

# Найчастіші помилки під час роботи з електронними ключами та шляхи їх вирішення

*Наразі українці вимушені жити в умовах війни. Багато хто переселився з окупованих територій у більш спокійні регіони, дехто переїхав за кордон, у більшості немає можливості працювати в офісному приміщенні. Серед таких українців чимало замовників та постачальників, які працюють віддалено та яким, зокрема для участі або оголошення процедури закупівлі в електронній системі закупівель (далі — ЕСЗ), необхідно використовувати електронний підпис. Нерідко виникають складнощі з використанням ключів на відстані. У цьому матеріалі наведемо найтипівіші проблеми з цього питання, які виникають, та надамо поради щодо їх вирішення.*

Згідно з підпунктом 6 пункту 24 постанови КМУ від 09.12.2020 № 1236 «Про встановлення карантину та запровадження обмежувальних протиепідемічних заходів з метою запобігання поширенню на території України гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2» **протягом періоду карантину тимчасово дозволяється:** застосування електронних підписів чи печаток на базі сертифікатів відкритого ключа, які видав кваліфікований надавач електронних довірчих послуг (далі — ЕДП) без відомостей стосовно того, що особистий ключ міститься в засобі кваліфікованого електронного підпису чи печатки, користувачами ЕДП для проведення електронної взаємодії, електронної автентифікації та ідентифікації фізосіб, юридичних осіб, а також представників юридичних осіб у разі, коли законодавством передбачено застосування лише кваліфікованих електронних підписів чи печаток (засобів кваліфікованого електронного підпису чи печатки, кваліфікованих ЕДП) або засобів електронної ідентифікації з високим рівнем довіри, крім здійснення правочинів в електронній формі, стосовно яких необхідне нотаріальне посвідчення та / або держреєстрація в установлених законом випадках та випадках, пов'язаних із високим ризиком для інформаційної безпеки, що визначається власниками відповідних інформаційних та інформаційно-комунікаційних систем з урахуванням обмежень, які встановлює абзац 2 частини 2 статті 17 Закону України «Про електронні довірчі послуги».

Відповідно до пункту 1 вищезгаданої постанови КМУ постановив згідно зі [статтею 29](#) Закону України «Про захист населення від інфекційних хвороб» установити з 19.12.2020 до 31.05.2022 на території України карантин, щоб запобігти поширенню в Україні хвороби COVID-19, викликаного коронавірусом SARS-CoV-2.

Таким чином, **представники бізнесу можуть користуватися електронними підписами та печатками на базі кваліфікованих сертифікатів відкритих ключів (тобто УЕП) до 31.05.2022**, а представники органів державної влади та інші суб'єкти, визначені абзацом 2 частини 2 статті 17 ЗУ «Про електронні довірчі послуги», з 07.11.2020 мають

користуватись виключно **КЕП на захищеному носії**.

Отож, представникам бізнесу після скасування карантину **слід бути готовими замінити свій електронний підпис на КЕП на захищеному носії**.

## Який носій вважається захищеним

На сьогодні в Україні широко використовуються два типи захищених носіїв:

**Токен** (або апаратний ключ) — фізичний носій, який є флеш-накопичувачем із присвоєним йому унікальним інвентарним номером, що затверджується перед видачею Держслужбою спецзв'язку. Головні фактори, що забезпечують захищеність та цілісність підпису на токені:

- під час процедури підписання користувачем документа сервіс електронного документообігу проглядає та перевіряє не тільки сам файл підпису, а й параметри його носія;
- ключ не копіюється з токена на інший пристрій, оскільки носій захищений від відкриття даних;
- встановлена максимально допустима кількість введень паролю.

**Хмарне сховище в мережевому криптомодулі** — програмне середовище, яке має необхідні ступені захисту від втручання, копіювання чи видалення сторонніми особами. Електронний підпис, що зберігається у такому хмарному середовищі, захищений аналогічно до файлу на токені та має додаткові переваги:

- немає потреби зберігати фізичний носій, який можна пошкодити чи загубити;
- файл підпису доступний для власника з будь-якого електронного пристрою (у тому числі зі смартфона чи планшета) та в будь-який час.

Відповідно до [частини 4 статті 18 Закону України «Про електронні довірчі послуги»](#) саме КЕП — підпис із високим рівнем довіри — прирівнюється до власноручного.

