LIMESYSTEMS

СИСТЕМА ІНТЕРНЕТ-БАНКІНГ «iTiny» для клієнтів банків

ПЕРШИЙ ВХІД В СИСТЕМУ

Огляд функціональності

Інструкція користувача

Version 2023.11

2023

ЗМІСТ

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.

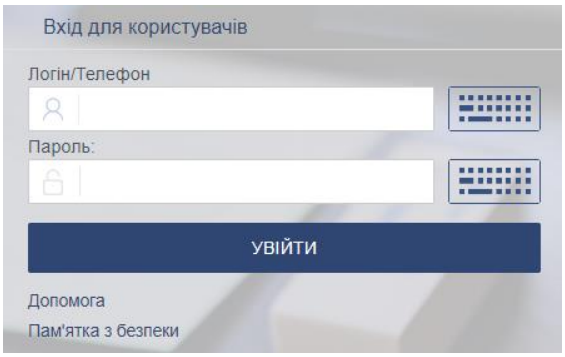


Рис. 1. Панель входу в систему (за логіном)

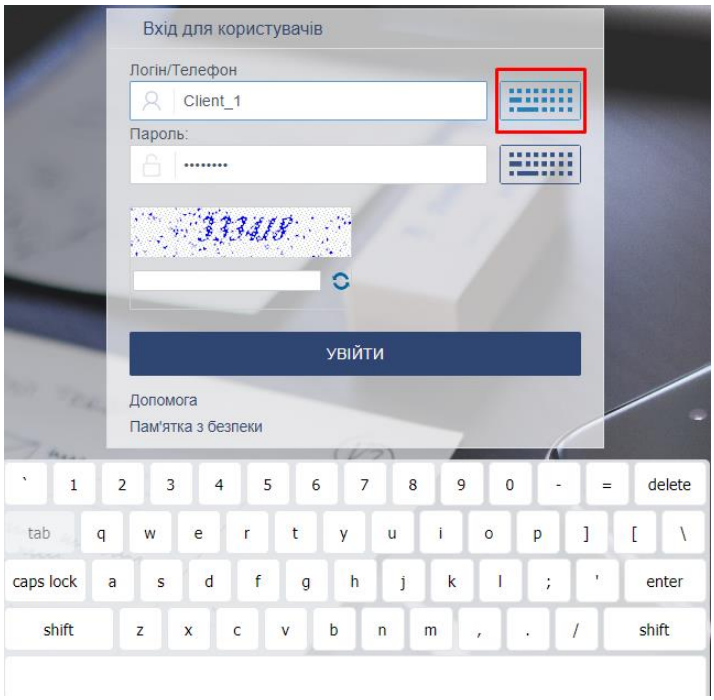


Рис. 2. Виклик екранної клавіатури

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

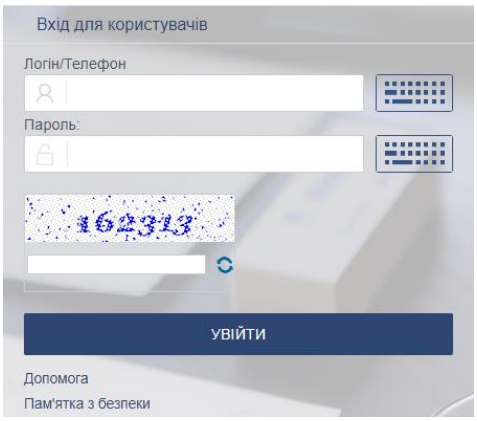


Рис. 3. Підтвердження CAPTCHA

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».

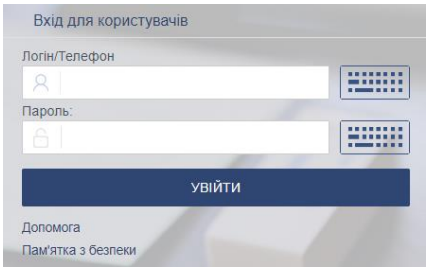


Рис. 4. Панель входу в систему (за логіном / телефоном)

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>.**

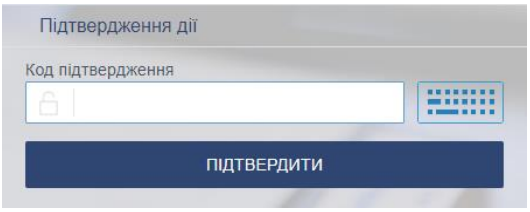


Рис. 5. Підтвердження одноразовим паролем

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).

