

Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «КИЄВО-МОГИЛЯНСЬКА АКАДЕМІЯ»
Кафедра інформатики факультету інформатики

Демонстраційна частина до курсової роботи
за спеціальністю „Програмна інженерія” 6.050103

НА ТЕМУ

«Механізми захисту протоколу авторизації OAuth 2.0»

Керівник курсової роботи:
доцент, кандидат технічних наук
Ткаченко Олексій Миколайович

Виконав: студент групи ІПЗ-5
Ханін Максим Юрійович

Об'єкт, предмет і мета дослідження



Об'єкт

Процес роботи протоколу банківської авторизації OAuth 2.0

Предмет

Механізми захисту протоколу авторизації OAuth 2.0

Мета

Удосконалити механізми захисту протоколу OAuth 2.0 за рахунок підписання даних ЕЦП та шифрування.

Завдання дослідження

- Аналіз існуючих протоколів авторизації систем, їх характеристика та порівняльний аналіз.
- Виявлення переваг та недоліків застосування протоколу авторизації
- Формування рекомендацій щодо удосконалення механізмів захисту протоколу авторизації OAuth 2.0 шляхом підписання даних ЕЦП та шифрування



Актуальність роботи

Більша частина веб-додатків потребують ідентифікації користувача, але з різних причин користувач не хоче надавати логін та пароль маловідомому сервісу, що ставить під загрозу конфіденційність його даних. Також зручно знати лише один логін та пароль від одного сервісу, якому користувач довіряє, наприклад Google, Facebook або особистий кабінет веб-банкінгу. Однак, було зафіксовано ряд атак на вразливості існуючих протоколів авторизації. З цих причин постає необхідність пошуку й розробки більш надійного та швидкого способу авторизації.

Розділи дипломної роботи



Розділ 1

Нормативно-правове забезпечення. Аналіз існуючих протоколів авторизації, їх порівняльна характеристика.



Розділ 2

Схема роботи протоколу OAuth 2.0, переваги й недоліки. Формування рекомендацій для покращення роботи протоколу.



