Національний банк України

КОНЦЕПЦІЯ
відкритого банкінгу

Зміст

Вступ

Ця Концепція встановлює принципи відкритого банкінгу в Україні, зокрема права користувача платіжних послуг у відкритому банкінгу, включаючи принципи управління згодою користувача і захисту персональних даних, побудови архітектури відкритого банкінгу, класифікації та застосування API, забезпечення безпеки та кіберзахисту, процесу взаємодії учасників платіжного ринку та відповідальності сторін, використання варіативності моделей відкритого банкінгу.

Ця Концепція не є нормативно-правовим актом. Кінцева реалізація порядку роботи відкритого банкінгу може відрізнятися від принципів, установлених цією Концепцією та зазнати змін за результатами розробки нормативно-правових актів необхідних для упровадження відкритого банкінгу.

Мета цієї Концепції – визначити напрями розвитку, дорожню карту та ключові вимоги до впровадження відкритого банкінгу в Україні.

Відкритий банкінг – екосистема, що впроваджується, щоб надати користувачам платіжних послуг більш різноманітні та привабливіші пропозиції.

За допомогою відкритого банкінгу користувачі мають змогу ефективніше втілювати свої повсякденні фінансові рішення, використовуючи консолідовану в одному застосунку інформацію про рух коштів та їх залишок на своїх рахунках, відкритих у різних фінансових установах. Водночас упровадження відкритого банкінгу впливає на розвиток фінансового сектору загалом: через збільшення конкуренції серед учасників платіжного ринку, поліпшення якості платіжних послуг, зниження вартості та більшої зручності їх використання, фінансову інклюзію, інновації.

Важливим є забезпечення довіри користувачів до нової екосистеми, що досягатиметься шляхом упровадження правил та механізмів, які узгоджені НБУ та стейкхолдерами.

Правила, що встановлюватимуться в новій екосистемі та принципи взаємодії і обміну даними в межах відкритого банкінгу, повинні бути зрозумілими та прийнятними для банків, надавачів фінансових та нефінансових платіжних послуг, технологічних операторів.

Об’єднання регулятора та стейкхолдерів для обговорення порядку роботи відкритого банкінгу допоможе напрацювати оптимальні рішення регуляторного та технічного характеру щодо стандартизованих механізмів взаємодії надавачів платіжних послуг. Також таке об’єднання допоможе напрацювати відповідні екосистемні рішення для забезпечення захисту інформації (у тому числі кіберзахисту) та мінімізації ризику шахрайства, установлення прозорих механізмів управління запитами та вирішення спорів між учасниками відкритого банкінгу.

Додатковою важливою складовою для вдалої роботи відкритого банкінгу є впровадження технології миттєвих платежів, що поліпшить досвід користувача та дасть змогу створювати нові продукти та сервіси.

Розділ 1. Терміни та скорочення

Терміни та скорочення в цій Концепції вживаються в такому значенні:

Автентифікація – процедура, що дає змогу надавачу платіжних послуг установити та підтвердити особу користувача платіжних послуг та/або належність користувачу платіжних послуг певного платіжного інструменту, наявність у нього підстав для використання конкретного платіжного інструменту, у тому числі шляхом перевірки індивідуальної облікової інформації користувача платіжних послуг.

Пункт 1 частини першої статті 1 Закону України “Про платіжні послуги”

Авторизація – визначена Законом “Про платіжні послуги” (далі – Закон) процедура допуску до провадження діяльності з надання платіжних послуг, обмежених платіжних послуг, допоміжних послуг, що здійснюється шляхом видачі ліцензії та/або включення до Реєстру платіжної інфраструктури.

Пункт 2 частини першої статті 1 Закону України “Про платіжні послуги”

Відкритий банкінг – це структурований і безпечний обмін даними між надавачами платіжних послуг та технологічним оператором платіжних послуг через відкриті API.

Відкриті API (Application Programming Interface, далі − API) – прикладні програмні інтерфейси, що ґрунтуються на загальних стандартах та забезпечують обмін даними між надавачами платіжних послуг, технологічними операторами платіжних послуг. Поділяються на базові та комерційні.

Вразливі платіжні дані – дані (їх сукупність), включаючи індивідуальну облікову інформацію, за допомогою яких можуть вчинятися шахрайські дії.

Пункт 4 частини першої статті 1 Закону України “Про платіжні послуги”

Емітент платіжних інструментів (далі – Емітент) – надавач платіжних послуг, який надає послугу емісії платіжних інструментів на підставі отриманої ліцензії.

Заходи безпеки – сукупність заходів з виконання вимог Положення про автентифікацію та застосування посиленої автентифікації на платіжному ринку (далі – Положення SCA) та інших вимог, що визначені законами України та нормативно-правовими актами Національного банку України (далі – НБУ) у сфері захисту інформації та кіберзахисту на платіжному ринку.

Підпункт 7 пункту 3 розділу 1 Положення про SCA

Інтерфейс – сукупність програмно-апаратних засобів, призначених для здійснення функцій електронної взаємодії між різноманітними пристроями та програмним забезпеченням учасників платіжного ринку в інформаційно-телекомунікаційних системах надавача платіжних послуг, мережі загального користування з метою проведення процедур автентифікації та надання фінансових та/або нефінансових платіжних послуг.

Підпункт 9 пункту 3 розділу 1 Положення SCA

Інцидент кібербезпеки (далі – кіберінцидент) – одна подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють ймовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів.

Пункт 3 частини першої статті 1 Закон України “Про основні засади забезпечення кібербезпеки України”

Кваліфікований сертифікат відкритого ключа – сертифікат відкритого ключа, який видається кваліфікованим надавачем електронних довірчих послуг, засвідчувальним центром або центральним засвідчувальним органом і відповідає вимогам Закону України «Про електронні довірчі послуги».

Пункт 25 частини першої статті 1 Закону України “Про електронні довірчі послуги”

Користувач платіжних послуг (далі – користувач) – фізична або юридична особа, яка отримує чи має намір отримати платіжну послугу як платник або отримувач (або обидва одночасно) та/або є власником електронних грошей (цифрових грошей НБУ), а в разі надання послуг банком – клієнт банку.

Пункт 28 частини першої статті 1 Закону України “Про платіжні послуги”

Надавач платіжних послуг – юридична особа, яка в установленому Законом та нормативно-правовими актами НБУ порядку отримала дозвіл на надання принаймні однієї платіжної послуги.

Несанкціоновані або шахрайські дії – вчинення сторонніми особами та/або відповідальними особами дій з втручання в інформаційно-телекомунікаційну систему незаконним протиправним шляхом, які можуть призвести до порушення цілісності, доступності та конфіденційності інформації, яку надавач платіжних послуг використовує при наданні платіжних послуг.

Підпункт 13 пункту 3 розділу 1 Положення про SCA

Посилена автентифікація (далі – SCA) – процедура автентифікації, яка передбачає використання двох чи більше сукупностей даних, що належать до таких різних категорій:

1) знань [володіння інформацією (даними), що відома лише користувачу];

2) володінь (застосування матеріального предмета, яким володіє лише користувач);

3) притаманність [перевірка біометричних даних або інших властивостей (рис, характеристик), притаманних лише користувачу, що відрізняють його від інших користувачів].

Пункт 70 частини першої статті 1 Закону України “Про платіжні послуги”

Реєстр платіжної інфраструктури (далі – Реєстр) – електронний реєстр, що ведеться Національним банком України за допомогою відповідного комплексу організаційно-технічних засобів, у якому зазначаються відомості про надавачів платіжних послуг та інших осіб, відомості про яких підлягають включенню до Реєстру відповідно до Закону.

Пункт 79 частини першої статті 1 Закону України “Про платіжні послуги”

Стейкхолдери – це надавачі платіжних послуг та їх асоціації.

Сторонні надавачі платіжних послуг – банки та надавачі платіжних послуг, які отримали право на надання нефінансових платіжних послуг.

Технологічний оператор платіжних послуг (далі − hub) − юридична особа, що надає послуги процесингу, клірингу або виконує операційні, інформаційні та інші технологічні функції, пов’язані з наданням платіжних послуг, без залучення коштів за платіжними операціями на свій рахунок.

AISP (Account Information Service Provider) – надавач платіжних послуг з надання відомостей з рахунків.

