МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

Кваліфікований надавач електронних довірчих послуг – акредитований центр сертифікації ключів Міністерства внутрішніх справ України

Програмний комплекс «Користувач АЦСК МВС»

ІНСТРУКЦІЯ КОРИСТУВАЧА

Генерація ключів на
захищений носій особистих ключів

Київ 2019

Перелік скорочень та визначень

АЦСК МВС	кваліфікований надавач електронних довірчих послуг – акредитований центр сертифікації ключів Міністерства внутрішніх справ України
ВПР	відокремлений пункт реєстрації - представництво АЦСК МВС
засіб кваліфікованого електронного підпису чи печатки	апаратно-програмний або апаратний пристрій чи програмне забезпечення, які реалізують криптографічні алгоритми генерації пар ключів та/або створення кваліфікованого електронного підпису чи печатки, та/або перевірки кваліфікованого електронного підпису чи печатки, та/або зберігання особистого ключа кваліфікованого електронного підпису чи печатки, який відповідає вимогам Закону України «Про електронні довірчі послуги» (далі - Закон)
ЗНОК	захищений носій особистих ключів - засіб кваліфікованого електронного підпису чи печатки, що призначений для зберігання особистого ключа та має вбудовані апаратно-програмні засоби, що забезпечують захист записаних на ньому даних від несанкціонованого доступу, безпосереднього ознайомлення із значенням параметрів особистих ключів та їх копіювання
КЕП	кваліфікований електронний підпис (печатка) - удосконалений електронний підпис (печатка), який створюється з використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті відкритого ключа
сертифікат відкритого ключа	кваліфікований сертифікат відкритого ключа – сертифікат відкритого ключа, який видається кваліфікованим надавачем електронних довірчих послуг і відповідає вимогам Закону
Підписувач	фізична особа, яка створює електронний підпис
створювач електронної печатки	юридична особа, яка створює електронну печатку

Генерація особистих та відкритих ключів

Особисті та відкриті ключі Підписувача (створювача електронної печатки) можуть бути згенеровані на робочому місці Підписувача (створювача електронної печатки), на робочій станції генерації ключів в АЦСК МВС або його ВПР. Особистий ключ Підписувача (створювача електронної печатки) генерується засобом КЕП (зокрема ЗНОК) та захищається паролем.

Підписувач (створювач електронної печатки) зобов’язаний забезпечувати конфіденційність та неможливість доступу інших осіб до особистого ключа.

Для генерації особистих та відкритих ключів на ЗНОК на робочому місці Підписувача (створювача електронної печатки) застосовується засіб кваліфікованого електронного підпису чи печатки «Програмний комплекс «Користувач АЦСК МВС» (далі – ПК «Користувач АЦСК МВС»), інсталяційний пакет якого можна завантажити з вкладки «Завантажити» на офіційному веб-сайті АЦСК МВС (https://ca.mvs.gov.ua/user-downloads).

Для генерації особистих та відкритих ключів Підписувачу (створювачу електронної печатки) необхідно підключити до комп'ютера ЗНОК, після чого запустити ПК «Користувач АЦСК МВС» та в пункті меню «Особистий ключ» обрати підпункт «Згенерувати ключі» (рис. 1.1). У вікні «Генерація ключів» (рис. 1.2) необхідно обрати пункт «для державних алгоритмів і протоколів» та натиснути кнопку «Далі».

