



LIMESYSTEMS

СИСТЕМА ІНТЕРНЕТ-БАНКІНГ «iTiny»

МОДУЛЬ LS-CRYPT

Огляд функціональності

Інструкція користувача

Version 2.15.0

ЗМІСТ

1 ВИМОГИ ДЛЯ РОБОТИ З МОДУЛЕМ LS-CRYPT	3
1.1 НАЛАШТУВАННЯ ДЛЯ РОБОТИ З JAVAWEBSTART	3
2 СТВОРЕННЯ ЕЛЕКТРОНОГО ЦИФРОВОГО ПІДПISУ	6
3 ПІДПИСАННЯ ОБ'ЄКТІВ ЕЛЕКТРОННИМ ЦИФРОВИМ ПІДПИСОМ.....	10

1 ВИМОГИ ДЛЯ РОБОТИ З МОДУЛЕМ LS-CRYPT

Для роботи з модулем LS-Crypt необхідно наявність на комп'ютері користувача WEB-браузера і ПЗ Oracle Java.

1. При роботі з ЕЦП за технологією Java-applet:

- Браузер з підтримкою NPAPI (Java-applet):
 - Internet Explorer 11.
 - Mozilla Firefox (версії, які офіційно підтримуються розробником).
 - Safari (версії, які офіційно підтримуються розробником).
- ПЗ Oracle Java версій 7.x / 8.x .

2. При роботі с ЕЦП за технологією Java Web Start:

- WEB Браузер:
 - Internet Explorer 11.
 - Microsoft EDGE (версії, які офіційно підтримуються розробником).
 - Mozilla Firefox (версії, які офіційно підтримуються розробником).
 - Google Chrome (версії, які офіційно підтримуються розробником).
 - Opera (версії, які офіційно підтримуються розробником).
 - Safari (версії, які офіційно підтримуються розробником).
 - Інші сучасні браузери, які офіційно підтримуються розробником і відповідають сучасним стандартам.
- ПЗ Oracle Java вище версії Java 6.0.
- Додатково необхідно виконати налаштування, відповідно до опису в п. «Налаштування для роботи з JAWAWebStart».
- Встановлення останніх оновлень JAVA рекомендується, але не є обов'язковим умова використання.

П р и м і т к а : Вибір технології для підписання ЕЦП (Java-applet/Java Web Start), в залежності від підтримки браузера, визначається налаштуваннями Адміністратора.

1.1 Налаштування для роботи з JAWAWebStart

В першу чергу необхідно налаштувати асоціацію типу файлу і програми. Для цього відкрити **Пуск – Панель управління – Програми за замовчуванням**.

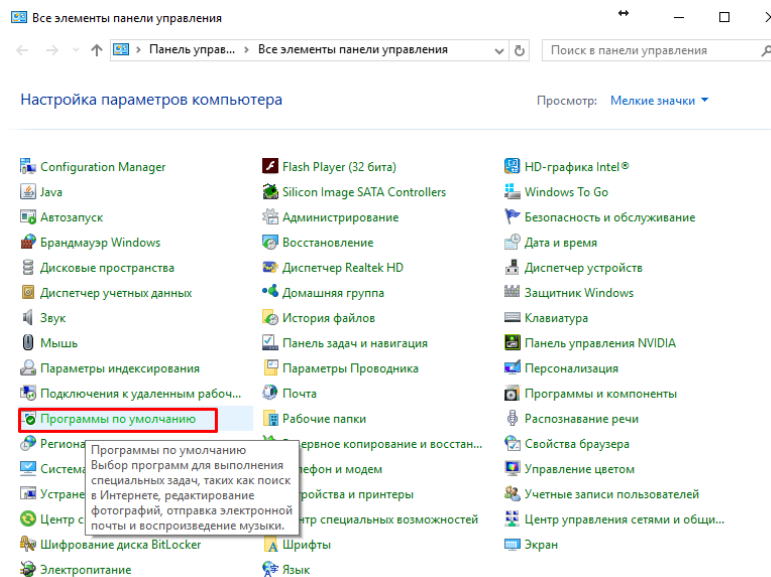


Рис. 1. Виклик діалогового вікна «Пуск - Панель управління - Програми за замовчуванням»

У діалоговому вікні вибрати пункт «Зіставлення типів файлів або протоколів з конкретними програмами».