Розглянемо детальніше основні складнощі, з якими можуть стикатися працівники під час використання електронних ключів, та загальні варіанти самостійного вирішення цих ситуацій. У разі появи якоїсь помилки, коли не маєте змоги зв'язатися з АЦСК, що видав електронний ключ, задля налаштування його правильної роботи, ви можете виконати певні дії, які здатні допомогти самостійно вирішити низку труднощів та налаштувати роботу ключа.

## Ситуація 1. Якщо відповідальна / уповноважена особа перебуває поза межами України, КЕП залишила на

## робочому місці й не має його при собі

По-перше, хочемо наголосити, що згідно з положеннями постанови КМУ від 12.04.2022 № 440 робота державних службовців та працівників державного органу за межами України допускається лише в разі службового відрядження, оформленого в установленому порядку.

Якщо ж ці обмеження не застосовуються до працівника та він має змогу працювати з-за кордону, для вирішення питання щодо переведення існуючого КЕП у хмарне середовище в мережевому криптомодулі або замовлення нового хмарного ключа **слід в обов'язковому порядку звертатися напряму до АЦСК** для уточнення умов, бо кожен АЦСК має свої вимоги та можливості по оформленню.

Також нагадуємо про те, що 21.04.2022 було зареєстровано законопроект № 7309, спрямований на врегулювання можливості для суб'єктів господарювання використовувати електронні цифрові підписи й печатки у сфері електронних довірчих послуг.

Таким чином, Верховна Рада України планує тимчасово запустити процедуру визнання нашою країною іноземних ЕДП, поки з Євросоюзом не буде укладена угода про взаємне визнання дійсними кваліфікованих ЕДП. Тому в найближчому майбутньому цілком вірогідно, що наша засвідчувальна система зможе розпізнавати й кваліфікувати електронні підписи, видані іншими державами.

## Ситуація 2. Якщо відповідальна / уповноважена особа перебуває поза межами України та КЕП має при собі, але закінчується термін дії електронного ключа

Відповідно до положень постанови Кабінету Міністрів України від 17.03.2022 № 300 «Деякі питання забезпечення безперебійного функціонування системи надання електронних довірчих послуг» здійснюється **автоматичне формування нових сертифікатів** відкритих ключів усім користувачам за один день до закінчення строку чинності старих сертифікатів, терміном дії на один рік. При цьому особистий ключ користувача не змінюється.

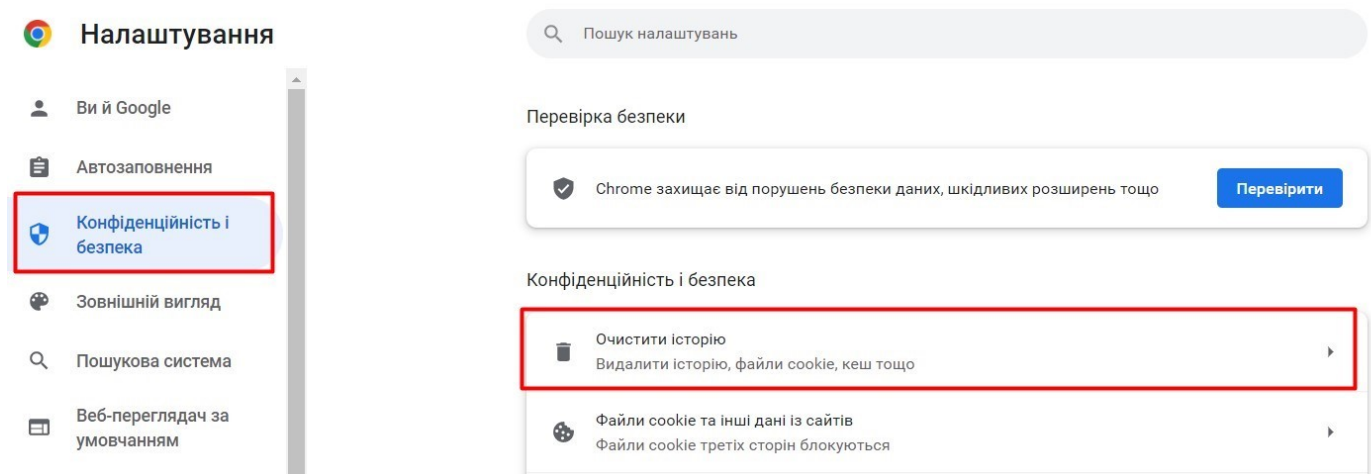
Крім цього, користувачі, які мають чинні сертифікати (до закінчення строку чинності сертифікатів залишилося декілька днів), незмінні реєстраційні дані (ПІБ, адреса реєстрації місця проживання, код ЄДРПОУ організації тощо) чи особистий ключ, доступний лише користувачу та який не є скомпрометованим, можуть на офіційному інформаційному ресурсі КН ЕДП ІДД ДПС (<https://acskidd.gov.ua>) дистанційно сформувати нові сертифікати.

