LIMESYSTEMS

СИСТЕМА ІНТЕРНЕТ-БАНКІНГ «iTiny» для клієнтів банків

ПЕРШИЙ ВХІД В СИСТЕМУ

Огляд функціональності

Інструкція користувача

Version 2.11.0

2019

ЗМІСТ

1 АУТЕНТИФІКАЦІЯ В СИСТЕМІ 3
2 ОЗНАЙОМЛЕННЯ З ІНСТРУКЦІЯМИ 5
3 ПЛАНОВА ЗМІНА ПАРОЛЯ 6
4 ВАЖЛИВІ ПОВІДОМЛЕННЯ 7
5 СТВОРЕННЯ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ 8
6 ПІДПИСАННЯ ЕЛЕКТРОННИМ ЦИФРОВИМ ПІДПИСОМ 12

1 АУТЕНТИФІКАЦІЯ В СИСТЕМІ

Після того, як банк проведе реєстрацію користувача в системі, на номер телефону, вказаний в картці користувача, буде надіслано SMS з паролем першого входу.

Запустіть систему «iTiny» - відкриється стартова сторінка, призначена для аутентифікації користувача і входу в систему.

Для входу в систему введіть у відповідні поля (Рис. 1): **Логін** (встановлюється банком) і **Пароль** першого входу (з SMS-повідомлення з паролем). Введення значень можна виконати вручну з клавіатури або для забезпечення додаткової безпеки скористатися кнопкою виклику екранної клавіатури (Рис. 2).

УВАГА! Пароль чутливий до регістру букв.

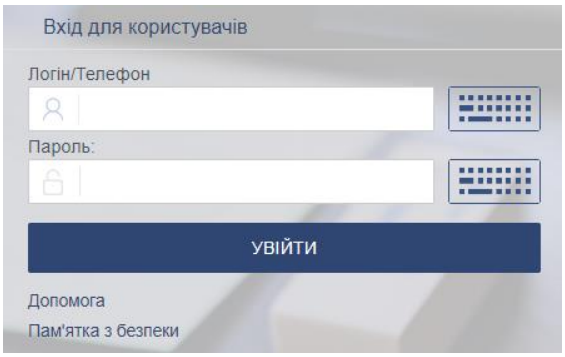

Рис. 1. Панель входу в систему (за логіном)

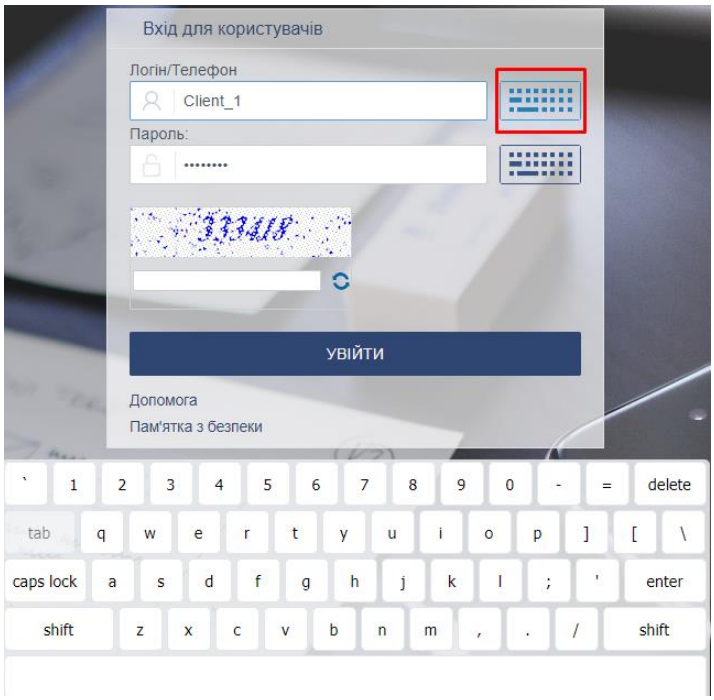

Рис. 2. Виклик екранної клавіатури

Залежно від налаштувань системи, для авторизації може бути включений додатковий захист в вигляді розпізнавання користувачем символів (CAPTCHA).

