ТОВ «САЙФЕР ПРО»
Адреса: 04107, Київ, вул. Нагірна, 25-27
Тел.: +38 044 484 46 12, 484 46 17
E-mail: info@cipher.com.ua

Системи захисту інформації
www.cipher.com.ua

Мережний криптографічний модуль Шифр-HSM

Інструкція користувача для налаштування Сайфер Шифр-HSM в ІІТ Користувач

ЗМІСТ

СПИСОК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАЧЕНЬ

CMP	Certificate management protocol
HSM	Hardware security module
PIN	Personal Identification Number
PKCS#10	Certification Request Syntax Specification
ІІТ	Інститут інформаційних технологій
МКМ	Мережний криптографічний модуль
ОС	Операційна система

ПІДГОТОВКА РОБОЧОГО МІСЦЯ

Встановлення IIT Користувач

Завантажити з офіційного сайту IIT дистрибутив – Користувач центру сертифікації ключів. Інсталяційний пакет (ОС Microsoft Windows), або одразу завантажити файл за посиланням.

Встановлення та налаштування клієнтської бібліотеки

Отримати від розробника Сайфер Шифр-HSM набір бібліотек чи дистрибутив setup_CiHSM_Client.exe з набором бібліотек.
Пакет містить набір файлів, наприклад, для архітектури x86-64.

Назва	Опис
cihsm.dll	PKCS#11 бібліотека для роботи з Мережним криптографічним модулем "Шифр-HSM"
libcrypto-1_1.dll	Бібліотека залежностей
libssl-1_1.dll	Бібліотека залежностей
pkcs11_tester.exe	Тестова утиліта, яка дозволяє здійснити перевірку доступність і працездатність МКМ

Налаштування IIT Користувач

Розміщення клієнтських бібліотек

Перейти за шляхом:

```
C:\Program Files (x86)\Cipher\CiHSM_Client\PKCS11\Win
```

та скопіювати повний вміст папки у папку, де розміщуються бібліотеки для роботи з IIT Користувач:

```
C:\Program Files (x86)\Institute of Informational Technologies\Certificate Authority-1.3\End User
```

Варто зауважити, що бібліотеки мають бути тієї розрядності, як і IIT Користувач, на даний момент це x86.

Вказівка CMP-серверу ЦСК

Для того, щоб вказати адресу, треба запустити IIT Користувач, перейти за шляхом «Встановити параметри» - «CMP-сервер» - вказати позначку «Використовувати CMP-сервер».
В даному випадку використовується Тестовий ЦСК Сайфер, то адреса буде наступна

```
http://ca39.cipher.com.ua/cmp
```

Натискаємо «Ок» для збереження змін.