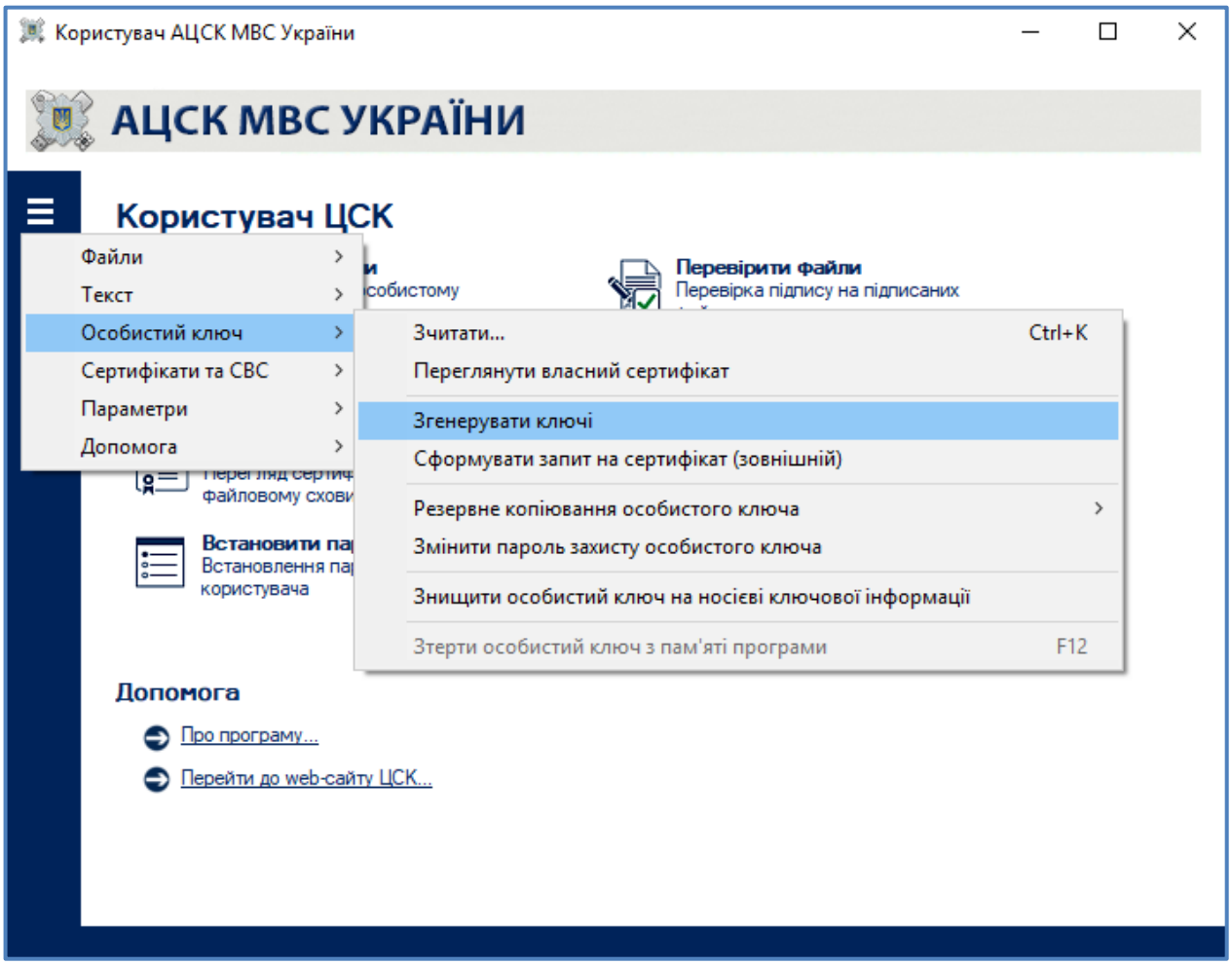

Рисунок 1.1

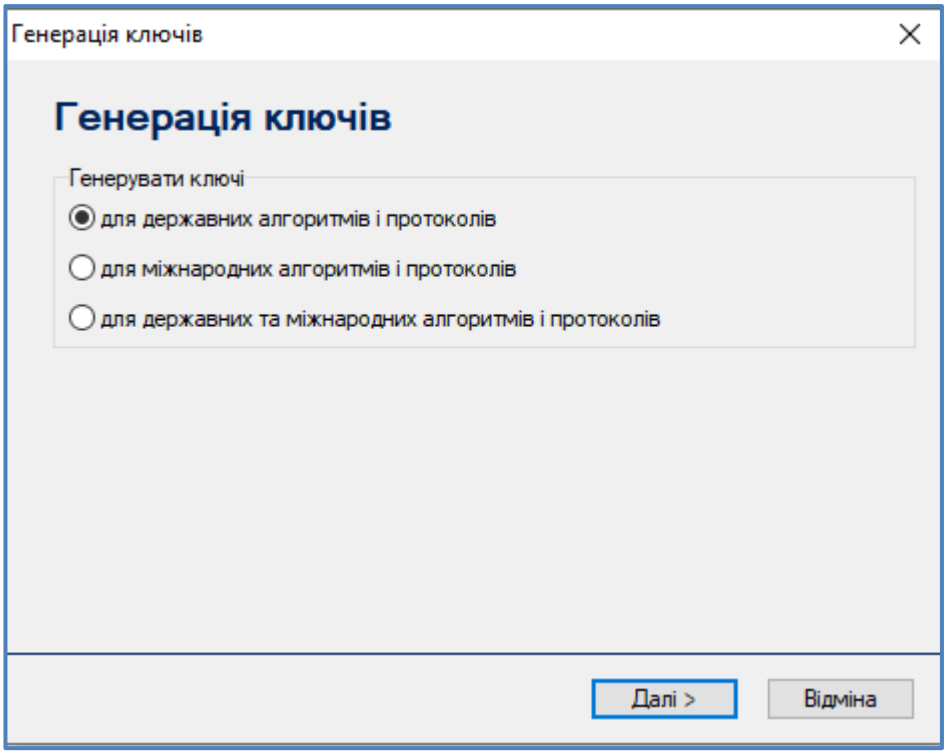

Рисунок 1.2

У вікні «Генерація ключів» (рис. 1.3) необхідно встановити параметр «Використовувати окремий ключ для протоколу розподілу», при цьому буде згенеровано дві ключові пари, одна з яких буде використовуватись для підписання даних, а друга (ключ протоколу розподілу ключів) - для шифрування даних. Для продовження генерації ключів необхідно натиснути кнопку «Далі».

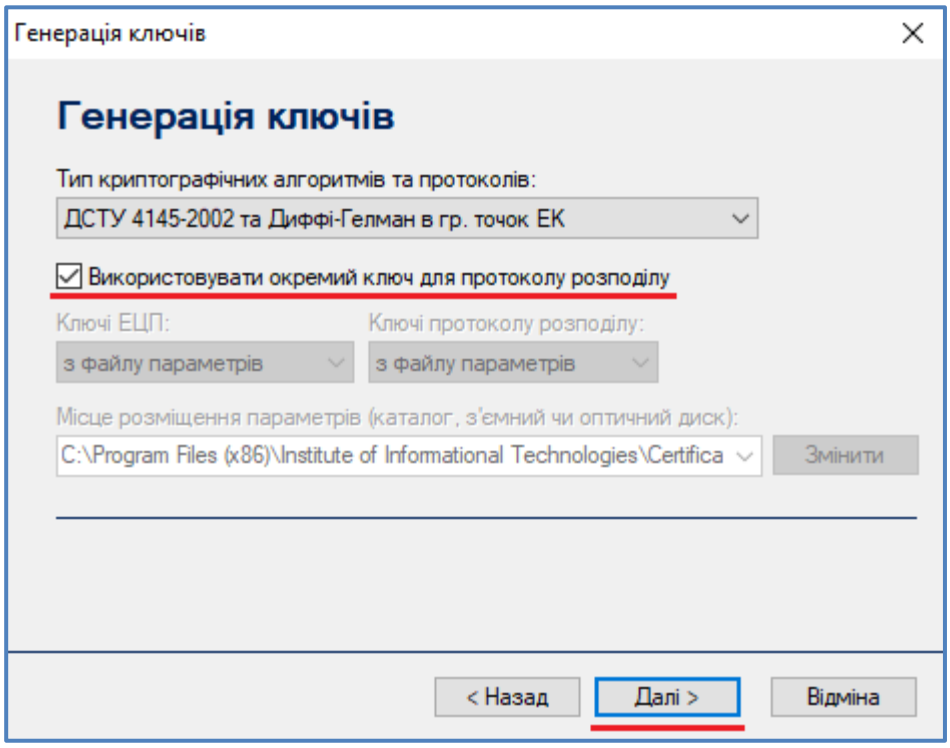

Рисунок 1.3

У вікні «Запис особистого ключа» (рис. 1.4) необхідно обрати тип ЗНОК (та номер ЗНОК), на якому будуть генеруватися ключі, встановити параметр «Попередньо відформатувати», двічі ввести пароль захисту особистого ключа (у поле «Пароль» та «Повтор»), натиснути кнопку «Записати».

Пароль захисту особистого ключа повинен відповідати наступним вимогам:

1. Довжина паролю повинна бути не менше ніж 8 символів.
2. Пароль повинен складатися з:
   - великих літер латиниці «A - Z»;
   - прописних літер латиниці «a - z»;
   - цифр «0 – 9».

