6.2. ????????? ????????????? ????? ?????????? ??????

Початкова конфігурація шлюзу безпечного обміну виконується Адміністратором вебсервісів.

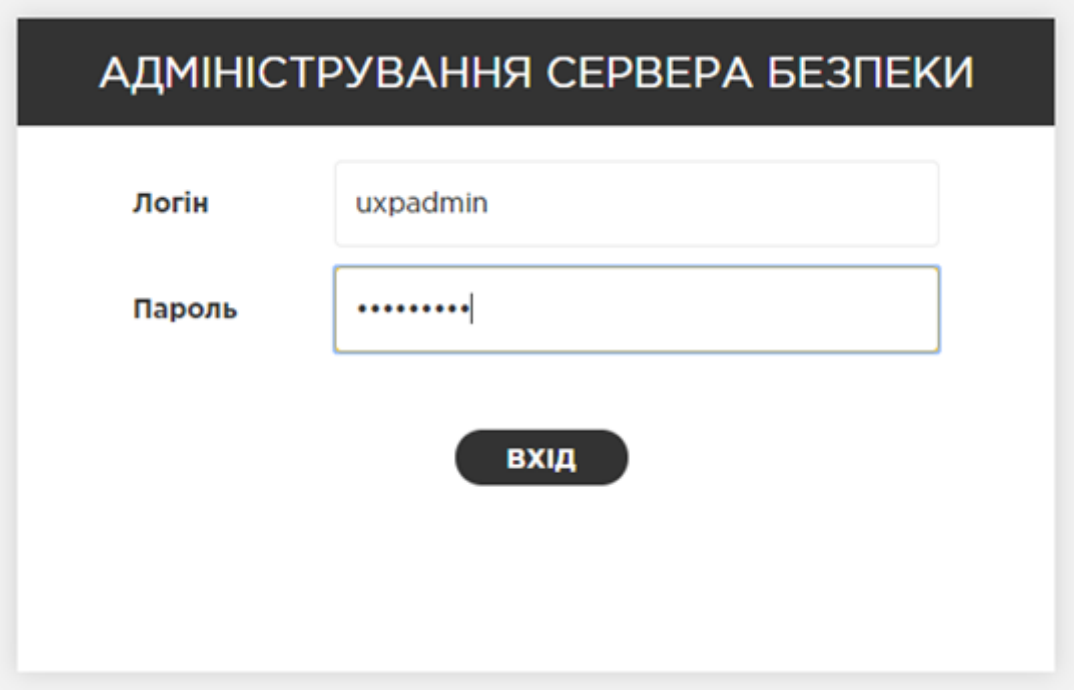
6.2.1. ???????????? ???????? ??? ????? ?????????? ??????

Для роботи ШБО в тестовому 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,

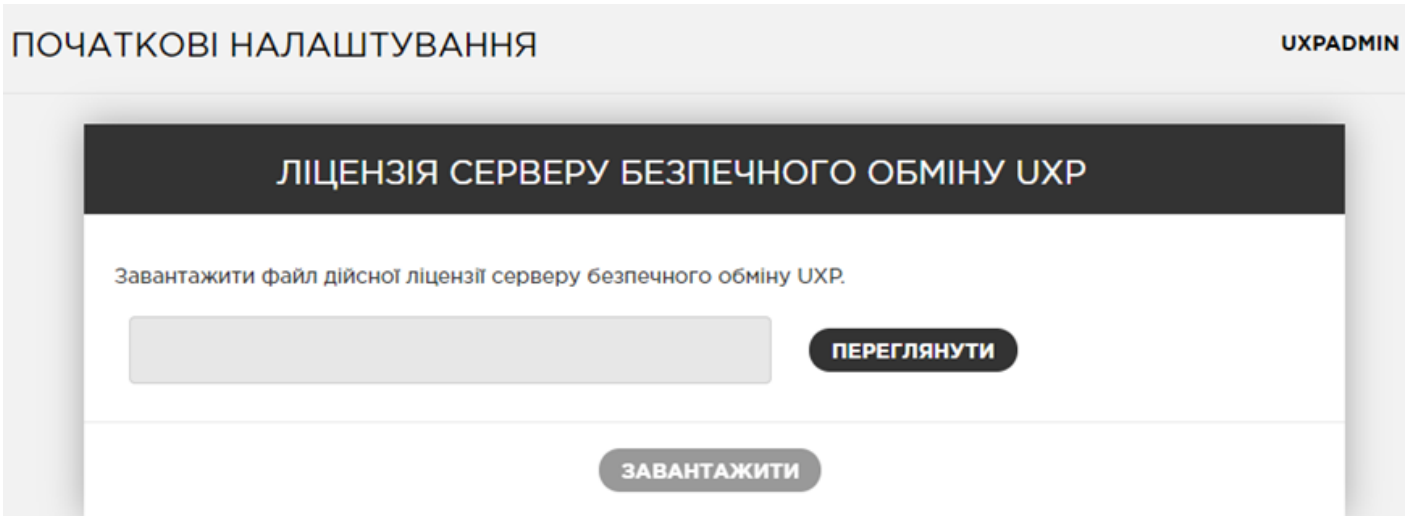
використовуючи атрибути доступу користувача з роллю Адміністратор вебсервісів:



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

> **Примітка.** У першу хвилину після перезапуску ШБО його вебінтерфейс може відображати повідомлення «502 Bad Gateway» (зазвичай менше однієї хвилини). Необхідно оновлювати сторінку входу, 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 тестового середовища member.test.license.lic.



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

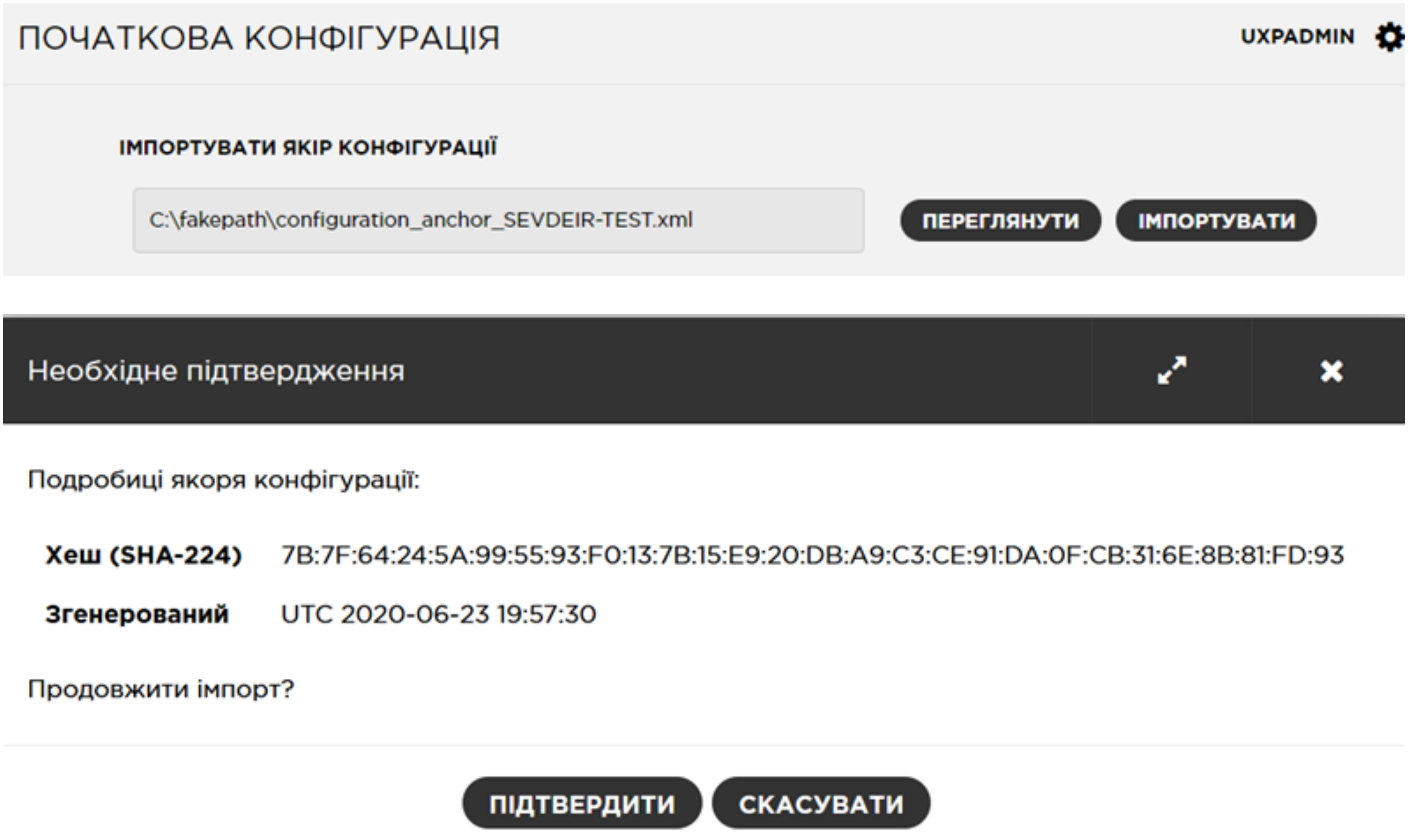
Після завантаження необхідно його підтвердити, натиснувши на кнопку «Зберегти ліцензію».

