ІНСТРУКЦІЯ
по самостійній генерації сертифікатів ключів Користувачами СДО CorpLight/Corp2 АТ «ОЩАДБАНК»

2023

Зміст

1. Системні вимоги до робочого місця користувача..... 3
2. Формування власного сертифікату ключа 8
3. Видалення попереднього сертифікату з носія 11
4. Оновлення ПЗ BarsCryptor Cloud Client..... 13

Дана інструкція описує процедуру формування сертифікату особистого ключа КНЕДП АТ «Ощадбанк».

Сформувати новий сертифікат особистого ключа можливо лише за умови наявності у Користувача діючого (або стартового) сертифікату КНЕДП АТ «Ощадбанк». У разі відсутності діючого (або стартового) сертифікату, Користувачу потрібно звернутись до центрів реєстрації КНЕДП, контакти яких розміщено на сайті КНЕДП, або відділення Банку, в якому проводилась процедура видачі попереднього сертифікату у разі підключення Користувача до системи дистанційного обслуговування (СДО).

1. Системні вимоги до робочого місця користувача

Для формування сертифікату особистого ключа необхідно використовувати операційну систему (ОС) **Windows 7, 8.x, 10, 11** та браузер **Internet Explorer** не нижче 6-ї версії (або **Microsoft Edge** в режимі Internet Explorer, інші браузери не підтримуються).

На робочому місці Користувача, на якому буде здійснюватися формування сертифікату, повинно бути встановлено наступне програмне забезпечення (ПЗ):

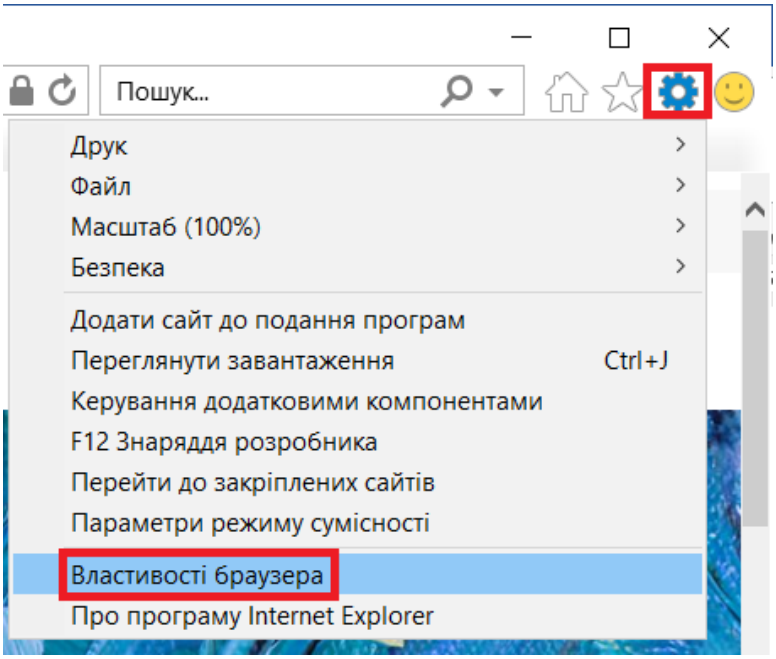
- **VegaCSP,**
- **VegaCryptoPack,**
- **Avtor Cryptographic Provider,** яке доступне для завантаження за посиланням: **https://ca.oschadbank.ua/storage/app/media/uploaded-files/Vega2.zip**

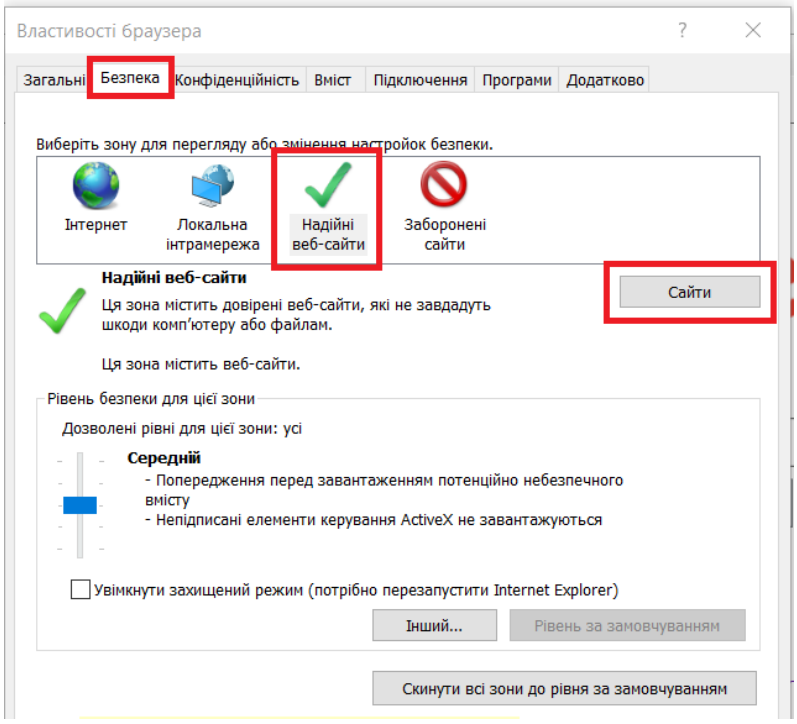
Після завантаження архіву, необхідно:

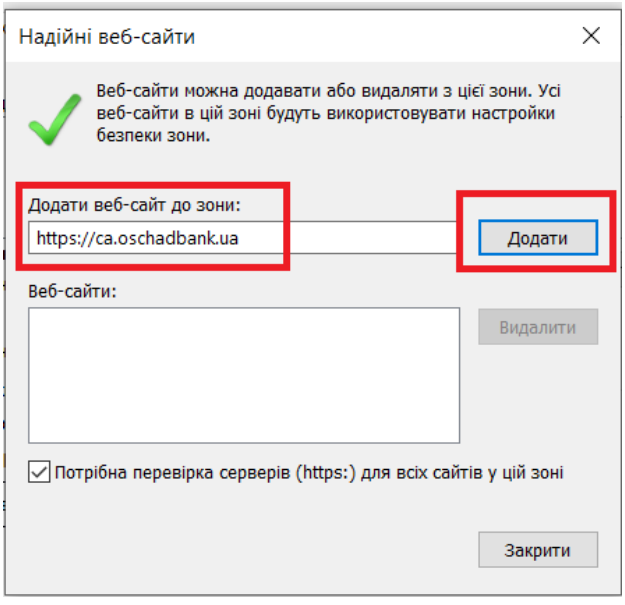
- на ОС **Windows (32-bit):**
  запустити на встановлення **VegaCSP-1.1.msi**;
  запустити на встановлення **VegaCryptoPack-2.0.msi**;
  запустити на встановлення **VegaAvtorSupport.msi**.

