

# 7.2. ?????????? ?????????????? ?????? ?????????????? ????????

Початкова конфігурація шлюзу безпечного обміну виконується Адміністратором вебсервісів.

## 7.2.1. ?????????????? ?????????? ??? ?????? ?????????????? ???????

Для роботи ШБО в промисловому середовищі потрібна діюча ліцензія, без неї він не працюватиме. Файл ліцензії можна знайти в Особистому кабінеті Каталогу системи «Трембіта» в розділі «Адміністрування» на вкладці «Матеріали».

Для того, щоб завантажити ліцензію на ШБО необхідно перейти до його вебінтерфейсу за посиланням: <https://<Your-security-server-IP>:4000>,

де **<Your-security-server-IP>** - це внутрішня (локальна) IP-адреса шлюзу безпечного обміну,

використовуючи атрибути доступу користувача з роллю Адміністратор вебсервісів:

АДМІНІСТРУВАННЯ СЕРВЕРА БЕЗПЕКИ

Логін

Пароль

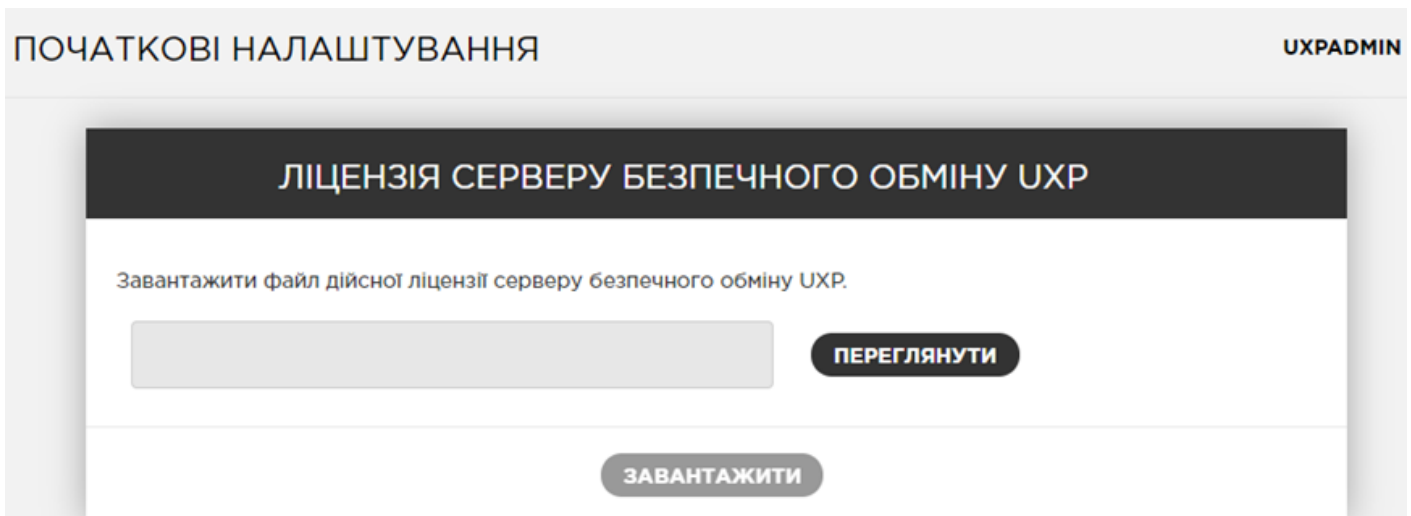
**ВХІД**

**Примітка.** При першому доступі до вебінтерфейсу ШБО може з'явитись попередження про те, що використовується сертифікат, виданий недовіреним центром сертифікації. При встановленні шлюзу безпечного обміну використовується самопідписаний сертифікат, тому слід додати виняток для цього сертифікату у

браузері.

**Примітка.** У перші хвилини після перезапуску шлюзу безпечного обміну вебінтерфейс ШБО може відображати повідомлення «502 Bad Gateway» (зазвичай менше однієї хвилини). Необхідно періодично оновлювати сторінку авторизації, поки не відобразиться форма входу.

Після першої авторизації в вебінтерфейсі ШБО користувачеві буде відображено діалогове вікно вибору файлу ліцензії, в якому необхідно завантажити файл ліцензії промислового середовища member.live.license.lic.



В даному діалоговому вікні необхідно натиснути на кнопку «Переглянути» та завантажити файл ліцензії.

Після завантаження необхідно його підтвердити, натиснувши кнопку «Зберегти ліцензію».