6.2.2. ????????????? ????? ?????????? ??????

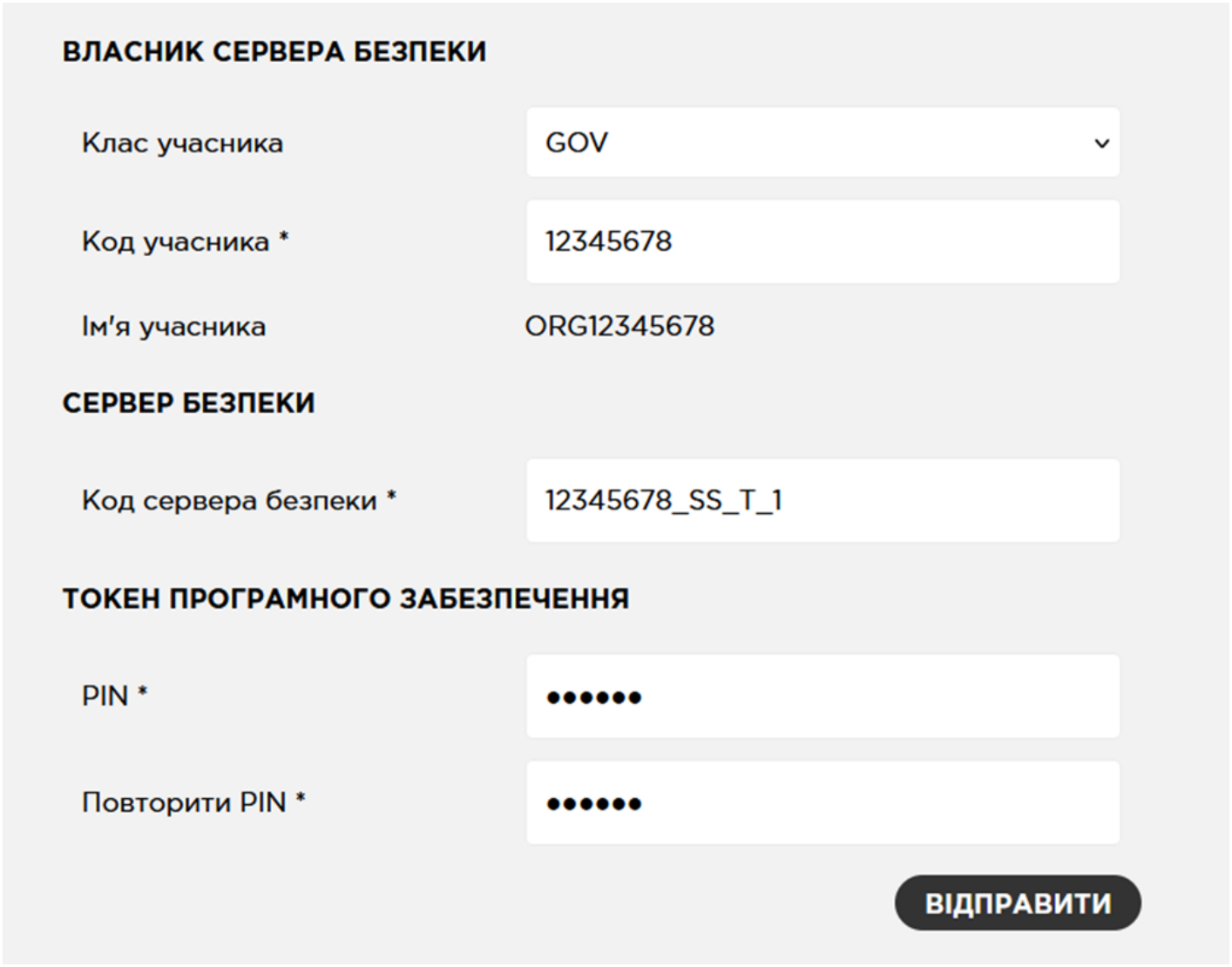
При ініціалізації ШБО необхідно завантажити файл якоря конфігурації тестового середовища (файл configuration anchor).

