

ІНСТРУКЦІЯ

по роботі з програмним забезпеченням

«ІТ Користувач ЦСК–1.3»

<i>Початок роботи з програмним забезпеченням «ІТ Користувач ЦСК–1.3».....</i>	2
<i>Процедура підписання файлів(розширення *.p7s) за допомогою програмного забезпечення «ІТ Користувач ЦСК–1.3».....</i>	6
<i>Процедура перевірки підписаних файлів за допомогою програмного забезпечення «ІТ Користувач ЦСК–1.3»</i>	11
<i>Процедура пролонгації кваліфікованих сертифікатів за допомогою програмного забезпечення «ІТ Користувач ЦСК–1.3».....</i>	15


Початок роботи з програмним забезпеченням «ІТ Користувач ЦСК–1.3»

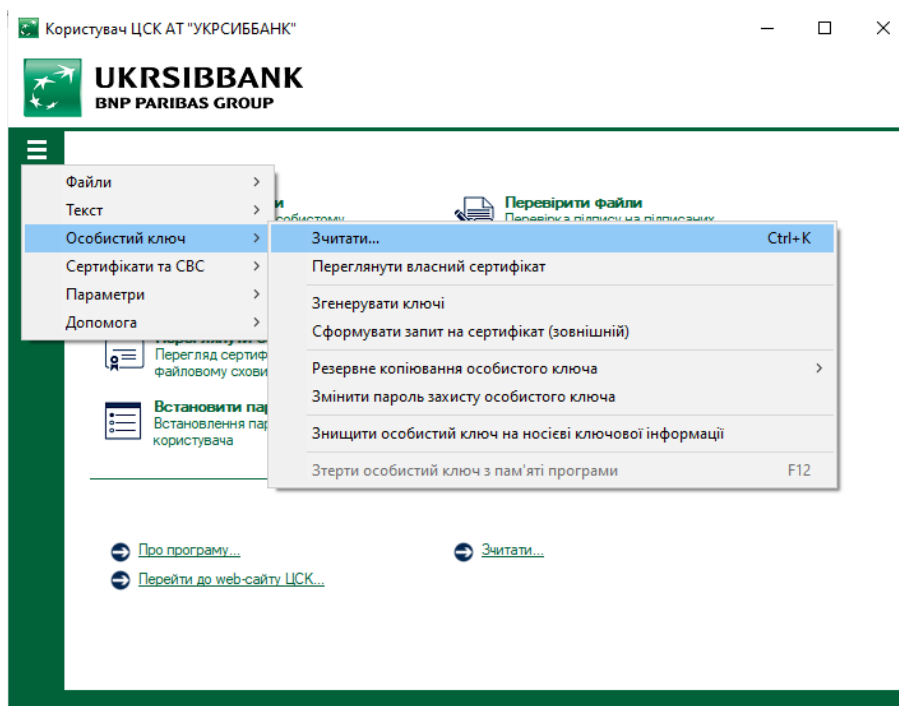
Для коректної роботи з програмним забезпеченням «ІТ Користувач ЦСК–1.3» необхідно імпортувати сертифікати до файлового сховища сертифікатів. Дані дії необхідно виконувати у наступних випадках:

- ПЗ «ІТ Користувач ЦСК–1.3» було інстальовано на ПК;
- отримано нові власні сертифікати у КНЕДП АТ «УКРСИББАНК»;
- змінено директорію файлового сховища сертифікатів.

Для імпорту сертифікатів на головній сторінці необхідно натиснути на вкладку «Зчитати».

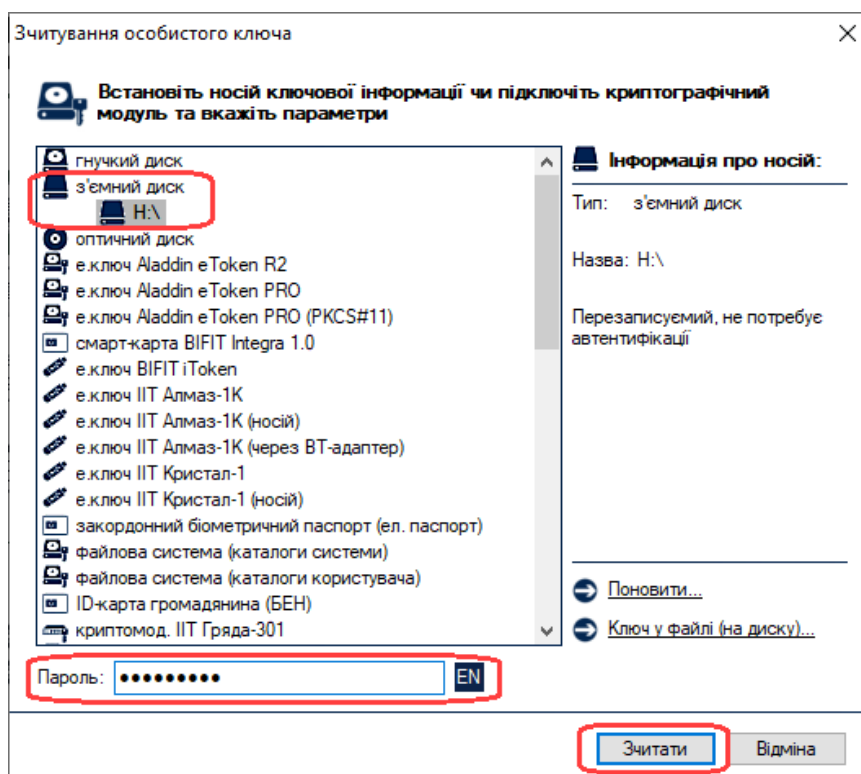


або у верхньому лівому куті головного вікна програми натиснути на значок «», далі вибрати «Особистий ключ» і натиснути «Зчитати»



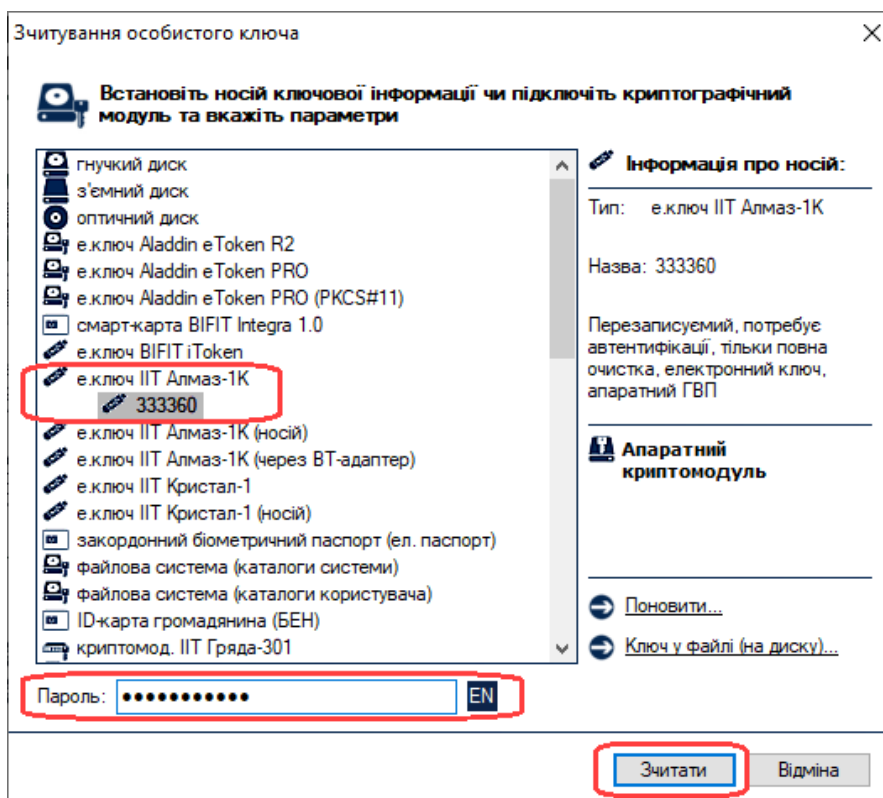
У вікні «Зчитування особистого ключа» необхідно:

1. Натиснути «З'ємний диск» і вибрати USB-флешку, на якій знаходиться файл особистого ключа.
2. Ввести пароль захисту ключа у відповідній графі.
3. Натиснути «Зчитати»

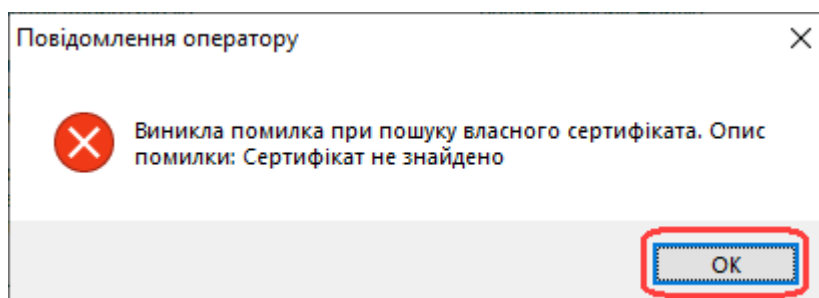


Якщо особистий ключ знаходиться на захищеному носії особистого ключа (наприклад Алмаз-1К, Кристал-1 тощо) – необхідно:

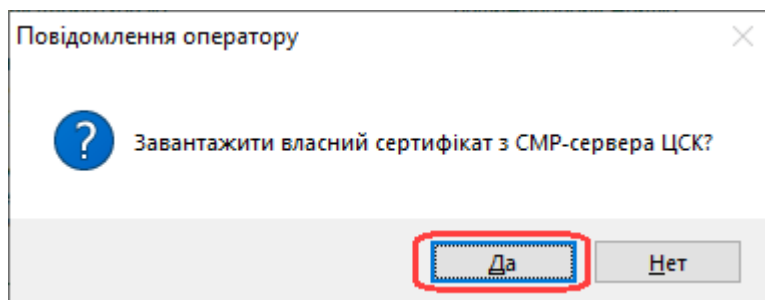
1. Вибрати «е.ключ ІТ Алмаз-1К» або «е.ключ ІТ Кристал-1».
2. Вибрати номер носія особистого ключа.
3. Ввести пароль захисту ключа у відповідній графі.
4. Натиснути «Зчитати»



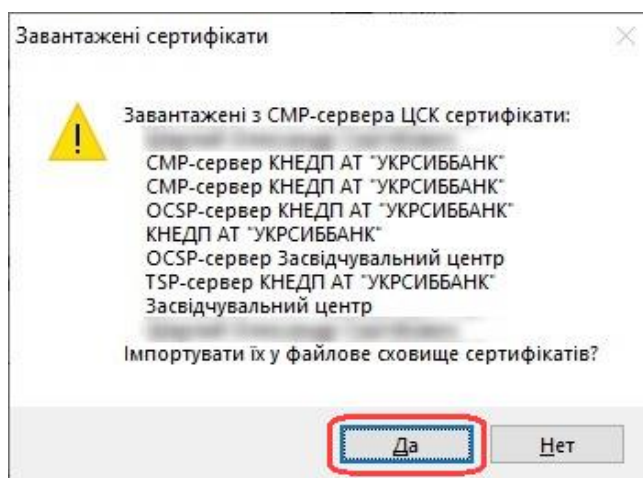
З'явиться повідомлення з помилкою «Сертифікат не знайдено»(тобто власний сертифікат ще не імпортовано до файлового сховища сертифікатів на ПК). Необхідно натиснути «ОК»



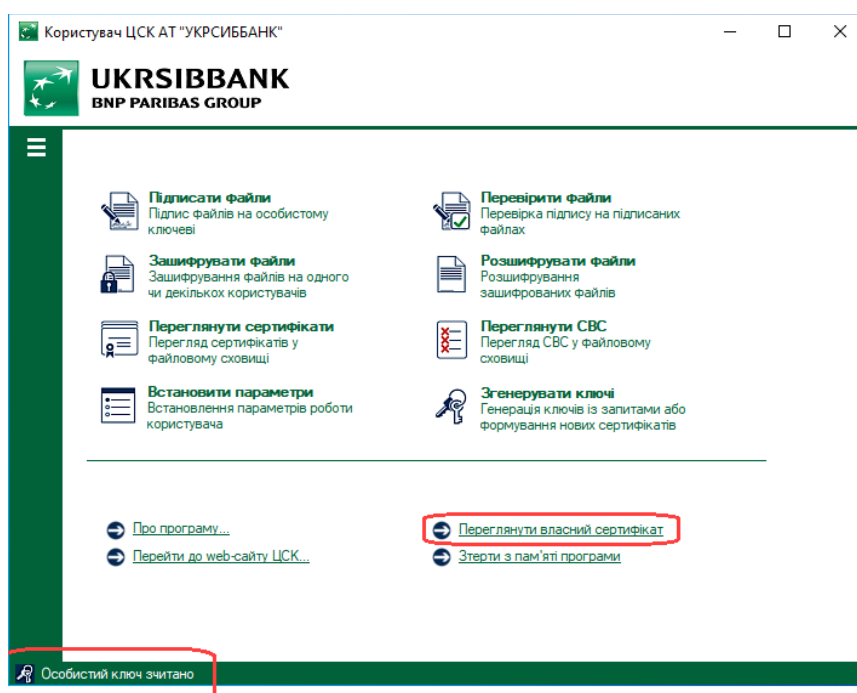
Наступне повідомлення пропонує завантажити сертифікат з СМР-сервера. Необхідно натиснути «Да»



Далі система відобразить завантажені сертифікати і запропонує імпортувати їх до файлового сховища. Натиснувши «Да», власні сертифікати потрапляють до файлового сховища сертифікатів і при наступному зчитуванні особистого ключа не буде з'являтися помилка «Сертифікат не знайдено».

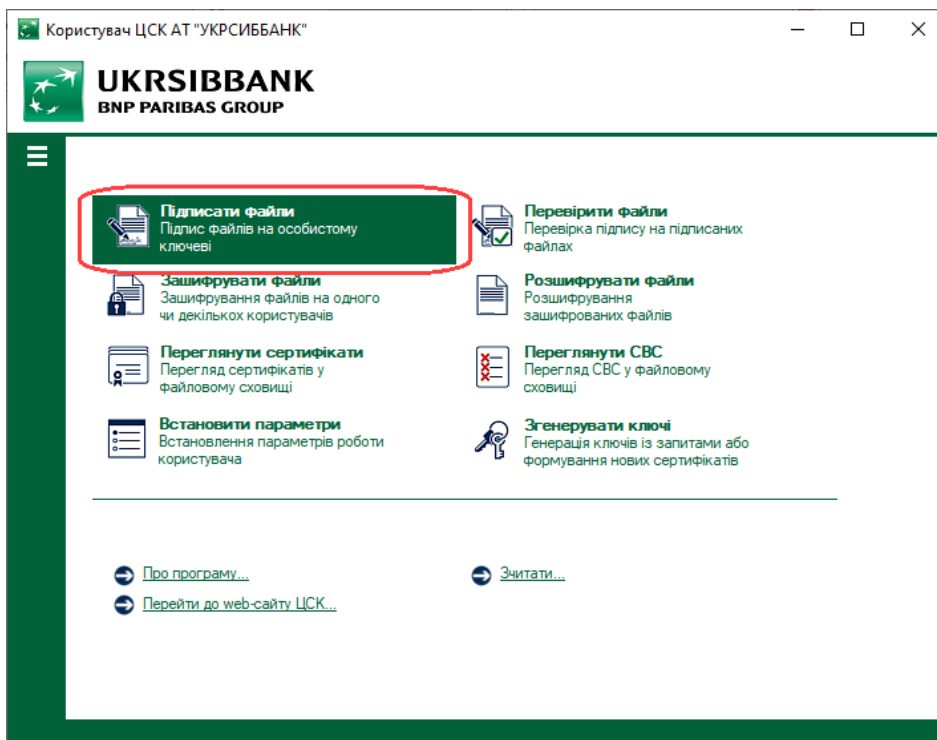



В нижньому лівому куті головної сторінки з'явиться напис «Особистий ключ зчитано». Зчитування та імпорт сертифікатів виконано успішно. Додатково можна переглянути деталі власного сертифікату, натиснувши на «Переглянути власний сертифікат»

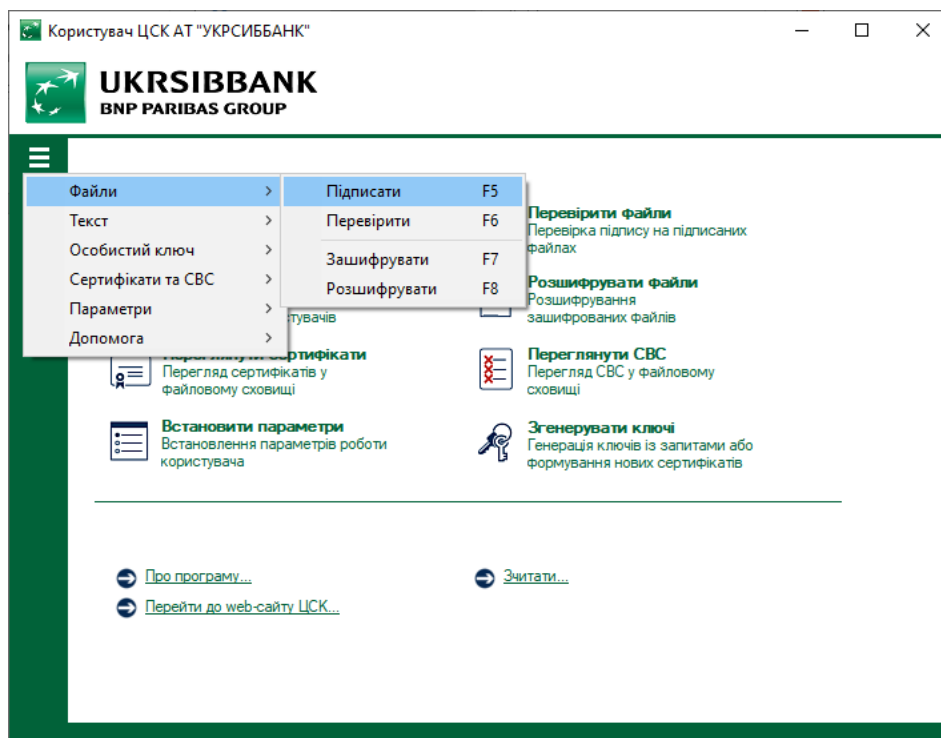


Процедура підписання файлів(розширення *.p7s) за допомогою програмного забезпечення «ІТ Користувач ЦСК–1.3»

Для підписання файлів необхідно запустити «ІТ Користувач ЦСК–1.3». На головній сторінці необхідно натиснути на вкладку «Підписати файли».

