DOI https://doi.org/10.30525/978-9934-26-424-5-21

ПРАВОВЕ РЕГУЛЮВАННЯ ВІДКРИТОГО БАНКІНГУ У ПРОЦЕСІ ТРАНСФОРМАЦІЇ УКРАЇНСЬКОГО БАНКІВСЬКОГО СЕКТОРУ

Сергієнко А. С.

ВСТУП

Банківський сектор є осердям економічного життя будь-якої країни, оскільки вможливлює належне функціонування фінансової системи, а отже має забезпечуватись ефективним юридичним механізмом. На сьогодні відкритий банкінг – один із ключових інноваційних трендів, які трансформують світову фінансову систему. Тому відкритий банкінг – одна з найбільш обговорюваних тем у фінансовому світі, яка зачіпає споживачів, банки та різні фінтех-компанії, що значно актуалізує тематику дослідження.

Україна не є винятком: у серпні 2023 року Національний банк України затвердив Концепцію відкритого банкінгу, яка визначає «напрями розвитку, дорожню карту та ключові вимоги до впровадження в Україні відкритого банкінгу». На практиці норми мають запрацювати з серпня 2025 року. У цьому розділі розглядається концепція відкритого банкінгу, його переваги та недоліки, перспективи та ризики впровадження в Україні у контексті євроінтеграційних процесів.

Відкритий банкінг – це концепція, яка передбачає вільний обмін фінансовою інформацією між різними фінансовими установами, включно з банками, фінтех-компаніями й іншими провайдерами. На практиці відкритий банкінг надає стороннім провайдерам доступ до фінансових даних споживачів із банків і фінансових установ через інтерфейси прикладного програмування (API). При цьому, споживачі отримують більше контролю над власними фінансами та можливість надавати доступ до власної фінансової інформації, а також одночасно можуть користуватися послугами різних провайдерів у зручному для себе форматі.

1. Теоретико-методологічні аспекти правового регулювання відкритого банкінгу

Це дослідження спиратиметься на роботи вчених, які вже пропрацьовували подібну тематику, таких як: Довгань Ж. М.[1], Єсіна О. Г.[2], Заславська О. І.[3], Охрименко І. Б.[4] й інших.

[1] Довгань, Ж. М., Галіцейська, Ю. М. (2021). Open-банкінг як тренд розвитку фінансових технологій. *Інноваційна економіка*. 5–6’2021 [88]. С. 111–116.

[2] Єсіна, О. Г. (2023). Розвиток цифрових фінансових технологій у банківській сфері. *Проблеми сучасних трансформацій. Серія: економіка та управління*. 7.

Початком відкритого банкінгу у Європейському Союзі зазвичай уважають пілотний проєкт з упровадження онлайн-банкінгу, який проведений Федеральною поштою Німеччини 1980 року. У рамках зазначеного проєкту 300 провайдерів і близько 2000 фізичних осіб змогли протестувати нові банківські послуги у режимі онлайн. Учасники могли здійснювати грошові перекази через Інтернет, використовуючи номер *300# – інноваційне рішення 1980-х років, яке проклало шлях до банківського самообслуговування в усьому світі. Тільки декілька господарств у підсумку перейшли на цю систему, проте, інтерфейс залишався діючим до 2005 року.

Директива щодо платіжних послуг (PSD1), яка розроблена Європейською Комісією наприкінці 2007 року, сприяє розвитку конкуренції та розширення залучення банків і небанківських організацій у платіжній індустрії, зосереджуючи особливу увагу на захисті прав споживачів, а також на правах й обов'язках як постачальників, так і користувачів різних платіжних послуг[5].

У 2015 році Європейський парламент схвалив пропозицію Європейської Комісії щодо додавання до загального переліку нових правил для захисту онлайн- і мобільних платежів (PSD2)[6]. Вона набула чинності 2018 року. PSD2 відкриває банки для сторонніх провайдерів, що означає, що вони мають забезпечити інтерфейс, зазвичай шляхом створення API, який уможливлює стороннім провайдерам безпосередньо ініціювати платежі чи запити щодо рахунків. Окрім цього, PSD2 запровадила надійну автентифікацію клієнтів (SCA). Зазначена пропозиція Європейської Комісії мала значний вплив на відкритий банкінг, оскільки зробила електронні платежі безпечнішими, стимулювала інновації та сприяла зростанню у створенні програмних інтерфейсів.

Зокрема, у ній ідеться, що постійний розвиток інтегрованого внутрішнього ринку для безпечних електронних платежів має вирішальне значення для підтримки зростання економіки Європейського Союзу та

---

[3] Заславська, О. І., Петканич, М.-В. М. (2023). Цифрова трансформація банківського бізнесу в умовах розвитку фінансових технологій. *Науковий вісник Ужгородського Університету. Серія Економіка*. 2 (62). С. 116–122.

[4] Охрименко, І. Б., Шуляк, Д. А. (2023). Інновації open-banking у розвитку банкострахування. *Актуальні питання у сучасній науці*. 11 (17). С. 193–208.

[5] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC (Text with EEA relevance). European Parliament. URL: https://eur-lex.europa.eu/eli/dir/2007/64/oj (дата звернення: 09.02.2024).

[6] Consolidated text: Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance). European Parliament. URL: https://eur-lex.europa.eu/eli/dir/2015/2366/2015-12-23 (дата звернення: 09.02.2024).

забезпечення того, щоб споживачі, продавці та компанії мали можливість вибору та прозорості платіжних послуг, щоб отримати повну вигоду від внутрішнього ринку.

Отже, необхідно встановити нові правила, щоб усунути нормативні прогалини, водночас, забезпечуючи більшу правову ясність і послідовне застосування законодавчої бази в усьому Європейському Союзі. Існуючим і новим гравцям на ринку мають бути гарантовані еквівалентні умови роботи, що дозволить новим платіжним засобам вийти на більший ринок і забезпечить високий рівень захисту споживачів під час використання цих платіжних послуг по всьому Європейському Союзі в цілому. Це має підвищити ефективність платіжної системи в цілому та призвести до більшого вибору та прозорості платіжних послуг, одночасно зміцнюючи довіру споживачів до гармонізованого платіжного ринку.

Зазначається, що в останні роки ризики безпеки, які пов'язані з електронними платежами, зросли. Це пов'язано зі зростаючою технічною складністю електронних платежів, безперервним зростанням обсягів електронних платежів у всьому світі та новими видами платіжних послуг. Безпечні та надійні платіжні послуги є життєво необхідною умовою для належно функціонуючого ринку платіжних послуг. Тому користувачі платіжних послуг мають бути належним чином захищені від таких ризиків. Платіжні послуги необхідні для функціонування життєво важливих економічних і соціальних видів діяльності.

Так, Директива PSD2 щодо прозорості та вимог до інформації для надавачів платіжних послуг, а також щодо прав й обов'язків щодо надання та використання платіжних послуг також має застосовуватися, якщо це доцільно, до операцій, у яких один із надавачів платіжних послуг знаходиться за межами Європейської економічної зони, наприклад, в Україні, щоб уникнути різних підходів між країнами-членами на шкоду споживачам. У відповідних випадках зазначену директиву необхідно поширити на операції в усіх офіційних валютах між надавачами платіжних послуг, розташованими у Європейській економічній зоні.