## Ситуація 3. Не відображається файл ключа удосконаленого електронного підпису (УЕП) або кваліфікованого електронного підпису (КЕП)

Причиною може бути закешованість браузера, тому в першу чергу рекомендуємо очистити кеш. У кожному браузері принцип схожий.

**У браузері Chrome** слід натиснути на позначку з трьома крапками у правому верхньому кутку екрана та вибрати пункт «Налаштування». Потім виберіть «Конфіденційність та безпека».

У верхній частині вікна, що відкрилося, виберіть часовий діапазон «За весь час» та позначте галочками: «Файли cookie та інші дані сайтів» і «Зображення та інші файли, збережені в кеші». Натисніть кнопку «Видалити дані». Після цього оновіть сторінку браузера.



**У браузері Opera** слід перейти в розділ налаштувань користувача (клік по головній кнопці в лівому верхньому куті інтерфейсу). У новому вікні перейдіть на вкладку «Додатково — Безпека». Натисніть кнопку «Очистити історію відвідувань».

**У браузері Mozilla Firefox** у верхньому правому куті слід натиснути піктограму меню, перейти в бібліотеку, натиснути «Історія» та «Видалити історію». У діапазоні часу для очищення виберіть «Усі», встановіть прапорці пунктів «Куки та Кеш» і натисніть кнопку «Видалити зараз».

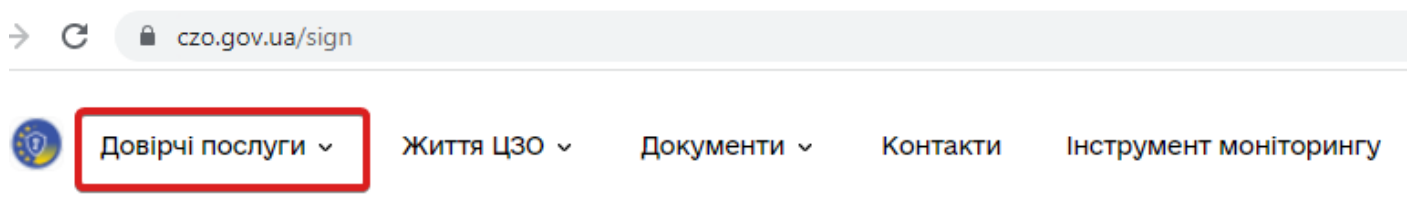
## Ситуація 4. Виникла помилка при взаємодії з криптографічною бібліотекою під час підписання

## кваліфікованим електронним підписом (КЕП), або виникла помилка з файловим сховищем сертифікатів та СВС, або не відображається файл ключа

Для вирішення цієї проблеми необхідно перевірити, чи програма агента підпису **ІТ Користувач ЦСК-1.3. Агент підпису** встановлена на комп'ютер та коректно налаштована.

Перейдіть на [сайт Центрального засвідчувального органу](#) (далі — ЦЗО), відкрийте розділ «Довірчі послуги — Підписати документ — Підписати файл за допомогою електронного підпису», виберіть «Токен» та слідкуйте за вказівками на екрані.

Для того щоб завантажити або оновити версію програми **ІТ Користувач ЦСК-1.3. Агент підпису**, натисніть на «[Інсталяційний пакет бібліотеки підпису \(web-розширення\)](#)».



Крок 1 з 4

### Підписати файл за допомогою

Файловий **Токен** Хмарний

Для роботи з криптографічною бібліотекою необхідно встановити додаткове програмне забезпечення (web-бібліотеку підпису) після чого натиснути "Оновити сторінку"