   Приклад паролю: JN8oPkgQ.
3. Пароль не повинен містити:

- інформацію, що має якесь відношення до логіну Підписувача (створювача електронної печатки);
- власне ім’я, прізвище Підписувача (створювача електронної печатки);

• інформацію про Підписувача (створювача електронної печатки) (назву міста, у якому проживає; назву вулиці, номер будинку; номер телефону; номер кредитної картки; дату народження тощо);

• прості сполучення символів («qwerty12» або «12345678»);

• символи та розділові знаки, зокрема ! « » ? , . ; : % ^) @ (& * $ # № _.

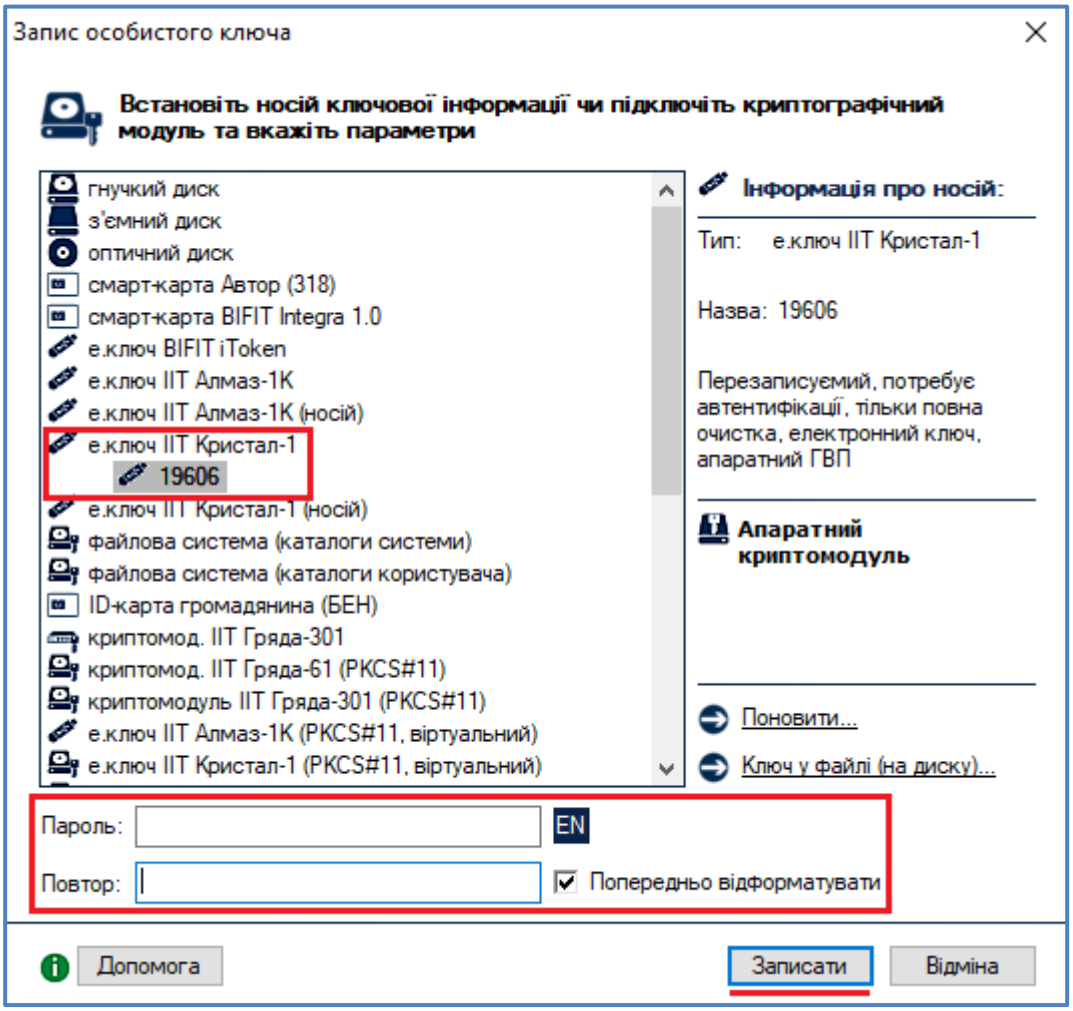

Рисунок 1.4

Якщо після натискання кнопки «Записати» з'явилося повідомлення, що пароль не відповідає вимогам (рис. 1.5), є можливість повернутися на попередній етап (кнопка «Нет») для введення нового паролю, або погодитися на використання уже створеного паролю, що не відповідає вимогам (кнопка «Да»).

