

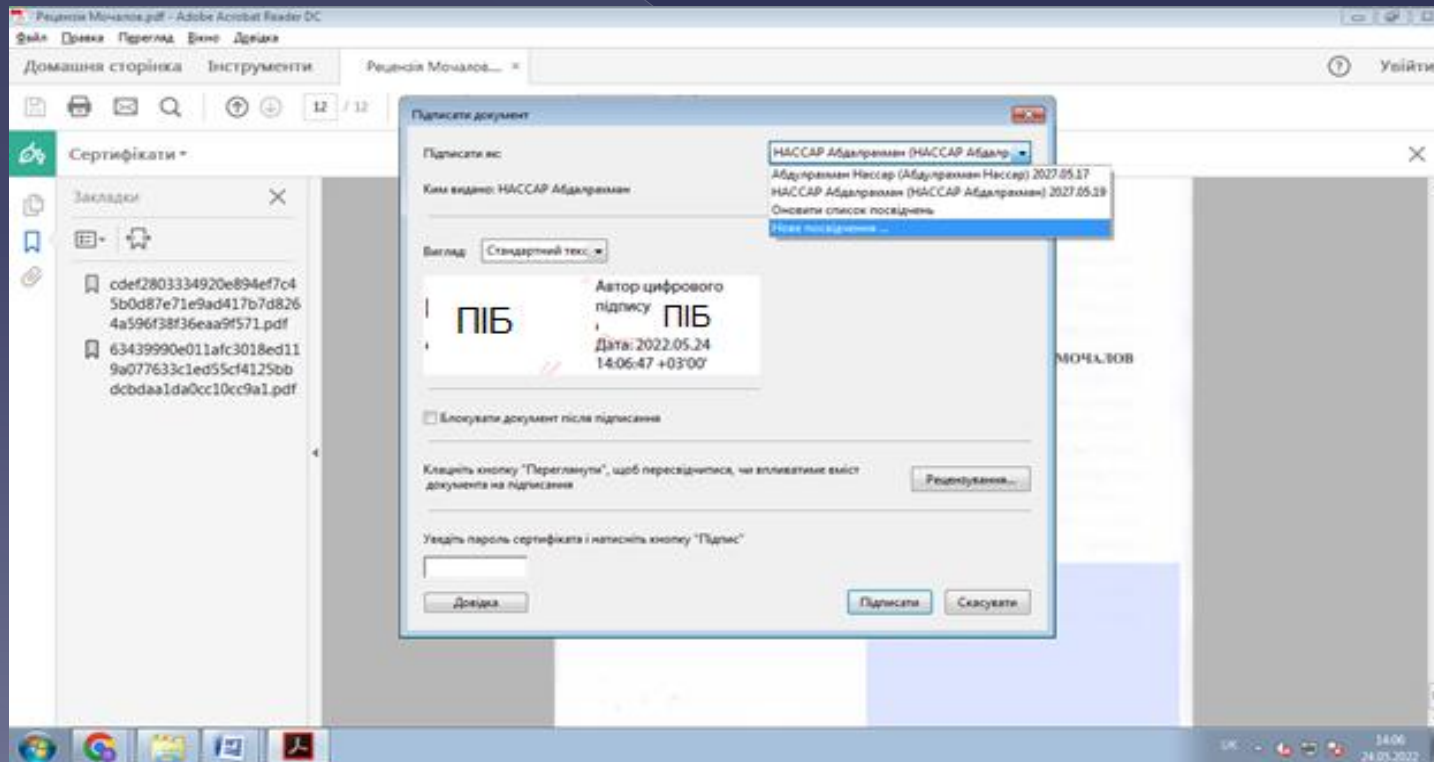


Відділ СРСВР

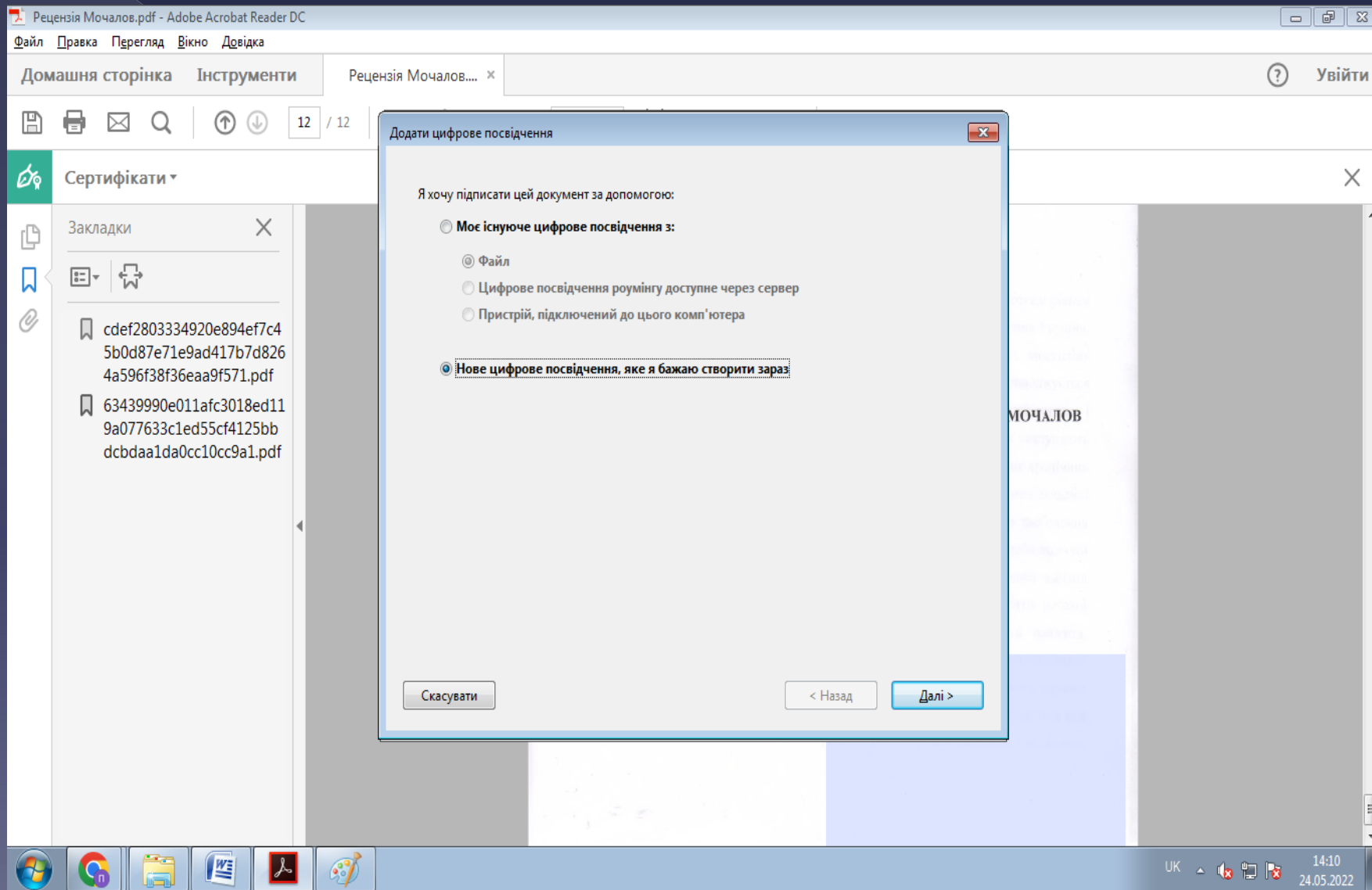
**СТВОРЕННЯ ЕЛЕКТРОННИХ КОПІЙ
ДИСЕРТАЦІЙ ТА РЕЦЕНЗІЙ (ВІДГУКІВ)
У ФОРМАТІ PDF/A З ТЕКСТОВИМ
ШАРОМ З НАКЛАДЕННЯМ
ЕЛЕКТРОННОГО ПІДПИСУ
РЕЦЕНЗЕНТА
(ОФІЦІЙНОГО ОПОНЕНТА)**