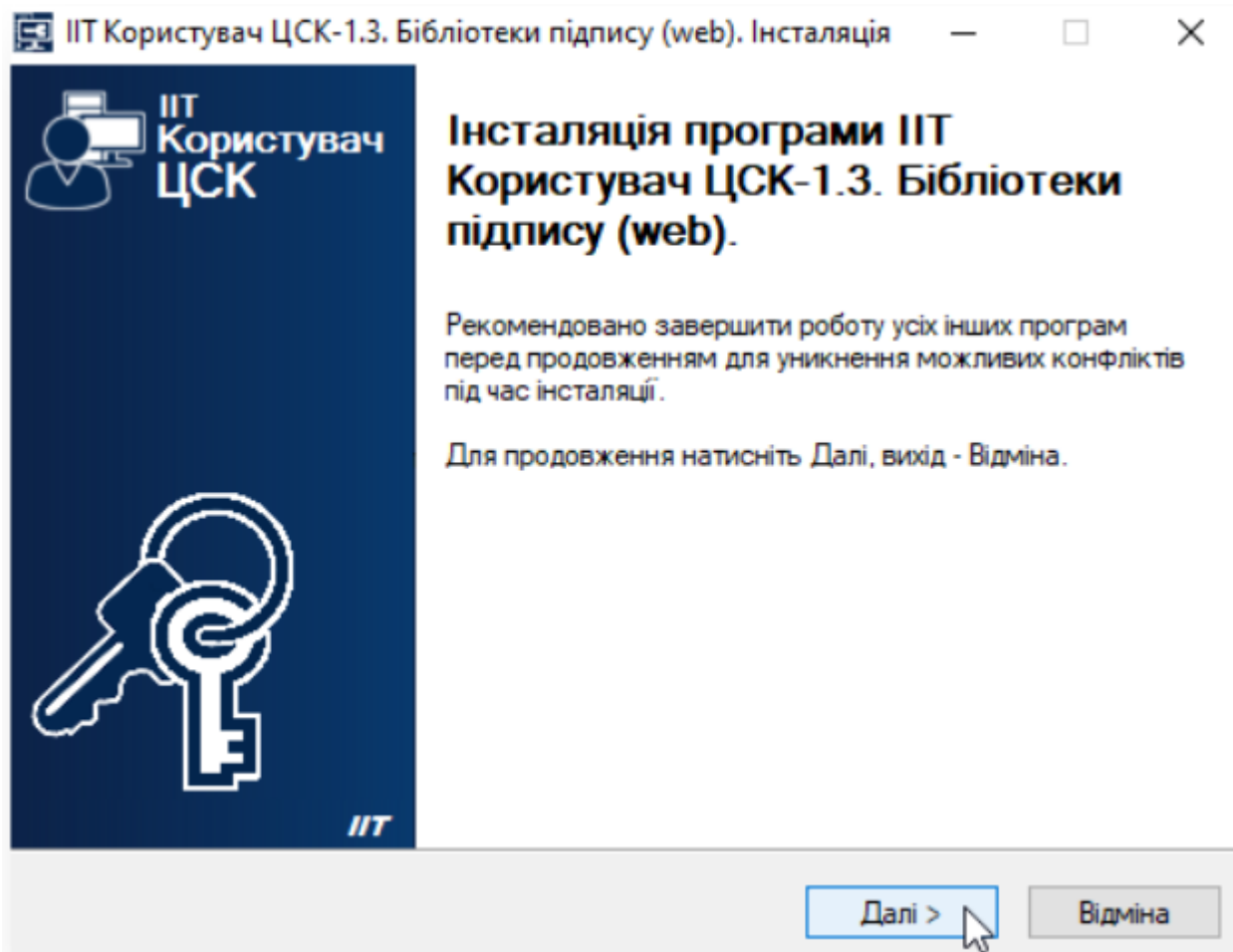
[Інсталяційний пакет бібліотеки підпису \(web-розширення\)](#)

[Настанова користувача](#)

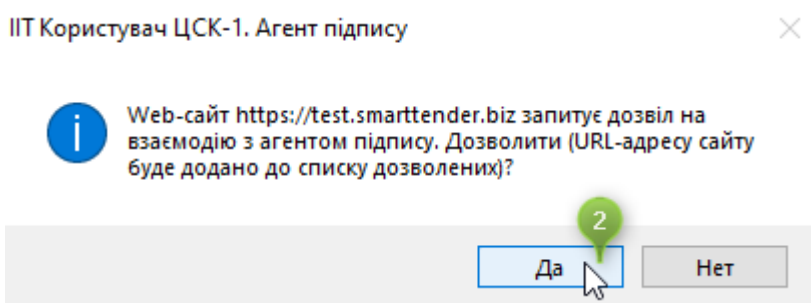
**Оновити сторінку**

Інший варіант завантаження оновленої версії програми — це завантажити програму за [посиланням](#). Запустіть завантажений файл **EUSignWebUpdate.exe**, натисніть «Далі» та встановіть, погоджуючись з умовами використання. Виберіть «**Я приймаю цю угоду**» і

натисніть «Далі».



