Интеграция с Active Directory (LDAP-обогащение)

> 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.com/KUMA/4.0/ru-RU/217926.htm

> Видео «Обогащение событий данными с LDAP сервера»: https://rutube.ru/video/e07d36a0ad26ad29143c4aca8e58c672/?playlist=540937

При наличии интеграции KUMA со службой каталогов Active Directory появляется возможность импортировать информацию о доменных учетных записях пользователей.

Перечень импортируемых атрибутов доступен в онлайн-справке.

После настройки интеграции информация об учетных записях Active Directory становится доступной в карточке событий, окне алертов и инцидентов. Данные из LDAP можно использовать при обогащении событий в коллекторах и в аналитике. Также становится доступным возможность ручного или автоматического запуска действий по реагированию через Active Directory:

- Добавить учетную запись в группу
- Удалить учетную запись из группы
- Сбросить пароль учетной записи
- Блокировать учетную запись

Настройка интеграции KUMA с Active Directory включает следующие этапы:

- Создание секрета в KUMA
- Создание подключения к LDAP-серверу
- Импорт информации о пользователях из Active Directory
- Настройка обогащения событий данными Active Directory

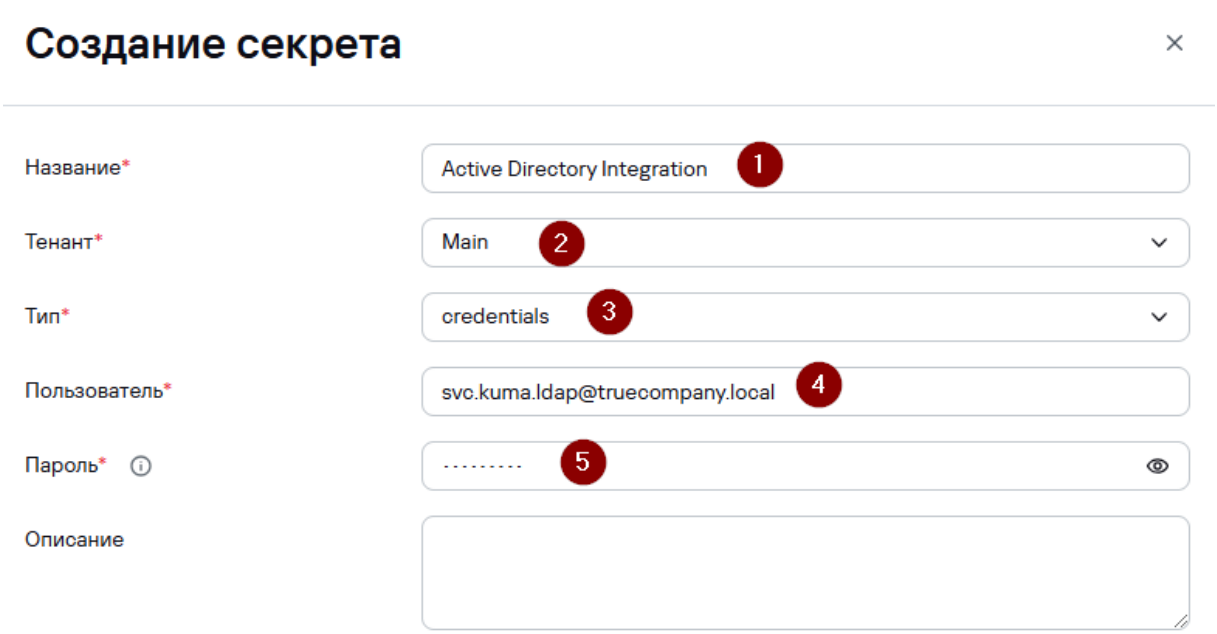
- Проверка работы обогащения

Создание секрета в KUMA

> Для импорта информации о доменных учетных записях пользователей предварительно создайте в домене сервисную учетную запись, которая будет использоваться для интеграции KUMA с Active Directory.

После создания сервисной учетной записи требуется добавить секрет в веб-интерфейсе KUMA. Этот ресурс будет хранить учетные данные для подключения к Active Directory. Чтобы создать секрет в KUMA выполните следующие действия:

- Откройте раздел веб-интерфейса KUMA **Ресурсы** → **Секреты**. Отобразится список доступных секретов.
- Нажмите на кнопку **Добавить**, чтобы создать новый секрет.
- В появившемся окне **Создание секрета** введите данные секрета:
  - В поле **Название** укажите имя для добавляемого секрета.
  - В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать создаваемый ресурс.
  - В раскрывающемся списке **Тип** выберите **credentials**.
  - В поле **Пользователь** укажите имя созданной сервисной учетной записи (может быть указано в одном из двух форматов: <user>@<domain> или <domain>\<user>).
  - В поле **Пароль** укажите пароль учетной записи.
  - Нажмите **Создать**.