Ужгород - 2024

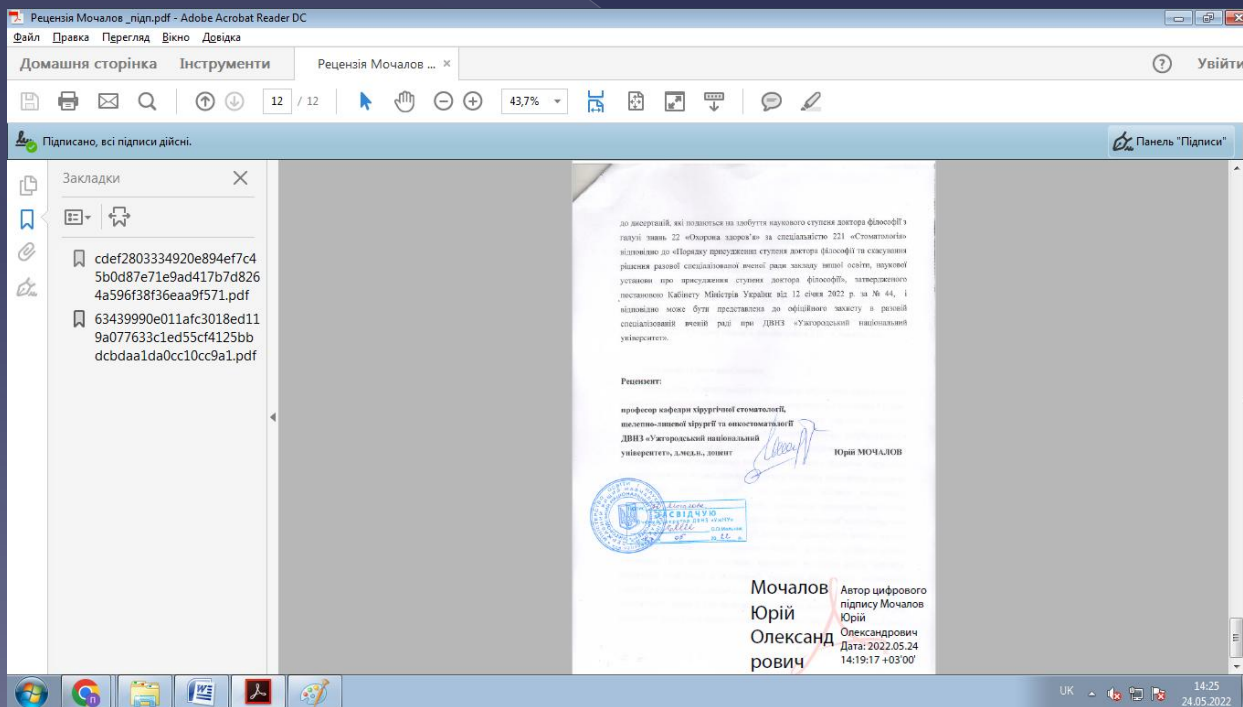
- ❖ Накладання текстового шару (один із можливих варіантів; можливо використовувати свій алгоритм накладання текстового шару):
 1. Відкриваємо в програмі Adobe Acrobat Reader pdf файл (відгук або рецензія, дисертація). Важливо, щоб текст можна було копіювати з документа.
 2. Далі «Інструменти» -> «Сертифікати» -> «Додати цифровий підпис» -> Згідно скріна «Нове посвідчення»:



❖ «Нове цифрове посвідчення, яке я бажаю створити зараз»



- ❖ «Нове цифрове посвідчення, яке я бажаю створити зараз» -> «Далі»
- ❖ «Створити файл цифрового посвідчення PKCS#12-> «Далі»
- ❖ «Додати цифрове посвідчення» і ввести інформацію згідно запиту (ім'я, організація і т.д.) -> «Далі» -> «Додати цифрове посвідчення» -> Створити пароль-> «Завершити»
- ❖ «Увести пароль сертифікату і натиснути кнопку «Підпис»»



Після збереження даного файлу конвертувати в PDF/A за допомогою будь якого конвертора (який зберігає підпис).

