ЗАТВЕРДЖУЮ
Командир військової частини А0136
полковник
Віталій КИНЧЕВСЬКИЙ
“___” _____ 2024 року

Настанова, щодо порядку використання програмного забезпечення ІІТ “Користувач ЦСК-1”

Київ 2024

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

ЕП	–	Електронний підпис чи печатка;
ЗНОК	–	Захищений носій ключової інформації;
ЖМД	-	жорсткий магнітний диск ПК
ПК	–	Персональна комп'ютер;
ПЗ	–	Програмне забезпечення "ІІТ Користувач ЦСК-1";
СВС	–	Список відкликаних сертифікатів;
ІТС	–	Інформаційно-телекомунікаційна система
КН	–	Кваліфікований надавач електронних довірчих послуг "Центр сертифікації ключів Збройних Сил України";
ЕНІ	–	електронний носій інформації типу ЖМД, Flash носій, CD, DVD тощо.

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Ця Інструкція узагальнює вимоги щодо порядку генерації пари ключів (особистий та відповідний йому відкритий ключ) ЕП в установах Збройних Сил України з метою подальшого отримання кваліфікованої електронної довірчої послуги (формування, перевірка та підтвердження чинності сертифіката ЕП) в **кваліфікованого надавача електронних довірчих послуг "Центр сертифікації ключів Збройних Сил України".**

Терміни в інструкції застосовуються у зазначеннях, наведених в Законі України "Про електронні довірчі послуги", постанові Кабінету Міністрів України від 1 серпня 2023 р. № 798 "Про затвердження "Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності" (далі – ПКМУ 798), Регламенті роботи кваліфікованого надавача електронних довірчих послуг "Центр сертифікації ключів Збройних Сил України" (далі – Регламент) та наказі Головнокомандувача Збройних Сил України від 15.01.2021 № 11 "Про затвердження Порядку отримання електронних довірчих послуг у Збройних Силах України" (далі – Наказ ГК ЗСУ № 11).

Генерація пари ключів кваліфікованого ЕП повинна здійснюватись особисто підписувачем чи створювачем (уповноваженим представником створювача)[1] електронної печатки за допомогою засобу кваліфікованого електронного підпису чи печатки. *(стаття 20 Закону України "Про електронні довірчі послуги")*

Підписувачі КН здійснюють генерацію пар ключів ЕП особисто за допомогою **Комплексу програмного користувача центру сертифікації ключів "ІІТ Користувач ЦСК-1"** (Експертний висновок від 05.04.2019 № 05/02/02-1424).

Надання допомоги підписувачам під час генерації пар ключів здійснює відповідальний підрозділ (працівник, особа) за організацію використання кваліфікованих електронних довірчих послуг в установі *(пункт 6 ПКМУ 749, п 2.2 Наказ ГК ЗСУ № 11).*

Генерація пар ключів для технічних та/або програмних засобів, обслуговуючого персоналу, а також мережевих ресурсів (поштових серверів, вебсайтів, тощо) здійснюється посадовою особою зі складу служби захисту інформації (СЗІ та КБ) в ІТС визначеною наказом керівника установи відповідальною за генерацію пар ключів. Генерація здійснюється відповідно до вимог інструкціями зі складу документації комплексних систем захисту інформації, затверджених в установленому порядку. *(пункти 2.1 та 2.2 наказу Генерального штабу Збройних Сил України від 17.07.2018 № 266 "Про затвердження Порядку надання електронних довірчих послуг для інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем Міністерства оборони та Збройних Сил України")*

---

[1] Далі підписувач або створювач електронної печатки (уповноважений представник створювача) – підписувач.

2. ВСТАНОВЛЕННЯ КОМПЛЕКСУ ПРОГРАМНОГО КОРИСТУВАЧА ЦЕНТРУ СЕРТИФІКАЦІЇ КЛЮЧІВ “ІІТ КОРИСТУВАЧ ЦСК-1”

Увага! Встановивши дане ПЗ ви зобов’язуєтесь використовувати його виключно за призначенням та в порядку визначеному цією Інструкцією.

Для встановлення ПЗ необхідно завантажити файл з інсталяційним пакетом з вебсайту КН http://ca.mil.gov.ua за наступним посиланням у розділі **ЗАВАНТАЖИТИ**.

Далі здійснити інсталяцію ПЗ виконавши наступні дії:

1.1. Запускаємо інсталятор ПЗ – EUInstall.exe (рис. 1.1).

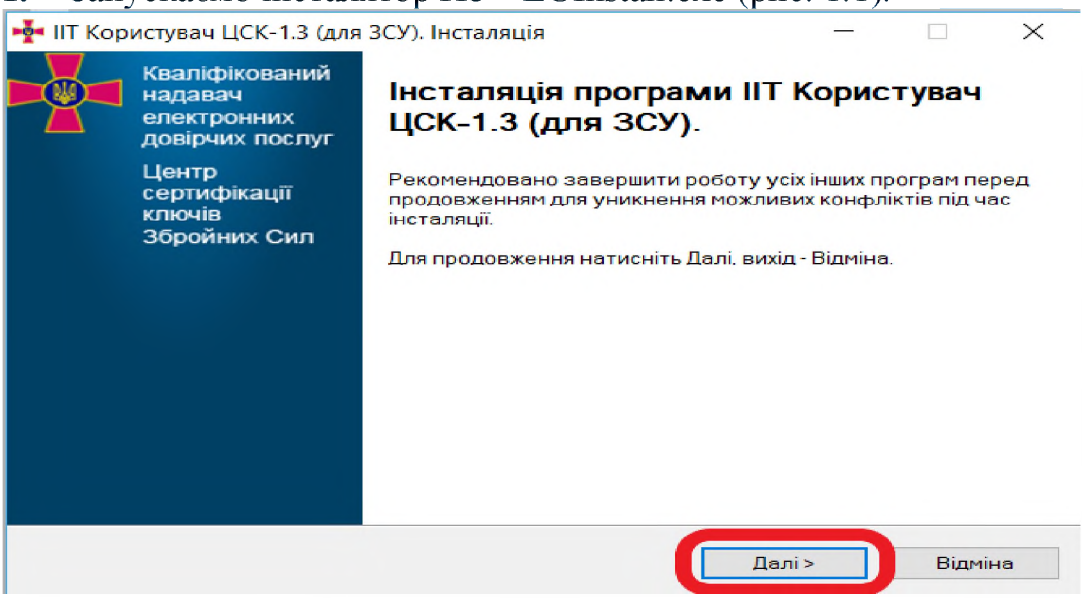


Рисунок 1.1

1.2. Ознайомлюємось з ліцензійною угодою та погоджуємось з її умовами, для продовження інсталяції натискаємо кнопку “Далі” (рис. 1.2).

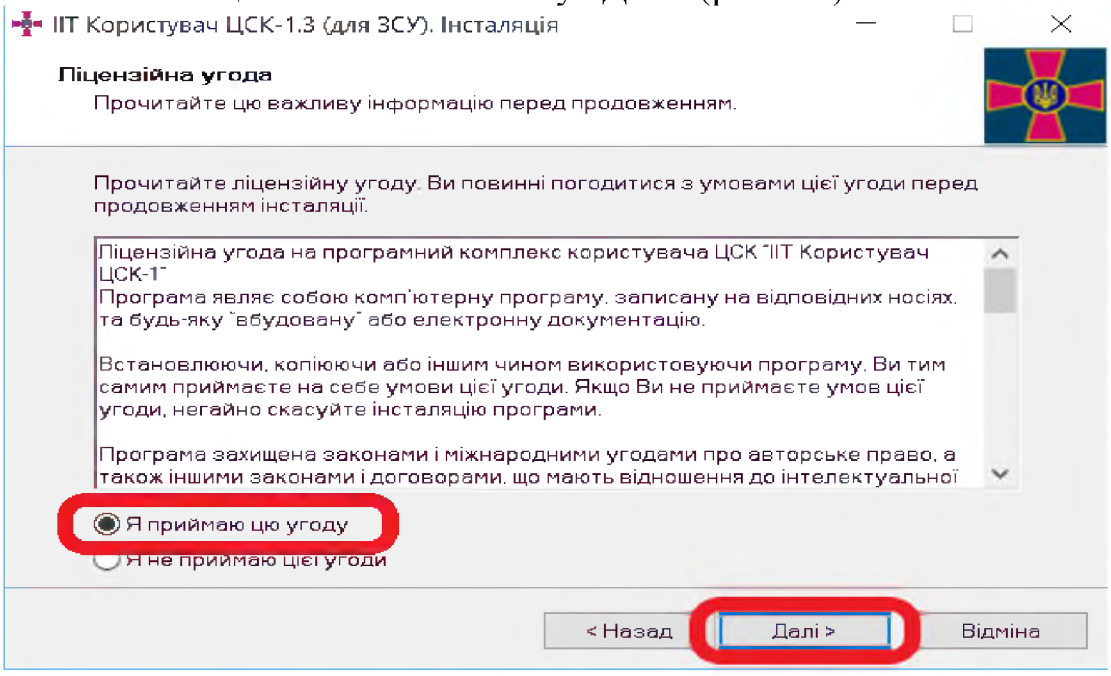


Рисунок 1.2

1.3. Каталог ПЗ у меню “Пуск” створюється автоматично, змінювати його не рекомендується, натискаємо кнопку “Далі” (рис. 1.3).

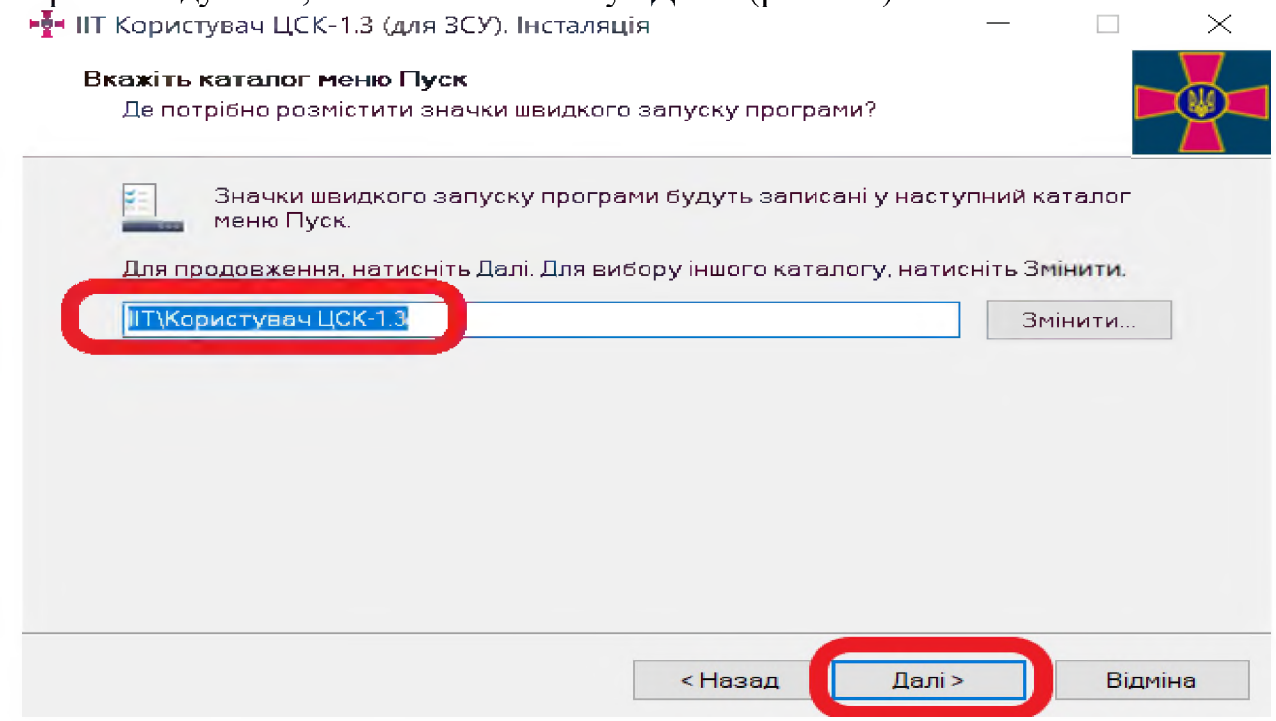


Рисунок 1.3

1.4. Під час встановлення ПЗ файлове сховище (локальний каталог, призначений для зберігання посилених сертифікатів та СВС) створюється в розділі C:\ автоматично. Для зміни розташування файлового сховища необхідно натиснути кнопку “Змінити” та обрати відповідний каталог. Для продовження інсталяції натискаємо кнопку “Далі” (рис. 1.4).

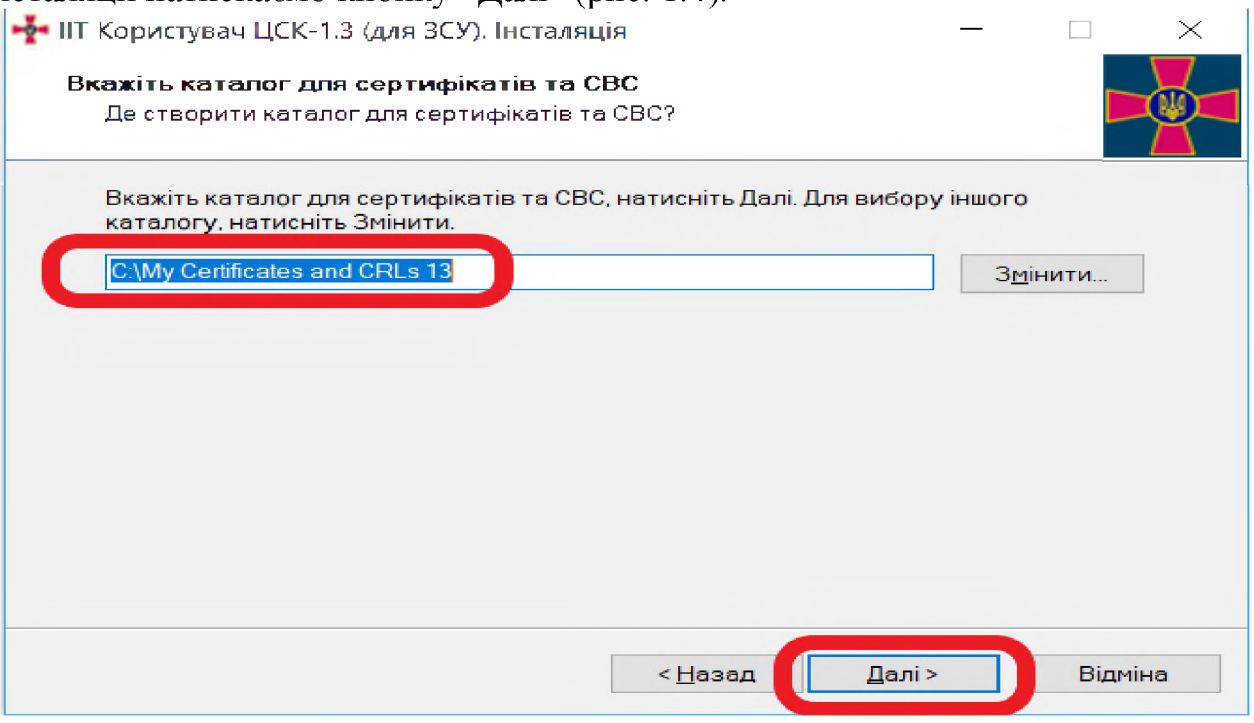


Рисунок 1.4

1.5. За необхідності можна створити ярлик на робочому столі та запустити ПЗ після завершення його інсталяції. Для цього необхідно проставити відповідні позначки (рис. 1.5). Для продовження інсталяції натискаємо кнопку “Далі”.