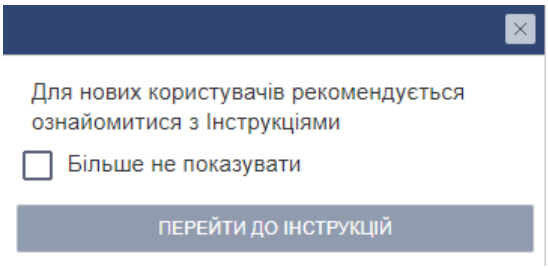


Рис. 6. Повідомлення «Перейти до інструкцій»

3 ПЛАНОВА ЗМІНА ПАРОЛЯ

При першому вході в систему «iTiny» користувач повинен змінити пароль першого входу на власний. Відкриється окрема сторінка примусової зміни пароля (Рис. 7). Переміщення користувача по інших сторінок системи буде заблоковано до моменту зміни пароля.

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.

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

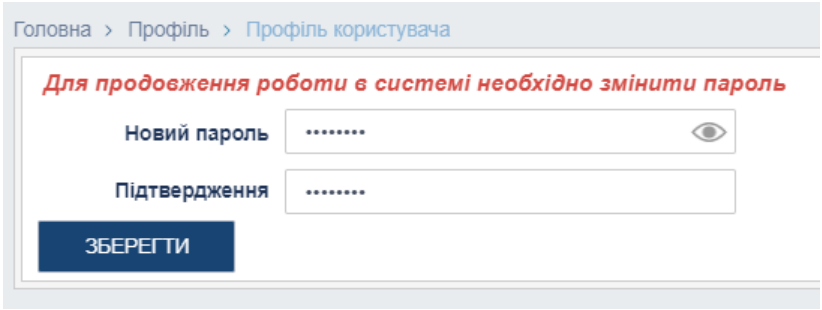


Рис. 7. Сторінка примусової зміни пароля при першому вході в систему

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>.**

П р и м і т к а : У тілі важливого повідомлення можуть бути присутніми файли-вкладення. Для перегляду вкладення, його необхідно клацанням мишки завантажити на робочий простір.

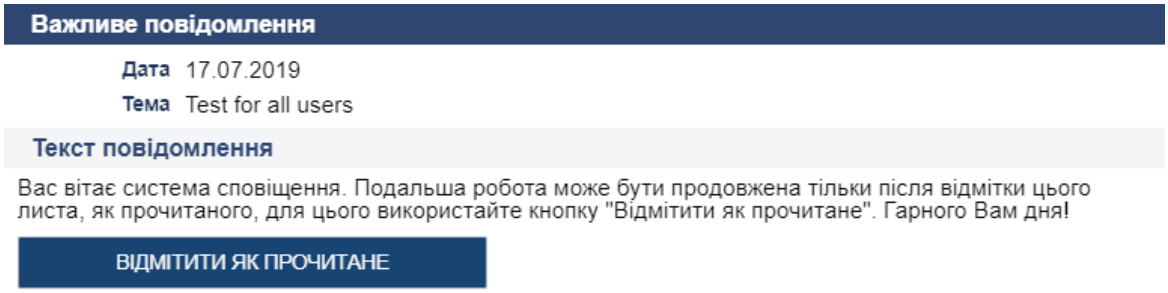


Рис. 8. Повідомлення обов'язкове до прочитання

5 Реєстрація файлового ключа в системі

Для роботи з КЕП в інтернет-банкінгу iTiny, попередньо необхідно зареєструвати ключ в системі.

Для цього необхідно:

1. Перейти у розділ Система -> Ключі за допомогою іконки ключа справа зверху.
2. Натиснути кнопку «Зареєструвати ключ».