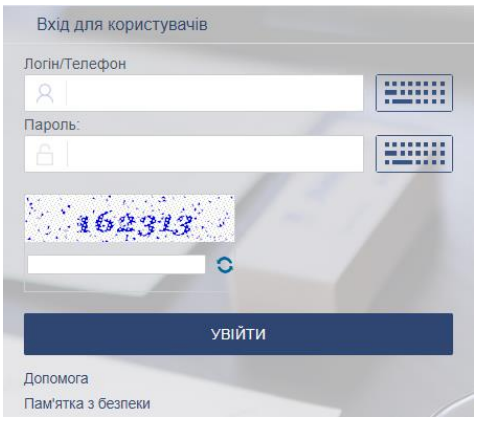

Рис. 3. Підтвердження CAPTCHA

Вхід в систему «iTiny» може також здійснюватися за **Номером телефону** користувача (Рис. 4). При введенні в поле **Логін/Телефон** номера телефону, система виконує пошук відповідного логіна за номером телефону, і авторизація відбувається за стандартною схемою через логін, але користувач цього не бачить. Якщо при пошуку логіна за телефоном було знайдено більше одного збігу, користувачеві виводиться повідомлення «Вхід за даним телефоном неможливий, введіть ваш логін або інший номер телефону».

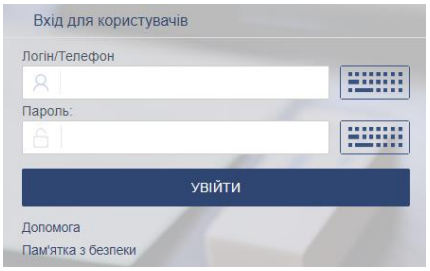

Рис. 4. Панель входу в систему (за логіном / телефоном)

Для завершення авторизації натисніть кнопку **<Ввійти>.**

У разі помилки при введенні логіна і/або пароля система видасть повідомлення «Неправильний логін або пароль!». Перевірте правильність введених даних і спробуйте ще раз спробу входу в систему.

Після 3-х невдалих спроб входу (кількість допустимих спроб може варіюватися в залежності від налаштувань системи), доступ буде повністю заблокований, на певний час.

Системою може бути передбачено підтвердження входу одноразовим паролем через SMS. У цьому випадку, після перевірки коректності введеного логіна/телефону і пароля, користувачеві буде відправлено SMS з кодом, який необхідно ввести в діалогове вікно підтвердження дії (Рис. 5) і натиснути **<Підтвердити>.**

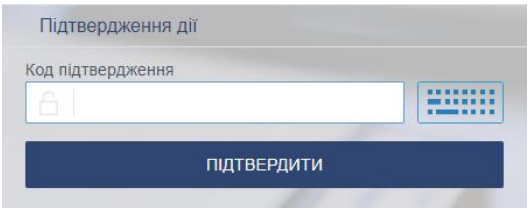

Рис. 5. Підтвердження одноразовим паролем

В результаті вдалого входу в систему на екрані відобразиться основна сторінка «iTiny».

2 ОЗНАЙОМЛЕННЯ З ІНСТРУКЦІЯМИ

Для нових користувачів після успішної авторизації відкривається сторінка зміни пароля з спливаючих пропозицією переглянути документацію (Рис. 6).

Якщо ви не хочете, щоб дане повідомлення виводилося надалі, встановіть прапорець «Не показувати».

При натисканні кнопки **<Перейти до інструкцій>** відкривається нова вкладка зі списком документації (розділ Меню **Допомога**), а на першій вкладці залишається сторінка зміни пароля (пропозиція переглянути інструкції закривається).

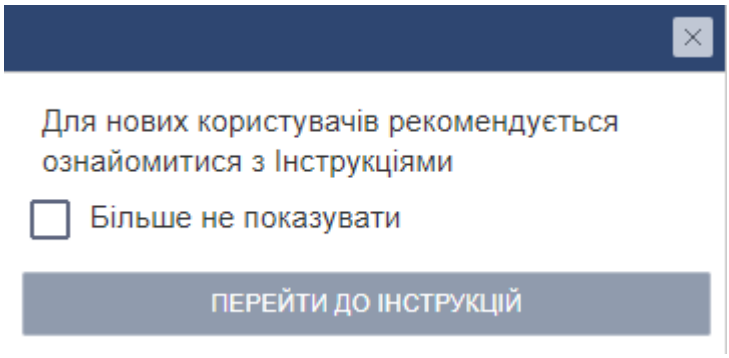

Рис. 6. Повідомлення «Перейти до інструкцій»

3 ПЛАНОВА ЗМІНА ПАРОЛЯ

При першому вході в систему «iTiny» користувач повинен змінити пароль першого входу на власний. Переміщення користувача по іншим сторінкам системи буде заблоковано до моменту зміни пароля.