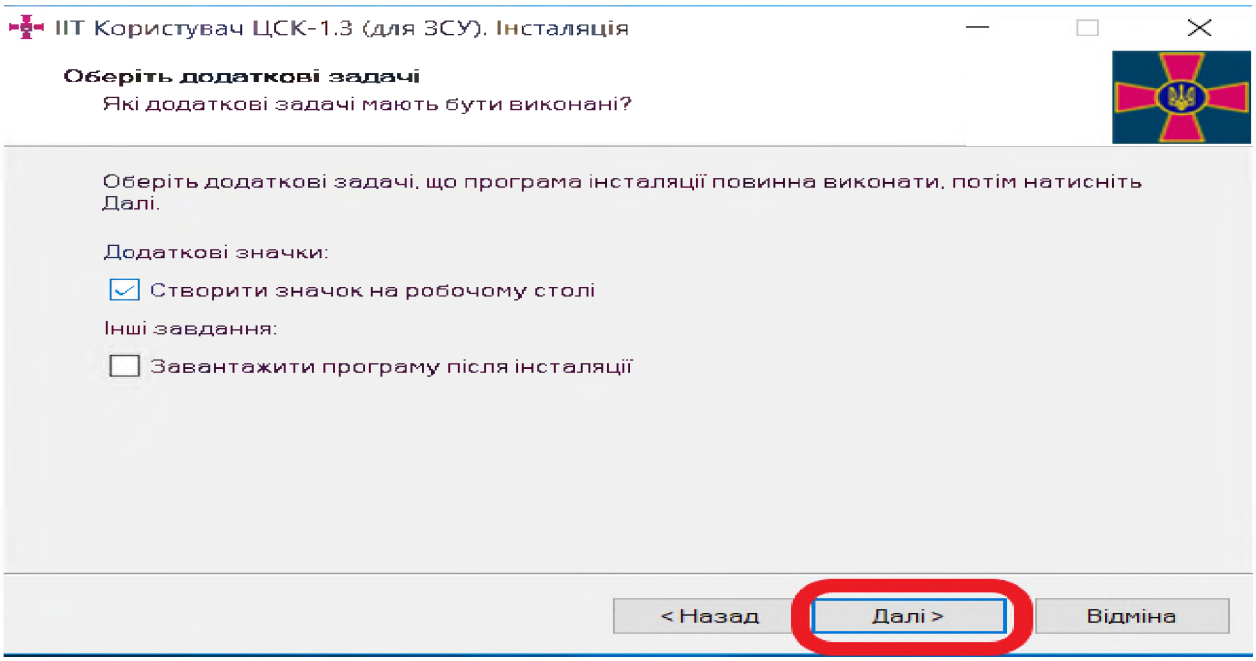


Рисунок 1.5

1.6. У вікні готовності до інсталяції натискаємо кнопку “Встановити” (рис. 1.6). Якщо параметри інсталяції не задовольняють користувача, їх можна змінити натиснувши кнопку “Назад”. Для виходу з ПЗ без інсталяції необхідно натиснути “Відміна”.

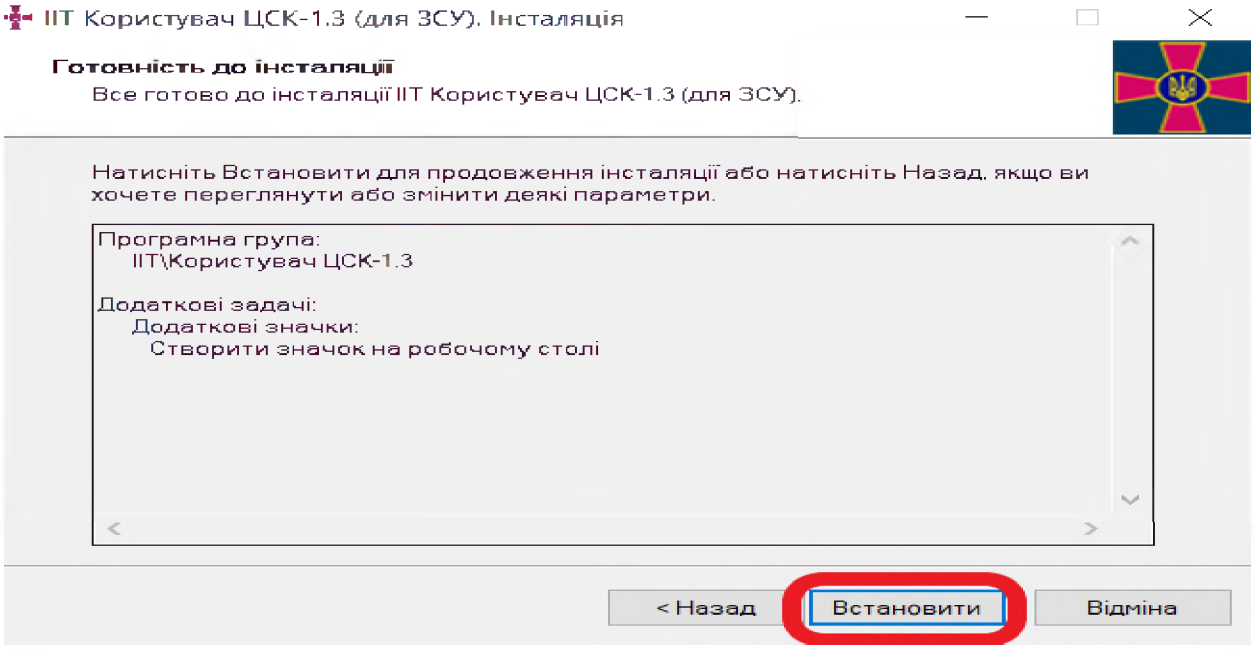


Рисунок 1.6

1.7. Після завершення інсталяції запущена ПЗ має вигляд – рис. 1.7. Перед використанням програму необхідно налаштувати.

Рисунок 1.7

1.8. У зв’язку з відсутністю в ПЗ функції автоматичного оновлення версій, подальше його обслуговування здійснюватиметься шляхом розміщення на вебсайті (http://ca.mil.gov.ua.) оновленого файлу з інсталяційним пакетом. Про оновлення інсталяційного пакету ПЗ буде завчасно сповіщатись в розділі “Новини” вебсайту (http://ca.mil.gov.ua.).

3. ГЕНЕРАЦІЯ ПАРИ КЛЮЧІВ

Для генерації особистих та відкритих ключів ЕП на робочому місці підписувача застосовується засіб кваліфікованого електронного підпису – "ІІТ Користувач ЦСК-1".

Генерація пар ключів може бути здійснена на захищеному носії особистого ключа (ЗНОК) або зі збереженням особистого ключа на електронний носій інформації (незахищений), при чому **особисті ключі ЕП** автоматично захищається паролем.

Увага! Відповідальність за забезпечення конфіденційності особистого ключа ЕП та паролю до нього несе підписувач. У разі передачі носія з особистим ключем електронного підпису та пароля до нього сторонній особі ключ вважається скомпрометованим.

Для генерації ключа пар ключів у ПЗ необхідно обрати підпункт "Згенерувати ключі" в пункті меню "Особистий ключ" (рис. 2.1).

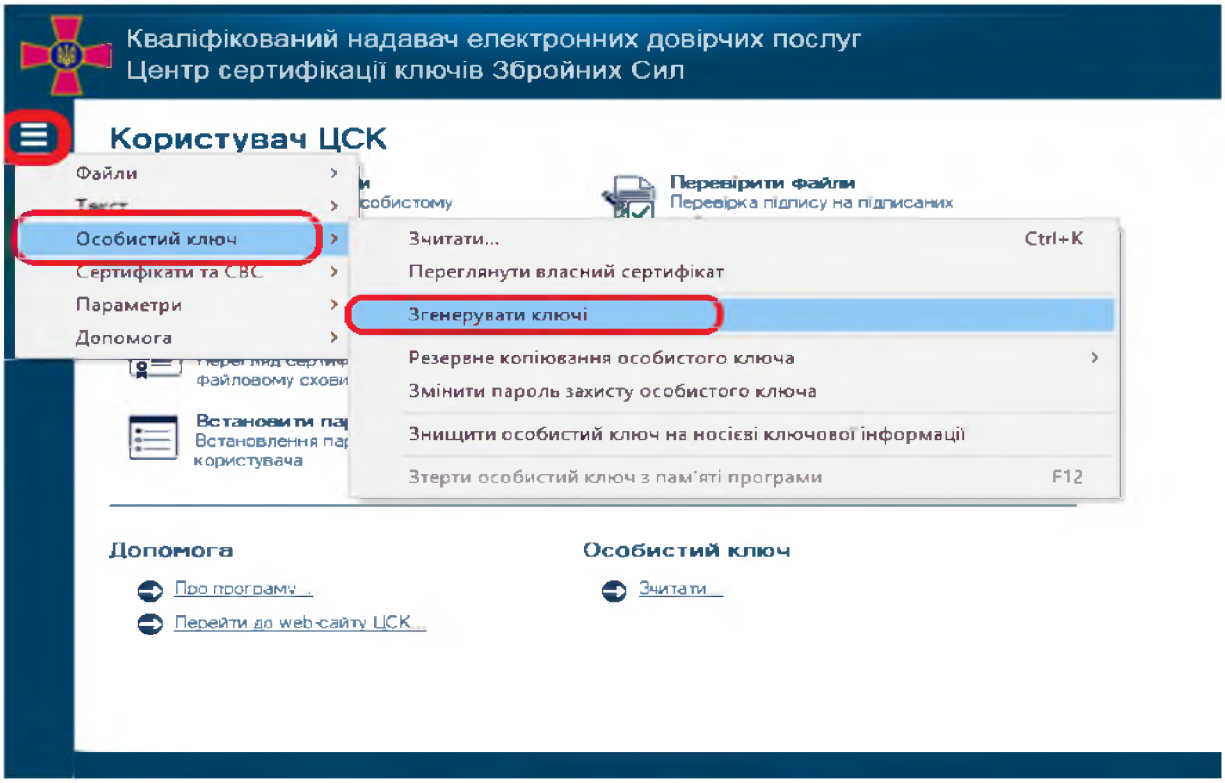


Рисунок 2.1

Згенеровані **відкриті ключі ЕП** у вигляді файлів формату PKCS#10 (запити на формування сертифікатів) зберігаються на ЕНІ робочого місця підписувача.

Файли відкритих ключів, разом з комплектом реєстраційних документів подаються до КН або його ВПР для формування кваліфікованих сертифікатів підписувача. Відкриті ключі, можуть надаватись для сертифікації особисто підписувачем, створювачем електронної печатки, відповідальною особою, або пересилатися через систему електронного документообігу з застосуванням кваліфікованого електронного підпису для підтвердження їх цілісності та автентичності.

3.1. Генерація пари ключів зі збереженням особистого ключа на електронний носій інформації (незахищений).

Генерація пари ключів електронного підпису зі збереженням особистого ключа на електронний носій інформації (незахищений) дозволена тільки для підписувачів що не здійснюють повноваження, спрямовані на набуття, зміну чи припинення прав та/або обов'язків установи відповідно до закону, не здійснюють інформаційний обмін з іншими установами, а також не ідентифікуються за ЕП в ІТС військового призначення.

Щоб згенерувати особистий ключ потрібно вказати параметри генерації ключів. Параметри генерації пари ключів підписувача необхідно встановити **"для державних алгоритмів та протоколів"** (рис. 2.2).

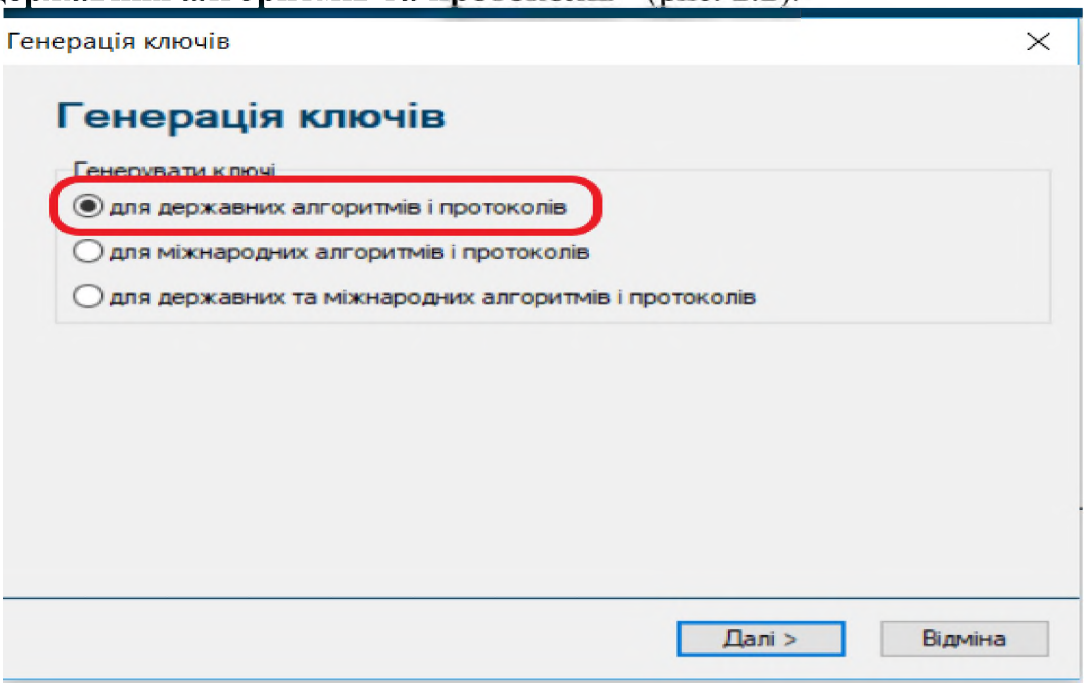


Рисунок 2.2

На наступній сторінці вказані параметри вказати відповідно до (рис 2.3). Для продовження необхідно натиснути кнопку "Далі".

