

## Механизмы авторизации, протокол OAuth 2.0

Сервер Star Wars API предоставляет доступ к информации любому, кто попросит. Заходи кто угодно, запрашивай что хочешь.

Однако большинство API не столь щедры: для доступа к данным сервисы требуют аутентификации, а авторизация ограничивает пользователю доступ. Даже в «общедоступном» (на первый взгляд) Star Wars API пользователи ограничены в правах: например, ни один анонимный пользователь не может изменить, добавить или удалить информацию: анонимные пользователи не авторизованы для таких действий.

Освежим в памяти понятия «авторизация» и «аутентификация».

**Авторизация** (англ. *authorization*, «разрешение, одобрение») — предоставление пользователю прав на выполнение каких-то действий («...пользователю по имени Стас Басов разрешён доступ ко всем, даже самым секретным данным проекта»).

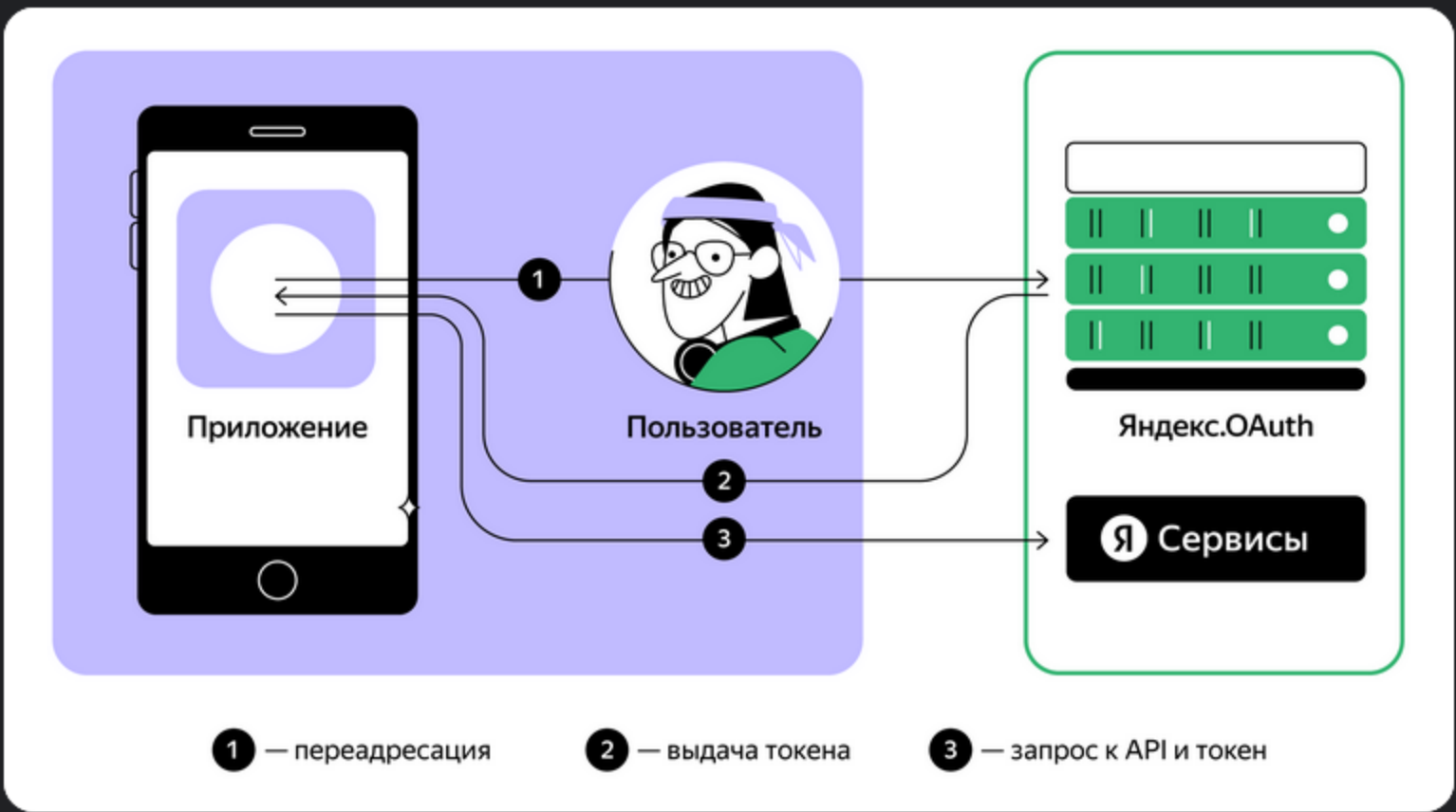
**Аутентификация** (англ. *authentication*, «опознание») — процедура проверки подлинности пользователя («...а ты точно Стас Басов? Покажи документики или токен!»).