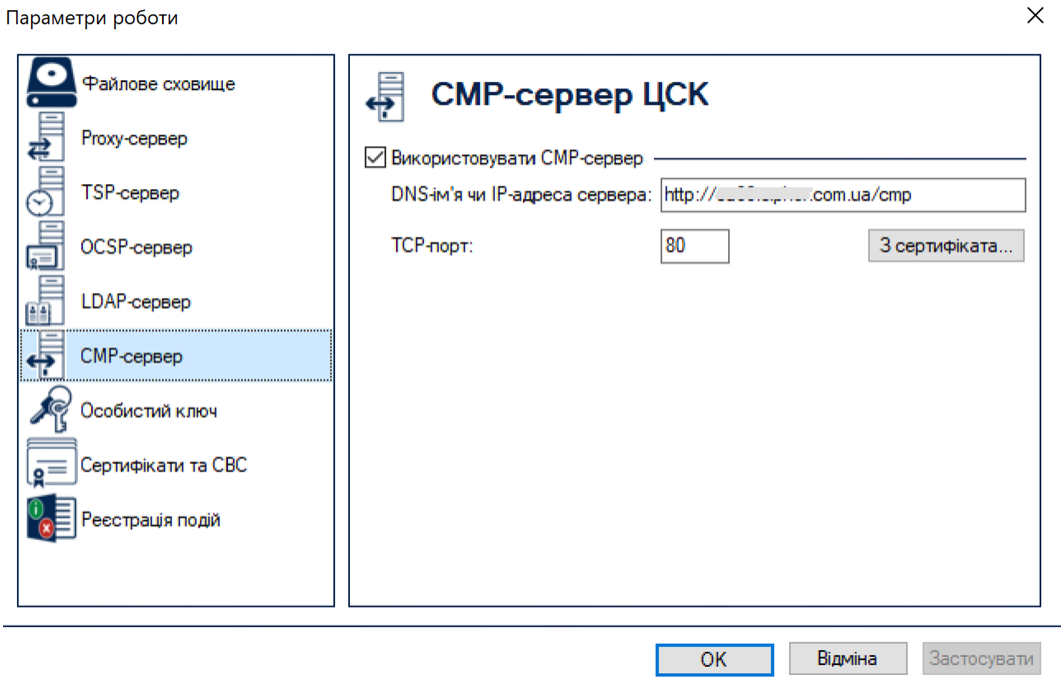

Рис. 1. Налаштування параметрів CMP-серверу ЦСК

Налаштування бібліотеки для ОС Windows

Для роботи бібліотек, які було скопійовано раніше, вказується адреса і порт МКМ у захищеній мережі МКМ через створення змінної середовища ОС.

В ОС Windows переходимо у "Властивості системи", розділ «Змінні середовища», Рис. 2-4.

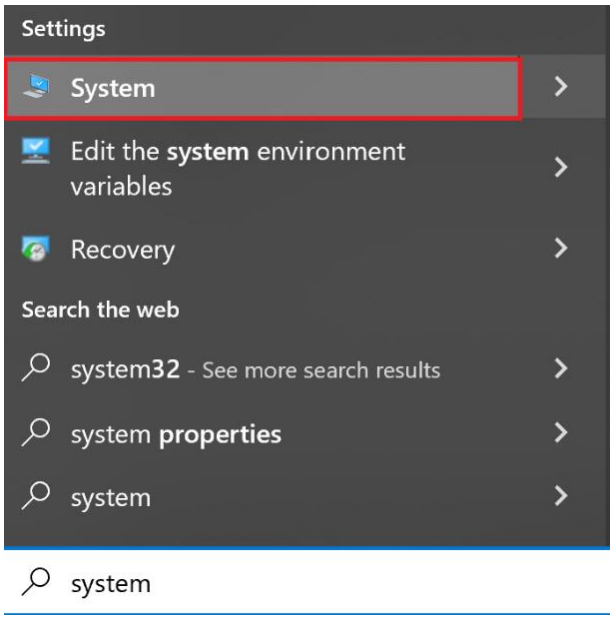

Рис. 2. Пуск "Зміна системних змінних середовища"