Файл якоря конфігурації тестового 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»):



Після чого відкриється вікно ініціалізації ШБО:



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». **Важливо!** 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 Каталогу Учасників (після введення коду Учасника) відповідно до заявки на реєстрацію Учасника у системі «Трембіта».
Шлюз безпечного обміну (Security Server)	

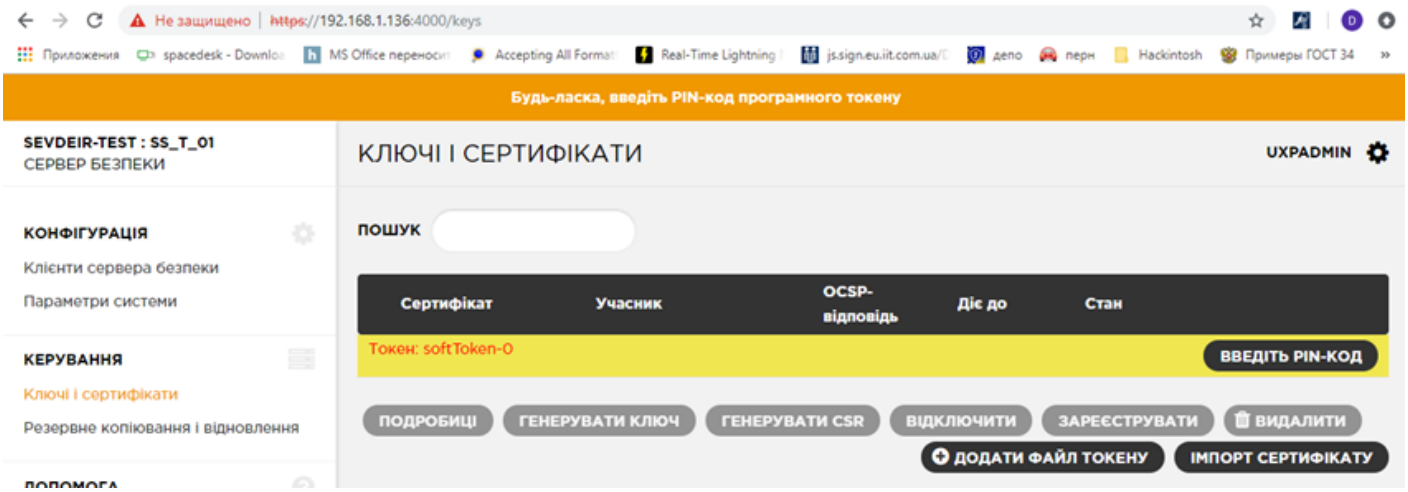
Код сервера безпеки (Security Server Code)	Унікальний код ШБО («сервера безпеки» в вебінтерфейсі) в тестовому середовищі системи «Трембіта», який потрібно створити відповідно до наступного шаблону: MemberCode_SS_T_Number_FreeSymbols, де: **MemberCode** – код ЄДРПОУ організації; **SS** – означення ШБО (security server); **T** – абревіатура тестового середовища системи, не змінюється; > **Важливо!** Варто звернути увагу, що _SS_T_ потрібно вводити великими латинськими літерами з використанням символу нижнього підкреслення «_». **Number** – порядковий номер ШБО організації (наприклад 01, 02, 03 і тд); > **Примітка.** Нумерація ШБО для тестового та промислового середовищ системи незалежна. **FreeSymbols** – (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). > **Важливо!** Додаткові символи повинні містити лише цифри та великі літери англійського алфавіту.
Програмний токен (Software Token)	
PIN	Необхідно придумати PIN-код, який буде використаний для захисту ключів автентифікації, що зберігаються у програмному сховищі (файловій системі ОС). > **Важливо!** Адміністратор вебсервісів має зберігати PIN-код у безпечному місці, оскільки після втрати PIN-коду необхідно відновлювати токен, повторно видавати та реєструвати новий сертифікат автентифікації.
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 «OK».