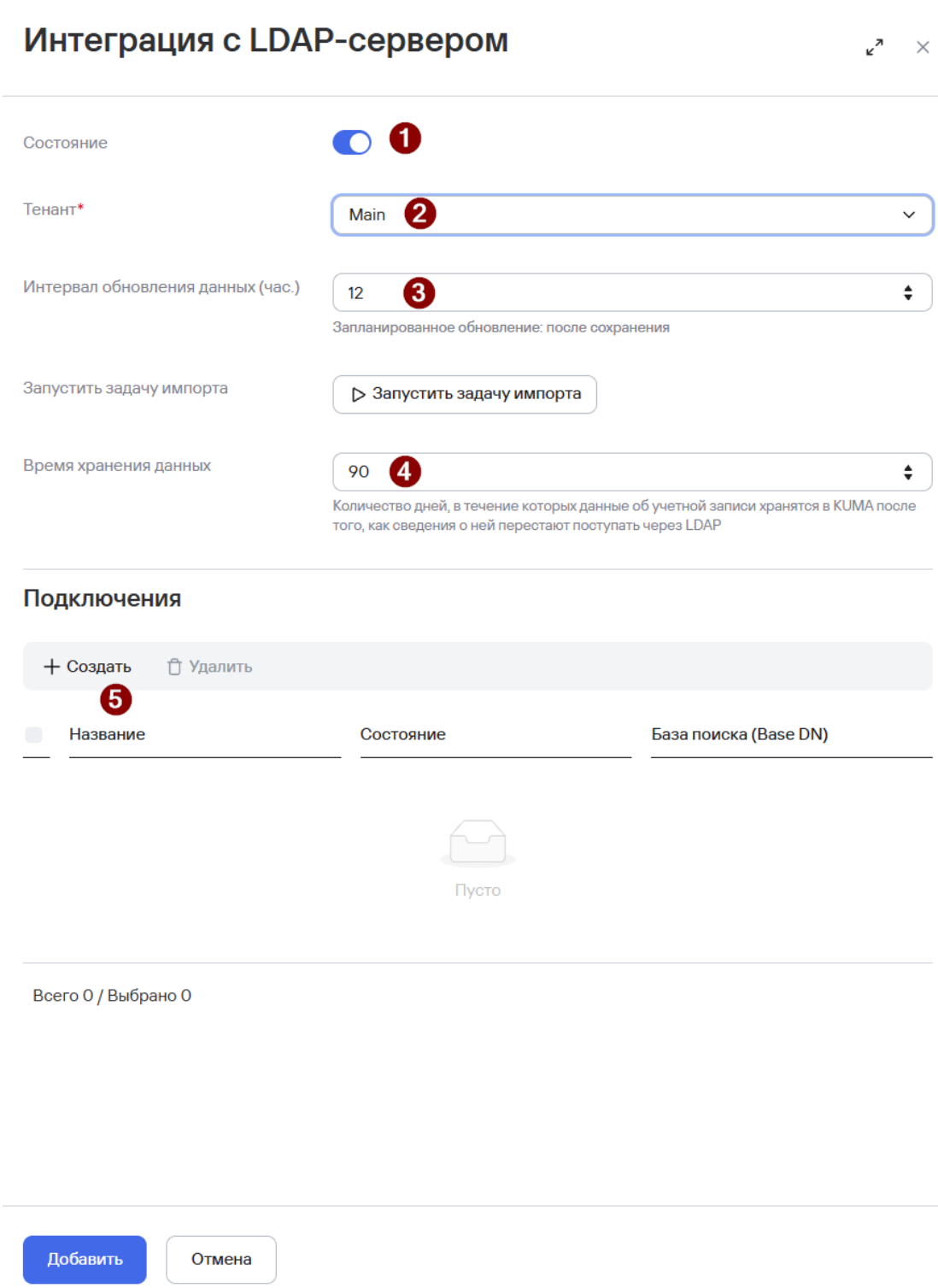


Из соображений безопасности после сохранения секрета строки, указанные в полях **Пользователь** и **Пароль,** скрываются

Создание подключения к LDAP-серверу

Чтобы создать LDAP-подключение к Active Directory:

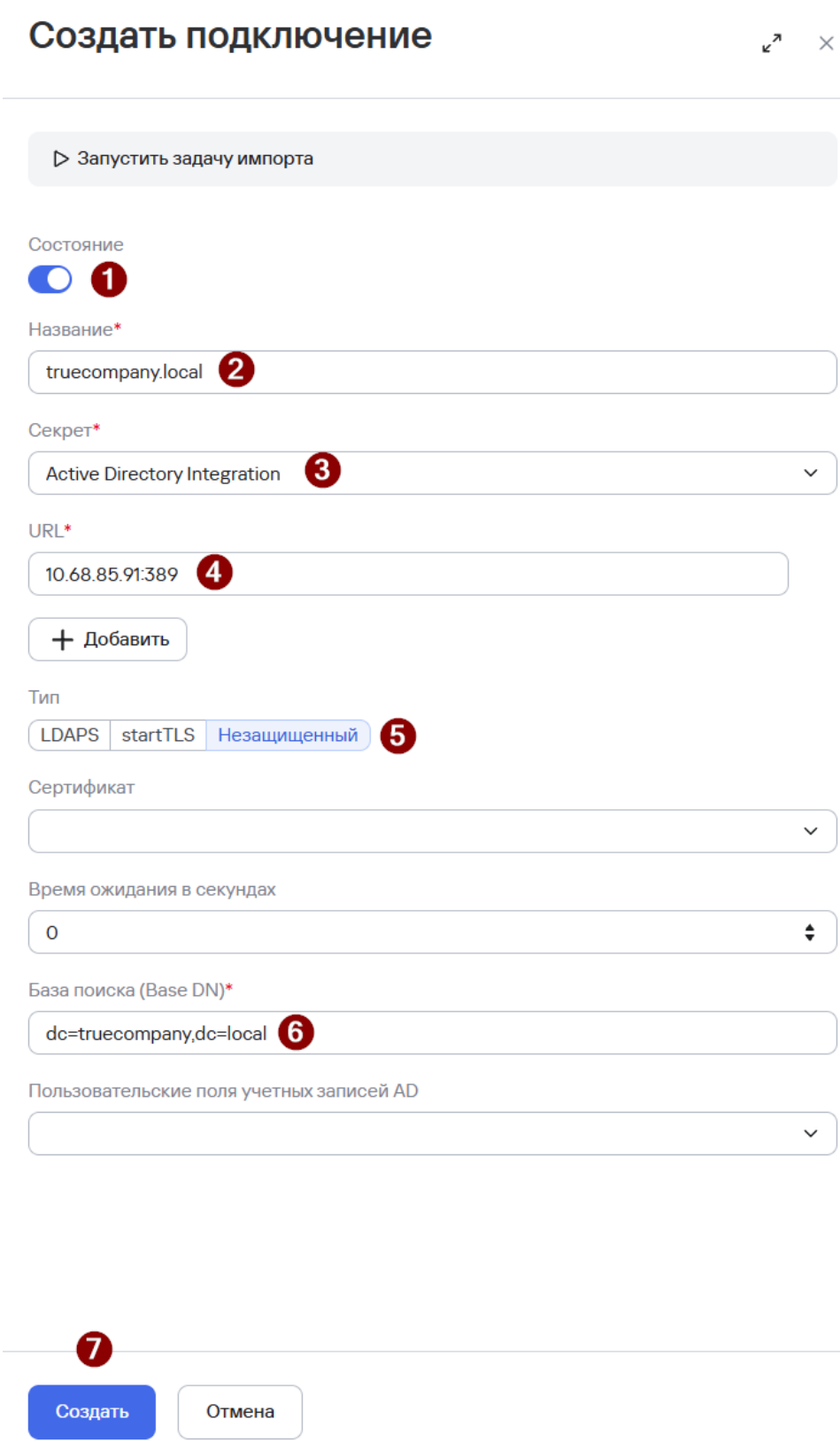
- Перейдите в раздел **Параметры** → **Интеграции** → **LDAP-сервер** в веб-интерфейсе KUMA.
- Откроется окно **Интеграция с LDAP-сервером по тенантам**.
- Нажмите на кнопку **Добавить параметры для нового тенанта**.
- В появившемся окне **Интеграция с LDAP-сервером** активируйте параметр **Состояние**, выберите тенант и укажите **Интервал обновления данных (час.)** (по умолчанию, 12 часов) и **Время хранения данных** (по умолчанию, 90 дней).
- Далее в секции **Подключения** нажмите **Создать**.



- В появившемся окне **Создать подключение**:
  - Активируйте параметр **Состояние**.
  - В поле **Название** введите уникальное имя LDAP-подключения.
  - В поле **Секрет** укажите ранее созданный секрет для подключения к Active Directory.
  - В поле **URL** введите адрес контроллера домена в формате <hostname или IP-адрес сервера>:<порт>. Вы можете указать адреса нескольких серверов с контроллерами домена на случай, если один из них будет недоступен, нажав на кнопку **Добавить.** Все указанные серверы должны находиться в одном

домене.

- В поле **Тип** выберите один из следующих вариантов (в нашем примере будет использоваться **Незащищенный** тип. В продуктивной среде рекомендуется использовать один из вариантов с использованием шифрования передаваемых данных **startTLS** или **LDAPS**):
  - **LDAPS**.
    - При использовании LDAPS устанавливается шифрованное соединение по порту 636.
  - **startTLS**.
    - При использовании метода startTLS сначала устанавливается незащищенное соединение по порту 389, а затем отправляется запрос на шифрование. Если команда STARTTLS завершается с ошибкой, соединение обрывается. Убедитесь, что порт 389 открыт.
  - **Незащищенный**.
- Если на предыдущем шаге вы включили TLS-шифрование, добавьте TLS-сертификат. Следует использовать сертификат удостоверяющего центра, которым подписан сертификат сервера LDAP.
- В поле **Время ожидания в секундах** укажите сколько времени требуется ожидать ответа от сервера контроллера домена.
- В поле **База поиска (Base DN)** введите базовое отличительное имя каталога, в котором должен выполняться поисковый запрос.
- Нажмите на кнопку **Создать**.