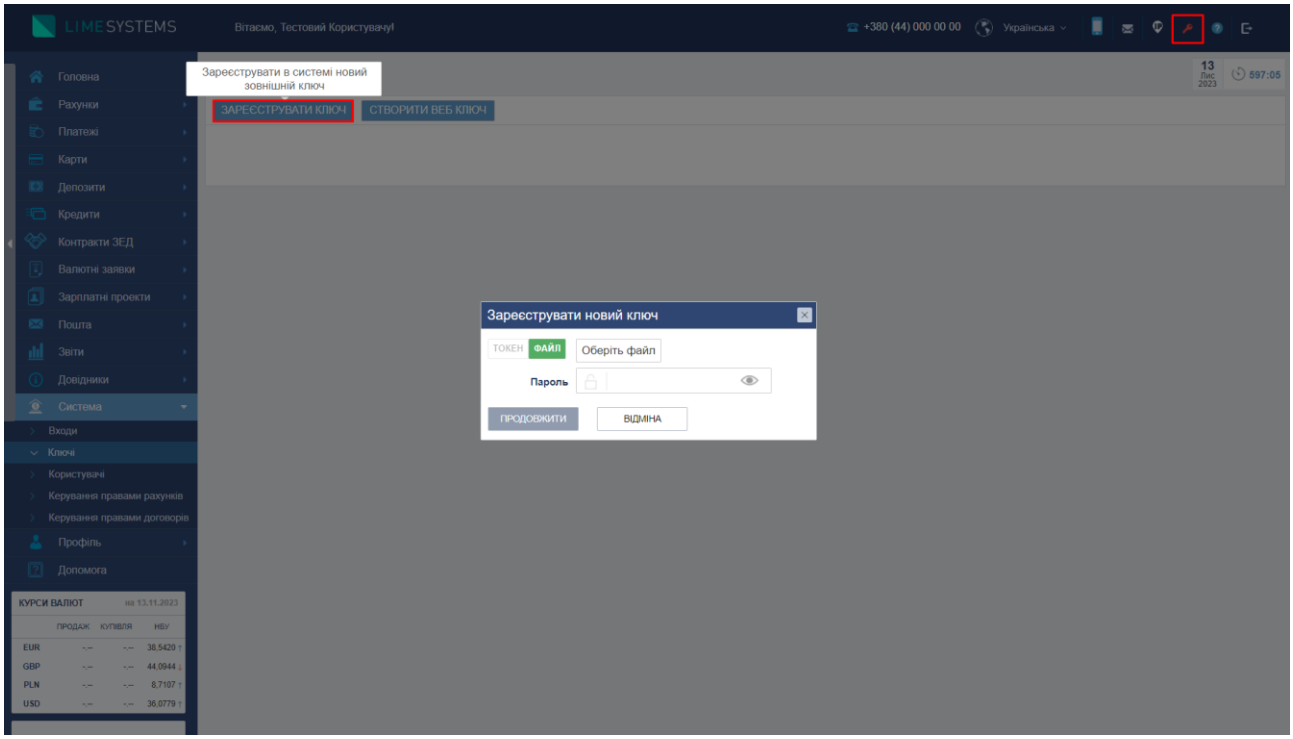


Рис. 9. Натискання кнопки «Зареєструвати ключ»

3. Обрати носій обраного ключа: файл або токен.

Примітка: при використанні токену (захищений носій) необхідно додатково встановити ПЗ «IIT Користувач. Агент підпису», детальніше в п.6.