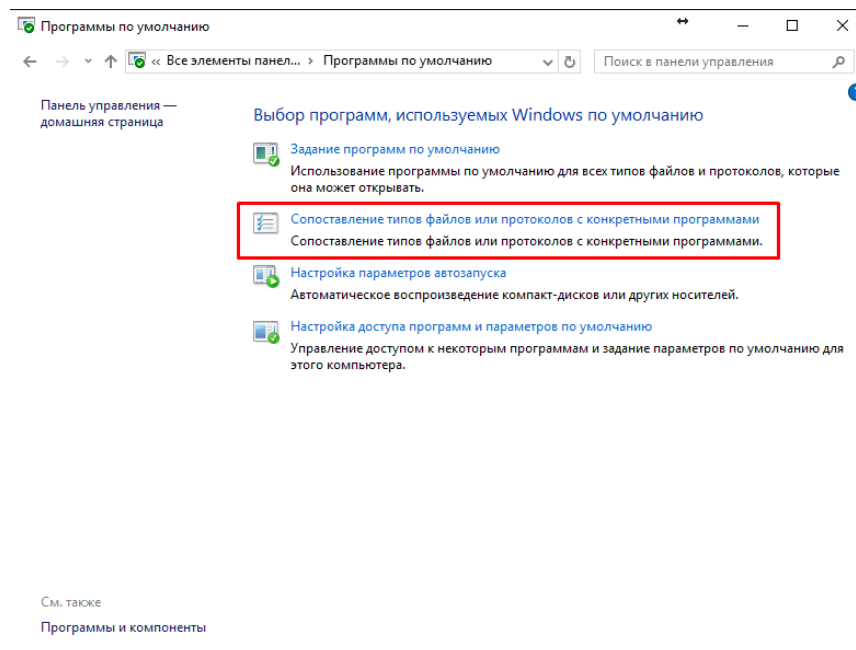


Рис. 2. Вибір пункту «Зіставлення типів файлів або протоколів з конкретними програмами»

У списку, вибрати розширення .jnlr і натиснути кнопку <Змінити програму >.

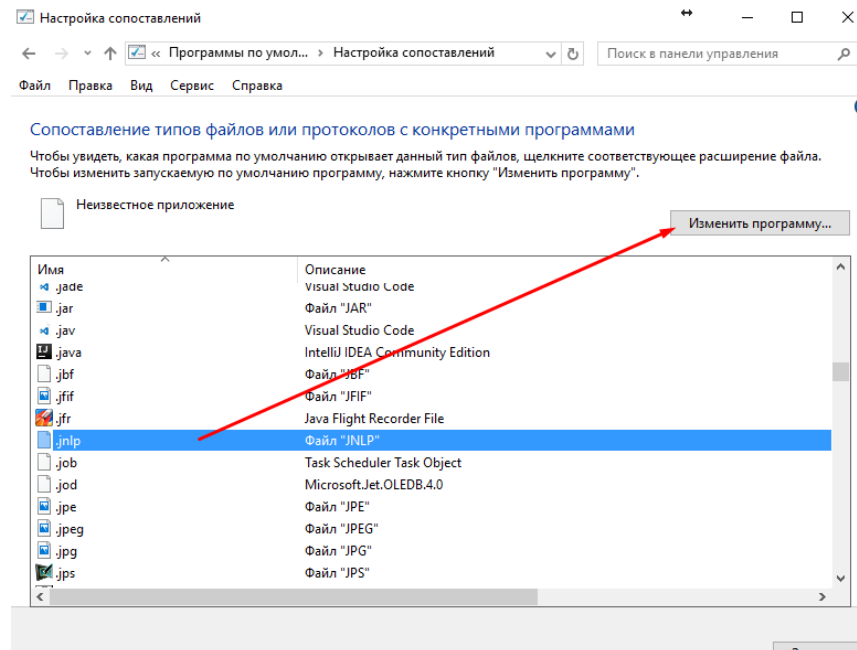


Рис. 3. Діалогове вікно «Зіставлення типів файлів або протоколів з конкретними програмами»

Зі списку обрати «Java(TM) Web Start Launcher» та натиснути кнопку **<OK>**.

