

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»



ЗАТВЕРДЖУЮ

Ректор НТУ «ХПІ»

Євген СОКОЛ

« 20 » 06 2024 р.

ІНСТРУКЦІЯ
ВИКОРИСТАННЯ ЦЕНТРУ СЕРТИФІКАЦІЇ КЛЮЧІВ

1. РОБОТА З АГЕНТОМ ЄДИНОГО СЕРВІСУ КРИПТОГРАФІЧНИХ ОПЕРАЦІЙ

У веб-браузері перейти за посиланням - <https://cryptocenter.cipher.kiev.ua/> до Клієнту єдиного сервісу криптографічних операцій (ЄСКО).

Стартове вікно Клієнту єдиного сервісу криптографічних операцій показано на Рис. 1.

The screenshot displays the 'Клієнт єдиного сервісу криптографічних операцій' (Client of the Unified Service of Cryptographic Operations) interface. The top header includes the company logo, name 'ТОВ САЙФЕР ПРО', and status indicators for 'Агент ЄСКО' (Agent ESKO) with a 'запустити' (start) button, and 'ЄСКО' (ESKO) with a 'підключено' (connected) status and language toggles for 'УКР' and 'ENG'. A note 'Людям із порушенням зору' (For people with visual impairment) is also present. The main content area has two tabs: 'Особистий ключ' (Personal key) and 'Перевірити ЕП' (Verify EP). The 'Особистий ключ' tab is active, showing two sections: 'Параметри сесії' (Session parameters) and 'Параметри ключа' (Key parameters). In the 'Параметри сесії' section, there is a field for 'Період активації ключа, хв:' (Key activation period, min) with the value '15'. The 'Параметри ключа' section contains several fields: 'КНЕДП:' (KNEDP) with a dropdown menu showing 'Тестовий ЦСК Сайфер'; 'Тип ключа:' (Key type) with a dropdown menu showing '[Файл на диску]'; 'Шлях до контейнеру:' (Container path) with a text input field and a 'Вибрати файл' (Select file) button; and 'Пароль:' (Password) with a text input field and a visibility toggle icon. At the bottom of this section are two buttons: 'Розпочати роботу з ключем' (Start work with key) and 'Очистити форму' (Clear form).

Рис. 1. Стартове вікно ЄСКО

На вкладці «Особистий ключ» у розділі «Параметри сесії» слід вказати у хвилинах період активації ключа, за замовчуванням 15 хв.

На вкладці «Особистий ключ» у розділі «Параметри ключа» слід вказати:

1. КНЕДП/ЦСК, у якому було отримано ключ (надається перелік);
2. Тип ключа: [файл на диску];
3. Шлях до контейнеру: завантажуюємо файловий ключ;
4. Вводимо пароль до файлового ключа, Рис. 2.

Клієнт єдиного сервісу криптографічних операцій
ТОВ САЙФЕР ПРО

Агент ЕСКО ⓘ
запустити

ЕСКО ⓘ
підключено
УКР ENG

Людам із порушенням зору

Особистий ключ | Перевірити ЕП

Параметри сесії

Період активації ключа, хв:
15

Параметри ключа

КНЕДП: НЕДП НТУ «ХПІ» 1

Тип ключа: [Файл на диску] 2

Шлях до контейнеру: Testoviy_Koristuvach1.pfx Вибрати файл 3

Пароль: ***** 4

Розпочати роботу з ключем | Очистити форму

Рис. 2. Заповнення розділу «Параметри ключа»

Після заповнення всіх полів, слід натиснути кнопку «Розпочати роботу з ключем». Відкривається робоча область, де стають доступні всі функції та операції в Агенту ЕСКО, Рис. 3.

Клієнт єдиного сервісу криптографічних операцій
ТОВ САЙФЕР ПРО

00:11:32

Агент ЕСКО ⓘ
запустити

ЕСКО ⓘ
підключено
УКР ENG

Людам із порушенням зору

Особистий ключ | Перевірити ЕП | Створити ЕП | Ключі VPN

Дії

Загальна інформація

Сертифікат ключа підпису

Завершити роботу з ключем

Загальна інформація про ключ ЕП

Повне ім'я	Тестовий Користувач
Серійний номер сертифікату	C5B0BCACC90F40FB
Початок дії	31.07.2023, 17:36:30 GMT+3
Закінчення дії	30.07.2025, 00:00:00 GMT+3
Електронна печатка	Ні
Кваліфікований	Ні
Стартовий	Ні

Рис. 3. Робоча область Агенту ЕСКО

Після завантаження даних ключового контейнеру у вікні «Клієнту єдиного сервісу криптографічних операцій» з'являються такі поля та відповідні опції, Рис. 4:

1. Вкладка «Особистий ключ», яка містить кнопки:

- «Загальна інформація» - коротка інформація про ключі.
- «Сертифікат ключа підпису» - повна інформація про сертифікат ключа підпису. За наявності.
- «Завершити роботу з ключем» - завершується сесія.