## 7.2.2. ?????????????? ????? ?????????????? ??????

При ініціалізації ШБО необхідно завантажити файл якоря конфігурації промислового середовища (файл configuration anchor).

Файл якоря конфігурації промислового середовища можна знайти в Особистому кабінеті Каталогу системи «Трембіта» в розділі «Адміністрування» на вкладці «Матеріали».

Якір конфігурації необхідно завантажити в наступному діалоговому вікні та підтвердити імпорт, натиснувши на кнопку «Підтвердити» («Confirm»):

## ІМПОРТУВАТИ ЯКІР КОНФІГУРАЦІЇ

ПЕРЕГЛЯНУТИ

ІМПОРТУВАТИ

## Необхідне підтвердження



Подробиці якоря конфігурації:

**Хеш (SHA-224)** 7B:7F:64:24:5A:99:55:93:F0:13:7B:15:E9:20:DB:A9:C3:CE:91:DA:0F:CB:31:6E:8B:81:FD:93**Згенерований** UTC 2020-06-23 19:57:30

Продовжити імпорт?

ПІДТВЕРДИТИ

СКАСУВАТИ

Після чого відкриється вікно ініціалізації ШБО:

## ВЛАСНИК СЕРВЕРА БЕЗПЕКИ

Клас учасника

GOV

Код учасника \*

12345678

Ім'я учасника

ORG12345678

## СЕРВЕР БЕЗПЕКИ

Код сервера безпеки \*

12345678\_SS\_P\_1

## ТОКЕН ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

PIN \*

●●●●●●

Повторити PIN \*

●●●●●●

ВІДПРАВИТИ

Для ініціалізації ШБО необхідно заповнити наступні дані:

Власник сервера безпеки (Security Server Owner)	
Клас Учасника (Member Class)	GOV
Код Учасника (Member Code)	У якості коду Учасника використовується код ЄДРПОУ організації, яка є Учасником системи «Трембіта». <b>Важливо!</b> Якщо ввести неправильний Member Code, то шлюз безпечного обміну не буде функціонувати коректно і його потрібно буде переінсталювати!
Ім'я Учасника (Member Name)	Ім'я Учасника автоматично отримується з сервера Каталогів Учасників (після введення коду Учасника) відповідно до заявки на реєстрацію Учасника у системі «Трембіта».
Шлюз безпечного обміну (Security Server)	

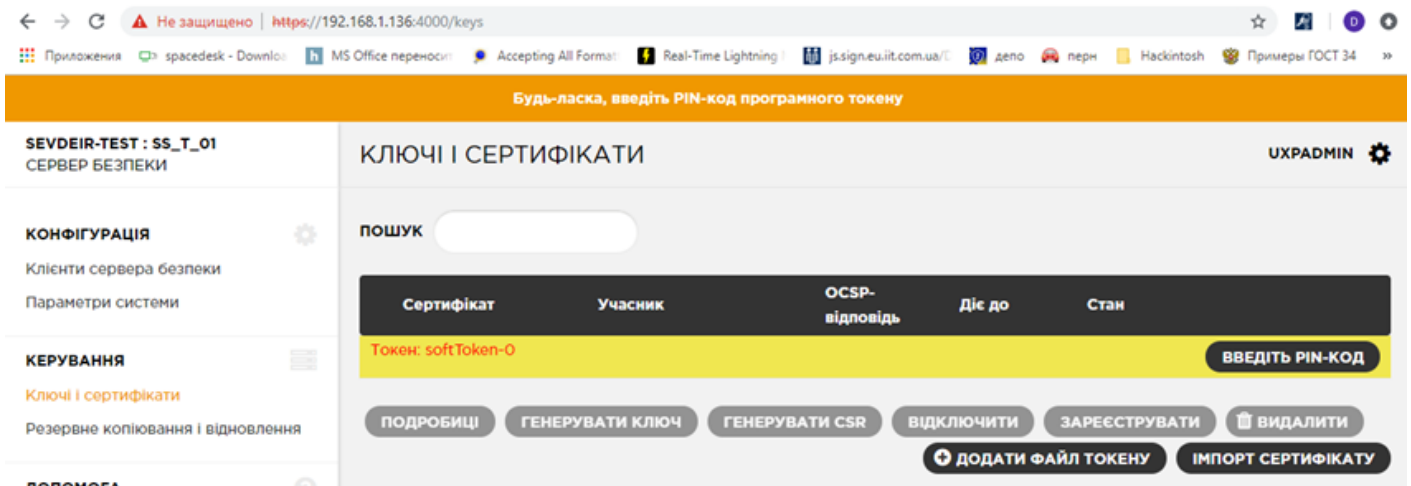
Код сервера безпеки (Security Server Code)	<p>Унікальний код ШБО («сервера безпеки» в вебінтерфейсі) в промисловому середовищі системи «Трембіта», який потрібно створити відповідно до наступного шаблону:</p> <p><b>MemberCode_SS_P_Number_FreeSymbols</b>, де:</p> <p><b>MemberCode</b> – код ЄДРПОУ організації;</p> <p><b>SS</b> – означення ШБО (security server);</p> <p><b>P</b> – абrevіатура промислового середовища системи, не змінюється;</p> <div data-bbox="815 416 1485 600" style="background-color: #f9e79f; padding: 5px;"> <p><b>Важливо!</b> Варто звернути увагу, що <b>_SS_P_</b> потрібно вводити великими латинськими літерами з використанням символу нижнього підкреслення «_».</p> </div> <p><b>Number</b> – порядковий номер ШБО організації;</p> <div data-bbox="815 633 1485 748" style="background-color: #e1f5fe; padding: 5px;"> <p><b>Примітка.</b> Нумерація ШБО для тестового та промислового середовищ системи незалежна.</p> </div> <p><b>FreeSymbols</b> – (за потреби) цифри та літери, які можна додавати до ідентифікатора ШБО задля власної зручності (наприклад, позначення центру обробки даних, позначення інформаційної системи, в якій використовується ШБО тощо).</p> <div data-bbox="815 920 1485 1072" style="background-color: #f9e79f; padding: 5px;"> <p><b>Важливо!</b> Додаткові символи повинні містити лише цифри та великі літери англійського алфавіту.</p> </div>
Програмний токен (Software Token)	
PIN	<p>Необхідно придумати PIN-код, який буде використаний для захисту ключів автентифікації, що зберігаються у програмному сховищі (файловій системі ОС).</p> <div data-bbox="815 1263 1485 1480" style="background-color: #f9e79f; padding: 5px;"> <p><b>Важливо!</b> Адміністратор вебсервісів має зберігати PIN-код у безпечному місці, оскільки після втрати PIN-коду необхідно відновлювати токен, повторно видавати та реєструвати новий сертифікат автентифікації.</p> </div>
Повторити PIN	Ввести повторно значення PIN-коду.

