КОНЦЕПЦИЯ
развития открытых банковских API Республики Беларусь

Минск, 2021

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Концепция развития открытых банковских API Республики Беларусь (далее – Концепция) разработана в рамках проекта по внедрению открытых интерфейсов прикладного программирования (далее – открытые API) в банковскую систему Республики Беларусь.

В настоящей Концепции изложены подходы к описанию, разработке, внедрению открытых API, отражены основные вопросы информационной безопасности при их внедрении, рассмотрены основные варианты моделей предоставления доступа посредством открытых API, отражены основные аспекты, которые необходимо учитывать при разработке технических нормативных правовых актов и технической документации, устанавливающих требования к открытым API.

В настоящей Концепции рассмотрены открытые API, программные продукты их использующие, а также отношения, возникающие между заинтересованными сторонами при создании, реализации, использовании и выводе из эксплуатации открытых API.

Настоящая Концепция не регулирует отношения, возникающие между заинтересованными сторонами при создании, реализации, использовании и выводе из эксплуатации закрытых API (в рамках партнерских программ, осуществления кросс-продаж, иных видов сотрудничества).

Настоящая Концепция разработана при содействии банков, мобильных операторов, Научно-технологической ассоциации ”Конфедерация Цифрового Бизнеса“ и других заинтересованных сторон.

Целями реализации настоящей Концепции являются:

определение стратегии развития открытых API в Республике Беларусь;

упрощение свободного обмена информацией между банками, платежными агрегаторами, иными юридическими и физическими лицами;

повышение эффективности проведения расчетов;

повышение конкурентоспособности платежной системы Республики Беларусь;

повышение привлекательности инвестиционного климата за счет привлечения финтех-компаний и экспорта платежных услуг;

повышение доступности платежных и информационных услуг в различных регионах Республики Беларусь.

Открытые API в результате их внедрения должны стать важным связующим звеном банковской системы и новых инструментов финансовой сферы.

Посредством открытых API между банками и другими организациями финансовой сферы будет происходить обмен финансовыми и информационными сообщениями, содержащими информацию о самих банках, банковских услугах, транзакционных данных, а также иную информацию.

Задачами настоящей Концепции являются:

анализ развития открытых API в мире;

описание текущей практики по внедрению открытых API в банковской системе Республики Беларусь;

изучение бизнес-моделей, доступных при внедрении открытых API в банковскую систему Республики Беларусь;

обоснование необходимости внедрения и стандартизации открытых API в Республике Беларусь;

описание построения экосистемы открытых API в Республике Беларусь;

описание принципов разработки, моделей и методов открытых API.

В настоящей Концепции используются термины и определения, применяемые в проекте Закона Республики Беларусь ”О платежных системах и платежных услугах“, СПР 6.01-2020 ”Банковская деятельность. Информационные технологии. Открытые банковские API. Регламент взаимодействия поставщиков API и пользователей API“, утвержденном постановлением Правления Национального банка Республики Беларусь от 31 декабря 2019 г. № 552 (далее – СПР 6.01), а также следующие термины и определения:

HTTPS – расширение протокола HTTP для поддержки шифрования в целях повышения безопасности;

OAuth 2.0 – открытый протокол (схема) авторизации, который позволяет предоставить пользователю API ограниченный доступ к защищенным ресурсам клиента без необходимости передавать ему (пользователю API) логин и пароль;

REST – архитектурный стиль взаимодействия компонентов распределенного приложения в сети. REST представляет собой согласованный набор ограничений, учитываемых при проектировании распределенной системы;

JSON – текстовый формат обмена данными, основанный на JavaScript. Применяется в веб-приложениях как для обмена данными между браузером и сервером, так и между серверами;

XML – расширяемый язык разметки, определяющий набор правил для кодирования документов в формате, который удобен для чтения как человеком, так и компьютером;

XS2A (Access to account) – процесс предоставления доступа к счету клиента, реализуемый в рамках директивы Европейского Союза

2015/2366/ЕС (Вторая директива об оказании платежных услуг, PSD2), предполагающая для пользователей API и иных третьих сторон возможность получения доступа к счетам клиента с его разрешения, без заключения договора с банком;

открытый банкинг – комплекс подходов к предоставлению банковских услуг, основанный на простом, удобном, эффективном, мгновенном и безопасном способе оказания пользователям таких услуг, в том числе посредством предоставления их юридическим лицам, не являющимся финансовыми организациями, доступа к информации о банковских услугах и клиентах банков в соответствии с требованиями, установленными законодательством;

регулятор – Национальный банк;

третья сторона – субъект правоотношений, не являющийся поставщиком API или клиентом;

финтех-компании – субъекты хозяйствования, не являющиеся банками, использующие технологии и инновации для оказания финансовых услуг;

центр компетенций – независимая от иных участников экосистемы открытых API организация, полномочия которой в сфере регулирования открытых API будут определены законодательством и/или предусмотрены соглашениями, заключаемыми между данной организацией и иными участниками экосистемы открытых API;

экосистема открытых API – взаимосвязанная группа лиц, взаимодействующих в процессе создания, реализации, использования и вывода из эксплуатации открытых API для достижения взаимовыгодных целей, непосредственно сами открытые API, а также программные продукты, внедряемые при их использовании.

ГЛАВА 1
СОВРЕМЕННОЕ СОСТОЯНИЕ ОТКРЫТЫХ API В РЕСПУБЛИКЕ БЕЛАРУСЬ

1.1. Существующие реализации открытых API

На данный момент банки Республики Беларусь проявляют заинтересованность в открытии API для своих партнеров. Банки видят перспективным использование API для привлечения дополнительных клиентов, повышения уровня обслуживания имеющихся клиентов.

На сегодняшний день большинство банков Республики Беларусь имеют свои собственные закрытые API. Используются данные API, как правило, для работы собственных систем дистанционного банковского обслуживания (далее – СДБО), прежде всего – банковских приложений.

Посредством организации доступа через API к своим приложениям большинство банков разработали мобильные приложения, практически не уступающие по функциональности веб-версиям.

Несколько белорусских банков используют закрытые API со своими партнерами, предоставляя им возможность осуществлять через банк, например, оформление кредита клиентом с использованием API, что существенно ускоряет процесс оформления, рассмотрения и ответа по заявке на кредит.

Также на данный момент есть банки, которые внедрили открытые API. Посредством данных API пользователи API могут получать как общедоступную информацию, так и информацию ограниченного распространения.

В таблице 1 отражены примеры, поясняющие понятия ”закрытые API“, ”открытые API“; ”общедоступная информация“, ”информация ограниченного распространения“.

Таблица 1. Примеры, поясняющие некоторые понятия

	Кто имеет доступ	Пример
Открытые API	Любой заинтересованный	API Национального банка, доступный любому разработчику для использования в своих целях курсов валют
Закрытые API	Внутренние сервисы, ограниченное число партнеров	API любого банка, обеспечивающие программное взаимодействие между автоматизированной банковской системой и мобильным приложением банка
Информация ограниченного распространения	Ограниченное число лиц	Информация о счетах, остатках, движении денежных средств; информация об инициировании платежей; информация о банковских платежных карточках
Общедоступная информация	Любой заинтересованный	Список банковских отделений, банкоматов, устройств самообслуживания; информация о курсах валют

Банки заинтересованы в первую очередь в открытии API, направленных на продажу банковских и иных финансовых услуг, в том числе страхования.

Национальный банк одним из первых начал предлагать доступ к общедоступной информации посредством API. На данный момент доступно получение курсов валют, перечня банков, банковских отделений и другой информации.

Одним из передовых банков в реализации открытых API является ЗАО ”Альфа-Банк“. Данный банк предоставляет через API доступ к информации о курсах валют, установленных ЗАО ”Альфа-Банк“ и Национальным банком, к формированию платежных поручений (инициирование платежа) и списка на зачисление заработной платы, предоставлению выписок по банковским счетам. У данного банка есть тестовая среда API (”песочница“), где разработчики могут протестировать работу своих приложений. Доступ к API предоставляется после рассмотрения банком заявки на подключение, доступ бесплатный.

Также одним из первых начал предоставлять доступ через API ”Приорбанк“ ОАО. У данного банка также доступна тестовая среда API (”песочница“). Через API банк позволяет получить следующую общедоступную информацию: текущие курсы обмена валют, установленные банком и Национальным банком, адреса отделений, банкоматов, инфокиосков банка, перечень операций, совершаемых в отделениях, банкоматах и инфокиосках банка, режим работы отделений, доступность банкоматов, инфокиосков, и следующую информацию ограниченного распространения: данные об остатках и движении по текущим (расчетным) банковским счетам, данные о сокращенном наименовании, юридическом адресе и учетном номере плательщика клиента. Для доступа к API ”Приорбанк“ ОАО требуется регистрация, которая доступна для юридических лиц и индивидуальных предпринимателей.

ОАО ”Банк Дабрабыт“, ОАО ”АСБ Беларусбанк“, ОАО ”Белагропромбанк“ предоставляют доступ по API к общедоступной информации о собственной деятельности. В частности, посредством API можно получить информацию об отделениях банков, банковских устройствах самообслуживания, курсах валют и иные сведения по усмотрению банка.

ОАО ”Белгазпромбанк“ предоставляет доступ к API для организаций-партнеров на индивидуальных условиях.

ЗАО ”БСБ Банк“ в 2017 году предложил всем своим клиентам юридическим лицам WebAPI, который поддерживает полный жизненный цикл электронного документа: создание, подписание, отправка в банк и проверка статуса исполнения.

ОАО ”Банк БелВЭБ“ и ОАО ”Сбер Банк“ привлекают клиентов, предоставляя кредиты и дополнительные услуги через сайты партнеров с использованием API.

1.2. Проблемы, связанные с отсутствием унифицированных требований к API, и способы их решения

В настоящее время банки применяют различные форматы для обмена информацией, используя различные наименования для одних и тех же терминов и процессов и т.д.

Можно выделить основные вероятные проблемы, связанные с описанием, разработкой и внедрением нестандартизированных API:

низкая функциональная совместимость – стандарты данных, принятые различными заинтересованными сторонами, различаются;

угроза безопасности данных. Важно соблюдать обоснованные и достаточные требования к информационной безопасности, кибербезопасности, а также разрабатывать и внедрять совместно с поставщиками API другие политики и рекомендации, связанные с информационной безопасностью и конфиденциальностью данных. Самостоятельное создание открытого API подразумевает, что для каждой реализации необходимо согласование характеристик программного обеспечения с требованиями к безопасности данных, предъявляемыми нормативными правовыми актами. Такой подход может привести к существенным тратам ресурсов как банков, так и третьих сторон, и стать источником определенных рисков, которых можно избежать при стандартизированном подходе;

слабое сотрудничество между организациями.

Без установления унифицированных требований к API каждый раз, когда пользователь API пытается создать или обновить приложение, необходимо вносить изменения в процедуру взаимодействия с каждым банком.

Совместная работа над стандартизированными открытыми API позволяет избежать ошибок, которые неизбежно возникают при создании нестандартизированных API.

Роль стандартизации API заключается в использовании единого подхода к разработке архитектуры и внедрению API, что позволит упростить и ускорить внедрение программных продуктов, снизить общую стоимость их поддержки, а также повысить их эффективность. Стандартизация API позволит упростить разработку и внедрение API, в частности развертывание и интеграцию API в существующие и новые решения в банковской и финансовой системе.

Стандартизация является критически важным компонентом для обеспечения сопоставимости, эффективности, устойчивости и

функциональной совместимости программных продуктов (программного обеспечения).

ГЛАВА 2
ОСНОВНЫЕ ТЕНДЕНЦИИ МЕЖДУНАРОДНОЙ ТЕХНОЛОГИЧЕСКОЙ ТРАНСФОРМАЦИИ БАНКОВСКОГО БИЗНЕСА

2.1. Трансформация банковского бизнеса

Стремительный прогресс в области информационных технологий привел к появлению и развитию многих локальных и международных финтех-компаний. Этим компаниям были необходимы открытые API для технической реализации инновационных идей.

Толчком к развитию открытых API в Европейском Союзе (далее – ЕС) и ответом на потребности финтех-компаний стало принятие в 2015 году второй директивы об оказании платежных услуг (PSD2). Этот документ на сегодняшний день широко используется во всем мире с целью повышения прозрачности, стимулирования конкуренции и инноваций в банковском секторе.

С развитием онлайн и мобильного банкинга многие клиенты предоставляют третьим сторонам разрешение на доступ к своим личным банковским данным для получения банковских услуг. Обмен данными внес свой вклад в новые инновационные финансовые услуги. Это, например, инструменты управления финансами, которые объединяют все счета в одном приложении, удобные переводы денежных средств между счетами в разных банках, инструменты сравнения вкладов и кредитов.

Предоставление финансовых услуг клиентам теперь предлагается и третьими сторонами, такими как финтех-компании. В свою очередь, третьи стороны могут также создавать новые услуги, которые могут использовать в том числе и банки.

При переходе к оказанию онлайн-услуг, для сохранения конкурентоспособности и прибыльности, банки сталкиваются с проблемами определения стратегии развития своих онлайн-каналов. Это может привести к потере доходов.

Согласно отчету Open Banking Report 2019 мировая тенденция свидетельствует о том, что банки заинтересованы в развитии открытых API в целях появления новых банковских услуг и привлечения новых клиентов, а открытый банкинг является эволюцией банковской сферы.

Открытые API являются важным шагом на пути построения открытого банкинга, который подразумевает удобный и безопасный способ обмена информацией между банком и клиентом.

Оцифровка финансовых услуг ускоренно набирает обороты. В настоящее время Open Banking Monitor содержит более 300 функционирующих порталов разработчиков. Большинство из них запускаются банками ЕС, стремящимися соблюдать требования PSD2.

По оценкам аналитиков, Великобритания лидирует с точки зрения готовности к Открытому банкингу. Однако в 2019 году активную деятельность в данном направлении также начали осуществлять другие страны и регионы: Австралия, Гонконг, Сингапур, Япония. По данным Open Banking Monitor, азиатские банки DBS, OCBC и Citibank Singapore играют ведущую роль в увеличении объема услуг, предоставляемых через открытый банкинг. В то же время Новая Зеландия, Мексика, Индия и США на фоне стран, перечисленных выше, только начинают внедрять подходы к открытому банкингу, руководствуясь различными стратегиями.