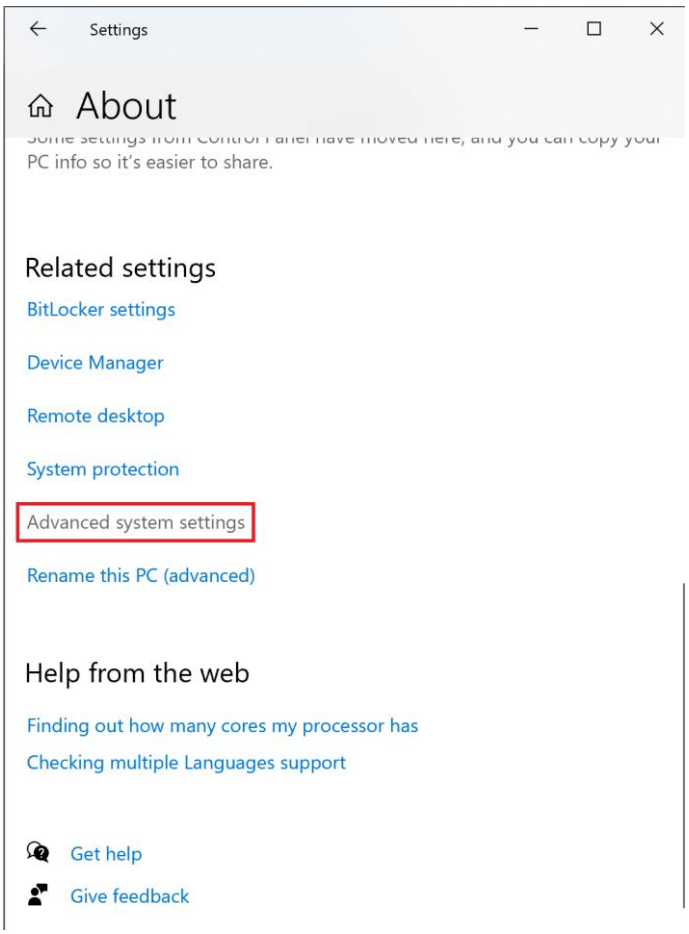

Рис. 3. Змінні середовища

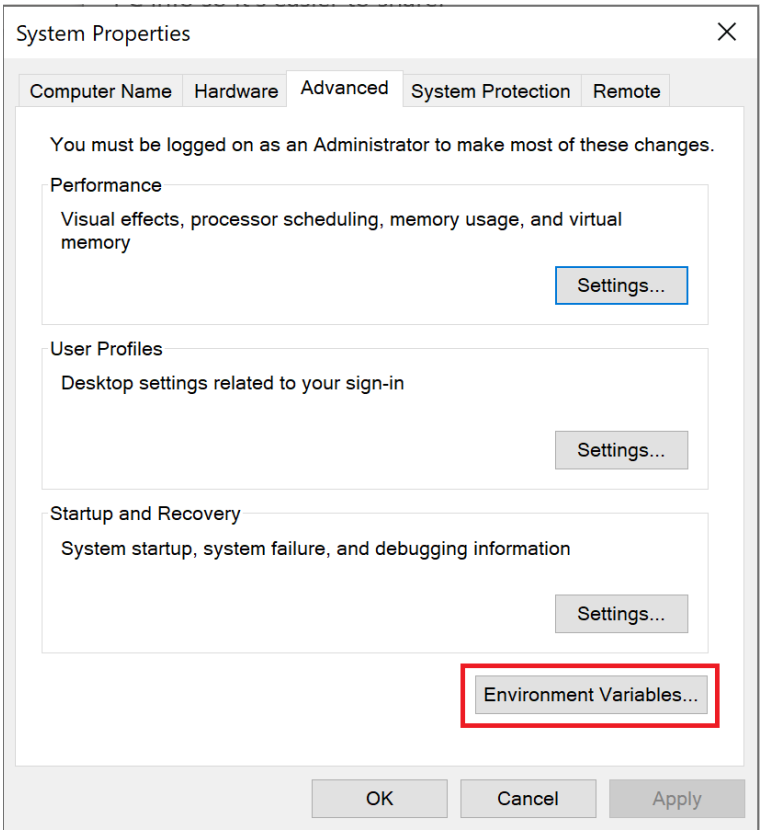

Рис. 4. Змінні середовища

Далі, створюємо нову змінну, Рис. 5.

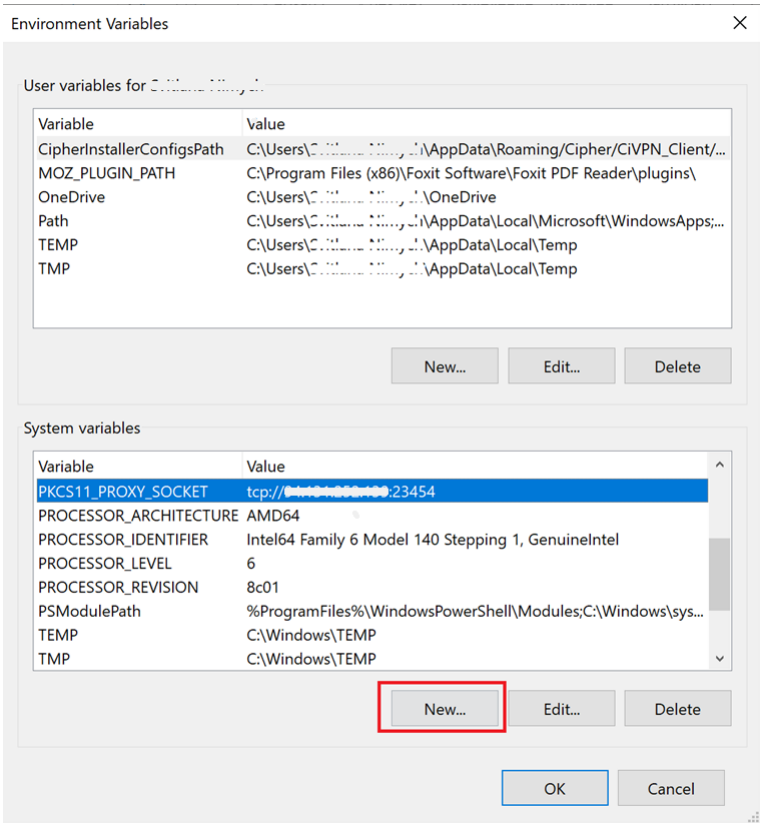

Рис. 5. Створення змінної

Вказуємо наступні значення для змінної. Наприклад, для серверу 0.0.0.0 з портом 23454, створюється змінна середовища PKCS11_PROXY_SOCKET, зі значенням змінної – «tcp://0.0.0.0:23454», Рис. 6.

