СТАНДАРТ БАНКА РОССИИ

ОТКРЫТЫЕ ПРОГРАММНЫЕ ИНТЕРФЕЙСЫ

Получение информации о банковских счетах Пользователя. Описание взаимодействия

Дата введения: 2026–10–01
Версия: 2.0.0

Москва
2025

Оглавление

1. ПРЕДИСЛОВИЕ

Настоящий стандарт разработан Ассоциацией развития финансовых технологий (Ассоциацией ФинТех) при участии Центрального банка Российской Федерации (Банка России).

ПРИНЯТ И ВВЕДЕН в действие приказом Банка России от 19 декабря 2025 года № ОД-2890 «О введении в действие стандарта Банка России СТО БР «О введении в действие стандарта Банка России СТО БР «Открытые программные интерфейсы. Получение информации о банковских счетах Пользователя. Описание взаимодействия» и внесении изменения в пункт 1 приказа Банка России от 23 октября 2020 года № ОД-1725».

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Банка России.

2. ВВЕДЕНИЕ

Настоящий стандарт содержит общее описание элементов, которые являются общими для всех API на получение информации о банковских счетах (далее – счета) Пользователя третьей стороной.

2.1 Область применения

Настоящий стандарт рекомендован к использованию организациями при обмене финансовыми сообщениями в среде Открытых программных интерфейсов.

Настоящий стандарт предназначен для:

- участников обмена информацией о финансовых продуктах, счетах и других финансовых инструментах Пользователя, а также связанной с ними информацией;
- разработчиков информационного и программного обеспечения.

Положения настоящего стандарта носят рекомендательный характер и применяются совместно со следующими документами:

- Стандарт Банка России СТО БР ФАПИ.СЕК-1.6-2024 «Безопасность финансовых (банковских) операций. Прикладные программные интерфейсы обеспечения безопасности финансовых сервисов на основе протокола OpenID» (далее - ФАПИ.СЕК).
- Стандарт Банка России СТО БР ФАПИ.ПАОК-1.0-2024 «Безопасность финансовых (банковских) операций. Обеспечение безопасности финансовых сервисов при инициации OpenID Connect клиентом потока аутентификации по отдельному каналу» (далее - ФАПИ.ПАОК).
- Стандарт Банка России СТО БР «Открытые программные интерфейсы. Общие положения».
- Стандарт Банка России СТО БР «Открытые программные интерфейсы. Глоссарий».
- •Стандарт Банка России СТО БР «Открытые программные интерфейсы. Профиль для расширенного режима безопасности».Стандарт Банка России СТО БР «Открытые программные интерфейсы. Получение информации о банковских счетах Пользователя. Правила взаимодействия».

- Стандарт Банка России СТО БР «Открытые программные интерфейсы. Получение согласия на доступ к информации о банковских счетах Пользователя. Методы для физических лиц».
- Стандарт Банка России СТО БР «Открытые программные интерфейсы. Получение согласия на доступ к информации о банковских счетах Пользователя. Методы для юридических лиц».
- Стандарт Банка России СТО БР «Открытые программные интерфейсы. Получение информации о банковских счетах Пользователя. Методы для физических лиц».
- Стандарт Банка России СТО БР «Открытые программные интерфейсы. Получение информации о банковских счетах Пользователя. Методы для юридических лиц».
- Другими документами комплекса стандартов Открытых API, размещенными на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет».

2.2 Термины и определения

В настоящем стандарте применяются термины и определения в соответствии со стандартами ФАПИ.СЕК, ФАПИ.ПАОК, «Открытые программные интерфейсы. Общие положения», «Открытые программные интерфейсы. Глоссарий», а также следующие:

Наименование	**Описание**
Ресурс согласия	Объект данных, представляющий собой разрешение, предоставленное Пользователем (субъектом данных) третьей стороне (СПУ) для доступа к определенным ресурсам или выполнения определенных действий от имени такого Пользователя (субъекта данных). В архитектуре Открытых программных интерфейсов ресурс согласия является основным элементом, который управляет правами доступа и определяет, какие данные или операции с такими данными разрешены
Разрешение	Текстовая константа, уникально определяющая области данных и операции с этими данными, запрашиваемые СПУ для авторизации доступа

Таблица 1. Термины и определения

3. ОБЩЕЕ ОПИСАНИЕ ПРОЦЕССА

В данном разделе описывается взаимодействие при получении информации о счете Пользователя третьей стороной через среду Открытых программных интерфейсов, которые позволяют СПУ:

- инициировать запрос на создание или отзыв ресурса согласия на доступ к информации о банковском счете (далее – доступ к счету);
- получать информацию, связанную со счетом Пользователя.