Розділ 3

Створення сервісу на основі протоколу з урахуванням запропонованих рекомендацій

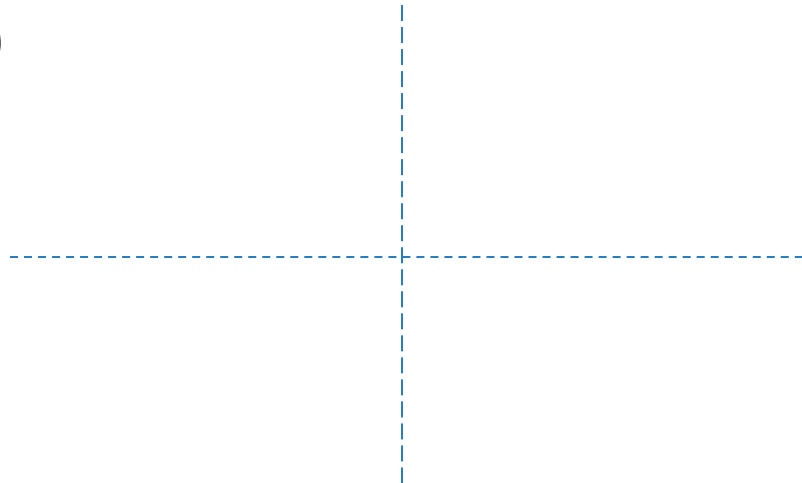
Існуючі протоколи авторизації

OAuth 1.0

OpenId

BrowserId

OAuth 2.0

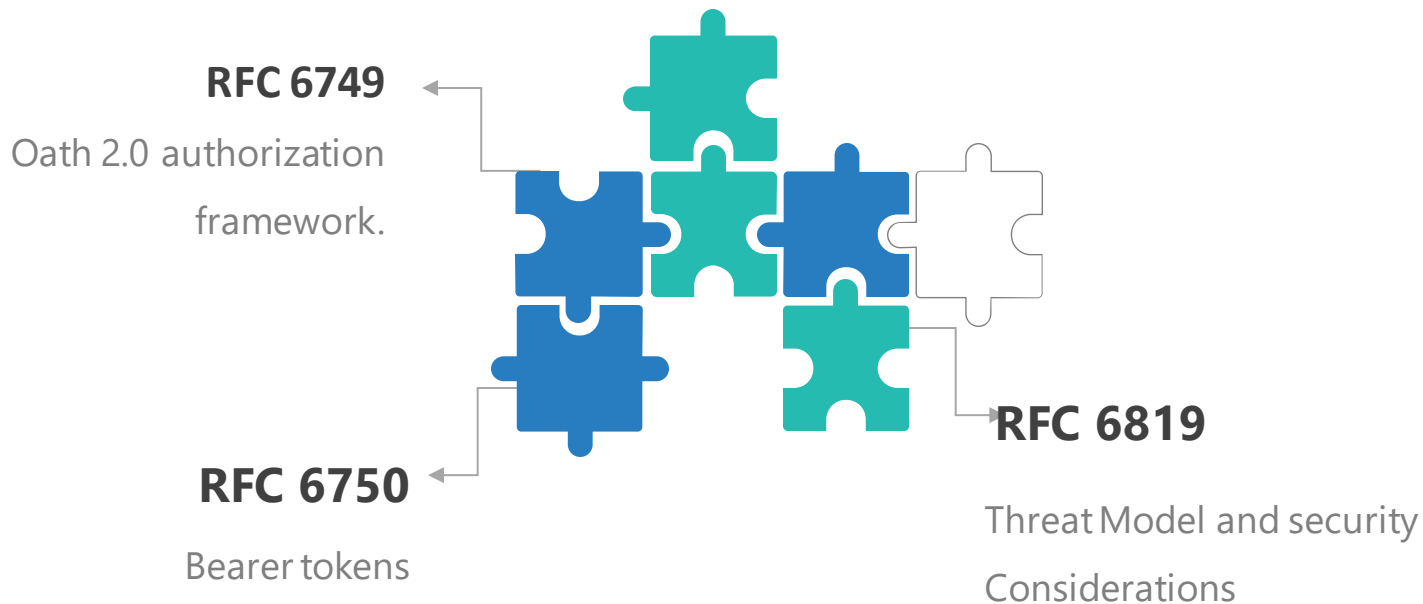


Порівняння найпоширеніших протоколів авторизації

	OpenId	Persona	OAuth 1.0	OAuth 2.0
Підтримка мобільних додатків	5	4	1	5
Зручність	3	4	3	5
Рівень захищеності	4	4	4	4
Підтримка серед сервісів	2	3	4	5