УВАГА! Пароль першого входу, отриманий за допомогою SMS, має обмежений термін дії, по закінченню якого необхідно звернутися в банк для генерації нового.

Після успішної авторизації в системі відкриється сторінка налаштування профілю користувача (розділ Меню **Профіль → Профіль користувача**) на вкладці «Безпека».

В панелі зміни пароля (Рис. 7) в поле **Старий пароль** введіть пароль першого входу (з SMS), після чого введіть **новий пароль** у поле Новий пароль і продублюйте його в поле **Підтвердження**. Для завершення зміни пароля натисніть кнопку **<Зберегти>.**

П р и м і т к а : В залежності від налаштувань безпеки, може бути встановлено додаткове підтвердження одноразовим паролем з SMS.

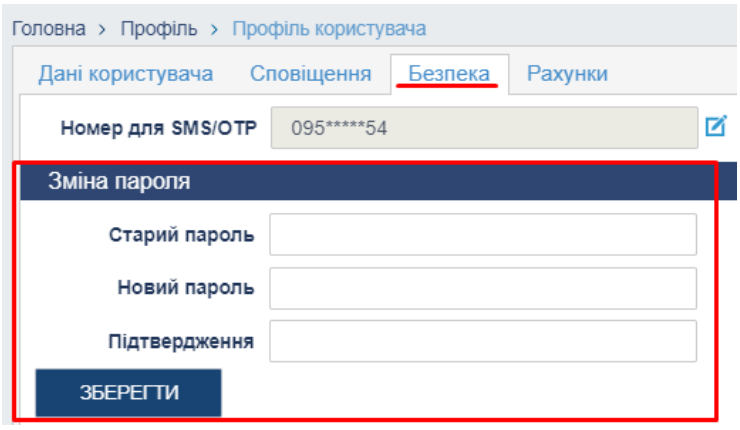

Рис. 7. Панель зміни пароля

Якщо спроба зміни пароля пройшла успішно, система видасть характерне інформаційне повідомлення.

4 ВАЖЛИВІ ПОВІДОМЛЕННЯ

Після обов'язкової зміни пароля, якщо банком передбачено важливі повідомлення, система перенаправить вас на сторінку з відображенням повідомлення від банку з позначкою «Важливе».

Важливі повідомлення є обов'язковими до прочитання і блокують подальшу роботу з системою. Після ознайомлення з текстом повідомлення, натисніть **кнопку <Позначити як прочитане>.**

Примітка: У тілі важливого повідомлення можуть бути присутніми файли-вкладення. Для перегляду вкладення, його необхідно клацанням мишки завантажити на робочий простір.