3.1 Пошаговое описание

Шаг 1 – Запрос информации по счету:

- Начало потока. Пользователь подтверждает СПУ намерение предоставить доступ к счету для получения сервиса на основе Открытых программных интерфейсов и авторизовать согласие на доступ СПУ к своим данным, содержащее информацию о том, к каким данным Пользователь готов предоставить доступ, срок действия согласия и даты начала и окончания периода операций по счету, к которым относится данное согласие.

Шаг 2 - Настройка согласия на доступ к счету:

- Между СПУ и сервером авторизации ПУ устанавливается защищенный канал связи.
- СПУ, используя тип доступа client credentials, получает на сервере авторизации ПУ токен доступа (access token).
- Между СПУ и сервером ресурсов ПУ устанавливается защищенный канал связи.
- СПУ с помощью запроса POST, используя токен доступа для авторизации, инициирует создание на сервере ресурсов ПУ новый ресурс согласия на доступ к счету. Это действие информирует ПУ о том, что один из его Пользователей намерен предоставить СПУ доступ к информации, относящейся к его счету. ПУ передает в ответе СПУ информацию о создании ресурса согласия на доступ к счету с идентификатором consentId.
- Для одного и того же СПУ может одновременно существовать несколько действующих согласий от одного Пользователя. Каждое такое согласие создается в результате отдельного, независимого процесса авторизации и может иметь разные параметры (например, разные счета (набор счетов) или разрешений).

Шаг 3 - Авторизация согласия:

Для авторизации согласия Пользователь перенаправляется к ПУ. СПУ инициирует процесс авторизации путем перенаправления Пользователя на интерфейс ПУ.

Для этого ПУ может использовать гибридный поток в соответствии с профилем, определенным в документе СТО БР Открытые программные интерфейсы. Профили API для расширенного режима безопасности или созданием потока аутентификации по отдельному каналу (в соответствии с профилем безопасности OpenID API, обозначенному в положениях ФАПИ.ПАОК).

- В случае, если СПУ выполняет запрос на авторизацию согласия, используя поток перенаправления для переадресации конечного Пользователя к ПУ:
  - в потоке перенаправления СПУ перенаправляет Пользователя в интерфейс ПУ;
  - перенаправление содержит consentId, созданный на предыдущем шаге, что позволяет ПУ в последствии идентифицировать согласие на доступ к счету;
  - ПУ аутентифицирует Пользователя;
  - Пользователь выбирает счета, по которым будет производиться обмен информацией со СПУ;
  - Пользователь, пройдя аутентификацию на стороне ПУ, знакомится с параметрами согласия и явно подтверждает (авторизует) его.

- ПУ обновляет статус ресурса согласия на доступ к счету, фиксируя, что согласие было авторизовано;
- По завершению авторизации согласия, Пользователь перенаправляется обратно к СПУ, а код авторизации (authorization code) передаётся СПУ системой ПУ;
- между СПУ и сервером авторизации ПУ устанавливается защищенный канал связи;
- СПУ использует тип доступа authorization code и обменивает на сервере авторизации ПУ код авторизации (authorization code) на токен доступа (access token), который связан с авторизованным согласием на доступ к счету (разрешение на доступ, связанное с согласием).

• В случае, если ПУ запрашивает аутентификацию у Пользователя на устройстве аутентификации, отличном от устройства потребителя, на котором Пользователь взаимодействует со СПУ (поток аутентификации по отдельному каналу):

- СПУ инициирует аутентификацию Пользователя с помощью запроса аутентификации по отдельному каналу;
- запрос содержит подсказку, которая идентифицирует Пользователя, связанного с авторизуемым согласием;
- ПУ аутентифицирует Пользователя и обновляет статус ресурса согласия на доступ к счету (account-consent), фиксируя, что согласие было авторизовано;
- как только согласие было авторизовано, ПУ может сделать обратный вызов для передачи результатов авторизации (auth_req_id) или использовать режим опроса для получения токена доступа (access-token), который связан с авторизованным согласием на доступ к счету (разрешение на доступ, связанное с согласием).
- В данном потоке предполагается, что управление согласием производится между Пользователем и СПУ, поэтому на этом этапе не могут изменяться детали согласия на доступ к счету.
- Пользователь может только полностью авторизовать или отклонить данные о согласии на доступ к счету.