Наприклад:

- ❑ <https://avepdf.com/ru/convert-to-pdfa>
- ❑ <https://www.freepdfconvert.com/ru/pdf-to-pdfa>
- ❑ <https://xodo.com/uk/pdf-y-pdfa>
- ❖ -> Далі зберігаємо



Для підпису дисертації використовуєте сервіс
центрального засвідчувального органу Міністерства
цифрової трансформації України

<https://czo.gov.ua/>

АБО

<https://diia.gov.ua/services/pidpisannya-dokumentiv>

ВАЖЛИВО:

потрібно накласти електронні ключі в
форматі CAdES. Дані та підпис
зберігаються в CMS файлі .p7s

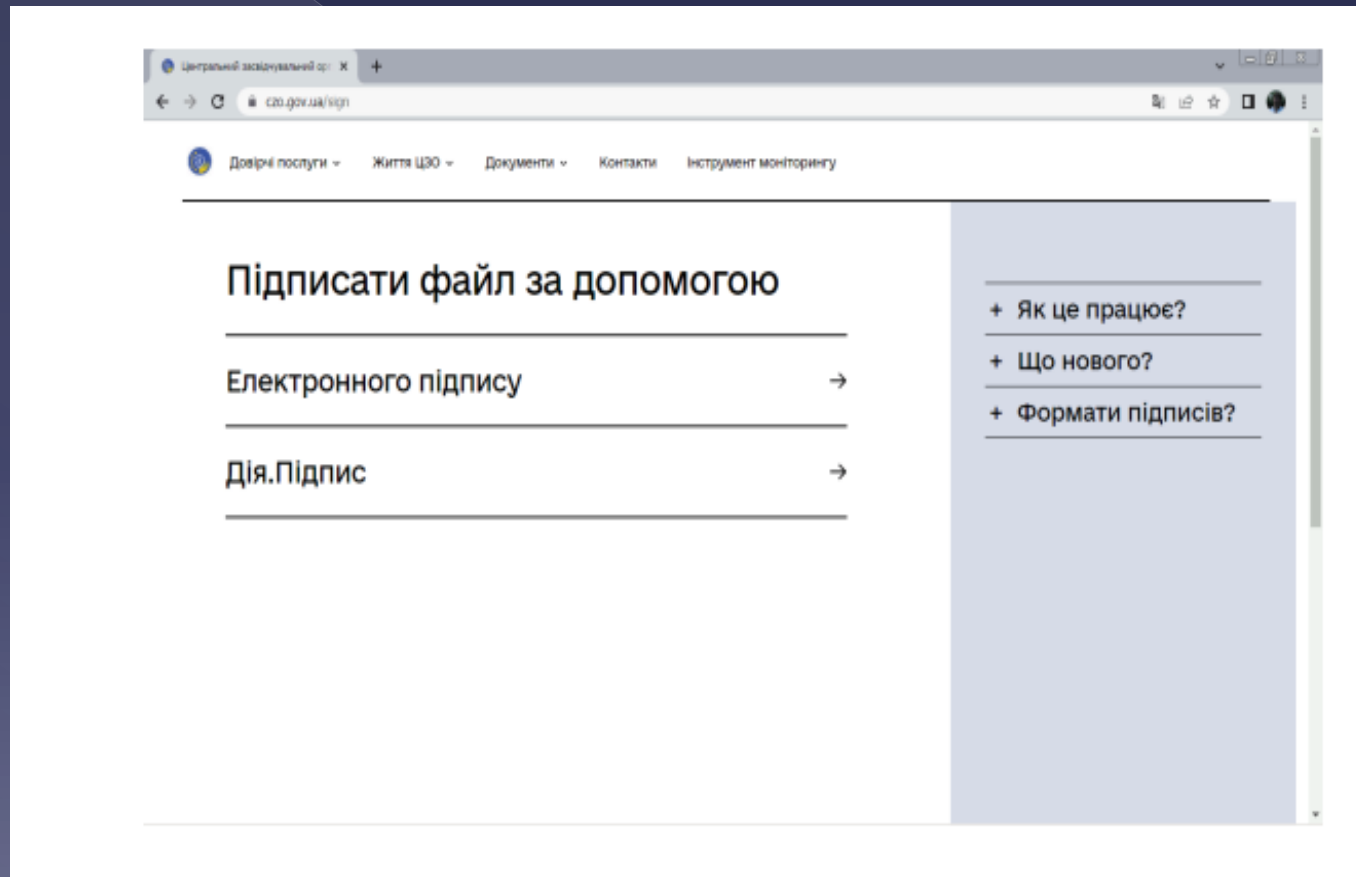
АБО

PAdES. Дані та підпис зберігаються в PDF
файлі (*.pdf)



На даній сторінці <https://czo.gov.ua/> в меню вибираєте “Довірчі послуги” далі “Підписати документ” тут вибираєте підписати файл за допомогою електронного підпису, після чого необхідно виконати 4 кроки

1.