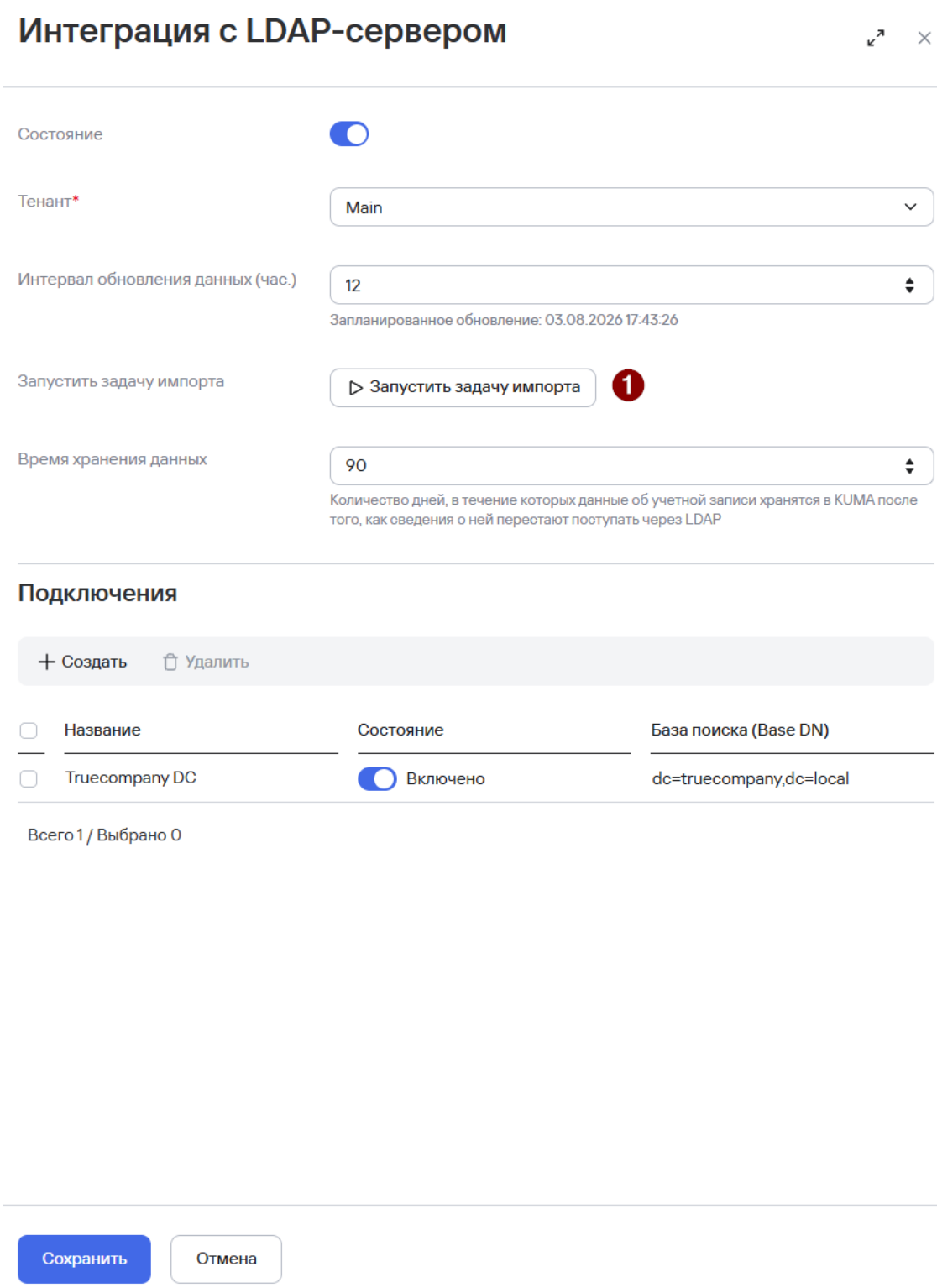


LDAP-подключение к Active Directory создано и отображается в окне **Интеграция с LDAP-сервером**. Нажмите **Добавить**.

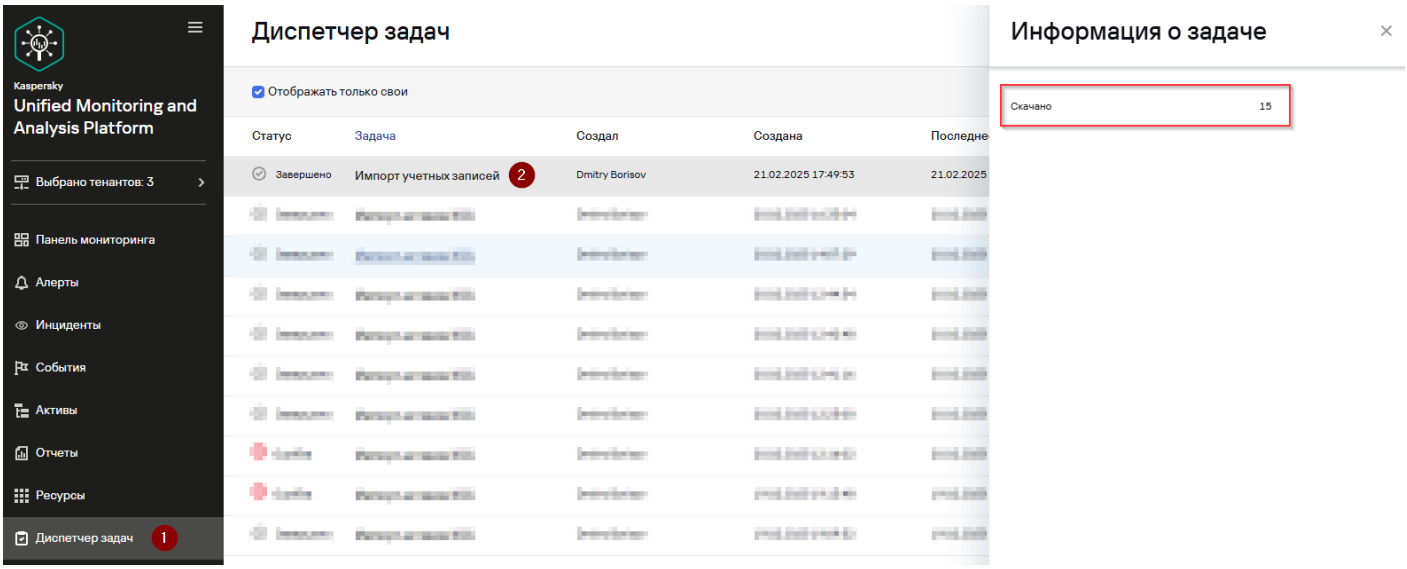
Импорт информации о пользователях из Active Directory

Чтобы выполнить импорт информации о пользователях из Active Directory:

- Откройте веб-интерфейс KUMA и перейдите в раздел **Параметры → Интеграции → LDAP**.
- Выберите тенант, в котором ранее было создано подключение к Active Directory.
- В появившемся окне **Интеграция с LDAP-сервером** нажмите на кнопку **Импортировать учетные записи**. Будет создана задача по импорту учетных записей.