• При успешной авторизации согласия ПУ передает информацию на ПКС (с момента ввода ПКС в промышленную эксплуатацию и принятия необходимых нормативно-правовых актов).

Шаг 4 - Запрос данных:

• Между СПУ и сервером ресурсов ПУ устанавливается защищенный канал связи.

• СПУ, используя для авторизации полученный на шаге 3 токен доступа, при помощи вызова GET /accounts получает идентификаторы счета Пользователя, к которым ему предоставлен доступ (accountId) и выполняет запросы к серверу ресурсов ПУ для получения информации о счете (счетах) Пользователя.

3.2 Диаграмма последовательности

На рисунке 1 представлена диаграмма последовательности потока получения информации о счете:

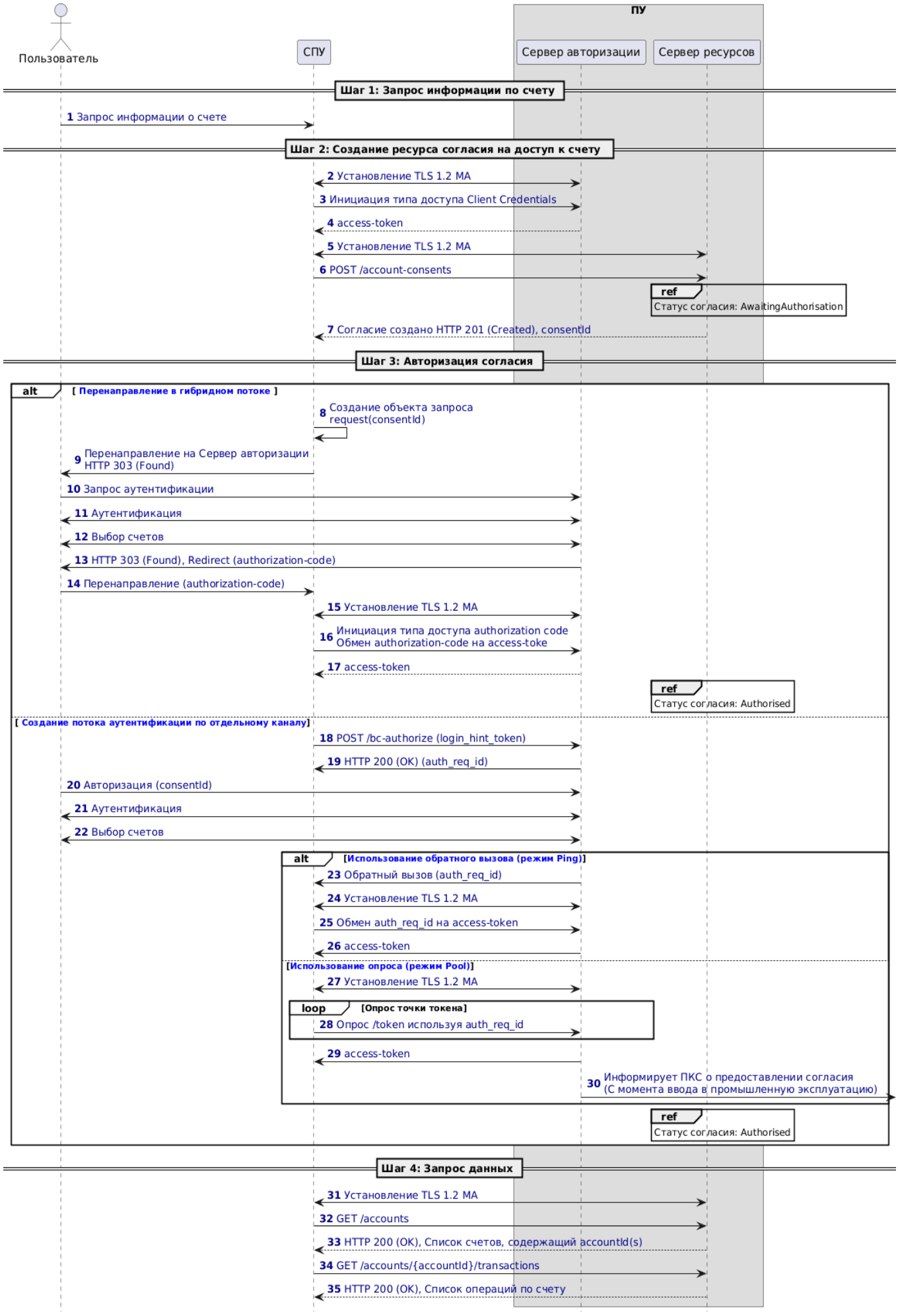

Рисунок 1. Диаграмма последовательности потока получения информации о счете

3.3 Альтернативные потоки и потоки с ошибками

3.3.1 Токен доступа отсутствует или просрочен

Этот поток предполагает, что следующие шаги были успешно выполнены:

- Шаг 1. Запрос информации по счету.
- Шаг 2. Создание согласия на доступ к счету.
- Шаг 3. Авторизация согласия.