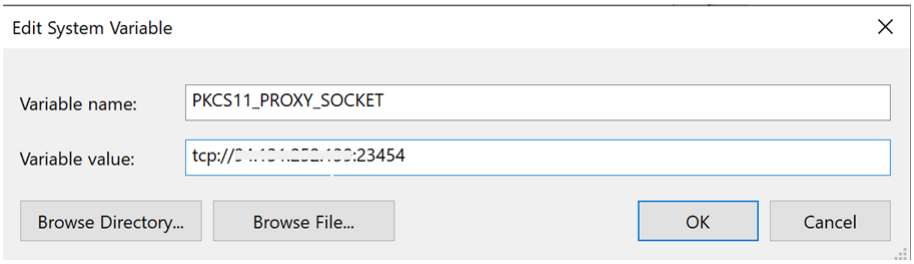

Рис. 6. Створення нової змінної

Перегляд новоствореної змінної середовища та збереження змін, Рис. 7.

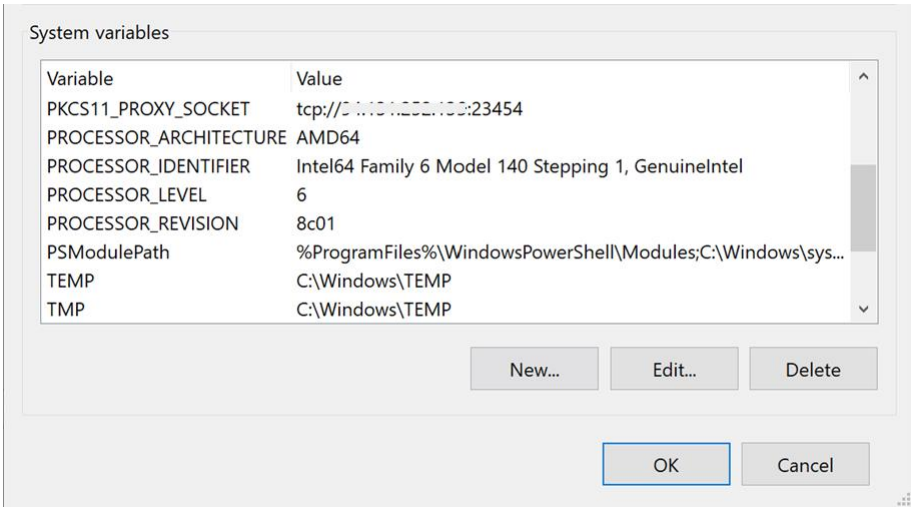

Рис. 7. Оновлений список змінних середовища

Натискаємо «Ок» для збереження змін, Рис. 8.