ASPSP (Account Servicing Payment Service Provider) – надавач платіжних послуг з обслуговування рахунку (банки, платіжні установи, малі платіжні установи, філії іноземних платіжних установ, установи електронних грошей, поштові оператори).

PISP (Payment Initiation Service Provider) – надавач платіжних послуг з ініціювання платіжної операції.

Інші терміни вживаються в значеннях, наведених у Законі та інших законодавчих актах.

Розділ 2. Міжнародний досвід та шлях України до відкритого банкінгу

Концепція відкритого банкінгу з'явилася в Європейському Союзі (далі – ЄС) у результаті прийняття другої редакції Директиви ЄС про платіжні послуги (PSD2) і швидко піднялася вгору у порядку денному галузі. Упровадження відкритого банкінгу викликало стрімке поширення відкритих API у всьому світу.

Наразі у світі немає єдиних узгоджених підходів щодо стандартизації API, крім того, країни перебувають на різних етапах у реалізації відкритого банкінгу загалом. Великобританія − єдина країна, яка на законодавчому рівні прийняла рішення щодо створення організації для побудови, розвитку та підтримки правил відкритого банкінгу, що в результаті дає змогу її ринку йти попереду в упровадженні нових продуктів та послуг. Однак деякі країни стрімко просуваються у розвитку власного відкритого банкінгу. У іншій групі − країни ЄС (загалом), Австралія та Мексика, які зробили значні кроки в законодавчому регулюванні та імплементації. Канада, Гонконг, Індія, Японія, Нова Зеландія, Сінгапур та США досягають прогресу в підготовці своїх ринків до ініціатив відкритого банкінгу.

Європейське банківське управління (European Banking Authority – EBA) відіграє провідну роль у впровадженні PSD2 в ЄС, видаючи керівні принципи та рекомендації зацікавленим сторонам через свої нормативні технічні стандарти.

Однак в ЄС ринкам дозволено самостійно розробляти власні стандарти відкритих API. З огляду на це кілька робочих груп представили свої напрацювання. Найбільшої популярності набули стандарти Берлінської групи (Berlin Group).

Україна рухається до інтеграції в європейський платіжний простір. Відповідно до Стратегії Національного банку України активізація економічного зростання та цифровізація є пріоритетами для регулятора. Для створення належних передумов для розвитку інноваційних платіжних послуг, а також з метою адаптації українського законодавства до стандартів ЄС, 30 червня 2021 року Верховна Рада України схвалила Закон № 1591-IX "Про платіжні послуги". Законом закладені основи нормативного врегулювання відкритого банкінгу, а повноцінний запуск цього правового режиму відбудеться в серпні 2025 року.

Розділ 3. Взаємодія НБУ з стейкхолдерами

Як зазначалось вище, запорукою успішного запуску відкритого банкінгу в Україні є широкий консенсус учасників платіжного ринку щодо принципів та стандартів його роботи. Отже, НБУ працюватиме для побудови діалогу з усіма учасниками платіжного ринку та їх асоціаціями, що на принципі рівноправності здійснюватиметься для напрацювання та обговорення пропозицій до стандарту відкритого банкінгу.

Асоціації учасників платіжного ринку, самі учасники, експерти можуть надавати пропозиції щодо принципів, основ, порядку, особливостей функціонування відкритого банкінгу, відповідності усталених на ринку бізнес-процесів до нормативно-правових актів, та пропозицій стосовно їх удосконалення.

Згідно із встановленими законодавством функціями НБУ визначатиме основні засади роботи відкритого банкінгу та напрями його подальшого розвитку відповідно до актуальних чи майбутніх потреб ринку, а також забезпечуватиме нормативно-правове регулювання правил роботи відкритого банкінгу та нагляд за дотриманням надавачами платіжних послуг вимог такого регулювання.

Технічні специфікації затверджуватимуться НБУ на основі спільних напрацювань.

Розділ 4. Екосистема відкритого банкінгу

Екосистема відкритого банкінгу – сукупність регулятора, учасників платіжного ринку, правил їх взаємодії, затверджених нормативно-правових актів НБУ, та IT-інфраструктури надавачів платіжних послуг.

Учасниками відкритого банкінгу є користувачі, Емітенти, ASPSP, PISP, AISP, hub.

Користувачі є головними бенефіціарами екосистеми відкритого банкінгу, які мають виключне право на надання згоди щодо доступу стороннім надавачам платіжних послуг до своїх рахунків або конкретного обсягу інформації за рахунками.

ASPSP надають стороннім надавачам платіжних послуг можливість взаємодіяти зі своїми системами (зокрема обмінюватися даним) через API.

Надавачі нефінансових платіжних послуг можуть залучати до співпраці треті сторони з метою надання ними послуг користувачу (див. додаток 5). Правила роботи з третіми сторонами розроблятимуться в межах відкритого НБУ проєкту щодо впровадження відкритого банкінгу.

Взаємодія учасників відкритого банкінгу повинна ґрунтуватися на принципах взаємної вигоди, недискримінації, урахування інтересів усіх сторін, що призводить до задоволення потреб користувачів.

4.1. Авторизація діяльності надавачів платіжних послуг

Авторизація діяльності надавачів платіжних послуг здійснюється відповідно до Законів України “Про платіжні послуги”, “Про фінансові послуги та державне регулювання ринків фінансових послуг[1]”, а також передбачених цими законами нормативно-правових актів НБУ.

Підтвердженням успішної авторизації діяльності надавача платіжних послуг є включення інформації щодо нього до Реєстру. Відомості, що містяться в Реєстрі, є відкритими і загальнодоступними. НБУ оприлюднює відомості з Реєстру в установленому ним порядку. Доступ до Реєстру є безкоштовним.

Для проходження авторизації ASPSP та Емітент мають отримати відповідну ліцензію.

Надавачі нефінансових платіжних послуг можуть суміщати діяльність як PISP та AISP.

Банки, платіжні установи, установи електронних грошей та філії іноземних платіжних установ мають виключне право на суміщення діяльності з надання фінансових платіжних послуг з діяльністю з надання нефінансових платіжних послуг із занесенням відповідних відомостей до Реєстру.

[1] З 01 січня 2024 року втратить чинність через те, що буде введений в дію Закон України “Про фінансові послуги та фінансові компанії”.

4.2. Моделі взаємодії учасників в екосистемі відкритого банкінгу

Модель 1: за участю ASPSP, PISP,AISP, Емітента

Модель 2: за участю ASPSP, PISP, AISP, Емітента, hub

Взаємодія ASPSP, PISP, AISP та Емітента з hub здійснюється на підставі укладених між ними договорів.

Надавачі платіжних послуг можуть користуватися послугами hub для забезпечення операційних, інформаційних та технологічних функцій на підставі договорів та не повинні використовувати і зберігати для власних потреб вразливі платіжні дані користувача.

Приклади базових сценаріїв обміну даними (див. додаток 2).

Ініційовані в межах відкритого банкінгу платіжні операції здійснюються виключно з рахунку на рахунок.

Розділ 5. Підходи до побудови відкритого банкінгу

5.1. Загальні засади та вимоги до учасників екосистеми відкритого банкінгу

Розробка власних відкритих API учасниками екосистеми здійснюється відповідно до затверджених та опублікованих НБУ технічних специфікацій з урахуванням вимог щодо інформаційної безпеки та кібербезпеки. Створення технічних специфікацій API має здійснюватися згідно з урахуванням засад цієї Концепції.

Надавачі платіжних послуг зобов'язані:

ASPSP:

- у порядку, установленому НБУ, забезпечувати можливість постійного доступу в режимі реального часу до рахунків (крім кореспондентських рахунків банку та розрахункового рахунку надавача платіжних послуг) своїх користувачів стороннім надавачам платіжних послуг;
- здійснювати тарифікацію операцій за рахунком користувача на однаковому рівні як через канали дистанційного банківського обслуговування ASPSP, так і в межах відкритого банкінгу;
- надавати Емітенту підтвердження доступності коштів на рахунку платника лише з дотриманням таких умов:
  - якщо рахунок платника доступний у режимі реального часу в момент надходження запиту;
  - якщо платник надав ASPSP згоду на надання інформації на запити конкретного Емітента щодо сум ініційованих платником платіжних операцій (згода платника має надаватися перед першим запитом Емітента про підтвердження доступності коштів на рахунку платника);
  - у разі тимчасової неможливості виконувати свою діяльність та/або наявності неактивних API, на всі запити щодо API надавати інформацію про недоступність API, до якого надходить запит.

