Програмний комплекс ЄДЕБО

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ по налаштуванню спеціального програмного забезпечення робочих станцій у зв'язку з плановою заміною сертифіката шлюзу захисту

У зв'язку з плановою заміною сертифіката шлюзу захисту в спеціальне програмне забезпечення робочих станцій, які задіяні для роботи в ЄДЕБО, повинен бути доданий новий сертифікат шлюзу захисту у файлове сховище сертифікатів.

Новий сертифікат шлюзу захисту додається у файлове сховище сертифікатів вже до існуючих сертифікатів, при цьому ніякі інші сертифікати видаляти зі сховища не потрібно.

Існує 2 (два) варіанти імпорту сертифіката шлюзу захисту у файлове сховище сертифікатів: **автоматичний режим та ручний режим**.

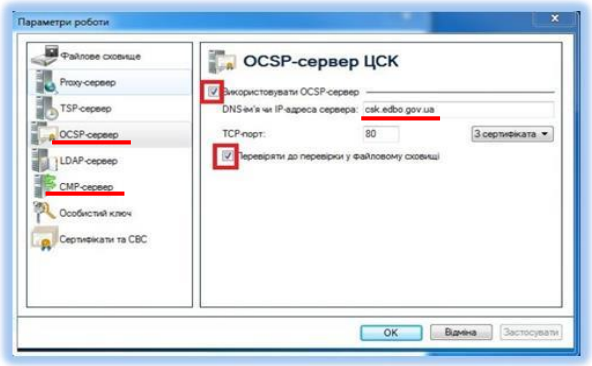
Варіант № 1 (автоматичний режим)

Необхідно перевірити наявність відміток в полях **«Використовувати OCSP-сервер»** та **«Перевіряти до перевірки у файловому сховищі», а також встановити відмітку в полі «Використовувати CMP-сервер»** в клієнті криптозахисту (*при наявності цих відміток сертифікат шлюзу захисту повинен автоматично імпортуватися у файлове сховище сертифікатів*).

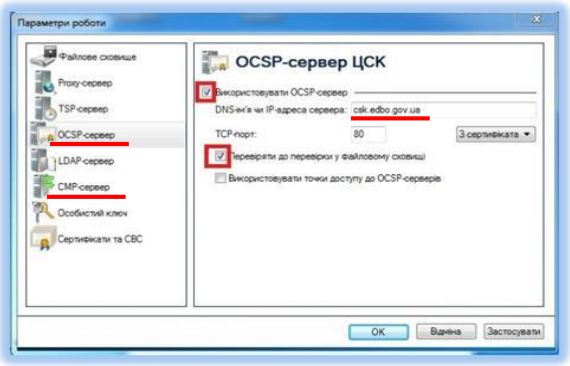
ПРИКЛАДИ:

Windows

«ІІТ Захист з`єднань-2. Клієнт»



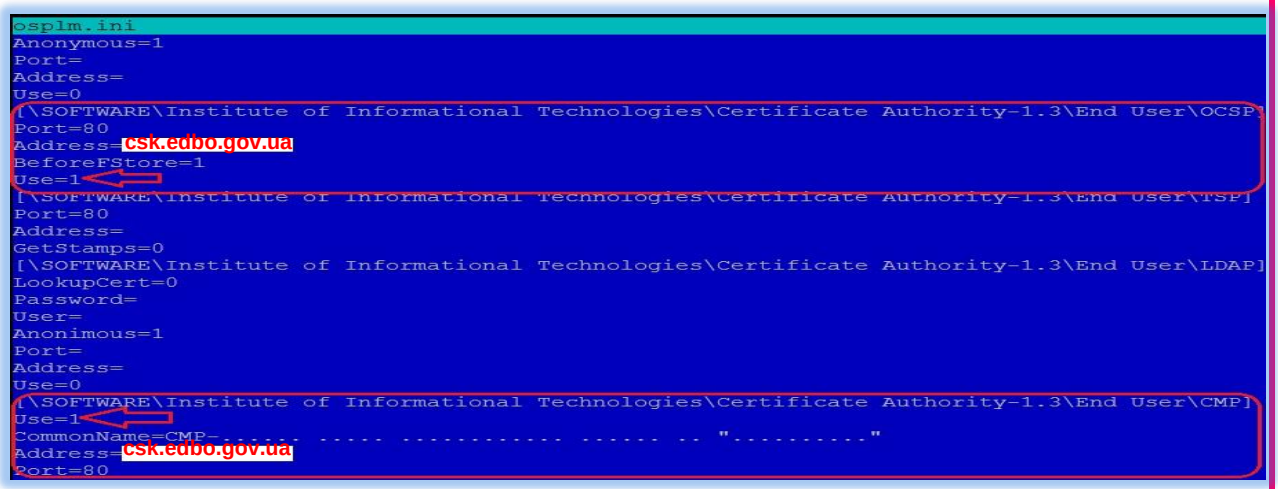
«ІІТ Захист з`єднань-2. Управління Proxy захисту»