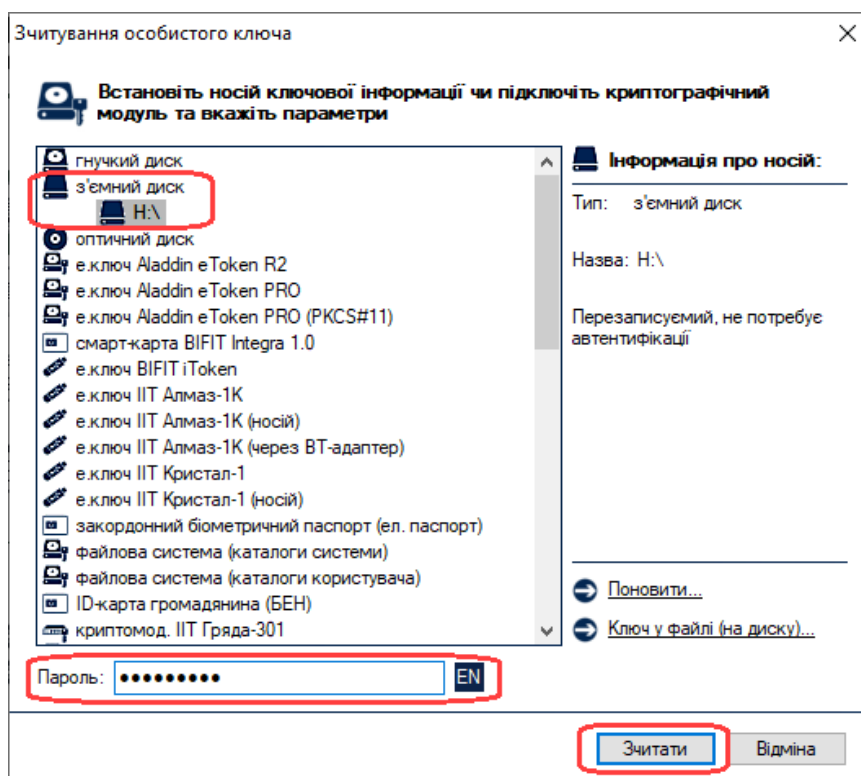


або у верхньому лівому куті головного вікна програми натиснути на значок «», далі вибрати «Файли» і натиснути «Підписати»



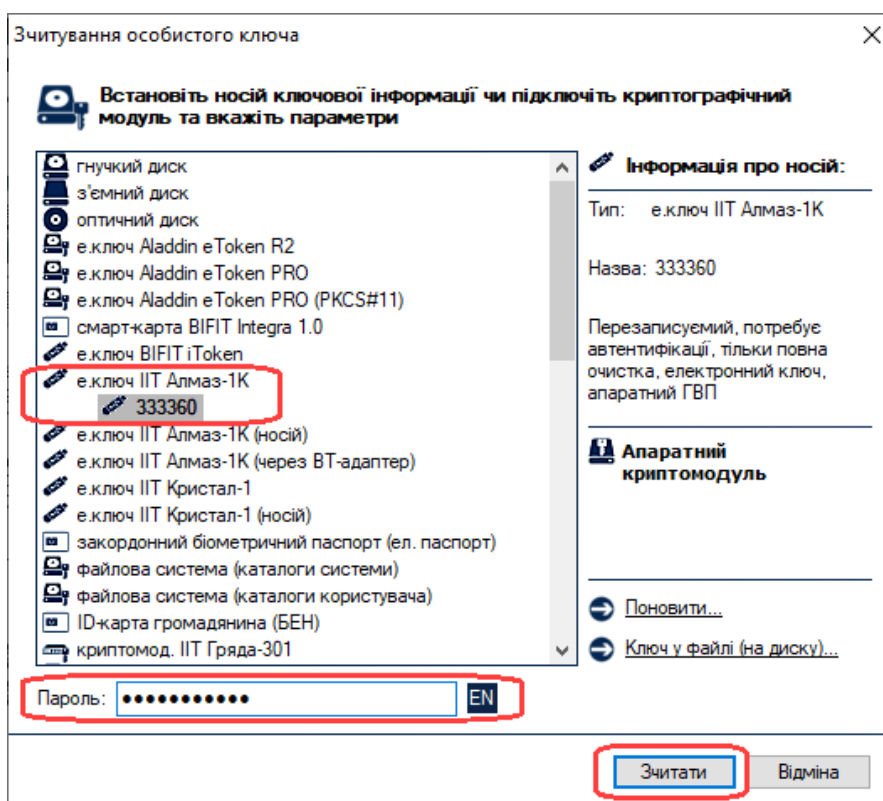
У вікні «Зчитування особистого ключа» необхідно:

1. Натиснути «З’ємний диск» і вибрати USB–флешку, на якій знаходиться файл особистого ключа.
2. Ввести пароль захисту ключа у відповідній графі.
3. Натиснути «Зчитати»

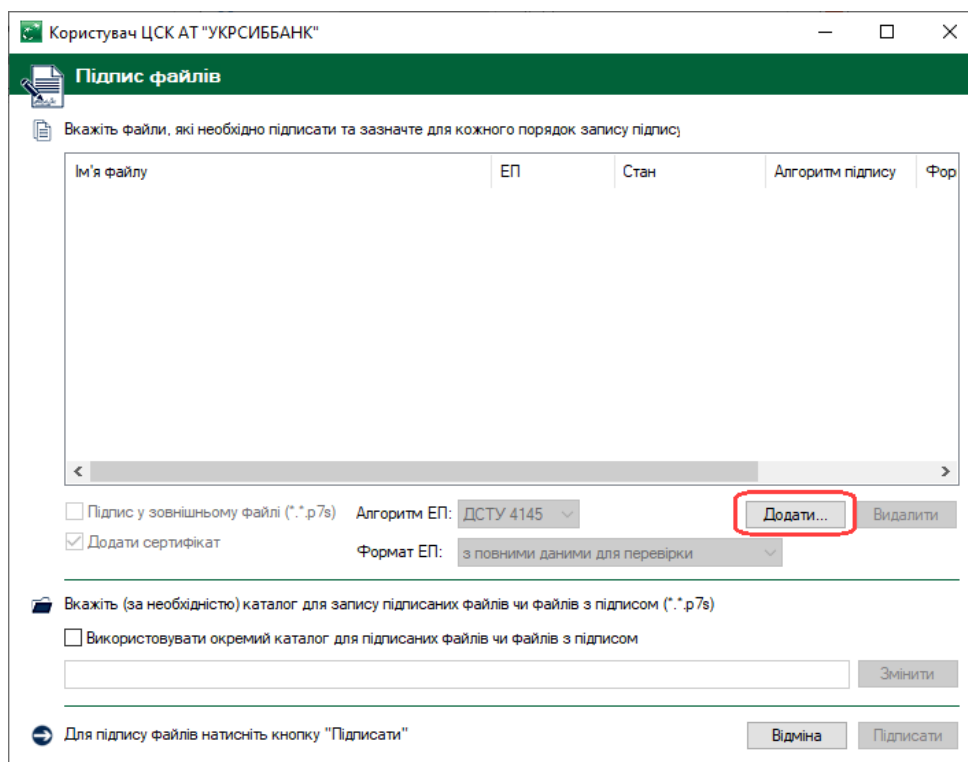


Якщо особистий ключ знаходиться на захищеному носії особистого ключа (наприклад Алмаз-1К, Кристал-1 тощо) – необхідно:

1. Вибрати «е.ключ ІТ Алмаз-1К» або «е.ключ ІТ Кристал-1».
2. Вибрати номер носія особистого ключа.
3. Ввести пароль захисту ключа у відповідній графі.
4. Натиснути «Зчитати»



Після успішного зчитування особистого ключа відкриється наступне вікно, в якому потрібно натиснути «Додати» і вибрати файл(и), який(і) необхідно підписати.