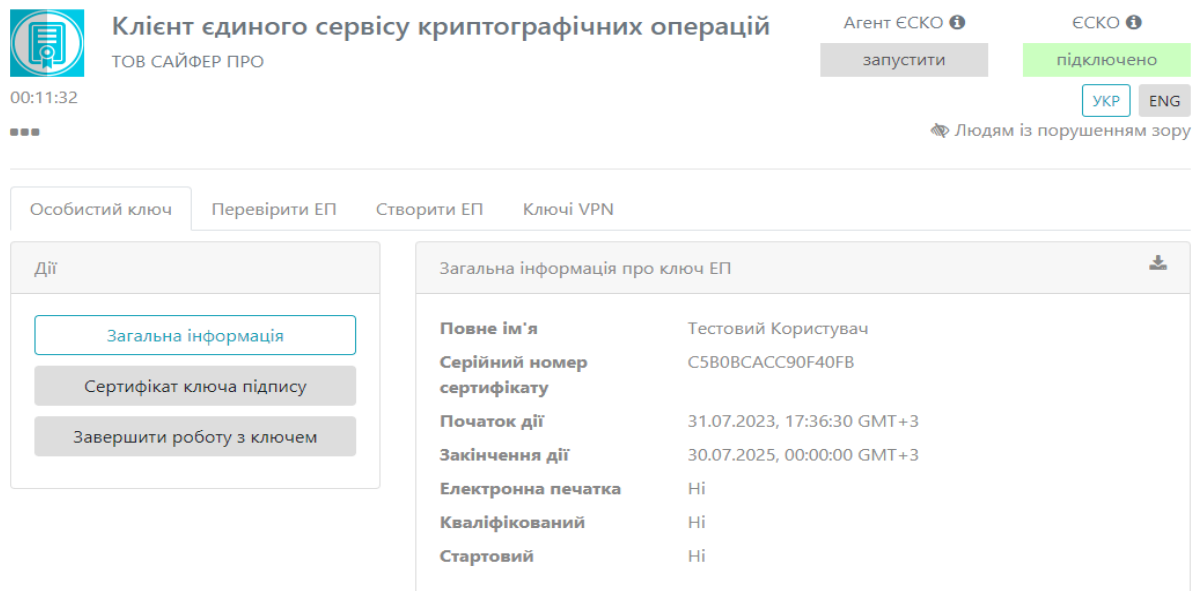


Рис. 4. Робоча область Агенту ЄСКО

2. СТВОРЕННЯ ЕЛЕКТРОННОГО ПІДПИСУ

Вкладка «Створити ЕП» містить такі розділи: Параметри створення ЕП, Текстові дані та Файл.

Обираємо тип підпису – Вбудований або Відкріплений, за необхідності вказуємо позначку «Додати підпис до вже існуючого» (таким чином, можуть підписувати один файл кілька осіб).

Поле «Формат підпису» («З повним даними для перевірки (CAdES-X Long)»).

Обираємо файл, який треба підписати (файл можна обрати тільки один) та натискаємо кнопку «Створити ЕП», Рис. 5.

The screenshot displays the 'Створити ЕП' (Create EP) tab of the 'Клієнт єдиного сервісу криптографічних операцій' (Client of the Unified Service of Cryptographic Operations) application. The interface includes a header with the application name, version (ТОВ САЙФЕР ПРО), and status (Агент ЄСКО, підключено). The main area is divided into three sections: 'Параметри створення ЕП' (EP Creation Parameters), 'Файл' (File), and 'Текстові дані' (Text Data). In the 'Параметри створення ЕП' section, the 'Тип підпису' (Signature Type) is set to 'Відкріплений' (Detached) (marked with a red circle 2), and the 'Формат підпису' (Signature Format) is set to 'З повним даними для перевірки (CAdES-X Long)' (marked with a red circle 3). The 'Додати підпис до вже існуючого' (Add signature to existing) checkbox is unchecked. In the 'Файл' section, there is a large empty box for file selection and a dashed box for file upload (marked with a red circle 1). The 'Створити ЕП' (Create EP) button is highlighted.

Рис. 5. Вкладка «Створити ЕП»

Натискаємо кнопку «Зберегти ZIP» для збереження архіву з підписом, Рис. 6.