- Перейдите в раздел **Диспетчер задач**.
- Нажмите на задачу **Импорт учетных записей** со статусом **Завершено**. В окне справа **Информация о задаче** будет указано количество учетных записей, информация о которых была импортирована в KUMA.



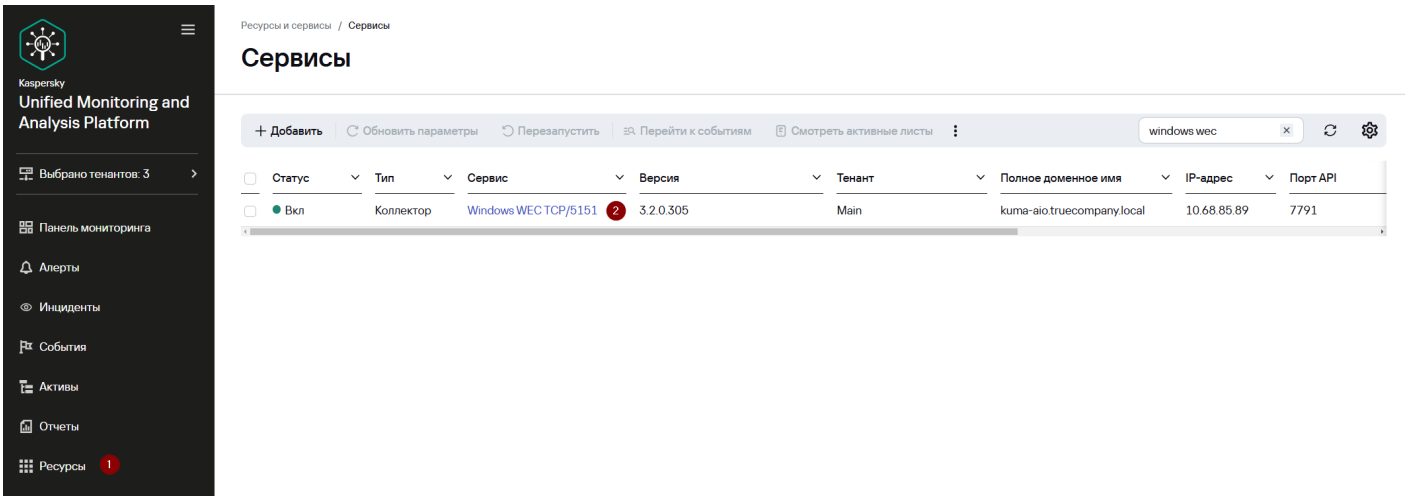
Информация об учетных записях успешно импортирована.

Настройка обогащения событий данными Active Directory

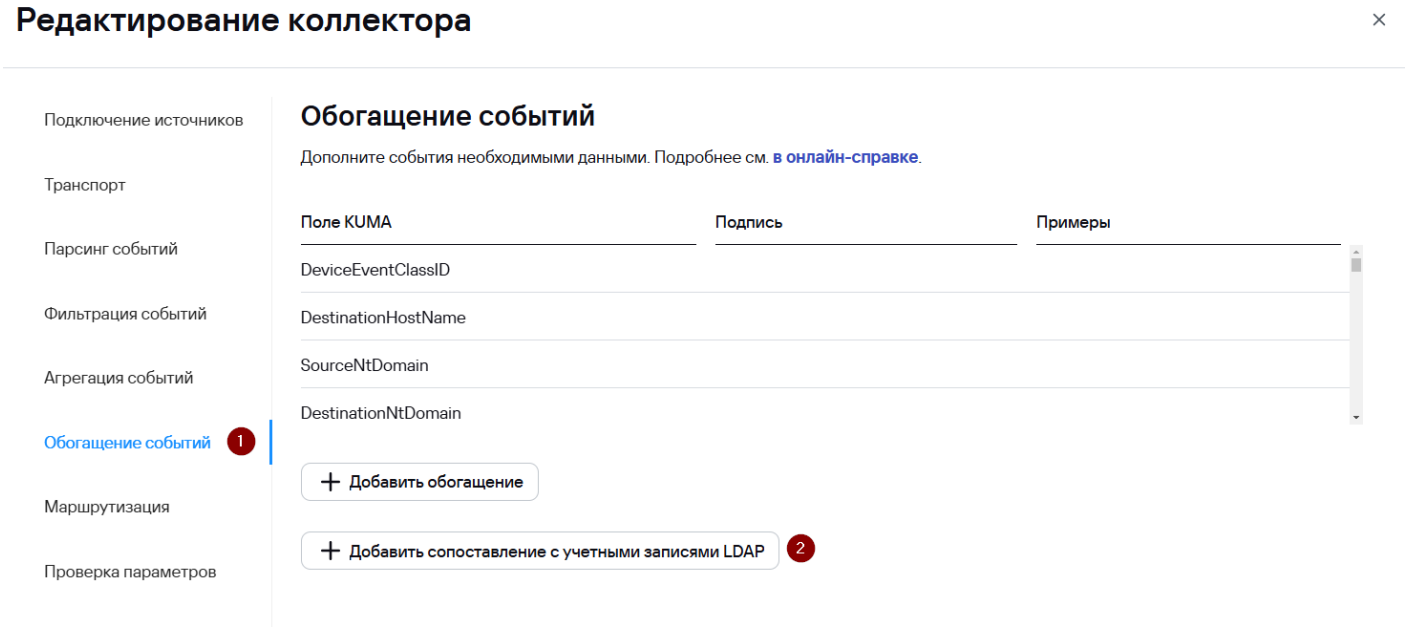
Обогащение событий данными Active Directory настраивается на уровне коллектора и позволяет дополнить события информацией о доменных учетных записях (атрибутах, импортированных из AD). На основе полученных атрибутов доступно выполнение действий по реагированию с помощью Active Directory, а также написание правил корреляции по атрибуту memberOf. Остальные атрибуты, импортируемые из AD, служат справочной информацией и используются при расследовании алертов и инцидентов.

Чтобы настроить обогащение событий данными Active Directory:

- Перейдите в раздел **Ресурсы → Активные сервисы**.
- Выберите ранее созданный сервис коллектора для сбора и обработки событий Windows.



- В появившемся окне **Редактирование коллектора** перейдите на шаг **Обогащение событий** и нажмите **Добавить сопоставление с учетными записями LDAP**.