Після встановлення програми, під час активації чек-бокса «**Апаратний ключ**» система буде запитувати дозвіл на взаємодію з агентом підпису. Для підтвердження натисніть «**Так**»:



Якщо після цих дій електронний підпис не буде відображатись, то сайт ЦЗО запропонує налаштувати проху-сервер. Користуючись вказівками на екрані, заповніть DNS-ім'я чи IP-адресу сервера.



Що таке токен?

Виникла помилка при зчитуванні особистого ключа. Опис помилки: Надавач не підтримує автоматичний пошук сертифіката за ос. ключем. Необхідно обрати надавача самостійно

 [Налаштувати проху-сервер](#)

Кваліфікований надавач електронних довірчих послуг

Визначити автоматично

Носій особистого ключа

193210002f860902(е.ключ чи смарт-карта Автор 338 (PKCS#11))

Пароль захисту ключа

.....

## Ситуація 5. З'являється помилка, коли встановлено актуальний ІІТ Користувач ЦСК-1.3. Агент підпису та програму запущено, а апаратний ключ зчитується під час накладення підпису в інших браузерях

Для усунення помилки достатньо встановити розширення для браузера, яке розміщено у меню налаштувань браузера. Знайти його можна за ключовим словом «ІІТ».

[Разные](#) > [Расширения](#) > [ИИТ Пользователь ЦСК-1. Библ. подп. \(web-p.\)](#)



ИИТ Пользователь ЦСК-1. Библ. подп. (web-p.)

Установить

★★★★★ 155 | [Социальные сети и общение](#) | Пользователей: 300 000+

Також слід **перевірити версію браузера**. Наприклад, у Firefox останніх версій (вище 90.0.2) відкрийте меню та виберіть пункт «Довідка», у підменю натисніть на «Про Firefox».



## Висновки

Якщо токена немає із собою, слід звертатися до АЦСК.

Якщо закінчується термін дії ключа, потрібно сформувати нові сертифікати самостійно, якщо цього не відбудеться автоматично.

Якщо не відображається файл ключа, почистіть кеш у браузері.

Якщо під час підписання кваліфікованим електронним підписом (КЕП) на екрані монітора з'явиться напис «виникла помилка при взаємодії з криптографічною бібліотекою» або «виникла помилка з файловим сховищем сертифікатів та СВС», або не відображається файл ключа, встановіть або оновіть програму ІІТ Користувач ЦСК-1.3. Агент на комп'ютері та за потреби налаштуйте проху-сервери (після проведених маніпуляцій також варто перезавантажити комп'ютер).

Якщо апаратний ключ не зчитується в одному з браузерів, встановіть розширення для браузера та оновіть браузер до останньої версії.

Для вирішення складнощів із використанням удосконалених електронних підписів (УЕП) слід перевірити:

чи правильно введено пароль (мова, літери тощо);



чи не закешовані дані у браузері.

Для вирішення складнощів із використанням кваліфікованих електронних підписів на токенах (КЕП) перш за все слід перевірити найдрібніші деталі:

чи вставлена флешка у комп'ютер;

чи запущена програма ІТ Користувач ЦСК-1.3. Агент підпису;

чи правильно введено пароль (мова, літери тощо);

чи не закешовані дані у браузері.

Після цього переконайтеся, що програма ІТ Користувач ЦСК-1.3. Агент та браузер останньої версії, що в браузері встановлено відповідне розширення та налаштований проху-сервер.

Сподіваємось, що ця стаття стане вам у пригоді та допоможе у вирішенні питань, пов'язаних з використанням удосконалених електронних підписів (УЕП) та кваліфікованих електронних підписів на токенах (КЕП). Слава Україні! Ще більше корисної інформації читайте на порталі [RADNUK.COM.UA](https://radnuk.com.ua) у таких статтях:

[«Відповідальність за використання КЕП не на захищеному носієві»;](#)

[«Антимонопольна практика щодо накладення підпису фізичною особою»;](#)

[«Електронний підпис не підпадає під усунення невідповідностей протягом 24 годин»;](#)

[«Документи ТП підписуються КЕП чи власноручним підписом уповноваженої особи».](#)