Linux

(перевірка налаштувань в конфігураційному файлі osplm.ini)

«ІІТ Захист з`єднань-2. Управління Proxy захисту»



Якщо відмітки в полях відсутні, їх необхідно поставити. Більш **детальний порядок перевірки налаштувань** в спеціальному програмному забезпеченні, яке використовується для захищеного з`єднання з ЄДЕБО, **описано нижче**.

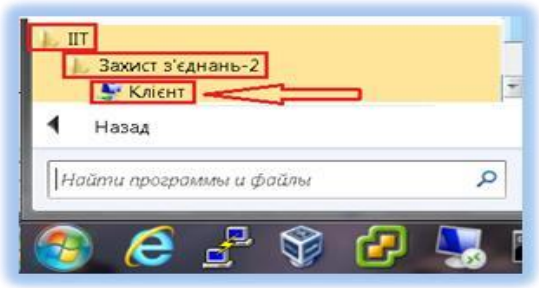
ЗВЕРТАЄМО УВАГУ!

- **Користувачам з сертифікатом (підключення через клієнт криптозахисту)** необхідно перевірити налаштування ТІЛЬКИ в програмному забезпеченні «ІІТ Захист з`єднань-2. **КЛІЄНТ**» (***ліцензія на РОБОЧІ СТАНЦІЇ***).

- Перевірку налаштувань у програмному забезпеченні «ІІТ Захист з`єднань-2. **Управління PROXY захисту**» здійснюють ТІЛЬКИ ті навчальні заклади, які його використовують (***ліцензія на PROXY-підключення*** або ***ліцензія на програмне підключення REST***)

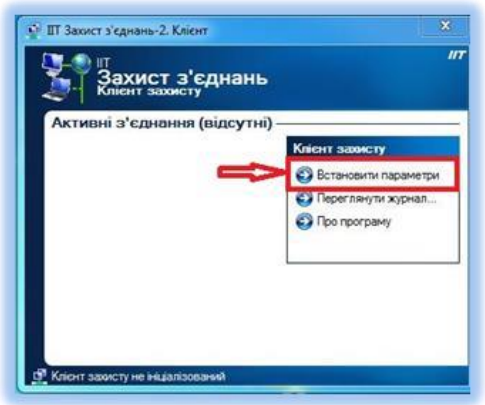
1. Порядок перевірки налаштувань в програмному забезпеченні «ІІТ Захист з`єднань-2. Клієнт»

Запустіть програму **«ІІТ Захист з'єднань – 2. Клієнт»** за допомогою меню **"Пуск"**, обравши в розділі **"Всі програми/ ІІТ / Захист з'єднань-2"** підпункт **"Клієнт"**