2.2. Феномен ”открытых API“. Технологическая платформа как способ передачи функций банков третьей стороне

Увеличение использования цифровых устройств и быстроразвивающиеся методы обработки данных трансформируют способы предоставления банковских услуг по всему миру.

Обмен данными используется для создания приложений, которые обеспечивают более быстрые и простые платежи, более широкие возможности управления и отслеживания финансовой информации для владельцев счетов, новые и улучшенные услуги управления счетами.

Ряд стран принимают решение или рассматривают вопрос о разработке открытых API для упрощения обмена данными банков с третьими сторонами.

Большинство стран, участвующих в инициативе по открытому банкингу, допускают получение информации о счетах клиентов, то есть использование API ”для чтения“.

В дополнение к информации о счетах ЕС, Великобритания, Япония и Новая Зеландия экспериментируют с инициированием платежей, то есть, используют API ”для записи“. Представители ряда стран[1] заявляют, что их подходы подразумевают поэтапное открытие данных, и утверждают, что начинать следует с предоставления информации о счетах клиента, а также общей информации о банковских услугах. Такую последовательность действий проще реализовать с точки зрения информационной безопасности и готовности банковской инфраструктуры.

[1] Open Banking Report 2019 https://thepaypers.com/reports/the-open-banking-report-2019-insights-into-the-global-open-banking-landscape-2/r780814

Допуск третьих сторон постоянно дорабатывается и совершенствуется, однако в большинстве стран нет четкого понимания и единых требований к лицензированию и аттестации.

ЕС и Австралия установили многоуровневую систему аттестации, где полномочия проведения аттестации будут иметь ”местный компетентный орган“ и Австралийская комиссия по конкуренции и защите прав потребителей (ACCC) соответственно. Гонконг использует альтернативный подход, при котором банки сами решают, с какой третьей стороной сотрудничать.

2.3. Международный опыт создания открытых API

Ряд стран успешно занимается развитием банковских открытых API и разрабатывает стандарты, принимаемые на национальном уровне. Ниже описан опыт стран, наиболее преуспевших в этом направлении. Сравнительные таблицы, описывающие международный опыт создания и внедрения открытых API, приведены в приложении 1 и приложении 2 к настоящей Концепции.

2.3.1. Великобритания

В 2016 году Управление по конкуренции и рынкам (далее – CMA) опубликовало отчет о розничном банковском рынке Великобритании, в котором было отражено, что наиболее крупным банкам становится сложнее конкурировать за клиентов, а мелким и новым банкам трудно расти и получать доступ к рынку.

Чтобы решить эту проблему был предложен ряд мер, которые позволили физическим лицам и предприятиям малого и среднего бизнеса безопасно делиться информацией о своих счетах с другими (сторонними) организациями.

Инициатива, возглавляемая CMA, называется Open Banking. В 2017 году сфера деятельности была расширена и теперь включает кредитные карты, электронные кошельки и предоплаченные карты. Благодаря регистрации через открытый банковский каталог (реестр), третьи стороны и поставщики платежных услуг могут работать с ведущими финансовыми учреждениями над новыми решениями, которые расширяют возможности клиентов.

Организация по внедрению открытого банковского обслуживания (OBIE) была создана CMA в 2016 году для предоставления открытого банковского обслуживания, разработки стандартов программного обеспечения и отраслевых руководящих принципов, которые стимулируют конкуренцию и инновации в розничном банковском обслуживании Великобритании. Торговое название данной организации (OBIE) – Open Banking Limited.

Open Banking Limited управляется CMA и финансируется девятью крупнейшими банками Великобритании: Allied Irish Bank, Bank of Ireland, Barclays, Danske, HSBC, Lloyds Banking Group, Nationwide, RBS Group и Santander.

Open Banking Limited выполняет следующие функции:

разработка спецификаций для API, которые банки используют для безопасного предоставления данных;

создание стандартов безопасности и обмена сообщениями;

поддержка пользователей и банков при использовании данных стандартов;

управление реестром, который позволяет участникам регистрироваться и оказывать услуги в рамках стандарта открытых API;

разработка рекомендаций для всех участников экосистемы Open Banking;

арбитраж, разрешение споров и жалоб.

Учитывая тот факт, что для клиентов важно понимать и проверять с кем они делятся своей информацией, регулирование деятельности третьих сторон обеспечивает определенный уровень безопасности персональных и платежных данных клиентов.

Правовой статус любой компании, зарегистрированной в Open Banking, регулируется законодательством страны регистрации. В Великобритании ответственным органом является Управление финансового поведения (Financial Conduct Authority – FCA).

Как только клиент дает явное согласие на передачу своих персональных данных, следует перенаправление на страницу аутентификации в приложении обслуживающего клиента банка, где он напрямую вводит свои данные для идентификации и аутентификации. Это позволяет банку получить разрешение на безопасную передачу данных третьим сторонам.

Клиент может найти и проверить законность деятельности пользователей API и иных третьих сторон на веб-сайте FCA.

Каждый субъект, участвующий в Open Banking, должен соблюдать законодательство о защите данных. В мае 2018 года на территории Европейского Союза принят Общий регламент о защите данных (далее – GDPR), который предусматривает штрафы в размере до 20 млн. евро, или 4 % от оборота компании для организаций, которые игнорируют (нарушают) требования законов о защите данных. Регулирующие органы придают большое значение защите персональных данных. Любая организация, которая не выполняет обязательства и нарушает требования, попадает под штрафные санкции.

Виды данных и функции, поддерживаемые Open Banking UK:

сведения об учетной записи клиента;

сведения о балансе счета, перечень транзакций;

инициирование платежей;

подтверждение достаточного количества денежных средств;

регистрация клиента;

информация об отделениях и банковских устройствах самообслуживания;

информация о банковских услугах: счета физических и юридических лиц, кредитные карты;

информация о кредитах: условия оформления, комиссии;

иная информация.

К январю 2020 года выпущено 3 версии стандарта Open Banking UK, которые включают:

версию 1 (март 2017): информация об отделениях и ATM, информацию о банковских услугах (о счетах физических и юридических лиц, кредитных картах), кредитах (об условиях оформления, комиссиях и другая информация);

версию 2 (март 2018): сведения об учетной записи клиента, сведения о балансе счета, перечень транзакций, инициирование платежей, подтверждение достаточного количества средств;

версию 3 (сентябрь 2018): обновление стандарта версии 2, добавление инструкций по внедрению стандарта.

Также в Великобритании ведется статистика по развитию Open Banking, согласно которой в инициативе участвуют 9 банков (Bank of Ireland, Bank of Scotland, Barclays Bank и другие) и 18 компаний (среди которых, например, American Express Services Europe Limited), а количество обращений к API на октябрь 2019 года достигло 180 млн. Британский финансовый регулирующий орган FCA в ноябре 2019 года представил новую концепцию Open Finance, которая расширяет принципы Open Banking и предоставляет людям и компаниям еще больше контроля над их финансами, данными по кредитам, депозитам, инвестициям и страхованию[2].

2.3.2. Германия

2.3.2.1. Open Bank Project

Являясь пионером в разработке концепций и технологий открытого банкинга, Open Bank Project[3] с 2010 года является одним из глобальных стандартов и платформой с открытым исходным кодом.

Open Bank Project поддерживает региональные стандарты и структуры, такие как Open Banking UK, STET и Berlin Group.

---

[2] https://www.fca.org.uk/news/speeches/open-finance-opportunity-financial-services

[3] Open Bank Project — https://www.openbankproject.com

Открытый исходный код проекта подразумевает, что организации могут в любое время свободно протестировать свое программное решение. Для коммерческого использования пользователи API должны получить лицензию.

Проект поставляется с собственным API Manager, который позволяет поставщикам API управлять уровнем доступа, мониторингом и аутентификацией, предоставляя поставщикам API контроль над отношениями с пользователями API. Банки могут решать, какие API открывать и кому, а также могут отозвать доступ в любое время.

Проект поддерживает более 250 методов API в следующих категориях:

сведения о банковских отделениях и банковских устройствах самообслуживания;

данные по счетам и транзакциям;

инициирование платежа;

прочие данные по организациям (например, логотип).

Весь разработанный проект включает полный набор необходимых для поставщиков API и пользователей API инструментов:

специфичный для банка API-шлюз;

готовый каталог API;

API портал;

”песочница“;

надежный клиентский сервер аутентификации.

Список партнеров проекта включает в себя более 40 организаций из разных стран мира, участвующих в инициативах открытых банковских операций – от разработки до внедрения.

Проект предоставляет высоконадежное решение для управления API Open Banking. Для более быстрой интеграции с существующей клиентской инфраструктурой архитектура проекта является модульной.

Проект предполагает быстрое время выхода поставщика API на рынок и эффективное развертывание системы менее, чем за 6 месяцев.

2.3.2.2. The Berlin Group

The Berlin Group [4] состоит из почти 40 банков, ассоциаций и платежных провайдеров со всего ЕС. Цель организации состоит в том, чтобы создать открытые и общепринятые стандарты открытых API в банковской сфере. Для достижения этой цели The Berlin Group создала технический орган по стандартизации, сосредоточив внимание на подробных технических и организационных требованиях, которые вошли в стандарт API под названием NextGenPSD2. Он был разработан

[4] The Berlin Group — https://www.berlin-group.org/

для унификации коммуникаций между поставщиками API и пользователями API.

Основываясь на требованиях PSD2 и технического стандарта аутентификации (Technical Standards on strong customer authentication and secure communication under PSD2), The Berlin Group работала над детальной структурой доступа к счетам клиентов с моделью данных на концептуальном, логическом и физическом уровнях – XS2A. NextGenPSD2[5] построен из документов, опубликованных бесплатно:

вводный документ;

документ правил, который охватывает описание сервиса, логическую модель данных и подробные описания потоков и процессов;

рекомендации по реализации, которые определяют интерфейс XS2A в технических деталях, включая схемы XML/JSON;

библиотеки OpenAPI для разработчиков (доступ к счетам, внутренние платежи, безопасность и другие).

В дополнение к основным руководствам по внедрению также был опубликован документ ”Приложения с определениями по инициированию внутренних платежей“.

Ниже описаны ключевые цели создания и особенности реализации NextGenPSD2 Framework, опубликованные представителями группы:

современный, открытый и совместимый набор API как эффективный способ безопасного предоставления данных;

снижение сложности и стоимости внедрения XS2A, решение проблемы нескольких конкурирующих стандартов в Европе;

позволить европейским банковским клиентам получать выгоду от инновационных услуг, предоставляя сторонним приложениям безопасный и надежный (аутентифицированный и авторизованный) доступ к своим банковским счетам и финансовым данным;

современный ”RESTful“ API-интерфейс, использующий HTTP/1.1 с TLS 1.2 в качестве транспортного протокола;

поддержка всех параметров, необходимых для инициирования платежа, информации об учетной записи и подтверждения доступности средств, а также платежи с указанием будущей даты, множественные/массовые и повторяющиеся платежи;

поддержка мультивалютных счетов;

несколько моделей архитектуры для строгой аутентификации клиентов (SCA): перенаправление, OAuth 2.0 и другие;

многоуровневый подход SCA;

структуры данных JSON с моделью данных на основе ISO 20022 или XML с pain.001 для платежей и camt.05x для информации по счетам;

---

[5] NextGenPSD2 — https://www.berlin-group.org/nextgenpsd2-downloads

продуманные и прозрачные процессы управления изменениями и управления версиями;

расширяемый набор дополнительных услуг.

2.3.3. Польша

Стандарт PolishAPI [6] является ключевым стандартом открытого банкинга на польском финансовом рынке. Он описывает интерфейс, позволяющий пользователям API получать доступ к счетам клиентов.

Целью данной инициативы является снижение затрат на реализацию Директивы PSD2 (и других сопутствующих правовых актов) для поставщиков API и пользователей API.

Создатели стандарта предполагают его постоянное развитие в ответ на нормативные, технологические и бизнес-изменения на польском и европейском рынках. Изменения должны быть опубликованы как последующие версии спецификации стандарта API Польши.

Среди участников проекта: Польская банковская ассоциация вместе с коммерческими и кооперативными банками, кооперативными сберегательно-кредитными союзами (SKOK), Польская организация небанковских платежных учреждений (PONIP) вместе со своими ассоциированными членами, Польская палата информационных технологий и Телекоммуникации (PIIT), Польская страховая ассоциация (PIU), Национальный клиринговый центр (KIR), Бюро кредитной информации (BIK) и Польский стандарт оплаты (PSP).

Спецификация описывает процессы инициирования платежей (PIS), передачи информации по счетам (AIS) и подтверждения доступности средств (CAF).

2.3.4. Сингапур

Монетарное управление Сингапура (далее – MAS) активно поддерживает принципы открытых API и призывает участников финансового рынка открывать доступ к своим данным[7].

В ноябре 2016 года MAS и Ассоциация банков опубликовали документ Finance-as-a-Service API Playbook ”Финансы как услуга“ [8], который содержит рекомендации организациям финансового сектора по использованию открытых API в целях обеспечения возможности проводить эффективный обмен финансовой информацией и запускать инновационные проекты. API охватывают банки, страховые компании, компании по управлению активами и государственные учреждения. Эти

[6] PolishAPI — https://polishapi.org/en

[7] http://www.cbr.ru/Content/Document/File/50679/Consultation_Paper_171229.pdf

[8] Monetary Authority of Singapore — https://www.mas.gov.sg/-/media/MAS/Smart-Financial-Centre/MASABS-API-Conference-EBook.pdf

API были разделены по функциям, включая маркетинг, продукты, платежи, регулирование, продажи и обслуживание.

Принятый документ является добровольным для применения, поскольку правительство считает, что такой подход будет более успешным, чем установление сроков принятия и внедрения. Рынок очень лояльно отнесся к данной инициативе и интерес постоянно растет.