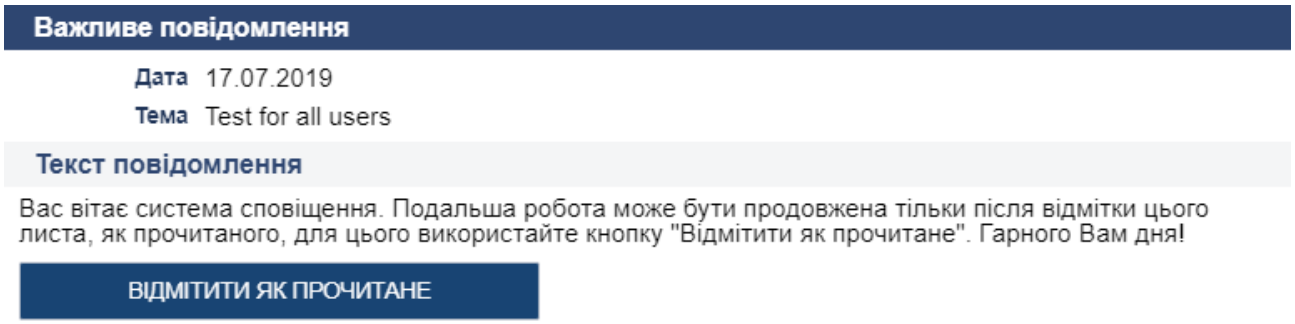

Рис. 8. Повідомлення обов'язкове до прочитання

5 СТВОРЕННЯ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ

Користуватися всіма основними функціями системи «iTiny» (будувати виписки, формувати документи, валютні заявки і т.п.) можна без ключа ЕЦП. Але для можливості підписання документів і відправки їх в банк, клієнт повинен створити ключ і чекати його сертифікації з боку адміністратора банку.

У системі передбачено поділ типів ключів в залежності від права підпису користувача (директор / головний бухгалтер), ці підписи називаються «Ключ першого підпису» і «Ключ другого підпису».

Для роботи з криптографічною системою електронних підписів, необхідно встановити і активувати Java-applet/Java Web Start, який використовується для зчитування ключів. Інформаційні повідомлення з інструкціями (Рис. 9, Рис. 10) допоможуть налаштувати Java-додаток створення ЕЦП в разі виникнення проблем.



Рис. 9. Інформаційне повідомлення при запуску операції з роботою ЕЦП

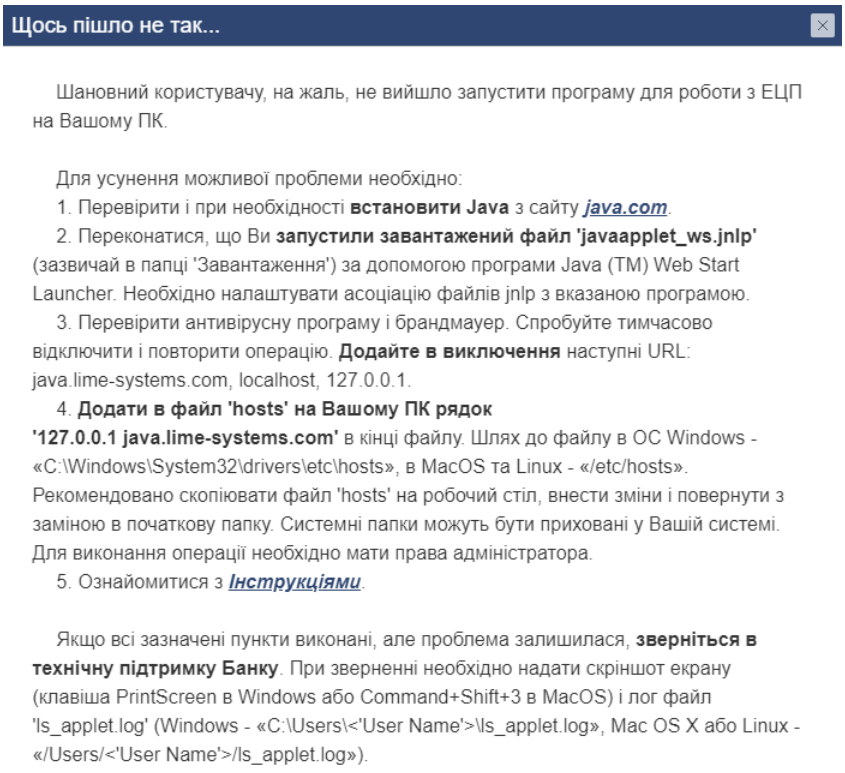

Рис. 10. Інформаційне повідомлення, в разі якщо операція по роботі з ЕЦП була запущена, але не виконана

Якщо поточний користувач має право підпису, після прочитання важливих повідомлень, система перенаправить його до модуля по роботі з ключами ЕЦП. Якщо автоматичне

перенаправлення не відбулося з якої-небудь причини, перейдіть вручну, скориставшись розділом Меню Система → Ключі або використовуйте швидкий перехід, натиснувши піктограму **«Ключі »,** розташовану у верхній частині екрану.

У системі передбачено поділ типів ключів в залежності від права підпису користувача (директор/головний бухгалтер), ці підписи називаються «Ключ першого підпису» і «Ключ другого підпису».