Відкритий банкінг має значні переваги, які забезпечують підґрунтя його впровадження в усьому світі:

– сприяє підвищенню конкуренції у банківському секторі, що стимулює банки покращувати свої послуги та знижувати комісійні ставки для своїх клієнтів;

– клієнти отримують зручну можливість управляти власними фінансами через єдиний застосунок, який об'єднує дані з різних банків і фінтех-компаній;

– сприятиме розвитку та поширенню нових фінансових послуг і програмних продуктів, а саме: персоналізованих рекомендацій, управління заборгованістю й інвестиційний портфель;

– буде посилено стандарти безпеки для захисту особистих даних і транзакцій клієнтів.

Проте, у відкритого банкінгу є й окремі ризики,які необхідно враховувати під час його подальшого впровадження:

– можливість порушення конфіденційності особистих фінансових даних у випадку недотримання високих стандартів безпеки;

– із розширенням доступу до фінансових даних суттєво зростає ймовірність кіберзлочинних атак і шахрайства;

– деякі складнощі зі впровадженням відкритого банкінгу, які пов'язані з різними регуляторними вимогами тощо.

Відкритий банкінг насамперед спрямований на стимулювання інновацій у фінансовому секторі, розширення фінансової сфери, сприяння автоматизації та персоналізації обслуговування клієнтів. Цей процес не зупиняється та постійно розвивається. Згідно даних незалежної аналітичної компанії Forrester Research прогнозується, що за період з 2022 по 2027 рік використання відкритого банкінгу у країнах ЄС подвоїться[7].

В оприлюдненому звіті від 26 вересня 2023 року глобальна технологічна компанія платіжної індустрії MasterCard зазначила, що відкритий банкінг останнім часом трансформується у відкриті фінанси[8]. Так, на регуляторному рівні Європейського Союзу запропоновано Регламент щодо доступу до фінансових даних (FIDA), який виходить за рамки даних про платіжні рахунки у відкритому банкінгу й охоплює більше фінансових питань[9]. Водночас, у ньому наголошується на необхідності того, щоби будь-які фінансові установи в усіх країнах ЄС «керувалися однаковими правовою базою та технічними стандартами».

Як зазначає Європейська комісарка з фінансових послуг, фінансової стабільності та ринків капіталу Марейд Мак-Гіннесс відкриті фінанси мають забезпечити клієнтам ефективний контроль особистих даних і знання того, які дані, кому та чому передаються[10]. Одним із засобів здійснення цього контролю є створення інформаційних панелей дозволів. Це інтерфейс, який надає клієнтам простий огляд їхніх особистих даних, якими вони за бажанням можуть поділитися. За допомогою таких панелей клієнтам простіше надати чи відкликати дозвіл на обмін інформацією. Водночас, компанії, які отримують доступ до даних, мають регулюватися та контролюватися у такий спосіб, як і компанії, які зберігають ці дані.

[7] European Open Banking Forecast, 2022 To 2027. Forrester. URL: https://www.forrester.com/report/european-open-banking-forecast-2022-to-2027/RES178412 (дата звернення: 09.02.2024).

[8] Four European takes on open banking. Mastercard Data & Services. URL: https://www.mastercardservices.com/en/advisors/archived-practices/open-banking/insights/four-european-takes-open-banking (дата звернення: 09.02.2024).

[9] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a framework for Financial Data Access and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554. European Parliament. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023PC0360 (дата звернення: 09.02.2024).

[10] Keynote speech by Commissioner McGuinness at event in European Parliament "From Open Banking to Open Finance: what does the future hold?". European Commission. URL: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_23_1819 (дата звернення: 09.02.2024).

Тут також є значний потенціал у вигляді отримання клієнтами більш персоналізованих пропозицій, які краще відповідають їхнім потребам.

Закон України «Про платіжні послуги» передбачає, що в рамках відкритого банкінгу «надавачі платіжних послуг з обслуговування рахунку зобов'язані у порядку, встановленому Національним банком України, забезпечувати можливість постійного доступу в режимі реального часу до рахунків (крім кореспондентських рахунків банку та розрахункового рахунку надавача платіжних послуг) своїх користувачів банкам та іншим надавачам платіжних послуг, що отримали право на надання нефінансових платіжних послуг»[11].

Відповідно до затвердженої у 2023 році Концепції відкритого банкінгу Національний банк України має намір розробити та затвердити необхідні нормативно-правові акти для впровадження відкритого банкінгу[12]. Згідно із запропонованою дорожньою картою, першу версію технічних специфікацій має бути розроблено у четвертому кварталі 2023 року, а сам пілот має бути проведено на продуктивному середовищі обмеженою кількістю учасників у третьому кварталі 2025 року. Отже, відкритий банкінг повноцінно має запрацювати в Україні з серпня 2025 року.

Відкритий банкінг продовжує змінювати фінансову сферу, надаючи клієнтам більше можливостей і доступ до інноваційних рішень. Мобільні додатки інтернет-банкінгу стають дедалі популярнішими у користувачів. Інтерфейс прикладного програмування (API) є основним елементом відкритого банкінгу, та їхня кількість постійно зростає. Особистий фінансовий аналіз стає дедалі важливішим для користувачів. Відкритий банкінг надає можливість збирати й аналізувати дані щодо витрат, бюджетування й інвестицій, щоб допомогти клієнтам покращити керування власними фінансами.

Процес цифрової трансформації українського банківського сектору став особливо помітним в останні декілька років, оскільки був обумовлений низкою обставин:

– втратою довіри клієнтів до традиційного банківського сектору під час світової фінансової кризи 2020 року та необхідності переходу до каналів дистанційного обслуговування;

– підвищенням рівня очікувань від послуг, які надаються, зокрема, фінансових. Споживач стає дедалі більше орієнтованим на постійне оновлення та прискорення процесів, більшу доступність технологій і зручність послуг в умовах застарілості й обмеженості традиційних продуктів як за формою, так і за змістом;

– поширенням мобільного Інтернету, яке призвело до того, що фокус стратегії залучення клієнтів банку почав зміщуватися з відкриття чергового відділення на створення онлайн-сервісів і підтримку мобільної версії сайту;

[11] Про платіжні послуги : Закон України від 30.06.2021 № 1591-IX. URL: https://zakon.rada.gov.ua/laws/show/1591-20#Text (дата звернення: 09.02.2024).

[12] Затверджено Концепцію відкритого банкінгу в Україні. Національний банк України. URL: https://bank.gov.ua/ua/news/all/zatverdjeno-kontseptsiyu-vidkritogo-bankingu-v-ukrayini (дата звернення: 09.02.2024).

– успіхом технологічних компаній в інших секторах економіки (роздрібна торгівля, медицина тощо). Поява успішних компаній, які суттєво змінили свої ринки та запропонували більш конкурентоспроможні продукти та послуги, викликала інтерес у банків й інших установ фінансового сектору.

Отже, щоби бути готовими до впровадження стандартів відкритого банкінгу та спроможними скористатися його перевагами, українським банкам і страховикам необхідно:

1) враховувати зміни, які йдуть, у своїх стратегічних планах;

2) банкам уже сьогодні розробляти та поступово інтегрувати концептуальні засади відкритого банкінгу у своїй діяльності;

3) розробляти програми фінансової грамотності щодо відкритого банкінгу, що дозволить підвищити фінансову інклюзію потенційних клієнтів;

4) краще аналізувати ринки своїх послуг і більш ретельно підходити до планування лінійки програмних продуктів і розробки нових комплексних продуктів;

5) страховикам налагоджувати нові зв'язки з банківськими установами, водночас, більш зважено підходити до акредитації партнера;

6) і банкам, і страховим компаніям розвивати відносини з фінтах-компаніями та підвищувати рівень технологічності бізнесу;

7) посилювати кібер-безпеку бізнес-процесів і захист персональних даних;

8) підвищувати фаховий рівень і мотивацію власного персоналу.

