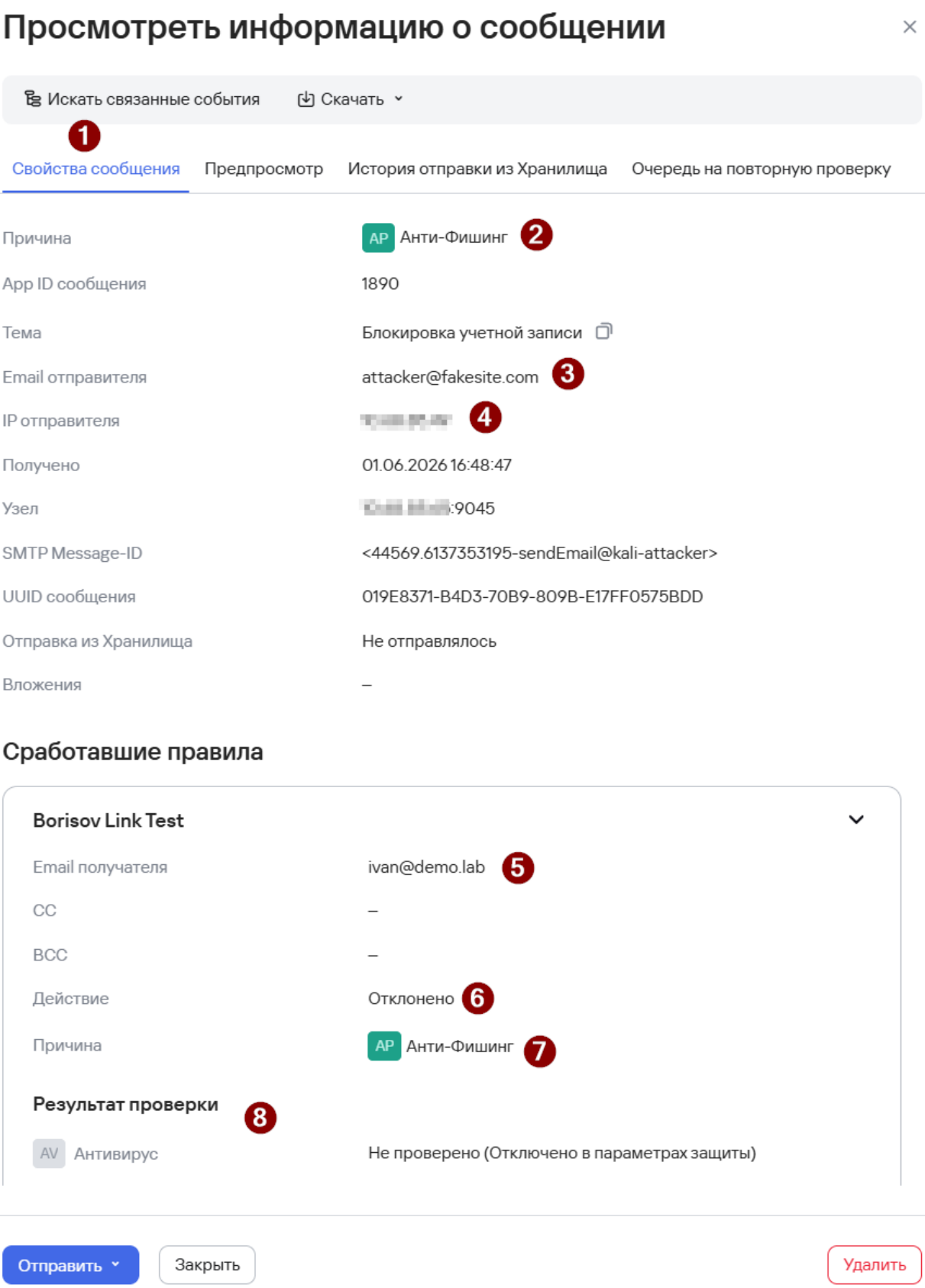
- Выполните переход по ссылке.