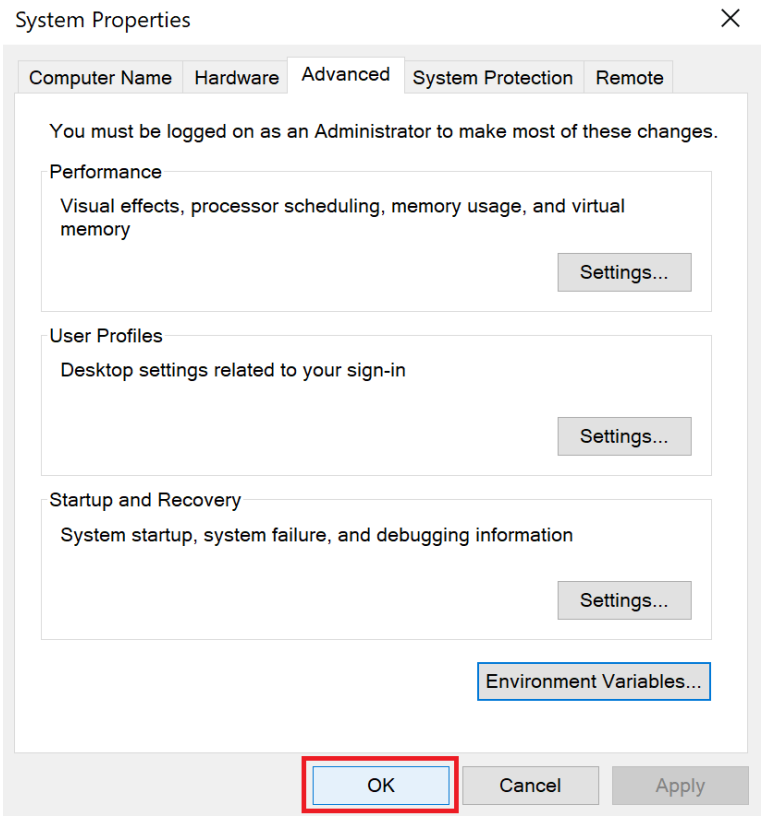

Рис. 8. Збереження змін

ЗЧИТУВАННЯ КЛЮЧА

Запускаємо IIT Користувач та обираємо в розділі «Особистий ключ» - «Зчитати», Рис. 9.

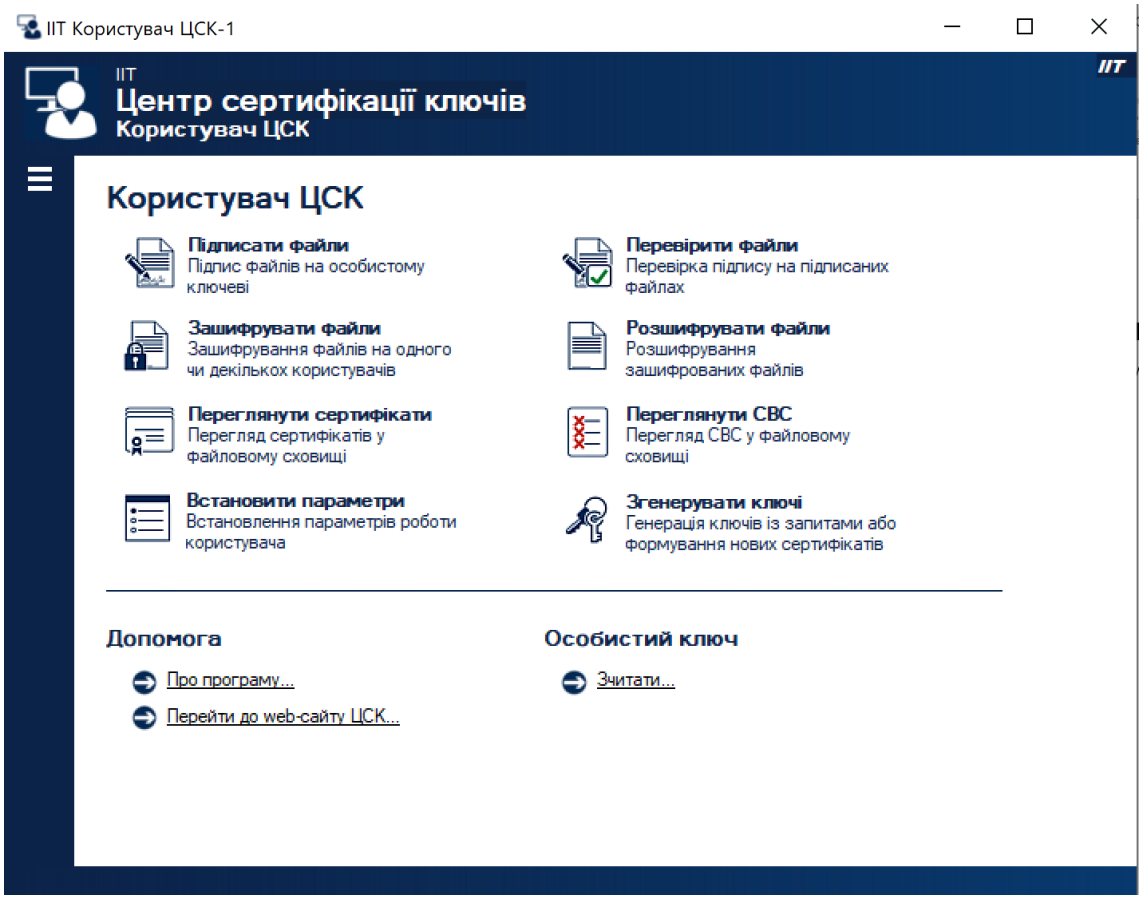

Рис. 9. Зчитування ключа

З'являється вікно з переліком носіїв, серед них треба обрати «криптомодуль Сайфер Шифр-HSM», натиснувши на нього стає доступним пункт Cipher-HSM, Рис. 10.