Заборонено використовувати окремий ключ для протоколу розподілу та/або змінювати місце розміщення параметрів.

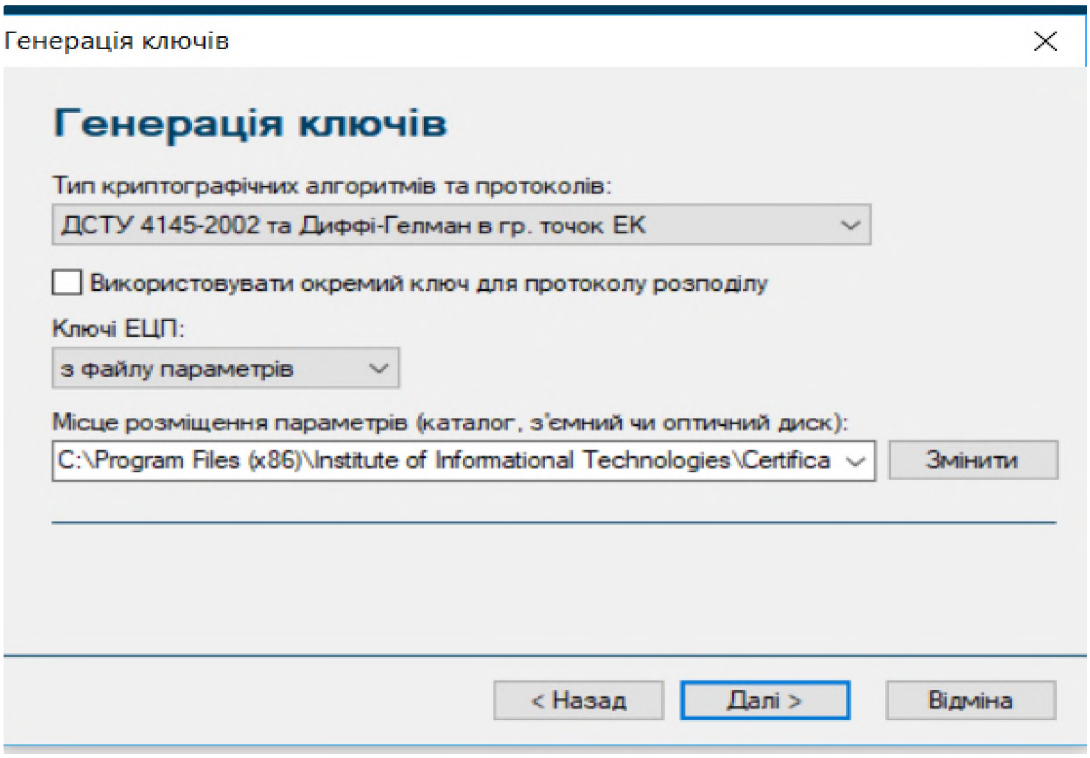


Рисунок 2.3

Далі необхідно встановити **ЕНІ** для запису особистого ключа у пристрій запису та на наступній сторінці (рис. 2.4) вказати:

– тип носія ключової інформації;
– назву носія (назва каталогу);
– пароль доступу до файлу особистого ключа – 2 рази.

ЕНІ можуть бути наступних типів:

– з'ємні диски (flash-диски);
– оптичні диски (CD-R, CD-RW, DVD-R або DVD-RW);
– ЖМД робочого місця підписувача.

Пароль захисту особистого ключа повинен відповідати наступним вимогам:

– довжина - не менше 8 символів;
– не повинен містити однакові символи;
– не повинен містити підряд більше ніж 2 символи з розкладки клавіатури;
– дозволені символи - 'a-z', 'A-Z', '0-9', '+', '-'.

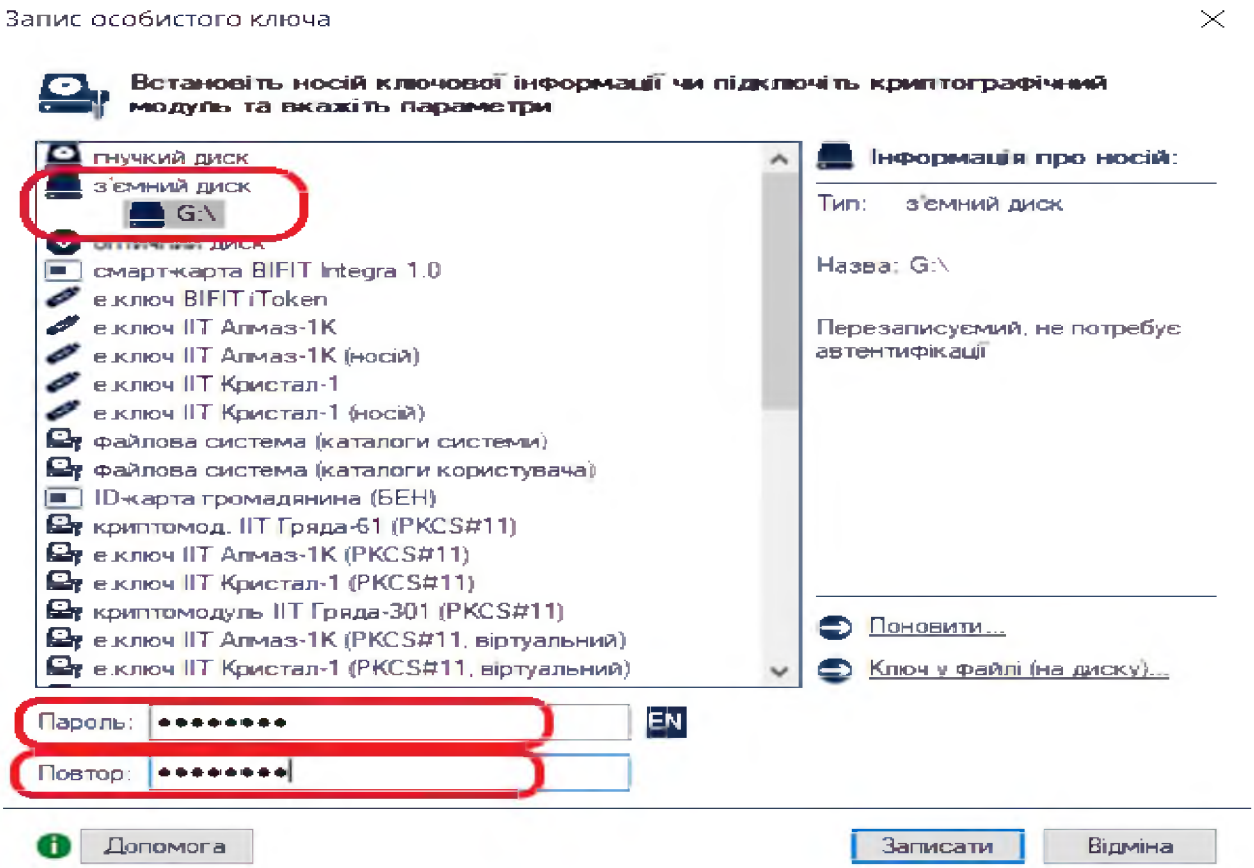


Рисунок 2.4

Після запису особистого ключа на ЕНІ, буде виведено вміст простого запиту на формування сертифікату з відкритим ключем ЕП для державних алгоритмів та протоколів (рис. 2.5) (самопідписаного відкритого ключа), після перевірки вмісту простого запиту необхідно натиснути “ОК”.

На наступній сторінці майстра (рис. 2.6) потрібно вказати спосіб збереження запиту на формування сертифіката (відкритого ключа), обираємо **Зберегти у файл**.

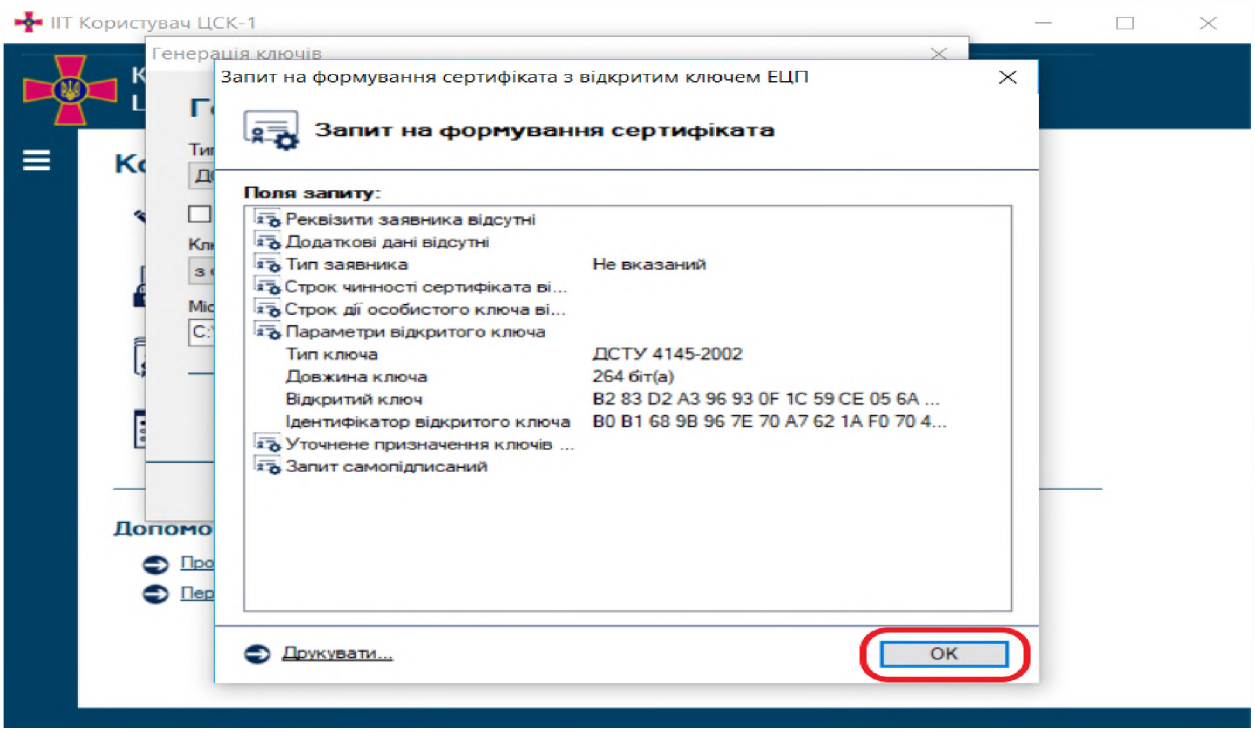


Рисунок 2.5

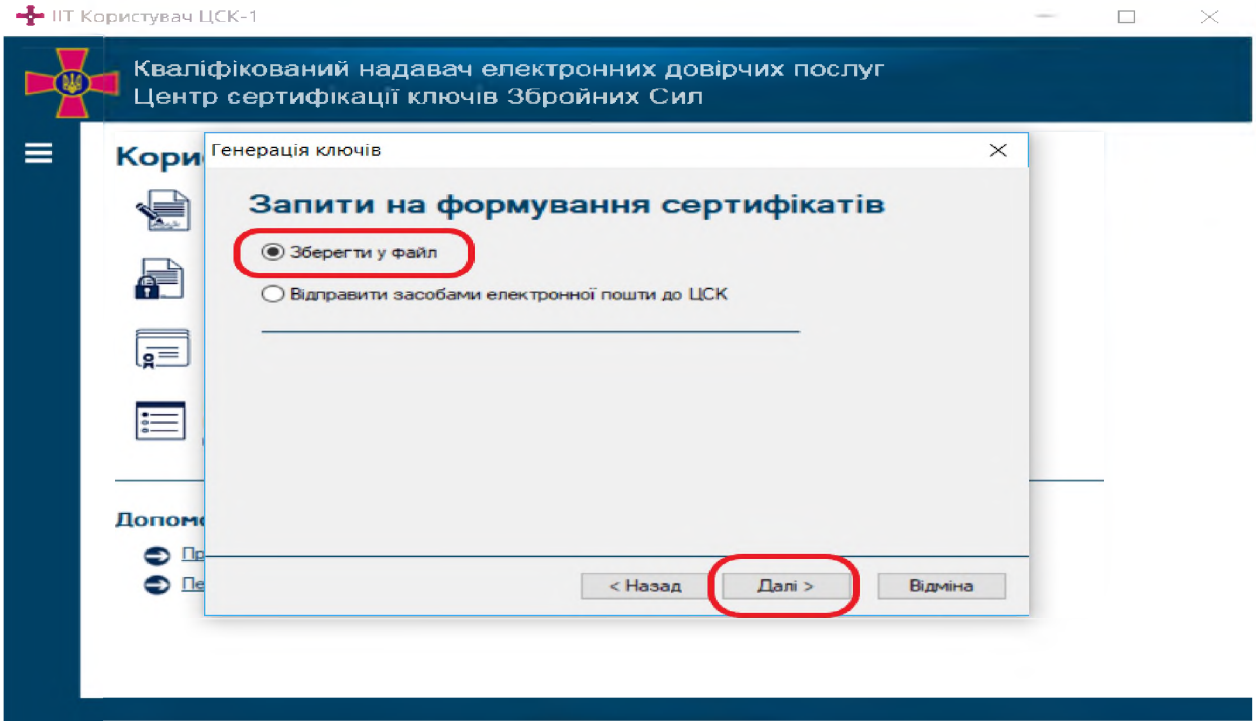


Рисунок 2.6

У наступному вікні (рис. 2.7) необхідно буде вказати ім’я файлу для запису запиту на формування сертифіката у файл. Запит повинен бути записаний на носій інформації чи на жорсткий диск. Після цього запит повинен бути переданий до КН або його ВПР для формування кваліфікованого сертифіката.

Увага! Для коректної ідентифікації запитів з відкритим ключем ЕП підписувача файл запиту на формування кваліфікованого сертифіката відкритого ключа обов’язково зберігатись з ім’ям у наступному форматі:

“EU- ПІБ.p10”, де: ПІБ – прізвище та ім’я по батькові підписувача, що є власником особистого ключа;

“*.p10”, “EU-” – унікальне розширення та ідентифікатор файлу запиту, що формується програмним забезпеченням за замовчуванням та повинно залишатись без змін.