Так, результати SWOT аналізу показують, що традиційні банки мають сильні сторони, які вможливлюють їм представляти себе у конкурентному середовищі порівняно з іншими учасниками ринку, такими як фінтех-компанії. Проте, у них є і слабкі сторони, які заважають їм використовувати весь потенціал відкритого банкінгу. З огляду на вищезазначене, можна визначити сильні та слабкі сторони банків, а також можливості та загрози у контексті відкритого банкінгу (рис. 1).

Рис. 1. SWOT аналіз у контексті відкритого банкінгу

Отже, можна зробити висновок про те, що банки все ще можуть протистояти загрозам. Схоже, що сильні та слабкі сторони банків відображаються у компетенції інших учасників фінансового ринку. Це дозволяє зробити висновок щодо необхідності співпраці зі сторонніми надавачами платіжних послуг задля спільного покращення споживчого досвіду.

2. Концепція відкритого банку в Україні

Ця Концепція визначає засади відкритого банкінгу в Україні, зокрема, права користувачів платіжних послуг у відкритому банкінгу (включно із засадами управління згодою користувачів і захистом їхніх персональних даних, створенням структури відкритого банкінгу, класифікацією та використанням API, безпекою та кіберзахистом, процесом взаємодії учасників платіжного ринку та їхньою відповідальністю, а також застосуванням різних моделей відкритого банкінгу.

Концепція відкритого банку не є нормативно-правовим актом. Остаточна реалізація процедур відкритого банкінгу може відрізнятися від принципів, які викладені у цій Концепції, та може бути змінена за результатами розроблення нормативно-правових актів, які необхідні для впровадження відкритого банкінгу в Україні.

Метою зазначеної Концепції є визначення напрямків розвитку, дорожньої карти та ключових вимог щодо впровадження відкритого банкінгу в Україні.

Відкритий банкінг – це система, яка створена задля надання різноманітніших і привабливіших пропозицій користувачам платіжних послуг.

Відкритий банкінг уможливлює користувачам ухвалювати ефективніші повсякденні фінансові рішення завдяки інформації щодо руху коштів і залишків на рахунках, які відкриті у різних фінансових установах, агрегованій в одному застосунку. Водночас, упровадження відкритого банкінгу вплине на загальний розвиток фінансового сектору, а саме: посилення конкуренції між учасниками платіжного ринку, підвищення якості платіжних послуг, зниження вартості та більшої зручності їхнього використання, розширення доступу до фінансових послуг й інновації.

Тому важливо забезпечити довіру користувачів до нової системи, що буде досягнуто шляхом упровадження правил і механізмів, які узгоджені Національним банком України й іншими зацікавленими сторонами.

Так, правила, які будуть установлені в новій системі, та принципи взаємодії й обміну даними в рамках відкритого банкінгу мають бути зрозумілими та прийнятними для банків, надавачів фінансових і нефінансових платіжних послуг, а також технологічних операторів.

Об’єднання регулятора та зацікавлених сторін для обговорення операційних процедур відкритого банкінгу допоможе виробити оптимальні нормативні та технічні рішення щодо стандартизованих механізмів взаємодії надавачів платіжних послуг. Таке об’єднання також допоможе забезпечити інформаційну безпеку (зокрема, кібербезпеку), розробити відповідні системні рішення задля мінімізації ризику шахрайства, а також

створити прозорі механізми управління запитами та вирішення спорів між усіма учасниками відкритого банкінгу.

Ще одним важливим складником успіху відкритого банкінгу є впровадження технології миттєвих платежів, що покращить користувацький досвід і надасть змогу створювати нові програмні продукти та послуги.

У цій Концепції використовуються певні терміни та скорочення, які визначені відповідними нормативно-правовими актами.

«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 відповідно до пункту 2 частини першої статті 1 Закону України «Про платіжні послуги» це «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».

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

Відкриті API (Application Programming Interface) – це інтерфейси прикладного програмування, які ґрунтуються на загальних стандартах і забезпечують обмін даними між надавачами платіжних послуг і технологічними операторами платіжних послуг. Їх можна розділити 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 – надавач платіжних послуг, який надає послугу з емісії платіжних інструментів на підставі наявної ліцензії.

Заходи безпеки – сукупність заходів із виконання вимог Положення про автентифікацію та застосування посиленої автентифікації на платіжному ринку (Положення SCA)[13] й інших вимог законодавства України та нормативно-правових актів Національного банку України у сфері інформаційної та кібербезпеки на платіжному ринку (підпункт 7 пункту 3 розділу 1 Положення SCA).

[13] З метою зниження ризиків шахрайства надавачі платіжних послуг застосуватимуть посилену автентифікацію. Національний банк України. URL: https://bank.gov.ua/ua/news/all/z-metoyu-znijennya-rizikiv-shahraystva-nadavachi-platijnih-poslug-zastosuvatimut-posilenu-avtentifikatsiyu-16500 (дата звернення: 09.02.2024).

Інтерфейс – сукупність програмних й апаратних засобів, які призначені для виконання функцій електронної взаємодії між різними пристроями та програмним забезпеченням учасників платіжного ринку в інформаційно-комунікаційних системах надавача платіжних послуг, мережах загального користування з метою здійснення процедур автентифікації та надання фінансових і/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 Закону України «Про основні засади забезпечення кібербезпеки України»)[14].

«Відкритий ключ (дані для підтвердження електронного підпису чи електронної печатки) – дані, що використовуються для підтвердження електронного підпису чи електронної печатки» (пункт 25 частини першої статті 1 Закону України «Про електронну ідентифікацію та електронні довірчі послуги»)[15].

«Користувач платіжних послуг (далі – користувач) – фізична особа 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 Національного банку України), 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 отримала ліцензію щодо надання хоча б однієї платіжної послуги у порядку, встановленому Законом і нормативно-правовими актами Національного банку України.

Несанкціоновані чи шахрайські дії – вчинення сторонніми та/або відповідальними особами втручання в інформаційно-телекомунікаційні системи у незаконний спосіб, що може призвести до порушення цілісності, доступності та конфіденційності інформації, яка використовується надавачем платіжних послуг під час надання платіжних послуг (підпункт 13 пункту 3 розділу 1 Положення SCA).

[14] Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 09.02.2024).

[15] Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 05.10.2017 № 2155-VIII. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 09.02.2024).

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

а) знань (володіння інформацією (даними), що відома лише користувачу);

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

в) 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 цього Закону» (пункт 79 частини першої статті 1 Закону України «Про платіжні послуги»).

Зацікавлена сторона – надавачі платіжних послуг і їхні об'єднання.

Сторонні надавачі платіжних послуг – банки та надавачі платіжних послуг, які отримали право надавати нефінансові платіжні послуги.

Технологічний оператор платіжних послуг (hub) – юридичні особи, які забезпечують процесингові та клірингові послуги чи виконують операційні, інформаційні або інші технологічні функції, які пов'язані з наданням платіжних послуг, без залучення грошових коштів від платіжних операцій на власні рахунки.

AISP (Account Information Service Provider) – надавачі платіжних послуг, які надають послуги з обробки інформації про рахунки.

ASPSP (Account Servicing Payment Service Provider) – надавачі платіжних послуг, які управляють рахунками (банки, платіжні установи, малі платіжні установи, філії іноземних платіжних установ, установи електронних грошей, поштові оператори).

PISP (Payment Initiation Service Provider) – надавачі платіжних послуг, які ініціюють платіжні операції.

Інші терміни використовуються у значеннях, які наведені у Законі й інших нормативно-правових актах.