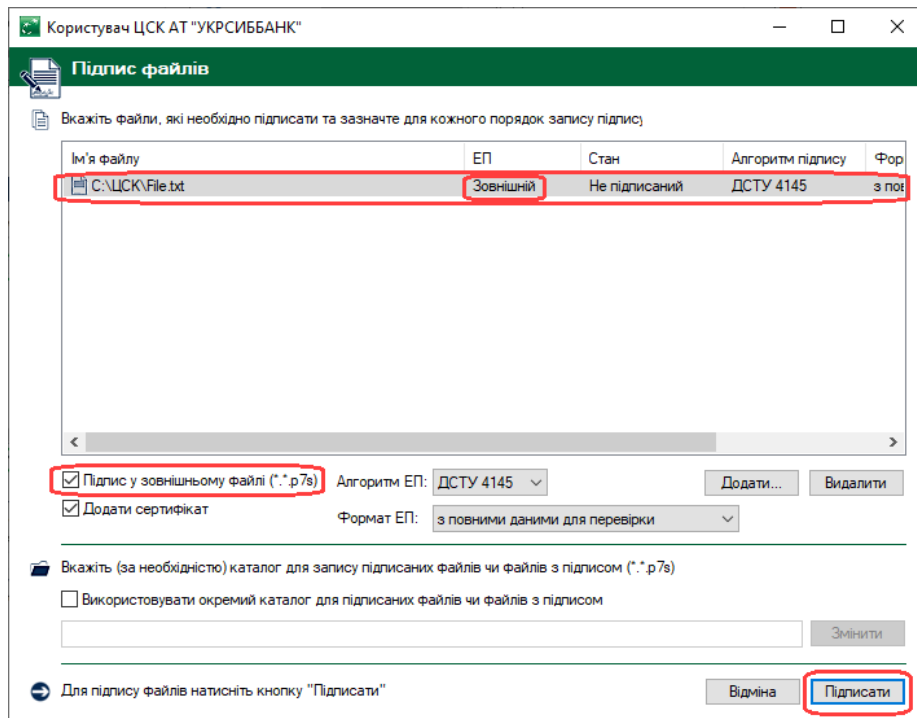


Якщо файл підпису і файл з даними мають бути в окремих файлах слідуйте лівій колонці інструкції, якщо в одному файлі – правій колонці.

Підпис та дані в окремих файлах

Після завантаження файлу(ів) до програми необхідно:

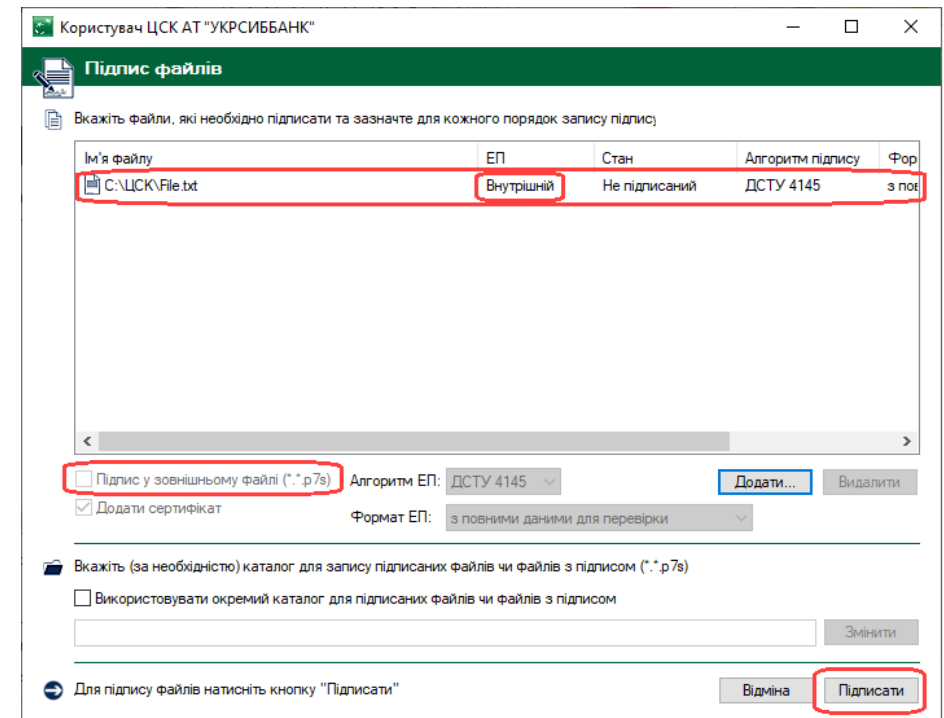
1. Натиснути на рядок із завантаженим файлом, щоб виділити весь рядок.
2. Поставити відмітку «Підпис у зовнішньому файлі (*.*.p7s)»
3. Натиснути «Підписати»



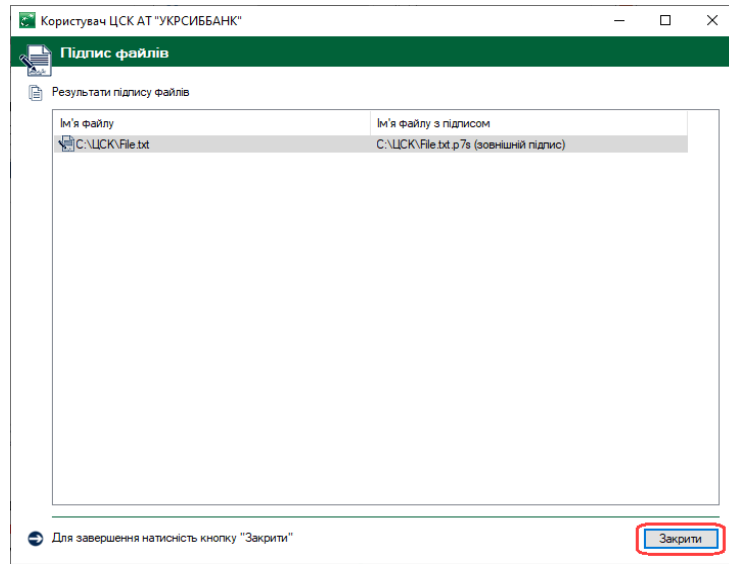
Підпис та дані в одному файлі

Після завантаження файлу(ів) до програми необхідно:

1. Натиснути на рядок із завантаженим файлом, щоб виділити весь рядок.
2. Переконайтесь у відсутності відмітки напроти «Підпис у зовнішньому файлі (*.*.p7s)»
3. Натиснути «Підписати»

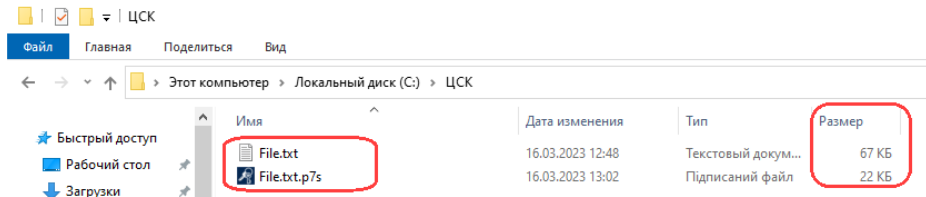


Після підписання файлу відкриється вікно «Результати підпису файлів» і нижче відобразатимуться підписані файл(и) та директорія(каталог), в яку вони збереглись:

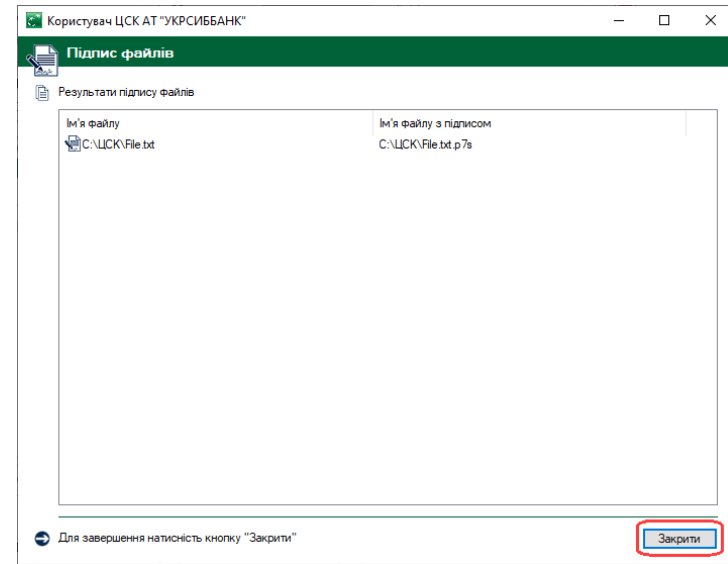


Процедуру підпису файлу(ів) завершено, можна натискати «Закрити».