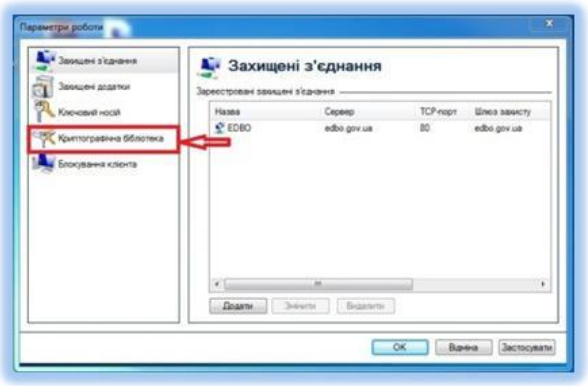


або за допомогою ярлика на робочому столі

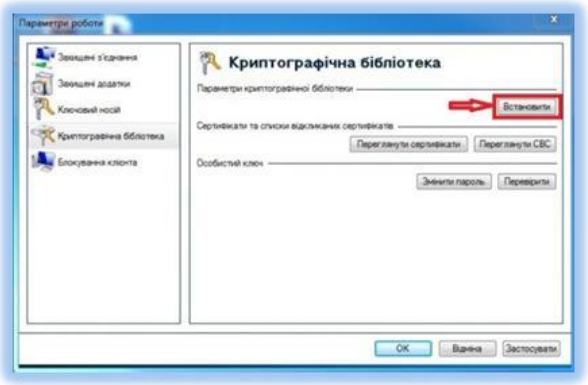
КРОК 1



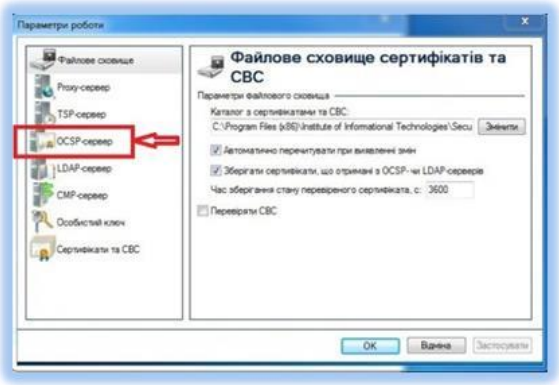
КРОК 2



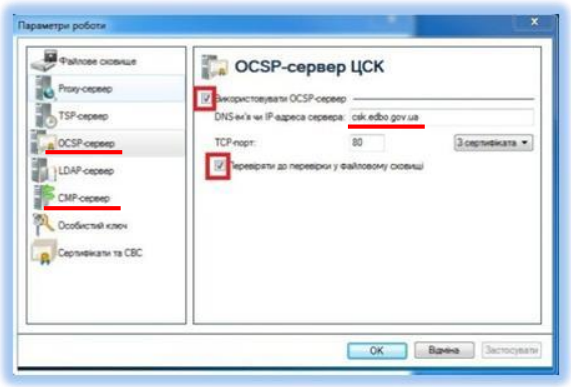
КРОК 3



КРОК 4



КРОК 5



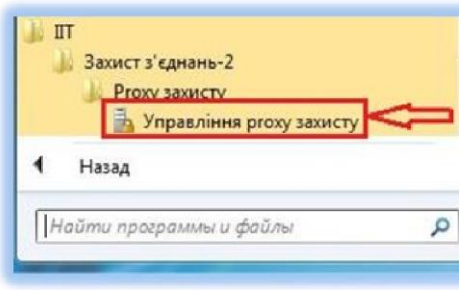
КРОК 6

Якщо відмітки у відповідних полях стоять ☑, то налаштування змінювати ***не потрібно****.*

Якщо відмітки в полях відсутні ☐, їх необхідно ***проставити*** *☑ та натиснути* **«Застосувати»** *і* **«ОК»** *у всіх відкритих вікнах програми.*

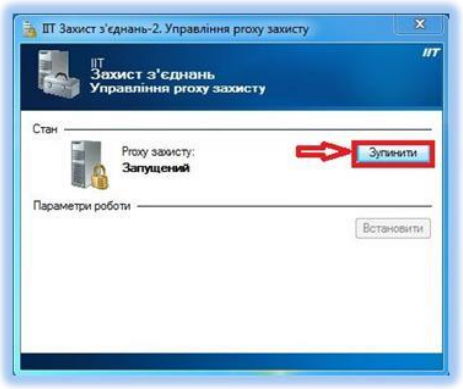
2. Порядок перевірки налаштувань в програмному забезпеченні «ІІТ Захист з`єднань-2. Управління Proxy захисту»

Запустіть програму **«ІІТ Захист з'єднань – 2. Управління Proxy захисту»** за допомогою меню **«Пуск»**, обравши **Всі програми/ ІІТ /Захист з'єднань-2/ Proxy захисту /Управління Proxy захисту**