В случае предоставления от СПУ в адрес ПУ просроченного или отсутствующего токена доступа в попытке запросить данные, ПУ отвечает ошибкой HTTP 401 (Unauthorized).

Рисунок 2. Токен доступа отсутствует или просрочен

3.3.2 Неполная или некорректная полезная нагрузка запроса:

Этот поток предполагает, что следующие шаги были успешно выполнены:

- Шаг 1. Запрос информации по счету.
- Шаг 2. Создание согласия на доступ к счету.
- Шаг 3. Авторизация согласия.

СПУ предоставляет неверно сформированный запрос или запрос с некорректной полезной нагрузкой к ПУ для согласия на доступ к счету. ПУ отвечает ошибкой HTTP 400 (Bad Request).

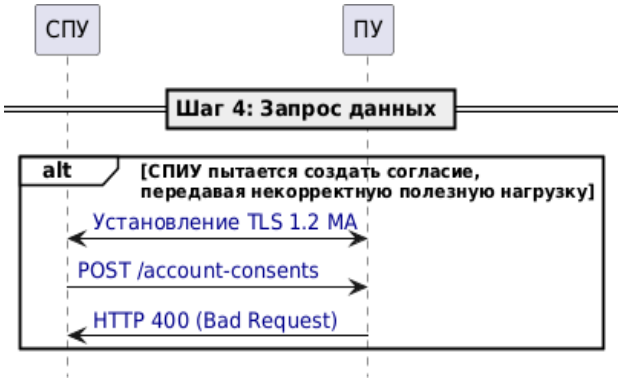

Рисунок 3. Неполная или не корректная полезная нагрузка запроса

3.3.3 Отсутствует или недействительна область применения токена доступа

Этот поток предполагает, что следующие шаги были успешно выполнены:

- Шаг 1. Запрос информации по счету.
- Шаг 2. Создание согласия на доступ к счету.
- Шаг 3. Авторизация согласия.

СПУ предоставляет действительный токен доступа, который не имеет допустимой области применения или ссылки на правильные разрешения для запроса данных. ПУ отвечает ошибкой HTTP 403 (Forbidden).