Зверніть увагу, що розмір файлу підпису менший за розмір файлу з даними та має розмір приблизно: 20КБ – 25КБ.

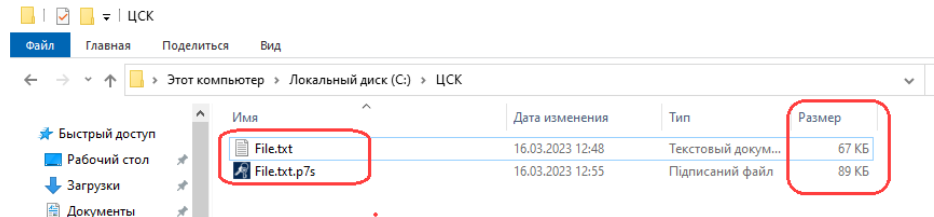


Після підписання файлу відкриється вікно «Результати підпису файлів» і нижче відобразатимуться підписані файл(и) та директорія(каталог), в яку вони збереглись:



Процедуру підпису файлу(ів) завершено, можна натискати «Закрити».


Зверніть увагу, що розмір файлу підпису більший за розмір файлу з даними та має розмір приблизно: «розмір файлу с даними + (20КБ – 25КБ)»

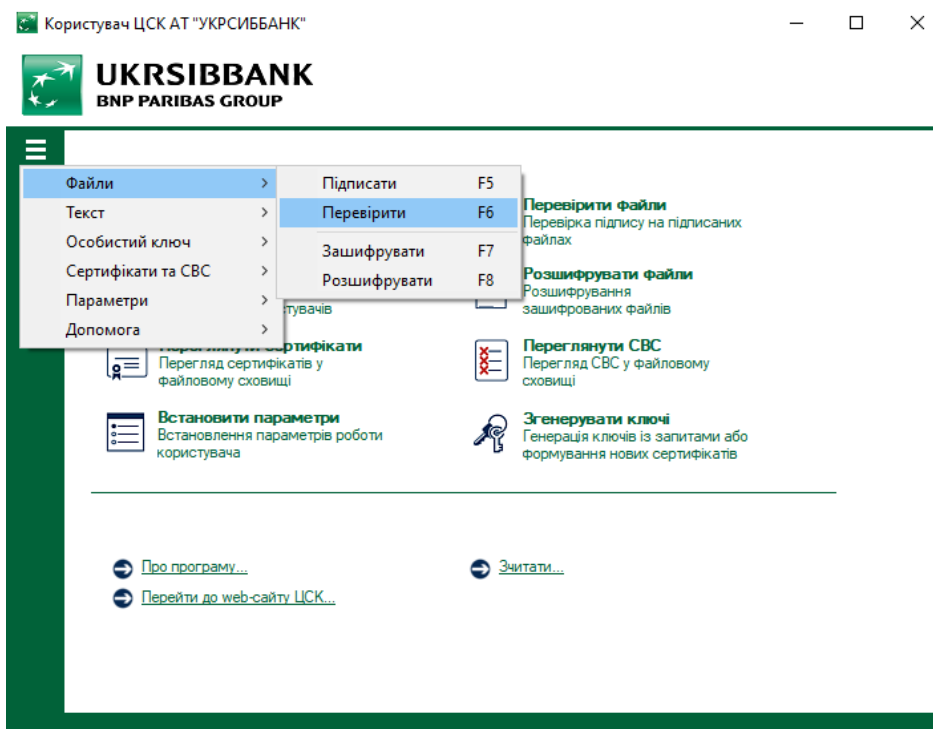


Процедура перевірки підписаних файлів за допомогою програмного забезпечення «ІТ Користувач ЦСК–1.3»

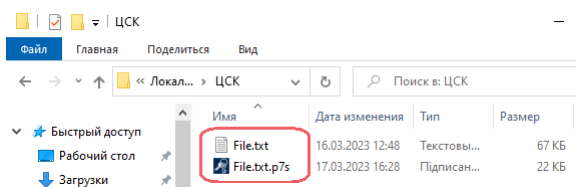
Для перевірки підписаних файлів необхідно запустити «ІТ Користувач ЦСК–1.3». На головній сторінці необхідно натиснути на вкладку «Перевірити файли».



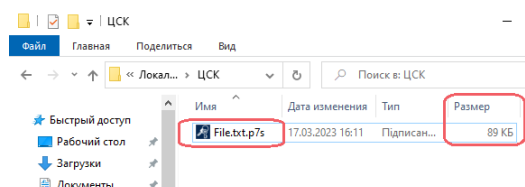
або у верхньому лівому куті головного вікна програми натиснути на значок «», далі вибрати «Файли» і натиснути «Перевірити».



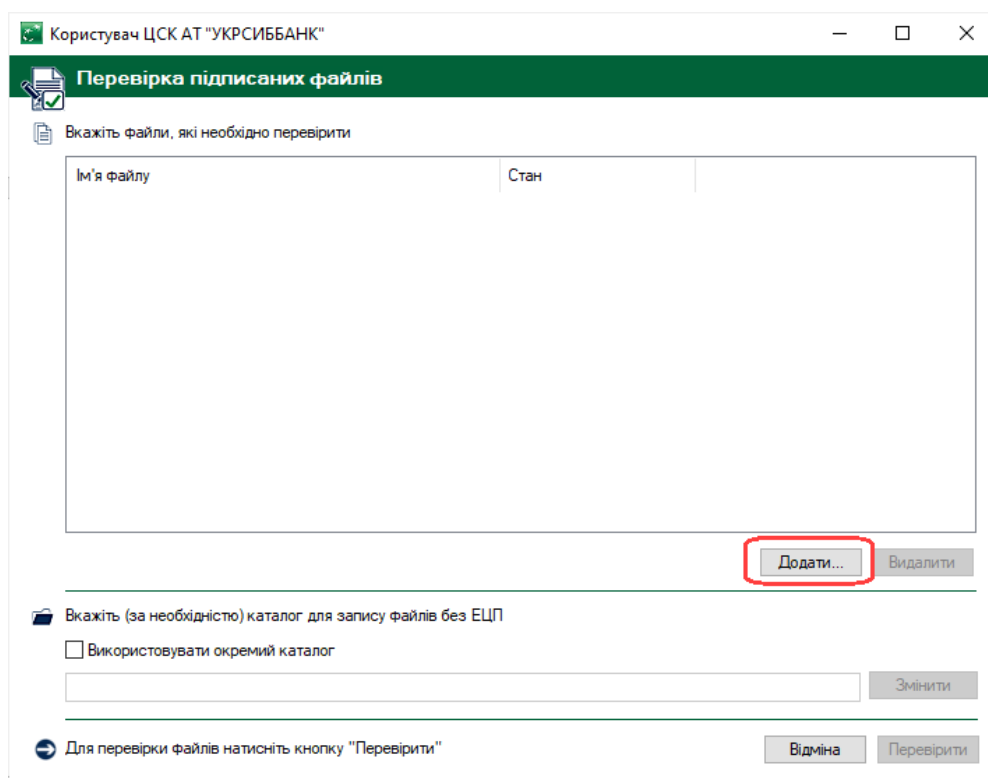
Увага: Якщо під час процедури підписання було використано метод «Підпис та дані в окремих файлах» - файл з підписом(розмір 20КБ – 25КБ) і файл з даними мають знаходитись в одній директорії (каталозі).



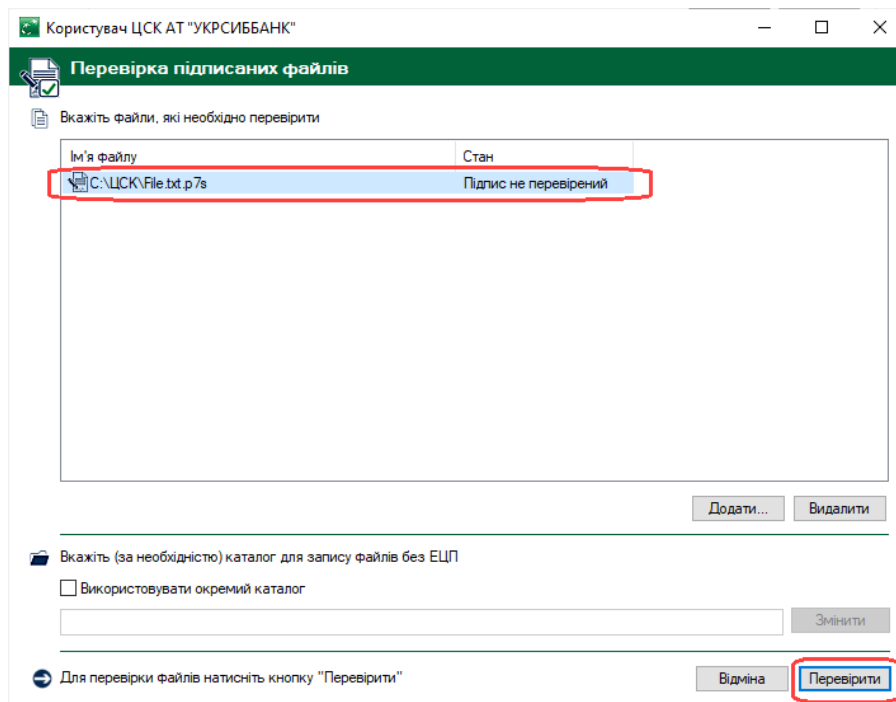
Якщо під час процедури підписання було використано метод «Підпис та дані в одному файлі» - файл з підписом і файл з даними можуть знаходитись в різних директоріях (каталогах).