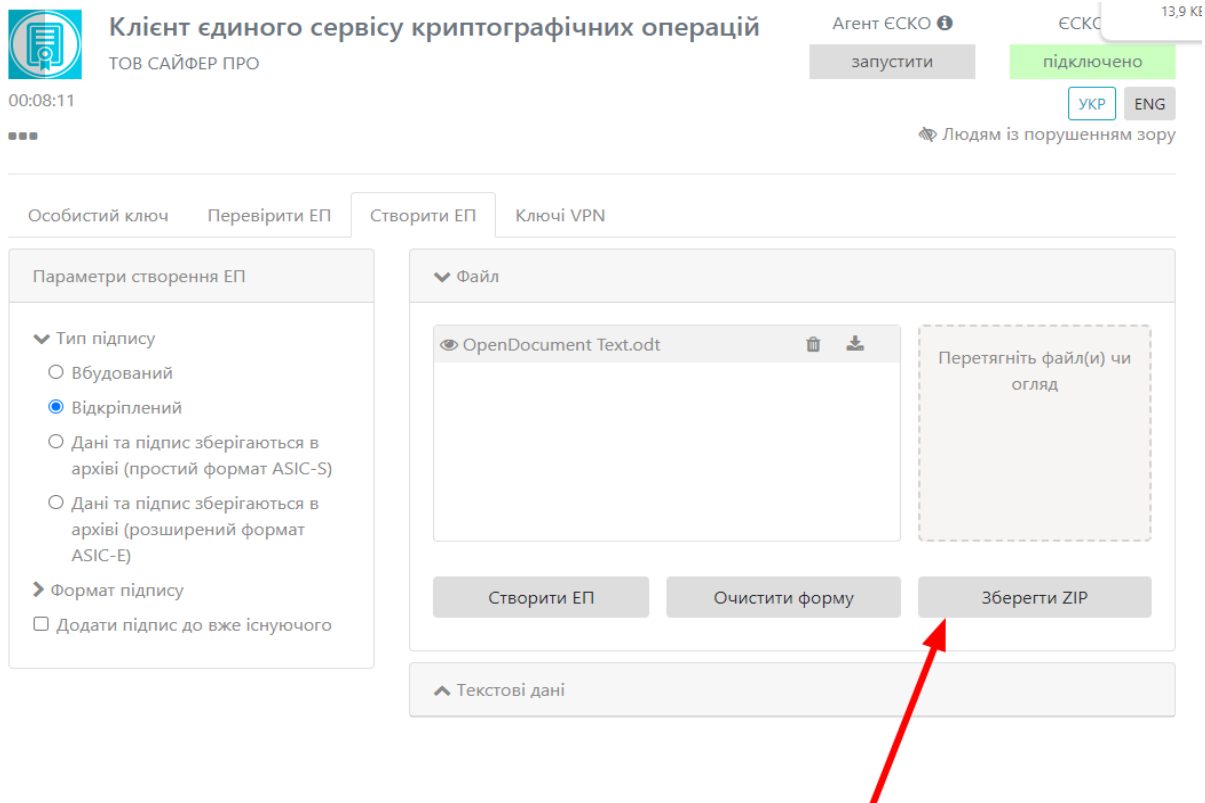


Рис. 6. Збереження архіву з підписом

Також можна продовжити працювати в цьому вікні та підписувати інші файли не виходячи із системи. Процедура ідентична.

3. ПЕРЕВІРКА ПІДПISУ

Дана функція є доступною і без ключа.

Для перевірки підпису натискаємо на вкладку «Перевірити ЕП».

1. Обираємо файл, який підписували (документ без електронного підпису).
2. Обираємо раніше збережений документ з підписом.
3. Натискаємо кнопку Перевірити ЕП, Рис. 7.