PISP/AISP/Емітент:

- ініціювати доступ до рахунків та виконання операцій лише на підставі активного статусу згоди користувача;
- щоразу під час виконання нефінансової платіжної послуги, ідентифікувати себе перед ASPSP;
- забезпечити безпечний обмін інформацією з ASPSP, платником та отримувачем лише захищеними каналами зв'язку з урахуванням вимог Закону та нормативно-правових актів НБУ;
- забезпечити недоступність індивідуальної облікової інформації користувача будь-яким іншим сторонам, крім користувача та ASPSP, у якому обслуговується рахунок користувача, та передавати її лише захищеними каналами зв'язку з урахуванням вимог Закону та нормативно-правових актів НБУ.

5.2. Принципи побудови API

Під час побудови та впровадження надавачами платіжних послуг API повинні враховуватися такі принципи:

- створення цінності – метою розроблення відкритих API є вирішення актуальних проблем та потреб користувачів на підставі аналізу користувацького досвіду;
- уніфікація та прозорість – відкриті API мають бути побудовані відповідно до єдиних правил (нормативно-правові акти та технічні специфікації), які затверджуватимуться та публікуватимуться на сайті НБУ;
- здатність до розширення – система відкритих API має забезпечувати можливість її розширення за допомогою доопрацювання наявних або створення нових API;
- безпека – розроблені API мають відповідати вимогам щодо безпеки, зокрема кібербезпеки, і має бути забезпечена доступність проведення аудиту як на етапі тестування перед впровадженням в експлуатацію, так і протягом усього періоду експлуатації;
- відкритість і недискримінація – умови доступу до API, що надаються учасниками екосистеми відкритого банкінгу, повинні бути однаковими для будь-якого учасника, не повинні створювати жодних перешкод (як організаційних, так і технічних) для доступу або преференцій для будь-кого з учасників та такими, що не порушують законодавство про захист економічної конкуренції;
- відповідальність – вирішення спорів відбувається відповідно до законодавства України, з урахуванням прав та обов'язків учасників, керуючись інтересами користувачів.

5.3. Класифікація API

Ця Концепція передбачає два види API: базові та комерційні.

Базові API – прикладні програмні інтерфейси, які упроваджуються відповідно до Закону, їх специфікації затверджені НБУ, а забезпечення їх функціонування є обов'язковим для всіх учасників відкритого банкінгу на безоплатній основі. Учасники гарантують підтримку та доступ до базових API.

Використання базових API не потребує встановлення договірних відносин між ASPSP та сторонніми надавачами платіжних послуг.

До базових API відповідно до Закону, у межах надання послуг з ініціювання платіжної операції, надання відомостей з рахунків та підтвердження доступності коштів на рахунку, належать такі API:

для PISP:

- ініціювання разового платежу в межах України;
- ініціювання разового платежу за межі України.

для AISP:

- отримання балансу (доступні кошти) конкретного рахунку(ів);
- отримання історії трансакцій (за останні 30 діб) конкретного рахунку(ів);
- для Емітента підтвердження доступності коштів на рахунку.

API-запити для встановлення згоди користувача та взаємодії в межах використання базових API, опрацьовуються безкоштовно.

Комерційні API – програмні інтерфейси, які не належать до базових API і їх використання може відбуватися на платній основі (див. додатки 1 та 3). Правила підключення до комерційних API мають бути визначеними і опублікованими на веб-сайті ASPSP.

Розрахунки за використання комерційних API відбуваються на підставі індивідуальних договорів кожного надавача платіжних послуг з ASPSP. У разі роботи з залученням hub взаєморозрахунки відбуваються централізовано hub на підставі індивідуальних договорів з кожним надавачем платіжних послуг та ASPSP.

5.4. Функціонування API

Усі учасники, які є власниками API, зобов'язані забезпечити:

- доступність API в режимі 24/7 (цілодобову доступність); водночас операції ініціювання платежу, а також отримання даних за рахунками здійснюються відповідно до затвердженого регламенту операційного дня;
- послуги з ініціювання платіжної операції та з надання відомостей з рахунків. не надаються, якщо до рахунку користувача немає доступу в режимі реального часу; у разі технічного збою, що викликає недоступність API, інформація про факт збою та прогнозовані терміни усунення розміщується на вебсайті API;
- роботу резервного спеціалізованого інтерфейсу, який автоматично функціонуватиме в разі будь-яких проблем з основним каналом;
- доступність/актуальність/повноту документації з описом розроблених базових та комерційних API на своєму вебсайті;
- повну відповідність API, які використовуються в продуктовому режимі та в режимі тестування, які зі свого боку мають бути розділені між собою фізично та розміщені в різних інформаційних середовищах;
- відсутність жодних заборон доступу до власних API для авторизованих PISP/AISP/Емітента, крім випадків протидії реалізації кіберзагроз;
- під час обробки запитів кількох учасників відсутність випадків надання пріоритету обробці запитів окремих учасників;
- щоб час відповіді на запити під час використання API відповідав актуальним значенням згідно із затвердженими параметрами технічних регламентів.

5.5. Базові компоненти архітектури API

Показник	Значення
1	2
Архітектура API	RESTful
Стандарт обміну даними	JSON
Транспортний протокол	TLS 1.2 або вище
Електронна ідентифікація надавачів платіжних послуг	Відповідний запис у Реєстрі платіжної інфраструктури та перевірка кваліфікованого сертифіката відкритого ключа надавача
Формати повідомлень	JSON зі структурою даних на основі ISO20022

5.6. Підходи до створення ефективного користувацького досвіду (UX) у межах використання та підключення до відкритого банкінгу

Ця Концепція містить загальні принципи, яких необхідно дотримуватися під час розробки екранних форм та взаємодії користувача/PISP/AISP/ASPSP/Емітента в межах відкритого банкінгу.

PISP/AISP/ASPSP/Емітент повинен забезпечити повноту та зрозумілість інформації, яка надається в процесі обслуговування користувача.

AISP/Емітент повинен забезпечити актуальність інформації щодо наданих згод користувача під час кожного відкриття користувачем платіжного застосунку AISP/Емітента.

Користувач не повинен потребувати окремих спеціальних знань чи навичок для користування сервісами відкритого банкінгу.

Повідомлення про статус і дати трансакцій, дії користувача, мають бути чіткі та зрозумілі, тобто такі, що мають однозначне тлумачення.

Під час взаємодії AISP/PISP/Емітентом та ASPSP щодо надання відомостей з рахунків користувача та/або ініціювання платежів, та/або підтвердження доступності коштів екранні форми вебінтерфейсу або платіжного застосунку надавача платіжних послуг, що відображаються користувачу, не повинні містити зайвої інформації, зокрема реклами, інших посилань.

Інтуїтивно зрозумілий дизайн

Екранні форми ASPSP/AISP/PISP/Емітента під час надання/відкликання згоди мають надавати користувачу інформацію щодо згоди.

Мінімальна інформація, яка має бути відображена:

- найменування ASPSP/AISP/PISP/Емітента та/або їх торгова марка/комерційна торговельна марка, логотип;
- дата закінчення терміну дії згоди;
- дата й час останнього оновлення даних облікового запису користувача.

Якщо згода не була пролонгована у визначений термін або відкликана користувачем, то інформація про це вже відображається в архіві скасованих згод.

Для переходу до екрану згод користувач має здійснити не більше трьох натискань.

Максимальна прозорість

Якщо надавач платіжних послуг під час відображення інформації щодо балансу за рахунком (загальної суми доступних коштів) не здійснює розподіл між власними коштами користувача та доступним йому кредитним лімітом, то це відображення має супроводжуватись інформаційним повідомленням із попередженням про можливе списання коштів за рахунок кредитного ліміту (стягнення додаткових комісій з користувача) у разі ініціювання платіжної операції із зазначеного рахунку.

PISP у разі ініціювання платіжної операції зобов'язаний відображати розмір комісії (за наявності) ASPSP для такої послуги. Якщо такої інформації немає, то PISP відображає інформаційне повідомлення із попередженням, що ініціювання платіжної операції може призвести до стягнення комісії з користувача.

Перелік усіх активних згод користувача, про які відомо надавачу платіжних послуг, має бути відображений одночасно (на одному екрані) з можливістю переходу деталізованої інформації щодо окремої згоди (наприклад, номер рахунку, валюта, глибина виписки).