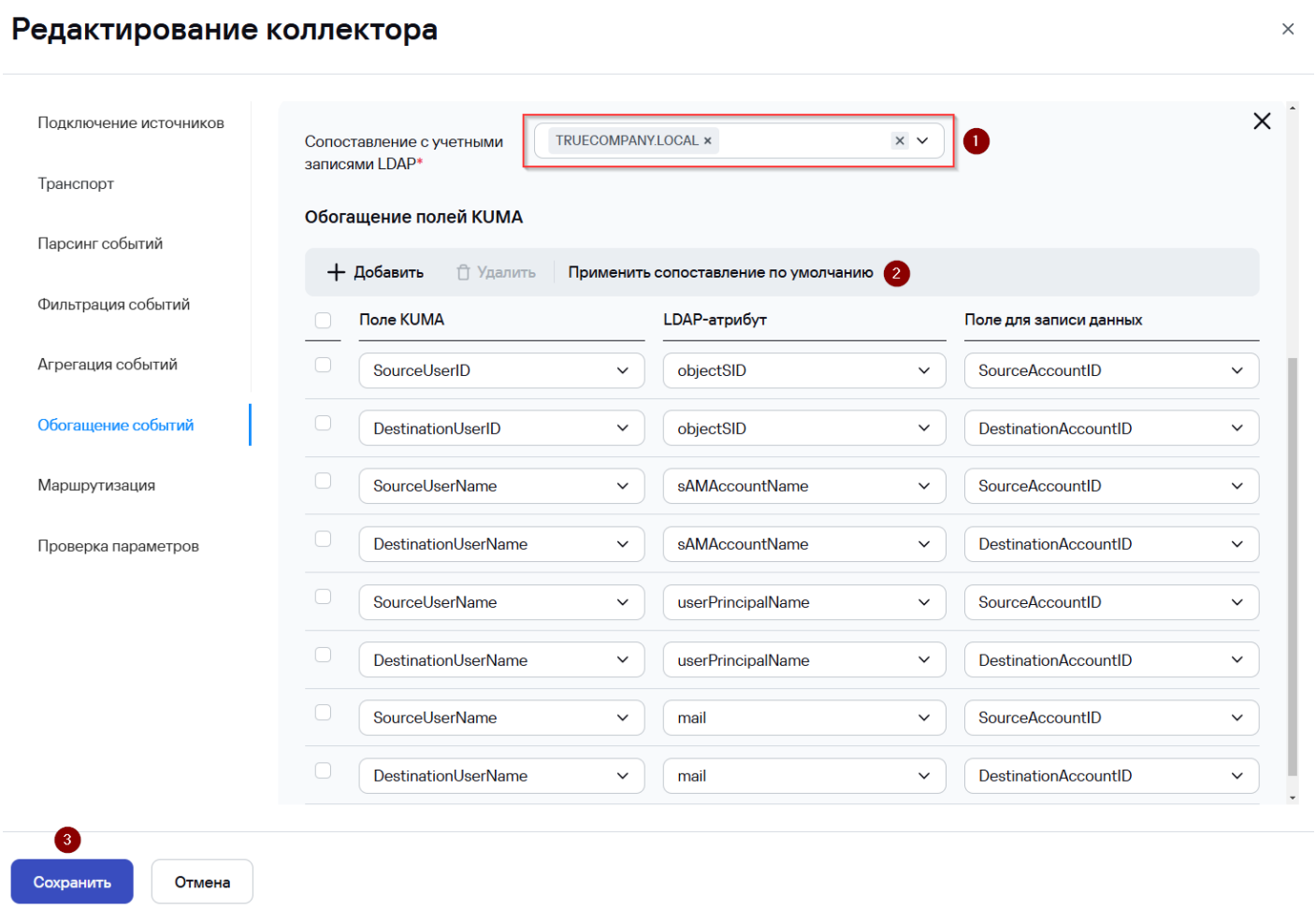


- Откроется блок параметров обогащения с помощью LDAP.
- В поле **Сопоставление с учетными записями LDAP** введите домен (в верхнем регистре), из которого ранее был выполнен импорт учетных записей. Доменов можно указать несколько.

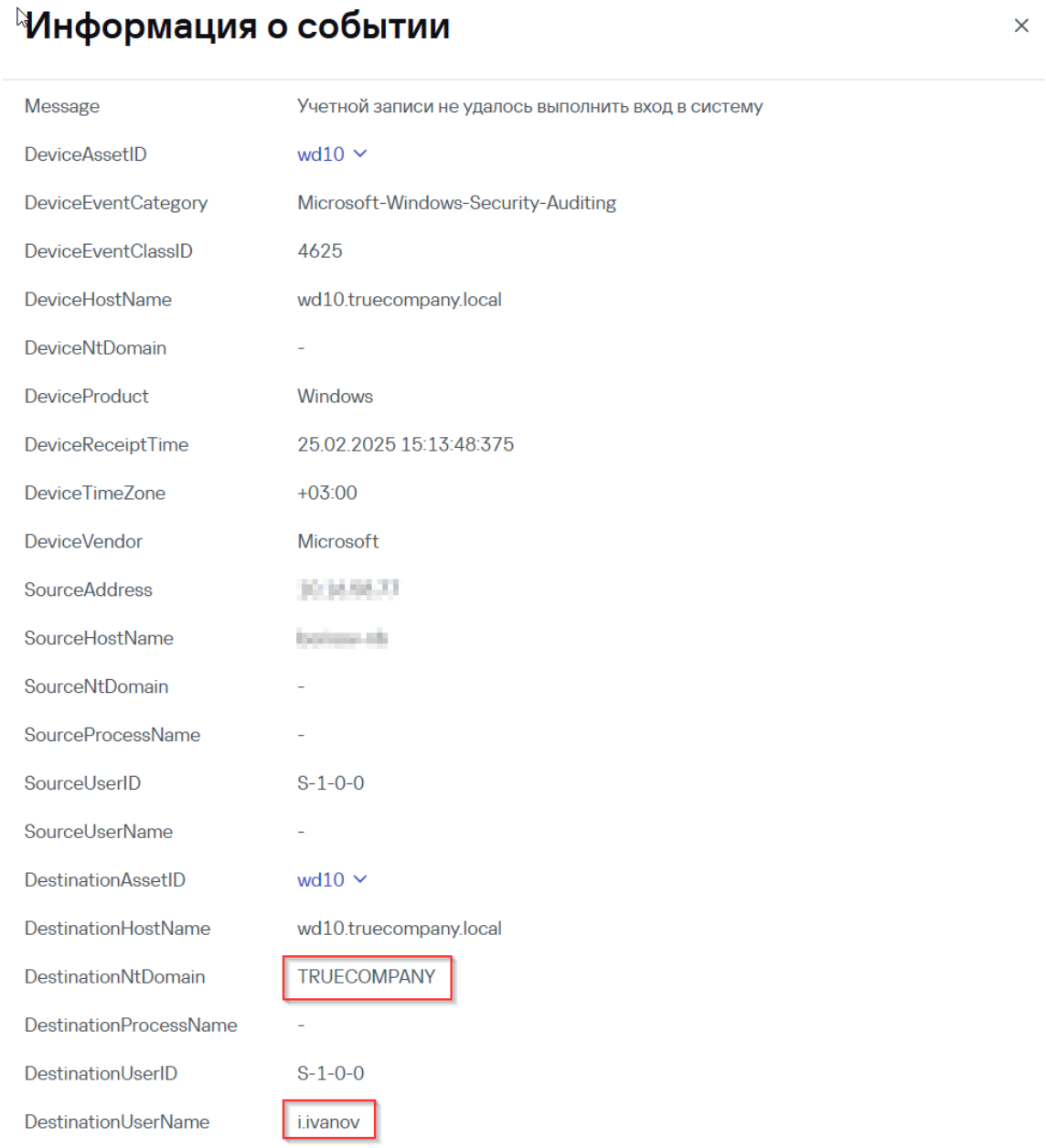
> В случае, если Вы не знаете полного наименования домена для импортированных учетных записей, подключитесь к компоненту Ядра KUMA по SSH. Далее воспользуйтесь следующей статьей.