Концепція відкритого банкінгу виникла у Європейському союзі внаслідок ухвалення другої редакції Директиви ЄС про платіжні послуги (PSD2) та швидко ввійшла до порядку денного галузі. Впровадження відкритого банкінгу призвело до швидкого поширення відкритих API по всьому світу.

На сьогодні не існує єдиного глобального підходу до стандартизації API, а стадія впровадження відкритого банкінгу загалом варіюється від країни до країни. Велика Британія – єдина країна, у якій законодавчо закріплено вимогу щодо створення організації для розроблення, розвитку та підтримання правил відкритого банкінгу, що дає ринку цієї країни

перевагу під час упровадження нових програмних продуктів і послуг. Проте, деякі країни стрімко розвивають відкритий банкінг у себе: ЄС (загалом), Австралія та Мексика. Канада, Гонконг, Індія, Японія, Нова Зеландія, Сінгапур і США готують свої ринки до прийняття ініціативи відкритого банкінгу.

Європейське банківське управління (European Banking Authority – EBA) керує впровадженням PSD2 у країнах ЄС, випускаючи керівництва та рекомендації для зацікавлених сторін у вигляді нормативних технічних стандартів регулювання.

Проте, Європейський Союз дозволяє ринку розробляти власні стандарти для відкритих API. У зв'язку з цим декілька робочих груп представили власні напрацювання. Найбільш популярними стали стандарти Берлінської групи (Berlin Group).

Україна рухається у напрямку інтеграції у європейський платіжний простір. Згідно зі стратегією НБУ, економічне зростання та сприяння цифровізації є пріоритетами для регулятора. Так, 30 червня 2021 року з метою створення умов для розвитку інноваційних платіжних послуг і приведення українського законодавства у відповідність до стандартів ЄС ВРУ схвалила Закон № 1591-IX «Про платіжні послуги». Закон створює підґрунтя нормативного врегулювання відкритого банкінгу, а наповну він має запрацювати із серпня 2025 року.

Варто зазначити, що запорукою успіху відкритого банкінгу в Україні є загальний консенсус учасників платіжного ринку стосовно принципів і стандартів його функціонування. З цією метою Національний банк України прагнутиме налагодити діалог зі всіма учасниками платіжного ринку та їхніми об'єднаннями, який ґрунтуватиметься на принципі рівноправності, для розроблення й обговорення пропозицій щодо стандартів відкритого банкінгу.

Об'єднання учасників платіжного ринку, власне, учасники й експерти можуть надавати свої пропозиції щодо принципів, засад, порядку й особливостей функціонування відкритого банкінгу, а також відповідності бізнес-процесів, які усталені на ринку, законодавчим актам і їхнє можливе вдосконалення.

Національний банк України відповідно до своїх функцій, які встановлені законодавством, має розробити зведення ґрунтовних принципів відкритого банкінгу та напрямки його подальшого розвитку згідно з поточними чи майбутніми потребами ринку, водночас, забезпечуючи нормативно-правове ругулювання та нагляд за його дотриманням надавачами платіжних послуг.

Технічні специфікації затверджуються Національним банком України, ґрунтуючись на спільних напрацюваннях.

Система відкритого банкінгу – це сукупність регулятора, учасників платіжного ринку, правил їхньої взаємодії, які затверджені нормативно-правовими актами Національного банку України, й ІТ-інфраструктури надавачів платіжних послуг.

Учасниками відкритого банкінгу є користувачі, емітенти, технологічні оператори платіжних послуг, AISP, ASPSP і PISP.

Користувачі є основними бенефіціарами системи відкритого банкінгу, оскільки мають виключне право надавати згоду щодо доступу до власних рахунків і конкретного обсягу інформації за ними стороннім надавачам платіжних послуг.

ASPSP надають можливість взаємодіяти зі своїми системами (зокрема, здійснювати обмін даними) через API стороннім надавачам платіжних послуг.

Надавачі платіжних послуг, які не є фінансовими установами, можуть укладати договори із третіми сторонами щодо надання ними послуг для своїх користувачів. Правила роботи із третіми сторонами буде розроблено в рамках проєкту Національного банку України щодо впровадження відкритого банкінгу.

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

Авторизація діяльності надавачів платіжних послуг регулюються ЗУ «Про платіжні послуги», а також ЗУ «Про фінансові послуги та фінансові компанії»[16], який уведений у дію з 01 січня 2024 року на заміну ЗУ «Про фінансові послуги та державне регулювання ринків фінансових послуг», і нормативно-правовими актами Національного банку України, які передбачені у зазначених законах.

Надавач платіжних послуг отримує підтвердження успішної авторизації діяльності шляхом включення інформації про нього до Реєстру. Інформація, яка міститься у Реєстрі, є відкритою та загальнодоступною. Національний банк України публікує інформацію, яку містить Реєстр, у встановленому ним порядку. Доступ до Реєстру є безоплатним.

Для того щоби пройти авторизацію ASPSP й емітенти зобов’язані отримати відповідні ліцензії.

Надавачі нефінансових платіжних послуг можуть поєднувати свою діяльність як PISP й AISP.

Банки, платіжні установи, установи електронних грошей і філії іноземних платіжних установ мають виключне право поєднувати фінансові та нефінансові платіжні послуги за умови внесення відповідної інформації до Реєстру.

Розглянемо дві моделі взаємодії учасників системи відкритого банкінгу:

– модель 1: за участю AISP, ASPSP, PISP й емітента;

– модель 2: за участю AISP, ASPSP, PISP, емітента та технологічного оператора платіжних послуг.

Взаємодія між AISP, ASPSP, PISP, емітентом і технологічним оператором платіжних послуг здійснюється на підставі укладених угод.

[16] Про фінансові послуги та фінансові компанії : Закон України від 14.12.2021 № 1953-IX. URL: https://zakon.rada.gov.ua/laws/show/1953-20#Text (дата звернення: 09.02.2024).

Надавачі платіжних послуг можуть використовувати послуги технологічного оператора платіжних послуг задля забезпечення операційних, інформаційних і технічних функцій згідно з угодами та не мають використовувати чи зберігати враздиві платіжні дані користувачів для власних потреб.

Платіжні операції, ініційовані у рамках відкритого банкінгу, здійснюються тільки між рахунками.

Учасники системи мають розробляти власні відкриті API відповідно до технічних специфікацій, які затверджені й опубліковані Національним банком України, з урахуванням вимог інформаційної безпеки та кібербезпеки. Технічні специфікації API мають бути розроблені відповідно до принципів цієї Концепції.

Надавачі платіжних послуг зобов'язані:

ASPSP:

– забезпечити постійний доступ сторонніх надавачів платіжних послуг до рахунків своїх користувачів (за винятком кореспондентських рахунків банків і розрахункового рахунку надавача платіжних послуг) у режимі реального часу відповідно до порядку, який установлений Національним банком України;

– стягувати однаковий розмір комісії за проведення операцій за рахунком користувача як у рамках каналу дистанційного банківського обслуговування ASPSP, так й у рамках відкритого банкінгу;

– надавати емітенту підтвердження доступності грошових коштів на рахунку платника тільки за дотримання таких умов:

а) рахунок платника на момент запиту доступний у режимі реального часу;

б) платник погодився надати ASPSP інформацію про суми платіжних операцій, які ініційовані платником, на запити конкретного емітента (згода платника вимагається тільки у випадку першого запиту емітента щодо підтвердження доступності грошових коштів на рахунку платника);

в) у випадку, якщо він тимчасово не може здійснювати свою діяльність і/або якщо API неактивний, відповідати на всі запити з надання інформації щодо API про те, що API, до якого адресовано запит, недоступний.