Наприклад: **EU-Іванов І.І.p10**

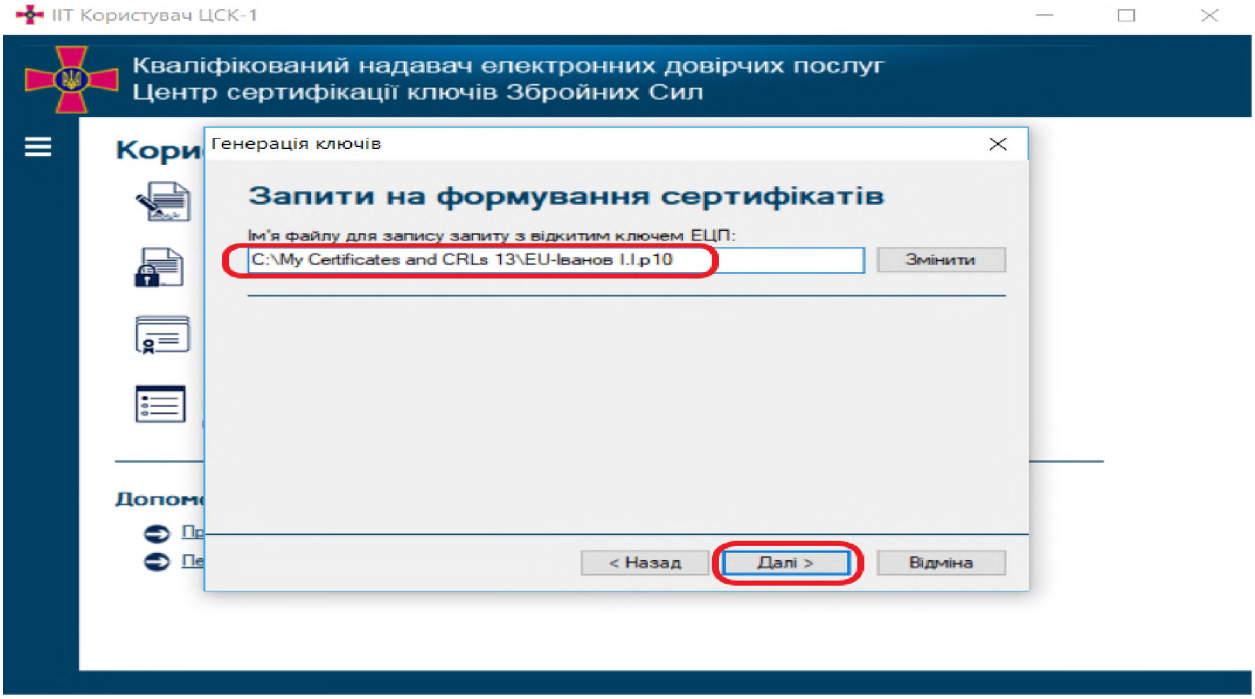


Рисунок 2.7

3.2. Генерація пар ключів для роботи за державними алгоритмами та протоколами на захищеному носії особистого ключа (ЗНОК).

Щоб згенерувати особистий ключ потрібно вказати параметри генерації ключів **“для державних алгоритмів та протоколів”** (рис. 2.8).

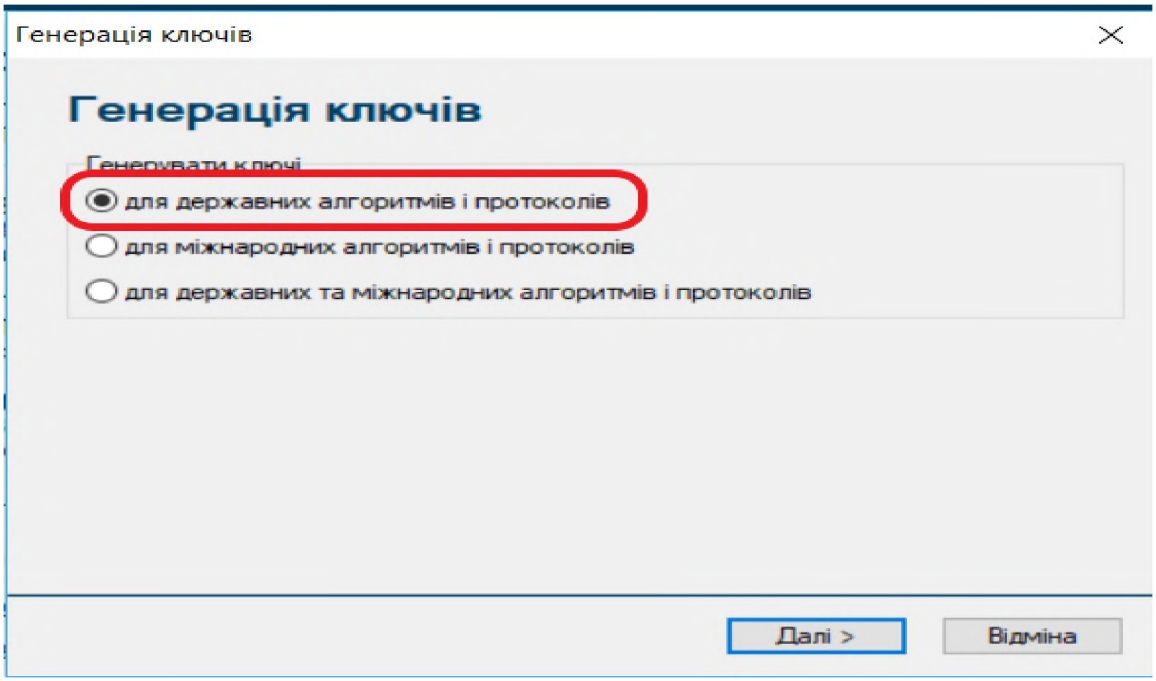


Рисунок 2.8

На наступній сторінці вибрати параметр **“Використовувати окремий ключ для протоколу розподілу”** та інші параметри відповідно до до рисунку 2.9, при цьому буде згенеровано дві ключові пари, одна з яких буде використовуватись для підписання даних, а друга (ключ протоколу розподілу) буде використовуватись для шифрування даних. Для продовження генерації ключа необхідно натиснути кнопку “Далі”.

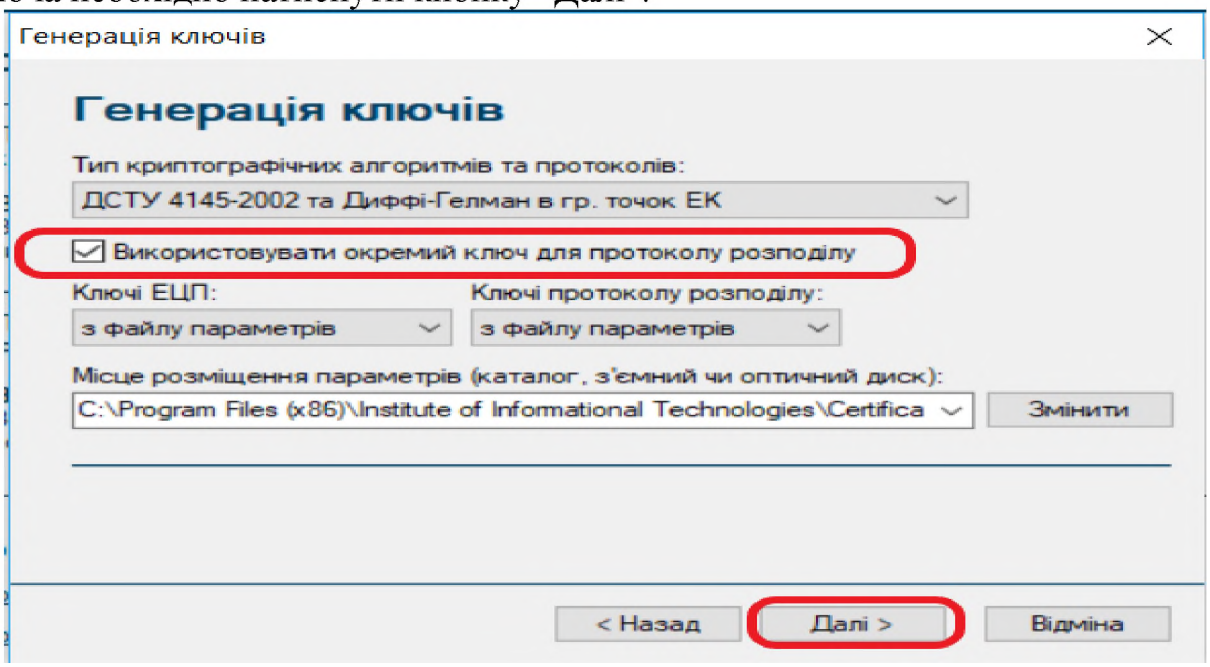


Рисунок 2.9

Далі необхідно встановити **ЗНОК** для запису особистого ключа у пристрій запису та на наступній сторінці майстра (рис. 2.10) вказати:

- тип ЗНОК;
- серійний номер ЗНОК;
- новий пароль доступу до ключового носія;
- попередньо від форматувати.

Генерація пари ключів електронного підпису здійснюється в режимі “Апаратний криптомодуль”.

Заборонено вибирати для генерації ключа типи носія ключової інформації “гнучкий диск”, “з’ємний диск”, “оптичний диск”, “файлова система” або тип носія з приміткою “(носій)”.

Пароль захисту особистого ключа повинен відповідати наступним вимогам:

- довжина – не менше 8 символів;
- не повинен містити однакові символи;
- не повинен містити підряд більше ніж 2 символи з розкладинки клавіатури;
- дозволені символи - 'a-z', 'A-Z', '0-9', '+', '-'.

Примітка. Такі вимоги носять рекомендаційний характер.

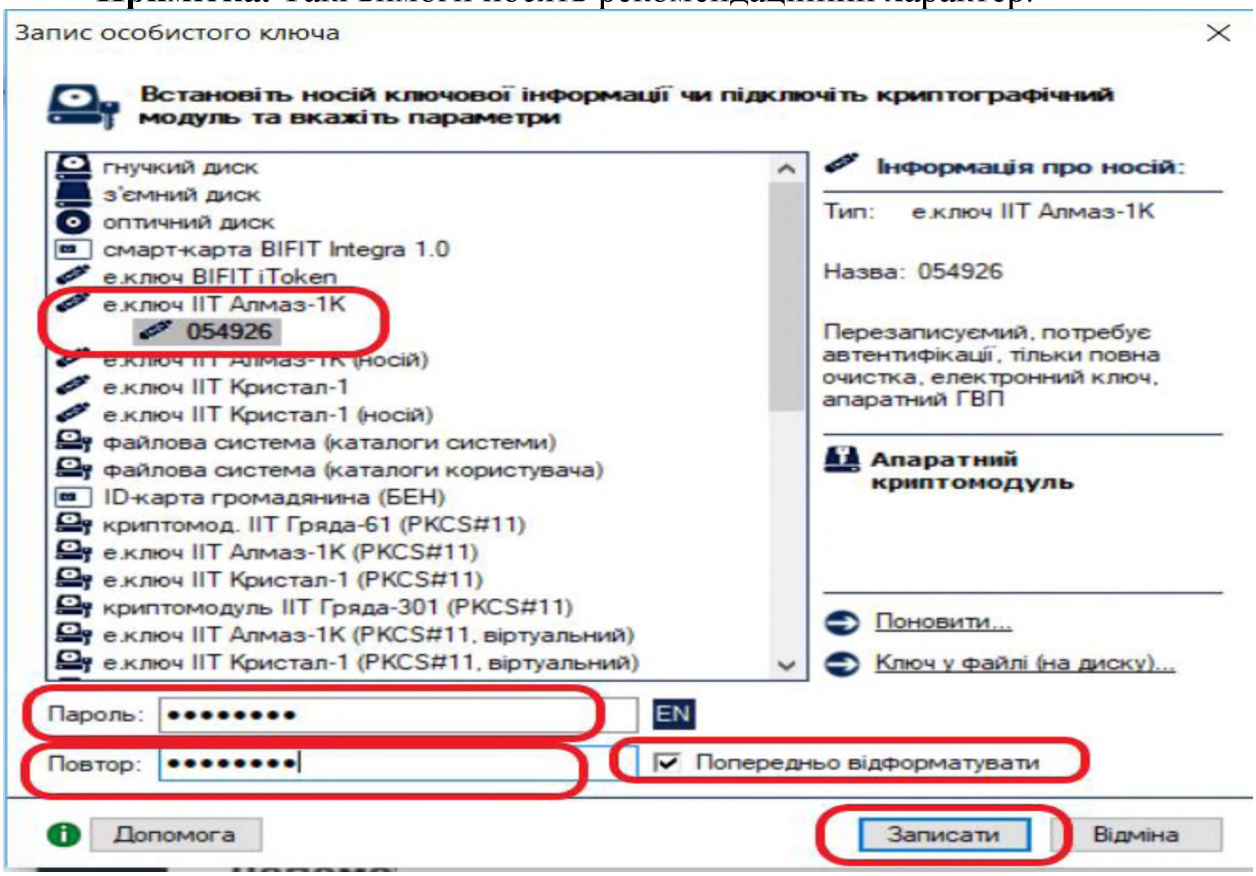


Рисунок 2.10

Після форматування (знищення всіх ключів, що зберігались на ЗНОК) та запису особистого ключа на ЗНОК, буде виведено вміст простого запиту на формування сертифікату з відкритим ключем ЕП для державних алгоритмів та протоколів (рис. 2.11), потрібно переконатись що особистий ключ згенеровано на ЗНОК, після перевірки вмісту простого запиту необхідно натиснути “ОК”. На

наступній сторінці майстра (рис. 2.12) потрібно вказати спосіб збереження запиту на формування сертифіката, обираємо **Зберегти у файл**.