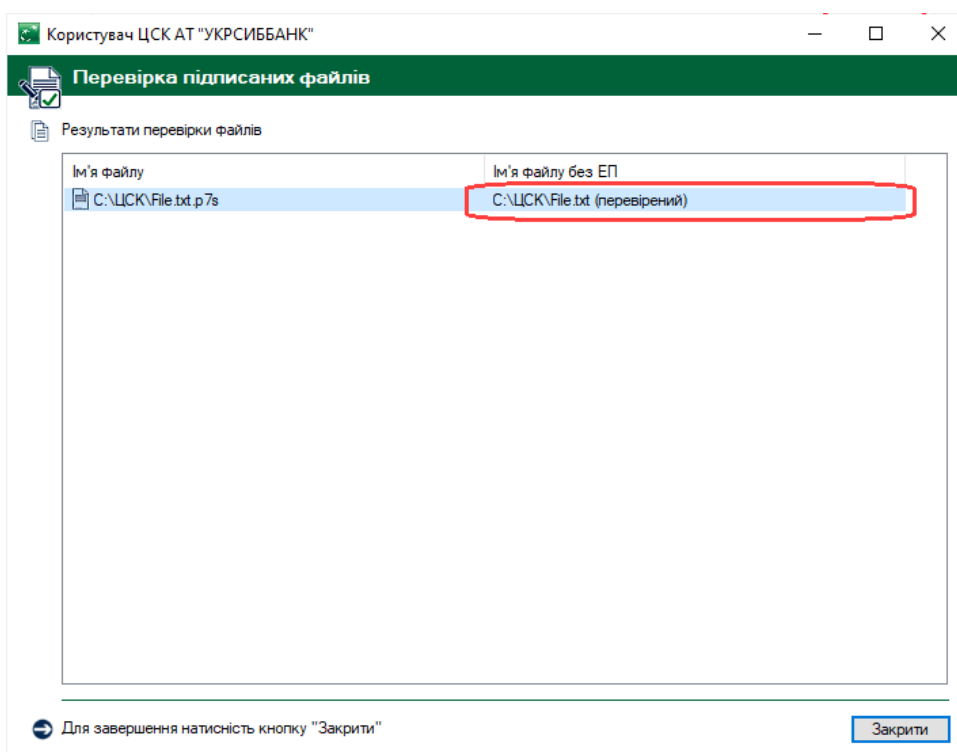
У вікні «Перевірка підписаних файлів» необхідно натиснути «Додати» і вибрати файл(и) з підписом, який(і) необхідно перевірити.



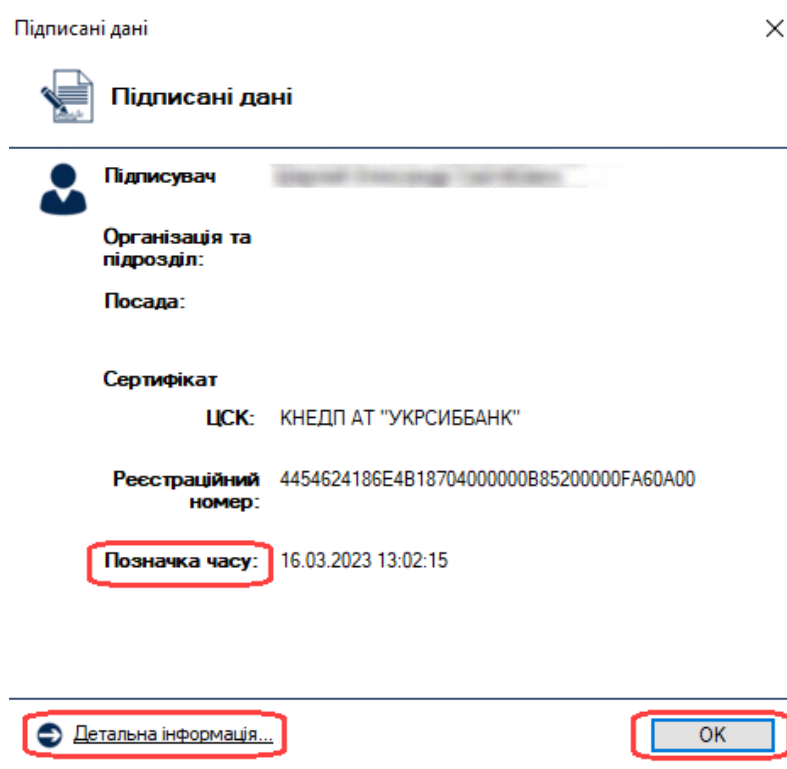
Після завантаження файлу(ів) до програми необхідно натиснути «Перевірити».



У наступному вікні відображається результат перевірки підпису. «(перевірений)» поруч з файлом підпису свідчить про успішну перевірку підписаних файлів.



Натиснувши двічі на рядок з перевіреним файлом, відкриється інформація(підписувач, позначка часу тощо) стосовно перевірки.



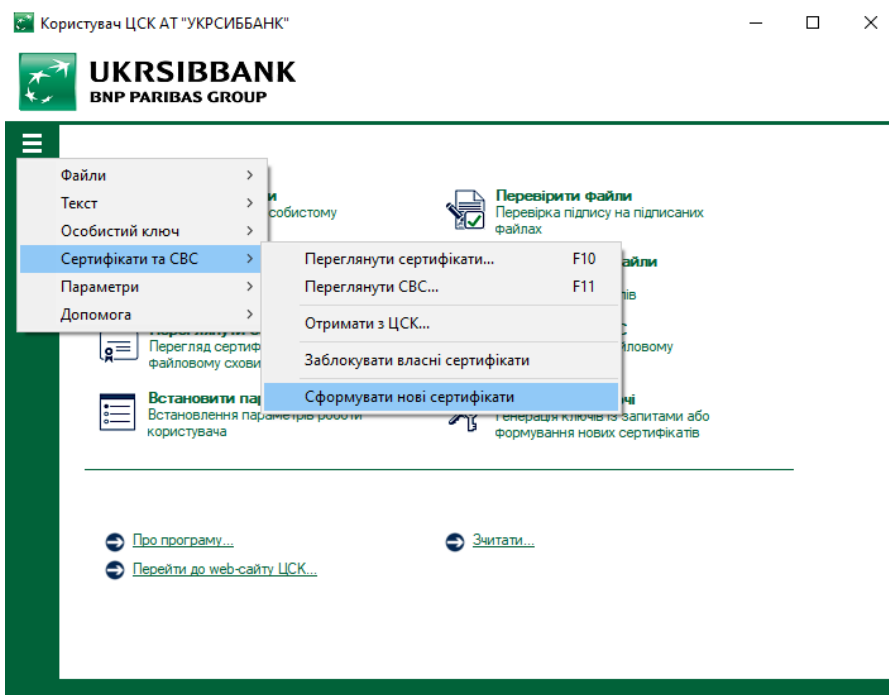
Увага! Якщо замість фрази «Позначка часу:» буде фраза «Час підпису:» такі документи до розгляду **НЕ ПРИЙМАЮТЬСЯ**. Позначка часу не була отримана у Надавача електронних довірчих послуг.

Перевірку підписаних файлів завершено.

Процедура пролонгації кваліфікованих сертифікатів за допомогою програмного забезпечення «ІТ Користувач ЦСК-1.3»

УВАГА: ПРОЛОНГАЦІЯ КВАЛІФІКОВАНОГО СЕРТИФІКАТУ ЕЛЕКТРОННОГО ПІДПISУ МОЖЛИВА ЛИШЕ ПРИ УМОВІ, ЩО ТЕРМІН ДІЇ СЕРТИФІКАТУ ЩЕ НЕ ЗАВЕРШИВСЯ!