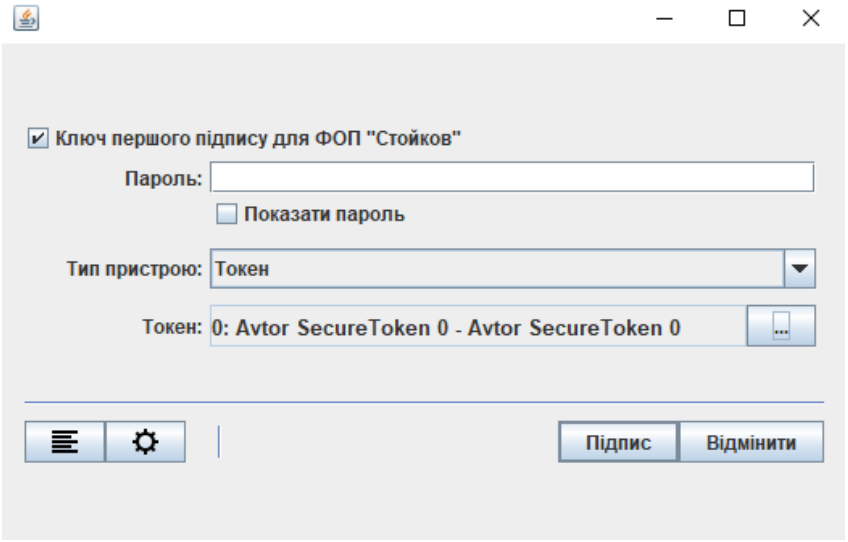

Рис. 11. Форма створення ключа ЕЦП

Для створення ключа натисніть кнопку <Створити новий ключ>. На екрані в окремому вікні відкриється Java-додаток створення ЕЦП, де користувач системи повинен:

- Обрати **Тип ключа**. Кількість зв'язків в випадаючому списку залежить від числа підприємств, до яких прив'язаний користувач і роль на них (перший / другий підпис на конкретному підприємстві).
- Створити **Пароль**, що складається з не менше 6-и символів. Пароль задається для підвищення надійності та захищеності ключа ЕЦП. Без знання пароля використання ключа неможливо.
- Ввести пароль повторно.
- Обрати **Тип пристрою**, де буде збережений ключ: як файл на диск або відкритий носій (флешку), або у вигляді токена на захищений носій (OTP-токен)
- Вказати **Шлях** для зберігання файлу (ключа).

Для завершення генерації ключа за вказаним шляхом і з зазначеним паролем, натисніть кнопку **<Згенерувати>.**

Після завершення операції вікно Java-додатку закриється - відбудеться закриття тільки графічного інтерфейсу користувача, Java-додаток залишиться запущеним в згорнутому стані системного трея в очікуванні нового звернення. При бажанні користувач може примусово закрити Java-додаток, який знаходиться в пасивному режимі, через контекстне меню.

Після того як ключ створений, інформацію про нього можна переглянути на сторінці розділу Меню **Система → Ключі.** До очікування сертифікації в банку ключ вважається не активним і його статус *Реєстрація* (підсвічується червоним кольором).

Тип ключа	Ключ 1 підпису	08.05.2019 11:29	04.11.2019 (залишилось 109 днів)
Власник	StoykovIV		
Ідентифікатор	5B1B38ED0511404880FAD6793A288F31	**Зареєстрований**	08.05.2019
Хеш	4960D14273BDAF6765D6CA82B6ABF880	**Стан**	Реєстрація

Рис. 12. Інформація про ключ

Подальша робота можлива тільки після процедури сертифікації ключа Адміністратором системи. Тому вам необхідно роздрукувати і надати в банк заяву на сертифікацію ключа.

Для виведення на друк сертифіката відкритого ключа ЕЦП натисніть кнопку **<Заявка на сертифікацію>**. Відкриється друкована форма сертифіката в режимі перегляду. Щоб роздрукувати заяву натисніть кнопку .