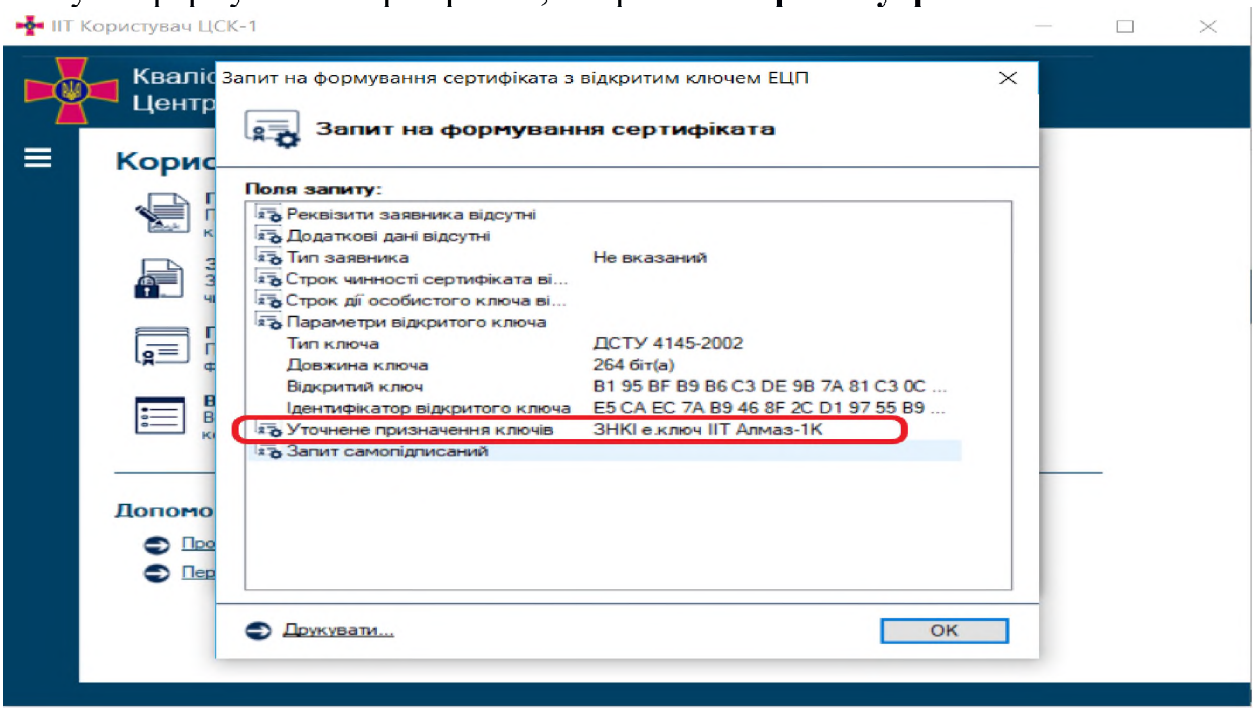


Рисунок 2.10

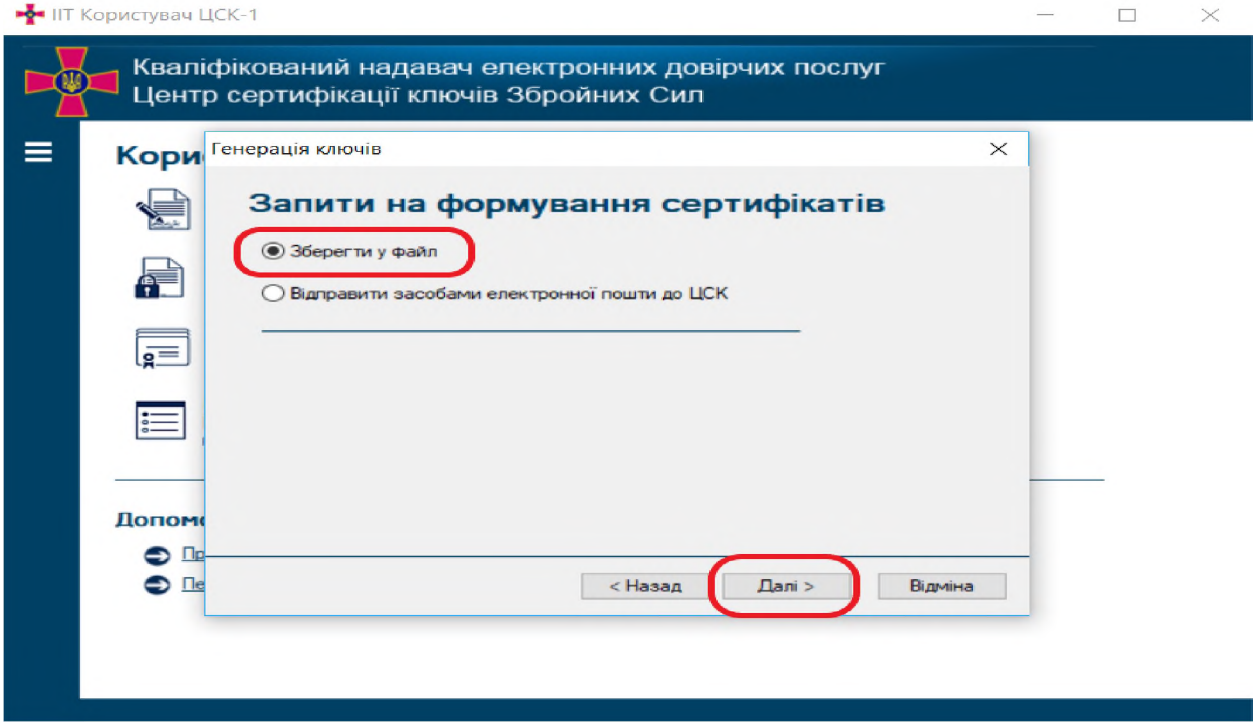


Рисунок 2.11

У наступному вікні (рис. 2.12) необхідно буде вказати ім’я файлу для запису запиту на формування сертифіката у файл. Запит повинен бути записаний на носій інформації чи на жорсткий диск. Після цього запит повинен бути переданий до КН або його ВПР для формування кваліфікованого сертифіката.

Увага! Для коректної ідентифікації запитів з відкритим ключем ЕП та протоколом розподілу ключів підписувача файли запиту на формування кваліфікованих сертифікатів обов’язково зберігатись з ім’ям у наступному форматі:

“EU-ПІБ.p10” – відкритий ключ електронного підпису за державними алгоритмами та протоколами (буде використовуватись для підписання даних);

“EU-KEP- ПІБ.p10” – відкритий ключ протоколу розподілу (буде використовуватись для шифрування даних).

ПІБ – прізвище та ім’я по батькові підписувача, що є власником особистого ключа.

“*.p10”, “EU-” та “EU-KEP-” – унікальні розширення та ідентифікатори файлу запиту, повинні залишатись без змін.

Наприклад: **EU-Іванов І.І.p10, EU-KEP-Іванов І.І.p10.**

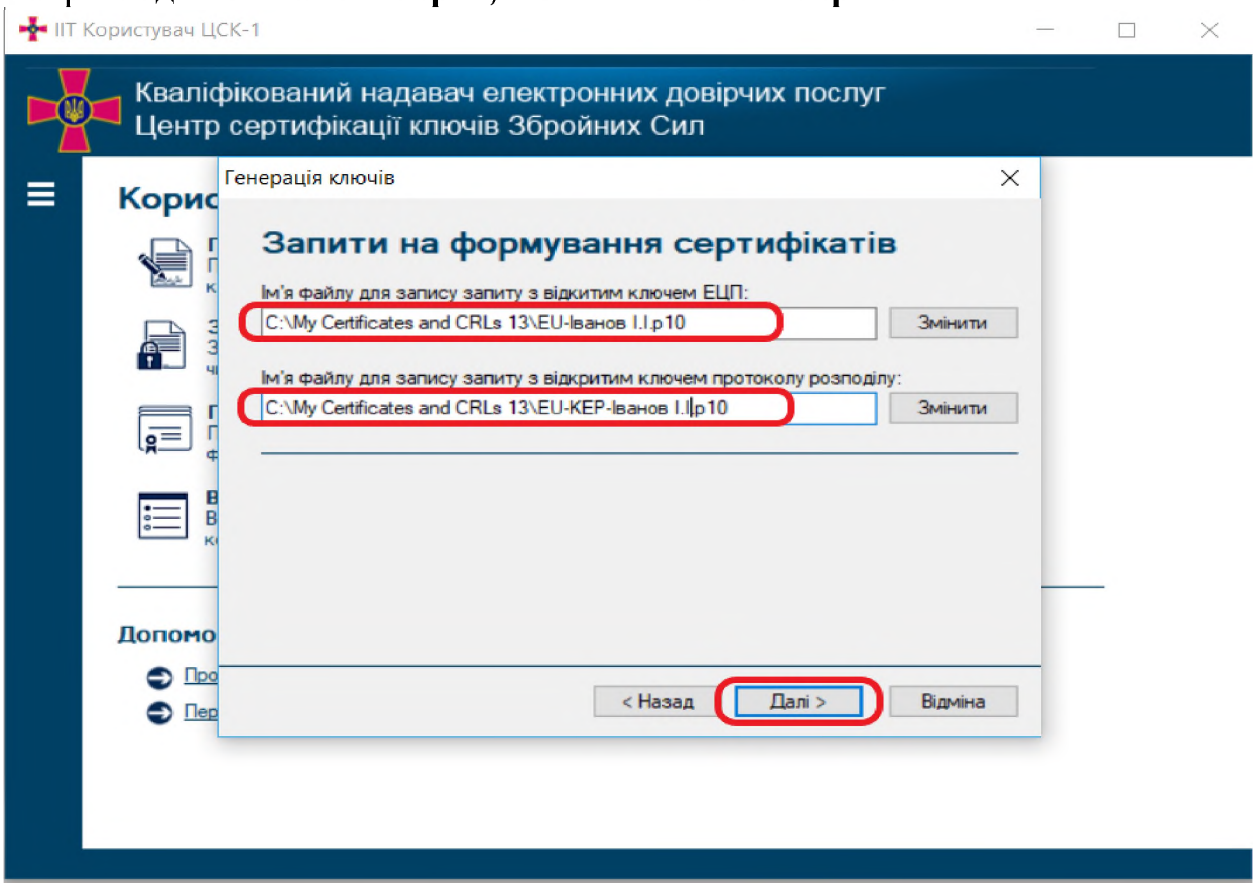


Рисунок 2.12

3.3. Генерація пар ключів для державних та міжнародним алгоритмів та протоколів на захищеному носії особистого ключа (ЗНОК).

Генерація пар ключів підписувачів для роботи за державними разом з міжнародними алгоритмами та протоколами здійснюється виключно на ЗНОК.

Щоб згенерувати особистий ключ потрібно вказати параметри генерації ключів **“для державних та міжнародних алгоритмів та протоколів”** (рис. 2.13).

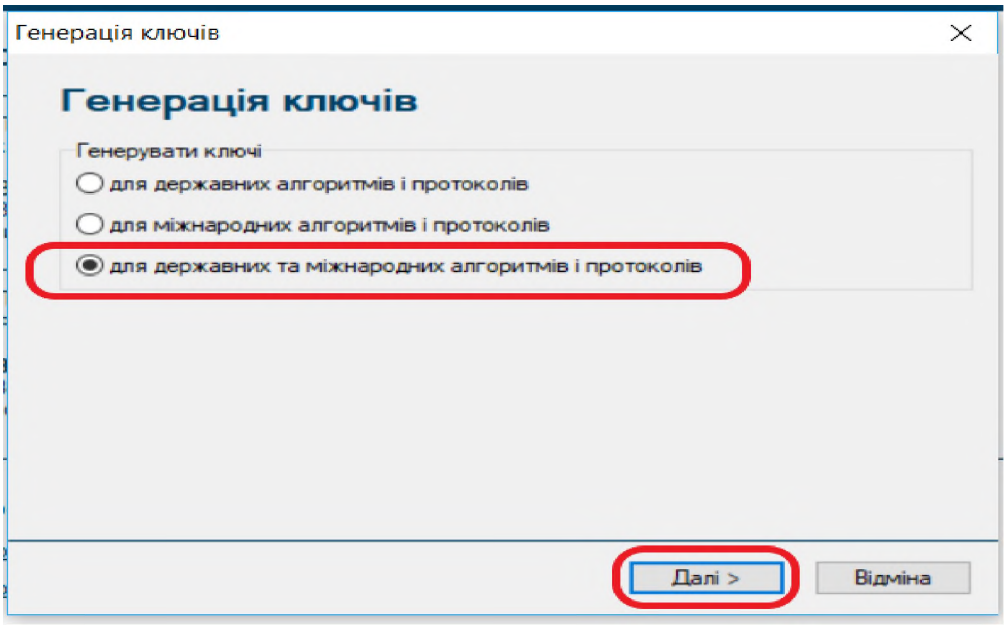


Рисунок 2.13

На наступній сторінці вибрати параметр відповідно до рисунку (рис 2.14), Для продовження генерації ключа необхідно натиснути кнопку “Далі”.

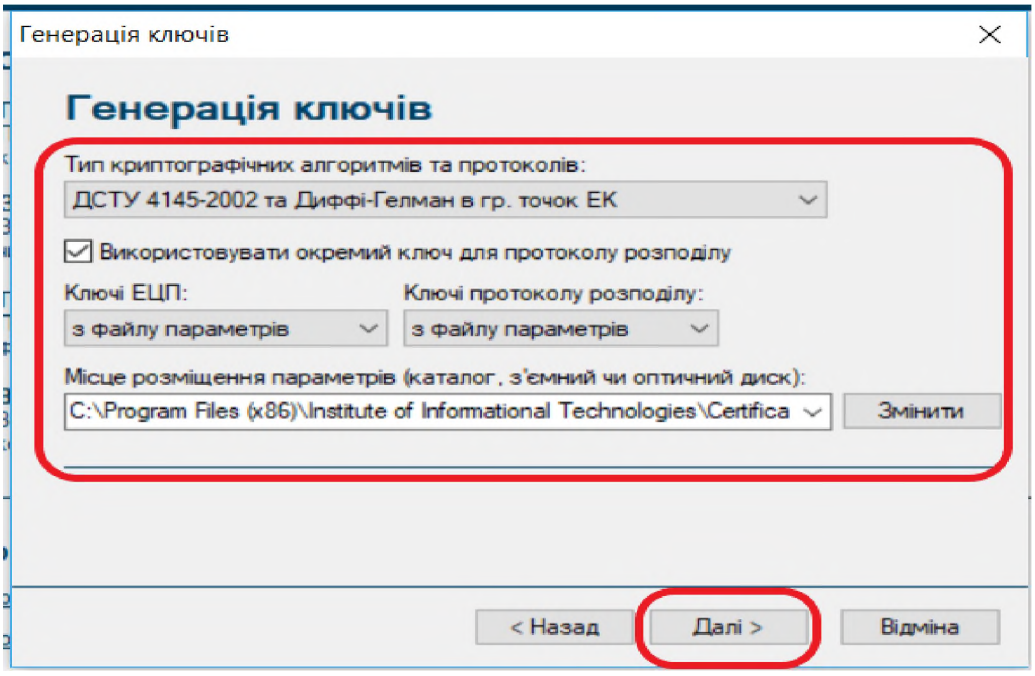


Рисунок 2.14

На наступній сторінці вибрати параметр відповідно до рисунку (рис 2.15), Для продовження генерації ключа необхідно натиснути кнопку “Далі”

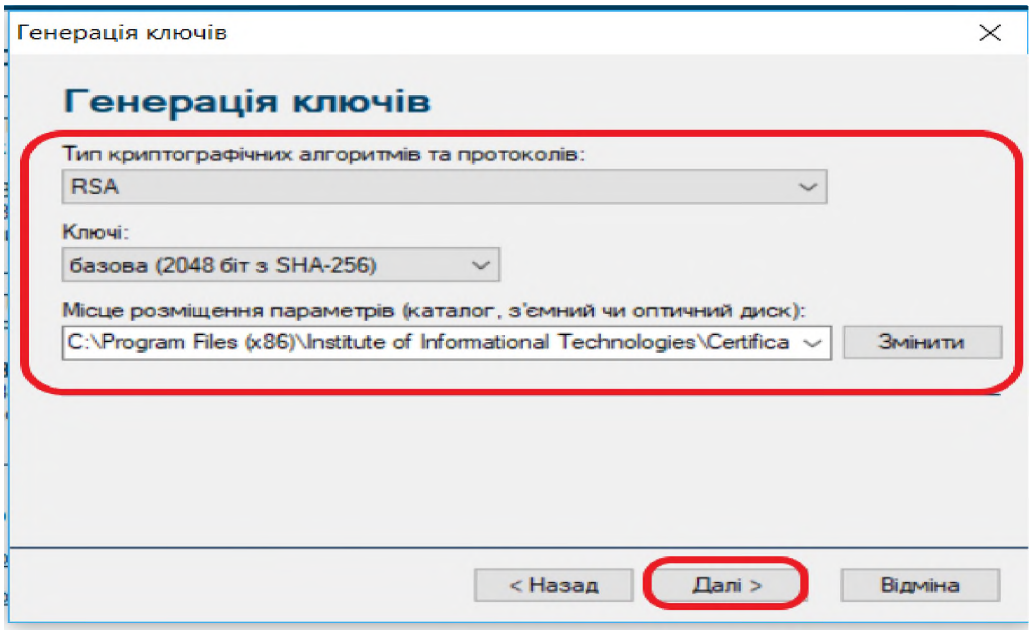


Рисунок 2.15

Далі необхідно встановити **захищений носій особистого ключа** для запису особистого ключа у пристрій запису та на наступній сторінці майстра (рис. 2.16) вказати:

- тип ЗНОК;
- серійний номер ЗНОК;
- новий пароль доступу до ключового носія;
- попередньо від форматувати.