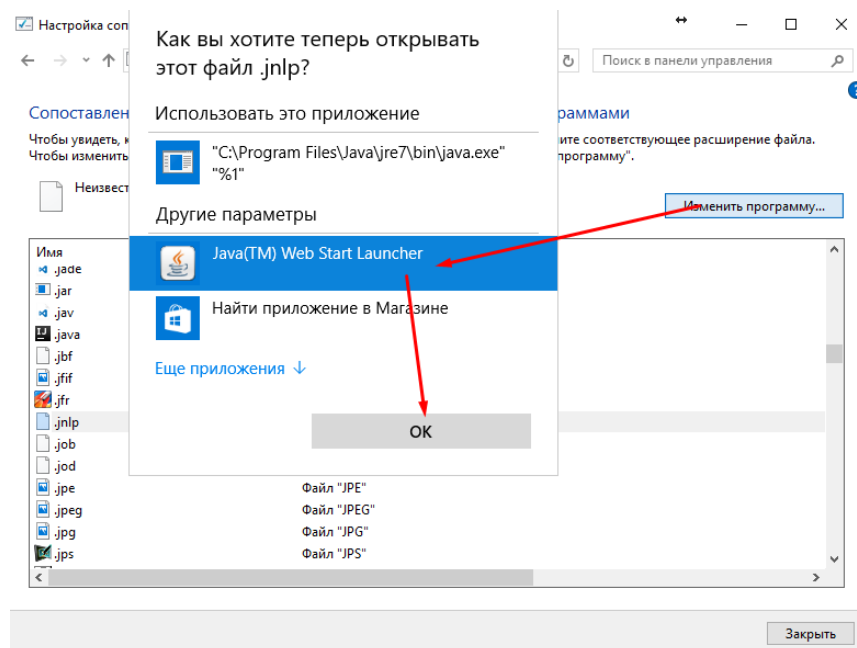


Рис. 4. Зіставлення файлів типу *.jnlp програмі Java(TM) Web Start Launcher

2 СТВОРЕННЯ ЕЛЕКТРОНОГО ЦИФРОВОГО ПІДПИСУ

Для роботи з криптографічною системою електронних підписів, необхідно встановити і активувати Java-applet / Java Web Start використовується для зчитування ключ.

При запуску операцій з роботою ЕЦП в разі виникнення проблем з'являться інформаційні повідомлення з інструкціями, які допоможуть налаштувати Java-додаток створення ЕЦП (Рис. 5, Рис. 6).

Додатково рекомендуємо ознайомитися з інструкцією: *iTiny2_Робота с Java_V2.15.0_RU.docx*