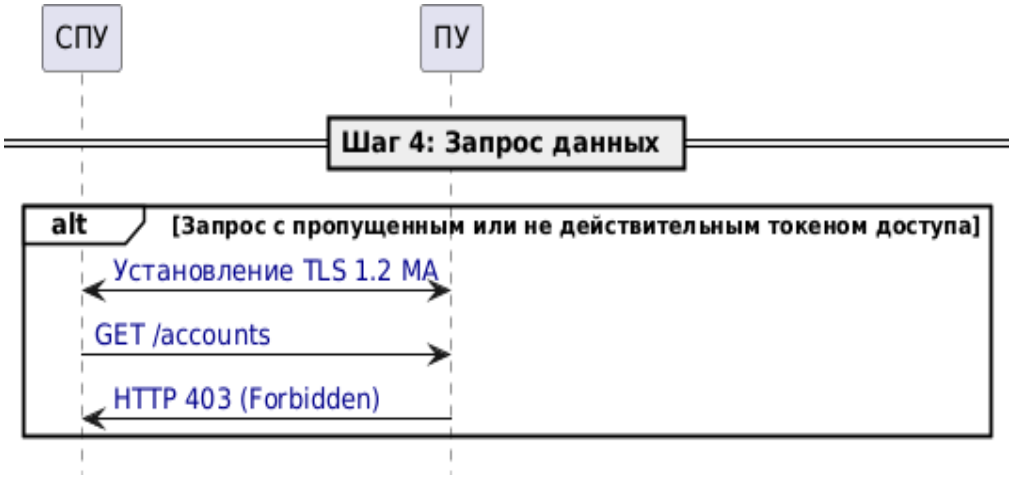

Рисунок 4. Отсутствует или недействительна область применения токена доступа

3.3.4 Недопустимая множественность вызовов API

Этот поток предполагает, что следующие шаги были успешно выполнены:

- Шаг 1. Запрос информации по счету.
- Шаг 2. Создание согласия на доступ к счету.
- Шаг 3. Авторизация согласия.

СПУ предоставляет (действительный) токен доступа, который используется для генерации пакета из нескольких запросов на получение подробной информации о счете. ПУ возвращает ответ 429 (Too Many Requests).

Рисунок 5. Недопустимая множественность вызовов API

3.3.5 Ошибка авторизации согласия

Этот поток предполагает, что следующие шаги были успешно выполнены:

- Шаг 1: Запрос информации по счету.
- Шаг 2. Создание согласия на доступ к счету.
- Шаг 3. Пользователь предоставил недопустимые учетные данные для ПУ или отказался предоставить доступ к счету для СПУ, в результате чего код авторизации не был создан.