Пароль повинен відповідати наступним вимогам:

- довжина - не менше 8 символів;
- не повинен містити однакові символи;
- не повинен містити підряд більше ніж 2 символи з розкладинки клавіатури;
- дозволені символи - 'a-z', 'A-Z', '0-9', '+', '-'.

Примітка. Такі вимоги носять рекомендаційний характер.

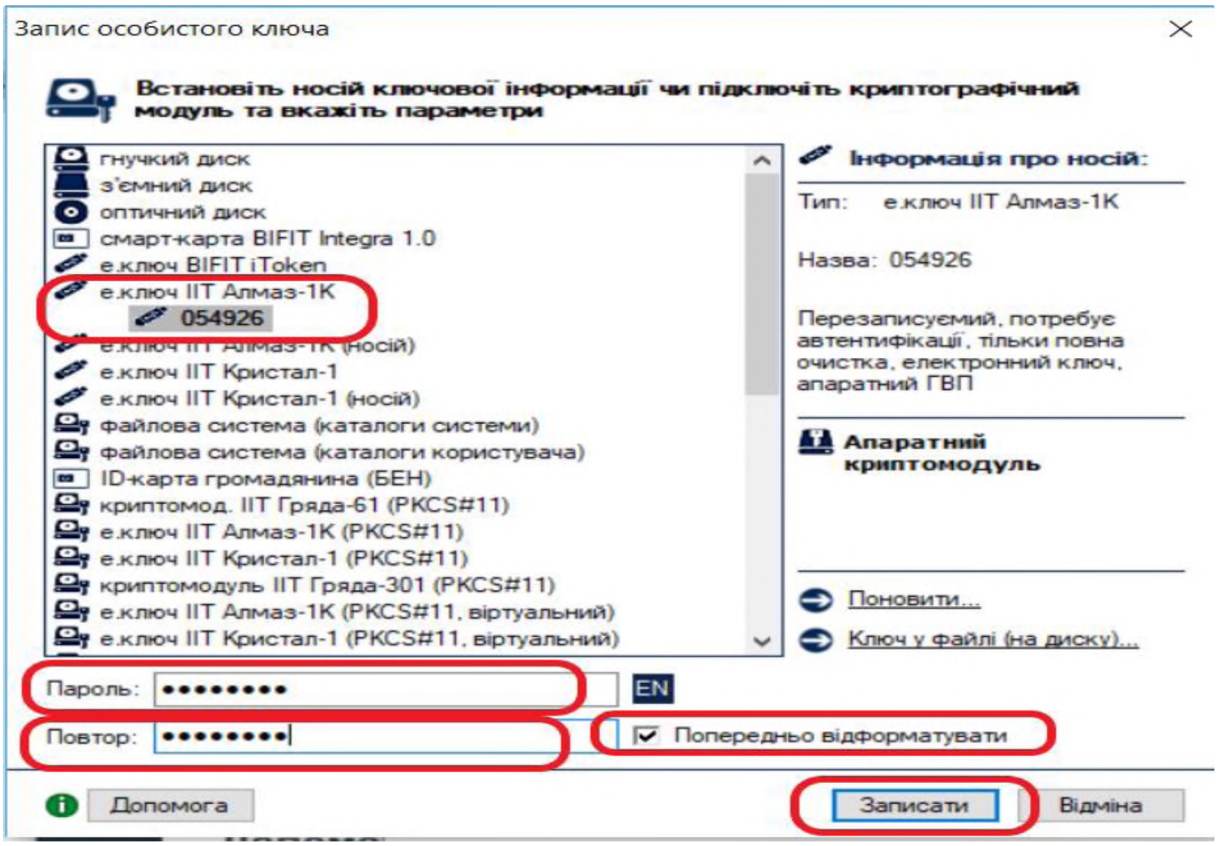


Рисунок 2.16

Після запису особистого ключа на ЗНОК, буде виведено вміст простого запиту на формування сертифікату з відкритим ключем ЕП для державних та міжнародних алгоритмів та протоколів (рис. 2.17, 2.18, 2.19), потрібно переконатись що особистий ключ згенеровано на ЗНОК[2]. Після перевірки вмісту простого запиту необхідно натиснути ”ОК”. На наступній сторінці майстра (рис. 2.20) потрібно вказати спосіб збереження запиту на формування сертифіката, обираємо **Зберегти у файл**.

[2] Уточнене призначення для ключа RSA – відсутнє навіть при генерації на ЗНОК.

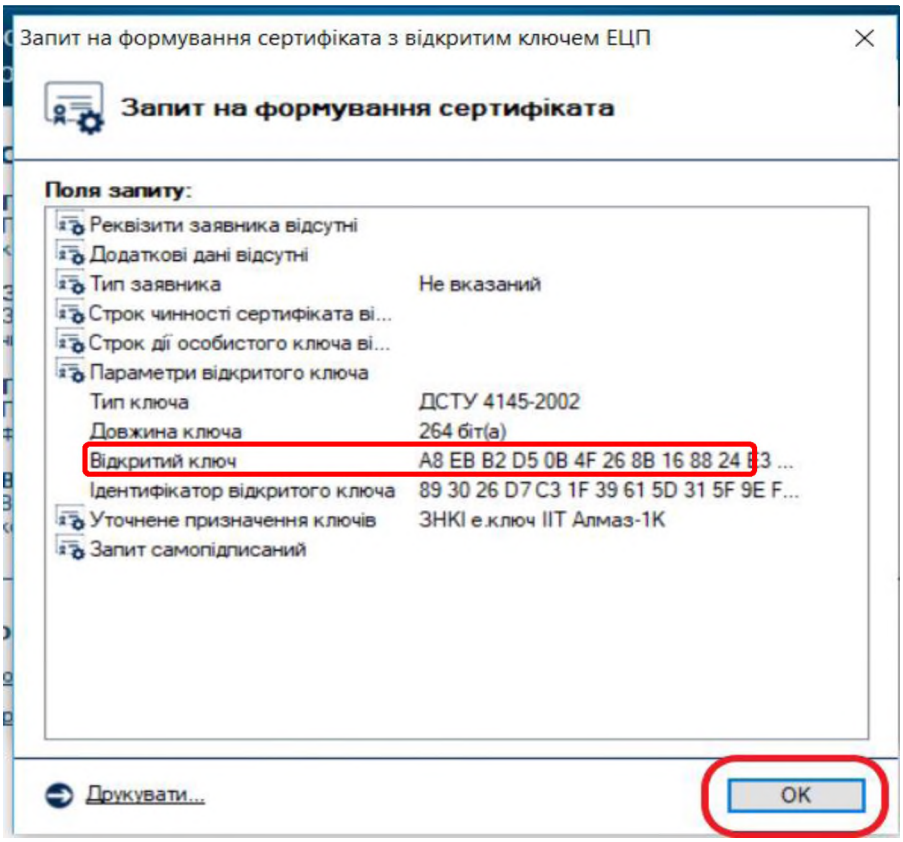


Рисунок 2.17

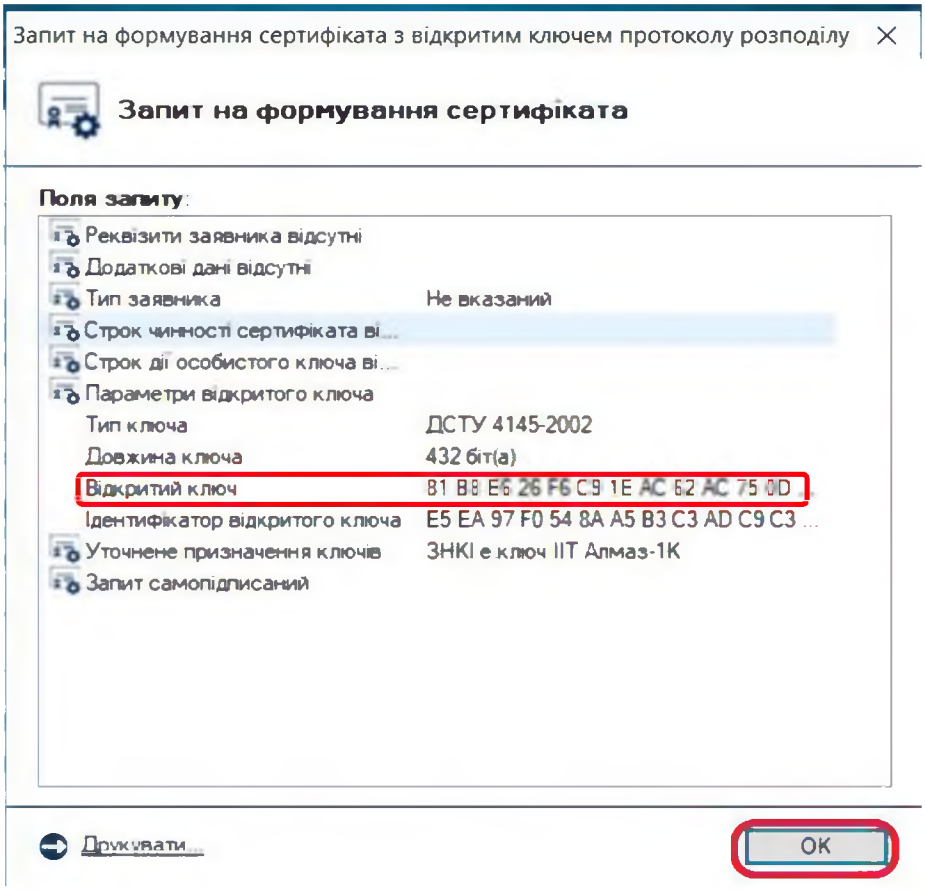


Рисунок 2.18

Рисунок 2.19

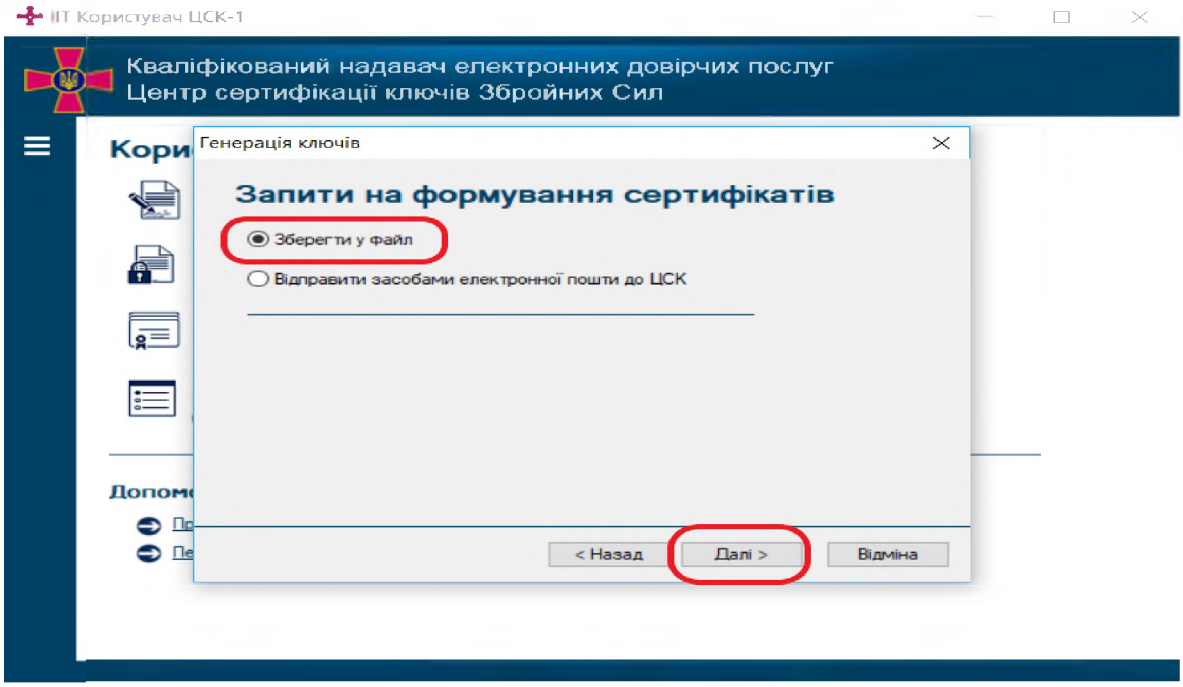


Рисунок 2.20

У наступному вікні (рис. 2.21) необхідно буде вказати ім'я файлу для запису запиту на формування сертифіката у файл. Запит повинен бути записаний на носій інформації чи на жорсткий диск. Після цього запит повинен бути переданий до КН або його ВПР для формування кваліфікованого сертифіката.

Увага! Для коректної ідентифікації запитів з відкритим ключем ЕП та протоколом розподілу ключів підписувача файл запиту на формування

кваліфікованого сертифіката відкритого ключа обов'язково зберігатись з ім'ям у наступному форматі:

"EU-ПІБ.p10", де: ПІБ – прізвище та ім'я по батькові;

"EU-КЕР- ПІБ.p10";

"EU-RSA- ПІБ.p10".

"EU- ", "EU-КЕР-", "EU-RSA-" та "*.p10"– унікальні ідентифікатори та розширення файлів запиту, що формується програмним забезпеченням за замовчуванням та повинно залишатись без змін.

Наприклад:

EU-Іванов І.І.p10, EU-КЕР-Іванов І.І.p10, EU-RSA-Іванов І.І.p10.