PISP/AISP/емітент:

– ініціювати доступ до рахунків і виконання транзакції тільки ґрунтуючись на активному статусі згоди користувача;

– ідентифікувати себе перед ASPSP щоразу, коли він виконує нефінансову платіжну послугу;

– забезпечувати безпечний обмін інформацією з ASPSP, платником й отримувачем платежу тільки захищеними каналами зв'язку, з урахуванням вимог законодавства та нормативно-правових актів Національного банку України;

– забезпечити, щоб особиста облікова інформація користувача не була доступна нікому, крім самого користувача й ASPSP, де, власне, й обслуговується рахунок користувача.

Під час створення й упровадження послуг API надавачі платіжних послуг мають ураховувати такі принципи:

– створення цінності – метою розробки відкритих API є розв'язання актуальних проблем і забезпечення потреб користувачів, ґрунтуючись на аналізу їхнього досвіду;

– уніфікація та прозорість – відкриті API мають створюватися відповідно до єдиних правил у вигляді нормативно-правових актів і технічних специфікацій, які затверджуються та публікуються на офіційному веб-сайті Національного банку України;

– розширюваність – система відкритих API має забезпечувати можливість її розширення шляхом модифікації наявних або створення нових API;

– безпека – розроблені API мають відповідати вимогам безпеки, включно з кібербезпекою, та забезпечувати можливість аудиту як на етапі передпускового тестування, так й у період експлуатації;

– відкритість і недискримінація – умови доступу до API, які надаються учасниками системи відкритого банкінгу, мають бути однаковими для всіх учасників і не мають створювати організаційних або технічних бар'єрів для доступу чи преференцій для будь-якого учасника та такими, які не порушують законодавство щодо захисту економічної конкуренції;

– відповідальність – спори вирішуються відповідно до українського законодавства, з урахуванням прав й обов'язків учасників, водночас, керуючись інтересами користувачів.

У цій Концепції передбачено два типи API: базові та комерційні.

Базові API – це прикладні програмні інтерфейси, які реалізуються відповідно до українського законодавства, їхні специфікації затверджуються Національним банком України та функціонування яких є обов'язковим і безоплатним для всіх учасників відкритого банкінгу. Учасники мають гарантувати підтримку та доступ до базових автоматизованих банківських систем.

Використання базових API не потребує укладення угоди між ASPSP і сторонніми надавачами платіжних послуг.

Відповідно до Закону базовими вважаються API у межах надання послуг з ініціювання платіжних операцій, а також надання інформації щодо рахунку та підтвердження доступності грошових коштів на рахунку:

для PISP:

– ініціювання разового платежу у межах країни;

– ініціювання разового платежу за межами країни.

для PISP:

– отримання інформації щодо залишку (доступні кошти) на конкретному рахунку;

– отримання історії операцій (за останні 30 днів) за конкретним рахунком;

– для емітента підтвердження доступності грошових коштів на рахунку.

У рамках використання базового API запити на встановлення згоди та взаємодії з користувачем обробляються безоплатно.

Комерційні API – це програмні інтерфейси, які не належать до базових API та можуть бути використані на платній основі. Правила підключення до комерційних API мають бути визначені й опубліковані на сайті ASPSP.

Оплату за використання комерційних API здійснюють на підставі окремої угоди між відповідним надавачем платіжних послуг й ASPSP. У випадку операцій за участю технологічних операторів платіжних послуг, взаємні розрахунки здійснюються ними централізовано на підставі окремих угод між кожним надавачем платіжних послуг й ASPSP.

Усі учасники, які є володільцями API, мають забезпечити:

– доступність API у режимі 24/7 (цілодобово), при цьому виконання операцій з ініціювання платежів й отримання даних щодо рахунків здійснюється відповідно до затверджених положень про операційний день;

– не надання послуги з ініціювання платіжних операцій та отримання даних щодо рахунку, якщо доступ до рахунку користувача неможливий у режимі реального часу, у випадку технічного збою, який робить API недоступним, інформація про збій та очікувані строки усунення має бути розміщена на веб-сайті API;

– резервну роботу інтерфейсу, який функціонує автоматично у випадку проблем з основним каналом;

– доступність/актуальність/повноту документації, яка описує розроблені базові та комерційні API, на своєму веб-сайті;

– повну відповідність API, які використовуються у продуктивному та тестовому режимах, і які мають бути фізично розділеними та розміщеними у різних інформаційних середовищах;

– відсутність обмежень доступу для авторизованих PISP/AISP/емітента до власних API, крім як задля протидії кіберзагрозам;

– відсутність потреби під час опрацювання запитів від декількох учасників установлювати пріоритет для запитів від окремих учасників;

– щоб час відповіді на запит під час використання API відповідав поточному значенню відповідно до затверджених параметрів технічного регламенту.

Базові компоненти архітектури API представлені у таблиці 1.

Таблиця 1

Базові компоненти архітектури API

Показник	Значення
Архітектура API	RESTful
Стандарт обміну даними	JSON
Транспортний протокол	TLS 1.2 чи 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

Концепція містить загальні принципи, які необхідно враховувати під час розробки екранних форм і взаємодії користувача/AISP/ASPSP/PISP/емітента у відкритому банкінгу.

AISP/ASPSP/PISP/емітент має забезпечити, щоб інформація, яка надається користувачу, була повною та зрозумілою.

AISP/емітент має забезпечити, щоб кожного разу, коли користувач відкриває платіжний застосунок AISP/емітента, інформація щодо наданих згод користувача була актуальною.

Від користувача не має вимагатися спеціальних знань або навичок для використання послуг відкритого банкінгу.

Повідомлення щодо статусу та дати транзакцій та операцій користувача мають бути чіткими та зрозумілими.

Коли AISP/PISP/емітент й ASPSP взаємодіють задля надання інформації про рахунок користувача й/або ініціювання платежу та/або підтвердження доступності грошових коштів, екранна форма веб-інтерфейсу чи платіжного застосунку надавача платіжних послуг, яка показується користувачеві, не має містити непотрібної інформації, включно з рекламою або іншими посиланнями.

Екранні форми AISP/ASPSP/PISP/емітента мають надавати користувачам інформацію щодо згоди під час її надання/відкликання.

Мінімум інформації, який має відображатися:

– назва AISP/ASPSP/PISP/емітента та/або його торгова/комерційна марка чи логотип;

– дата закінчення строку дії згоди;

– дата та час останнього оновлення облікових даних користувача.

Якщо згоду не продовжено протягом визначеного терміну чи відкликано користувачем, інформація з'явиться в архіві вже анульованих згод.

Користувач може відобразити екран згоди, не натискаючи на нього більше трьох разів.

Якщо під час відображення інформації про баланс рахунку (загальну суму доступних коштів) надавач платіжних послуг не робить розподіл між власними коштами користувача та доступним кредитним лімітом, то це відображення має супроводжуватись інформаційним повідомленням, яке попереджає про те, що стягуватимуться додаткові комісії за рахунок списання коштів кредитного ліміту у випадку ініціювання платіжної операції зі вказаного рахунку.

PISP має відобразити інформаційне повідомлення з розміром комісії, яке попереджає користувача про те, що при ініціюванні платіжної операції може стягуватися комісія.

Перелік усіх активних згод користувача, які відомі надавачу платіжних послуг, має відображатися одночасно (на одному екрані) з можливістю переходу до деталізованої інформації щодо конкретної згоди (номер рахунку, валюта, глибина виписки тощо).

Надавачі платіжних послуг мають забезпечити зручні пошук/сортування/фільтр у переліку активних згод користувача. У випадку відкликання/анулювання згоди забороняється застосовувати до користувача будь-які обмеження.