Представьте, что вы поехали отдыхать и вам нужна виза. **Авторизацию** можно сравнить с получением этой визы, процессом её изготовления.

Допустим, вы успешно получили визу (прошли процесс **авторизации**) и прилетели на отдых: пограничник проверит вашу визу, сравнит фотографию и паспортные данные — выполнит процедуру **аутентификации** и пропустит вас через границу, если вы на это авторизованы. И каждый раз, когда вы вновь решите посетить эту страну, вам будет нужно пройти процедуру **аутентификации** на паспортном контроле.

Вы часто проходите авторизацию и аутентификацию по логину и паролю: вы входите в систему и получаете предоставленный доступ к сервису. Но иногда нужно предоставить лишь частичный доступ. Например, вы просите другого человека загрузить фотографии в свой аккаунт социальной сети, но не хотите давать доступ к вашим личным сообщениям. Или вы пишете приложение для автоматической загрузки фотографий в социальную сеть, но не хотите наделять эту программу полным доступом к своей учётной записи. Тут на помощь приходит протокол авторизации OAuth.

**OAuth** (Open Authorization) — это схема авторизации, предоставляющая третьей стороне (другому пользователю или приложению) ограниченный доступ к ресурсам сервиса от вашего имени, без необходимости передавать логин и пароль. Это становится возможным благодаря **OAuth-токену**.



**Токен** (англ. *token*, «опознавательный знак, жетон») — это уникальная строка из цифр и латинских букв, он может выглядеть так:

```
854234bfefcf1f000d92df5e4c5e8858b9ebcb4821e12cd806add07e17f587c4c93e3b50d5adbdae2b2
```

OAuth-токен выдаётся пользователю для упрощения доступа к серверу. Это что-то вроде пропуска для входа на определённый ресурс. Такой пропуск может быть временным — выдаваться на какой-то срок — или бессрочным.

В обычной жизни вы, например, можете выдать своему другу «токен» с ограниченными правами — доверенность на машину. Друг сможет управлять вашей машиной, но у него не будет права её продать.

При аутентификации достаточно лишь «показать пропуск» — передать токен вместе с запросом на сервер. По этому токену сервер поймёт, кто к нему обращается и к каким данным владелец токена имеет доступ.

Если злоумышленник завладеет вашим токеном (найдёт на улице ваш пропуск), то он получит доступ к данным и сможет совершать запросы от вашего имени; крайне важно хранить токен в секрете и никому его не сообщать. А если беда всё же случилась — токен можно отозвать в любой момент, это удобно и добавляет безопасности.

Отметьте верные утверждения:

- ☐ При аутентификации на основе логина и пароля информация о пользователе не хранится ни на сервере, ни на его компьютере.
- ☐ OAuth-токен — это официальный бумажный документ, доверенность, которую можно выдать любому пользователю информационной системы, чтобы он мог представлять интересы других пользователей этой системы.
- ☒ OAuth-токен может быть временным или бессрочным
- Верно.
- ☒ Авторизация — предоставление пользователю прав на выполнение определённых действий
- Верно.

Ваше знакомство с базовой теорией по API окончено. Коротко о главном по теме — в [шпаргалке](#).