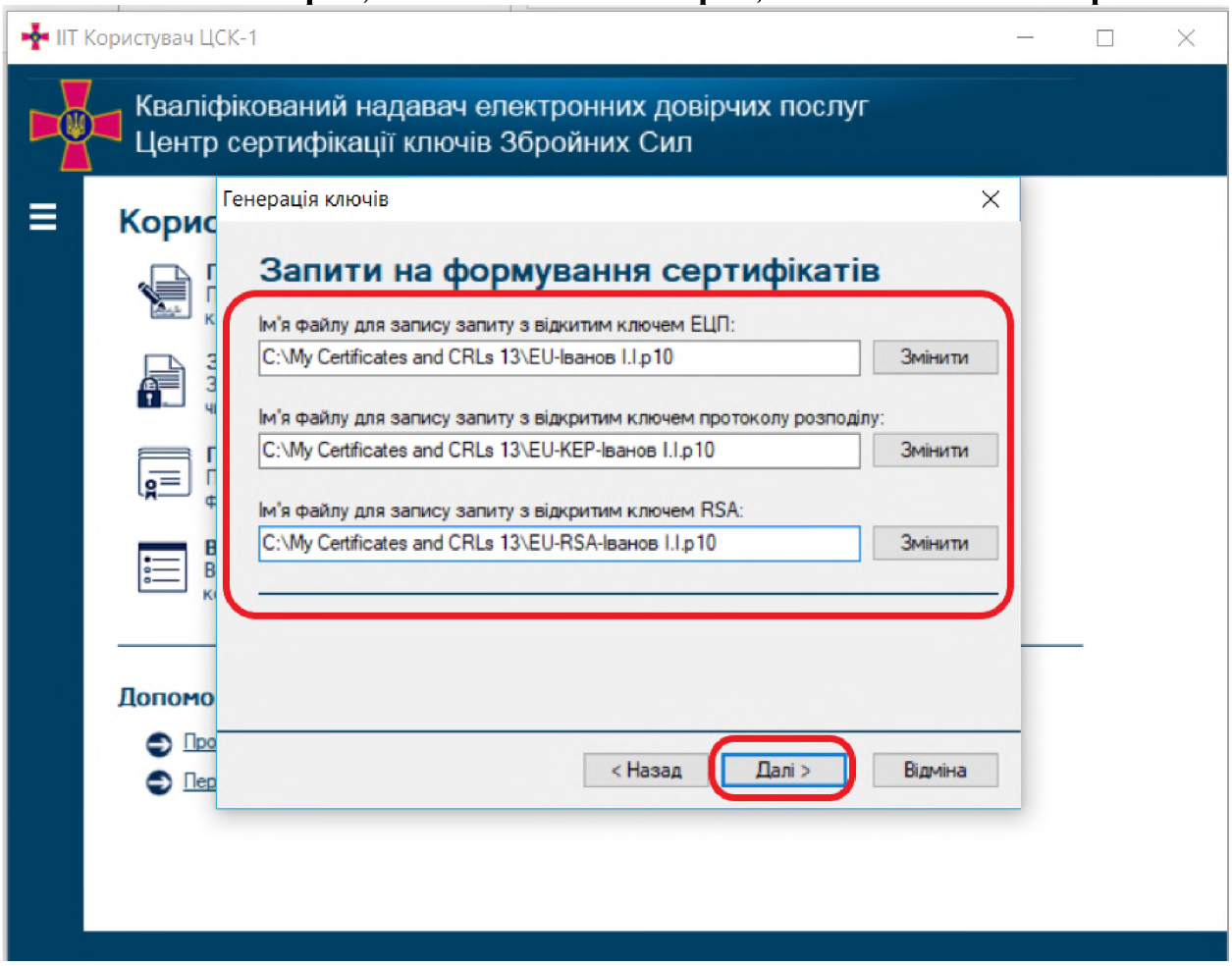


Рисунок 2.21

3.4. Додаткова генерація пари ключів для роботи за міжнародними алгоритмами та протоколами на вже існуючий ЗНОК з особистими ключами ЕП підписувача.

У разі необхідності додатково використовувати ключі за міжнародними алгоритмами та протоколами генерація пар ключів підписувачів здійснюється на ЗНОК на якому вже існують особисті ключі ЕП підписувача за державними алгоритмами та протоколами.

Щоб додатково згенерувати особистий ключ потрібно вказати параметри генерації ключів “для міжнародних алгоритмів та протоколів” та обрати необхідний алгоритм(рис. 2.22).

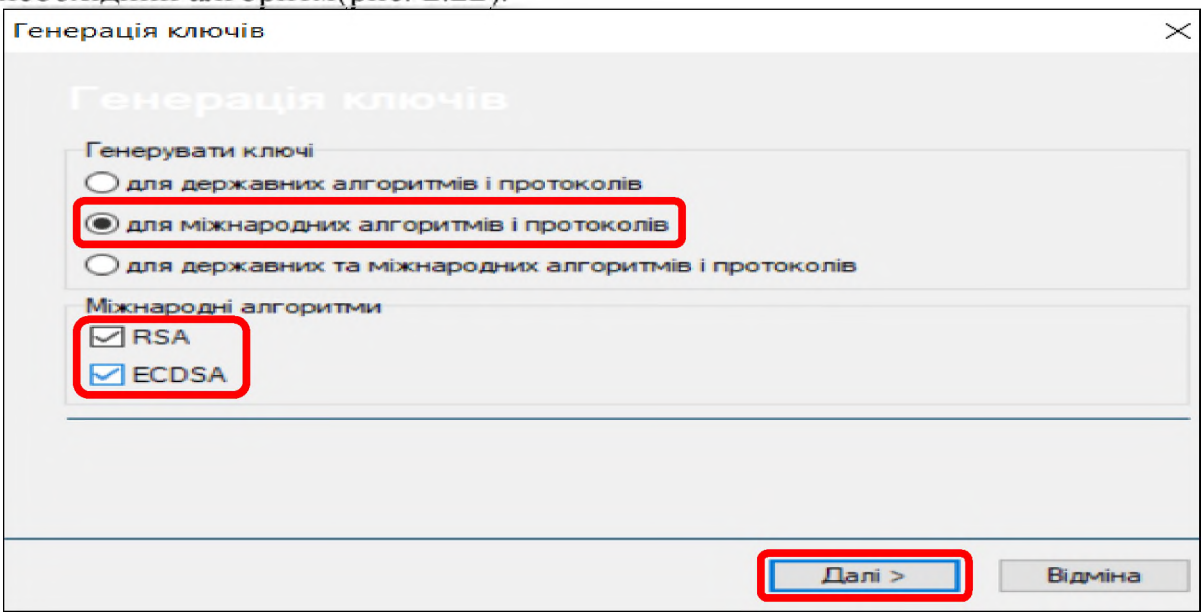


Рисунок 2.22

На наступній сторінці вибрати параметр відповідно до рисунку 2.23: тип криптографічних алгоритмів та протоколів: – RSA; ключі – базова (2048 біт з SHA-256). Для продовження генерації ключа необхідно натиснути кнопку “Далі”.

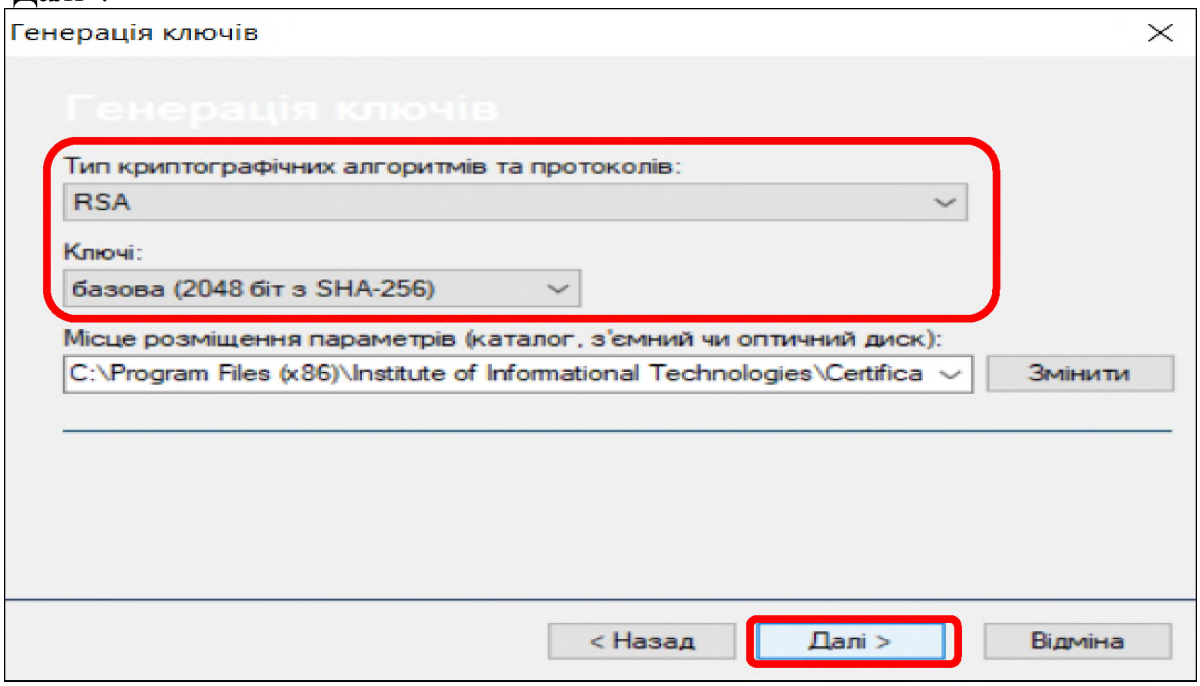


Рисунок 2.23

У випадку якщо також генерується за алгоритмом ECDSA, то необхідно обрати тип криптографічних алгоритмів та протоколів – ECDSA; ключі – базова (NIST P-256 256 біт з SHA-256) відповідно до рисунку 2.24. Для продовження генерації ключа необхідно натиснути кнопку “Далі”.

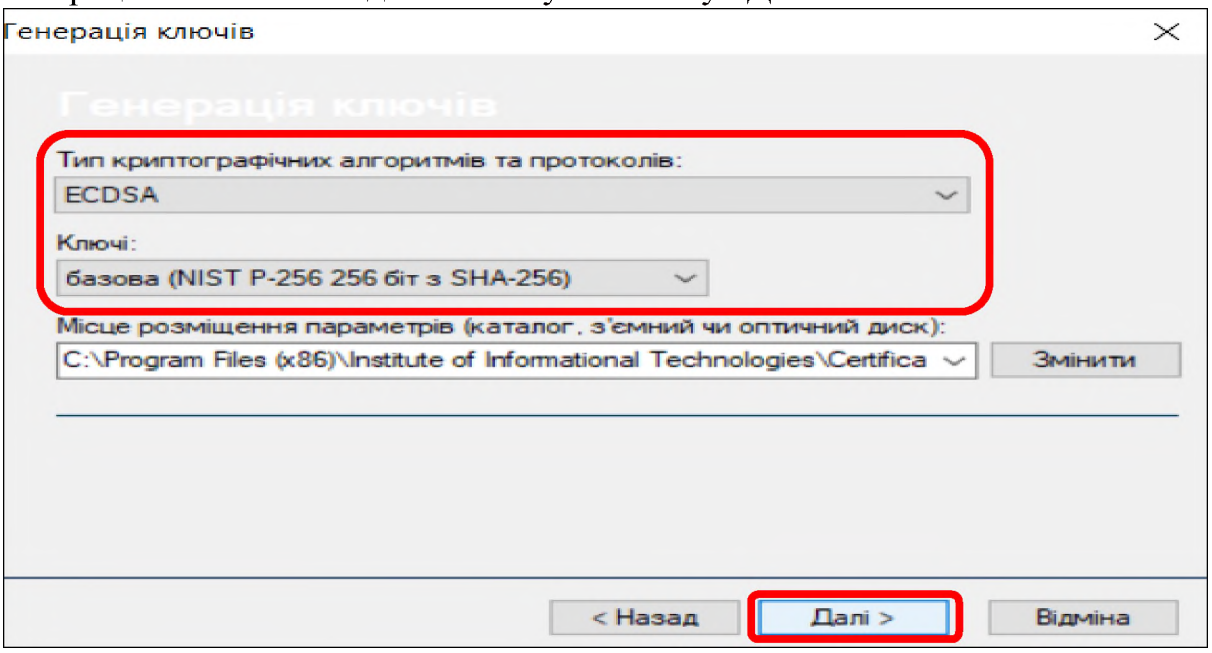


Рисунок 2.24

Далі необхідно встановити ЗНОК підписувача на якому вже є особисті ключі ЕП для додаткової генерації пари ключів за міжнародними алгоритмами та протоколами та на наступній сторінці майстра (рис. 2.25) вказати:

– тип ЗНОК;

– серійний номер ЗНОК;

– існуючий пароль доступу до ключового носія (пароль ЕП).

Заборонено попередньо форматувати ЗНОК. У іншому разі існуючий ключ буде знищено безповоротно.

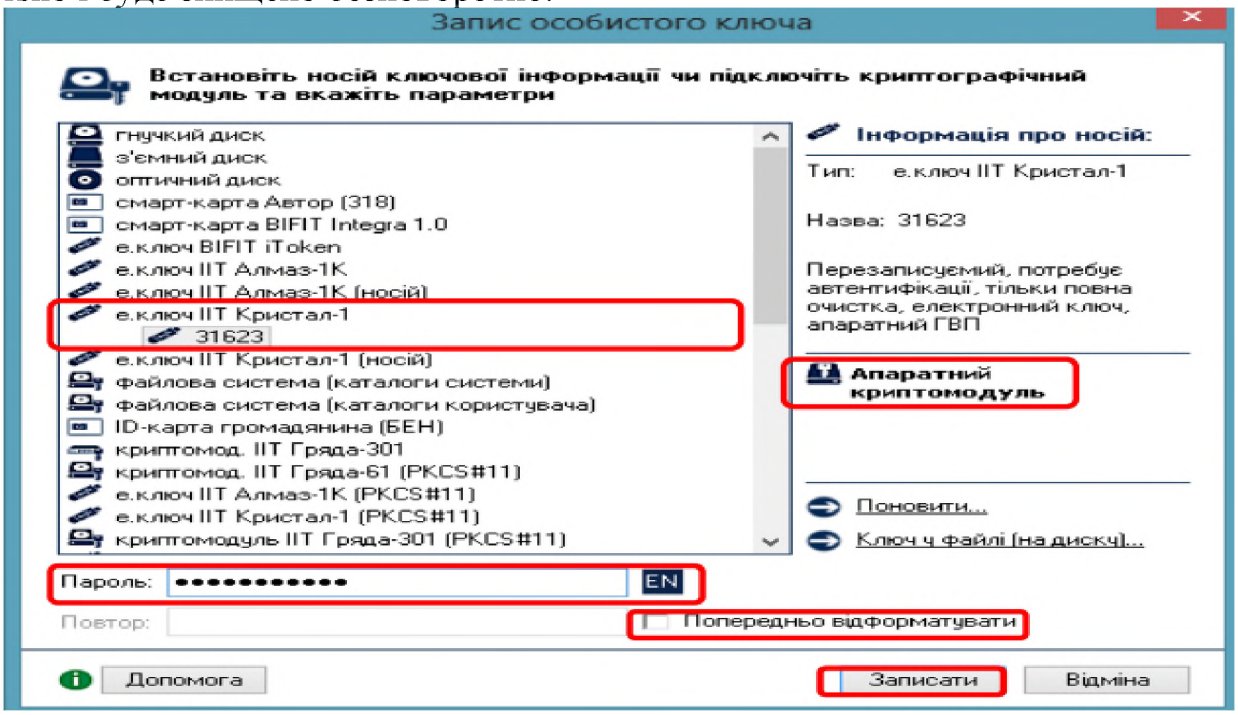


Рисунок 2.25

Після запису особистого ключа на ЗНОК, буде виведено вміст простого запиту на формування сертифікату з відкритим ключем ЕП для міжнародних алгоритмів та протоколів (рис. 2.26, рис. 2.27), після перевірки вмісту простого запиту необхідно натиснути “ОК”.