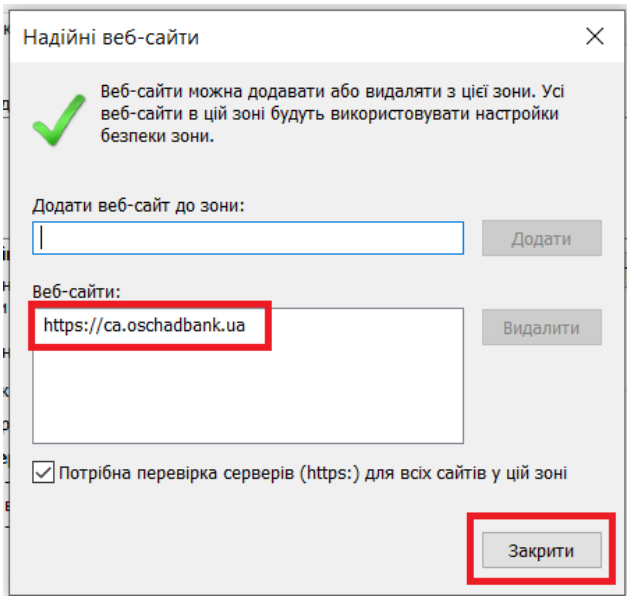
- на ОС **Windows (64-bit):**
  запустити на встановлення **VegaCSP-1.1.msi** та після цього запустити на встановлення **VegaCSP-1.5-x64.msi**;
  запустити на встановлення **VegaCryptoPack-2.0.msi** та після цього запустити на встановлення **VegaCryptoPack-2.0-x64.msi**;
  запустити на встановлення **VegaAvtorSupport.msi**.

В браузері **Internet Explorer** необхідно додати до зони «***Надійні веб-сайти***» в панелі «***Безпека***» веб-сайт центру сертифікації ключів. Для цього необхідно зайти в браузер **Internet Explorer**, натиснути «***Знаряддя***», «*Властивості браузера*», перейти на вкладку «***Безпека***», далі в «***Надійні веб-сайти***», «***Сайти***», прописати адресу сайту https://ca.oschadbank.ua та натиснути «***Додати***». Після цього вікно «***Надійні веб-сайти***» можна закрити:

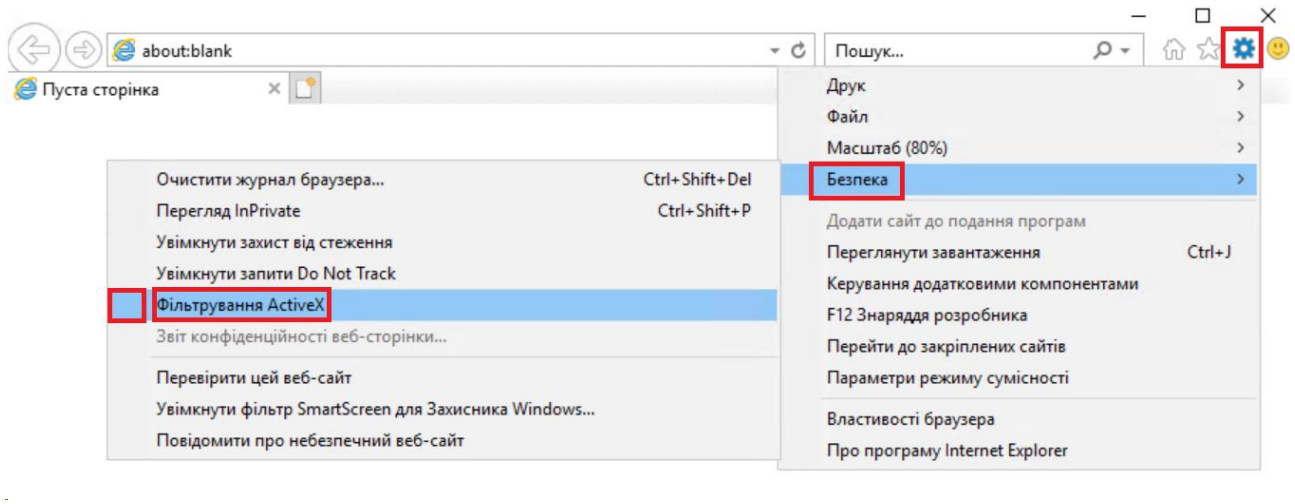

Пошук...
Друк
Файл
Масштаб (100%)
Безпека
Додати сайт до подання програм
Переглянути завантаження
Ctrl+J
Керування додатковими компонентами
F12 Знаряддя розробника
Перейти до закріплених сайтів
Параметри режиму сумісності
Властивості браузера
Про програму Internet Explorer


Властивості браузера
Загальні
Безпека
Конфіденційність
Вміст
Підключення
Програми
Додатково
Виберіть зону для перегляду або змінення настройок безпеки.
Інтернет
Локальна інтрамережа
Надійні веб-сайти
Заборонені сайти
Надійні веб-сайти
Ця зона містить довірені веб-сайти, які не завдадуть шкоди комп'ютеру або файлам.
Сайти
Ця зона містить веб-сайти.
Рівень безпеки для цієї зони
Дозволені рівні для цієї зони: усі
Середній
- Попередження перед завантаженням потенційно небезпечного вмісту
- Непідписані елементи керування ActiveX не завантажуються
Увімкнути захищений режим (потрібно перезапустити Internet Explorer)
Інший...
Рівень за замовчуванням
Скинути всі зони до рівня за замовчуванням