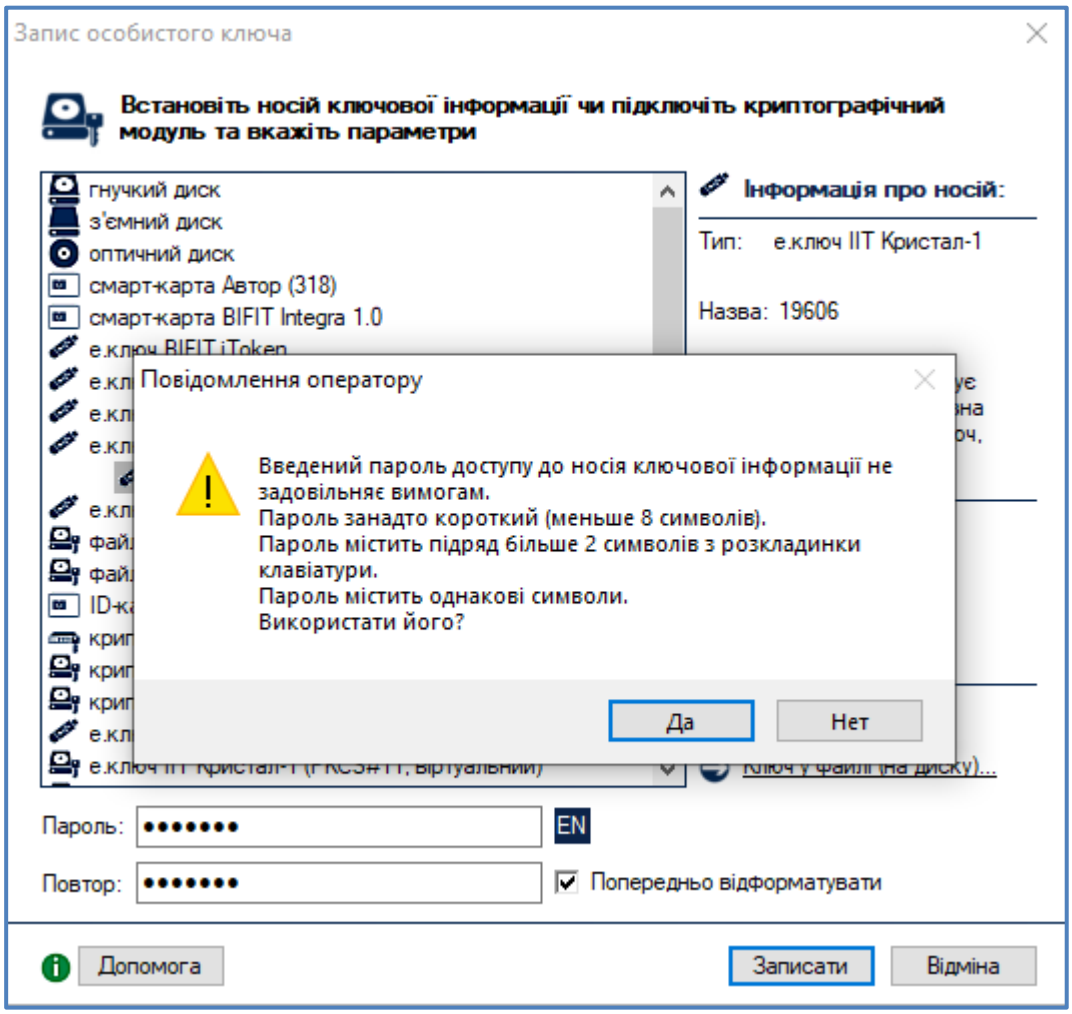

Рисунок 1.5

Після натискання кнопки «Записати» (рис. 1.4) на ЗНОК будуть згенеровані та збережені особисті ключі (для електронного підпису та шифрування) .

Після генерації ключів відображається повідомлення про запит на формування сертифіката відкритого ключа КЕП (рис. 1.6) та запит на формування сертифіката відкритого ключа протоколу розподілу ключів (рис. 1.7). Для продовження необхідно натиснути кнопку «ОК».