Надавач платіжних послуг має забезпечити зручний пошук у переліку активних згод користувача для користувача (наприклад, пошук, сортування, фільтр). Забороняється застосування будь-яких обмежень до користувача в разі відкликання (анулювання) згоди.

PISP/AISP може надавати користувачам можливість редагувати ім'я ASPSP, щоб його можна було замінити на псевдонім для полегшення ідентифікації користувачем своїх облікових записів.

Розділ 6. Управління згодою

ASPSP отримує від користувача через AISP/PISP/Емітента, який має договірні відносини з таким користувачем, згоду щодо:

- конкретного стороннього надавача платіжних послуг, якому він надає згоду на доступ;
- конкретного рахунку, згоду на доступ до якого він надає;
- конкретної нефінансової платіжної послуги, на яку він надає свою згоду, та конкретного обсягу інформації щодо рахунку і користувача такого рахунку.

Перед отриманням або одночасно з отриманням згоди ASPSP зобов'язаний отримати дозвіл користувача на розкриття інформації, що містить банківську таємницю, комерційну таємницю, таємницю надавача платіжних послуг. Дозвіл користувача надається через AISP/PISP/Емітента, який має договірні відносини з таким користувачем.

Під час надання згоди користувач проходить посилену автентифікацію на стороні ASPSP.

Згода може бути одноразовою або такою, яка надається на певний проміжок часу, але не більше 180 календарних днів.

Не є згодою користувача, яку ASPSP отримує від користувача, акцепт користувачем оферти договору про приєднання до умов та правил надання послуг або аналогів такого договору, реєстрація в платіжному застосунку, вебінтерфейсі або іншому програмно-технічному комплексі, що використовується відповідним надавачем платіжних послуг для забезпечення взаємодії з користувачем (далі – платіжний застосунок) PISP/AISP/Емітента.

У разі надання згоди за допомогою платіжного застосунку AISP/PISP/Емітента користувач повинен самостійно визначити обсяг інформації, до якої надається така згода (у формі явного підтвердження), не допускається підтвердження за замовчуванням. Також користувачу має бути явно доступна інформація про термін дії та умови відкликання згоди тощо.

Доступ до інформації про надані користувачем згоди має бути зафіксований як на боці AISP/PISP/Емітента, так і на боці ASPSP (в обсягах, доступних відповідному надавачу платіжних послуг), у тому числі їх платіжних застосунках.

Одна згода не повинна бути обумовлена іншою: для кожної послуги чи продукту користувач надає окрему згоду.

Користувач має змогу в будь-який час відкликати (анулювати) надану ним згоду як на боці AISP/PISP/Емітента, так і на боці ASPSP (окремо за кожним дозволом або всі дозволи одночасно), у тому числі через платіжні застосунки. Забороняється застосування будь-яких обмежень до користувача в разі відкликання (анулювання) згоди.

ASPSP повинен негайно припинити доступ до рахунків та/чи інформації, що надавалися за цією/цими згодою/згодами в разі відкликання згоди через ASPSP.

AISP/PISP/Емітент повинен негайно поінформувати про це ASPSP, який зі свого боку повинен негайно припинити доступ до рахунків та/чи інформації, що надавався за цією/цими згодою/згодами в разі відкликання згоди через AISP/PISP/Емітента.

Користувач отримує підтвердження про відкликання згоди від відповідного ASPSP. Наявність оновленого статусу згоди в платіжному застосунку ASPSP є достатнім для підтвердження факту інформування.

ASPSP/AISP/PISP/Емітент для кожної згоди повинен використовувати лише одну з таких позначок статусу згоди:

- активна – згода підтверджена користувачем та є чинною;
- прострочена – строк дії згоди закінчився;
- відкликана – згода відкликана (анульована) користувачем.

Відкликані (анульовані) згоди та згоди, за якими прострочений термін дії, вважаються не чинними, відповідно ASPSP не має підстав надавати будь-яку інформацію, передбачену такими згодами.

PISP/AISP/Емітенту рекомендовано не пізніше ніж за сім днів до закінчення строку дії згоди інформувати користувача щодо можливості продовження згоди.

Розділ 7. Безпека

Оскільки завдяки впровадженню відкритого банкінгу сторонні надавачі платіжних послуг отримують через API доступ до даних рахунків користувачів та матимуть змогу ініціювати платежі від їх імені, підвищуються вимоги до безпеки таких платежів, а вразливі платіжні дані користувачів потребують додаткового захисту від несанкціонованого доступу.

Для надавачів платіжних послуг необхідні засоби безперервного моніторингу подій, пов'язаних із взаємодією з користувачами, з метою створення та функціонування безпечного інформаційного середовища та застосування всіх необхідних заходів безпеки (відповідно до визначень Положення SCA).

7.1. Вимоги до безпеки користувачів

Платіжні послуги, що пропонуються для відкритого банкінгу, повинні надаватися з використанням технологій, здатних гарантувати безпечну автентифікацію користувача та мінімізувати ймовірність шахрайства.

Електронна взаємодія між надавачами платіжних послуг та користувачем, має здійснюватися лише після автентифікації користувача платіжних послуг.

Процедура автентифікації повинна включати механізми моніторингу спроб та способів несанкціонованого використання вразливих платіжних даних відповідно до вимог НБУ, що визначені в Положенні SCA.

Інформація про всі дії, що здійснюються особою в платіжному застосунку (як під час автентифікації, так і в разі подальшої взаємодії з надавачем платіжних послуг) має зберігатися надавачем платіжних послуг для можливості використання такої інформації під час розслідування кіберінцидентів.

7.2. Посилена автентифікація користувачів

Вимоги щодо проведення автентифікації користувачів, а також випадки, коли необхідно застосовувати посилену автентифікацію, зазначені в статті 68 Закону та Положенні SCA.

Порядок застосування посиленої автентифікації, а також визначення випадків, коли надавачі платіжних послуг мають право не вимагати застосування посиленої автентифікації користувача, зазначені в Положенні.

Винятки щодо посиленої автентифікації коли надавачі платіжних послуг мають право не вимагати застосування посиленої автентифікації користувача, зазначені в Положенні SCA.

7.2.1. Методи автентифікації користувачів

ASPSP під час отримання запиту на автентифікацію користувача через AISP/PISP/Емітента повинен застосовувати методи, що зазначені нижче та в додатку 4, і відповідати вимогам Положення SCA.

ASPSP має оптимізувати процес автентифікації з урахуванням потреби та достатності засобів захисту.

Методи автентифікації:

- автентифікація на підставі перенаправлення;
- відокремлена автентифікація;
- вбудована автентифікація.

У цій Концепції зазначені поширені методи автентифікації, детальний опис яких наведено в додатку 4. Надалі остаточний перелік методів автентифікації визначатиметься за результатами їх детального аналізу та відображатиметься в розробленому Порядку роботи відкритого банкінгу.

7.3. Вимоги до безпеки взаємодії AISP/PISP/Емітента та ASPSP

7.3.1. Основні вимоги до автентифікації надавачів платіжних послуг

Перед початком взаємодії ASPSP повинен провести автентифікацію PISP/AISP/Емітента, тобто встановити наявність права такого PISP/AISP/Емітента надавати відповідні платіжні послуги.

Автентифікація PISP/AISP/Емітента перед ASPSP здійснюється за допомогою використання кваліфікованих сертифікатів відкритих ключів відповідно до Положення SCA.

Вимоги до формування кваліфікованих сертифікатів відкритих ключів під час електронної взаємодії між AISP/PISP/Емітентами та ASPSP визначаються нормативно-правовим актом НБУ щодо порядку надання та використання електронних довірчих послуг банками, іншими особами, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює НБУ, операторами платіжних систем та/або учасниками платіжних систем, технологічними операторами платіжних послуг.

Для того щоб AISP/PISP/Емітент були впевнені, що звертаються до API відповідного ASPSP, він має забезпечити проведення взаємної автентифікації. Взаємна автентифікація має бути проведена з використанням протоколу шифрування mTLS.

Для забезпечення безпеки обміну даними між надавачами платіжних послуг через API потрібно використовувати протокол захисту транспортного рівня TLS версії 1.2 або вище.