Стає доступним поле для введення Паролю, але тут є особливість для правильного введення, Рис. 11.

Маска є наступною:

```
##SlotID##PIN
```

- SlotID – задається у 10-ковій чи в 16-ковій системі числення. Якщо значення вказується в 16-ковій системи числення вказується на початку"0x".

  Приклад заповнення:

  - 10-кова система числення – 1060006000
  - 16-кова система числення -0x3F2E6870
- PIN – пін-код до слоту.

Тобто, в даному випадку значення матиме наступний вигляд:

```
##1060006000##12345678
```

АБО

```
##0x3F2E6870##12345678
```

Не допускайте пробілів та інших спецсимволів.

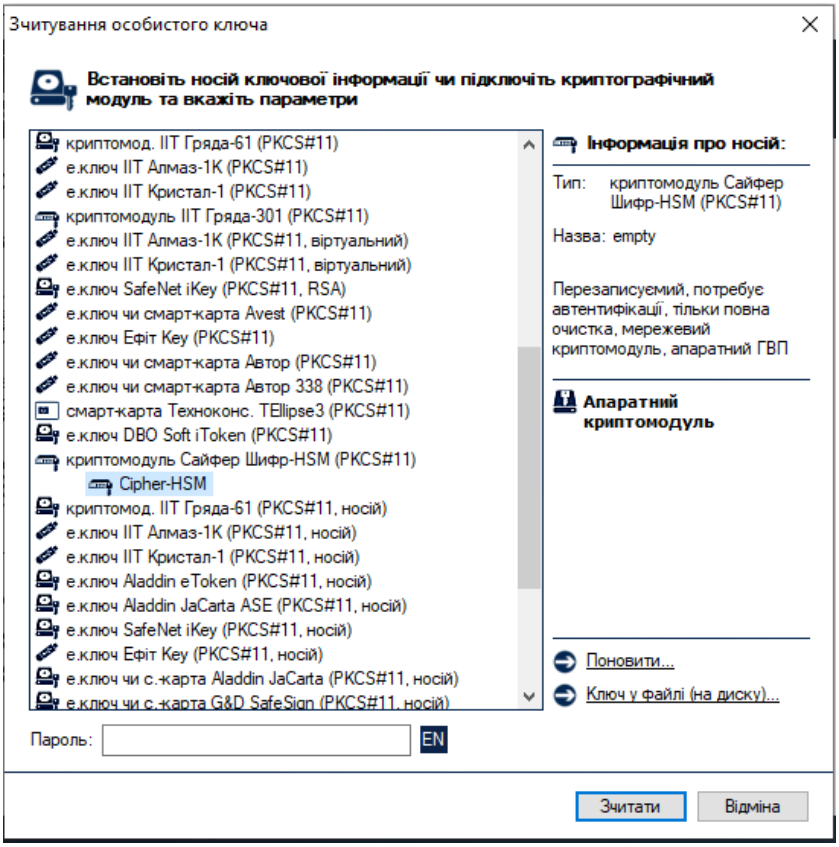

Рис. 10. Вибір криптомодуля Сайфер Шифр-HSM

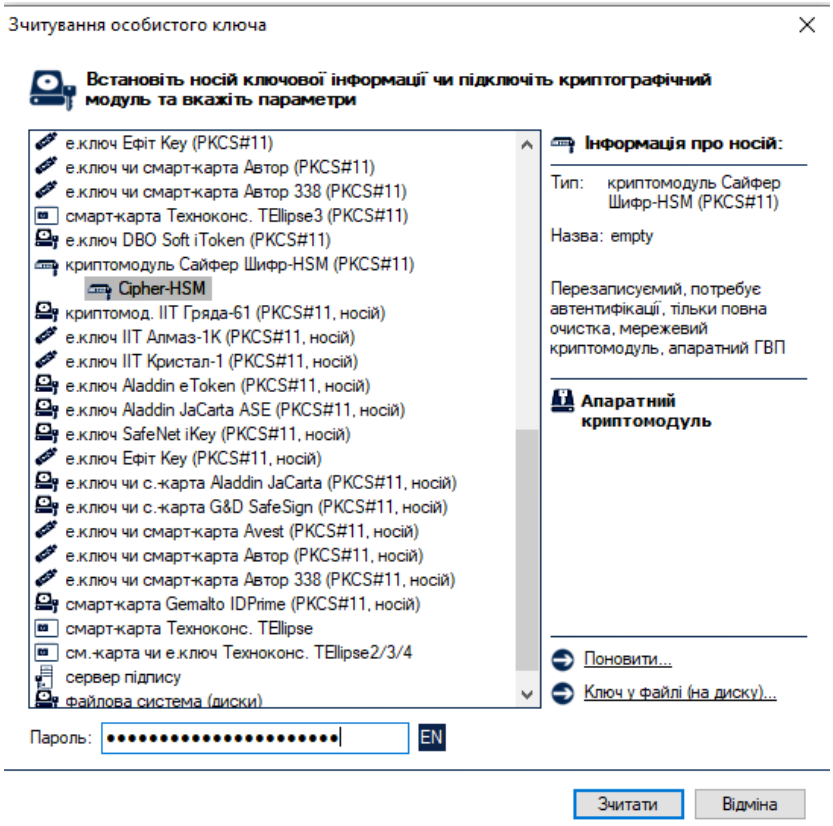