Рис. 5. Інформаційне повідомлення при запуску операцій з роботою ЕЦП

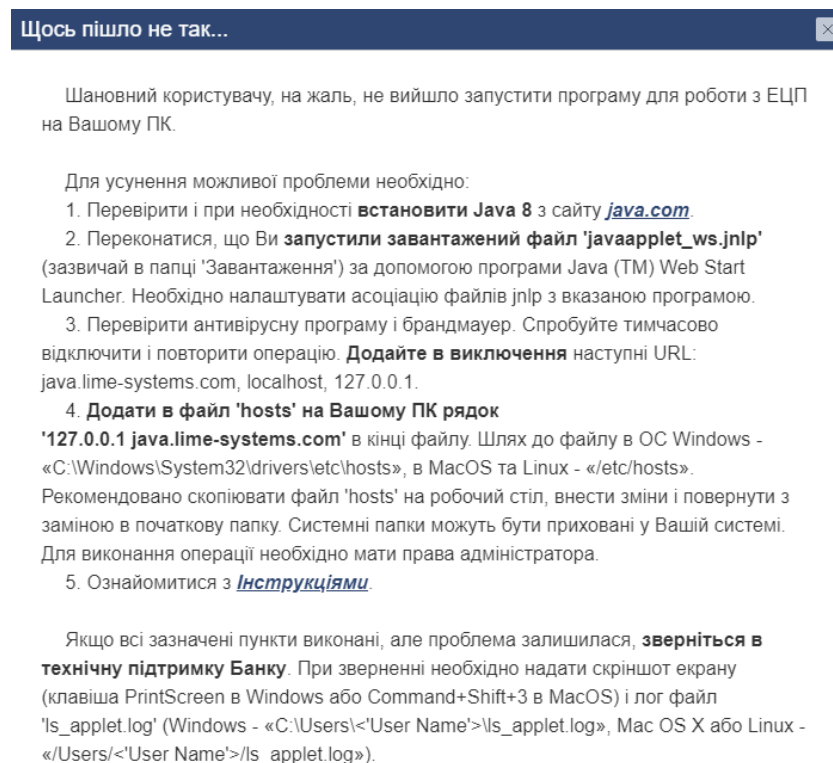



Рис. 6. Інформаційне повідомлення, в разі якщо операція по роботі з ЕЦП була запущена, але не виконана

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.

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

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 підписи), обов'язкових для відправки документа в банк, якщо тільки ці налаштування не перевищують фактичну наявність співробітників з правом підпису.

Налаштування і контроль ключей ЕЦП здійснюється в розділі Меню **Система → Ключи**.

П р и м е ч а н и е : Натягання піктограми «Ключи », розположеної в верхній правій частині екрана, здійснює швидкий перехід в розділ Меню **Система → Ключи**.

Для створення ключа натисніть кнопку **<СТВОРИТИ НОВИЙ КЛЮЧ>**. На екрані в окремому вікні відкриється Java-додаток створення ЕЦП (Рис. 7), де користувач системи повинен:

- Вибрати Тип ключа. Кількість зв'язків в випадяючому списку залежить від числа підприємств, до яких прив'язаний користувач і роль на них (перша / друга 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;
- Вибрати 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 до зберігання файлу(ключа). Файл надалі потрібен для накладання підпису на будь-який документ.

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

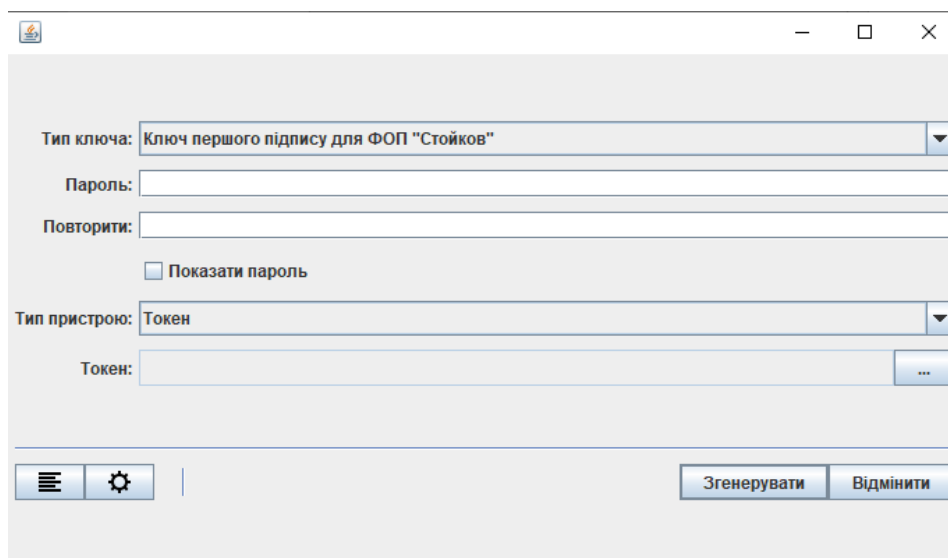


Рис. 7. Вікно Java-додатка створення ЕЦП (форма створення ключа ЕЦП)

Після завершення операції вікно Java-додатка 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, яке знаходиться в пасивному режимі, через контекстне меню.

Після того як ключ створений, інформацію про нього можна переглянути у вікні з розділу Меню **Система → Ключі**. Перш за все необхідно 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.

Інша інформація є довідковою та може бути використана при виникненні проблемних ситуацій.


До очікування сертифікації в банку ключ вважається не активним і його статус **Реєстрація** (підсвічується червоним кольором).