Правительство осторожно относится к безопасности и защите данных своих граждан и выдает банковские лицензии только традиционным банкам.

Более 5600 процессов были оценены с использованием установленной методики и отраслевых параметров для создания рекомендованного списка из 411 методов API (с учетом более 700 бизнес-процессов).

Основные принципы, предусмотренные стандартами Открытых API Сингапура:

открытость – все заинтересованные стороны могут получить доступ к API;

удобство использования – обеспечение высокого качества обслуживания пользователей;

функциональная совместимость – обеспечивает обмен данными между организациями без какой-либо зависимости от технологий;

повторное использование – использование существующих стандартов и определений, чтобы избежать двойной работы;

независимость – минимизация зависимостей от каких-либо поставщиков или технологий;

расширяемость – гибкость для расширения API для новых заинтересованных сторон;

стабильность – обеспечение согласованности и прозрачности изменений посредством коммуникации и управления;

прозрачность – обеспечение ясности в отношении поддерживаемых стандартов.

2.3.5. Российская Федерация

В Российской Федерации открытые API развиваются в рамках сотрудничества Ассоциации развития финансовых технологий [9] Российской Федерации (далее – Ассоциация ФинТех) и Центрального банка Российской Федерации (далее – Банк России).

Летом 2019 года в рамках Наблюдательного совета Ассоциации ФинТех была одобрена ”Концепция открытых API“, которая включает платежные, информационные, сервисные и регуляторные API.

[9] Ассоциация Финтех — https://fintechru.org

Концепцию разработали члены Ассоциации ФинТех. Дальнейшая работа участников Ассоциации ФинТех будет продолжена в соответствии с одобренной дорожной картой внедрения открытых API в России. Координировать внедрение открытых API на российском рынке будет Банк России совместно с Ассоциацией ФинТех.

В октябре 2020 года Банк России официально опубликовал спецификации стандартов открытых API, которые разрабатывались совместно с участниками рынка на площадке Ассоциации ФинТех. Их применение будет добровольным. Они содержат принципы и рекомендации внедрения открытых API для конкретных сервисов — получения организациями информации о счете клиента банка и инициирования денежных переводов. Стандарты также определяют общие положения работы открытых банковских интерфейсов и предлагают рекомендации по обеспечению информационной безопасности при использовании этой технологии.

2.3.6. Соединенные Штаты Америки

США не стали исключением, и, благодаря заинтересованным сторонам: корпорациям, финансовым учреждениям, финтех-компаниям, поставщикам услуг, государственным органам, органам по стандартизации и консультационным фирмам, видят в стандартизации API огромный потенциал, который позволит расширить возможности для обеспечения роста банковских инноваций и удовлетворить различные потребности клиентов в разных сегментах рынка.

Законодательство США пока никак не регламентирует внедрение Open Banking. Законодательный акт, который имеет отношение к этой концепции – Section 1033 из Dodd-Frank Wall Street Reform and Consumer Protection Act. Данный документ определяет, что финансовые институты должны предоставлять пользователям финансовую и транзакционную информацию по запросу, однако никак не обязывает банки предоставлять эту информацию третьим сторонам.

В выпущенном в 2018 году отчете ”Treasury Report“ Министерство финансов США подчеркивает, что между США и Великобританией есть существенная разница с точки зрения как размера, так и разнообразия в финансовом секторе, поэтому действующая в Европе платежная директива PSD2 неприменима для американского рынка. В результате для рынка США наиболее подходящим будет решение, исходящее от частного сектора, которое будет контролироваться регулирующими органами в тех случаях, когда это необходимо. Сейчас развитие Open

Banking в стране диктует не регулирующий орган, а сам рынок и его технологии.

2.3.7. Республика Казахстан

В рамках государственной программы ”Цифровой Казахстан“[10] в 2018 – 2020 годах Национальным банком Республики Казахстан реализуется проект ”Внедрение регулирования в части создания открытых платформ (Open API) в финансовой отрасли“. Данный проект направлен на повышение конкуренции на финансовом рынке и расширение финансовых услуг за счет технологических возможностей сторонних организаций (финтех-компаний).

В рабочую группу по проекту входят представители 7-ми банков второго уровня. Уже сейчас на казахстанском рынке функционирует АО ДБ ”Альфа-Банк“, который серьезно подошел к развитию открытых API и запустил свой портал для разработчиков, зарегистрировавшись на котором любая финтех-компания сможет получить доступ к сервисам банка и встроить их в свой продукт. В 2018 году этот финансовый институт стал первым в Казахстане, опубликовавшим информационный сервис, который в режиме реального времени позволяет получить доступ к информации о месторасположении и работоспособности банкоматов (банковских устройств самообслуживания).

2.3.8. Другие страны

В Австралии первый этап реформы открытого банковского обслуживания был проведен в июле 2019 года. Клиенты четырех крупнейших банков (Commonwealth Bank of Australia (CBA), the National Australia Bank (NAB), the Australia and New Zealand Banking Group (ANZ), Westpac) смогут использовать этот проект для обмена данными о транзакциях, депозитах, дебетовых и кредитных картах с другими аккредитованными поставщиками финансовых услуг. Техническая спецификация Великобритании будет использоваться в качестве отправной точки для разработки национальных стандартов.

В марте 2018 года принят Закон о банковской деятельности Японии. Он требует, чтобы банки внедрили и поддерживали открытые API. Будет опубликован всеобъемлющий структурный документ, охватывающий безопасность, защиту пользователей и спецификации о реализации инициативы открытых API.

В начале марта 2018 года в Мексике был принят законопроект, позволяющий регулирующим органам приступить к разработке

[10] Государственная программа ”Цифровой Казахстан“ — https://egov.kz/cms/ru/law/list/P1700000827

руководства, которое позволило бы использовать открытые API. Это позволит предоставлять информацию третьим сторонам через API.

В январе 2018 года Валютное управление Гонконга (HKMA) выпустило документацию по структуре Open API, в которой изложен предполагаемый подход HKMA к банковской отрасли в Гонконге.

2.3.9. Проблемы, возможности и особенности создания открытых API

Регулирующие органы, банки и финтех-компании стран, уже приступивших к созданию и внедрению открытых API, во всем мире оказывают поддержку для других стран и игроков рынка, только приступающих к созданию открытого банкинга. Это заметно на примере Великобритании и OBIE, оказывающих поддержку во внедрении стандартов открытых API в других странах.

Исходя из опыта других стран можно сделать некоторые выводы. Одним из важнейших факторов успешного создания и внедрения открытых API являются разумные сроки. Внедрение существенных изменений в сложные финансовые системы с многочисленными заинтересованными сторонами может требовать больших временных затрат.

Важным также является то, что многие страны не пытаются сами изобрести нечто новое, а берут за основу уже успешную модель и существующий стандарт и адаптируют его под свои особенности.

Следствием внедрения открытых API в Европе является наличие множества функционирующих открытых банковских API и финтех-компаний, доказавших свою эффективность.

Модель финансовых систем с ограниченным набором предложений устарела. Будущее за созданием новых услуг, адаптированных к конкретным потребностям потребителей, и первостепенное значение имеют технологические структуры, которые могут быстро адаптироваться.

Как показывает опыт преуспевающих стран в развитии открытых API, немаловажным является просвещение общественности о создаваемых решениях. В любое время, когда в банковских услугах происходят значительные изменения, потребителям необходимо образование и время, чтобы осознать и понять преимущества.

Проблема безопасности является одной из самых значительных, с которыми сталкиваются поставщики и потребители, использующие открытые API. Большинство компаний, выступающих за открытый банкинг, являются небольшими финтех-компаниями, а не технологическими гигантами, и отсутствие единообразных технических стандартов, определяющих требования безопасности, в сочетании со

сложными внутренними технологическими системами может сделать процесс подверженным мошенничеству.

Еще одна проблема, связанная с открытыми API, это ответственность к выбору пользователей API, поскольку привлечение сторонних пользователей API к банковскому процессу повышает риск получения мошенниками доступа к информации о клиентах и их финансам.

Наконец, отсутствие осведомленности о возможностях открытого банкинга снижает вероятность того, что потребители дадут согласие на обмен данными, что ограничит возможности банков и финтех-компаний внедрять инновации. Исследование Accenture в 2019 году показывает, что две трети потребителей не хотят делиться своими личными и финансовыми данными со сторонними пользователями API. В то же время анализ потребителей в ЕС показал, что 92 % из них никогда не слышали об открытом банкинге.

ГЛАВА 3
ВНЕДРЕНИЕ ОТКРЫТЫХ API В РЕСПУБЛИКЕ БЕЛАРУСЬ

3.1. Необходимость внедрения и стандартизации открытых API

3.1.1. Увеличение доступности цифровых услуг. Повышение эффективности банковской системы

Стандартизация при разработке и внедрении открытых API в мире рассматривается не как технический инструмент, а как потенциальный механизм для совместного развития финансовой сферы.

С помощью стандартизации разработчик может спроектировать и реализовать одно приложение, которое будет взаимодействовать со всеми банками без необходимости модификаций.

Основными преимуществами для участников банковской системы, платежного рынка и клиентов при внедрении открытых API будут являться:

появление актуальной информации по банковским отделениям, банковским устройствам самообслуживания, банковским услугам в едином формате для всех банков;

привлечение новых клиентов для банков за счет появления новых бизнес-моделей и участников рынка;

снижение банковских комиссий как для клиентов банка, так и для самих банков при расчетах без использования международных платежных систем;

расширение охвата и упрощение безналичных платежей физических лиц без использования международных платежных систем, что будет способствовать снижению банковских комиссий, а также

уменьшение числа возможных ошибок за счет сокращения цепочки прохождения платежа;

создание мобильных вариантов банков, тем самым увеличивается цифровая функциональность и снижаются операционные расходы банков;

разработка ИТ-компаниями и финтех-компаниями программных продуктов и онлайн-сервисов, реализация которых является дорогостоящей и/или нецелесообразной для банков;

реализация удобного управления своими финансами для клиентов банков, имеющих счета одновременно в нескольких банках.

3.1.2. Стандартизированные API как фактор развития рынка и решение проблемы фрагментации API

Стандартизация в области открытых API необходима для:

унификации финансовых сообщений, передаваемых между банками, пользователями API и иными третьими сторонами;

развития рынка финансовых инструментов и платежных услуг в Республике Беларусь;

повышения территориальной доступности банковских и иных финансовых услуг благодаря оказанию услуг через онлайн-каналы;

повышения конкуренции в банковском секторе;

упрощения разработки и внедрения API за счет сформированных требований и рекомендаций технических, юридических и по информационной безопасности;

появления новых финансовых инструментов и платежных услуг в платежной сфере Республики Беларусь.

Стандартизация в области открытых API включает также стандартизацию процессов взаимодействия участников экосистемы открытых API между собой, в том числе:

поставщиков API и пользователей API;

пользователей API и клиентов;

центра компетенций, поставщиков API, пользователей API.

В целях определения порядка взаимодействия поставщиков API и пользователей API принят СПР 6.01, применяемый при разработке приложений, использующих открытые API, и в процессах предоставления API их поставщиками. Для определения правовых и организационных основ функционирования платежных систем в Республике Беларусь, регулирования отношений, возникающих при оказании платежных услуг, планируется принятие Закона Республики Беларусь ”О платежных системах и платежных услугах“.

3.1.3. Необходимость наличия реестра пользователей и поставщиков API и осуществления регулирования

В целях систематизации и поддержания в актуальном состоянии сведений о пользователях API, поставщиках API, информирования и соблюдения прав потребителей банковских и иных финансовых услуг целесообразно наличие реестра пользователей API и поставщиков API (далее – реестр).

Предполагается, что доступ к платежным API будет предоставляться пользователям API первого типа, а также пользователям API второго типа, внесенным в реестр.

Процедура внесения в реестр должна быть максимально прозрачной для всех участников экосистемы открытых API.

Помимо регулятора регулирующие функции в области Открытых API может осуществлять центр компетенций.

Также регулятор и/или центр компетенций определяют виды участников экосистемы открытых API (пользователей API), критерии, которым должен соответствовать пользователь API, при необходимости разрабатывают регламент внесения пользователей API в реестр, исключения пользователей API из реестра при фиксировании недобросовестных действий с их стороны.

Центр компетенций предоставляет всем заинтересованным лицам информацию обо всех участниках экосистемы открытых API онлайн путем размещения реестра и основной информации о них на едином портале открытых API.

Порядок формирования и ведения реестра, в том числе порядок включения в реестр и исключения из реестра, внесения в него изменений, состав включаемых в реестр сведений, определяется регулятором и/или центром компетенций.

3.2. Варианты использования открытых API

К открытым API можно отнести следующие типы API:

информационные API;

платежные API;

статистические API.

Указанная классификация типов API основывается на положениях СПР 6.01, является условной и не препятствует описанию, разработке и внедрению иных открытых API, которые могут являться самостоятельными типами или относиться к одному из вышеперечисленных типов (являться видом соответствующего типа открытого API).

Управлять классификацией типов открытых API может центр компетенций на основе анализа рыночных потребностей.

3.2.1. Информационные API

Посредством информационного API предоставляется:

информация о курсах валют (при проведении операций с наличными и (или) безналичными денежными средствами, в том числе с использованием банковских платежных карточек, систем дистанционного банковского обслуживания, программно-технической инфраструктуры с использованием банковских платежных карточек);

информация о пунктах обслуживания клиентов банка (отделения, филиалы, обменные пункты, пункты самообслуживания с использованием программно-технической инфраструктуры с использованием банковских платежных карточек, в том числе банкоматы и инфокиоски) с указанием адреса и времени работы, контактных телефонов, адресов электронной почты, со списком оказываемых услуг и иная информация о каждом пункте обслуживания;

информация о банковских услугах (предоставлении кредитов, привлечении денежных средств во вклады (депозиты), выпуске в обращение (эмиссии) банковских платежных карточек, привлечении драгоценных металлов во вклады (депозиты), условия реализации драгоценных камней и монет, условиях осуществления денежных переводов, включая переводы без открытия счета, условиях предоставления услуг, тарифах и вознаграждениях (комиссиях), а также иная информация).