Нормативно-правове забезпечення

Стандарт RFC



Абстрактний опис протоколу авторизації OAuth 2.0

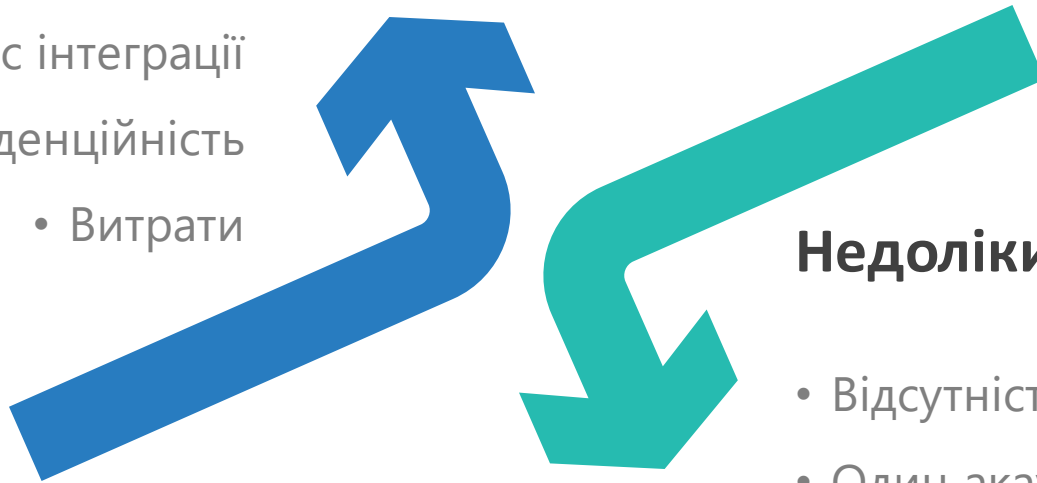


API SERVICE

Переваги й недоліки протоколу OAuth 2.0

Переваги

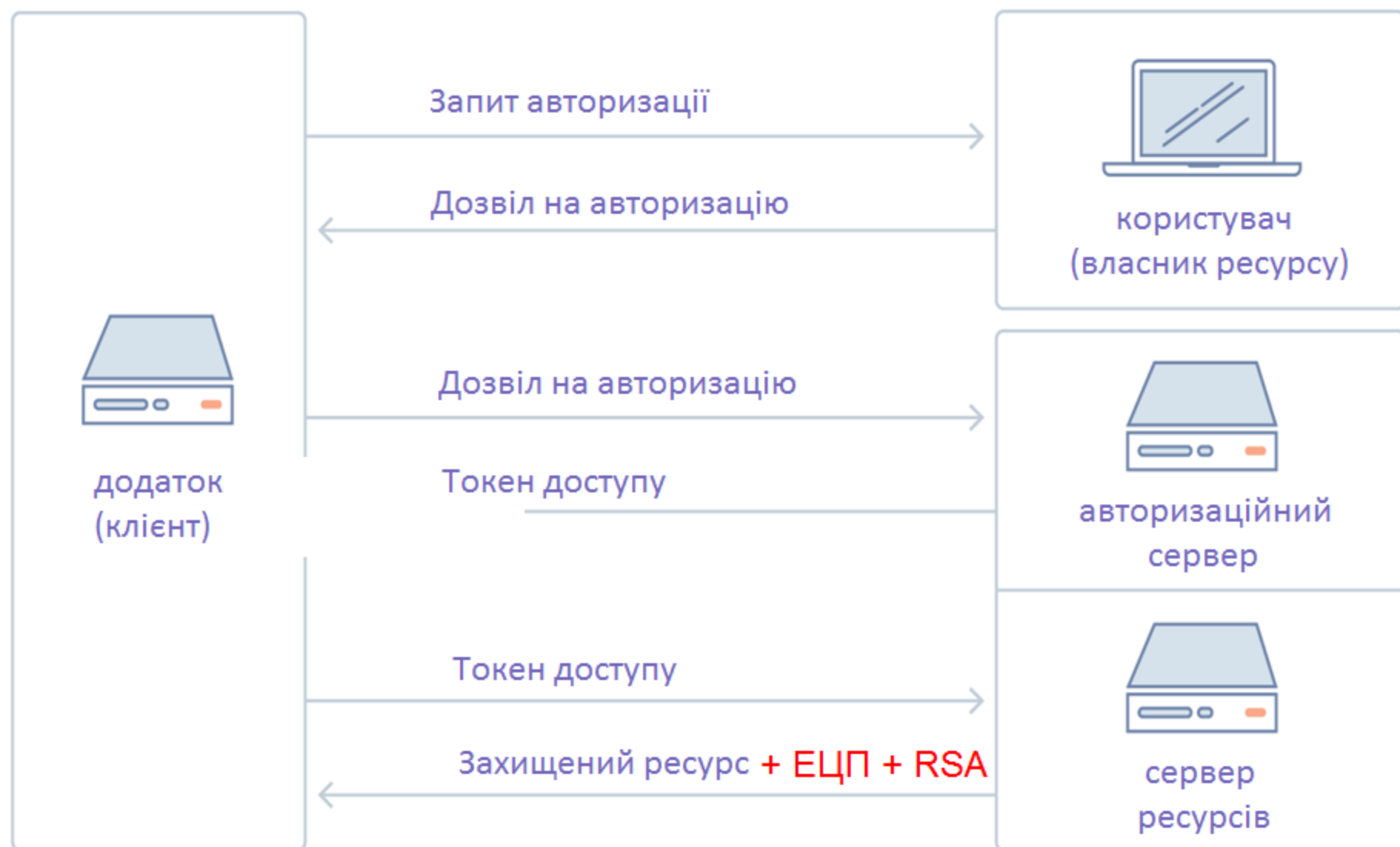
- Легкість
- Час інтеграції
- Конфіденційність
- Витрати



Недоліки

- Відсутність анонімності
- Один акаунт для багатьох сервісів
- Фішинг
- Ненасичений ринок

Рекомендації щодо покращення роботи протоколу OAuth 2.0



API SERVICE

Проект створення сервісу на основі потоколу OAuth 2.0

UserID

Спосіб електронної ідентифікації громадян через українські банки для надання адміністративних послуг через інтернет.

Цілі створення сервісу

Надійна та зручна верифікація користувача через його власний інтернет-банкінг на порталах адміністративних послуг.

Метод авторизації користувачів



OAuth 2.0

Проект побудований на основі протоколу OAuth 2.0



ЕЦП

У проекті дані підписуються ЕЦП для перевірки авторства.