2. Завантажуєте ваш електронний ключ і вказуєте пароль захисту ключа

Центральний засвідчувальний орган

← → ↻ czo.gov.ua/sign

Довірчі послуги Життя ЦЗО Документи Контакти Інструмент моніторингу

Крок 1 з 4

Зчитайте ключ

Файловий Токен Хмарний

Кваліфікований наданий електронних довірчих послуг

Визначити автоматично

Перетягніть сюди файл ключа
або завантажте його зі свого носія
(зазвичай його назва "Key-6.dat" або *.pfx, *.pk8, *.zst, *.jks)

Пароль захисту ключа

Назад Зчитати

Що таке файловий носій?

Файловий носій – це спеціальний файл, який містить ваш особистий ключ.

Зазвичай цей файл має назву Key-6 з розширенням *.dat (зустрічаються також розширення *.pfx, *.pk8, *.zst, *.jks).

Для того, щоб скористатись файловим носієм, вам необхідно:

1. Обрати зі списку свого надавача електронних довірчих послуг – суб'єкта, до якого ви зверталися для отримання електронного підпису.
2. Завантажити із зовнішнього носія чи власного комп'ютера файл з вашим особистим ключем.

3. Перевірка ваших даних

Центральний засвідчувальний ЦЗУ

← → ↻ 🏠 🔍 <https://czo.gov.ua/sign> ☆ 📧 ⬇️ 🔗 🖨️ ✎️ ☰

Крок 2 з 4

Перевірте дані

Ваше прізвище, ім'я

Організація
ФІЗИЧНА ОСОБА
РНОКПП
2825804735

Сертифікати

📄 ЕЦП (ДСТУ 4145)
EU-2B6C7DF9A3891DA1040000002FA5BF00AEC06903.cer ⬇️

📄 Протоколи розподілу ключів (ДСТУ 4145)
EU-2B6C7DF9A3891DA1040000002FA5BF00AFC06903.cer ⬇️

Назад

Далі

Що таке сертифікат?

Сертифікат є засобом підтвердження приналежності відкритого (публічного) ключа його власникові.

Сертифікат видається кваліфікованим надавачем електронних довірчих послуг та використовується для перевірки, що відкритий ключ належить саме тому власнику, чиї дані зазначено в ньому.

Файл сертифікату має розширення ".cer", зазвичай зазначені файли можливо відкрити вбудованими засобами операційної системи.

Файл сертифікату містить ідентифікаційні дані, які однозначно визначають кваліфікованого надавача та користувача електронних довірчих послуг.

4. Підписати та зберегти, натискаємо «Ні, обрати інший формат»

Центральний засвідчувальний

← → ↻ 🏠 <https://cso.gov.ua/sign> ☆

Довірчі послуги ▾ Життя ЦЗО ▾ Документи ▾ Контакти Інструмент моніторингу

Крок 3 з 4

Підписати та зберегти

👉 **Рекомендуємо підписувати документи у форматі ASiC-E.**

Це уніфікований формат електронного документообігу, який гарантує, що ваші документи прийматимуть всі держоргани.

Так, підписати в форматі ASiC-E **Ні, обрати інший формат**

Що таке ASiC?

ASiC – структурований контейнер, що дозволяє зберігати набір файлових об'єктів з пов'язаними е-підписами та/або е-позначками часу, що відповідає специфікації ZIP.

ASiC-S дозволяє зберігати один файловий об'єкт з пов'язаним е-підписом та в подальшому додавати нові. Також дає можливість додавати файли для захисту е-позначок часу.