Вся информация, предоставляемая через информационные API, является общедоступной. На рисунке 1 представлена Схема взаимодействия при использовании информационных API, на рисунке 2 – схема получения данных посредством информационных API.

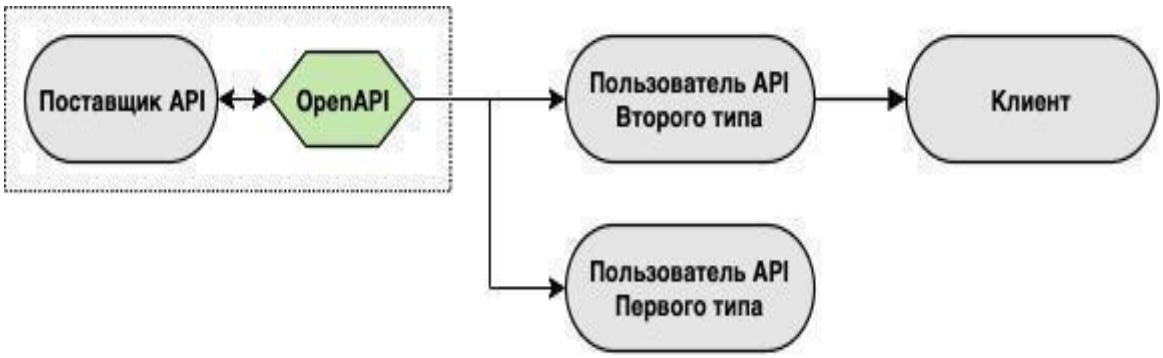


Рисунок 1. Схема взаимодействия при использовании информационных API

3.2.1.1. Вариант использования № 1: получение информации о курсах валют и иной общедоступной информации

Запросы в соответствии с этим вариантом использования могут направляться для получения информации о курсах валют, установленных поставщиком API на заданную дату и для заданного типа обмена.

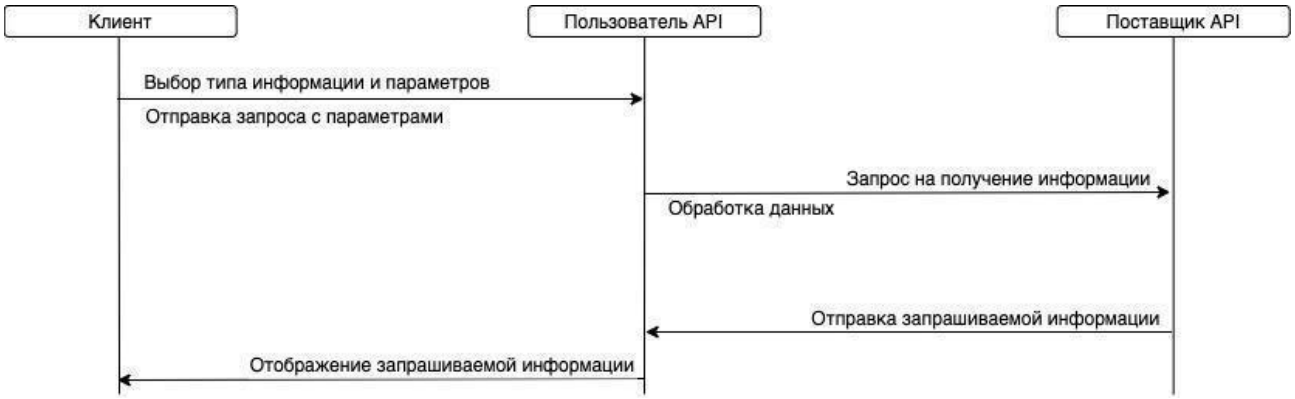


Рисунок 2. Схема получения информации посредством информационных API

Иными примерами использования информационных API в соответствии с указанной схемой являются:

получение информации о местонахождении (карты) банковских отделений и банковских устройств самообслуживания;

сравнение ставок по кредитам и депозитам;

поиск кредитов для определенных категорий физических лиц (например, пенсионеров);

сравнение условий предоставления кредитов, в том числе для определенных категорий физических лиц;

получение курсов валют для использования в процессе осуществления расчетов и ведения бухгалтерского учета.

3.2.2. Платежные API

Платежные API используются для предоставления банком пользователю API информации о состоянии банковского счета клиента, информации о наличии на нем необходимой суммы денежных средств и их движении, другой информации по счету клиента, инициирования платежей между счетами, а также подключения, изменения и отключения услуг, используя приложение пользователя платежных API.

Посредством открытых платежных API передаются данные, которые необходимо защищать от недобросовестных участников платежной системы или иных третьих сторон. Поставщикам API, пользователям API необходимо обеспечивать безопасность своих программных продуктов, а также защиту персональных данных

клиентов, банковской тайны и иной информации ограниченного распространения.

Примерами использования платежных API являются:

открытие банковского счета;

оформление заявки на выпуск банковской платежной карточки;

совершение платежа со счета в банке;

экспорт банковских операций в бухгалтерское ПО (например, 1С);

агрегация банковских услуг различных банков в едином приложении (например, единое приложение для управления банковскими платежными карточками различных банков);

агрегация выписок по счетам клиента в разных банках, аналитика расходов и доходов;

контроль дебиторской задолженности внутри учетного ПО или CRM-системы.

Платежи с помощью банковских платежных карточек не рассматриваются в рамках стандарта платежных API, но могут быть включены в него при наличии рыночного спроса.

Ниже рассмотрены основные варианты использования платежных API:

инициирование платежа;

получение списка доступных счетов;

получение списка операций по счету.

3.2.2.1. Вариант использования № 1: инициирование платежа

Запросы в соответствии с этим вариантом использования могут направляться для инициирования платежа в форме перевода денежных средств со счета клиента на счет получателя денежных средств.

Фактически платежная операция должна изначально инициироваться клиентом в интерфейсе приложения пользователя API, технически платежная операция инициируется пользователем API перед поставщиком API.

Поставщик API должен отказать в исполнении API запроса, если пользователь API не может быть идентифицирован и аутентифицирован или если API запрос не будет авторизован.

В зависимости от решения поставщика API могут использоваться различные методы (способы) идентификации и аутентификации клиента.

Схема осуществления платежной операции представлена на рисунке 3.

Основные этапы платежной операции включают следующие шаги:

001. Инициирование платежа включает в себя обработку платежа, инициатором которого является клиент, в электронной или иной форме, и передачу информации поставщику API и/или пользователю API,

необходимой для осуществления последним (последними) платежа и (или) приема денежных средств (электронных денег) по платежу;

002. Прием информации о платеже поставщиком API;

003. Передача на исполнение платежного указания (платежной инструкции) в СДБО поставщика API;

004. Перевод денежных средств на счет получателя платежа;

005. Списание денежных средств со счета клиента;

006. Зачисление денежных средств на счет получателя платежа;

007. Информирование о статусе проведения платежной операции клиента и пользователя API.

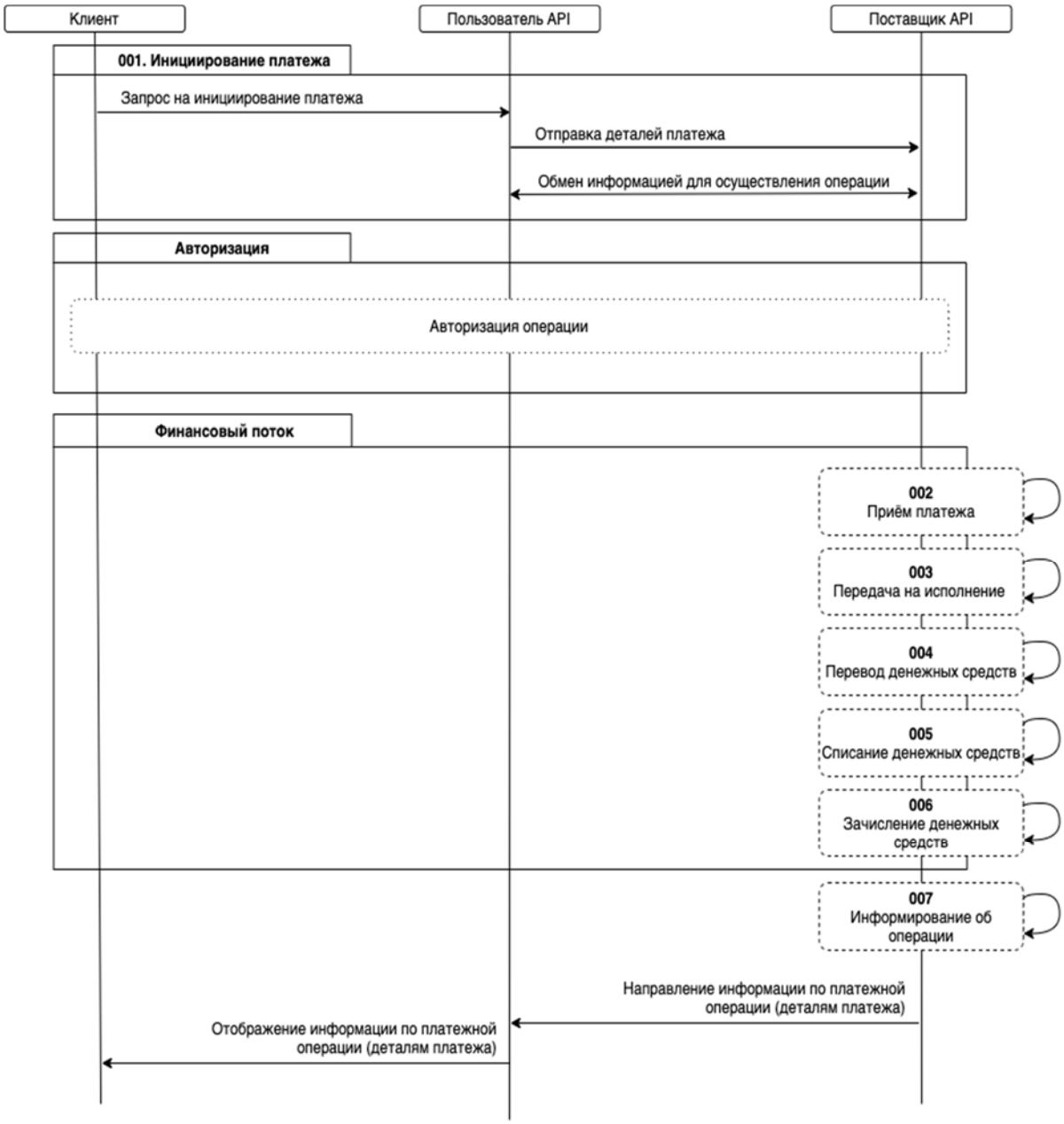


Рисунок 3. Платежная операция, осуществляемая через открытые API

3.2.2.2. Вариант использования № 2: получение списка доступных счетов

В соответствии с этим вариантом использования пользователем API направляются запросы для получения списка доступных счетов клиента, предоставляемого поставщиком API (Рисунок 4). Термин «доступные счета» относится к банковским счетам, доступным онлайн. Поставщик API поддерживает различные виды счетов.

В результате применения данного варианта использования пользователь API получит список счетов клиента. Дополнительная информация о счетах не входит в данный вариант использования. Если пользователю API было предоставлено право на получение дополнительной информации, то он может использовать полученные номера счетов для получения дополнительной информации (например, получение списка операций по данным счетам).

Поставщик API должен отказать в осуществлении транзакции, если пользователь API не может быть идентифицирован и аутентифицирован или если транзакция не будет авторизована.

В зависимости от решения поставщика API могут использоваться различные методы (способы) идентификации и аутентификации клиента.

Схема получения списка доступных счетов представлена на рисунке 4.

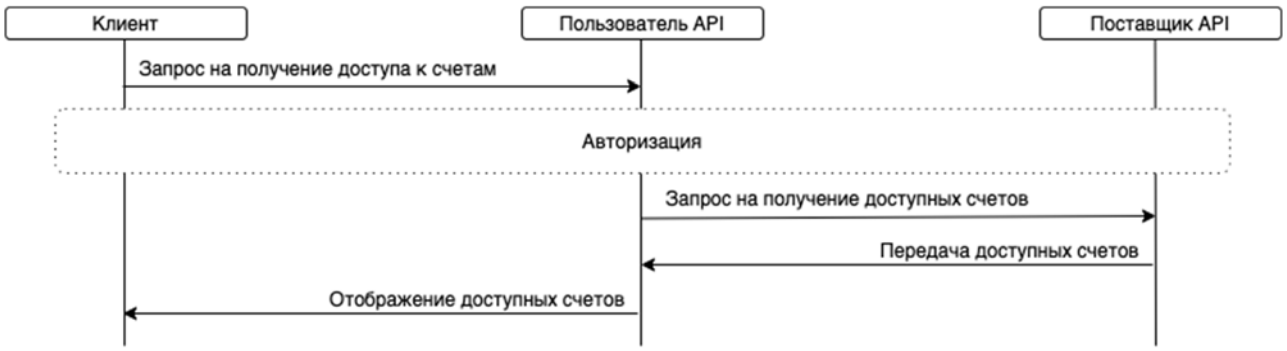


Рисунок 4. Получение списка доступных счетов

3.2.2.3. Вариант использования № 3: получение списка операций по счету

Пользователь API может направлять запросы в соответствии с этим вариантом использования для получения информации о платежных транзакциях счетов определенного клиента. В результате пользователь API получит информацию обо всех платежных операциях, выполненных в течение периода времени, указанного в запросе. Кроме того, поставщик API может предоставлять также балансы соответствующих счетов.

Вариант использования предполагает автоматическое получение списка операций по счету Пользователем API в фоновом режиме, от клиента требуется лишь однократное инициирование данного процесса путем авторизации.

Поставщик API должен отказать в исполнении API запроса, если пользователь API не может быть идентифицирован и аутентифицирован или если API запрос не будет авторизован.

В зависимости от решения поставщика API, могут использоваться различные методы (способы) идентификации и аутентификации клиента.