7.3.2. Вимоги до захисту під час обміну даними між PISP/AISP/Емітентом та ASPSP

Для забезпечення конфіденційності обміну даними між PISP/AISP/Емітентом та ASPSP мають бути здійснені потрібні заходи та впроваджені відповідні стандарти інформаційної взаємодії та кібербезпеки, а також має бути забезпечена відповідність вимогам нормативно-правового акта НБУ, яким встановлені вимоги до автентифікації та застосування посиленої автентифікації на ринку платіжних послуг.

Мають також враховуватися всі вимоги інших нормативно-правових актів НБУ та відповідного законодавства України в частині захисту комунікацій для всіх учасників відкритого банкінгу.

7.3.3. Адміністрування доступу до рахунку користувача

Перед наданням сторонньому надавачу платіжних послуг доступу до рахунку користувача, ASPSP зобов'язаний перевірити авторизацію діяльності такого стороннього надавача платіжних послуг щодо відповідної платіжної послуги в порядку, установленому НБУ, зокрема, через перевірку відомостей в Реєстрі та/ або перевірку кваліфікованого сертифіката відкритого ключа.

ASPSP заборонено надавати доступ до рахунку користувача стороннім надавачам платіжних послуг, які не пройшли перевірку відомостей в Реєстрі та/ або перевірку кваліфікованого сертифіката відкритого ключа. ASPSP несе відповідальність за шкоду, заподіяну користувачу в разі недотримання ним умов надання доступу до рахунку, відповідно до законодавства.

Розділ 8. Вимоги до технічного опису та порталу для розробників

ASPSP на власному вебсайті має опублікувати окремий розділ щодо забезпечення взаємодії у відкритому банкінгу.

Інформація, розміщена в такому розділі, доступна безоплатно та не обмежено за колом осіб та має включати принаймні такі дані:

- перелік відкритих та комерційних API, до яких надає доступ ASPSP;

- документація щодо технічних характеристик усіх доступних API, із зазначенням процедур, протоколів та інструментів, потрібних AISP/PISP/Емітенту для організації взаємодії;
- опис тестового середовища, що може використовуватись AISP/PISP/Емітентом для перевірки результатів обробки запитів;
- способи звернення до служби підтримки ASPSP щодо питань взаємодії з API.

Відповідна інформація має підтримуватися в актуальному стані.

Розділ 9. Моніторинг API

ASPSP зобов'язані здійснювати моніторинг доступності та ефективності API.

Якщо API ASPSP не доступно для AISP/PISP/Емітента, такий факт має бути належним чином зафіксовано в операційній системі AISP/PISP/Емітента та є підставою для звернення AISP/PISP/Емітента до ASPSP/НБУ відповідно до нормативно-правових актів НБУ.

Надавачі платіжних послуг зобов'язані публікувати на своєму вебсайті щоквартальну статистику щодо порушень доступності та ефективності API.

Здійснення моніторингу API є зоною відповідальності як ASPSP, так і PISP, Емітенту.

Для проведення моніторингу доступності надавач платіжних послуг повинен збирати дані за такими параметрами (перелік не вичерпний):

- кількість отриманих запитів;
- кількість запитів із технічною помилкою;
- кількість запитів, у яких вичерпано термін очікування та не отримано відповідей;
- середній час відповіді на запит.

Для проведення моніторингу ефективності надавач платіжних послуг повинен збирати дані за такими параметрами (перелік не вичерпний):

- кількість користувачів;
- кількість активних згод;
- кількість відкликаних згод;
- кількість запитів до API;
- обсяг запитів на ініціювання платіжної операції.

Розділ 10. Захист даних та прав користувачів

Під час обслуговування користувача у відкритому банкінгу застосовуються аналогічні механізми захисту даних користувачів, як і під час надання інших платіжних послуг.

Дані користувача, платіжні дані, інформація щодо покупок користувача − повинні бути захищені надавачами платіжних послуг відповідно до нормативно-правових актів НБУ.

Користувач має право надати згоду на визначений строк, відкликати та обмежити доступ до рахунку відповідно до розділу 6 цієї Концепції.

Відкликання згоди можливо через ASPSP або AISP/PISP/Емітента.

Учасники платіжного ринку зобов'язані розробити внутрішні механізми вирішення звернень (скарг) користувача з визначеними ролями та обов'язками, мати достатньо каналів для подання заяв (повідомлень), уключаючи як фізичні, так і цифрові та, які є легкодоступні для користувача. Заява (повідомлення) користувача щодо спірних питань подається ASPSP та опрацьовується надавачем платіжних послуг відповідно до нормативно-правових актів щодо розгляду звернень користувача.

Розділ 11. Управління ризиками

Відкритий банкінг сприяє впровадженню інновацій в сфері платіжних послуг, розширює наявні та створює нові продукти та послуги, забезпечуючи обмін даними користувачів і взаємозв'язок систем, що потребує від учасників платіжного ринку створення системи управління операційними ризиками, кіберризиками та ризиками безпеки, пов'язаними з наданням платіжних послуг (виконанням платіжних операцій), комплаєнс-ризиком, зокрема ризиком легалізації (відмиванню) коштів, регуляторним ризиком тощо.

Надавачі платіжних послуг повинні знати про потенційні ризики та вживати відповідних заходів для їх пом'якшення. Це включає впровадження суворих заходів безпеки та конфіденційності, дотримання нормативних вимог, проведення ретельної перевірки сторонніх надавачів платіжних послуг, а також забезпечення навчання та обізнаності користувачів щодо ризиків і переваг відкритого банкінгу.

Потенційними, визначеними на цей час, видами ризиків у межах відкритого банкінгу є:

Ризики щодо конфіденційності та безпеки даних: є ризик несанкціонованого доступу, витоку даних або неправомірного використання даних користувачів, якщо не вжито таких належних заходів безпеки, як шифрування, автентифікація та керування згодою.

Шахрайство та ризики кібербезпеки: інформаційні системи надавачів платіжних послуг можуть бути вразливими до шахрайства та кібератак, таких як фішинг, зловмисне програмне забезпечення або атаки соціальної інженерії. Несанкціонований доступ до облікових записів користувачів, шахрайські трансакції або маніпулювання даними можуть створювати ризики як для користувачів, так і для надавачів платіжних послуг.

Регуляторні ризики та ризики відповідності: відкритий банкінг регулюється вимогами законодавства України та нормативно-правовими актами НБУ, зокрема щодо захисту даних, управління згодою та протидії відмиванню грошей (AML).

Операційні та технічні ризики: технічні збої, операційні помилки можуть призвести до перерв в обслуговуванні або втрати довіри користувачів.

Розділ 12. Відповідальність надавачів платіжних послуг

ASPSP несе відповідальність згідно із законодавством України та відповідно до умов укладених договорів з користувачами. У межах відкритого банкінгу надавачу платіжних послуг з обслуговування рахунку заборонено надавати доступ до рахунків користувачів стороннім надавачам платіжних послуг у разі невиконання/невідповідності умов надання доступу, визначених Законом.

ASPSP несе відповідальність за шкоду, заподіяну користувачу в разі недотримання ASPSP умов надання доступу до рахунку, відповідно до законодавства України.

ASPSP несе визначену Законом відповідальність перед користувачами за невиконання або неналежне виконання платіжних операцій, ініційованих через PISP.

У разі виникнення спірного питання щодо операції ASPSP несе відповідальність за несвоєчасне надання відповіді користувачу платіжних послуг та взаємодіє з учасником платіжного ринку (PISP або AISP), який зобов'язаний довести та обґрунтувати правомірність операції.

Надавачі нефінансових платіжних послуг зобов'язані страхувати свою відповідальність перед користувачами та ASPSP у порядку, що встановлюється нормативно-правовими актами НБУ.

PISP у разі невиконання або неналежного виконання послуги ініціювання платіжної операції з його вини, зобов'язаний відшкодувати ASPSP на вимогу останнього всі понесені збитки та суми, відшкодовані користувачам.

Надавачі платіжних послуг зобов'язані здійснювати контроль та несуть відповідальність за дотримання hub умов та порядку надання відповідних послуг надавачу платіжних послуг згідно з укладеними між ними договорами. З огляду на це надавачі платіжних послуг зобов'язані здійснювати контроль за наявністю відповідного статусу hub перед укладанням із ними договорів.

У разі залучення надавачем платіжних послуг третьої особи до виконання операційних функцій надавач платіжних послуг несе відповідальність перед користувачем за надання платіжної послуги чи виконання платіжної операції. Відносини та зобов'язання надавача платіжних послуг щодо користувачів у разі залучення третьої особи до виконання операційних функцій залишаються незмінними.