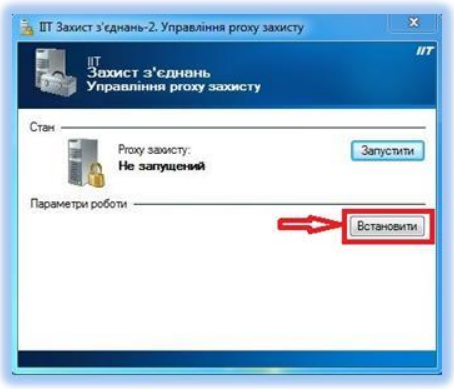


або за допомогою ярлика на робочому столі

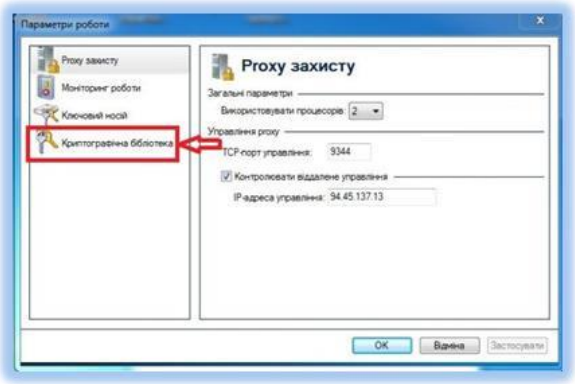
КРОК 1



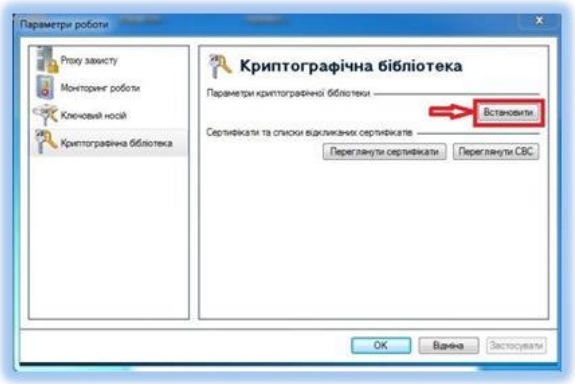
КРОК 2



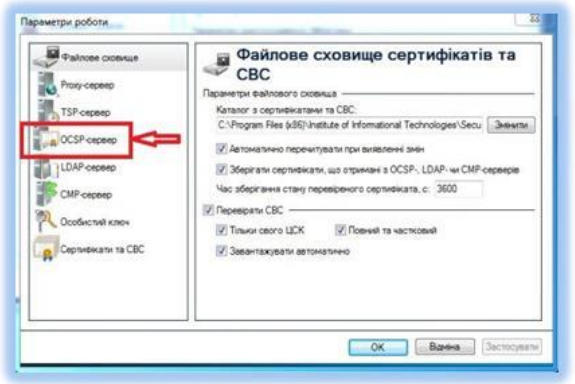
КРОК 3



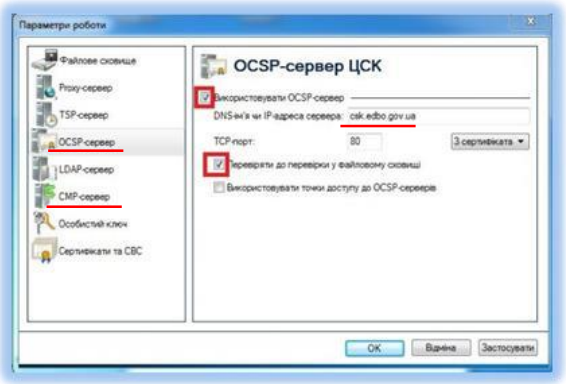
КРОК 4

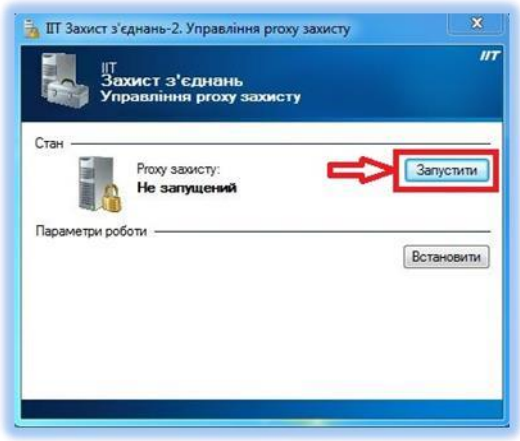


КРОК 5



КРОК 6



КРОК 7	КРОК 8
Якщо відмітки у відповідних полях стоять☑, то налаштування змінювати ***не потрібно***. *Якщо відмітки в полях відсутні ☐, їх необхідно* ***проставити***☑. *Після цього необхідно натиснути* **«Застосувати»** *та* **«ОК»** *у всіх відкритих вікнах програми.*	