Процесс получения списка операций по счету аналогичен получению списка счетов и представлен в виде схемы на рисунке 5.

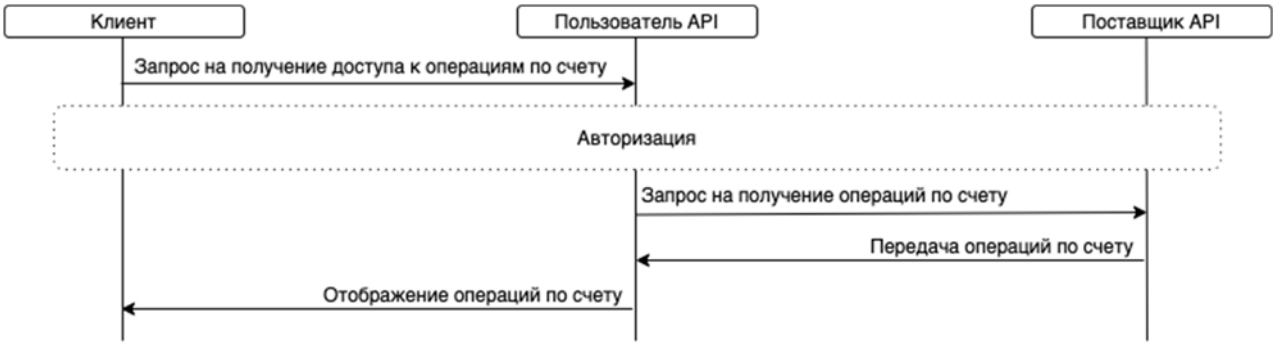


Рисунок 5. Получение списка операций по счету

3.2.3. Статистические API

Статистические API предоставляют доступ Национальному банку, иным государственным органам и организациям в соответствии с законодательством или по согласованию с регулятором к информации первичных учетных документов по операциям в банках, о первичных операциях в банках.

Примером использования статистических API является получение информации о деятельности банков и иных участников финансового рынка, необходимой отчетности, первичных учетных документов по операциям в банках, о первичных операциях в банках в необходимом объеме, в любое время и в едином формате.

3.3. Создание экосистемы открытых API

3.3.1. Участники экосистемы открытых API

В экосистему открытых API входят субъекты (участники), выполняющие определенные функции (роли) в рамках данной экосистемы:

1) Регулятор;

2) Центр компетенций;

3) Испытательная лаборатория (центр);

4) Поставщики API;

5) Пользователи API двух типов, в соответствии с СПР 6.01:

а) Пользователь API первого типа, использующий открытые API в личных целях, не предоставляя услуги клиентам;

б) Пользователь API второго типа, использующий открытые API для предоставления услуг клиентам;

6) Клиенты.

В таблице 2 представлены субъекты, которые встречаются в большинстве стандартов, основанных на PSD2, участники Экосистемы открытых API Республики Беларусь, а также субъекты платежных правоотношений, определенные в проекте Закона Республики Беларусь ”О платежных системах и платежных услугах“. Предварительное сопоставление произведено по ролям, которые будут выполняться соответствующими субъектами в рамках Экосистемы открытых API. В связи с различной сферой регулирования и целями принятия указанных документов наименование конкретного субъекта Экосистемы открытых API может отличаться от представленных в таблице 2 в зависимости от действий данного субъекта, выполняемых им в определенном процессе (этапе процесса) (например, при осуществлении платежной операции, оказании платежной услуги и др.).

Таблица 2. Сопоставление субъектов открытых API

Сокращение	Наименование	В настоящей Концепции	В проекте Закона ”О платежных системах и платежных услугах“
ASPSP	Account Servicing Payment Service Provider	Поставщик API	Банк
AISP	Account Information Service Provider	Пользователь API второго типа	Поставщик информационных платежных услуг
PISP	Payment Initiation Services Provider	Пользователь API второго типа	Поставщик платежных услуг инициирования платежа
PSP	Payment Services Provider	Пользователь API второго типа	Поставщик платежных услуг
PSU	Payment Services User	Клиент	Пользователь платежных услуг
TPP	Third Party Provider	Пользователь API второго типа	Поставщик информационных платежных услуг и Поставщик платежных услуг инициирования платежа

Участниками экосистемы открытых API являются регулятор, клиент, пользователь API, поставщик API, центр компетенций, испытательная лаборатория (центр).

Взаимоотношения между основными участниками построены на следующих принципах:

Регулятор реализует полномочия по регулированию взаимоотношений участников экосистемы открытых API в соответствии с законодательством и в рамках своей компетенции, определяет полномочия центра компетенций;

центр компетенций оказывает поддержку участников экосистемы открытых API, в том числе в рамках ведения портала открытых API;

взаимодействие между пользователем API и поставщиком API, пользователем API и испытательной лабораторией (центром), поставщиком API и испытательной лабораторией (центром) осуществляется на договорной основе;

взаимодействие пользователя API и клиента осуществляется на договорной основе с обязательным предоставлением клиентом согласия на доступ к информации ограниченного распространения, имеющейся у поставщика API. Согласие на доступ к такой информации может оставаться в силе до определенного поставщиком API количества дней, после этого необходимо повторное представление согласия. Согласие на доступ к информации ограниченного распространения может быть отозвано клиентом в любой момент;

во время заключения договора и/или предоставления согласия на доступ к информации ограниченного распространения клиент должен иметь возможность выбрать в отношении каких услуг он хочет предоставить доступ пользователю API к информации ограниченного распространения;

любая платежная операция должна быть авторизована клиентом. Авторизация может осуществляться в случае успешной идентификации и аутентификации клиента пользователем API с соблюдением положений законодательства.

Модели взаимодействия участников в экосистеме открытых API приведены в приложении 3 настоящей Концепции.

3.3.2. Роль и функции центра компетенций

В роли центра компетенций может выступать организация, которая обеспечивает развитие и функционирование экосистемы открытых API. Данная организация, как единый орган компетенции, должна обеспечивать единообразие подходов к созданию, реализации, использованию и выводу из эксплуатации открытых API, а также принятие иных решений по соответствующим вопросам в рамках имеющихся компетенций и полномочий. Также, к основным функциям данной организации могут относиться:

поддержка участников экосистемы открытых API на всех этапах развития, инициирование изменений спецификаций и согласование организационной работы всех участников, разработка методических рекомендаций;

оказание содействия регулятору при разработке новых стандартов открытых API, а также поддержание в актуальном состоянии существующих версий стандартов открытых API, рассмотрение и согласование предложений, пришедших от участников экосистемы;

содействие в организации процесса использования открытых API на рынке финансовых инструментов и платежных услуг в Республике Беларусь;

мониторинг использования открытых API всеми участниками экосистемы открытых API;

поддержка единого портала открытых API (портала разработчика);

разработка схемы и процесса проверки программных продуктов участников экосистемы открытых API;

ведение реестра пользователей и поставщиков API;

организация работы и процесса разрешения споров между участниками экосистемы открытых API;

оценка соответствия стандарту и спецификациям поставщиков API и пользователей API, возможно с привлечением испытательной лаборатории (центра).

3.3.3. Роль и функции испытательной лаборатории (центра)

Испытательная лаборатория (центр) осуществляет проверку требованиям стандартов открытых API и иным заданным центром компетенций критериям открытых API, внедренных поставщиком API, а также программных продуктов пользователей API – в случае если данная необходимость определена регулятором и/или актами законодательства. Порядок привлечения испытательной лаборатории (центра) определяется центром компетенций.

3.3.4. Экономическая модель открытых API

Развитие открытых API предполагает получение взаимных выгод всеми участниками экосистемы открытых API.

Заинтересованность поставщиков API предполагается в монетизации предоставления доступа к открытым API, а также развития партнерских каналов продаж банковских услуг за счет использования пользователями API второго типа открытых API.

В таблице 3 представлены возможные модели монетизации открытых API с описанием предполагаемых источников монетизации для каждой из них.

Таблица 3. Экономическая модель открытых API

Участник	Источник монетизации	Описание
Центр компетенций	Пользователи API, Поставщики API	Возможны различные схемы финансирования, в частности — оплата услуг Центра компетенций, перечисление части членских взносов при финансировании с привлечением различных ассоциаций (союзов) и др.
Испытательная лаборатория (центр)	Пользователи API, Поставщики API	Оплата за процедуру оценки соответствия стандарту, спецификациям и иным нормам.
Поставщики API	Пользователи API	Монетизация по одной из моделей: 1) подписка на доступ к открытым API 2) оплата за API-запросы 3) оплата за транзакции 4) разделение выручки
	Клиенты	Монетизация через новых клиентов, привлеченных через партнерскую (дилерскую) сеть, которая станет доступна за счет применения открытых API
Пользователи API второго типа	Клиенты	Монетизация за счет value-added сервисов поверх базовых финансовых инструментов поставщиков API
Пользователи API первого типа	Клиенты	Использование информации, получаемой посредством открытых API для получения конкурентных преимуществ в процессе последующего производства товаров, выполнения работ, оказания услуг (без непосредственного использования API для оказания услуг клиентам)

3.3.5. Правовое регулирование экосистемы

Стандарты открытых API должны базироваться на принятых международных стандартах, актах законодательства, в том числе

технических нормативных правовых актах Республики Беларусь, где это применимо.

Пользователи API второго типа несут ответственность перед клиентами в соответствии с актами законодательства и заключаемыми договорами за неисполнение (ненадлежащее исполнение) своих обязательств, связанных с предоставлением платежных услуг, а также за необеспечение (ненадлежащее обеспечение) защиты информации, распространение и (или) предоставление которой ограничено в соответствии с законодательством, в том числе сведений, составляющих банковскую и иную охраняемую законом тайну. В случае, если неисполнение (ненадлежащее исполнение) обязательств пользователя API второго типа, необеспечение (ненадлежащее обеспечение) защиты информации было вызвано действиями поставщика API или иных лиц, данный факт не является основанием для освобождения пользователя API второго типа от ответственности перед клиентом.

Пользователи API второго типа не должны нести ответственность за ущерб, причиненный клиентам неисполнением (ненадлежащим исполнением) обязательств перед ними, если такое неисполнение (ненадлежащее исполнение) обязательств было вызвано действием непреодолимой силы или действиями клиентов, а также в иных случаях, определенных законодательством.

Основными законодательными актами и нормативными правовыми актами Республики Беларусь, которыми следует руководствоваться при разработке стандартов открытых API, являются:

Банковский кодекс Республики Беларусь;

Гражданский кодекс Республики Беларусь;

Указ Президента Республики Беларусь от 18 апреля 2019 г. № 148 ”О цифровых банковских технологиях“;

Указ Президента Республики Беларусь от 16 декабря 2019 г. № 460 ”Об общегосударственной автоматизированной информационной системе“;

Закон Республики Беларусь от 10 ноября 2008 г. № 455-З ”Об информации, информатизации и защите информации“;

Закон Республики Беларусь от 9 января 2002 г. № 90-З ”О защите прав потребителей“;

Инструкция об использовании программно-аппаратных средств и технологий, проведении процедур удаленной идентификации, удаленного обновления (актуализации), утвержденная постановлением Правления Национального банка Республики Беларусь от 19 сентября 2019 г. № 379;

СПР 6.01.

Пользователи API второго типа предоставляют услуги клиентам на основании договоров возмездного оказания услуг, которые, как правило, являются публичными договорами и (или) договорами присоединения. Данные договоры заключаются на неопределенный срок и содержат общие условия взаимоотношений сторон при оказании соответствующих платежных и иных финансовых услуг, осуществлении платежной операции (платежных операций), ответственность пользователей API второго типа за неисполнение (ненадлежащее исполнение) принятых на себя обязательств. Указанные и иные условия могут быть конкретизированы и уточнены сторонами путем заключения отдельных договоров и (или) на основании договоров иных видов. При этом условия любых договоров, заключаемых между пользователями API второго типа и клиентами – физическими лицами, должны соответствовать требованиям законодательства о защите прав потребителей.

Пользователи API второго типа предоставляют клиентам до заключения договоров полную информацию об услугах, оказываемых ими с использованием собственных программных продуктов (приложений). Национальный банк для пользователей API второго типа вправе устанавливать требования к предоставлению информации об оказываемых ими платежных и иных финансовых услугах с использованием API путем принятия (утверждения) технических нормативных правовых актов, не относящихся к области технического нормирования и стандартизации.

Пользователи API второго типа обеспечивают равный и открытый доступ клиентам к оказываемым платежным и иным финансовым услугам, за исключением случаев, предусмотренных законодательством.

Поставщик API должен обеспечить равный во всех технических и юридических аспектах открытый доступ пользователям API к данным и услугам, за исключением случаев, предусмотренных законодательством. Правила доступа пользователей API к данным и услугам поставщика API должны быть объективными, не допускающими ограничение или получение каких-либо преимуществ, соразмерными и не препятствовать доступу к соответствующим данным и услугам больше, чем это необходимо для снижения (недопущения) таких платежных рисков, как расчетный, операционный и коммерческий риски, а также для защиты финансовой и операционной надежности поставщика API.

3.4. Стандартизация открытых API

3.4.1. Общие подходы к стандартам открытых API

Под стандартами открытых API в настоящей Концепции понимаются технические нормативные правовые акты и техническая

документация, определяющая порядок описания, разработки и внедрения открытых API.

Документация стандарта открытых API должна определять:

модели данных, которые отражают все элементы, необходимые для использования открытых API;

структуру сообщений, передаваемых между участниками, использующими открытые API;

способы обеспечения информационной безопасности;

модель управления изменениями открытых API.

Основные термины, форматы сообщений и все параметры запросов должны быть основаны на стандартах проведения расчетов (далее – СПР). Иные определения, термины и параметры, не описанные в СПР, должны включать в себя не противоречащие ему определения и наименования из стандарта ISO 20022, где это применимо.

Положения стандарта ISO 20022, при отсутствии соответствующих терминов и определений в СПР применимы в следующих предметных областях стандарта:

платежи и расчеты: инициирование платежей, управление денежными средствами;

банковские платежные карточки, платежи с их использованием;

конверсионные операции.