- В таблице **Обогащение полей KUMA** нажмите **Применить сопоставлению по умолчанию** для заполнения таблицы сопоставления стандартными значениями.
  - В **поле KUMA** указывается поле события KUMA, данные из которого следует сравнить с атрибутом LDAP.

- В **столбце LDAP-атрибут**, указывается атрибут, с которым необходимо сравнить поле события KUMA.
- В столбце **Поле для записи данных** указывается, в какое поле события KUMA следует поместить идентификатор пользовательской учетной записи, импортированной из LDAP, если сопоставление было успешно.



- В событиях журналов ОС Windows вместо DNS-имени домена может содержаться NetBIOS-имя, которое не будет совпадать с DNS-именем домена, импортированных в KUMA учетных записей. Например, TRUECOMPANY вместо TRUECOMPANY.LOCAL.



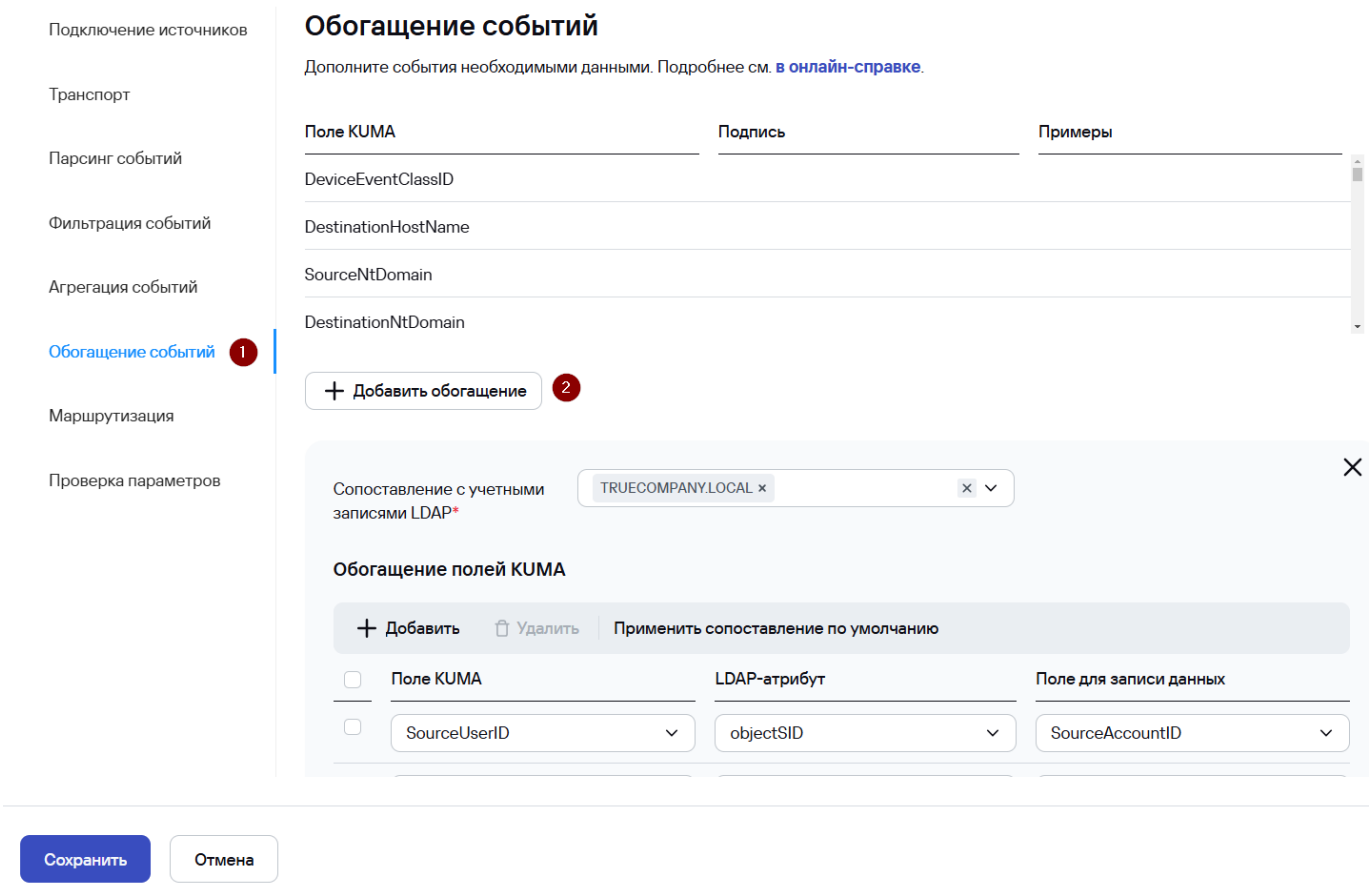
Поэтому в данном случае для корректной работы LDAP-обогащения необходимо добавить правило обогащения, с помощью которого NetBIOS-имя в полях SourceNtDomain/DestinationNtDomain будет преобразовано в DNS-имя домена.

> Для большого количества доменов рекомендуется настроить обогащение через словарь.

Для настройки правила обогащения:

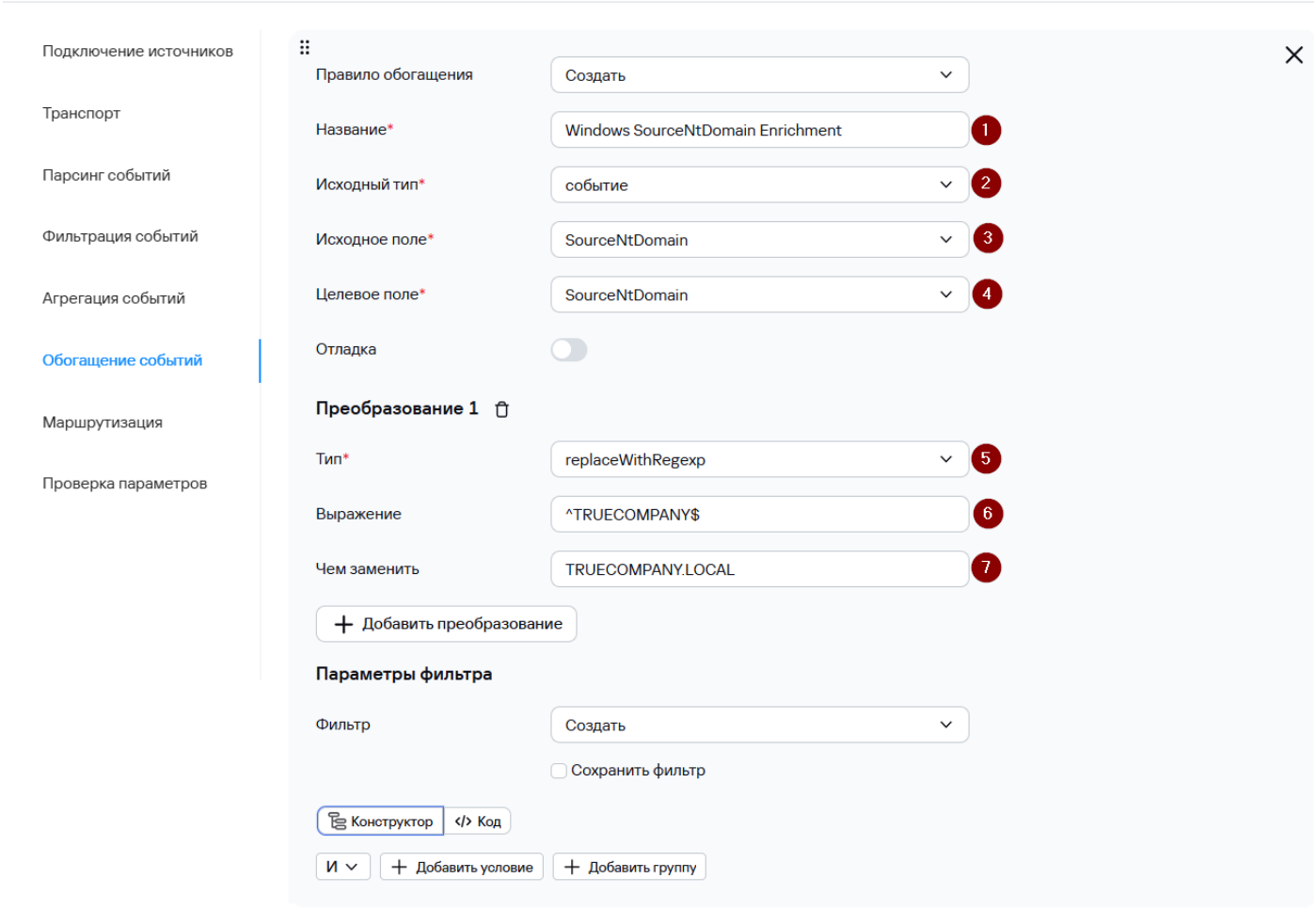
- На шаге **Обогащение событий** нажмите **Добавить обогащение.**

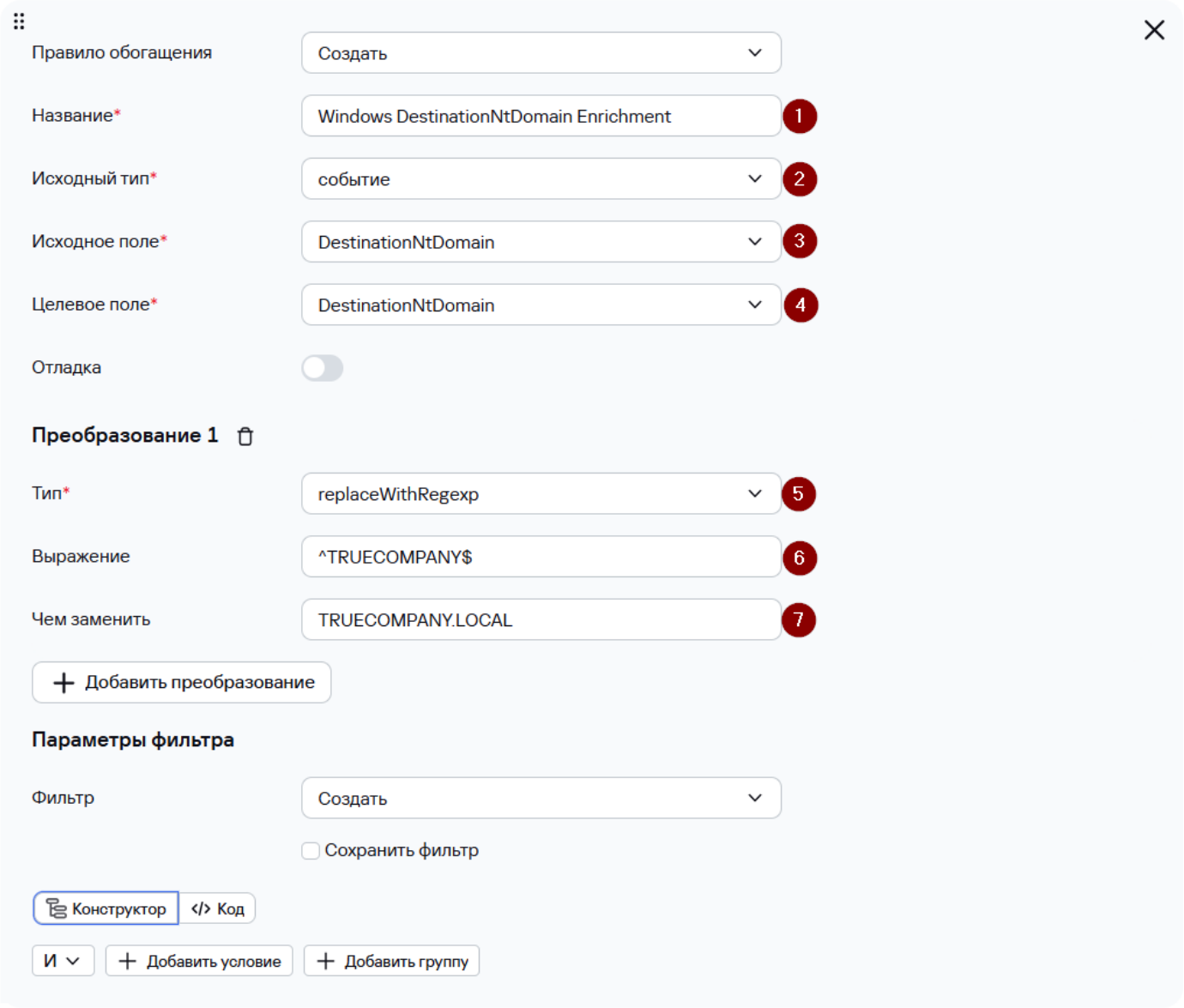
Редактирование коллектора



- В окне правила обогащения укажите:
  - **Название** правила обогащения
  - **Исходный тип** – Событие
  - **Исходное поле** – SourceNtDomain
  - **Целевое поле** – SourceNtDomain
  - Нажмите **Добавить преобразование**
  - Выберите **Тип** преобразования **replaceWithRegexp**
  - В поле **Выражение** укажите регулярное выражение с NetBIOS-именем. В поле **Чем заменить** укажите DNS-имя домена.
- Добавьте аналогичное правило обогащения для поля DestinationNtDomain.

Редактирование коллектора





- Нажмите **Сохранить**.
- В разделе **Активные сервисы** нажмите **ПКМ** на сервис коллектора Windows и далее **Перезапустить**.

