

Запрос кода авторизации

Необходимо запустить OAuth2 Authorization Code Flow with PKCE, и сгенерировать две случайные строки, уникальные для каждого запроса авторизации:

- `code_verifier`
- `state`

Хранить их необходимо в хранилище сеансов. Не раскрывать `code_verifier` третьим лицам. Не показывайте его в URL-адресах, не злоупотребляйте состоянием для его хранения, не отправляйте по небезопасным соединениям. Однако это нормально, если пользователь сам может извлечь `code_verifier`, что всегда будет возможно для полностью клиентских приложений.

После авторизации пользователь будет перемещен на `redirect_uri`.

Если авторизация не удалась, к перенаправлению будут добавлены следующие параметры строки запроса:

- `error`, в частности со значением `access_denied`, если пользователь отменил авторизацию
- `error_description` для облегчения отладки
- `state`, точно такое, как передано в параметре состояния

Если авторизация прошла успешно, к перенаправлению будут добавлены следующие параметры строки запроса:

- `code`, содержащий свежий кратковременный код авторизации
- `state`, точно такое, как передано в параметре состояния

Затем, чтобы защититься от подделки межсайтовых запросов, необходимо убедиться, что возвращаемое состояние соответствует состоянию, которое изначально сгенерировали.

Query параметры:

<code>response_type</code> обязательный	Должен быть <code>code</code>
<code>client_id</code> обязательный	Произвольный идентификатор, для индификации приложения.
<code>redirect_uri</code> обязательный	Абсолютный URL-адрес, на который следует перенаправить пользователя с результатом авторизации.
<code>code_challenge_method</code> обязательный	Должен быть <code>S256</code>
<code>code_challenge</code> обязательный	Вычислить <code>BASE64URL(SHA256(code_verifier))</code>
<code>scope</code>	Список запрошенных областей действия OAuth, разделенных пробелами, если таковые имеются.
<code>state</code>	Произвольное состояние, которое будет возвращено дословно с результатом авторизации.