Рис. 11. Вказівка PIN-коду

Після введення значень, натискаємо «Зчитати» для збереження змін. Далі може з'явитися вікно із запитом на завантаження сертифікату CMP-сервера з CMP-сервера ЦСК, Рис. 12. У випадку, якщо

натиснемо «No» подальший процес буде припинено, якщо погодимося, буде запропоновано підтягнути сертифікати за адресою, яку вказували в налаштуванні, Рис. 13.

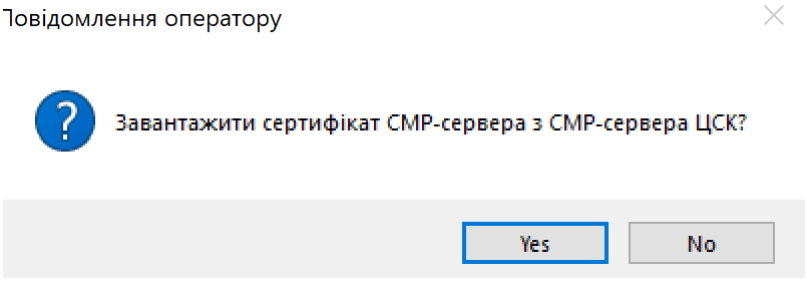

Рис. 12. Запит користувачеві

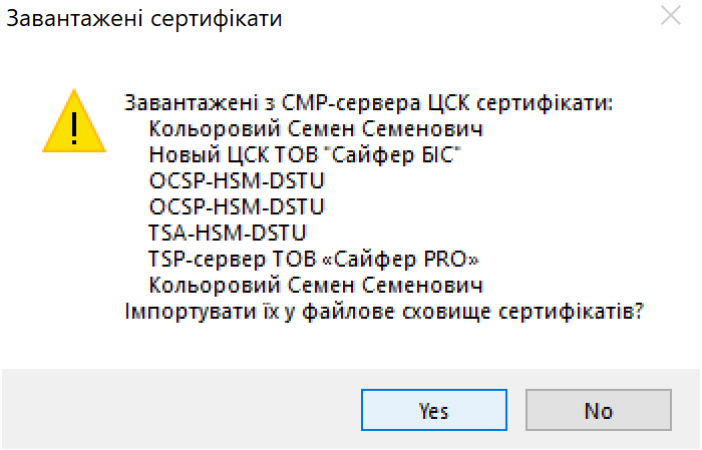

Рис. 13. Повідомлення про отримання сертифікатів

Як результат відображається головне вікно застосування, де зазначається, що особистий ключ успішно зчитано та можна здійснювати підписання документів, Рис. 14.