Після введення інформації необхідно натиснути на кнопку «Відправити» («Submit»). Ініціалізація може зайняти декілька хвилин. Коли буде відображено повідомлення про те, що сервер був ініціалізований, необхідно натиснути на кнопку «ОК».

### 7.2.3. ?????????? PIN-???? ?????????????? ????????

ШБО прив'язує всі особисті ключі до токенів безпеки. Після ініціалізації з'явиться помаранчеве повідомлення у верхній частині сторінки з написом «Будь ласка, введіть PIN-код програмного токenu». Це повідомлення вказує на те, що зазначений токен безпеки на даний час заблокований, а особисті ключі не можуть бути використані. Щоразу при

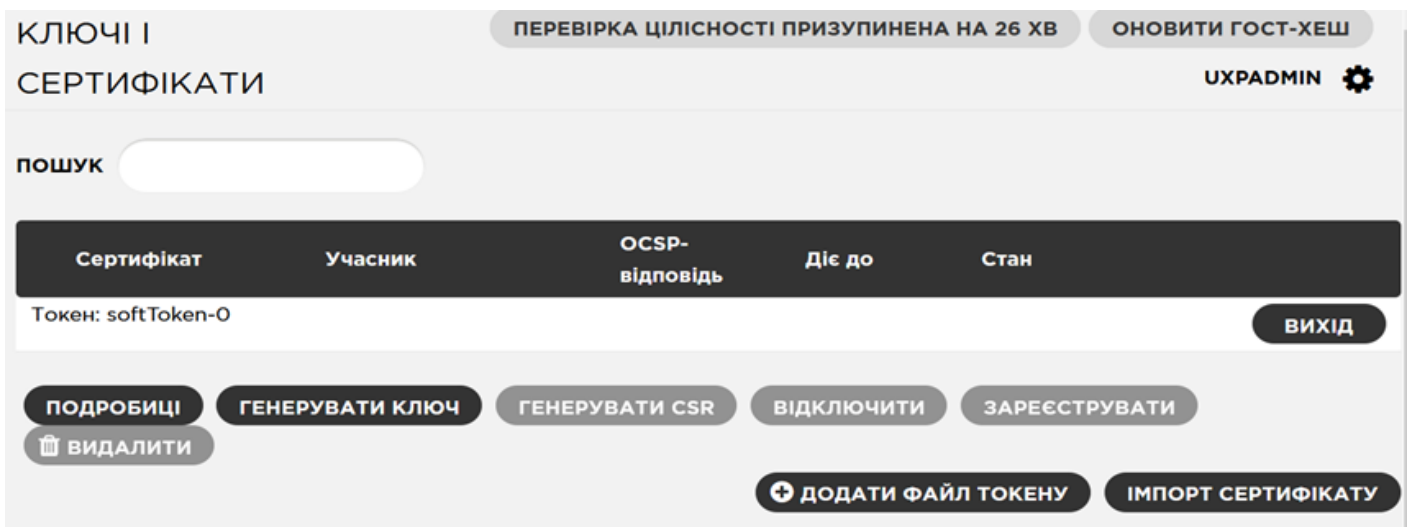
перезавантаженні ПЗ UXP Security Server або всієї операційної системи ШБО, потрібно вводити PIN-код токена безпеки (у всі використовувані токени безпеки).