При разработке требований к API следует учитывать принципы PSD2. Для разрабатываемых открытых API рекомендуется руководствоваться основными принципами:

законность, справедливость и прозрачность – персональные данные и банковская тайна клиентов должны быть недоступны третьим лицам, не имеющим права доступа к таким данным и информации в соответствии с законодательством, и должны передаваться в виде и посредством каналов передачи данных, которые соответствуют требованиям безопасности, установленным актами законодательства в области защиты информации. Персональные данные и банковская тайна клиентов предоставляются банком только после получения согласия соответствующего клиента на предоставление указанной информации конкретному лицу (например, пользователю API второго типа), за исключением случаев, установленных законодательными актами. При каждом запросе (сеансе связи) на предоставление банковской тайны клиента пользователь API должен быть однозначно идентифицирован и аутентифицирован поставщиком API;

наличие конкретных задач – все конкретные задачи должны быть закреплены в политике конфиденциальности (иных локальных правовых актах) пользователя API и должны четко соблюдаться;

минимизация использованных данных – использование адекватного количества данных для выполнения поставленных целей, ограниченных только необходимым количеством для выполнения конкретной задачи;

достоверность – персональные данные должны быть достоверными и не должны вводить в заблуждение, должно обеспечиваться исправление неправильных данных. Информация ограниченного распространения клиента предоставляется по правилам и (или) форматам и (или) в виде и (или) форме, установленным законодательством;

ограничение срока хранения данных – данные не должны храниться дольше чем нужно, периодически необходимо проводить аудит данных и удалять неиспользуемые данные;

целостность и конфиденциальность информации – хранение информации ограниченного распространения обеспечивается поставщиком API, пользователями API, которые имеют право на получение такой информации и ее хранение. Хранение указанных данных и информации обеспечивается в соответствии с требованиями законодательства об архивном деле и делопроизводстве, требованиями об информационной безопасности.

Для стандартизации открытых API первоначально необходимо определить виды информации по степени доступности.

3.4.2. Виды информации

Информация, используемая и передаваемая посредством открытых API, может быть:

общедоступной;

ограниченного распространения (распространение и (или) предоставление которой ограничено).

К общедоступной информации относится следующая информация:

информация о курсах валют (при приеме для обмена наличных и (или) безналичных денежных средств, в том числе с использованием банковских платежных карточек, систем дистанционного банковского обслуживания, программно-технической инфраструктуры с использованием банковских платежных карточек);

информация о пунктах обслуживания клиентов банка (отделения, филиалы, обменные пункты, пункты самообслуживания с использованием программно-технической инфраструктуры с использованием банковских платежных карточек) с указанием адреса и времени работы, контактных телефонов, адресов электронной почты, списком оказываемых услуг и иная информация о каждом пункте обслуживания;

информация о платежных услугах и иных банковских услугах (связанная с открытием и обслуживанием счетов, выдачей кредитов, открытием депозитов, обслуживанием кредитов и депозитов, эмиссией банковских платежных карточек, драгоценными металлами, монетами, условиями осуществления денежных переводов, включая переводы без открытия счета и др.).

К информации ограниченного распространения в рамках отношений между участниками экосистемы открытых API относятся:

1) информация, которая является банковской тайной:

а) сведения о счетах и вкладах (депозитах), в том числе о наличии счета в банке (небанковской кредитно-финансовой организации), его владельце, номере и других реквизитах счета, размере средств, находящихся на счетах и во вкладах (депозитах);

б) сведения о конкретных сделках, об операциях без открытия счета, об операциях по счетам и вкладам (депозитам);

в) сведения об имуществе, находящемся на хранении в банке;

2) персональные данные – основные и дополнительные персональные данные физического лица, подлежащие в соответствии с законодательными актами Республики Беларусь внесению в регистр населения, а также иные данные, позволяющие идентифицировать такое лицо. К основным персональным данным относятся:

а) идентификационный номер;

б) фамилия, собственное имя, отчество (если таковое имеется);

в) пол;

г) число, месяц, год рождения;

д) место рождения;

е) цифровой фотопортрет;

ж) данные о гражданстве (подданстве);

з) данные о регистрации по месту жительства и (или) месту пребывания;

и) данные о смерти или объявлении физического лица умершим, признании безвестно отсутствующим, недееспособным, ограниченно дееспособным;

3) иная информация, распространение и (или) предоставление которой ограничено.

3.4.3. Технические требования к стандартам открытых API

Основополагающим документом при разработке технических требований к открытым API является ISO/TS 23029:2020 ”Web-service-based application programming interface (WAPI) in financial services“. Документ определяет основные принципы дизайна открытых API финансовой отрасли.

При разработке API должен использоваться архитектурный стиль REST через веб-сервисы (RESTful). Формат обмена данными – JSON (JavaScript Object Notation) и/или XML, который широко используется в сообществе разработчиков.

К основным компонентам, которые включаются в стандарты открытых API, относятся:

описание портала разработчика;

каталог API и документация;

документация по управлению жизненным циклом API;

документация по управлению изменениями в стандарты API и поддержка;

документация по лучшим практикам применения открытых API для разработчиков.

3.4.3.1. Портал разработчика

Портал разработчика представляет собой платформу, содержащую основную информацию по методам API и другим ресурсам для разработчиков открытых API, а также тестовую среду (”песочницу“).

На портале должна быть возможность получения поддержки, обмена информацией, возможность обсуждения вопросов, связанных с описанием, разработкой, внедрением открытых API.

Предполагается, что разработка и поддержка портала должна входить в зону ответственности центра компетенций.

Портал для разработчика следует делать открытым для любых юридических и физических лиц. Базовая регистрация (имя, адрес электронной почты, название компании, URL, тип разработчика, адрес и др.) может использоваться для доступа к тестовой среде ”песочнице“, участия в форумах, получения поддержки от разработчика и т.п.

Портал разработчика должен предусматривать возможность формировать оперативную отчетность по показателям использования открытых API в разрезе конкретных пользователей и поставщиков API. Эти метрики обеспечат ключевые оперативные знания для эффективного обновления и поддержки стандарта по мере использования платформы и внедрения открытых API, а также могут быть использованы как единый и доверенный источник информации для проведения расчетов между поставщиками API и пользователями API в соответствии с используемой схемой монетизации.

Портал будет предоставлять основную информацию и описания API, доступных и планируемых для разработки, которые потенциальные пользователи API могут просматривать и использовать для тестирования в своих приложениях.

Портал разработчика будет придерживаться политик и процедур, которые определяют время разработки API, создание новой версии API или делать рефакторинг существующей версии и как происходит внутренняя интеграция с другими системами.

Будет использован подход к публикации, продвижению и контролю за открытыми API и средой, в которой они внедрены, и поддержка разработчиков программных продуктов с использованием API.

В приложении 4 настоящей Концепции представлен возможный набор API методов для разработки и внедрения открытых API.

3.4.3.2. Принципы разработки, внедрения и обновления стандартов открытых API

Версионность

Принцип управления версиями API предполагает использование обозначения версии с использованием двух чисел, разделенных разделителем: X.Y, где X – major-version (главная версия), Y – minor-version (дополнительная версия).

Главная версия используется для выявления несовместимых изменений в текущей опубликованной версии API.

Дополнительная версия используется для внесения изменений в функциональность API. Изменения, внесенные в дополнительную версию, не должны вызывать несовместимости в рамках одной главной версии.

Разработка пилотных проектов, анализ результатов, обновление стандартов на их основе

Для получения открытых API, которые соответствуют требованиям всех участников экосистемы, развития рынка и удовлетворения запросов клиентов, рекомендуется создавать пилотные проекты для понимания работы открытых API в реальных условиях.

При поддержке центра компетенции пилотные проекты могут создаваться поставщиком API совместно с пользователями API для демонстрации возможностей API, выявления слабых сторон и предоставления рекомендаций по улучшению составляющих API.

При успешном завершении пилотных проектов проводится сбор и обработка предложений от участников экосистемы открытых API по улучшению открытых API и расширению использования открытых API поставщиками API и пользователями API.

3.5. Информационная безопасность открытых API

Для организации безопасного доступа и использования банковских услуг посредством открытых API должны быть решены следующие задачи:

обеспечение надежности при проверке аутентичности поставщика API и пользователя API;

надежные аутентификация и идентификация клиента;

авторизация платежной операции клиентом;

обеспечение безотзывности платежной операции;

обеспечение конфиденциальности и целостности данных, передаваемых по открытым каналам связи в ходе получения банковской услуги, а также хранимых в информационных системах поставщика API (пользователя второго типа);

риск-ориентированный подход.

В Республике Беларусь существует Национальная система подтверждения соответствия, поэтому для решения указанных задач должны использоваться методы защиты информации, разрешенные в соответствующих актах законодательства или технических нормативных правовых актах. На дату публикации данного документа основными актами законодательства являются:

Указ Президента Республики Беларусь от 9 декабря 2019 г. № 449 ”О совершенствовании государственного регулирования в области защиты информации“;

приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 ”О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449“.

В рамках работы по разработке и утверждению конкретных стандартов API могут формироваться предложения по внесению изменений и дополнений в акты законодательства.

3.5.1. Проверка аутентичности

Открытые API могут предоставлять данные, используемые клиентом для принятия решений, в связи с этим клиенту требуются гарантии, что он обратился непосредственно к поставщику API, а не использует мошенническую реализацию (фрод). Таким образом, должен быть решен вопрос проверки клиентом аутентичности поставщика API (пользователя API второго типа).

Открытые API в качестве транспортного протокола используют протокол HTTPS. Поэтому для надежной аутентификации поставщика услуги целесообразно применять протокол TLS, предназначенный для защиты информации в HTTPS, с использованием криптографических методов, определяемых СТБ 34.101.65-2014 ”Информационные технологии и безопасность. Протокол защиты транспортного уровня (TLS)“ (далее – СТБ 34.101.65).

Это делает целесообразным применение СТБ 34.101.65 при разработке и внедрении открытых API.

Ошибки при проверке аутентичности должны приводить к отказу в доступе к поддельному ресурсу.

Данные аутентификации пользователя API и его сеанса, а также токены аутентификации не могут передаваться в форме параметров URI.

3.5.2. Идентификация и аутентификация клиента

При выполнении отдельных операций с использованием открытых API (например, получение баланса по банковскому счету) требуется обеспечить надежные идентификацию и аутентификацию клиента.

Процесс аутентификации клиента должен проходить с учетом международных практик и стандартов, в частности, должны соблюдаться принципы Strong Customer Authentication [11] (далее – SCA), которые являются обязательным требованием директивы PSD2 при оказании платежных услуг.

Подход SCA означает аутентификацию, основанную на использовании двух или более элементов (компонентов), классифицированных как ”Знание“ (то, что знает только пользователь: например, пароль), ”Владение“ (то, что есть только у пользователя: например, ключ электронной цифровой подписи (далее – ЭЦП)) и ”Человек“ (то, что присуще только одному человеку: например, отпечаток пальца). Все эти элементы являются независимыми в том смысле, что нарушение одного из них не ставит под угрозу надежность других.

Графически принципы SCA представлены на рисунке 6.

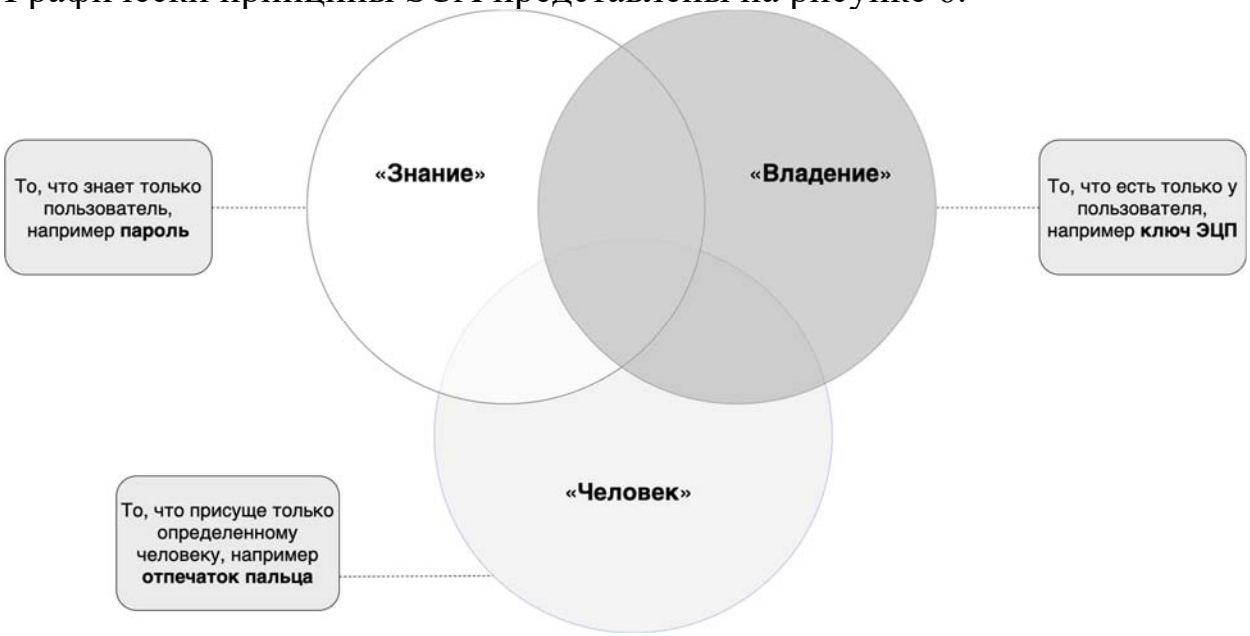


Рисунок 6. Принципы SCA

[11] Strong Customer Authentication — https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.069.01.0023.01.ENG&toc=OJ:L:2018:069:TOC

Рабочими группами Open Banking UK и Berlin Group NextGenPSD2 выделяются 4 подхода к аутентификации по принципу SCA:

переадресация на сторону поставщика API, которая подразумевает выполнение процедуры аутентификации на веб-сайте (странице) поставщика API тем способом, который поставщик API считает целесообразным для данного клиента или действия;

использование внешнего сервиса, что аналогично аутентификации с переадресацией на сторону поставщика API, только в роли поставщика API в рамках данной аутентификации выступает внешний сервис;

использование протокола OAuth 2.0. В этом сценарии роли oAuth распределяются следующим образом: пользователь API – клиент oAuth, клиент — владелец ресурса oAuth, поставщик API – сервер ресурсов oAuth;

использование встроенных механизмов пользователя API. Здесь предполагается использование внутренних механизмов, например, генерация ЭЦП на устройстве клиента.