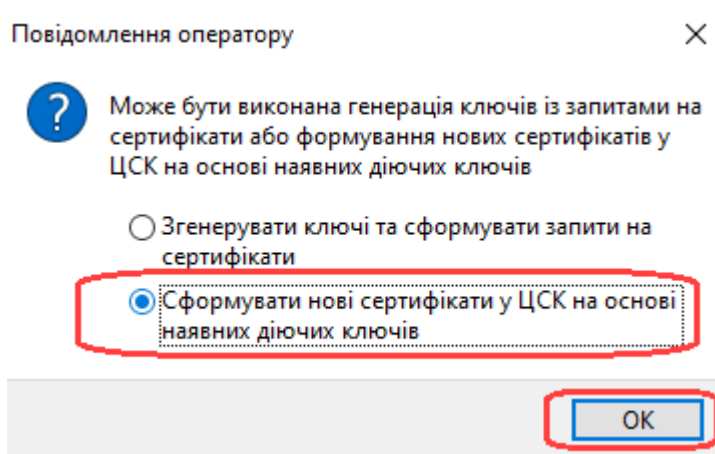
У верхньому лівому куті головного вікна програми натиснути на значок «☰», далі вибрати «Сертифікати та СВС» і натиснути «Сформувати нові сертифікати»



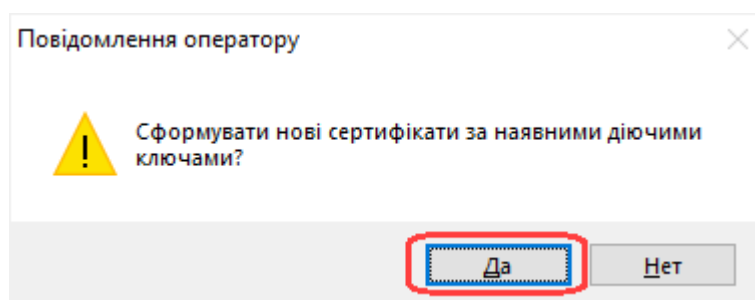
або на головній сторінці необхідно натиснути на вкладку «Згенерувати ключі».



У наступному повідомленні необхідно **обов'язково змінити перемикач** на пункт **«Сформувати нові сертифікати у ЦСК на основі наявних діючих сертифікатів»** та натиснути «ОК».



У наступному вікні необхідно натиснути «Да».

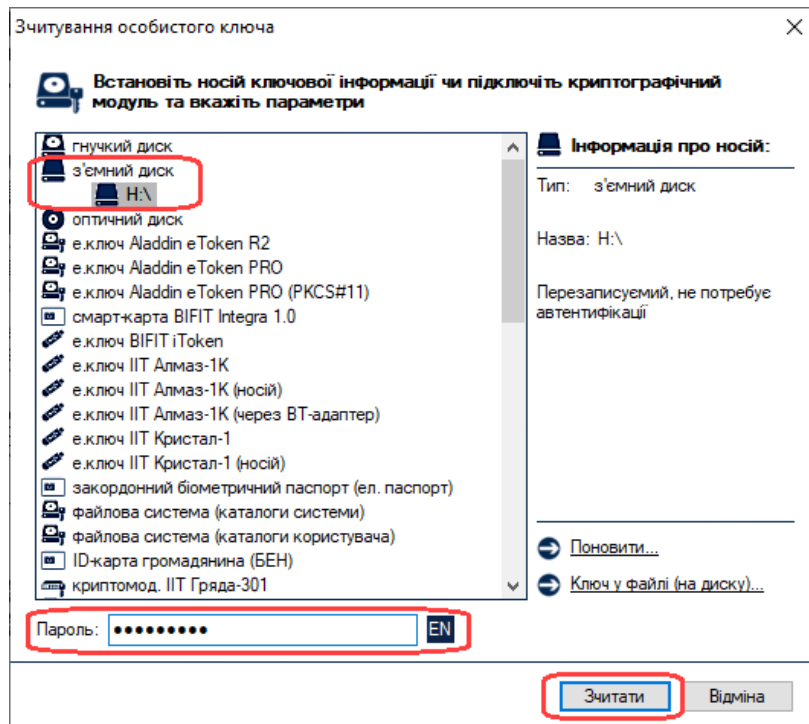


Якщо особистий ключ знаходиться на USB-флешці далі слідуєте лівій колонці інструкції, якщо особистий ключ знаходиться на захищеному носії особистого ключа (наприклад Алмаз-1К, Кристал-1) – правій колонці.

Особистий ключ знаходиться на USB-флешці

У вікні «Зчитування особистого ключа» необхідно:

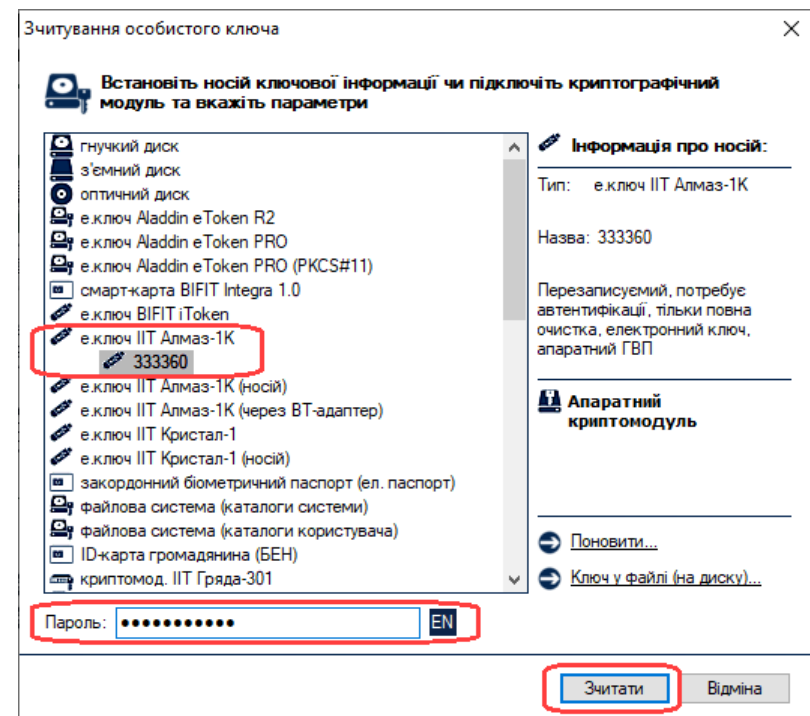
1. Натиснути «З'ємний диск» і вибрати USB-флешку, на якій зберігається файл особистого ключа.
2. Ввести пароль захисту ключа у відповідній графі.
3. Натиснути «Зчитати»



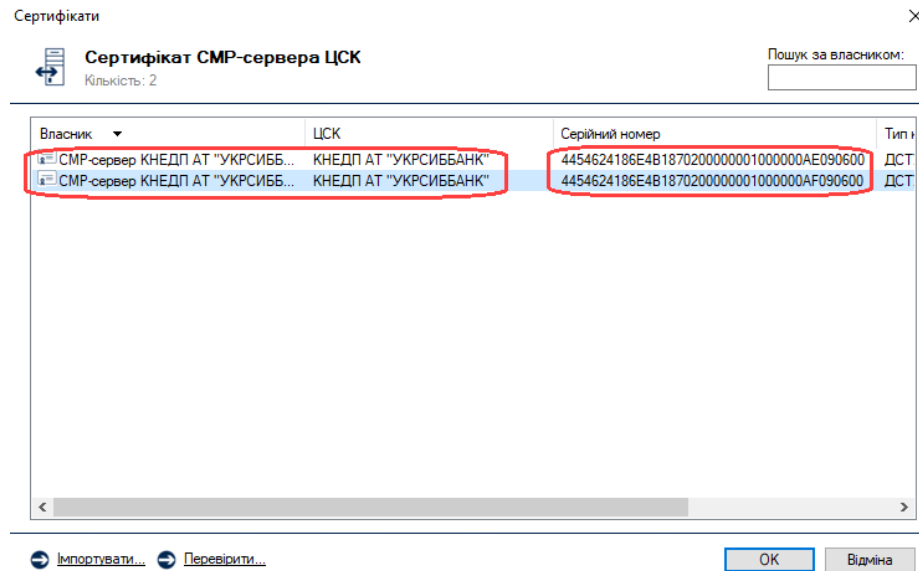
Особистий ключ знаходиться на захищеному носії особистого ключа (наприклад Алмаз-1К, Кристал-1)

У вікні «Зчитування особистого ключа» необхідно:

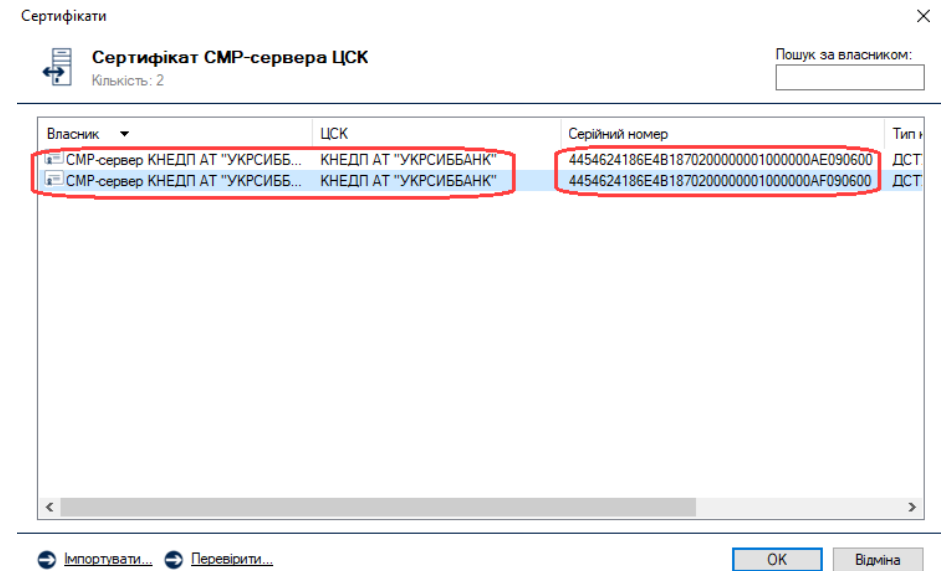
1. Вибрати «е.ключ ІТТ Алмаз-1К» або «е.ключ ІТТ Кристал-1».
2. Вибрати номер носія особистого ключа.
3. Ввести пароль захисту ключа у відповідній графі.
4. Натиснути «Зчитати».



У наступному вікні необхідно вибрати один із сертифікатів СМР-сервера КНЕДП АТ «УКРСИББАНК» (серійний номер повинен починатись з «4454»)



У наступному вікні необхідно вибрати один із сертифікатів СМР-сервера КНЕДП АТ «УКРСИББАНК» (серійний номер повинен починатись з «4454»)



У новому вікні «Формування нових сертифікатів» в блоці «Генерувати ключі» має бути вибрано пункт «для державних алгоритмів і протоколів». Нижче необхідно вибрати пункт «Згенерувати на новий носій» і натиснути «Далі», оскільки необхідно підготувати нову флешку, на яку буде записано файл особистого ключа.

У новому вікні «Формування нових сертифікатів» в блоці «Генерувати ключі» має бути вибрано пункт «для державних алгоритмів і протоколів». Нижче необхідно вибрати пункт «Згенерувати на поточний носій» і натиснути «Далі».

Формування нових сертифікатів

Генерація нових ключів

Генерувати ключі

для державних алгоритмів і протоколів

для міжнародних алгоритмів і протоколів

для державних та міжнародних алгоритмів і протоколів

Згенерувати на новий носій

Згенерувати на поточний носій

У наступному вікні потрібно натиснути «Далі»

Формування нових сертифікатів

Генерація нових ключів

Тип криптографічних алгоритмів та протоколів:

Використовувати окремий ключ для протоколу розподілу

Ключі ЕЦП: Ключі протоколу розподілу:

Місце розміщення параметрів (каталог, з'ємний чи оптичний диск):

Формування нових сертифікатів

Генерація нових ключів

Генерувати ключі

для державних алгоритмів і протоколів

для міжнародних алгоритмів і протоколів

для державних та міжнародних алгоритмів і протоколів

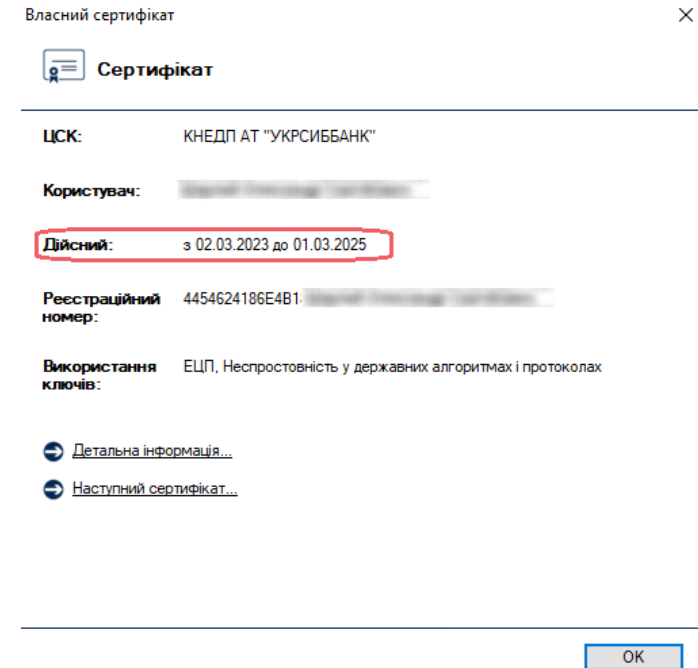
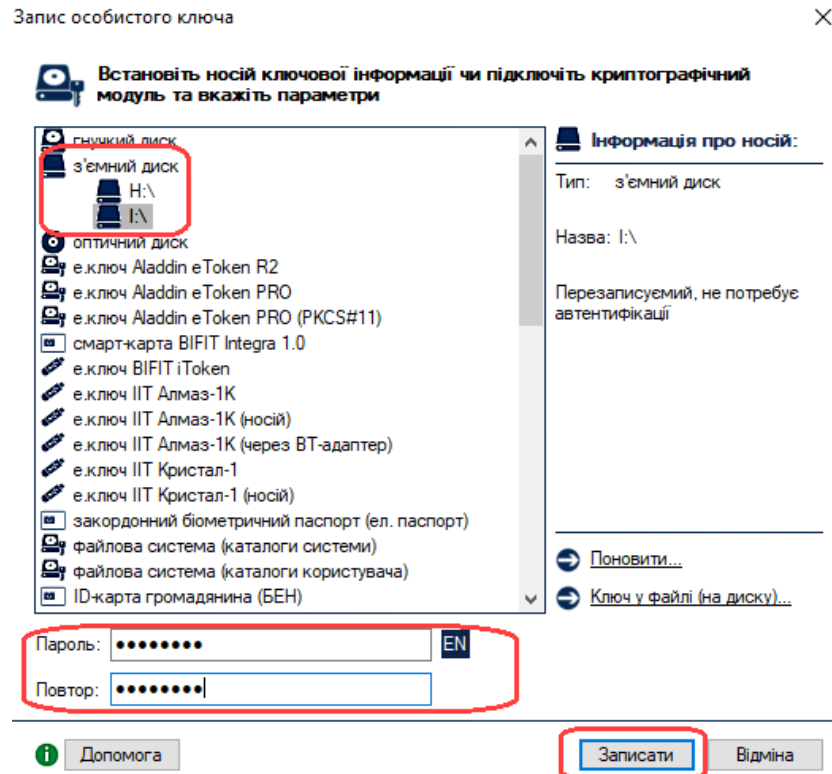
Згенерувати на новий носій

Згенерувати на поточний носій

У наступному вікні з'явиться інформація, що кваліфікований сертифікат продовжено із зазначенням терміну його дії.

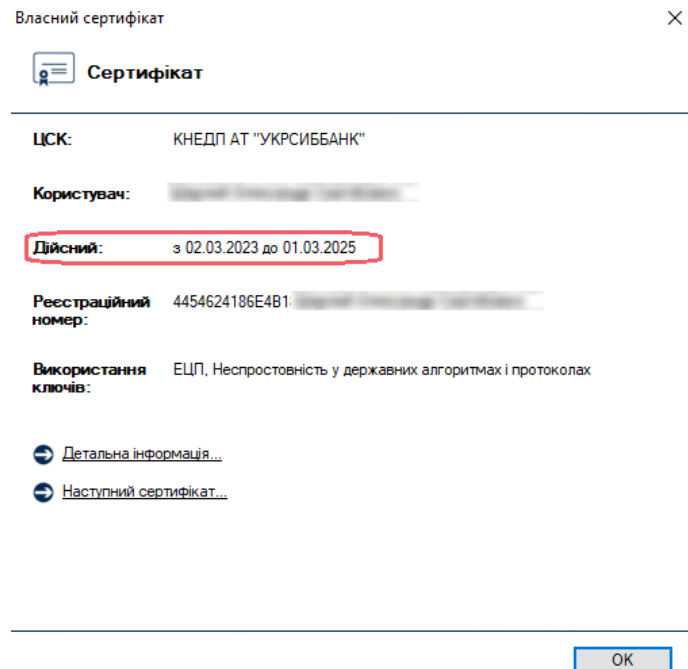
У вікні «Запис особистого ключа» необхідно:

1. Натиснути з'ємний диск і вибрати підготовлену USB-флешку, на яку буде записано файл особистого ключа.
2. Ввести новий пароль захисту ключа у графі «Пароль» і «Повтор».
3. Натиснути «Записати».



Процедуру пролонгації завершено успішно.

У наступному вікні з'явиться інформація, що кваліфікований сертифікат продовжено із зазначенням терміну його дії.



Процедуру пролонгації завершено успішно.