AISP/PISP можуть надати користувачам можливість редагувати своє ASPSP-ім'я, замінюючи його на псевдонім, щоб користувачам було простіше ідентифікувати свій обліковий запис.

ASPSP отримує згоду від користувача через AISP/PISP/емітента, який має угоду з цим користувачем, щодо:

– конкретних сторонніх надавачів платіжних послуг, яким він надає згоду щодо доступу;

– конкретних рахунків, згоду на доступ до яких він надає;

– конкретних нефінансових платіжних послуг, згоду на які він надає та конкретний обсяг інформації про рахунки та користувача цих рахунків.

До або одночасно з отриманням згоди ASPSP має отримати дозвіл користувача щодо розкриття інформації, яка містить банківську та комерційну таємницю, а також таємницю надавча платіжних послуг. Дозвіл користувача надається через AISP/PISP/емітента, який має угоду з таким користувачем.

Під час надання згоди користувач проходить посилену автентифікацію зі сторони ASPSP.

Згода може бути одноразовою чи надаватися на певний строк, який не перевищує 180 календарних днів.

Згода, яка отримана ASPSP від користувача, не є його згодою щодо акцепту оферти угоди про приєднання до умов і правил надання послуг, реєстрації у платіжному застосунку, веб-інтерфейсі або іншому програмно-технічному комплексі, який використовується таким надавачем платіжних послуг задля забезпечення взаємодії з користувачем AISP/PISP/емітента.

У випадку надання згоди через AISP/PISP/емітента користувач має самостійно визначити обсяг інформації, щодо якої надається ця згода (у формі явного підтвердження), підтвердження за замовчуванням не допускається. Користувачу також необхідно мати явний доступ до інформації щодо строку дії й умов відкликання згоди тощо.

Доступ до інформації щодо згоди, яка надана користувачем, має бути зафіксований як зі сторони AISP/PISP/емітента, так і зі сторони ASPSP (тією мірою, якою це доступно відповідному надавачу платіжних послуг), уключно з його платіжним застосунком.

Одна згода не може бути зумовлена іншою: на кожну послугу чи програмний продукт користувач має надавати окрему згоду.

Користувач має право у будь-який час відкликати (анулювати) надану згоду, зокрема через платіжні застосунки, як зі сторони AISP/PISP/емітента, так і зі сторони ASPSP (окремо для кожної згоди або одночасно для всіх). У випадку відкликання (анулювання) згоди будь-які обмеження щодо користувача забороняються.

ASPSP негайно призупиняє доступ до рахунку й/або інформації, яка надана у рамках цієї згоди, у випадку відкликання згоди через ASPSP.

AISP/PISP/емітент зобов'язаний негайно повідомити ASPSP щодо відкликання згоди через AISP/PISP/емітента, а ASPSP негайно призупинить доступ до облікового запису й/або інформації, яка надана згідно з цією згодою.

Користувач має отримати підтвердження від відповідного ASPSP щодо відкликання згоди. Для підтвердження факту повідомлення достатньо оновленого статусу згоди у платіжному застосунку ASPSP.

AISP/ASPSP/PISP/емітент має використовувати для кожної згоди тільки одну з таких позначок її статусу:

– активна – згода, яка підтверджена користувачем, і є чинною;

– прострочена – строк дії такої згоди вже закінчився;

– відкликана – згоду було відкликано (анульовано) користувачем.

Відкликані (анульовані) згоди та ті, які мають прострочений термін дії, вважаються недійсними й AISP не має підстав надавати інформацію, яка передбачена такими згодами.

Рекомендується, щоб AISP/PISP/емітент інформував користувача про можливість продовження згоди не менше ніж за сім днів до закінчення строку її дії.

У міру того як сторонні надавачі платіжних послуг отримують доступ до даних користувацьких рахунків через API та можуть ініціювати платежі від їхнього імені, вимоги до безпеки таких платежів тільки зростатимуть і вразливі платіжні дані користувачів мають бути додатково захищені від несанкціонованого доступу.

Надавачам платіжних послуг необхідно мати засоби для постійного моніторингу подій, які пов’язані зі взаємодією з користувачами, з метою створення та підтримання безпечного інформаційного середовища тазастосування всіх необхідних безпекових заходів (як це визначено у Положенні SCA).

Платіжні послуги, які пропонуються у рамках відкритого банкінгу, мають надаватися з використанням технологій, які можуть гарантувати безпечну автентифікацію користувачів і мінімізувати можливість шахрайства.

Електронна взаємодія між надавачем платіжних послуг і користувачами має здійснюватися тільки після їхньої автентифікації.

Процедура автентифікації має включати механізми моніторингу спроб і способів несанкціонованого використання вразливих платіжних даних згідно з вимогами Національного банку України, які викладені у Положенні SCA.

Інформація щодо всіх дій, які здійснюються фізичними особами у платіжному застосунку (під час автентифікації та подальшої взаємодії з надавачем платіжних послуг), має зберігатися надавачем платіжних послуг для того, щоб цю інформацію можна було використати під час розслідування кібер-інцидентів.

Вимоги до автентифікації користувача та випадки, коли не потрібна посилена автентифікація, встановлені у статті 68 ЗУ «Про платіжні послуги» та Положенні SCA.

Порядок застосування посиленої автентифікації та рішення про те, коли надавач платіжних послуг має право не вимагати посилену автентифікацію користувача, викладено у Положенні SCA.

Винятки з посиленої автентифікації, коли надавач платіжних послуг має право не вимагати посиленої автентифікації користувача, зазначені у Положенні SCA.

Коли ASPSP отримує запит на автентифікацію користувача через AISP/PISP/емітента, він має застосовувати методи, які зазначені нижче.

ASPSP має оптимізувати процес автентифікації, беручи до уваги необхідність і достатність безпекових заходів.

Методи автентифікації:

– автентифікація на підставі перенаправлення;

– відокремлена автентифікація;

– вбудована автентифікація.

Зазначена Концепція визначає загальні методи автентифікації. Надалі остаточний перелік методів автентифікації буде визначено, ґрунтуючись на детальному аналізі, та відображено у розробленому Порядку роботи відкритого банкінгу.

Перед початком взаємодії ASPSP має здійснити автентифікацію AISP/PISP/емітента, тобто, він має встановити, що AISP/PISP/емітент має право надавати відповідні платіжні послуги.

Автентифікація AISP/PISP/емітента в ASPSP має здійснюватися з використанням кваліфікованого сертифікату відкритого ключа згідно з Подоженням SCA.

Вимога щодо створення кваліфікованого сертифіката відкритого ключа для електронної взаємодії між AISP/PISP/емітентами й ASPSP ґрунтується на нормативно-правовому акті Національного банку України щодо порядку надання та використання електронних довірчих послуг банками й іншими особами, які діють на ринку фінансових послуг, і нагляд за якими здійснює НБУ, операторами платіжних систем і/або їхніми учасниками, а також технологічними операторами платіжних послуг.

Взаємна автентифікація має бути забезпечена для того, щоб AISP/PISP/емітент мав доступ до API відповідного ASPSP. Взаємна автентифікація має здійснюватися з використанням протоколу шифрування mTLS.

Для забезпечення безпечного обміну даними між надавачами платіжних послуг через API має використовуватися захисний протокол транспортного рівня TLS не нижче версії 1.2.

Для забезпечення конфіденційності обміну даними між AISP/PISP/емітентом й ASPSP має бути вжито необхідні заходи й упроваджено відповідні стандарти з інформаційної взаємодії та кібербезпеки, а також необхідно забезпечити дотримання вимог нормативно-правового акта Національного банку України, який регулює вимоги до автентифікації та використання посиленої автентифікації на ринку платіжних послуг.