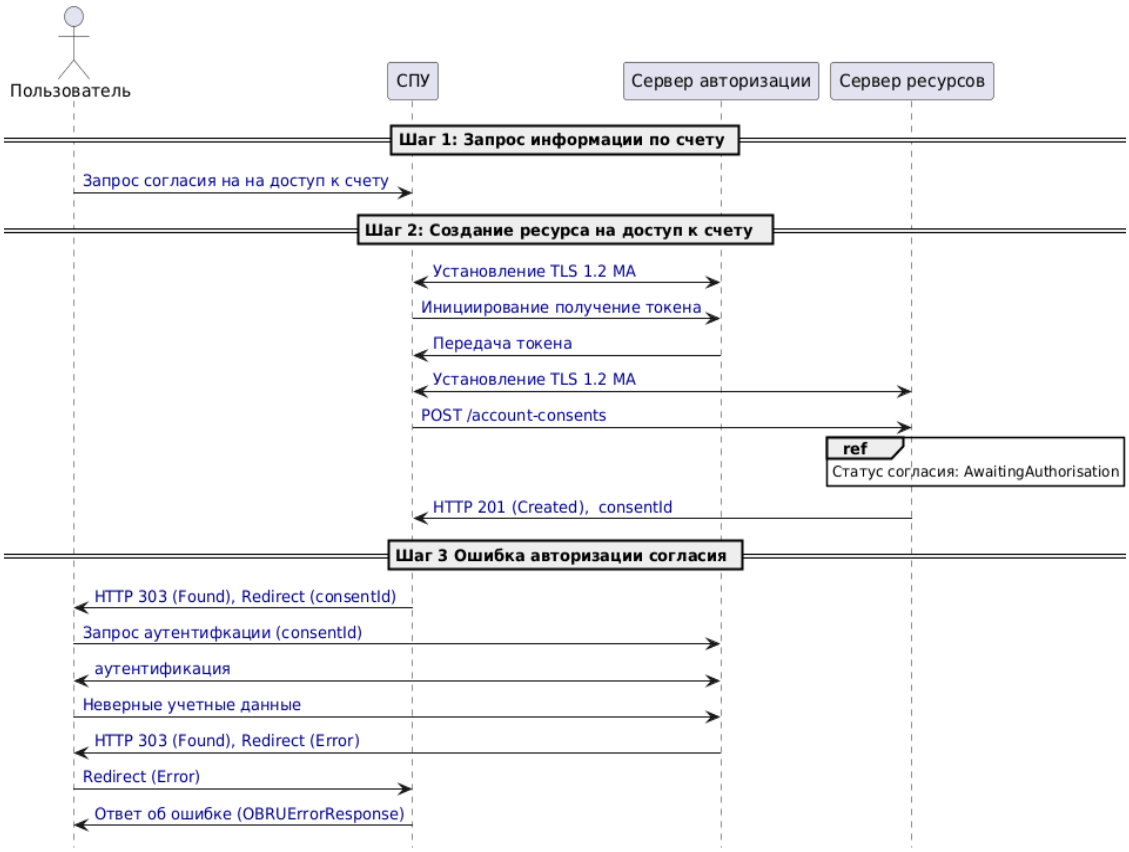

Рисунок 6. Ошибка авторизации согласия

4. РЕСУРС СОГЛАСИЯ

4.1 Состояние ресурса согласия

Состояние Ресурса согласия на доступ к счету определяется кодом его статуса, который может иметь следующие значения:

Значение	Описание
AwaitingAuthorisation	Ресурс согласия ожидает авторизации пользователя
Rejected	Ресурс согласия был отклонен
Authorised	Ресурс согласия был успешно авторизован
Revoked	Ресурс согласия был отозван

Таблица 2. Состояния ресурса согласия на доступ к счету

Изменение состояний ресурса согласия на доступ к счету соответствует следующей модели:

Рисунок 7. Диаграмма изменения состояний ресурса согласия на доступ к счету

После того, как Пользователь авторизовал согласие, ПУ изменяет статус ресурса на “Authorised”.

При отклонении согласия Пользователем, ПУ изменяет статус ресурса согласия на “Rejected”.

После того, как Пользователь отозвал ресурс согласия, ПУ изменяет статус ресурса на “Revoked”.

4.2 Срок действия согласия

expirationDateTime является необязательным полем, которое определяет срок истечения действия согласия для СПУ на доступ к данным Пользователя в ПУ.

expirationDateTime применяется ко всем разрешениям (кластерам данных), которые находятся в массиве ресурса согласия при его авторизации.

expirationDateTime определяет дату и время истечения срока действия согласия. По наступлении этой даты согласие не может быть возобновлено.
Для осуществления доступа к данным в течение срока действия согласия необходимо наличие активной авторизации, которая требует периодического подтверждения со стороны Пользователя.

4.3 Начальная/конечная дата доступа к операциям по счету

TransactionToDateTime и TransactionFromDateTime определяют согласие Пользователя на доступ к операциям по счету в определенный период времени. Оба поля являются необязательными, и одно поле может быть указано без другого.

ПУ может ограничить доступ к операциям по счету за рамками указанного временного периода, при запросах к ресурсам, содержащих информацию об операциях по счету.

4.4 Авторизация согласия

СПУ создает ресурс согласия на доступ к счету с помощью метода POST и получения доступа client credentials. Этот ресурс определяет разрешения (permissions) к кластерам данных, которые присылает СПУ от имени Пользователя. На начальном этапе согласие не авторизовано, поскольку ПУ еще его не актуализировал и не авторизовал во взаимодействии непосредственно с самим Пользователем.

ПУ отвечает сообщением, которое содержит идентификатор ресурса согласия consentId. Далее этот идентификатор используется при инициации доступа authorization code, который нужен для подтверждения Пользователем разрешений.

Во время получения доступа authorization code:

- ПУ аутентифицирует Пользователя.
- ПУ предоставляет ресурс согласия, полученный от СПУ, Пользователю для непосредственной авторизации его на стороне ПУ. Пользователь может авторизовать или отклонить согласие.
- ПУ предоставляет Пользователю список доступных счетов, для предоставления информации СПУ.
- Пользователь выбирает хотя бы один счет из списка и подтверждает авторизацию предоставления информации СПУ.

Согласие на доступ к счету считается авторизованным, если Пользователь выбрал хотя бы один счет

и подтвердил авторизацию согласия.

4.5 Повторная авторизация согласия

Повторная авторизация согласия - опциональный механизм, предназначенный для перевыпуска токенов для действующего согласия в результате утери или истечения срока токенов. Данный процесс инициируется через повторную аутентификацию Пользователей и не предполагает создание нового ресурса согласия или изменения его параметров. При этом параметр consentId не изменяется.