Варіант № 2 (Ручний режим)

Використовуючи браузер Internet Explorer, зайдіть на сайт ДП «Інфоресурс» за посиланням

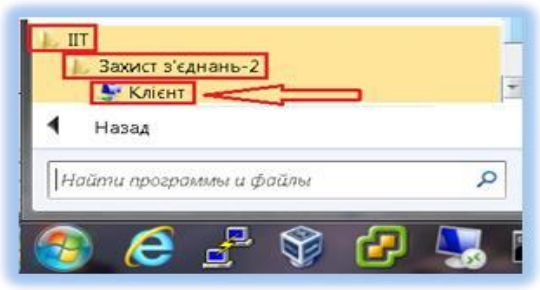
https://www.inforesurs.gov.ua/updates/EU-4018B4C4F73EF1A80400000039520000746B0000.7z

Завантажте архів з сертифікатом шлюзу захисту на робочий стіл персонального комп`ютера.

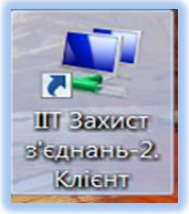
Розпакуйте архів з сертифікатом шлюза захисту **за допомогою архіватора 7-Zip, при цьому збережіть сертифікат на робочому столі персонального комп`ютера** для зручності його імпорту у файлове сховище сертифікатів.

1. Порядок імпорту сертифікату шлюзу захисту в програмному забезпеченні «ІІТ Захист з`єднань-2. Клієнт»

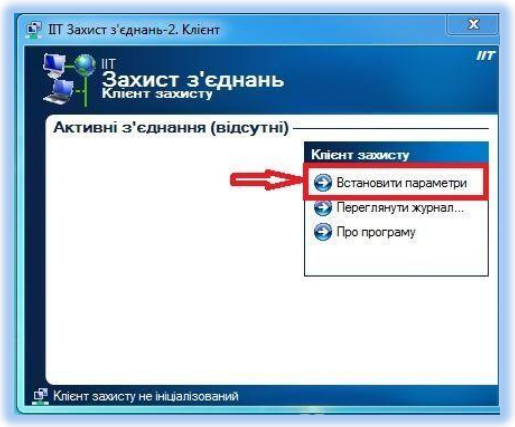
Запустіть програму **«ІІТ Захист з'єднань – 2. Клієнт»** за допомогою меню **"Пуск"**, обравши в розділі **"Всі програми / ІІТ / Захист з'єднань-2"** підпункт **"Клієнт"**



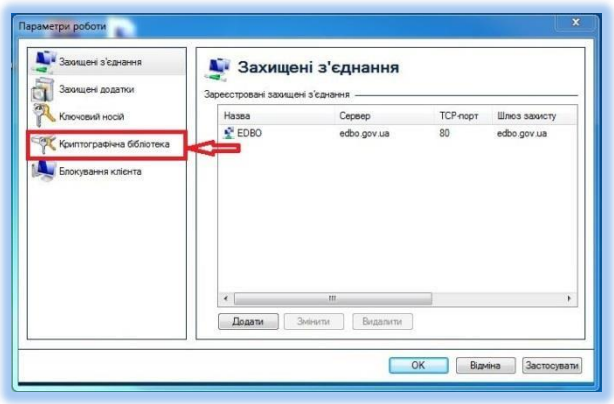
або за допомогою ярлика на робочому столі