СЕРТИФІКАТ ВІДКРИТОГО КЛЮЧА ЕЦП КЛІЄНТА

"29" травня 2015 р.
(Дата реєстрації відкритого ключа ЕЦП клієнта)

ПІБ користувача	Директор Один Навсех
Контактні дані	adress@adress, 0503213212
Клієнт	еще тест (1011194)
Логін	DON

Відкритий ключ ЕЦП користувача

Ідентифікатор ключа ЕЦП	E4BF579997894E51BF10833B378C3398 (275)
Хеш	EC-E7-7A-36-CF-84-36-99-2E-46-30-84-BD-85-BB-01
Дата та час реєстрації	29.05.2015 12:45:05
Дата та час створення	29.05.2015 12:45:04
Тип ключа	1 підпис

Достовірність приведених даних підтверджую

Власник ключа ЕЦП	Уповноважений представник банку
П.І.Б	П.І.Б
Дата та підпис	Дата та підпис

Підписи
Директор Один Навсех

Рис. 13. Друкована форма сертифіката

Під час активації ключа в банку проводиться перевірка відповідності відкритого ключа, що знаходиться на стороні банку, і секретного ключа, що знаходиться у клієнта (переданого в банк у вигляді роздрукованого заяви). У разі успішної сертифікації ключ набуває стан *Активний* (підсвічується зеленим). Починаючи з цього моменту і протягом терміну дії ключів ЕЦП, ви можете використовувати ключі для відправки платежів і накладення підпису.

При роботі з ключами, перш за все, треба звернути увагу на наступні поля:

[Стан] Показує поточний стан ключа в банку. Відправлення платежів можливе тільки з ключами в стані «Активний».

[Ідентифікатор]	Унікальний ідентифікатор відкритого ключа. Саме за цим кодом з'ясовується, чи правильним ключем підписаний платіж і, відповідно, виконується перевірка відповідності з відкритим ключем в банку.
[Придатний до]	Показує дату закінчення дії ключа і кількість днів до закінчення терміну придатності ключа. Цей параметр необхідно тримати під контролем, так як після закінчення строку дії ключа, можливість підписувати документи буде втрачено.

Решта полей є довідковими і можуть бути використані при виникненні проблемних ситуацій.

В системі передбачений функціонал сповіщення про закінчення повноважень підписанта, за N днів до закінчення терміну повноважень. Включення/відключення даного функціоналу і значення терміну закінчення повноважень підписанта визначається налаштуваннями Адміністратора системи. Якщо функціонал включений, то за N днів до терміну закінчення повноважень підписанта:

1) Буде виведено повідомлення в інтерфейсі головної сторінки - на піктограмі «Ключи  » відобразиться спливаюче повідомлення «У вас закінчуються повноваження до ...».

2) При підписанні документів буде виводитися повідомлення «У Вас закінчуються повноваження до ..., надайте відповідні документи в Банк, до закінчення дії повноважень. В іншому випадку - по закінченню їх дії, Ваш ключ буде заблокований».

3) З наступної дати закінчення повноважень ключ буде автоматично блокуватися.

Для зручності, в системі «iTiny» реалізована функція самопідпису нових ключів, які були згенеровані замість тих, які втрачають свою актуальність після закінчення терміну придатності. Для цього, на сторінці ключів, необхідно натиснути кнопку **<Перегенерувати>** в поле потрібного ключа, пройти стандартну процедуру створення ключа, після чого активувати його, натиснувши кнопку **<Сертифікувати>** і підписати старим ключем.

6 ПІДПИСАННЯ ЕЛЕКТРОННИМ ЦИФРОВИМ ПІДПИСОМ

Необхідність накладення підпису задається налаштуваннями системи.

П р и м і т к а : Для клієнтів-юросіб, до яких прив'язано кілька користувачів з різними ролями (головного бухгалтера або директора) можуть бути встановлені умови мінімальної кількості підписів (наприклад, один перший і два других підписів), обов'язкових для відправки документа в банк, якщо тільки ці настройки не перевищують фактичну наявність співробітників з правом підпису.

Щоб підписати об'єкт, відзначте його і натисніть кнопку **<Підписати>** (Рис. 14).