Розділ 13. Дорожня карта впровадження відкритого банкінгу

Завдання проєкту:	Термін виконання	Відповідальні
Розроблена перша версія технічних специфікацій	IV кв. 2023	Робочі групи та НБУ
Перша версія специфікацій погоджена зі сторони НБУ для тестування	IV кв. 2023	НБУ
Підготовка та проведення першого етапу тестування обмеженого набору API	II кв. 2024	Робочі групи та НБУ
Аналіз першого етапу тестування, визначення зон доопрацювання специфікацій, доопрацювання та розроблення другої версії технічних специфікацій	II -й кв. 2024	Робочі групи та НБУ
Підготовка та проведення другого етапу тестування API з розширенням набору API та учасників, підготовлена друга версія специфікацій	III -й кв. 2024	Робочі групи та НБУ
Сформовані вимоги зацікавлених сторін: загальні підходи до здійснення нагляду та захисту прав користувачів, IT-безпеки, захисту персональних даних користувачів	I кв. 2024	НБУ
Аналіз переліку НПА: сформовано перелік НПА та концептуальні зміни; визначено правову базу для пілотування	I кв. 2024	НБУ
Затверджено нормативно-правові акти з авторизації, доопрацьовано реєстр платіжної інфраструктури	IV кв. 2024	НБУ
Затверджено нормативно-правові акти. Порядок роботи відкритого банкінгу та технічні специфікації, інші нормативно-правові акти	IV кв. 2024	НБУ
Проведено пілот на продуктивному середовищі обмеженим колом учасників	III кв. 2025	Робочі групи та НБУ
Проведення заходів з підвищення фінансової грамотності користувачів	III кв. 2025	Робочі групи та НБУ
Закриття проєкту 01.08.2025	III кв. 2025	Робочі групи та НБУ

Додаток 1

Приклади комерційних API

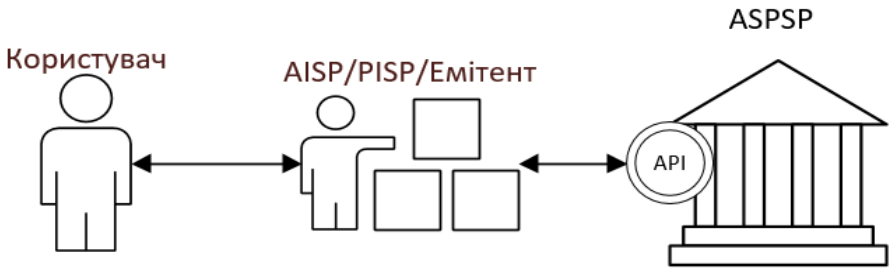
Назва	Тип
Ініціювання регулярного платежу	Комерційне
Отримання атрибутів (дата відкриття, IBAN) рахунків за запитом	Комерційне
Отримання інформації щодо розподілу трансакцій відповідно до місця проведення операції: за певний період (більше 30 днів),за конкретним рахунком, за запитом	Комерційне
Отримання переліку рахунків із залишком на рахунку на певну дату	Комерційне
Отримання детальної інформації щодо трансакції за запитом (використовуватиметься transaction ID)	Комерційне
Отримання повної інформації про трансакції за визначеним рахунком	Комерційне
Отримання повної інформації про трансакції за всіма рахунками	Комерційне
Отримання моніторингового нагадування зміни балансу за визначеним рахунком	Комерційне
Інформаційне повідомлення щодо здійснення певного типу/суми трансакцій за визначеними рахунками	Комерційне
Отримання моніторингового нагадування про зміни в списку рахунків клієнта	Комерційне

Додаток 2

Приклади базових сценаріїв обміну даними (інформаційні потоки)

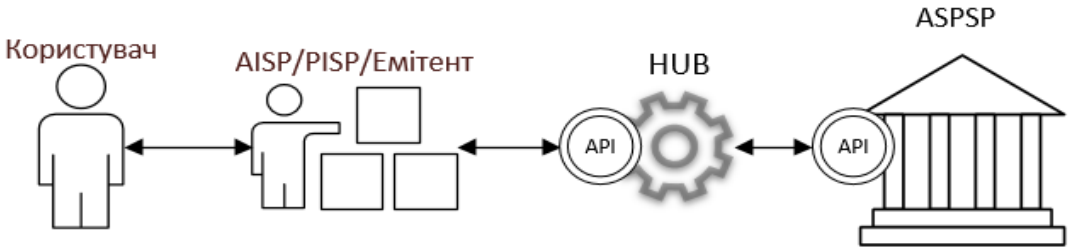
1. Надання відомостей з рахунків, ініціювання переказів, підтвердження доступності коштів на рахунку відбувається за такими сценаріями:

1.1. Користувач – платіжний застосунок AISP/PISP/Емітент – ASPSP



У цьому прикладі AISP/PISP/Емітент звертається через API безпосередньо до ASPSP. AISP/PISP/Емітент має налаштовувати з'єднання з кожним ASPSP окремо.

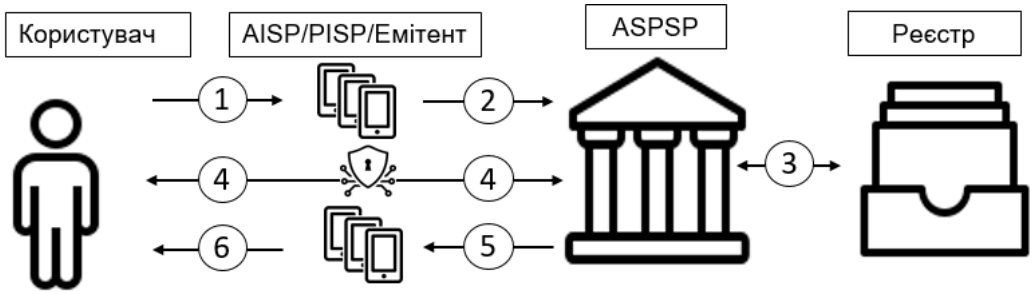
1.2. Користувач – платіжний застосунок AISP/PISP/Емітент – hub – ASPSP



У цьому прикладі AISP/PISP/Емітент звертається до ASPSP через hub. AISP/PISP/Емітент налаштовує технічне з'єднання тільки з hub, який зі свого боку має налаштувати з'єднання з відповідними ASPSP.

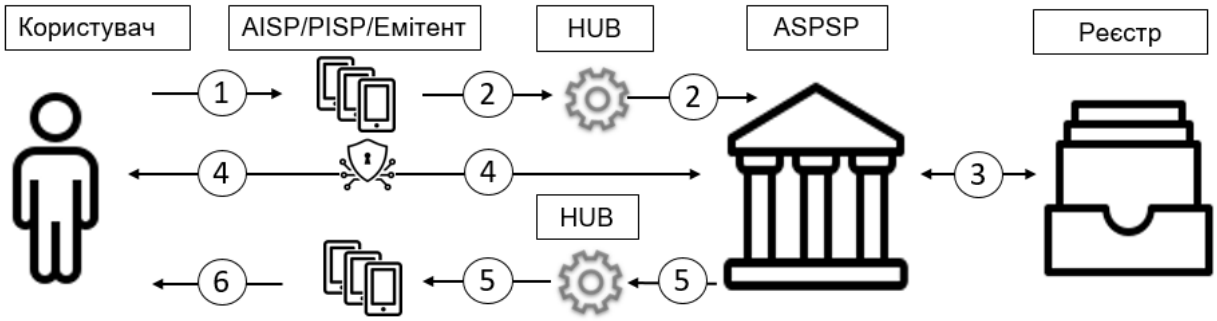
2. Відображення процесу перевірки стороннього надавача послуг у Реєстрі та проходження користувачем посиленої автентифікації під час надання відомостей з рахунку, ініціювання переказів, підтвердження доступності коштів на рахунку:

2.1.Схема без використання hub



1. Користувач ініціює операцію в платіжному застосунку AISP/PISP/Емітента.
2. AISP/PISP/Емітент надсилає запит користувача через API до ASPSP.
3. ASPSP перевіряє інформацію щодо AISP/PISP/Емітента у Реєстрі.
4. Користувач проходить посилену автентифікацію в ASPSP.
5. ASPSP через API повертає інформацію або результат виконання операції.
6. AISP/PISP/Емітент інформує користувача про результати виконання операції.

