

20-11-2025

До учасників платіжного ринку
України**Тема: Критичні аспекти вибору технологічного рішення для відкритого банкінгу**

Шановні колеги,

В рамках підготовки до обов'язкового впровадження відкритого банкінгу згідно з Постановою НБУ №80, учасники ринку стикаються з низкою стратегічних рішень, що безпосередньо впливають на технічну реалізацію, відповідність вимогам, безпеку та конкурентоспроможність.

У цьому листі висвітлюються три ключові ризики, які загрожують реалізації проєктів. До листа додано три документи з детальним аналізом кожного з цих ризиків.

1. Особливості "досвідченого вендора": чому досвіду роботи з АБС може бути недостатньо для відкритого банкінгу?

Перший документ підтверджує, що досвід вендора у розробці автоматизованих банківських систем (АБС) не є достатньою умовою для успішної реалізації проєктів відкритого банкінгу. Це обумовлено принциповою різницею у парадигмах розробки, вимогах до безпеки та архітектури.

- Закрита система (АБС) vs Відкрита екосистема (API): АБС функціонує в ізольованому периметрі, тоді як відкритий банкінг забезпечує масовий доступ зовнішніх TPP (AISP/PISP) через публічні API з використанням OAuth2, OIDC та QWAC/QSealC.
- Архітектурний ризик: Спроба інтеграції API-шлюзу в існуючу архітектуру АБС без її фундаментальної переробки створює загрозу низької продуктивності та системних збоїв.
- Перевірка досвіду: Рекомендується вимагати у вендорів конкретні кейси впровадження на базі стандарту Berlin Group 2.1, висновки аудитів на відповідність вимогам НБУ та демонстрацію робочого механізму управління згодами (Consent Management).

Висновок: Вибір вендора без підтвердженого профільного досвіду в відкритому банкінгу створює значні проєктні та операційні ризики в умовах обмеженого часу.

2. Ризики використання застарілих стандартів: чому Berlin Group 1.4 призводить до технічної та регуляторної невідповідності

Другий документ констатує критичну несумісність між версіями стандартів Berlin Group 1.4 та 2.1.

- Не оновлення, а повна переробка: Український стандарт (на основі Berlin Group 2.1) є не оновленням, а повною архітектурною переробкою з новими ендпоінтами, структурами даних та механізмами безпеки.
- Неможливість відповідності: Рішення, розроблене на версії 1.4, не зможе пройти технічний аудит, що робить неможливим отримання ліцензії для діяльності як ASPSP або TPP з 01.08.26.
- Неефективність витрат: Спроби адаптації рішення під новий стандарт за 5 місяців потребуватимуть ресурсів, що перевищують вартість розробки з нуля, і призведуть до створення ненадійної системи.

Висновок: Обрати вендора, що пропонує рішення на версії 1.4, — означає свідомо створити передумови для технічної невідповідності та втрати конкурентних позицій.

3. Ризики делегування: чому модель SaaS Технологічного Оператора несе системні загрози для банку (ASPSP)

Третій документ, на підставі аналізу НПА (Постанови №58, №82, №123, №80, №99), детально описує ризики залучення ТО у хмарній SaaS-моделі.

- Неділігована відповідальність: Відповідно до ЗУ "Про платіжні послуги" (ст. 9), банк несе повну відповідальність перед клієнтами та регулятором за будь-які порушення, допущені ТО.
- Критичні ризики безпеки: Втрата прямого контролю над посиленою автентифікацією (SCA), ускладнення валідації сертифікатів TPP, ризик концентрації (збій у ТО може паралізувати роботу відкритого банкінгу одночасно в кількох банках).
- Комплаєнс-ризик: Складність забезпечення дотримання вимог щодо місця зберігання даних, проведення глибокого аудиту мультитенантного середовища та контролю за ланцюжком субпідрядників.

Висновок: Модель ТО (SaaS) впроваджує системні ризики, що суперечать принципам безпеки та регуляторним вимогам, переводячи банк у стан залежності від зовнішнього постачальника.

Загальний висновок та рекомендації

Сукупність цих трьох факторів — недостатній профільний досвід вендора, невідповідний стандарт та неоптимальна модель розгортання — створює високий рівень провалу проекту відкритого банкінгу.

Рекомендується:

1. Чітко фіксувати в договорах: Вимушену відповідність рішення виключно стандарту Berlin Group NextGenPSD2 ver 2.1 ([Українська специфікація](#)).
2. Вимагати підтвердження: Конкретні приклади впровадження, незалежні висновки аудитів та демонстрацію всіх обов'язкових функціональних можливостей.
3. Віддавати перевагу виділеним рішенням: Розглянути архітектуру з розгортанням платформи відкритого банкінгу у власному захищеному периметрі банку для максималізації контролю та мінімізації ризиків, пов'язаних із ТО.

Час для прийняття обґрунтованих рішень обмежений. Коректний вибір є запорукою стабільності, безпеки та майбутніх конкурентних переваг.

З повагою,
Директор

Олександр Карпов

Додатки:

1. «Чому досвід вендора АБС не вичерпує вимоги до API-екосистеми?»
2. «Ver 1.4 BG Specs vs 2.1 BG Specs: Несумісність, яка коштуватиме часу і грошей»
3. «Ризики для ASPSP при використанні Технологічного Оператора (ТО) у хмарній SaaS-моделі»