[СТВОРИТИ НОВИЙ КЛЮЧ](#)

	СТВОРЕНИЙ	ПРОСТРОЧЕНИЙ	
ФОП "Стойков" СтойковІV			
Тип ключа	Ключ 1 підпису	26.12.2019 12:50	23.06.2020 (залишилось 180 днів)
Власник	СтойковІV		
Ідентифікатор	EA6CDF03FB624B6CA815AF2D688D40B3	Зареєстрований	26.12.2019
Хеш	1AF82412A1D308D13F0E239B81F69D30	Стан	Реєстрація

Рис. 8. Інформація про ключі

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 **<Друк  >**.

СЕРТИФІКАТ ВІДКРИТОГО КЛЮЧА ЕЦП КЛІЄНТА	
"29" _____ травня _____ 2015 р. (Дата реєстрації відкритого ключа ЕЦП клієнта)	
ПІБ користувача	Директор Один Навсех
Контактні дані	address@address, 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 12:45:08
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. 9. Друкована форма сертифікату

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.

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

- 1) Буде виведено повідомлення в інтерфейсі головної сторінки – на піктограмі «Ключі» 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 «іTіny» 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 полі потрібного ключа, пройти стандартну процедуру створення ключа, після чого активувати його, натиснувши кнопку **<СЕРТИФІКУВАТИ>** і підписати старим ключем.

3 ПІДПИСАННЯ ОБ'ЄКТІВ ЕЛЕКТРОННИМ ЦИФРОВИМ ПІДПИСОМ

Необхідність накладення и кількість ЕЦП задається налаштуваннями системи. Для відправки об'єкта в банк, користувач повинен накласти всі необхідні підписи – статус «Повністю підписаний». Мінімальна кількість підписів для юридичної особи визначено статично – одна підпис. Максимальна кількість підписів залежить від кількості прив'язаних до підприємства користувачів з правом підпису. Банк має можливість, за дорученням підприємства налаштувати різну кількість необхідних підписів, для відправки об'єктів в банк.

П р и м і т к а : Оскільки система «іTiny» передбачає можливість зв'язку одного користувача з декількома підприємствами, дозволяючи працювати під одним логіном, відповідно у користувача може бути кілька ключів.

П р и м і т к а : Під час накладання ЕЦП, якщо користувач має більш як один тип ключа, або зв'язок з декількома підприємствами, буде автоматично визначена даний зв'язок і виведено певний перелік ключів для підписання.

Якщо настройками системи включено автоматичне підписання ЕЦП, то при створенні об'єкта буде доступна кнопка **<ЗБЕРЕГТИ І ПІДПИСАТИ>**. При натисканні цієї кнопки виконується збереження об'єкта і автоматичний виклик функції підпису.

Якщо настройками системи вимкнено автопідписання ЕЦП, до при створенні об'єкта буде доступна кнопка **<ЗБЕРЕГТИ>**. У цьому випадку, після створення та збереження об'єкта, необхідно функцію підпису викликати вручну. Для цього виберіть об'єкт / об'єкти зі списку, встановивши прапор , після чого натисніть кнопку **<ПІДПИСАТИ>**.