Водночас, мають бути враховані всі вимоги інших нормативно-правових актів Національного банку України та відповідного українського законодавства щодо захисту комунікацій усіх учасників відкритого банкінгу.

Перш ніж дозволити сторонньому надавачу платіжних послуг доступ до рахунків користувача, ASPSP має підтвердити його авторизацію діяльності щодо такої платіжної послуги у порядку, встановленому Національним банком України, зокрема, шляхом перевірки інформації у Реєстрі та/або перевіркою сертифіката відкритого ключа.

ASPSP забороняється надавати доступ до рахунку користувача будь-якому сторонньому надавачу платіжних послуг, який не пройшов перевірку інформації у Реєстрі та/або перевірку кваліфікованого сертифіката відкритого ключа. ASPSP, відповідно до українського законодавства, несе відповідальність за будь-яку шкоду, яка понесена користувачем у випадку недотримання ним умов надання доступу до рахунків.

ASPSP публікує на своєму офіційному веб-сайті окремий розділ, який присвячений забезпеченню взаємодії у рамках відкритого банкінгу.

Інформація у цьому розділі має бути доступною безоплатно та не бути обмежена за кількістю осіб, а також має містити щонайменше такі дані:

– перелік відкритих і комерційних API, до яких ASPSP надає доступ;

– документація з технічними характеристиками всіх доступних API, зокрема, із зазначенням процедур, протоколів й інструментів, які необхідні AISP/PISP/емітенту для організації взаємодії;

– опис тестового середовища, яке може використовувати AISP/PISP/емітент для перевірки результатів обробки запиту;

– способи звернення до служби підтримки ASPSP із питань взаємодії з API.

Зазначена інформація має підтримуватися в актуальному стані.

ASPSP зобов'язаний моніторити доступність й ефективність API.

Якщо AISP/PISP/емітент не може використовувати API ASPSP, цей факт має бути зафіксований в операційній системі AISP/PISP/емітента й AISP/PISP/емітент матиме підставу для звернення до ASPSP/НБУ згідно з нормативно-правовими актами Національного банку України.

Надавачі платіжних послуг зобов'язані щоквартально публікувати на своїх офіційних веб-сайтах статистику щодо доступності й ефективності API.

Моніторинг API є обов'язком як ASPSP, так і PISP й емітенту.

Для моніторингу доступності надавачі платіжних послуг мають збирати дані за такими параметрами (перелік не є вичерпним):

– кількість отриманих запитів;

– кількість запитів із технічними помилками;

– кількість запитів, строк дії яких закінчився та на які не було надано відповідей;

– середній час відповіді на запит.

Для моніторингу ефективності надавачі платіжних послуг мають збирати дані за такими параметрами (перелік не є вичерпним).

– кількість користувачів;

– кількість активних згод;

– кількість відкликаних згод;

– кількість запитів до API;

– обсяг запитів з ініціювання платіжних операцій.

Під час надання послуг користувачам у рамках відкритого банкінгу використовуються ті самі механізми захисту даних користувачів, що й під час надання інших платіжних послуг.

Дані користувача, платіжні дані й інформація про покупки користувача мають захищатися надавачами платіжних послуг згідно з нормативно-правовими актами Національного банку України.

Користувач має право надавати та відкликати згоду на певний період часу й обмежувати доступ до рахунків.

Відкликання згоди може бути здійснено через ASPSP або AISP/PISP/емітента.

Учасники платіжного ринку мають створити внутрішні механізми для вирішення звернень (скарг) користувачів із чітко визначеними ролями й обов'язками та мати достатню кількість каналів подачі заяв (повідомлень), уключно з фізичними та цифровими каналами, які будуть легко доступними для користувачів. Заява (повідомлення) користувача про спірне питання подається ASPSP і розглядається надавачем платіжних послуг відповідно до правил розгляду звернень користувачів.

Оскільки відкритий банкінг сприяє інноваціям у сфері платіжних послуг, розширює наявні та створює нові програмні продукти та послуги, а також забезпечує обмін користувацькими даними та взаємозв'язок систем, учасникам платіжного ринку необхідно створити системи управління операційними, безпековими та кібер-ризиками, які пов'язані з наданням платіжних послуг (здійсненням транзакцій за допомогою платіжних систем), уключно з комплаєнс-ризиком, ризиками відмивання грошей, а також регуляторним тощо.

Надавачі платіжних послуг мають знати щодо потенційниз ризиків і вживати належних заходів щодо їхнього зниження. Це включає у себе застосування суворих безпекових заходів і конфіденційності, дотримання нормативних вимог, проведення перевірки сторонніх надавачів платіжних послуг, а також навчання й інформування користувачів про ризики та переваги відкритого банкінгу.

У рамках відкритого банкінгу наразі виявлено такі види потенційних ризиків, які представлені нижче.

Ризики конфіденційності та безпеки даних: несанкціонований доступ до особистих даних користувачів, витік даних або неправомірне використання у випадку відсутності відповідних заходів безпеки, таких як шифрування, автентифікація й управління згодою.

Ризики шахрайства та кібер-безпеки: інформаційні системи надавачів платіжних послуг можуть бути вразливими до шахрайства та кібер-атак, таких як фішинг, шкідливе ПЗ й атаки соціальної інженерії. Несанкціонований доступ до облікових записів користувачів, несанкціоновані транзакції та маніпуляції з даними можуть становити ризик як для користувачів, так і для надавачів платіжних послуг.

Регуляторні ризики та ризики відповідності: відкритий банкінг підпорядковується вимогам українського законодавства та нормативно-правових актів Національного банку України, зокрема щодо захисту даних, управління згодою та боротьби з відмиванням грошей (AML).

Операційні та технічні ризики: технічні збої й операційні помилки у роботі можуть призвести до переривання обслуговування та втрати довіри користувачів.

ASPSP несе відповідальність відповідно до українського законодавства й умов угоди, яка укладена з користувачем. У рамках відкритого банкінгу надавачам платіжних послуг з обслуговування рахунків заборонено надавати доступ до рахунків користувачів стороннім надавачам платіжних послуг, якщо вони не дотримуються умов доступу, які передбачені українським законодавством.

ASPSP несе відповідальність відповідно до українського законодавства за будь-яку шкоду, яка заподіяна користувачу у випадку недотримання ASPSP умов надання доступу до рахунків.

ASPSP несе відповідальність відповідно до ЗУ «Про платіжні послуги» перед користувачем за невиконання чи неналежне виконання транзакцій, які ініційовані через PISP.

У випадку виникнення спору щодо транзакції ASPSP несе відповідальність за несвоєчасну відповідь користувачеві платіжних послуг і взаємодіє з учасником платіжного ринку (AISP або PISP), а також зобов'язаний довести й обґрунтувати правомірність транзакції.

Надавачі нефінансових платіжних послуг зобов'язані гарантувати свою відповідальність перед користувачами й ASPSP у порядку, який встановлений нормативно-правовими актами Національного банку України.

У випадку невиконання чи неналежного виконання послуги з ініціювання платіжної операції PISP зобов'язаний відшкодувати ASPSP на його вимогу всі понесені збитки та суми, які були відшкодовані користувачу.

Надавач платіжних послуг зобов'язаний контролювати та нести відповідальність за дотриманням технологічним оператором платіжних послуг умов і порядку надання відповідних послуг надавачам платіжних послуг відповідно до укладеної між ними угоди. У зв'язку з цим надавач платіжних послуг зобов'язаний контролювати наявність відповідного статусу технологічного оператора платіжних послуг до укладення з ним угоди.