4.5.1 Инициация повторной аутентификации Пользователя

СПУ может запросить у Пользователя аутентификацию для повторной авторизации согласия, находящегося в состоянии «Authorised» в любой момент времени. Это может быть выполнено как до, так и после истечения срока действия базовых[1] токенов. ПУ может принимать данные запросы от СПУ. После успешной повторной авторизации согласия СПУ не использует токены доступа и токены обновления, которые ранее были выпущены для этого согласия. Когда ПУ выпускает новый токен доступа и токен обновления в результате повторной аутентификации согласия, он аннулирует ранее выпущенные токен доступа и токены обновления для этого согласия.

4.5.2 Ограничения клиентского пути

При повторной авторизации согласия Пользователь не изменяет параметры согласия (выбранные счета, разрешения и даты), клиентский путь ограничивается только аутентификацией Пользователя и подтверждением согласия.

4.5.3 Поведение при потерянном токене обновления

Если согласие уже авторизовано, а токен обновления утерян или более не действителен, то необходимо повторно авторизовать согласие без создания нового ресурса согласия.

4.6 Отзыв согласия

Пользователь может отозвать согласие на доступ к счету в любой момент времени.

Пользователь может отозвать авторизацию ресурса согласия напрямую на стороне ПУ. Механизмы реализации данного процесса и процессов, связанных с отзывов токенов определяются при разработке сервера авторизации ПУ. Если Пользователь отозвал согласие на доступ к счету на стороне ПУ, то статус ресурса account-consents меняется на «Revoked».

Пользователь может инициировать отзыв согласия на стороне СПУ. Если согласие будет отозвано на стороне СПУ:

- СПУ перестает обращаться к API с этого момента.
- СПУ может выполнить операцию DELETE для ресурса account-consent (до подтверждения отзыва согласия Пользователя), для информирования ПУ об отзыве согласия.

[1] Базовые токены – токены, выпущенные при первой авторизации согласия

- Либо СПУ может осуществить редирект Пользователя к ПУ для отзыва согласия.

Также согласие может быть отозвано на стороне ПУ через редирект к ПУ.

ПУ информирует ПКС об отзыве согласия (с момента запуска ПКС в промышленную эксплуатацию и принятия необходимых нормативно-правовых актов).

4.7 Удаление недоступных счетов из согласия

Пользователь выбирает счета, к которым применяется согласие в момент авторизации согласия.
В случае, если счет, в отношении которого дано согласие, перестает быть доступен для Пользователя, данный счет удаляется из списка предоставления доступа, но при этом ПУ не отменяет доступ СПУ к другим счетам, связанным с тем же авторизированным согласием.

4.8 Взаимодействие с ПКС

Пункт применяется с момента ввода ПКС в промышленную эксплуатацию и принятия необходимых нормативно-правовых актов.

ПУ информирует ПКС об изменении статуса согласия в следующих случаях:

- При авторизации согласия Пользователя на стороне ПУ, когда статус согласия переходит в состояние «Authorised».
- При отзыве согласия на стороне ПУ.
- При инициировании отзыва согласия на стороне СПУ, когда статус согласия переходит в состояние «Revoked».

ПУ получает от ПКС уведомление об инициировании отзыва согласия и выполнять следующие действия, в том числе:

- устанавливать соответствующий статус для ресурса согласия;
- удалять ресурс согласия и связанные токены, если инициирование отзыва согласия было выполнено на ПКС.

5. БЕЗОПАСНОСТЬ И КОНТРОЛЬ ДОСТУПА

5.1 Требование к профилю безопасности

Все взаимодействия при получении информации о счете Пользователя через среду Открытых программных интерфейсов осуществляются в соответствии со стандартом СТО БР «Открытые программные интерфейсы. Профили API для расширенного режима безопасности», а также в соответствии с положениями расширенного профиля безопасности OpenID API, определенным в ФАПИ.СЕК.

5.2 Типы предоставления доступа

5.2.1 Тип доступа client credentials

Для аутентификации клиента (СПУ) и получения токена доступа к Ресурсу согласия используется тип доступа client_credentials.

5.2.2 Тип доступа authorization code

Для получения токена доступа к ресурсам Пользователя в рамках сценария с перенаправлением используется гибридный поток с типом доступа authorization_code.

Примечание: Ресурс согласия на доступ к счету не является ресурсом Пользователя.

6. ИНФОРМАЦИЯ ДЛЯ ОЦЕНКИ РИСКОВ

Информация для оценки рисков будет доступна:

- В HTTP заголовках в соответствии с требованиями положения об обеспечении безопасности доступа к защищенным данным ФАПИ.СЕК.