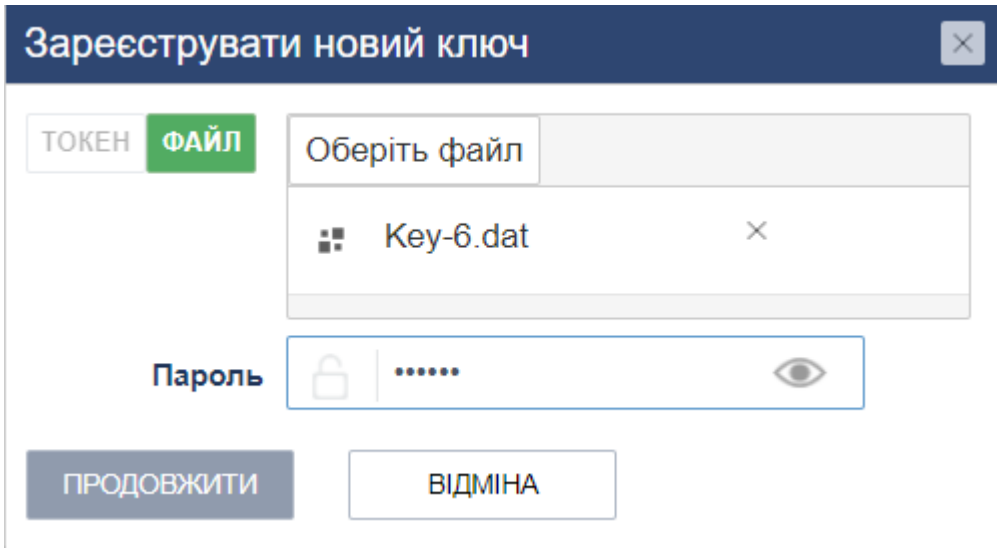


Рис. 10. Вибір файлу ключа для реєстрації

4. Ввести пароль до ключа.
5. Натиснути «Продовжити».
6. Після цього з’явиться вікно з підтвердженням реєстрації, де описаний власник ключа та підприємство.

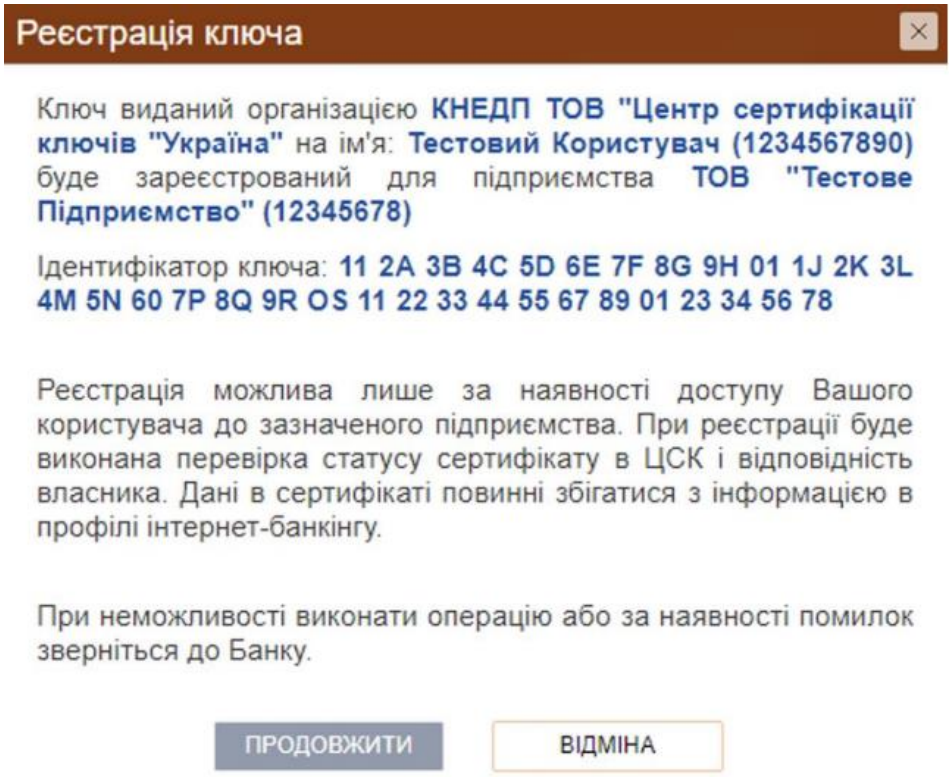


Рис. 11. Інформація про власника ключа

7. Натиснути «Продовжити».
8. Підтвердити реєстрацію одноразовим паролем з SMS.