Якщо надавач платіжних послуг передає свої операційні функції третій стороні, то він несе відповідальність перед користувачем за надання платіжних послуг або виконання платіжних операцій. У випадку залучення для виконання операційних функцій третьої сторони, відносини та зобов'язання надавача платіжних послуг щодо користувача залишаються незмінними.

Отже, незважаючи на схвалення Концепції відкритого банку в Україні, власне, відкритий банкінг усе ще перебуває у «зародковому стані», тому необхідно стежити за розвитком подій у країнах Європейського Союзу, які впровадили PSD2, щоб стимулювати відкриту діяльність банків.

Висновки

У результаті виконаного комплексного дослідження розглянуто концепцію відкритого банкінгу, його сильні та слабкі сторони, можливості та загрози впровадження в Україні у контексті євроінтеграційних процесів.

Варто зазначити, що відкритий банкінг є важливою тенденцією у фінансовій сфері й одночасно можливістю для банків протистояти складному ринковому середовищу.

Правове регулювання відкритого банкінгу здійснюється відповідно до Закону України «Про платіжні послуги», а також нормативно-правових актів Національного банку України, зокрема, Положення SCA, які мають бути розроблені згідно затвердженої Концепції відкритого банкінгу.

Відкрите банківське обслуговування має важливе значення для українського банківського сектору, а отже у якості еталону можна прийняти до уваги приклад відкритого банкінгу країн Європейського Союзу. При цьому, необхідно враховувати SWOT аналіз банків у контексті відкритого банкінгу. За його результатами встановлено, що банки мають зосередитися на своїх сильних сторонах, таких як: імідж надійного партнера, якому довіряють, щоб вижити у конкурентній боротьбі на ринку. Можливості також полягають у покращенні споживчого попиту за рахунок розширення програмних продуктів і послуг.

Значущим чинником для зміцнення своїх позицій на конкурентному ринку стане трансформація бізнес-моделей і IT. Цифрове середовище, безумовно, буде надактуальним у майбутньому, яке вже настає.

Концепція відкритого банкінгу в Україні все ще перебуває у «зародковому стані», тому доцільно спостерігати за розвитком подій у країнах Європейського Союзу, які ввели PSD2, що здійснює стимулюючий вплив на відкриту банківську діяльність. Клієнт має бути рушійною силою інновацій та ініціатив у цій сфері, оскільки на попит зі сторони споживача ринок реагує відповідним чином. Банки мають розробляти стратегію цифровізації з точки зору відкритих API для просування цифрового середовища, забезпечуючи дотримання основоположних прав і свобод людини та громадянина.

АНОТАЦІЯ

У дослідженні зосереджено увагу на теоретико-методологічних аспектах правового регулювання відкритого банкінгу та Концепції відкритого банкінгу в Україні. Систематизовано нормативно-правову базу, яка забезпечує зазначене правове регулювання, до якої можна віднести Закони України: «Про платіжні послуги», «Про основні засади забезпечення кібербезпеки України», «Про електронну ідентифікацію та електронні довірчі послуги», «Про фінансові послуги та фінансові компанії», а також Положення SCA Національного банку України. В аспекті євроінтеграційних процесів в Україні доведено необхідність ретельного вивчення досвіду країн Європейського Союзу, які ввели PSD2, й оцінено вплив цієї директиви на банківський сектор. Усі країни Європейського Союзу й Україна, як асоційований член, а у майбутньому, сподіваємося, повноцінний учасник, мають керуватись однаковою правовою базою та технічними стандартами. Надано коротку характеристику форм й інструментів підтримки та стимулювання впровадження цифрових технологій у фінансовій сфері. Ґрунтовно проаналізовано сучасні тренди

розвитку ринку інноваційних банківських послуг у контексті розширення використання електронних каналів надання банківських послуг, зокрема, AISP, ASPSP, PISP, емітента та технологічного оператора платіжних послуг. Зроблено висновок про те, що надалі необхідна реалізація скоординованих заходів у зазначеній сфері, а саме: дотримання збалансованого підходу у сфері правового регулювання ринку фінансових технологій; подальша реалізація стратегії відкритого банкінгу; сприяння процесу кооперації банків і фінтех-компаній.

Література

1. Довгань, Ж. М., Галіцейська, Ю. М. (2021). Open-банкінг як тренд розвитку фінансових технологій. *Інноваційна економіка*. 5–6’2021 [88]. С. 111–116.
2. Єсіна, О. Г. (2023). *Проблеми сучасних трансформацій. Серія: економіка та управління*. 7. URL: https://doi.org/10.54929/2786-5738-2023-7-08-01.
3. Заславська, О. І., Петканич, М.-В. М. (2023). Цифрова трансформація банківського бізнесу в умовах розвитку фінансових технологій. *Науковий вісник Ужгородського Університету. Серія Економіка*. 2 (62). С. 116–122.
4. Охрименко, І. Б., Шуляк, Д. А. (2023). Інновації open-banking у розвитку банкострахування. *Актуальні питання у сучасній науці*. 11 (17). С. 193–208.
5. Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC (Text with EEA relevance). European Parliament. URL: https://eur-lex.europa.eu/eli/dir/2007/64/oj (дата звернення: 09.02.2024).
6. Consolidated text: Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance). European Parliament. URL: https://eur-lex.europa.eu/eli/dir/2015/2366/2015-12-23 (дата звернення: 09.02.2024).
7. European Open Banking Forecast, 2022 To 2027. Forrester. URL: https://www.forrester.com/report/european-open-banking-forecast-2022-to-2027/RES178412 (дата звернення: 09.02.2024).
8. Four European takes on open banking. Mastercard Data & Services. URL: https://www.mastercardservices.com/en/advisors/archived-practices/open-banking/insights/four-european-takes-open-banking (дата звернення: 09.02.2024).
9. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a framework for Financial Data Access and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554. European Parliament. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023PC0360 (дата звернення: 09.02.2024).

10. Keynote speech by Commissioner McGuinness at event in European Parliament “From Open Banking to Open Finance: what does the future hold?”. European Commission. URL: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_23_1819 (дата звернення: 09.02.2024).

11. Про платіжні послуги : Закон України від 30.06.2021 № 1591-IX. URL: https://zakon.rada.gov.ua/laws/show/1591-20#Text (дата звернення: 09.02.2024).

12. Затверджено Концепцію відкритого банкінгу в Україні. Національний банк України. URL: https://bank.gov.ua/ua/news/all/zatverdjeno-kontseptsiyu-vidkritogo-bankingu-v-ukrayini (дата звернення: 09.02.2024).

13. З метою зниження ризиків шахрайства надавачі платіжних послуг застосуватимуть посилену автентифікацію. Національний банк України. URL: https://bank.gov.ua/ua/news/all/z-metoyu-znijennya-rizikiv-shahraystva-nadavachi-platijnih-poslug-zastosuvatimut-posilenu-avtentifikatsiyu-16500 (дата звернення: 09.02.2024).

14. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 09.02.2024).

15. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 05.10.2017 № 2155-VIII. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 09.02.2024).

16. Про фінансові послуги та фінансові компанії : Закон України від 14.12.2021 № 1953-IX. URL: https://zakon.rada.gov.ua/laws/show/1953-20#Text (дата звернення: 09.02.2024).

Information about the author:
Serhiienko Anfisa Serhiiivna,
Senior Lecturer at the Department of Fundamental
and Branch Legal Sciences
Kremenchuk Mykhailo Ostrohradskyi National University
20, University Str., Kremenchuk, 39600, Ukraine