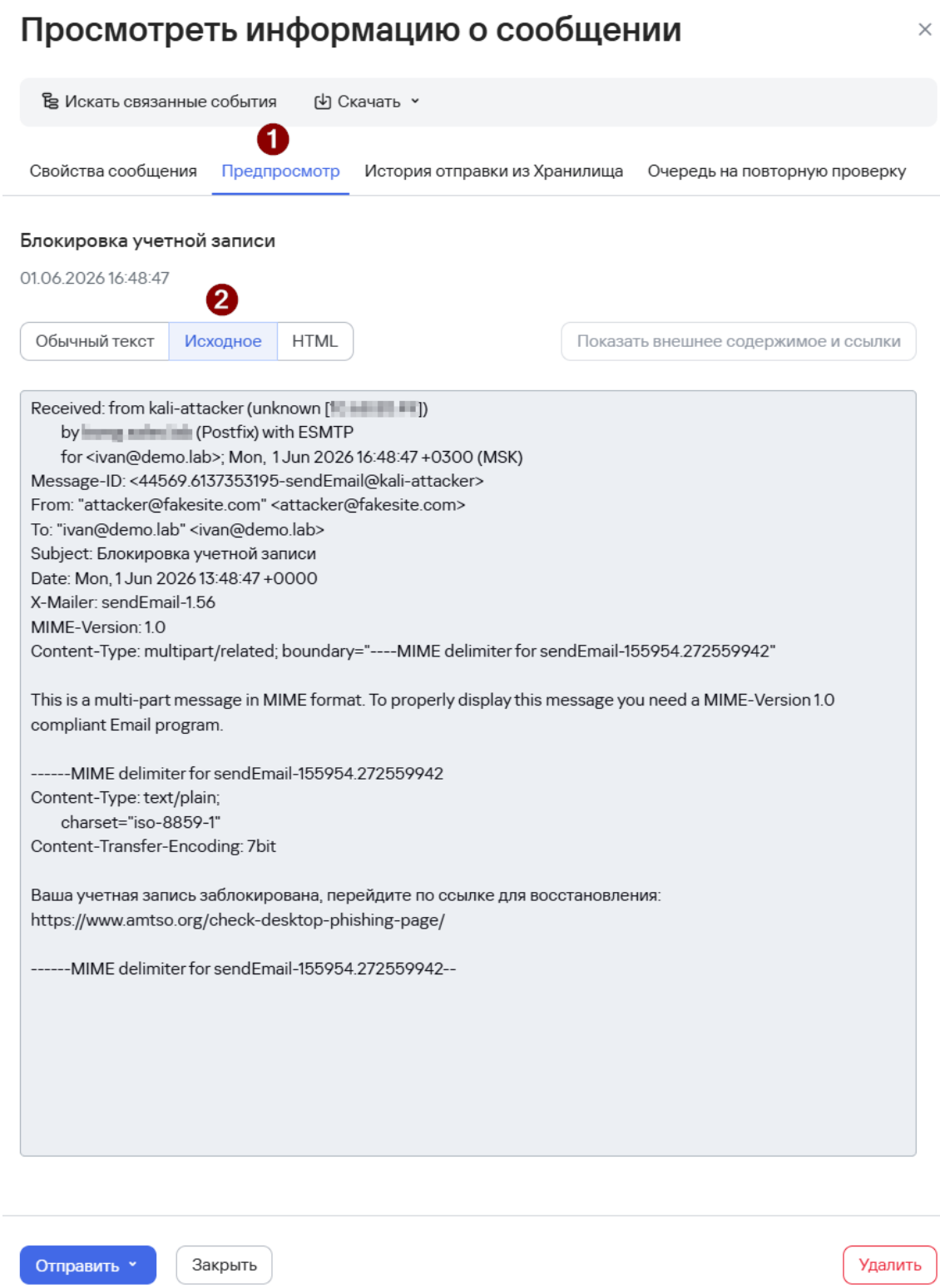
- В результате будет выполнен переход в Хранилище KSMG с фильтром по сообщению — будет отображаться только то почтовое сообщение, результаты анализа которого представлены в карточке события KUMA.