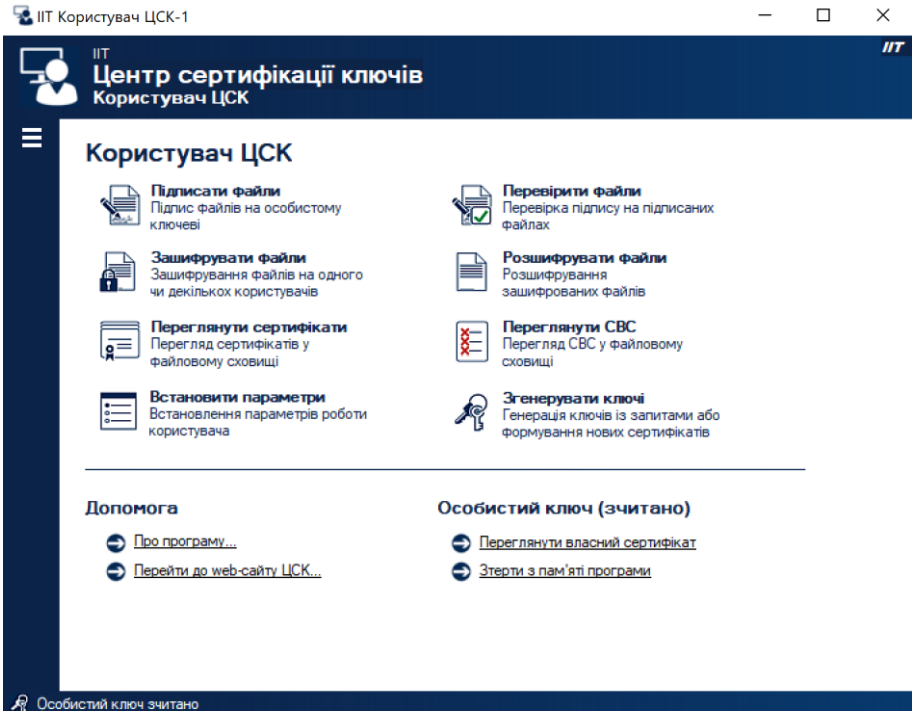

Рис. 14. Головне вікно застосунку

Натиснувши на пункт «Переглянути власний сертифікат», можна переглянути терміни дії сертифікатів, ким виданий та іншу детальну інформацію, Рис. 15.

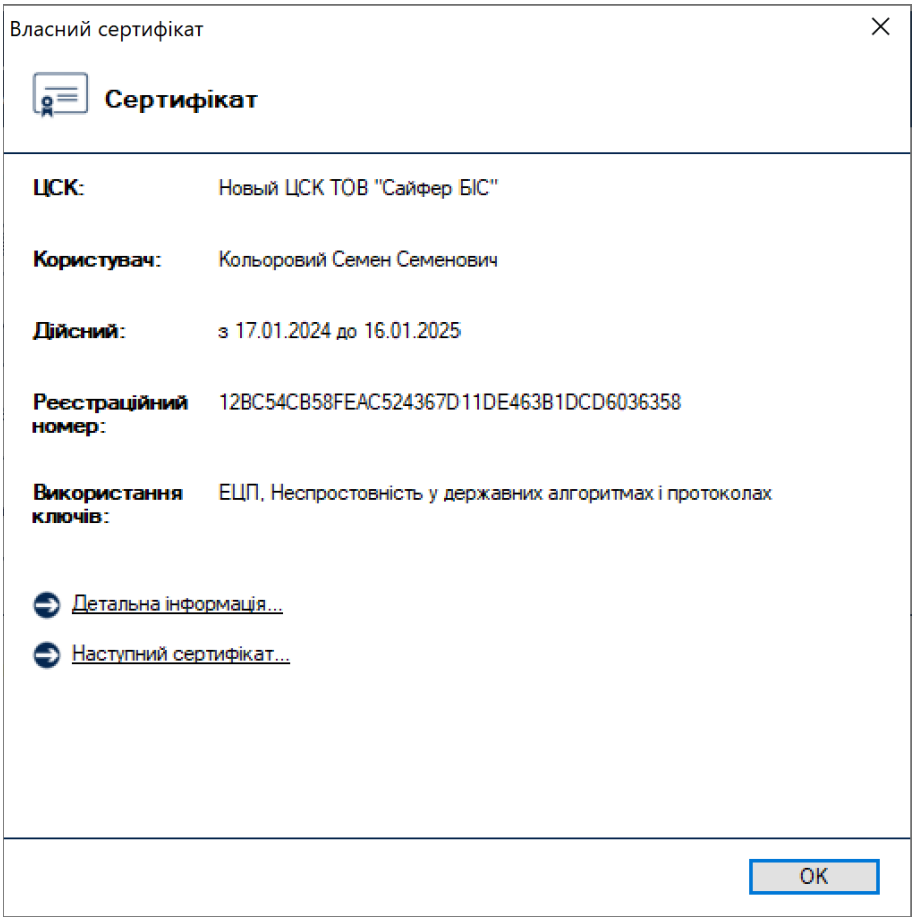

Рис. 15. Перегляд власного сертифікату