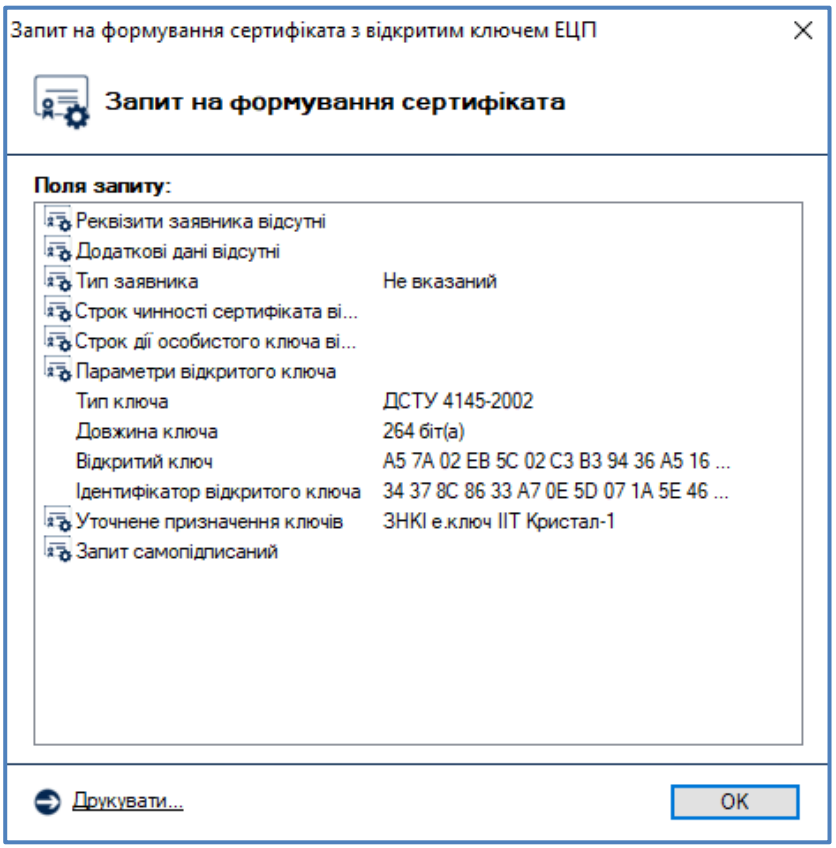

Рисунок 1.6

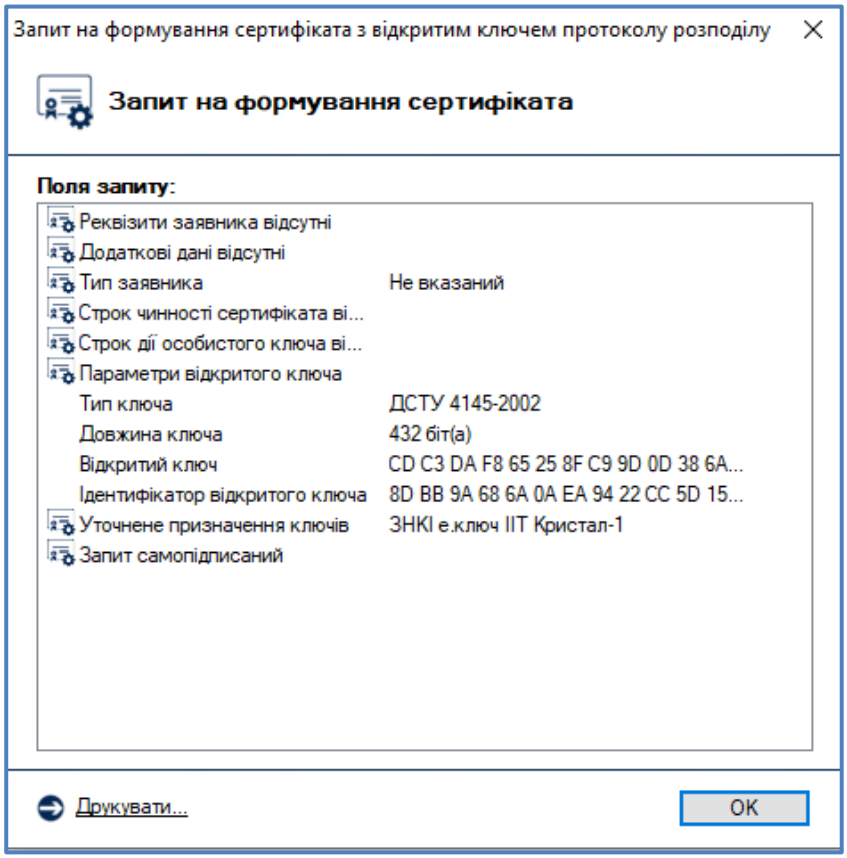

Рисунок 1.7

Для передачі запитів на формування сертифікатів відкритих ключів до АЦСК МВС або ВПР необхідно зберегти їх у файл. Для цього у вікні «Генерація ключів» встановити ознаку «Зберегти у файл» та натиснути кнопку «Далі».