Асиметричне шифрування

Для забезпечення конфіденційності даних в проекті використовується асиметричне шифрування за допомогою шифру RSA.

Використані технології

Клієнтська частина

- JavaScript ES6
 - HTML5
 - CSS3



Серверна частина

- C# Asp.Net Core WebApi
- Entity Framework
- PL-SQL

Застосування сервісу UserId

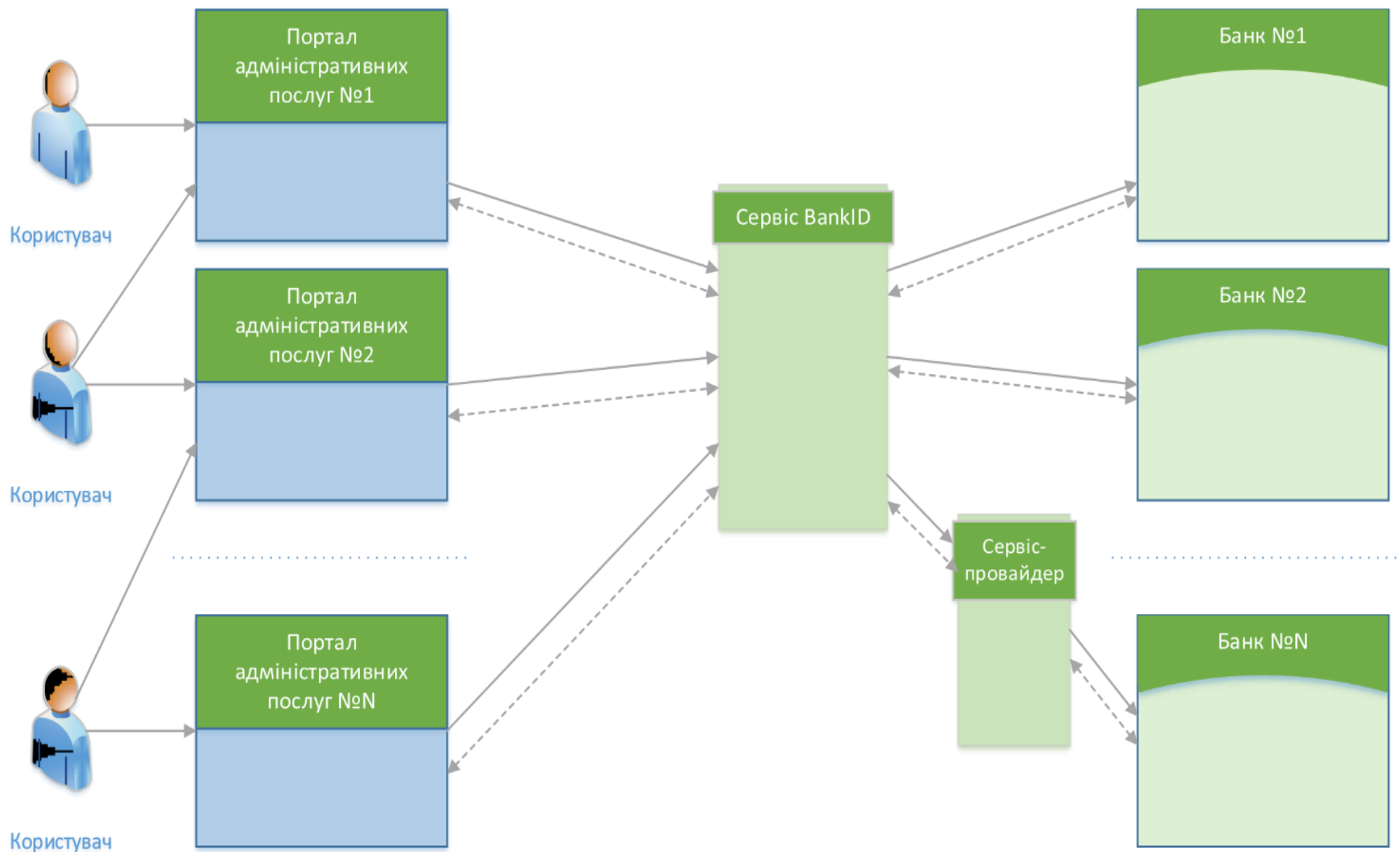
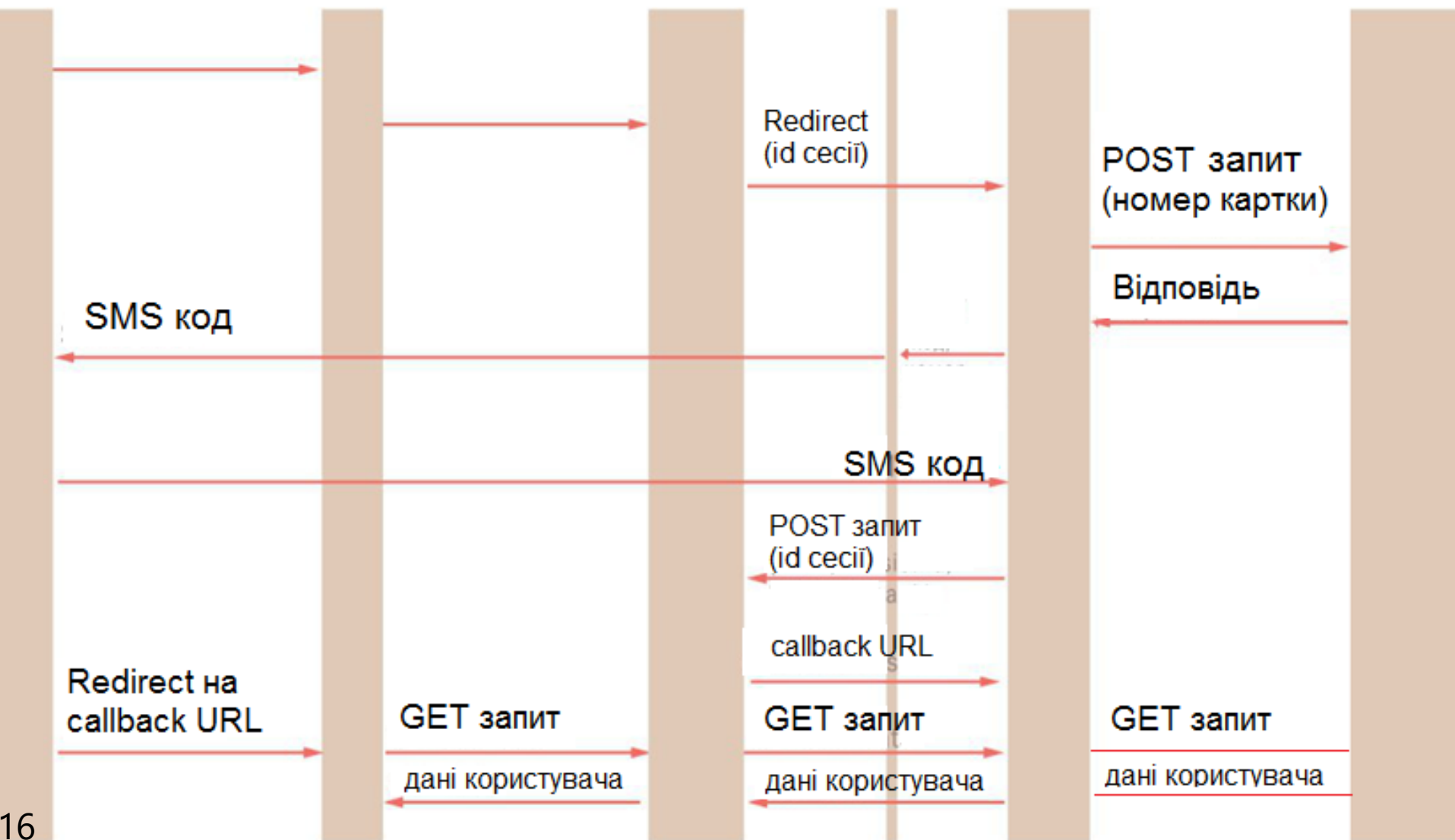


Схема роботи сервісу UserId

користувач ПАП НБУ SMPP UserId ПЦ банку



Висновки

- Проаналізовано існуючі протоколи авторизації.
- Проведено порівняльну характеристику протоколів.
- За рядом критеріїв обрано найперспективніший.
- Виявлено переваги й недоліки обраного протоколу.
- Сформовано рекомендації щодо удосконалення механізмів захисту протоколу OAuth 2.0 шляхом підписання даних ЕЦП та шифрування.
- За результатом проробленої роботи створено сервіс на основі протоколу з урахуванням запропонованих рекомендацій.
- Сервіс успішно розміщено на серверах та протестовано.
- Мета роботи досягнута.

Дякую за увагу!