Надійні веб-сайти
Веб-сайти можна додавати або видаляти з цієї зони. Усі веб-сайти в цій зоні будуть використовувати настройки безпеки зони.
Додати веб-сайт до зони:
https://ca.oschadbank.ua
Додати
Веб-сайти:
Видалити
Потрібна перевірка серверів (https:) для всіх сайтів у цій зоні
Закрити

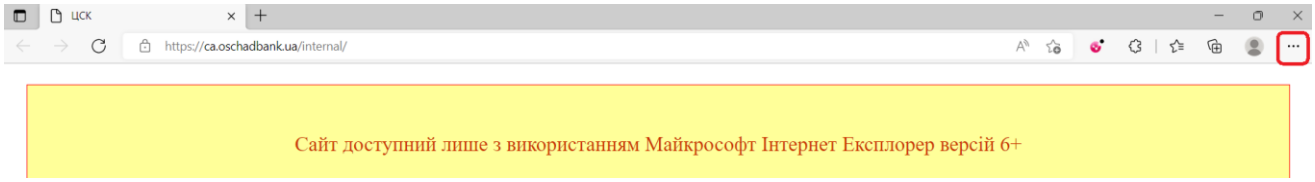

Надійні веб-сайти
Веб-сайти можна додавати або видаляти з цієї зони. Усі веб-сайти в цій зоні будуть використовувати настройки безпеки зони.
Додати веб-сайт до зони:
Додати
Веб-сайти:
https://ca.oschadbank.ua
Видалити
Потрібна перевірка серверів (https:) для всіх сайтів у цій зоні
Закрити

Також, в браузері **Internet Explorer** повинна бути знята галочка в полі «***Фільтрування ActiveX***»:

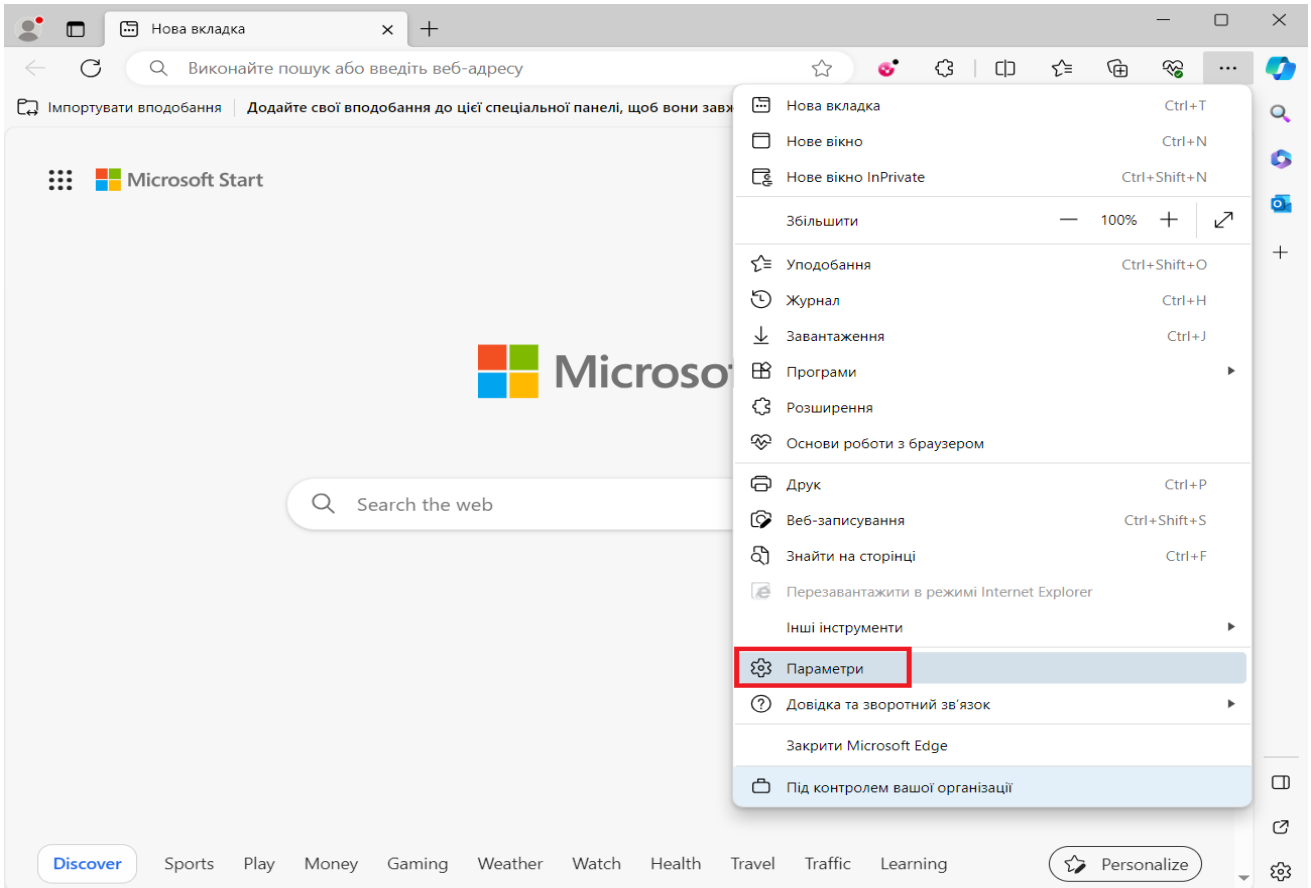


Налаштування браузера **Microsoft Edge** в режимі роботи Internet Explorer

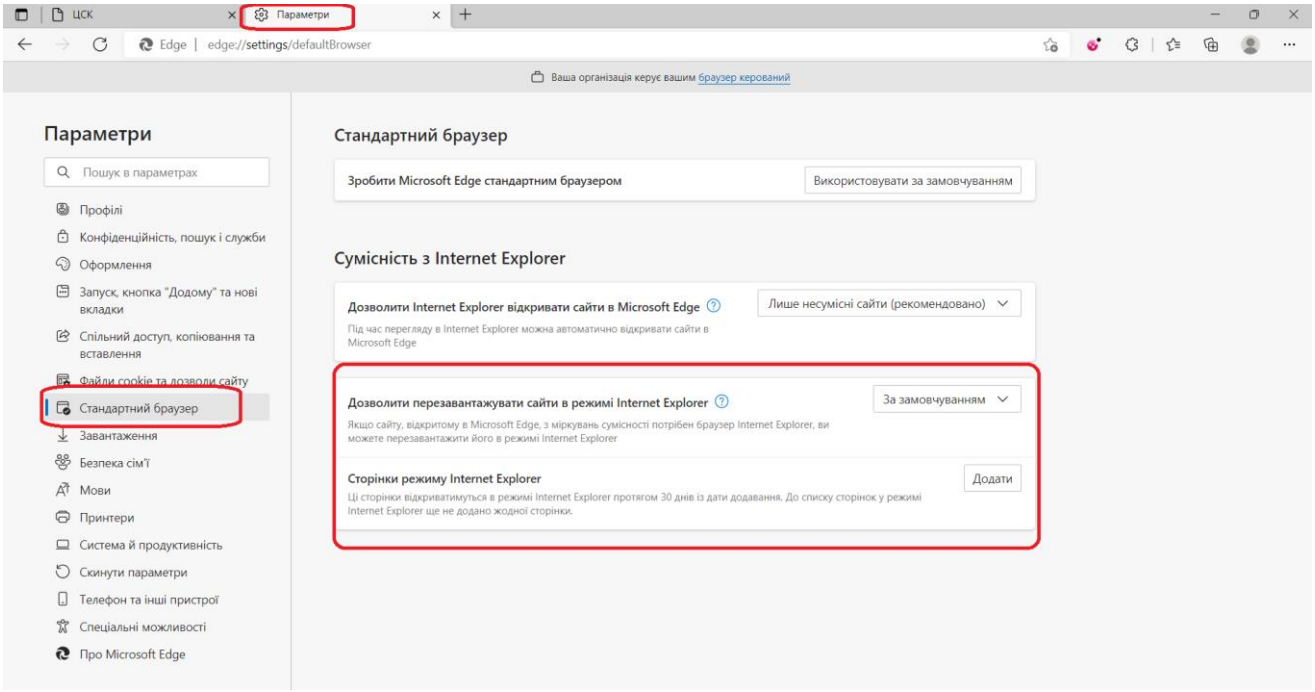
При появі наступного повідомлення у браузері **Microsoft Edge** при переході на сторінку центру сертифікації ключів **https://ca.oschadbank.ua/internal**, перейдіть в «Параметри та інше»:



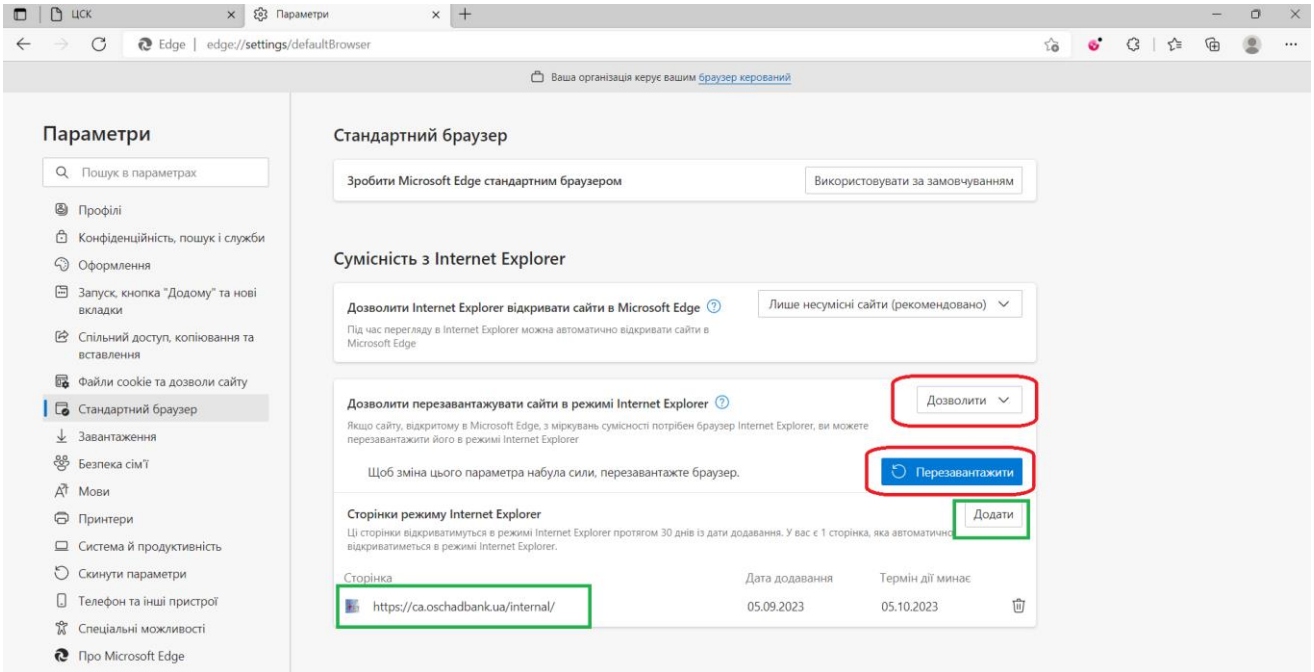
Далі в «Параметри»:



Перейдіть у вкладку «Стандартний браузер» та у розділ сумісності з Internet Explorer:

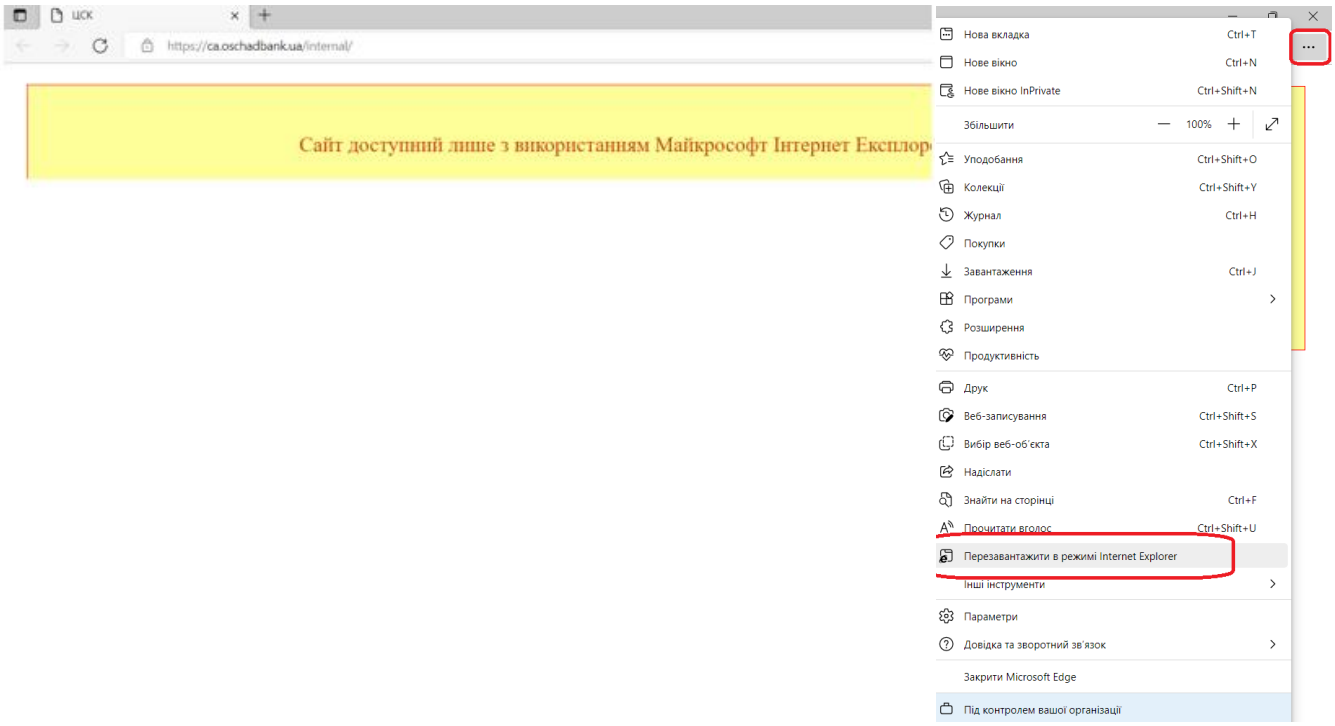


Далі виберіть «Дозволити» та натисніть «Перезавантажити» для застосування змін:

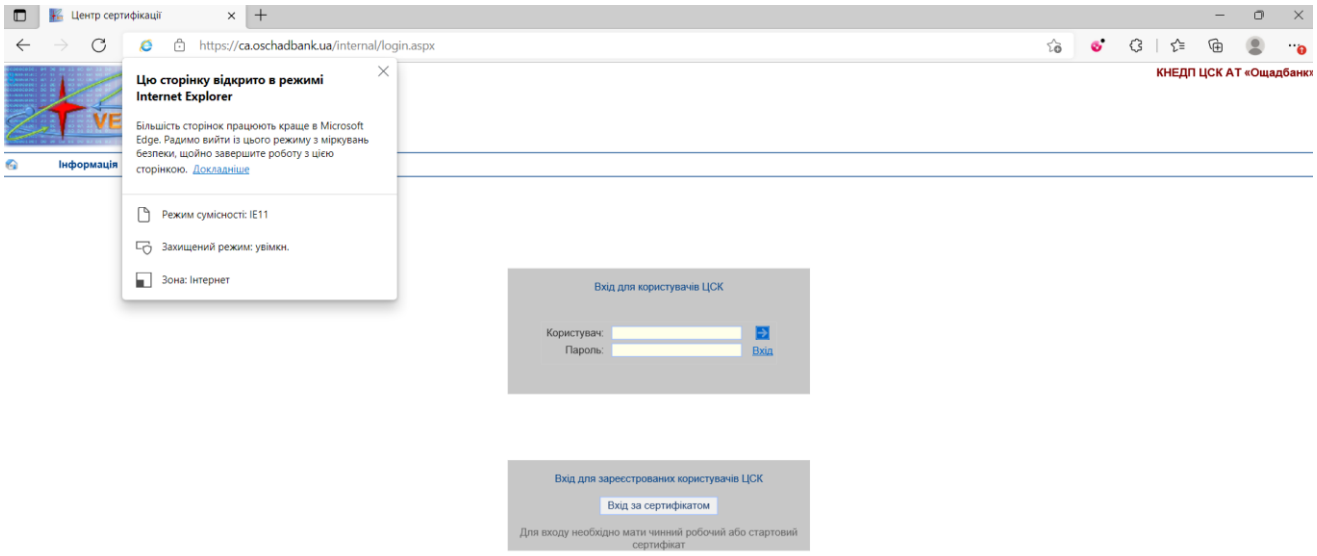


За бажанням, можна відразу додати адресу сайту центру сертифікації **https://ca.oschadbank.ua/internal** в сторінки, які завжди відкриватимуться в режимі Internet Explorer.