Адміністратор вебсервісів має увійти в програмний токен безпеки (softToken), використовуючи PIN-код, введений під час ініціалізації сервера, для чого необхідно:

1. Перейти в розділ «Ключі і сертифікати».
2. Знайти рядок із написом «Токен: softToken-0».
3. Натиснути на кнопку «Введіть PIN-код» в цьому рядку – відкриється діалогове вікно для введення PIN-коду.
4. Ввести PIN-код та натиснути на кнопку «ОК».

Якщо все зроблено коректно, повідомлення «Будь ласка, введіть PIN-код програмного токена» зникне, а кнопка «Вихід» – з’явиться замість кнопки «Введіть PIN-код»:




**Примітка.** Варто звернути увагу, що на шлюзі безпечного обміну в промисловому середовищі працює модуль контролю цілісності. Необхідно перевіряти значення

таймеру у верхній частині сторінки. Якщо користувач не встигатиме завершити необхідні налаштування, він має натиснути на кнопку «Перевірка цілісності призупинена на ## хв», щоб отримати більше часу. Після завершення налаштувань обов'язково потрібно натиснути на кнопку «Оновити ГОСТ-ХЕШ».

ПЕРЕВІРКА ЦІЛІСНОСТІ ПРИЗУПИНЕНА НА 10 ХВ

ОНОВИТИ ГОСТ-ХЕШ

UXPADMIN 

**Важливо!** Якщо користувач не встиг виконати всі необхідні налаштування та зберегти зміни шляхом оновлення ГОСТ-хешу, модуль контролю цілісності може призупинити роботу сервісів шлюзу безпечного обміну, а вебінтерфейс адміністрування стане недоступним. У цьому випадку Адміністратору локальних компонентів (системному адміністраторові) необхідно виконати наступні команди в командному інтерфейсі ШБО:

```
sudo uxp-ua-integritychecker.sh recalc_all
sudo uxp-ua-integritychecker.sh check
sudo uxp-ua-integritychecker.sh start_all
```

## 7.2.4. ?????????????? ?????????? ?????????? ??????

Шлюз безпечного обміну використовує зовнішню службу встановлення позначок часу (timestamping) для встановлення позначок часу на кожне повідомлення.

ШБО може мати декілька довірених служб позначок часу.

Адміністратор вебсервісів може обрати, які служби позначок часу будуть використовуватися даним ШБО (зазвичай, це служба, створена відповідним надавачем електронних довірчих послуг, у якого організація отримала сертифікати печатки та шифрування).

Необхідно додати цю службу в список служб встановлення позначок часу, використовуваних шлюзом безпечного обміну, наступним чином:

1. Перейти в розділ «Параметри системи». Список серверів позначок часу має бути порожнім («Немає (відповідних) записів»).
2. Натиснути на кнопку «Додати» в секції «Сервіси позначки часу».
3. Обрати зі списку доступний сервіс і натиснути на нього.
4. Натиснути на кнопку «ОК».

В результаті відобразиться інформація про обраний сервіс позначок часу і його URL в секції «Сервіси позначки часу».

# СЕРВІСИ ПОЗНАЧКИ ЧАСУ

+ ДОДАТИ

🗑️ ВИДАЛИТИ

Сервіс позначки часу

URL сервісу

TSP-сервер АЦСК органів юстиції України

<http://ca.informjust.ua/services/tsp/>

**Важливо!** Повинен бути зазначений саме TSP-сервер видавця КНЕДП, де організація отримувала електронну печатку!

Версія #10

Admin створив 2024-05-28 09:37:35 UTC

Admin оновив 2024-09-25 12:00:12 UTC