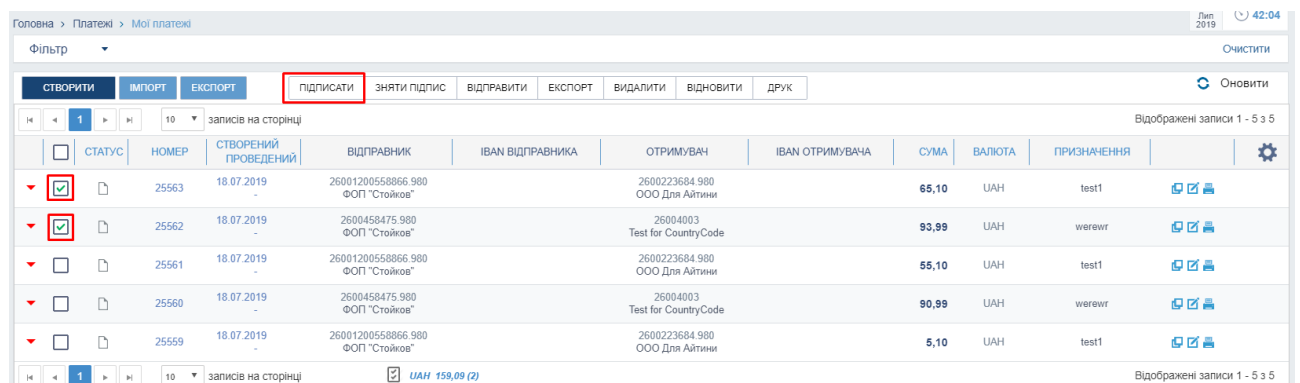


Рис. 10. Сторінка «Платежі → Мої платежі», виклик дії «Підписати»

При виконанні функції підписання на екрані відкриється вікно Java-додатка, в якому система запросить:

- Вибрати ключ, яким буде здійснений підпис. Встановіть прапорець на необхідному типі ключа.
- Введіть пароль, встановлений при генерації даного ключа (текстове поле, чутливе до регістру).
- Виберіть тип пристрою, на якому зберігається ключ (файл / токен).
- Вкажіть місце зберігання ключа, натиснувши кнопку (шлях вказується до папки, в якій зберігається ключ).

Натисніть кнопку **<Підписати>**.

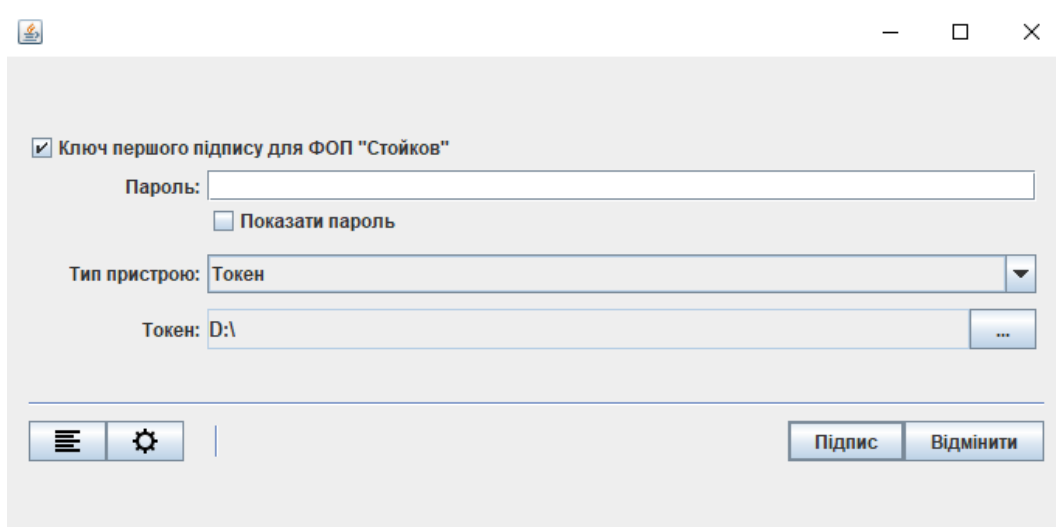


Рис. 11. Форма підпису ЕЦП

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

Якщо при спробі підписати документ або створити ключ відображається таке повідомлення (Рис. 12), необхідно натиснути на посилання «Встановити налаштування». відкриється сторінка **Профіль > Профіль користувача** і автоматично збережеться вільний порт в налаштуваннях користувача. Після чого можна повернутися до виконуваної дії.

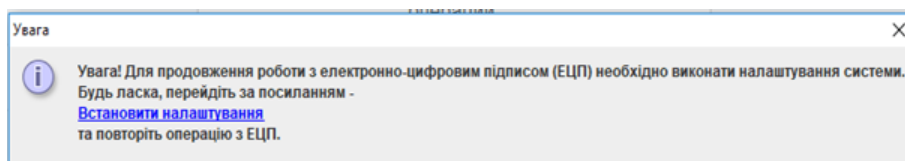


Рис. 12. Повідомлення при роботі з ЕЦП

Якщо підписати об'єкт не вдалося, система видасть попередження. 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.

Процес зняття підпису з об'єктів відбувається через кнопку **<ЗНЯТИ ПІДПИС>** і в цілому аналогічний процесу підписання.