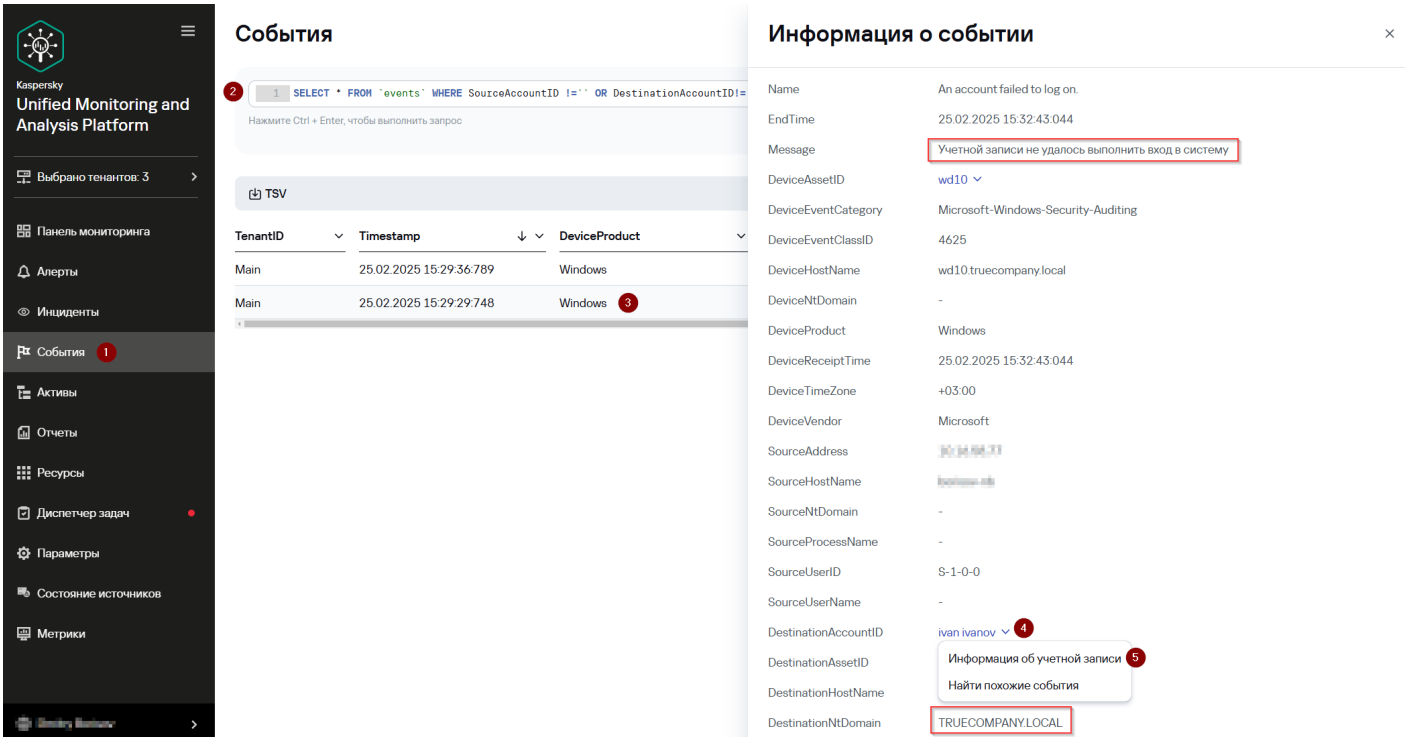
Проверка работы обогащения

- Перейдите в раздел **События** и укажите следующий поисковый запрос:

```
SELECT * FROM `events` WHERE SourceAccountID !='' OR DestinationAccountID!='' ORDER BY
Timestamp DESC LIMIT 250
```

- В результате будут выведены события, обогащенные информацией об учетных записях Active Directory.
- Нажмите на одно из событий в таблице событий.

- В появившемся окне **Информация о событии** нажмите на имя учетной записи и выберите **Информация об учетной записи**.



- Откроется окно **Информация об учетной записи** с данными об учетной записи, полученной из Active Directory.



Обогащение событий Windows данными Active Directory настроено.

> Если обогащение событий информацией из Active Directory не выполняется, попробуйте указать только те домены, которые есть в базе Ядра KUMA. Если эта рекомендация не помогла - попробуйте сделать обогащение только по одному домену.

Приложение А. Настройка минимальных прав для запуска действий по реагированию

Для запуска действий по реагированию через Active Directory рекомендуется создать отдельную доменную группу безопасности и далее добавить в эту группу сервисную УЗ, которая будет использоваться для интеграции KUMA и AD.

Настройка прав для запуска действий по реагированию выполняется за счет настройки ACL на контроллере домена.

ACL (Access Control List, список контроля доступа) - это список, который хранится у каждого объекта Active Directory (пользователя, группы, OU). Данный список определяет, кто и какие действия может выполнять над объектом. Для делегирования прав используется его часть DACL (Discretionary ACL).

ACE (Access Control Entry, запись контроля доступа) - это отдельная запись в ACL. Каждая запись содержит:

- субъект (пользователь или группа, которым выдаётся право);
- тип (Allow, то есть разрешить, или Deny, то есть запретить; Deny имеет приоритет);
- право (например, чтение или запись атрибута, сброс пароля);
- объект права (конкретный атрибут или extended right, например userAccountControl, member, Reset Password);
- область действия (на какой класс объектов распространяется: user, group; наследуется ли на дочерние объекты).

Просмотр и изменение ACL объектов Active Directory выполняется с помощью встроенной утилиты **dsacls**.

Для настройки ACL на контроллере домена запустите PowerShell с правами администратора домена или УЗ с правом изменения ACL и выполните следующие команды:

> В качестве примера ниже права назначаются на весь OU **Users** для группы **OSMP LDAP Response**

- Для сброса пароля учетных записей

```
dsacls "OU=Users,OU=HQ,DC=demo,DC=lab" /I:S /G "DEMO\OSMP LDAP Response:CA;Reset
Password;user"
```

```
dsacls "OU=Users,OU=HQ,DC=demo,DC=lab" /I:S /G "DEMO\OSMP LDAP Response:WP;pwdLastSet;user"
```

- Для блокировки УЗ:

```
dsacls "OU=Users,OU=HQ,DC=demo,DC=lab" /I:S /G "DEMO\OSMP LDAP
Response:WP;userAccountControl;user"
```

- Для добавления/удаления учетных записей из группы:

> Право member выдаётся на объект группы, членством в которой нужно управлять (в примере — группа Quarantine). Если таких групп несколько, его можно выдать на OU с этими группами с параметром /I:S. **Рекомендуется не выдавать право на OU с привилегированными группами**

```
dsacls "CN=Quarantine,OU=Groups,OU=HQ,DC=demo,DC=lab" /G "DEMO\OSMP LDAP Response:WP;member"
```

Для проверки назначенных прав введите команду:

```
dsacls "OU=Users,OU=HQ,DC=demo,DC=lab" | Select-String "OSMP LDAP Response" -Context 0,3
```

> Для привилегированных УЗ и групп (`adminCount=1`) делегированные права не применяются: их ACL периодически перезаписывается. Поэтому действия по сбросу пароля или отключению таких УЗ, а также изменению состава таких групп выполнены не будут.

> Для сервисной учётной записи рекомендуется:
> - запретить интерактивный вход и вход через RDP (политики Deny log on locally и Deny log on through Remote Desktop Services);
> - задать длинный случайный пароль;
> - включить и настроить на контроллерах домена аудит событий 4724 (сброс пароля), 4725/4722 (отключение/включение УЗ), 4728/4732/4756 (добавление в группы), 4729/4733/4757 (удаление из групп), 4738 (изменение УЗ);
> - настроить сбор этих событий в KUMA.

Revision #29
Created 2023-08-11 14:33:12 UTC by Boris Rzr
Updated 2026-10-27 09:49:27 UTC by Dmitry Borisov