На рисунках 7–10 представлены схемы данных подходов.

Рисунок 7. Аутентификация с переадресацией на сторону поставщика API

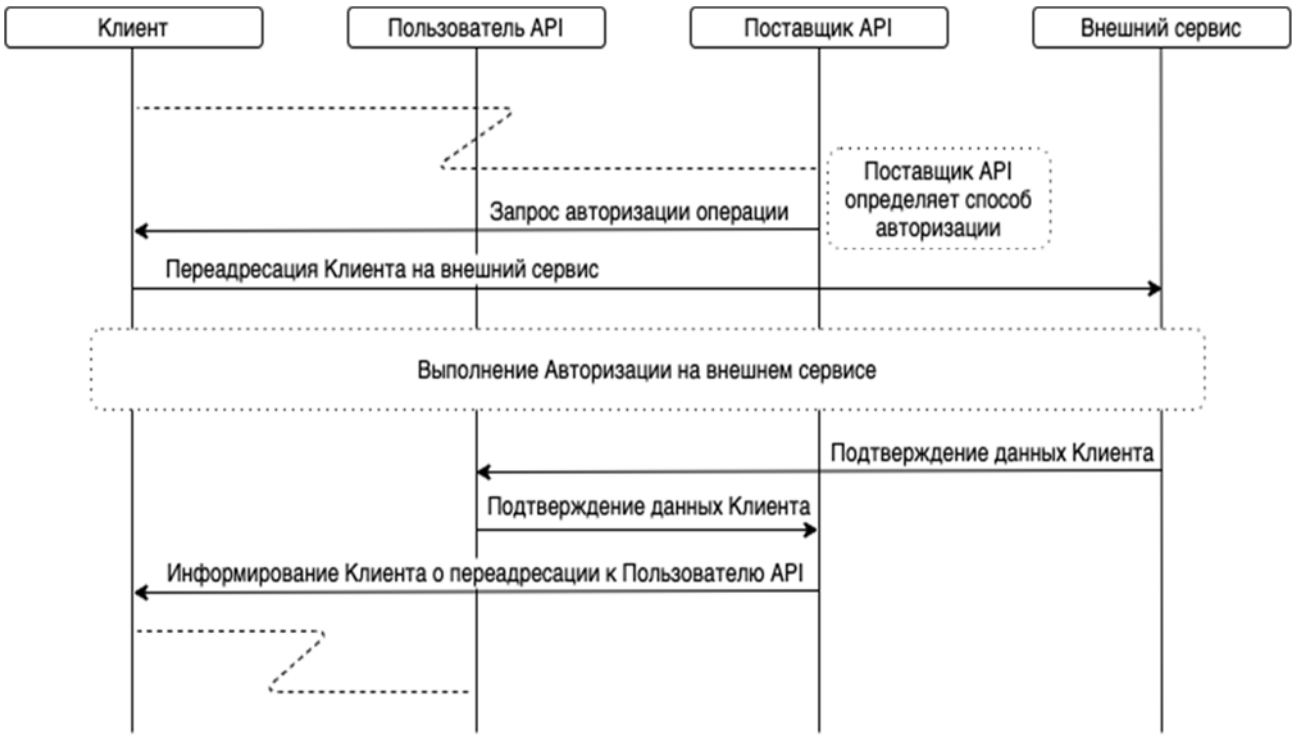


Рисунок 8. Аутентификация с использованием внешнего сервиса

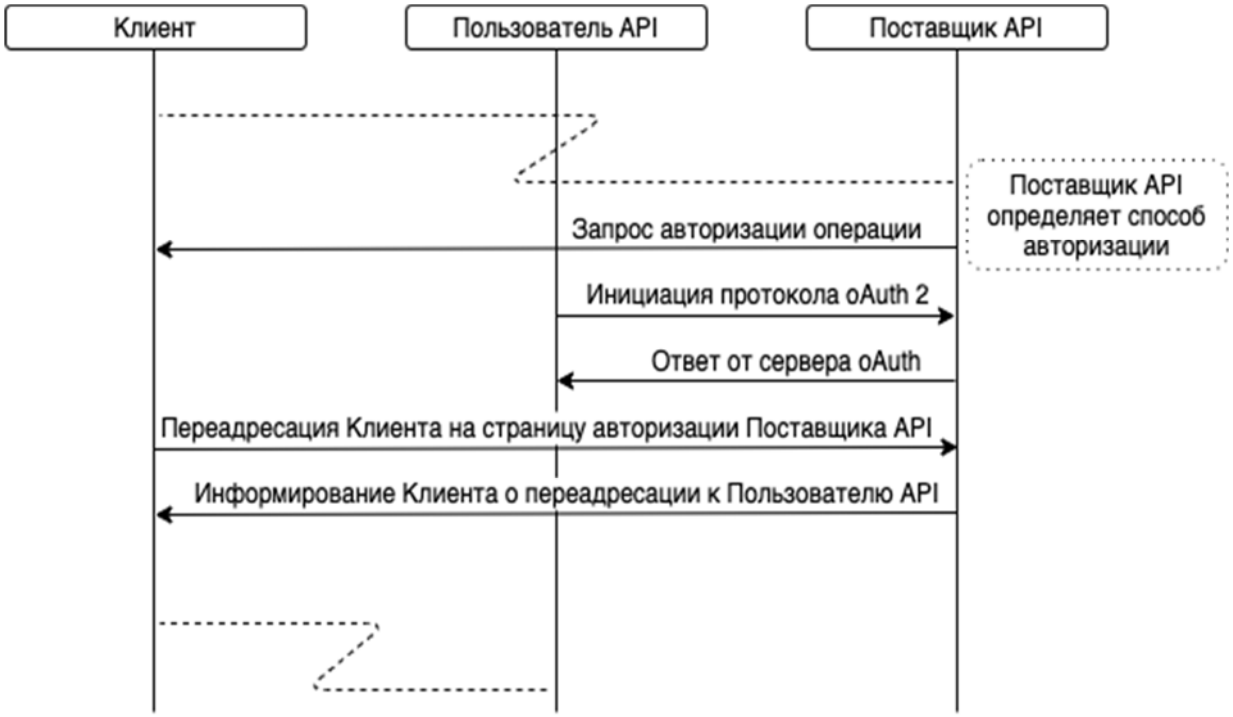


Рисунок 9. Аутентификация с использованием протокола OAuth 2.0

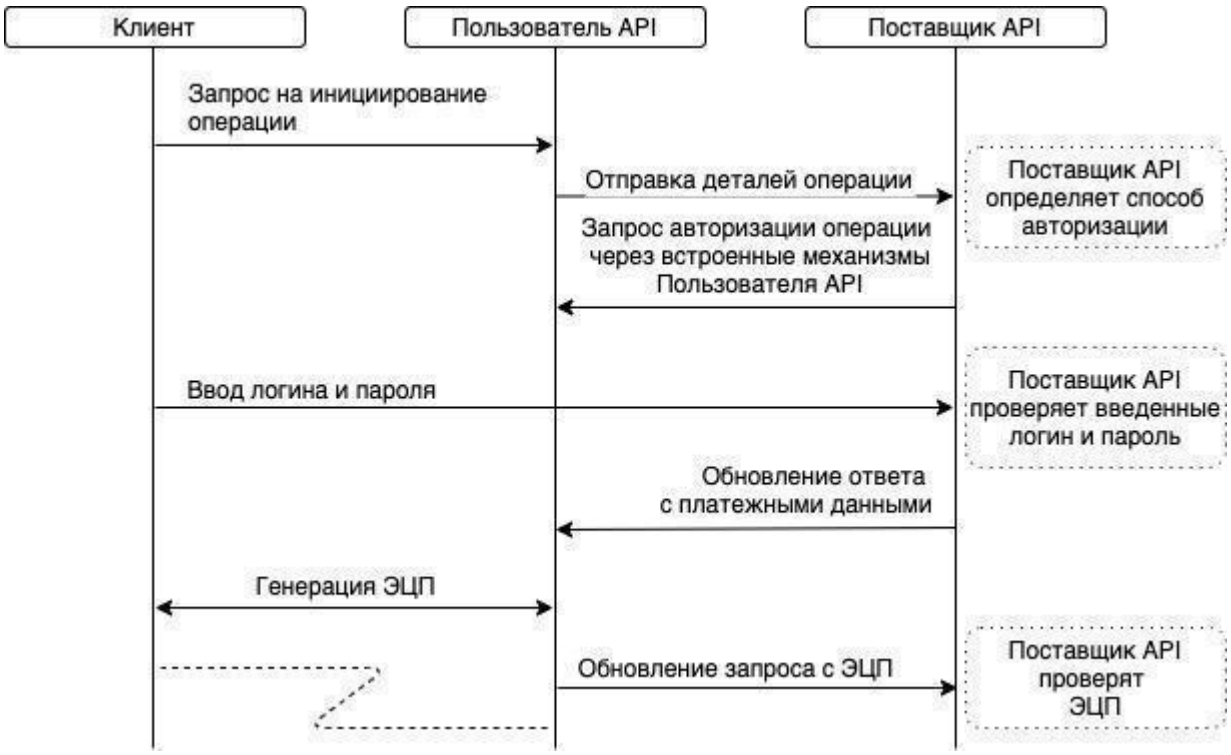


Рисунок 10. Аутентификация через встроенные механизмы пользователя API (например, ЭЦП)

Целесообразным является проведение работ по принятию лучших международных практик (ISO/IEC 29115:2013 ”Information technology. Security techniques. Entity authentication assurance framework“, NIST SP 800-63 ”Digital Identity Guidelines“) по стандартизации уровней гарантий в качестве государственных стандартов и его использованию в открытых API.

Целесообразным также является добавление к сеансу пользователя с поставщиком открытых API признака ”Уровень гарантий по аутентификации“, что позволит поставщику API осуществлять управление рисками.

3.5.2.1. Особенности реализации идентификации и аутентификации в Республике Беларусь

С 1 сентября 2021 г. в Республике Беларусь начата выдача идентификационных (ID) карт для граждан Республики Беларусь.

ID-карта реализует криптографический протокол аутентификации согласно СТБ 34.101.79-2019 ”Информационные технологии и безопасность. Криптографические токены“, который может использоваться для надежной аутентификации клиента. ID-карта может служить источником основных идентификационных данных клиента.

ID-карта также содержит приложение ЭЦП с сертификатами Государственной системы управления открытыми ключами проверки

электронной цифровой подписи Республики Беларусь (далее – ГосСУОК). В рамках протокола TLS согласно СТБ 34.101.65-2014 ”Информационные технологии и безопасность. Протокол защиты транспортного уровня (TLS)“ при аутентификации поставщика API одновременно может выполняться аутентификация клиента (пользователя API первого типа) с использованием сертификата ГосСУОК, что в совокупности обеспечивает надежную взаимную аутентификацию клиента и поставщика API. Массовое использование данного метода может быть ограничено сложностью его реализации, однако он может применяться в корпоративных информационных системах (с предустановленным программным обеспечением).

Это делает целесообразным поддержку ID-карт в открытых API каждым поставщиком API.

Согласно Указу Президента Республики Беларусь от 1 декабря 2015 г. № 478 ”О развитии цифровых банковских технологий“ в Республике Беларусь создана и функционирует Межбанковская система идентификации (далее – МСИ), которая является надежным источником идентификационных данных клиентов банков.

Это делает целесообразным использование МСИ в открытых API в качестве единого специализированного сервиса аутентификации, особенно при добавлении поддержки ID-карт.

Перечень сервисов аутентификации для открытых банковских API может расширяться с введением в эксплуатацию новых государственных или корпоративных информационных систем, предоставляющих данный сервис.

3.5.3. Авторизация операции

Пользователь API должен начинать выполнение платежной операции с создания ресурса согласия на эту операцию (consent). Этот ресурс определяет разрешения, которые присылает пользователь API от имени клиента. На начальном этапе согласие не авторизовано, поскольку поставщик API еще не верифицировал разрешения непосредственно с самим клиентом.

Поставщик API отвечает сообщением, которое содержит идентификатор ресурса согласия. Этот идентификатор используется при инициировании потока авторизации, который нужен для подтверждения клиентом разрешений.

Целесообразным является добавление к сеансу пользователя с поставщиком открытых API признака ”Уровень гарантий по аутентификации при авторизации“, что позволит поставщику API осуществлять управление рисками.

В зависимости от риска операции, выполняемой через открытые API, поставщик API может запрашивать способы аутентификации разного уровня гарантий – от ввода пароля для оплаты телефона до выработки ЭЦП для выполнения произвольного платежа.

3.5.4. Обеспечение безотзывности платежа или невозможности отказа от совершения операции

При выполнении отдельных операций через открытые API (например, проведение платежа) требуется обеспечить безотзывность платежа или невозможность отказа от совершения операции.

Унификация открытых API требует унификации способов обеспечения безотзывности платежа или невозможности отказа от совершения операции: могут вводиться уровни гарантий по невозможности отказа от совершения операции, может вводиться технологическая ЭЦП, чей сертификат открытого ключа будет включать специальную политику для определения уровня гарантий. Использование ЭЦП с сертификатами ГосСУОК или со специализированными технологическими сертификатами является предпочтительным.

Использование ЭЦП также не противоречит требованиям ISO 20022: каждое сообщение может содержать ЭЦП.

3.5.5. Обеспечение конфиденциальности и целостности данных

СТБ 34.101.65-2014 ”Информационные технологии и безопасность. Протокол защиты транспортного уровня (TLS)“ кроме аутентификации сервера (поставщика API, пользователя API второго типа) дополнительно определяет криптографические методы для обеспечения конфиденциальности и контроля целостности данных, передаваемых по открытым каналам связи в ходе получения банковской услуги.