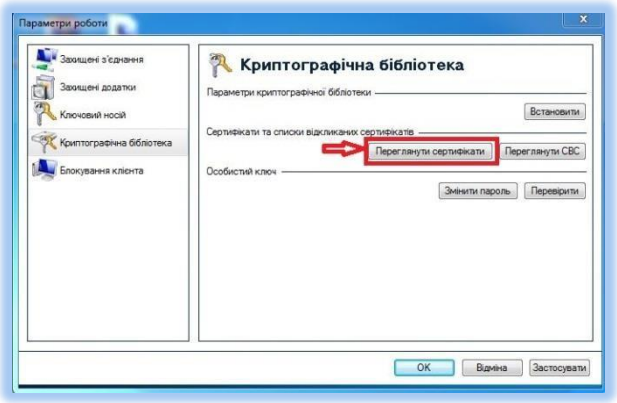
КРОК 1



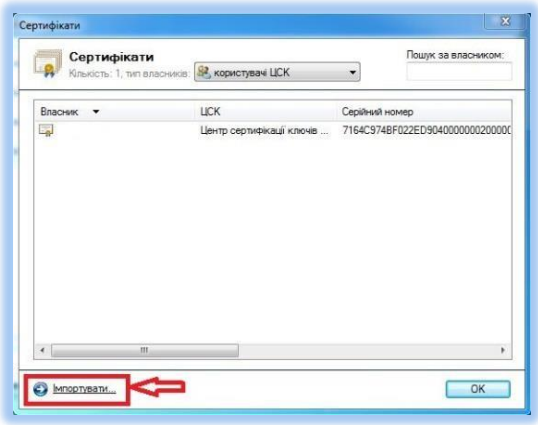
КРОК 2



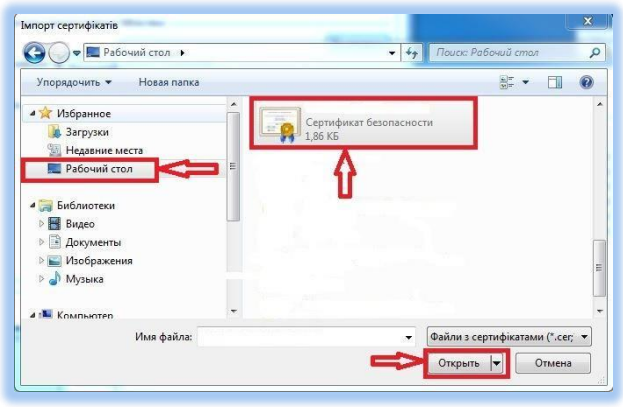
КРОК 3



КРОК 4



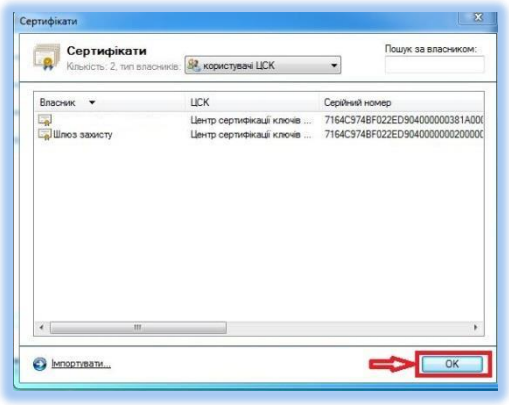
КРОК 5



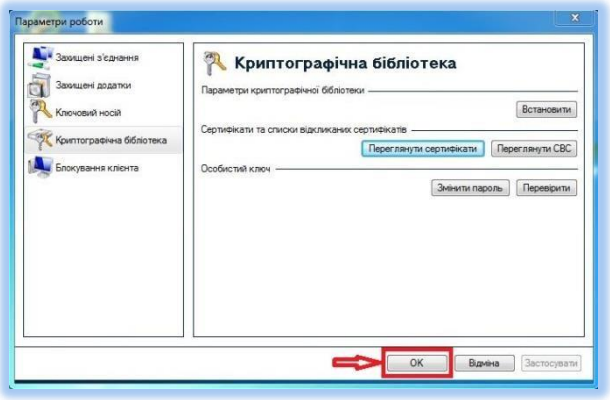
Примітка:

Якщо сертифікат шлюзу захисту було завантажено і збережено не на робочий стіл персонального комп`ютера, то адресу при імпорті сертифіката треба вказувати ту, куди було збережено сертифікат.

КРОК 6



КРОК 7



Примітка:

*Окрім варіанту імпорту сертифіката шлюзу захисту за допомогою програми **«ІІТ Захист з'єднань – 2. Клієнт»** його можна самостійно скопіювати у файлове сховище сертифікатів, тобто в папку **«Certificates»**, яка знаходиться за адресою:*

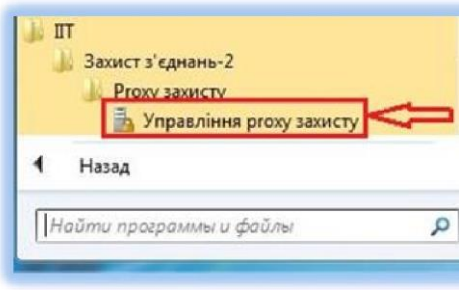
Локальний диск (C:)\ Program Files (x86)\Institute of Informational Technologies\Secure Connections-2\Client\Certificates.