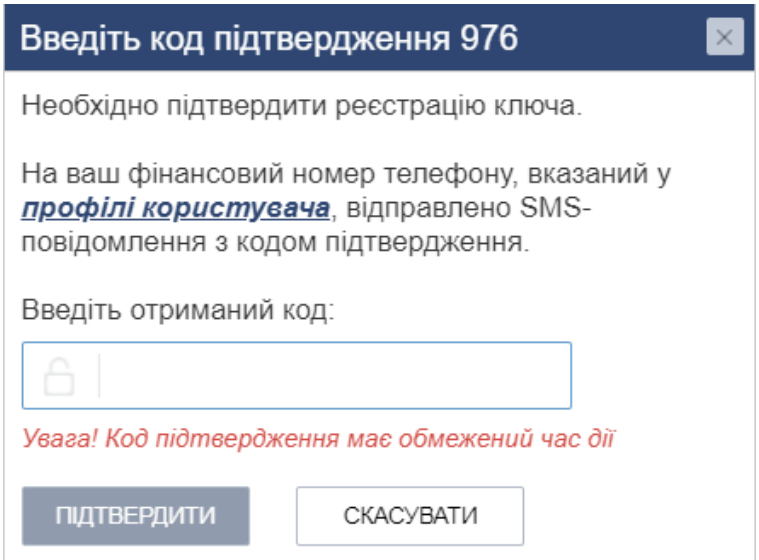


Рис. 12. Підтвердження реєстрації ключа

6 Робота з захищеними носіями

Для роботи з КЕП на захищеному носії (токену) попередньо необхідно встановити спеціалізоване програмне забезпечення компанії ІІТ, постачальника криптографічних бібліотек.

Є два варіанти використання:

- плагін для браузеру (рекомендується)
- ПЗ "Агент підпису" (часто використовується на ПК для роботи з державними сервісами)

Далі, покроково описано налаштування обох варіантів

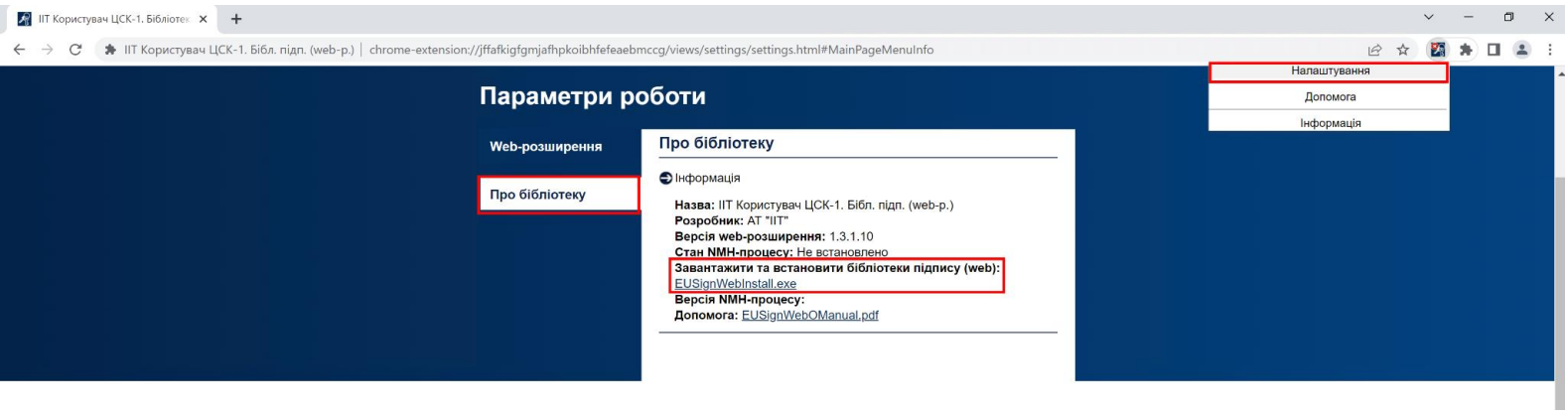
6.1 Налаштування розширення браузера

1. Встановити розширення ІІТ для браузеру:

- Google Chrome, Microsoft Edge, Opera - [IIT End User CA-1. Sign (web-extension)]
- Firefox - https://eu.iit.com.ua/download/productfiles/eusw@iit.com.ua.xpi

2. Після встановлення розширення, необхідно встановити web-бібліотеки підпису.