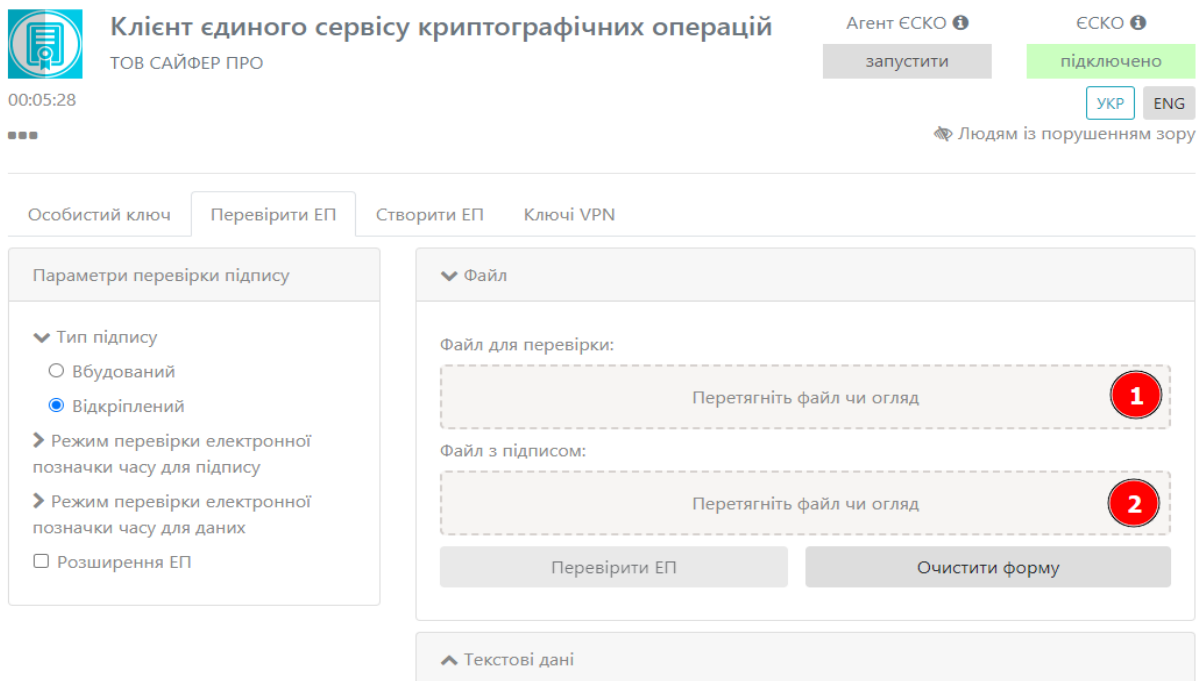


Рис. 7. Вкладка «Перевірити ЕП»

Перевірка пройшла успішно, Рис. 8.



Клієнт єдиного сервісу криптографічних операцій

ТОВ САЙФЕР ПРО

00:04:16

...

Агент ЕСКО ⓘ

запустити

ЕСКО ⓘ

підключено

УКР

ENG

🔊 Людям із порушенням зору

Особистий ключ

Перевірити ЕП

Створити ЕП

Ключі VPN

Параметри перевірки підпису

▼ Тип підпису

☐ Вбудований

☒ Відкріплений

➤ Режим перевірки електронної
позначки часу для підпису

➤ Режим перевірки електронної
позначки часу для даних

☐ Розширення ЕП

▼ Файл

Файл для перевірки:

OpenDocument Text.odt

Очистити

Файл з підписом:

OpenDocument Text.odt.p7s

Очистити

Протокол перевірки

Скопіювати

Підпис 1	Підписувач: Тестовий Користувач
Дійсний	Організація: НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
Некваліфікований	Посада: Тестувальник РНОКПП: 3107230001 ЄДРПОУ: 02071180 КНЕДП: НЕДП НТУ "ХПІ"
	Серійний номер сертифікату підписанта: C5B0BCACC90F40FB
	Дата підпису: 28.05.2024, 12:01:48 GMT+3
	Електронна позначка часу даних: дійсна; 28.05.2024, 12:01:49 GMT+3
	Серійний номер сертифікату електронної позначки часу даних: 5457EB6F28771F9F
	Електронна позначка часу підпису: дійсна; 28.05.2024, 12:01:49 GMT+3
	Серійний номер сертифікату електронної позначки часу ЕП: 5457EB6F28771F9F
	Електронна печатка: Ні
	Кваліфікований сертифікат: Ні
	Засіб КЕП: Ні
	Тип засобу КЕП: Не визначено
	Тип контейнеру: Відкріплений
	Формат підпису: 3 повними даними для перевірки (CAdES-X Long)

Рис. 8. Результат перевірки ЕП

4. ГЕНЕРАЦІЯ КЛЮЧА

4.1. Генерація ключа при особистій присутності.

- Співробітник особисто приходить до адміністратора з флешкою та всіма необхідними документами.
- Адміністратор генерує ключ, пароль для контейнера надає співробітник.
- Ключ зберігаються на флешці співробітника.

4.2. Генерація ключа при віддаленому підключенні.

- Співробітник надсилає документи на електронну пошту.
- Співробітник підключається до адміністратора через AnyDesk або TeamViewer.
- Адміністратор генерує ключ.
- Співробітник самостійно вводить пароль до контейнера у відповідному полі. Адміністратору пароль буде невідомий.

4.3. Генерація ключа offline.

- Співробітник надсилає документи на електронну пошту.
- Адміністратор генерує ключ без присутності співробітника.
- Адміністратор створює пароль для контейнера.
- Адміністратор передає пароль та контейнер зручними каналами зв'язку співробітнику.
- Співробітник може самостійно змінити пароль до контейнера у своєму екземплярі ключа. Оригінальний пароль залишається у адміністратора.

Завідувач кафедри кібербезпеки

Сергій БУСЕБ