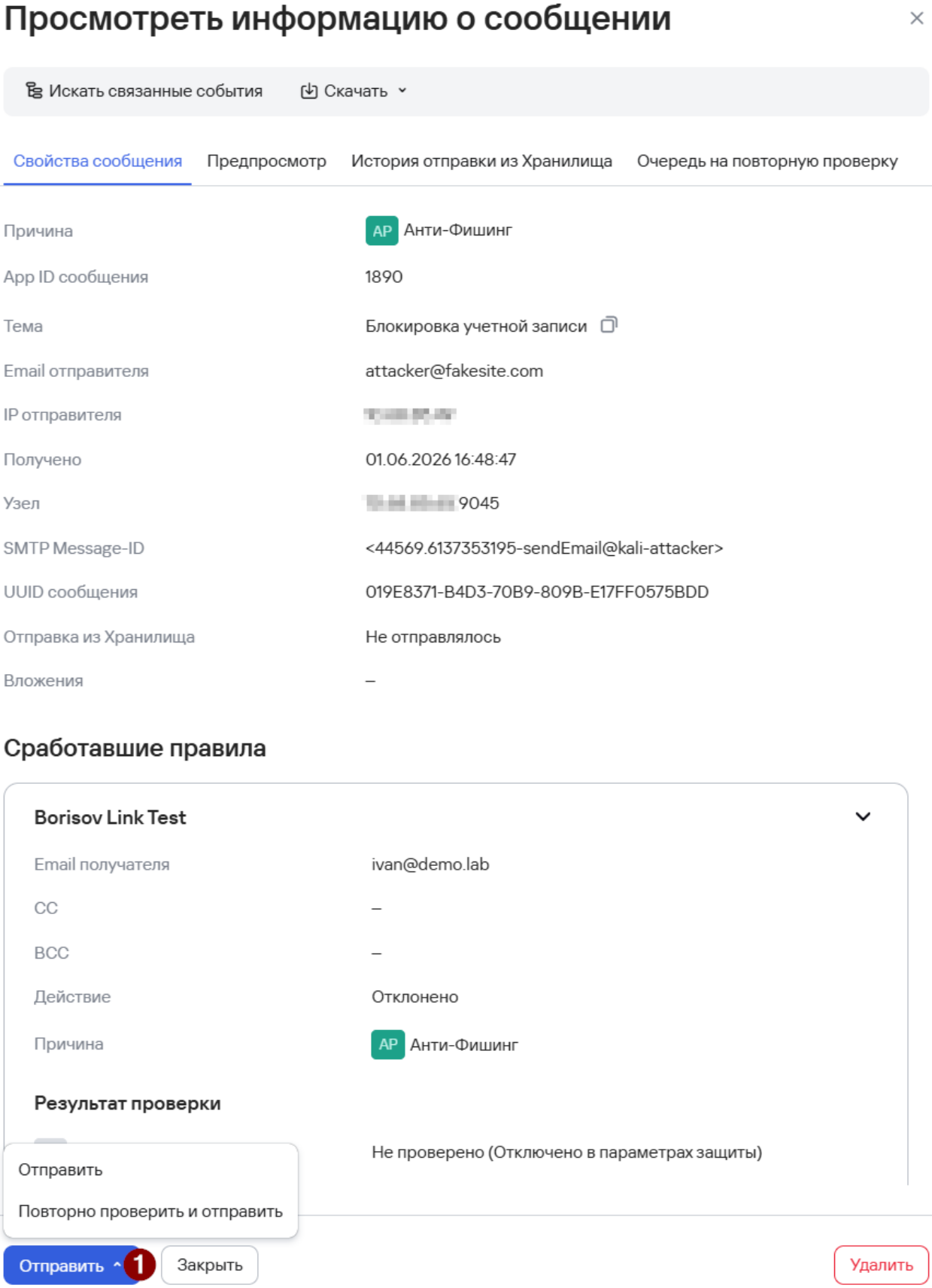
- Далее аналитик в интерфейсе KSMG может:
  - Просмотреть свойства сообщения (причину блокировки сообщения, данные отправителя, сработавшие правила).



- Выполнить предпросмотр сообщения, чтобы ознакомиться с оригинальным текстом сообщения.



- Скачать сообщение в формате eml.
- Выполнить отправку сообщения пользователю в случае False Positive или отправить на повторную проверку.



Revision #8
Created 2026-05-29 15:07:49 UTC by Dmitry Borisov
Updated 2026-06-01 14:52:09 UTC by Dmitry Borisov