Тепер при появі наступного повідомлення, ви будете мати можливість перезавантажити сторінку центру сертифікації в режимі Internet Explorer:



Результат успішного відкриття сторінки в режимі Internet Explorer:

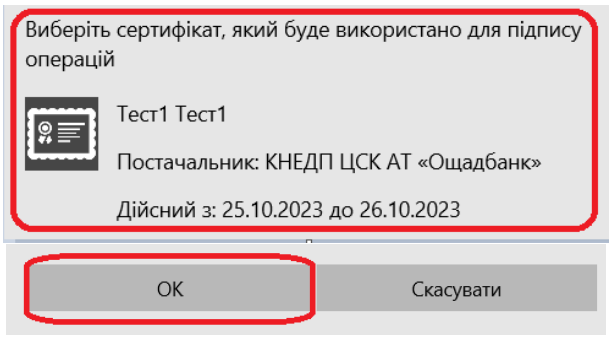


2. Формування власного сертифікату ключа

Для формування сертифікату необхідно підключити Ваш захищений носій з особистим ключем до Вашого робочого місця та відкрити через браузер **Internet Explorer** портал КНЕДП за наступним посиланням: **https://ca.oschadbank.ua/internal**

На сторінці, яка відкриється, необхідно натиснути **«Вхід за сертифікатом»**:

- обрати Ваш існуючий, і обов'язково діючий, сертифікат (або стартовий сертифікат) та натиснути **«ОК»**:



- в наступному вікні ввести ПІН-код до Вашого захищеного носія.

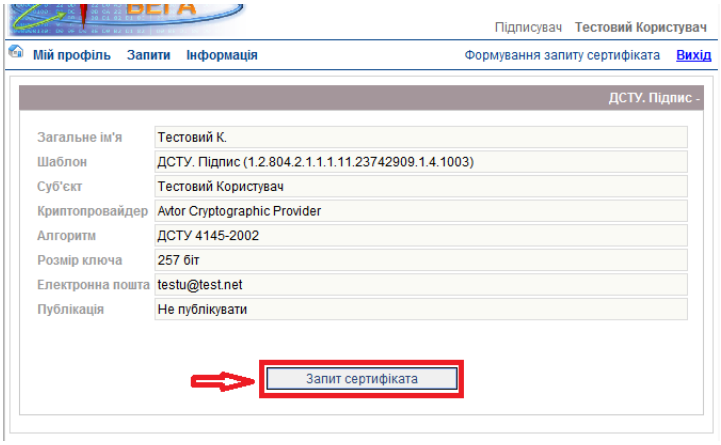
У разі успішного вводу ПІН-коду, Ви опинитесь в особистому кабінеті порталу КНЕДП АТ «Ощадбанк».

Далі оберіть шаблон «**ДСТУ. Підпис**» та натисніть «Далі»:

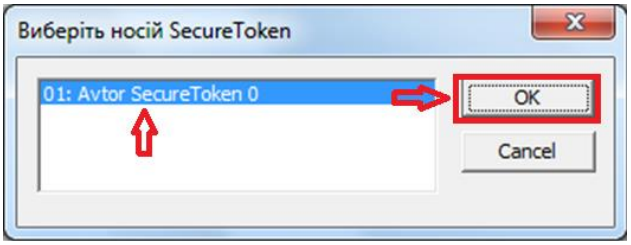
На наступному кроці оберіть відповідний криптопровайдер та натисніть далі:

- для **USB-токену** – «**Avtor Cryptographic Provider**»; - для **Карти** – «**Vega DSTU PlasticCard Crypto Provider**».

Для формування Вашого сертифікату необхідно натиснути кнопку **«Запит сертифіката»**:

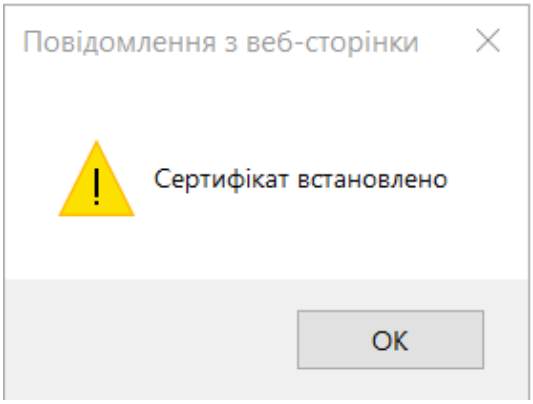


В наступному вікні виберіть носій та натисніть **«ОК»**:

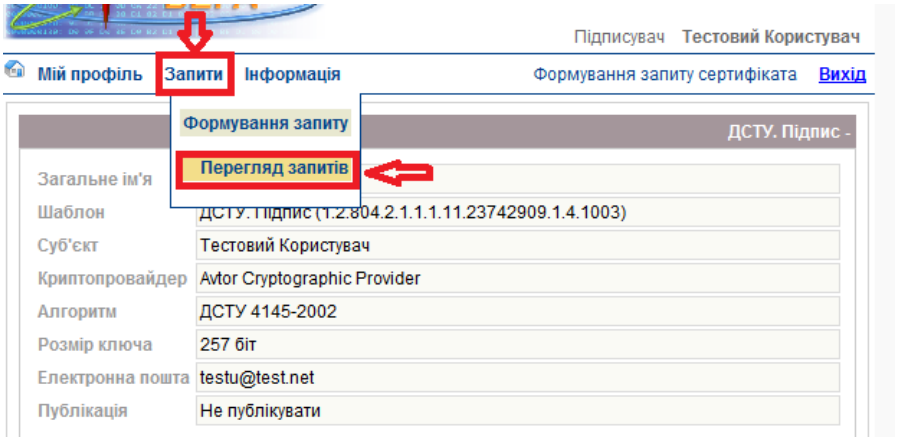


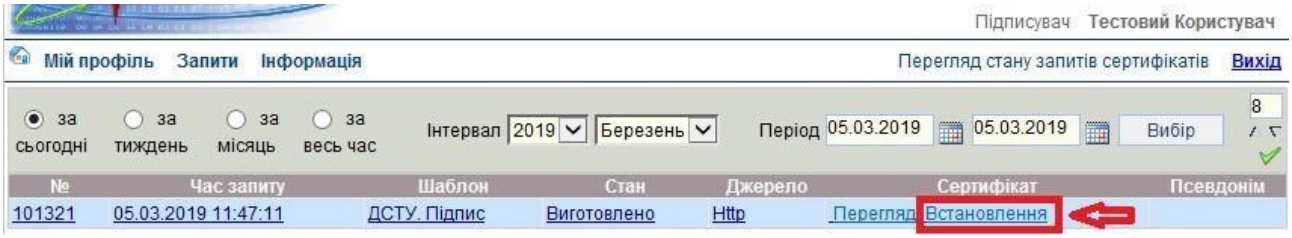
(дане зображення актуально до USB-токена)