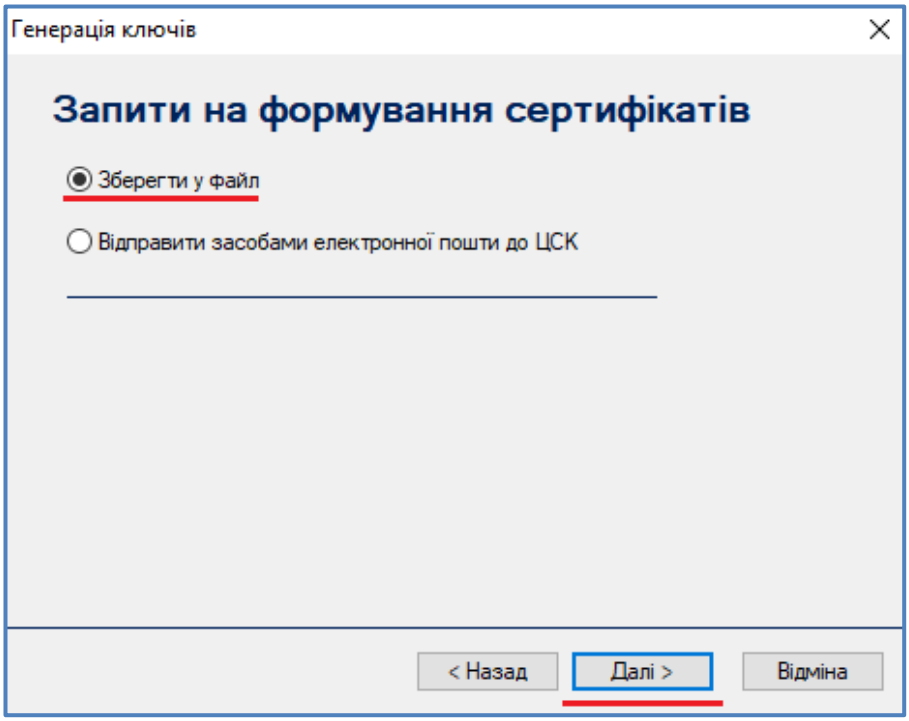

Рисунок 1.8

За замовчуванням файли запитів записуються на жорсткий диск комп'ютера, у папку: **C:\My Certificates and CRLs 13\.** Для визначення іншого місця збереження файлів запитів та зміни імені файлів запитів, натиснути кнопку «Змінити» (рис. 1.9), вибрати необхідну папку й вказати нові імена файлів запитів.

Увага! Файли запитів повинні зберігатись з ім'ям у наступному форматі: **EU-XXXXXXXX-ПрізвищеІніціали.p10** та **EU-KEP-XXXXXXXX-ПрізвищеІніціали.p10,**

де: **ПрізвищеІніціали** - прізвище та ініціали Підписувача (створювача електронної печатки).

Унікальні імена файлів запитів: EU-XXXXXXXX.p10 та EU-KEP-XXXXXXXX.p10, що формуються ПК «Користувач АЦСК МВС» за замовчуванням, повинні залишатись без змін та доповнюватися символом тире «-» , прізвищем та ініціалами Підписувача (створювача електронної печатки), які вказуються українською мовою, без пробілів та крапок перед розширенням файлу «**.p10**».

Наприклад:

EU-55F084F9-ІванюкВП.p10 та

EU-KEP-F3E4811A-ІванюкВП.p10.