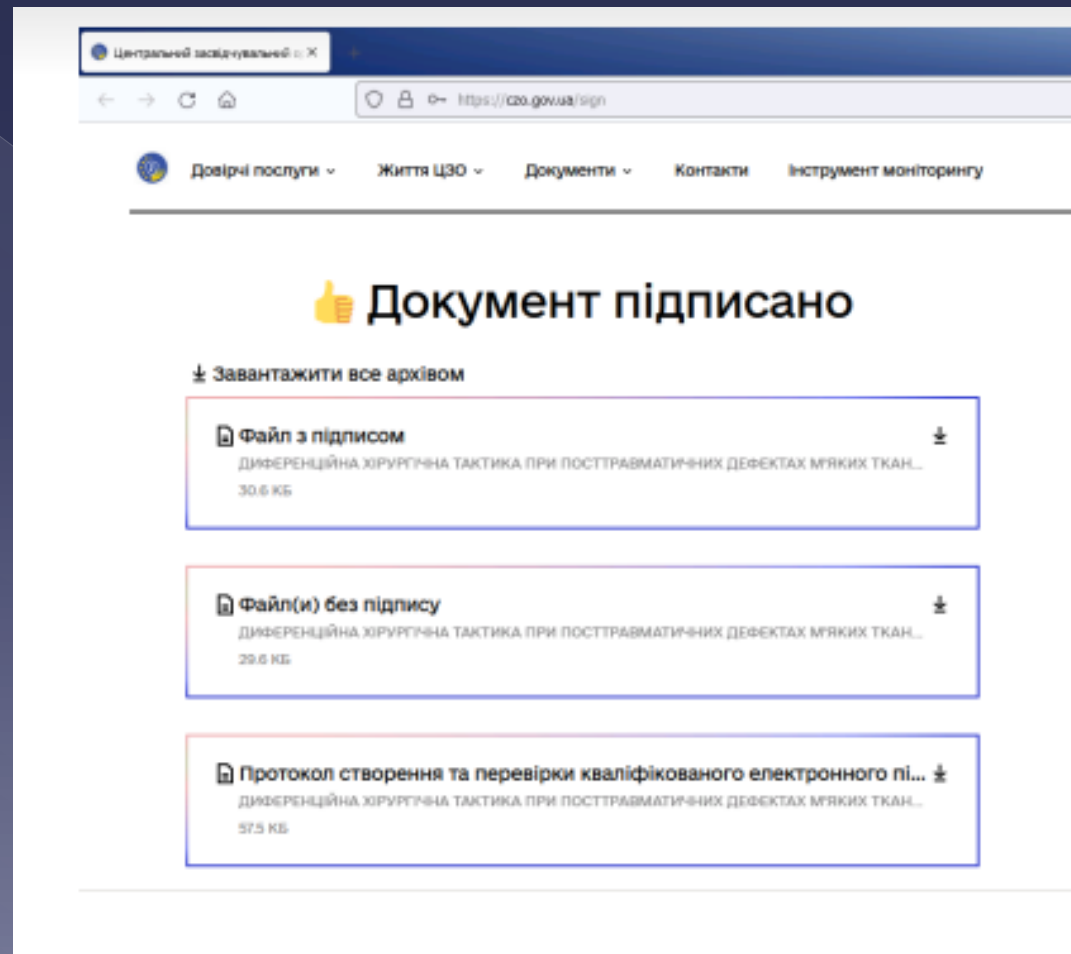
ASiC-E дозволяє зберігати один або кілька файлових об'єктів з пов'язаними е-підписами та в подальшому додавати файлові об'єкти, файли е-підпису та

Підписати та зберегти, на цьому кроці завантажуєте вашу дисертацію у форматі pdf/A з текстовим шаром, обираєте CAdES. Дані та підпис зберігаються в CMS файлі .p7s або PAdES. Дані та підпис зберігаються в PDF файлі (*.pdf) і натискаєте підписати.

Після чого ваша дисертація буде підписана і сформовані три файли - файл з підписом, файл без підпису, протокол створення та перевірки, які можете завантажити в архіві.

Можна також діяти згідно інструкції
НАЗЯВО:

<https://wiki.naq.gov.ua/system/kep>



Дякую за увагу