§ Важливо:

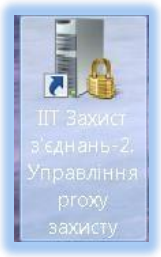
1. В залежності від розрядності операційної системи замість папки **«Program Files (x86)»** може бути папка **«Program Files».**
2. Якщо при установці програми **«ІІТ Захист з'єднань – 2. Клієнт»** було вибрано інший каталог і локальний диск, то адреса і літера диска можуть відрізнятися від тих, що вказані вище.

2. Порядок імпорту сертифікату шлюзу захисту в програмному забезпеченні «ІІТ Захист з`єднань-2. Управління Proxy захисту».

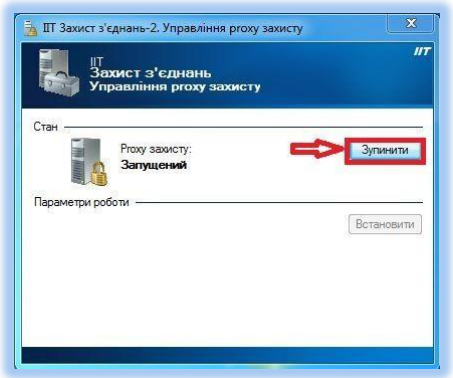
Запустіть програму **«ІІТ Захист з'єднань – 2. Управління Proxy захисту»** за допомогою меню **«Пуск»**, обравши **Всі програми/ ІІТ /Захист з'єднань-2/ Proxy захисту /Управління Proxy захисту**



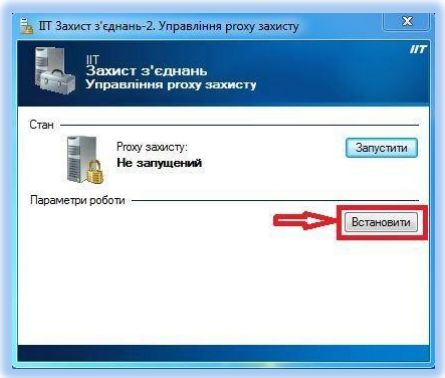
або за допомогою ярлика на робочому столі