Для обеспечения защиты информации о банковской операции при ее хранении в информационной системе – конфиденциальности, целостности и доступности – должна быть создана и в установленном порядке аттестована система защиты информации.

Целостность гарантирует, что сообщение (т.е. подписываемый контент) не было изменено при передаче и хранении.

В целях обеспечения надлежащей безопасности в модели, использующей механизм аутентификации на стороне поставщика API, перенаправление на веб-сайт (страницу) поставщика API и обратно на сайт пользователя API будет происходить в браузере (браузеры, отличные от системного, не должны быть разрешены, применение

WebView не допускается), а не в самом мобильном приложении. Пользователь API может использовать специальный URL в приложении, чтобы после перенаправления обратно на сторону пользователя API мобильное приложение автоматически возобновлялось.

Рекомендуется, чтобы в своей конфигурации у каждого поставщика API был список redirect_uri по каждому пользователю API, который можно использовать. Таким образом, поставщик API не будет перенаправлять клиента на неверный URL-адрес, который может быть предоставлен ненадежной (подмененной) стороной.

Рекомендуется, чтобы участвующие в экосистеме организации обменивались информацией о подозрительных и несанкционированных транзакциях, скомпрометированных IP-адресах и т. д.

3.5.6. Управление рисками

Как отмечалось выше, целесообразным является введение показателей ”Уровень гарантий по аутентификации“, ”Уровень гарантий по аутентификации при авторизации“, ”Уровень гарантий по неотказуемости“ для сеанса пользователя с поставщиком API.

Поставщик API в зависимости от значений данных показателей может управлять рисками при проведении операции: разрешать операцию, запрещать операцию, требовать пройти дополнительную аутентификацию для увеличения значения показателя.

3.5.7. Общие требования к открытым API в части информационной безопасности

Поставщик API должен обеспечивать доступность своих сервисов и использовать средства защиты информации, которые обеспечивают конфиденциальность и целостность данных клиентов.

Пользователь API вправе в случаях и порядке, установленных законодательством, получать сведения, составляющие банковскую и иную охраняемую законом тайну, в объеме, необходимом и достаточном для оказания платежных услуг. Соблюдение сохранности указанных сведений, особенности их использования и (или) обработки устанавливаются действующим законодательством.

Пользователь API не вправе:

сохранять данные клиента, составляющие банковскую тайну и содержащие информацию, распространение и (или) предоставление которой ограничено в соответствии с законодательством, получать и (или) использовать какие-либо данные в иных целях, кроме оказания услуги в соответствии с запросом клиента;

запрашивать у клиента какие-либо иные данные, кроме данных, необходимых для оказания услуги;

изменять сумму платежа, получателя платежа или иные детали платежной операции.

Пользователь API обязан обеспечить (организовать обеспечение) безопасность платежного инструмента и принять меры по обеспечению защиты персональных данных клиента, к которым предоставляется доступ посредством платежного инструмента, в том числе обеспечить защиту от несанкционированного доступа к указанным данным третьих лиц, до момента передачи платежного инструмента клиенту.

Приложение 1
к Концепции
развития открытых
банковских API
Республики Беларусь

Сравнительная таблица по опыту разработки и внедрения открытых API в Европе

Таблица 1

	Великобритания	Германия	Польша
Дата начала инициативы	2016	2010	2018
Инициатор	Правительство	Правительство/ субъекты рынка	Правительство
Наличие реестра пользователей API	Да	Нет	Нет
Кто управляет	Самостоятельное юридическое лицо	Самостоятельное юридическое лицо	Самостоятельное юридическое лицо
API для физических лиц	Да	Да	Да
API для юридических лиц	Да	Да	Да
Ориентация на ISO 20022	Да	Да	Нет
JSON/XML	JSON	JSON/XML	JSON
Использование API для инициирования платежей	Да	Да	Да

Приложение 2
к Концепции
развития открытых
банковских API
Республики Беларусь

Сравнительная таблица по мировому опыту разработки и внедрения открытых API

Таблица 1

		UK	AU	HK	SP	NZ	JP	MX	IN	US
Инициатор	Антимонопольный орган	+	+							
	Валютный орган	+		+			+	+	+	
	Отраслевой орган				+	+	+			+
Применяемость	Крупные банки	+	+	+	+	+	+	+	+	+
	Все банки (П – планируется)	+	П		+	П	+	+	+	
	Все финансовые организации (П – планируется)		П					+		
	Разные отрасли		П							
Стандартизация	Организовано (М – рынком, Р – регулятором)	Р	Р	Р	Р	М		Р	Р	
	Уровень стандартизации (В – высокий, С – средний, Н – низкий)	В	В	С	С	С	Н	В	С	Н
Охват услуг	Информация о продукте		+	+	+		+	+	+	+
	Информация о счете	+	+	+	+	+	+	+	+	+

		UK	AU	HK	SP	NZ	JP	MX	IN	US
	Инициирование платежей	+		+	+	+	+	+	+	+
	Другое		+	+	+		+	+		+
	Юридические лица	+	+	+	+	+	+	+	+	+
	Физические лица	+	+		+	+	+	+	+	+
Готовность (B – высокий, C – средний, H – низкий)		B	C	C	B	H	C	C	C	H
Коммерческая модель		+	+	+				+		
Авторизация	Переадресация в банк	+	+							
	Встроенное в приложение			+						
Лицензирование		+	+			+				

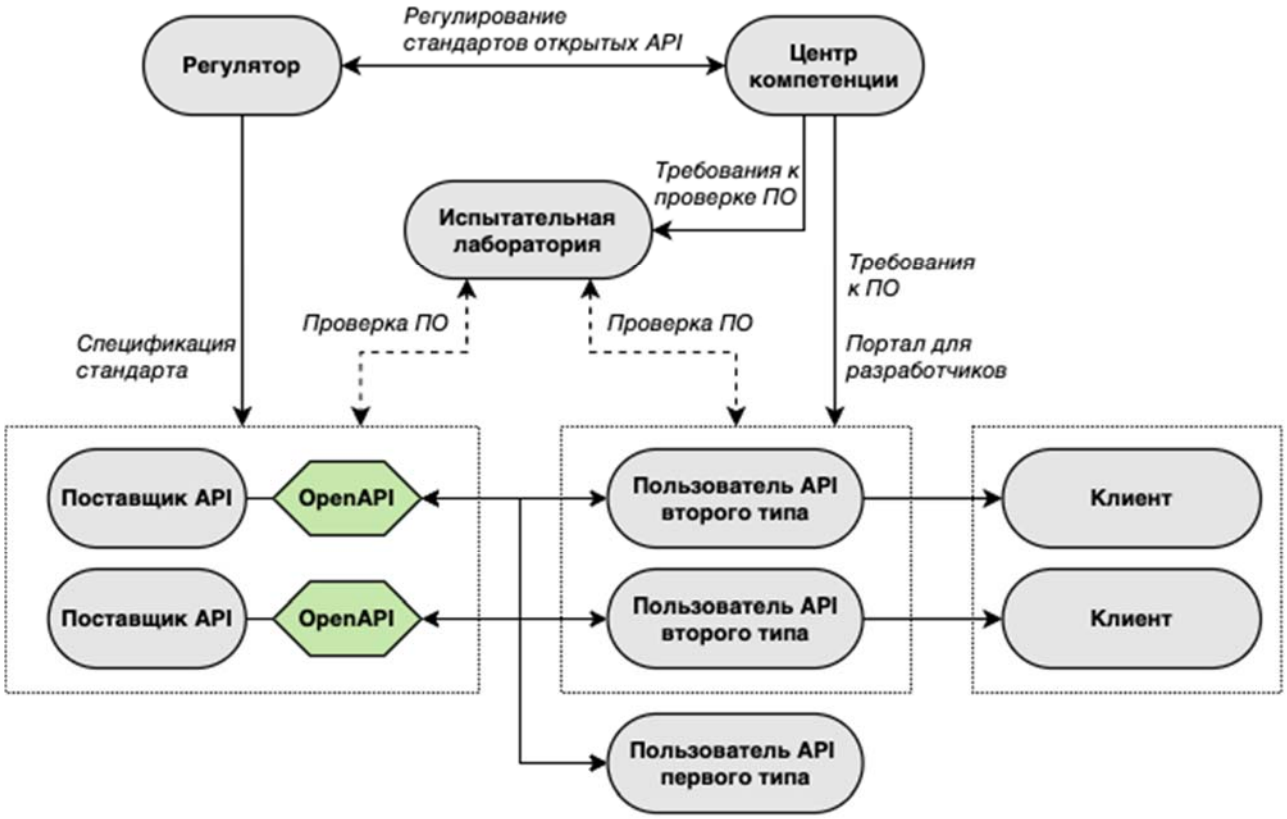
Таблица 2. Условные обозначения, используемые в Таблице 1

Обозначение	Страна
UK	Великобритания
AU	Австралия
HK	Гонконг
SP	Испания
NZ	Новая Зеландия
JP	Япония
MX	Мексика
IN	Индонезия
US	США

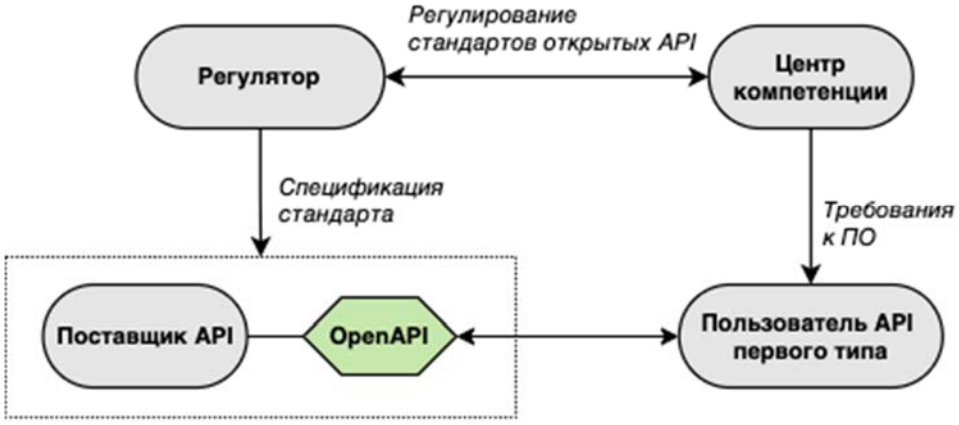
Приложение 3
к Концепции
развития открытых
банковских API
Республики Беларусь

Модели взаимодействия в экосистеме открытых API

1. Модель взаимодействия участников экосистемы при использовании открытых информационных и платежных API



2. Модель взаимодействия участников экосистемы при использовании статистических API



Приложение 4
к Концепции
развития открытых
банковских API
Республики Беларусь

Примерный перечень API методов для разработки и внедрения открытых информационных и платежных API

Таблица 1

Тип	Наименование (чтение)	Наименование (запись)	Тип информации
Информационные API	Получение списка ATM/инфокиосков		Общедоступная информация
Информационные API	Получение информации об ATM/инфокиоске		Общедоступная информация
Информационные API	Получить список всех услуг банка		Общедоступная информация
Информационные API	Получить услуги с типом ”депозит“		Общедоступная информация
Информационные API	Получение информации о депозите		Общедоступная информация
Информационные API	Получить услуги с типом ”кредит“		Общедоступная информация
Информационные API	Получение информации о кредитах		Общедоступная информация
Информационные API	Получение информации о банковских платежных карточках		Общедоступная информация
Информационные API	Получение информации об открытии счетов		Общедоступная информация

Тип	Наименование (чтение)	Наименование (запись)	Тип информации
Информационные API	Получение информации о курсах валют		Общедоступная информация
Информационные API	Получение информации об услугах с драгоценными металлами, драгоценными камнями, памятными монетами и т.п.		Общедоступная информация
Информационные API	Получить услуги с типом ”драгоценные камни“		Общедоступная информация
Информационные API	Получить услуги с типом ”монеты“		Общедоступная информация
Информационные API	Получение информации о денежных переводах, прямом дебетовании счетов		Общедоступная информация
Информационные API	Получить услуги с типом ”прямое дебетование“		Общедоступная информация
Платежные API	Получение контактной информации		Ограниченного распространения
Платежные API		Изменение контактной информации	Ограниченного распространения
Платежные API	Получение данных клиента		Ограниченного распространения
Платежные API		Изменение данных клиента	Ограниченного распространения

Тип	Наименование (чтение)	Наименование (запись)	Тип информации
Платежные API	Получение списка всех банковских счетов		Ограниченного распространения
Платежные API	Получение баланса по всем банковским счетам		Ограниченного распространения
Платежные API	Получение списка транзакций по всем банковским счетам		Ограниченного распространения
Платежные API	Получение статусов расчетных счетов		Ограниченного распространения
Платежные API	Получение баланса по конкретному банковскому счету		Ограниченного распространения
Платежные API	Получение списка транзакций по конкретному банковскому счету (выписки)		Ограниченного распространения
Платежные API	Получение информации о бронированиях денежных средств на банковском счете		Ограниченного распространения
Платежные API	Получение информации об арестах денежных средств на банковском счете		Ограниченного распространения
Платежные API		Создание платежной инструкции	Ограниченного распространения
Платежные API	Получение статуса исполнения платежной инструкции		Ограниченного распространения

Тип	Наименование (чтение)	Наименование (запись)	Тип информации
Платежные API		Платеж резиденту Республики Беларусь	Ограниченного распространения
Платежные API		Платеж нерезиденту Республики Беларусь	Ограниченного распространения
Платежные API		Отмена платежной инструкции	Ограниченного распространения
Платежные API		Удаление/изменение платежной инструкции	Ограниченного распространения
Платежные API	Получение статуса платежа		Ограниченного распространения
Платежные API	Получение деталей платежа		Ограниченного распространения
Платежные API		Авторизация платежа	Ограниченного распространения
Платежные API	Получение списка транзакций по банковским платежным карточкам		Ограниченного распространения