Процедура отримання сертифікату має завершитись через 10-30 секунд повідомленням **«Сертифікат встановлено»**:

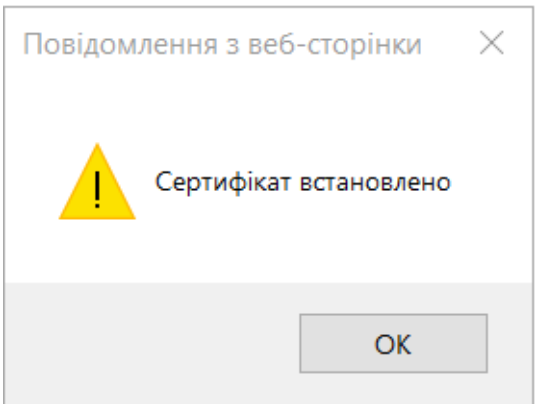


УВАГА!!! Якщо повідомлення про встановлення сертифікату не з'явилося, необхідно зайти в меню **«Запити»**, вибрати пункт **«Перегляд запитів»** та в графі **«Сертифікат»** натиснути кнопку **«Встановлення»**:





Після цього повинно з’явитись повідомленням **«Сертифікат встановлено»**:

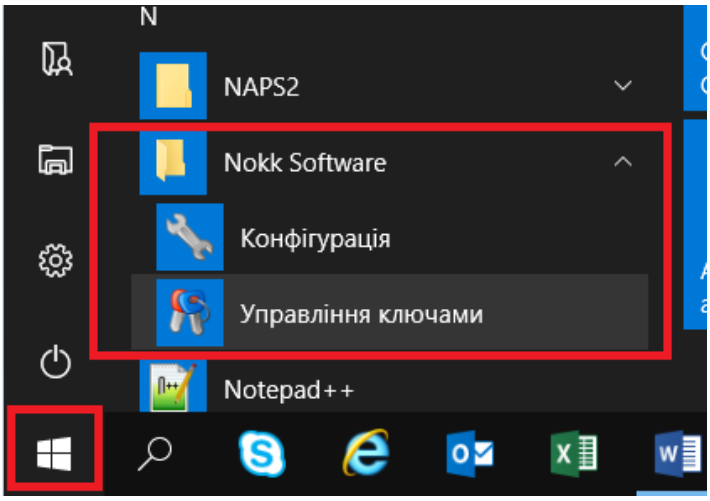


Правильність встановлення нового сертифікату на Ваш носій можна перевірити через процедуру повторного входу до особистого кабінету порталу КНЕДП АТ «Ощадбанк», використовуючи при вході Ваш новий (щойно сформований) сертифікат. Для цього необхідно на сторінці входу вибрати **«Вхід за сертифікатом»**, вибрати в наступному вікні Ваш новий сертифікат (Вам буде доступно попередній та новий сертифікат, якщо натиснути «Більше варіантів»), ввести ПІН-код до носія (у разі появи даного вікна). Очікуваний результат – вхід до особистого кабінету за допомогою Вашого нового сертифікату.

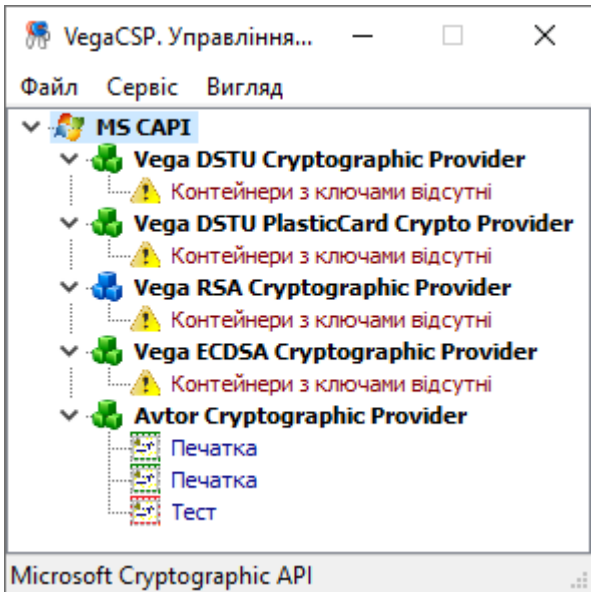
3. Видалення попереднього сертифікату з носія

Після успішного встановлення нового сертифікату (процедура встановлення детально описана в розділі 2 даної Інструкції), необхідно видалити на Вашому захищеному носії попередній (або стартовий) сертифікат, термін дії якого закінчується.

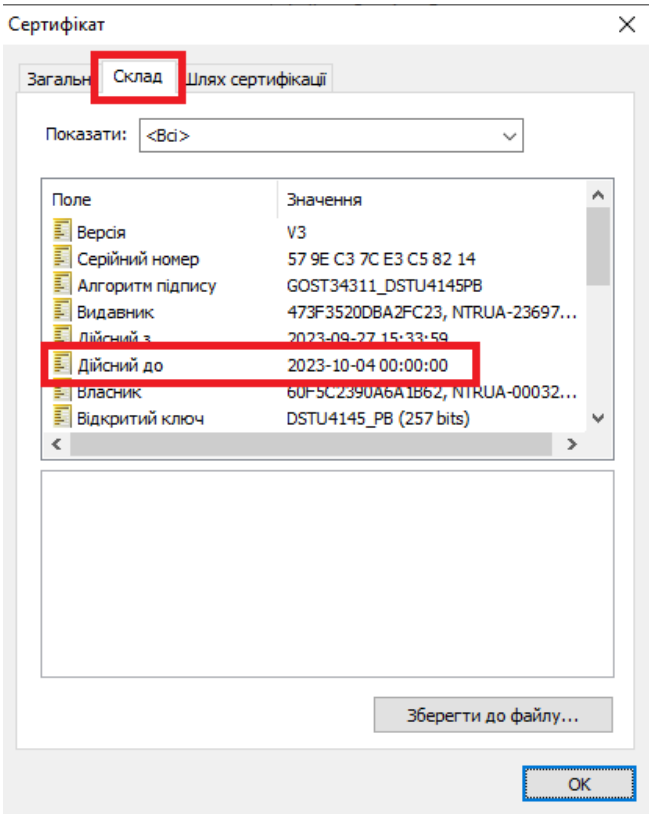
Для цього необхідно натиснути «Пуск - Nokk Software - Управління ключами»:



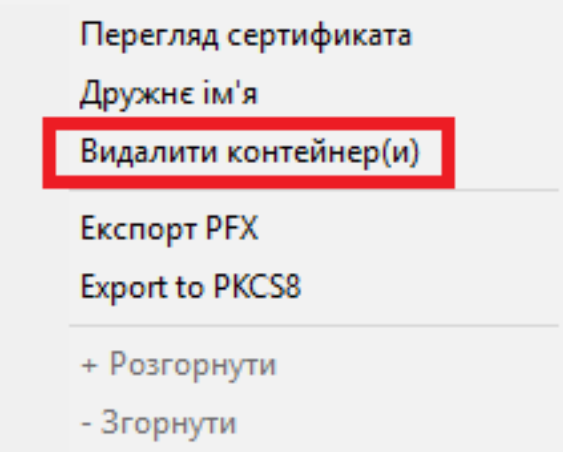
У вікні програми відобразяться наявні на Вашому носії сертифікати:



Натиснувши двічі лівою кнопкою миші на сертифікаті, можна переглянути дані про дату (час) його закінчення:



Обравши сертифікат, який планується видалити (необхідно залишити лише один сертифікат з найбільшим терміном дії), необхідно натиснути на ньому правою кнопкою миші та вибрати **«Видалити контейнер(и)»**:



Далі потрібно ввести ПІН-код до Вашого носія.

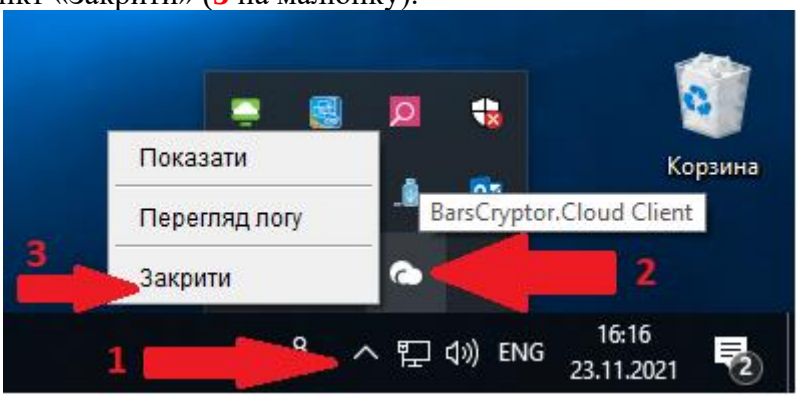
У разі вірного введення ПІН-коду, обраний сертифікат буде видалено з Вашого захищеного носія та на носії залишиться лише один (новий) сертифікат.

4. Оновлення ПЗ BarsCryptor Cloud Client

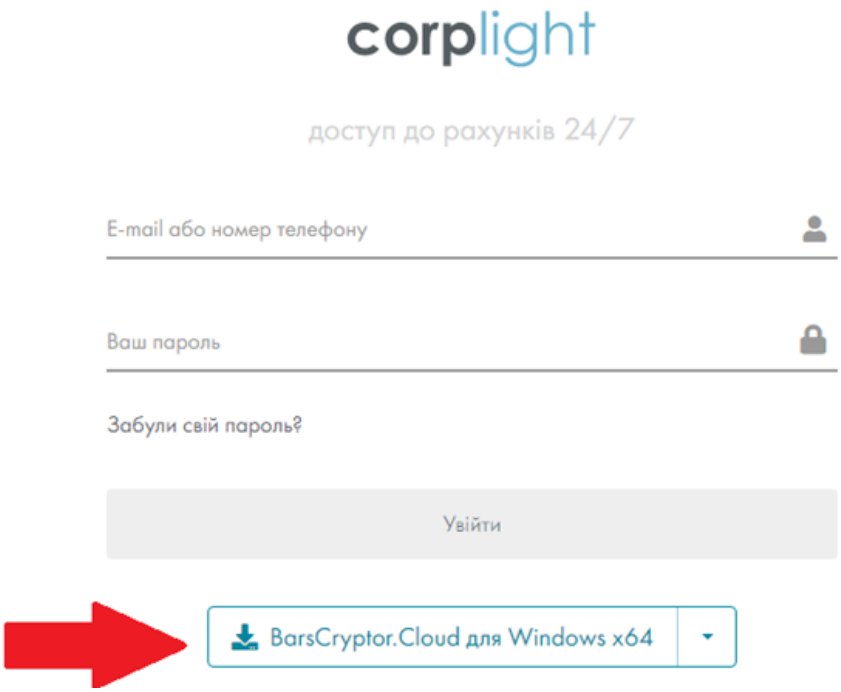
Увага! Подальші дії потрібно виконувати тільки користувачам СДО CorpLight

Після формування нового сертифікату потрібно оновити ПЗ BarsCryptor Cloud Client до останньої версії (наразі це є v 0.2.6.3).

1. Якщо програма BarsCryptor Cloud Client запущена, обов'язково з неї потрібно вийти. Для цього:
   - знайдіть програму в правому нижньому боці екрану в прихованих значках або на панелі (**1** на малюнку);
   - натисніть на значок програми правою кнопкою миші (**2** на малюнку);
   - оберіть пункт «Закрити» (**3** на малюнку).



2. Завантажте і встановіть нову версію ПЗ BarsCryptor Cloud Client, яка доступна на стартовій сторінці CorpLight https://cl.oschadbank.ua/auth/logon одразу під кнопкою «Увійти»:



3. Інструкція по встановленню ПЗ BarsCryptor Cloud Client доступна тут: https://cl.oschadbank.ua/assets/barsCryptorCloud/BarsCryptorCloud_User_Manual.htm