2.2. Схема з використанням hub



1. Користувач ініціює операцію в AISP/PISP.
2. AISP/PISP/Емітент надсилає запит користувача до ASPSP, використовуючи API, який надає hub, тобто спочатку запит йде до hub, а потім перенаправляється до ASPSP, відповідно до його API.
3. ASPSP перевіряє інформацію щодо AISP/PISP/Емітента в Реєстрі НБУ.
4. Користувач проходить посилену автентифікацію в додатку ASPSP.
5. ASPSP через своє API повертає інформацію або результат виконання операції до hub, який перенаправляє відповідь до AISP/PISP/Емітента.
6. AISP/PISP/Емітент інформує клієнта про результати виконання операції.

Додаток 3

Приклади послуг та продуктів в ЄС на базі API

Назва	Опис
Агрегація облікових записів	Дає змогу підключити та об'єднати усі банківські рахунки на одній платформі, аналізувати та сортувати інформацію за ними, контролювати трансакції та залишки
Управління особистими фінансами	Планування витрат, встановлення бюджетів у розрізі категорій, розумні заощадження, рекомендації "фінансового радника" в додатку щодо оптимізації витрат
Автоматизовані витрати	Налаштування регулярних платежів чи переказів із рахунків (таких як оплата комунальних платежів, «кишенькові» гроші дітям, сплата податків тощо)
Автоматична економія	Налаштування цілей для накопичення та заощадження у власному темпі
Поповнення	Встановлення правил автоматичного поповнення рахунку у разі досягнення визначеної суми залишку або наближення до використання кредитного ліміту
Управління згодами	Облік наданих згод користувача з метою контролю терміну їх дії чи відкликання за потреби
Кредитний скоринг	Швидке прийняття рішення про кредитування, завдяки формуванню портрета користувача, аналізу надходжень та витрат за його рахунками, історії трансакцій, оцінка платоспроможності. Налаштування умов кредитування та розміру відсоткової ставки відповідно до виявленого рівня ризику за користувачем. Перевірка, чи вчасно користувач виконує зобов'язання, такі як оплата орендних чи комунальних платежів
Знай свого клієнта	Миттєвий онбординг користувача, завдяки отриманню його даних та документів з установи, у якій він проходив ідентифікацію раніше
Моніторинг трансакцій	На підставі профіля користувача – виявлення нетипових для нього дій чи операцій з метою запобігання шахрайству
Верифікація власника рахунку	Підтвердження того, що рахунок належить отримувачу у разі відправки платежу, надання кредиту
Профіль споживчих витрат	Користувач може дозволити збирати інформацію про трансакції які він здійснює, їх періодичність та інше, отримуючи за це певні виплати. Інформація щодо профілю витрат використовується для визначення користувацького попиту на певні товари, таргетованої реклами, поліпшення сервісу тощо
Програма лояльності	Інструмент для формування профілю користувача на підставі його витрат (які бренди подобаються, яким мережам надає перевагу), нарахування балів чи виплата винагороди як заохочення. Наприклад, кешбек, якщо користувач надає перевагу покупкам у компаніях з високим рівнем соціальної відповідальності.

	Можливість відслідковування важливих дат, подій користувача та надання йому спеціальних пропозицій
Оплата в кредит	Вибір опції “оплата частинами” під час здійснення покупки. Завдяки відкритим даним здійснюється перевірка кредитоспроможності користувача та рішення приймається миттєво. Надалі платежі користувач або вносить самостійно, або налаштовує автоматичне списання з рахунку
Підтвердження коштів	Автоматичне підтвердження доступності коштів на рахунку для здійснення миттєвих платежів онлайн без додаткових комісій
Електронна комерція	Інтеграція нових методів оплати з рахунку за ініціативи користувача або третьою стороною, якій надана згода користувача щодо інтернет-торгівлі
Обмін валют	Можливість конвертувати кошти в інші валюти (у тому числі купувати криптовалюту на біржах) із миттєвим зарахування на рахунок чи гаманець
Поповнення рахунку	Зовнішній платіж із метою поповнення рахунку безпосередньо в додатку банку, рахунок якого поповнюється
Бухгалтерські послуги	Автоматичне ведення бухгалтерії для підприємства, формування та подання звітності
Управління діяльністю	Інтеграція з рахунками компанії на одній платформі для контролю всіх надходжень та витрат, своєчасної сплати податків та інших зобов’язань, платежів за договорами, рахунків-фактур
Бізнес аналітика	Фінансовий радник аналізує грошові потоки компанії в динаміці та надає рекомендації щодо підвищення ефективності її діяльності. Може містити інструменти для планування та побудови прогнозів, формування різних сценаріїв розвитку подій, ураховуючи макроекономічні чинники тощо

Додаток 4

Методи автентифікації користувачів

1. Автентифікація на підставі перенаправлення

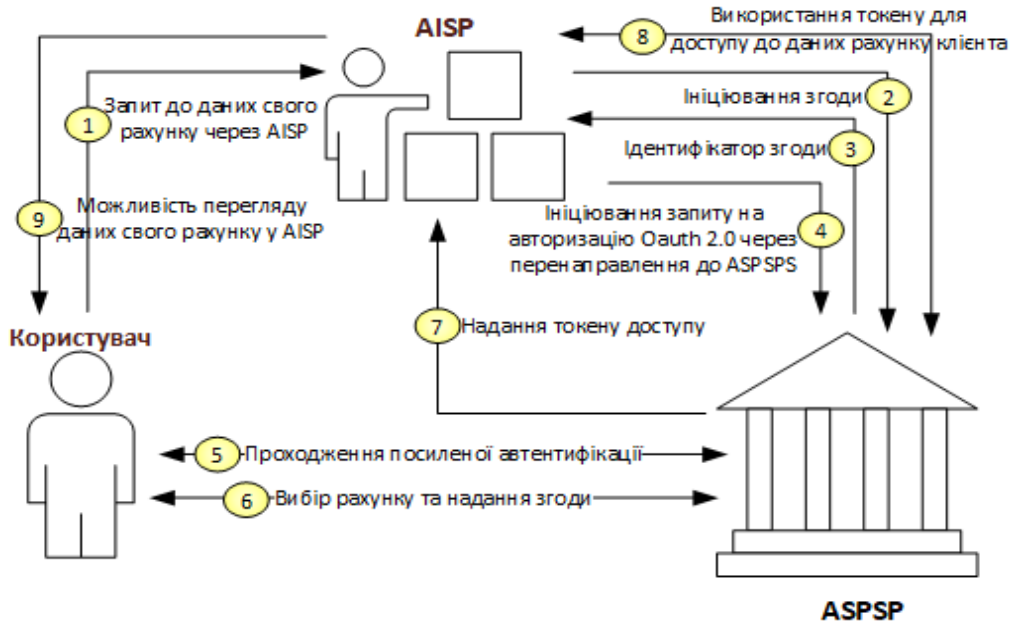
Цей метод виконується шляхом перенаправлення користувача з вебсторінки або платіжного застосунку AISP/PISP/Емітента до вебсторінки або платіжного застосунку ASPSP, де користувач проходить процес посиленої автентифікації, після чого відбувається повернення до платіжного застосунку AISP/PISP/Емітента. Усі кроки процесу мають виконуватися в межах одного пристрою.

Використання OAuth 2.0. Одним із варіантів перенаправлення може бути використання протоколу OAuth 2.0, що дає змогу користувачу надати доступ стороннім надавачам платіжних послуг так, щоб вони діяли від його імені.

Протокол позбавляє необхідності передавати сервісу логін і пароль, а також дає змогу надавати визначений набір прав, а не всі відразу.

Для впровадження OAuth 2.0 у відкритому банкінгу рекомендується використовувати відкритий стандарт децентралізованої системи автентифікації OpenID Connect, що дає користувачеві можливість використовувати єдиний обліковий запис для автентифікації на безлічі не пов'язаних один з одним інтернет-ресурсів. OpenID Connect створено на підставі специфікацій сімейства OAuth 2.0 з використанням спрощених потоків повідомлень REST/JSON.

Приклад схеми робочого процесу надання доступу до рахунку для AISP з використанням OAuth 2.0 та посиленої автентифікації



1. Користувач створює запит до відомостей свого рахунку через AISP.