Для цього можна перейти за посиланням через налаштування розширення:



або за посиланнями нижче:

Windows - https://iit.com.ua/download/productfiles/EUSignWebInstall.exe
Mac - https://iit.com.ua/download/productfiles/EUSignWebInstall.pkg
Linux x64 - https://iit.com.ua/download/productfiles/euswi.64.tar
Linux x86 - https://iit.com.ua/download/productfiles/euswi.tar

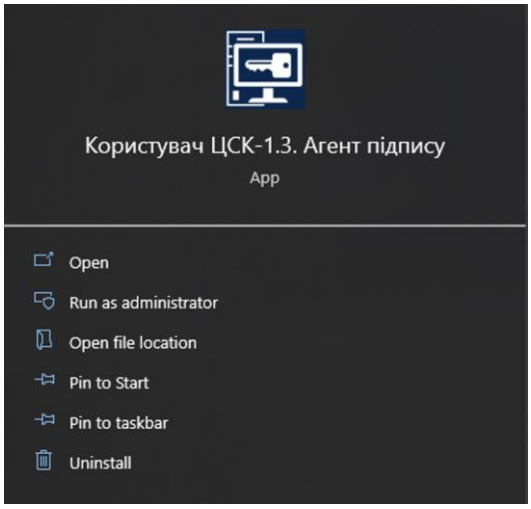
3. Встановити завантажений файл.

6.2 Налаштування агента підпису

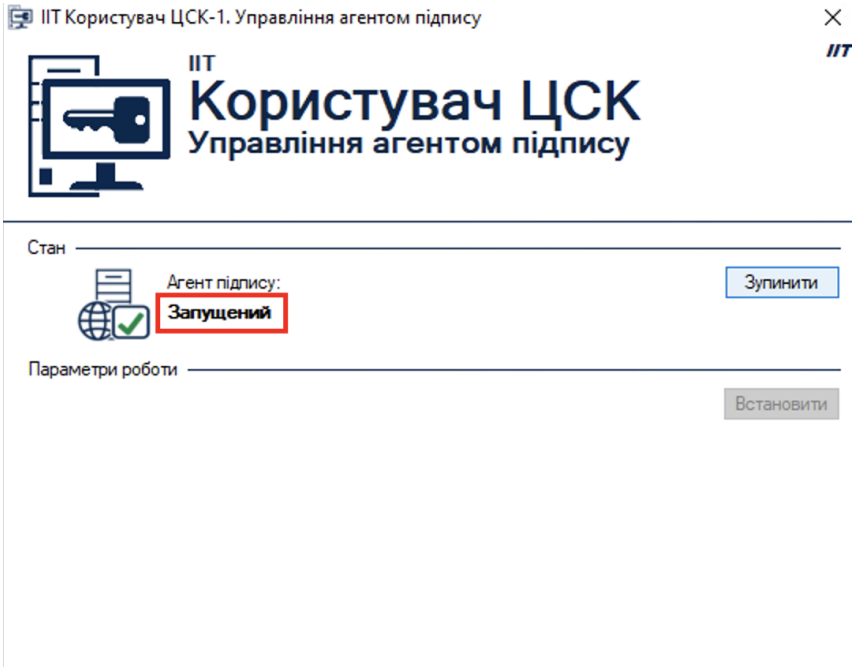
1. Встановити web-бібліотеки підпису.

Windows - https://iit.com.ua/download/productfiles/EUSignWebInstall.exe
macOS - https://iit.com.ua/download/productfiles/EUSignWebInstall.pkg
Linux x64 - https://iit.com.ua/download/productfiles/euswi.64.tar
Linux x86 - https://iit.com.ua/download/productfiles/euswi.tar

2. Запустити застосунок Агент підпису:



3. У застосунку натиснути кнопку Запустити, перевірити, що статус – «Запущений».



Після встановлення ПЗ IIT, продовжити реєстрацію ключа, як в п.5.