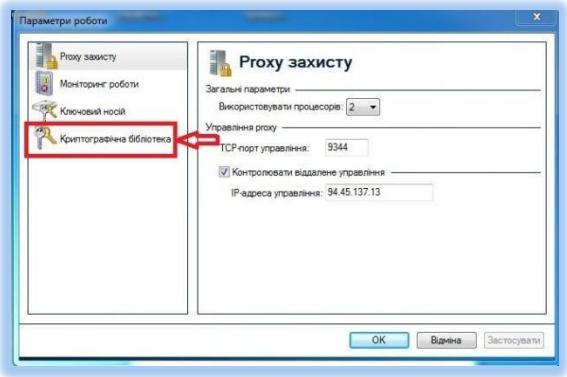
КРОК 1



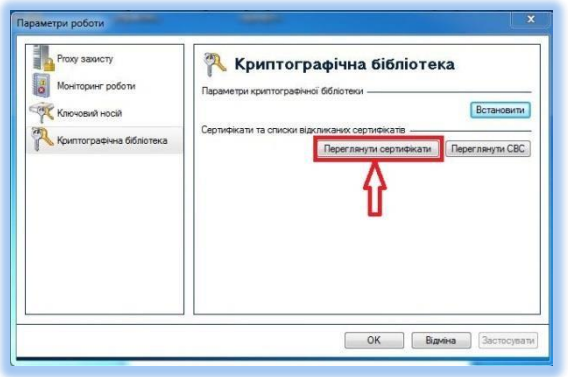
КРОК 2



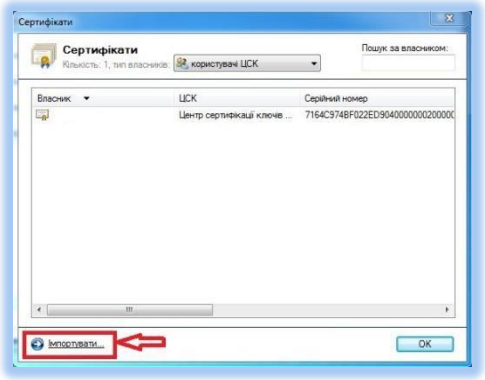
КРОК 3



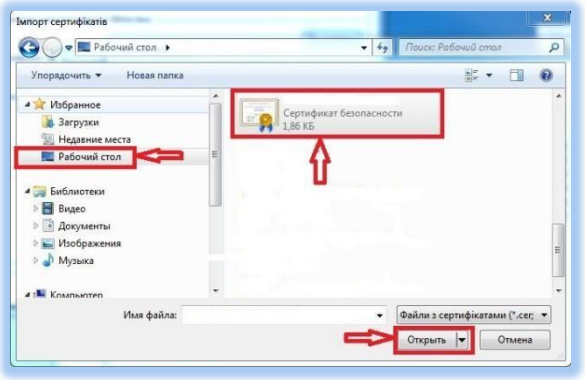
КРОК 4



КРОК 5



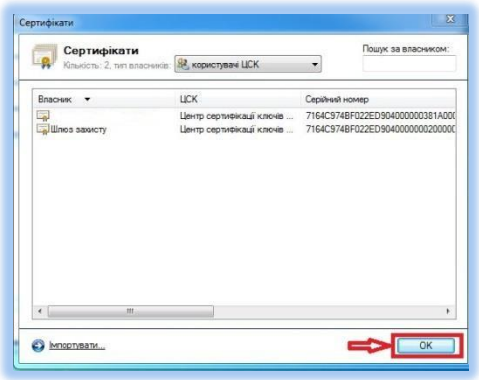
КРОК 6



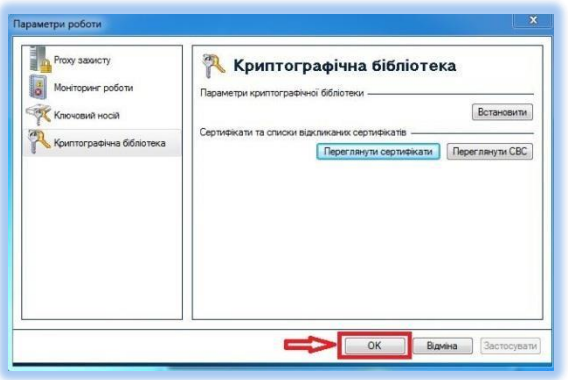
⚐ **Примітка:**

Якщо сертифікат шлюзу захисту було завантажено і збережено не на робочий стіл персонального комп`ютера, то адресу при імпорті сертифіката треба вказувати ту, куди було збережено сертифікат.

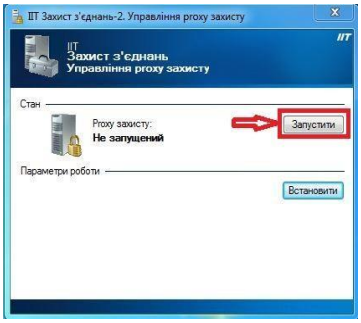
КРОК 7



КРОК 8



КРОК 9



Примітка:

Окрім варіанту імпорту сертифіката шлюзу захисту за допомогою програми ***«ІІТ Захист з'єднань – 2. Управління Proxy захисту»*** *його можна самостійно скопіювати у файлове сховище сертифікатів, тобто в папку* ***«Certificates»****, яка знаходиться за адресою:*

Локальний диск (C:)\ Program Files (x86)\Institute of Informational Technologies\Secure Connections-2\ Proxy \Certificates.

§ Важливо:

1. В залежності від розрядності операційної системи замість папки **«Program Files (x86)»** може бути папка **«Program Files».**
2. Якщо при установці програми **«ІІТ Захист з'єднань – 2. Управління Proxy захисту»** було вибрано інший каталог і локальний диск, то адреса і літера диска можуть відрізнятися від тих, що вказані вище.
3. Перед копіюванням сертифікату шлюзу захисту у файлове сховище програми **«ІІТ Захист з'єднань – 2. Управління Proxy захисту»** необхідно зупинити, а після копіювання запустити.