2. AISP надсилає запит до ASPSP з ініціюванням згоди.

3. ASPSP надсилає AISP унікальний ідентифікатор згоди.

4. AISP ініціює запит на авторизацію OAuth 2.0, що містить ідентифікатор згоди, перенаправляючи користувача до ASPSP.

5. Користувач проходить посилену автентифікацію на стороні ASPSP.

6. Користувач обирає відповідний рахунок та надає згоду на доступ до його відомостей для AISP.

7. ASPSP надає AISP токен доступу.

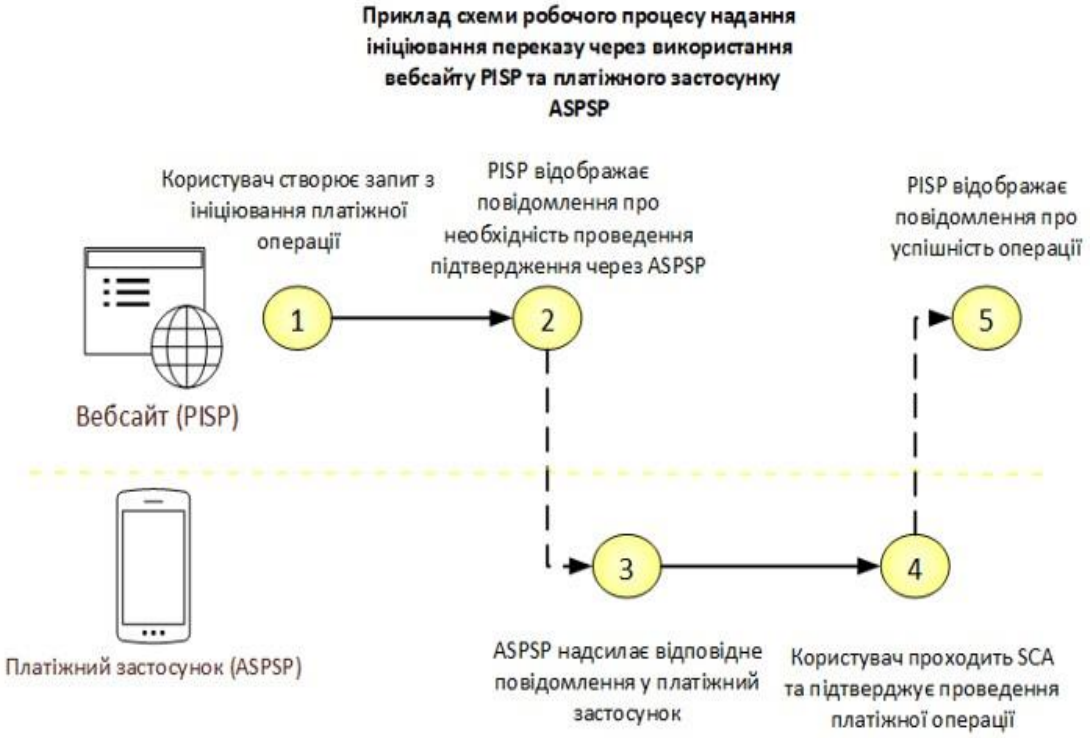
8. Використовуючи цей токен, AISP може отримувати відомості з рахунку користувача в ASPSP відповідно до раніше наданої згоди.

9. Користувач відтепер має доступ до відомостей свого рахунку через AISP.

2. Відокремлена автентифікація

Із цим методом автентифікація відбувається за межами прямої взаємодії між платіжними застосунками або вебсторінками AISP/PISP/Емітенту та ASPSP. Під час автентифікації можна використовувати будь-які пристрої, через які користувач взаємодіє з ASPSP, якщо це не протирічить політиці безпеки ASPSP. За допомогою відокремленої автентифікації ASPSP може автентифікувати користувача за допомогою іншого каналу, наприклад:

- використання статичного ідентифікатора користувача (комбінація певних знань про користувача, наприклад, його власне ім'я та пароль, що однозначно ідентифікують користувача). Користувач надає статичний ідентифікатор до AIPS/PISP/Емітенту, який потім передається до відповідного ASPSP для ідентифікації цього користувача в платіжному застосунку цього ASPSP;
- використання динамічного ідентифікатора (додаткова інформація про користувача, що формується динамічно та відображає його володіння додатковими ознаками – наприклад, одноразовий пароль в SMS або в платіжному застосунку) від ASPSP, який користувач передає до AISP/PISP/Емітенту для підтвердження автентифікації в ASPSP;
- використання динамічного ідентифікатора від AISP/PISP/Емітенту, який користувач передає ASPSP для підтвердження автентифікації.



1. Користувач створює запит з ініціювання платіжної операції через вебсайт PISP.

2. PISP надсилає відповідний запит до ASPSP та відображає повідомлення про потребу проведення підтвердження операції через ASPSP.

3. ASPSP надсилає повідомлення про потребу підтвердження операції в платіжний застосунок, встановлений у користувача.

4. Користувач проходить посилену автентифікацію в платіжному застосунку ASPSP і підтверджує проведення операції.

5. ASPSP проводить операцію та надсилає до PISP відповідь на запит з інформацією про успішність проведення операції, після чого PISP повідомляє про це користувача.

3. Вбудована автентифікація

З використанням цього методу користувачу надається можливість у платіжному застосунку AIPS/PISP/Емітента напряму через API виконати процедуру автентифікації до відповідного ASPSP без застосування перенаправлення або відокремленої автентифікації.

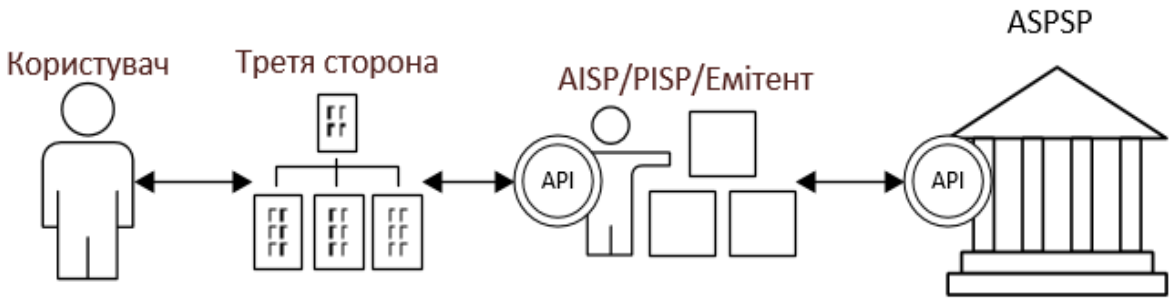
У цьому разі AIPS/PISP/Емітенти матимуть доступ до даних користувача, що використовуються під час автентифікації до ASPSP, що створює додаткову відповідальність для AIPS/PISP/Емітента.

Додаток 5

Приклади базових сценаріїв обміну даними (інформаційні потоки)

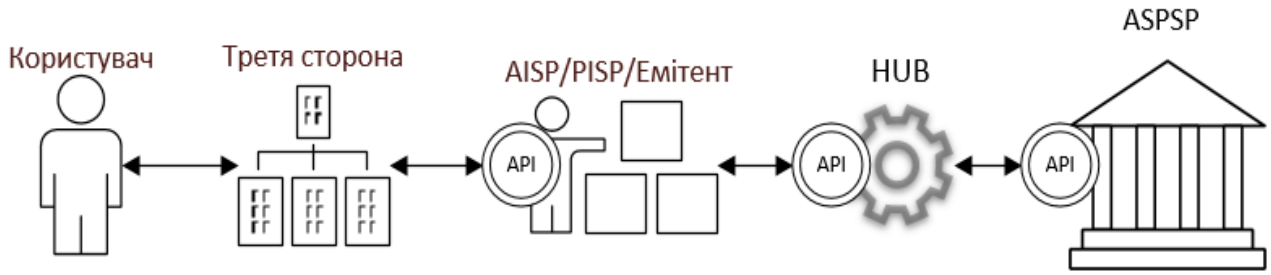
Приклади екосистеми із залученням третьої сторони

1. Користувач – платіжний застосунок третьої сторони − AISP/PISP/Емітент − ASPSP



У цьому разі користувач використовує платіжний застосунок третьої сторони, що взаємодіє з ASPSP від імені відповідного AISP/PISP/Емітента.

2. Користувач – платіжний застосунок третьої сторони − AISP/PISP/Емітент – HUB − ASPSP



Під час залучення третіх сторін AISP/PISP/Емітент може взаємодіяти з відповідними ASPSP через hub.