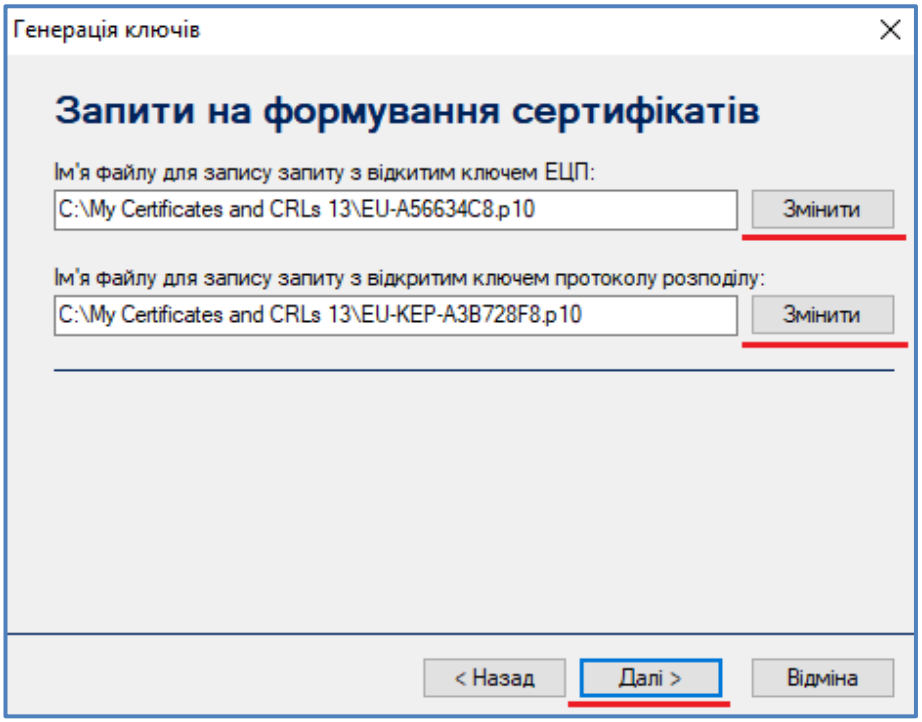

Рисунок 1.9

Для завершення генерації необхідно натиснути кнопку «Завершити» (рис. 1.10).

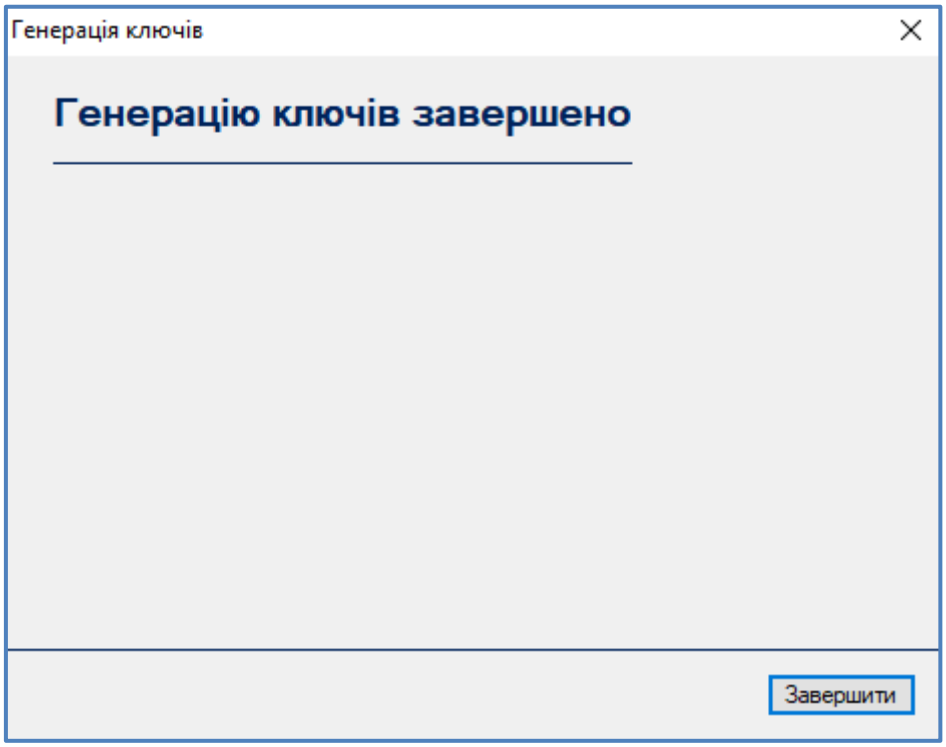

Рисунок 1.10

Після завершення операції генерації ключів Підписувач (створювач електронної печатки) переносить файли із запитами на формування сертифікатів

відкритих ключів з папки «C:\My Certificates and CRLs 13\» на знімний носій інформації (USB-Flash накопичувач). Знімний носій інформації надається АЦСК МВС або ВПР разом з пакетом відповідних документів для подальшого формування сертифікатів відкритих ключів.