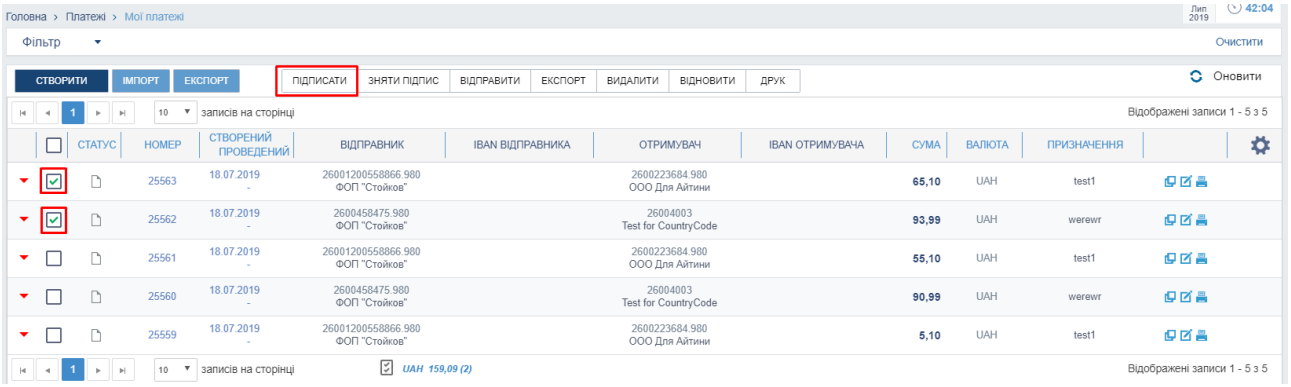

Рис. 14. Сторінка «Платежі → Мої платежі», виклик дії «Підписати»

На екрані відкриється вікно Java-додатку (Рис. 15).

Якщо користувач має більш ніж один тип ключа, або зв'язок з декількома клієнтами-юросібами, буде автоматично визначений даний зв'язок і виведений певний перелік ключів для підписання. Встановіть прапорець на необхідному типі ключа. Введіть **Пароль**, встановлений при генерації даного ключа (пароль чутливий до регістру). Виберіть **Тип пристрою**, на якому зберігається ключ (файл/токен). натиснувши кнопку ..., вкажіть **Шлях** до папки, де зберігається ключ. Натисніть кнопку **<Підпис>.**

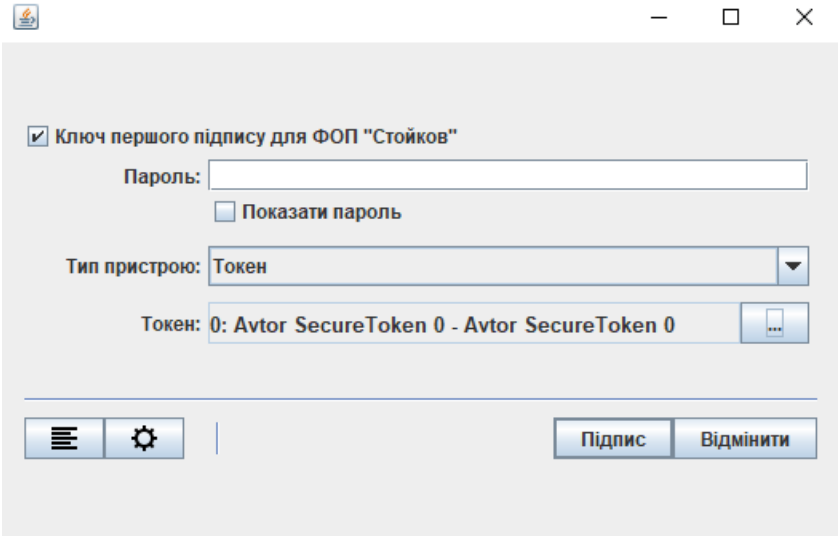

Рис. 15. Форма підпису ЕЦП

У разі успішної підпису, з'явиться відповідне повідомлення і обраний об'єкт змінить свій статус.

Якщо підписати об'єкт не вдалося, система видасть пояснює повідомлення. В даному випадку варто перевірити коректність введеного пароля або наявність ключа по заданому шляху.

УВАГА! Найменування файлу, де зберігається ЕЦП, має спеціальне, закодоване значення, в зв'язку з чим, щоб уникнути проблем при роботі з ключем, не рекомендується його перейменовувати.