6.2.2.1. ???????? PIN-???? ??????????? ??????

Шлюз безпечного обміну 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 токену». Це повідомлення вказує на те, що зазначений токен безпеки на даний час заблокований, а особисті ключі не можуть бути використані.

Кожен раз при перезавантаженні ПЗ UXP Security Server або всієї операційної системи ШБО, потрібно вводити PIN-код токену 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:

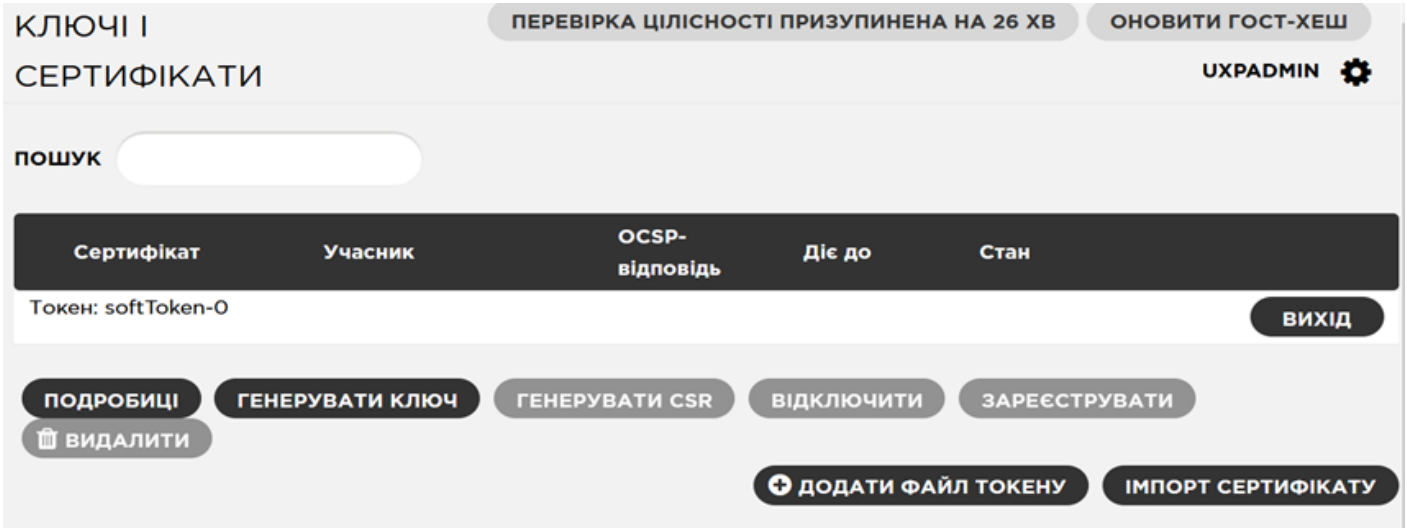
1. Перейти в розділ «Ключі і сертифікати».

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 токену» зникне, а кнопка «Вихід» – з’явиться замість кнопки «Введіть PIN-код»:



6.2.2.2. ??????????? ??????? ???????? ????

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:

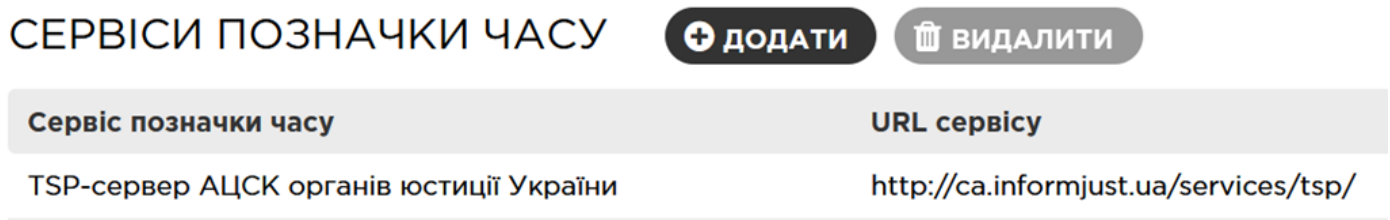
1. Перейти в розділ «Параметри системи». Список серверів позначок часу має бути порожнім («Немає (відповідних) записів»).

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».



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

Версія #6
Admin створив 2024-06-30 20:59:07 UTC
Administrator оновив 2025-11-27 12:34:05 UTC