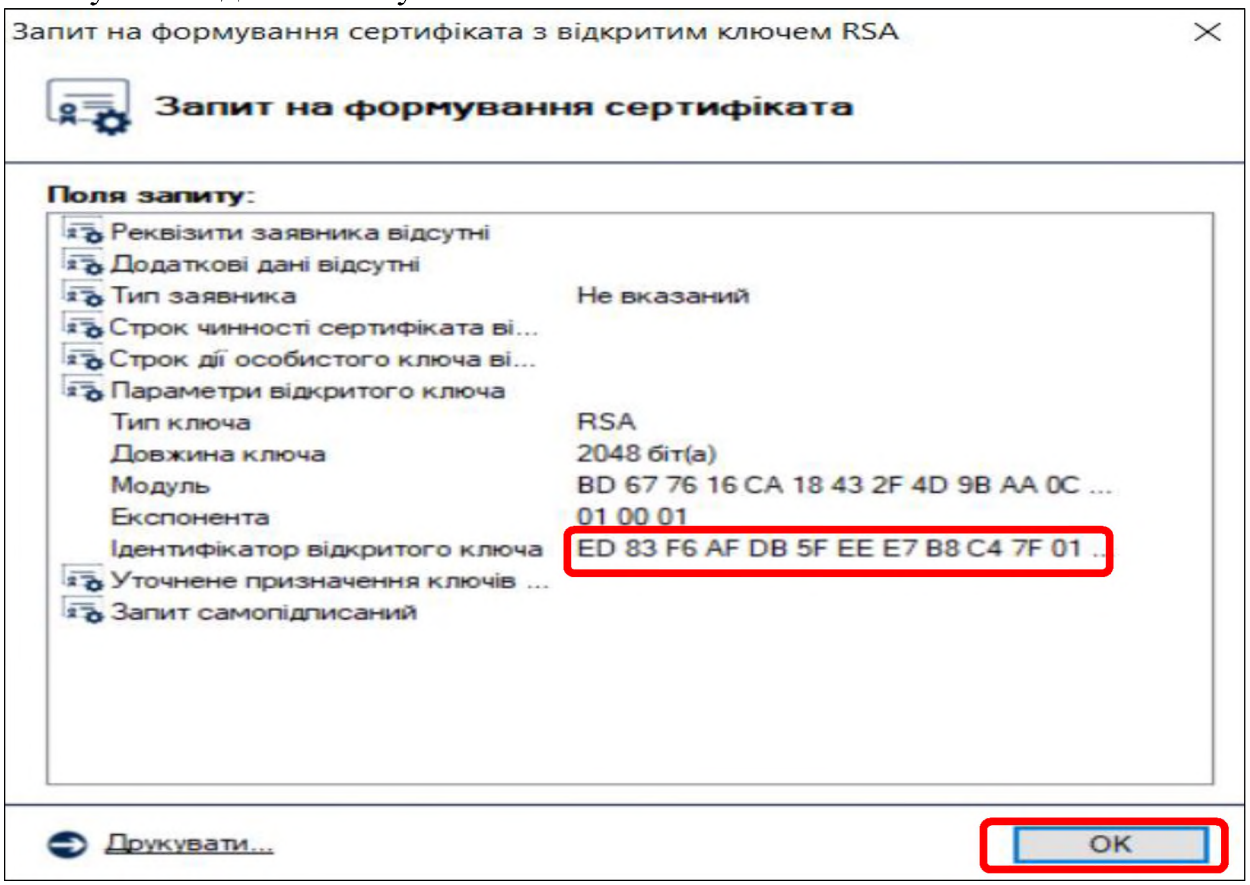


Рисунок 2.26

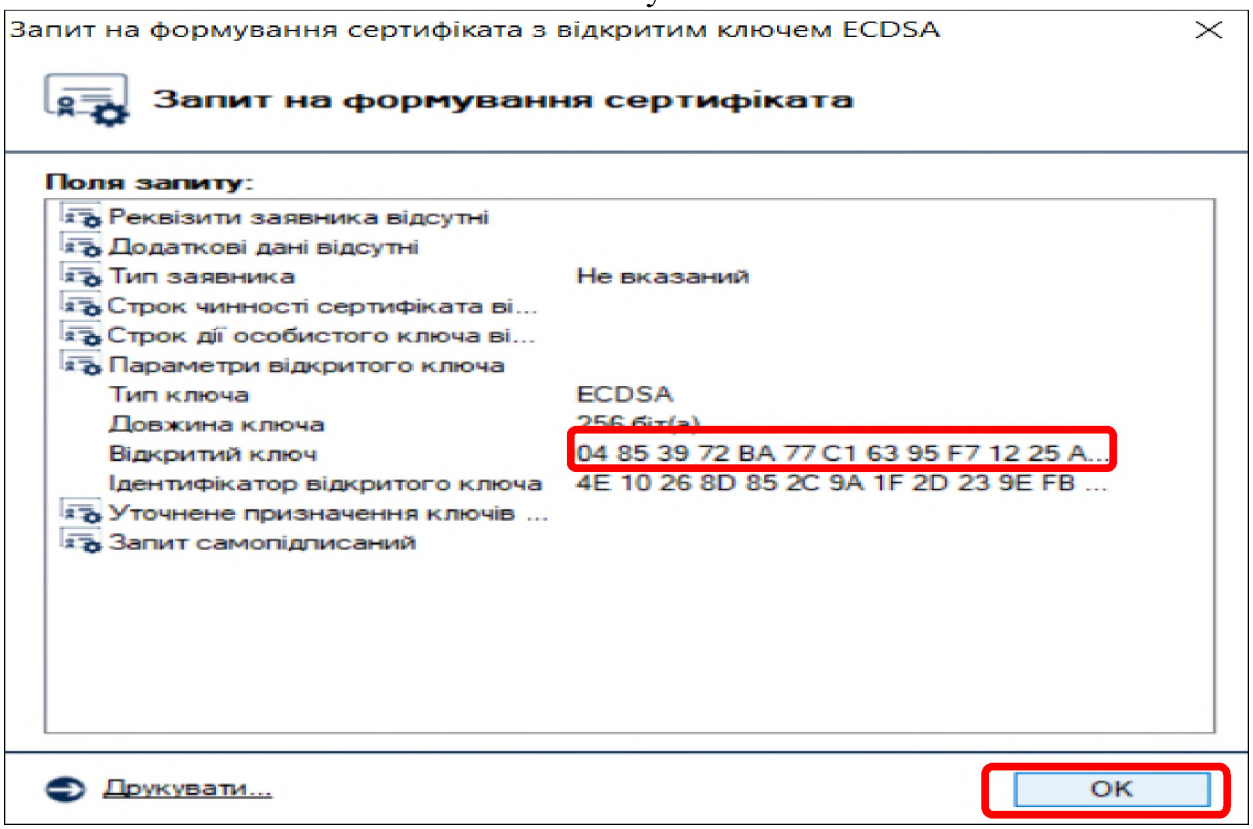


Рисунок 2.27

На наступній сторінці майстра (рис. 2.28) потрібно вказати спосіб збереження запиту на формування сертифіката, обираємо “Зберегти у файл”.

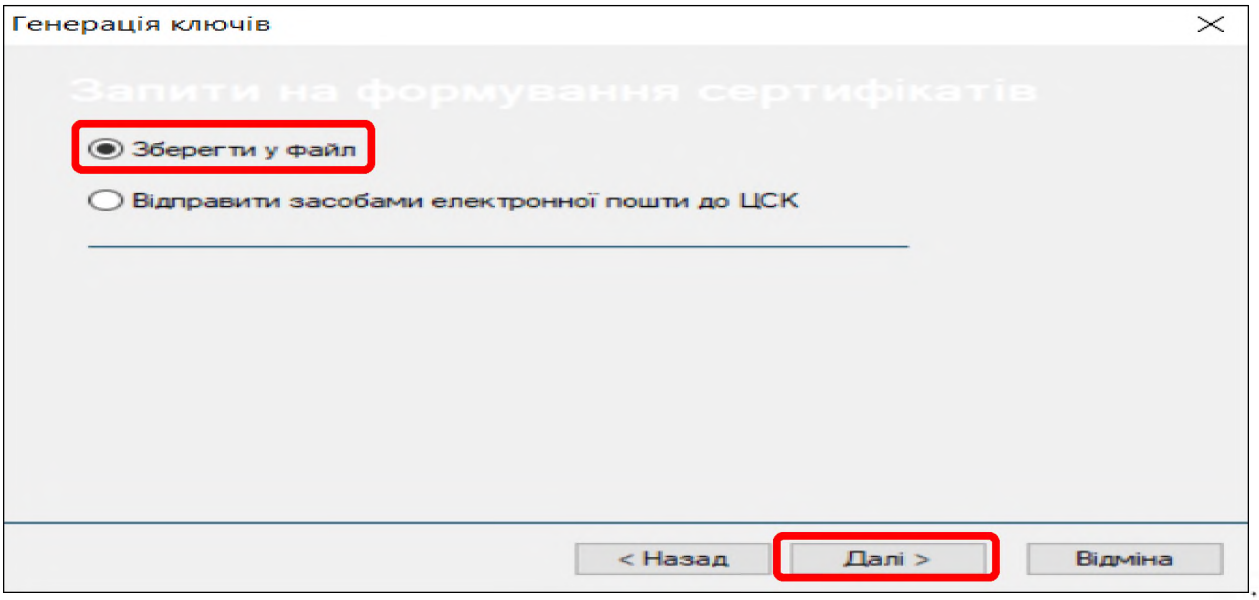


Рисунок 2.28

У наступному вікні (рис. 2.29) необхідно буде вказати ім’я файлу для запису запиту на формування сертифіката у файл. Запит повинен бути записаний на носій інформації чи на жорсткий диск. Після цього запит повинен бути переданий до КН або його ВПР для формування кваліфікованого сертифіката.

Увага! Для коректної ідентифікації запитів з відкритим ключем ЕП підписувача файл запиту на формування кваліфікованого сертифіката відкритого ключа обов’язково зберігатись з ім’ям у наступному форматі:

“EU-RSA- ПІБ.p10”, де: ПІБ – прізвище та ім’я по батькові ;

“EU-RSA-” та “*.p10”– унікальні ідентифікатор та розширення файлу запиту, що формується програмним забезпеченням за замовчуванням та повинно залишатись без змін.

Наприклад: EU-RSA-Іванов І.І.p10., EU-ECDSA-Іванов І.І.p10.

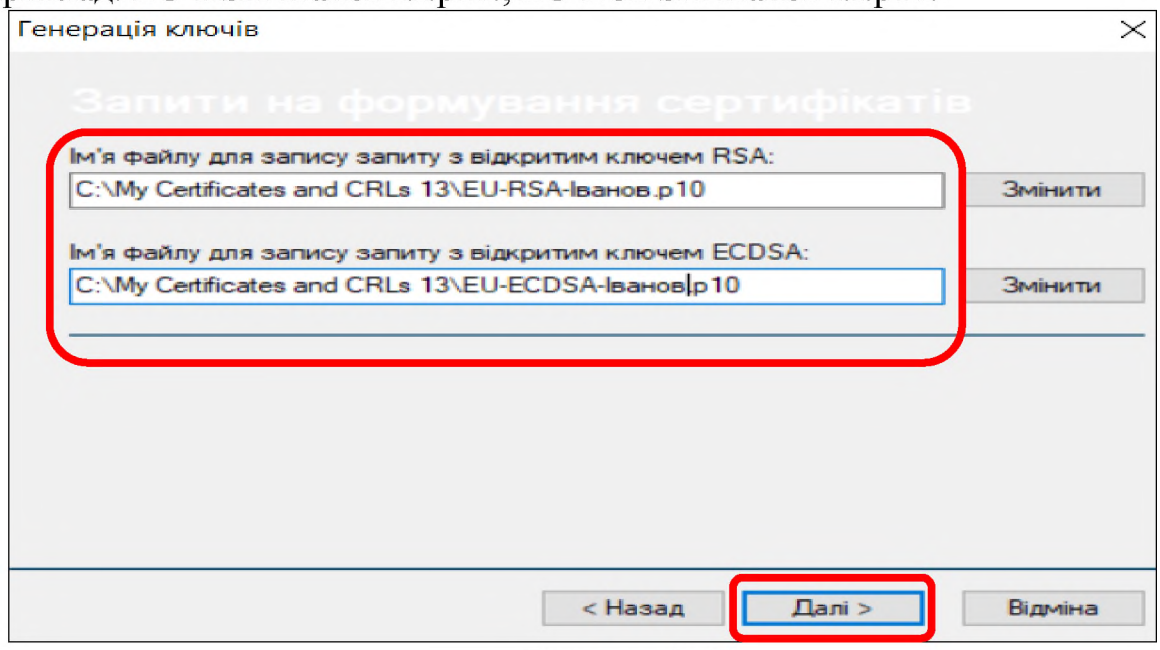


Рисунок 2.29

3.5. Генерація пари ключів електронної печатки на захищеному носії особистого ключа (ЗНОК).

Генерація пари ключів електронної печатки здійснюється створювачем електронної печатки (особою відповідальною за електронну печатку установи) **виключно** на ЗНОК в режимі “Апаратний криптомодуль”.

Щоб згенерувати пару ключів електронної печатки потрібно вказати параметри генерації ключів **“для державних алгоритмів та протоколів”** (рис. 2.30).

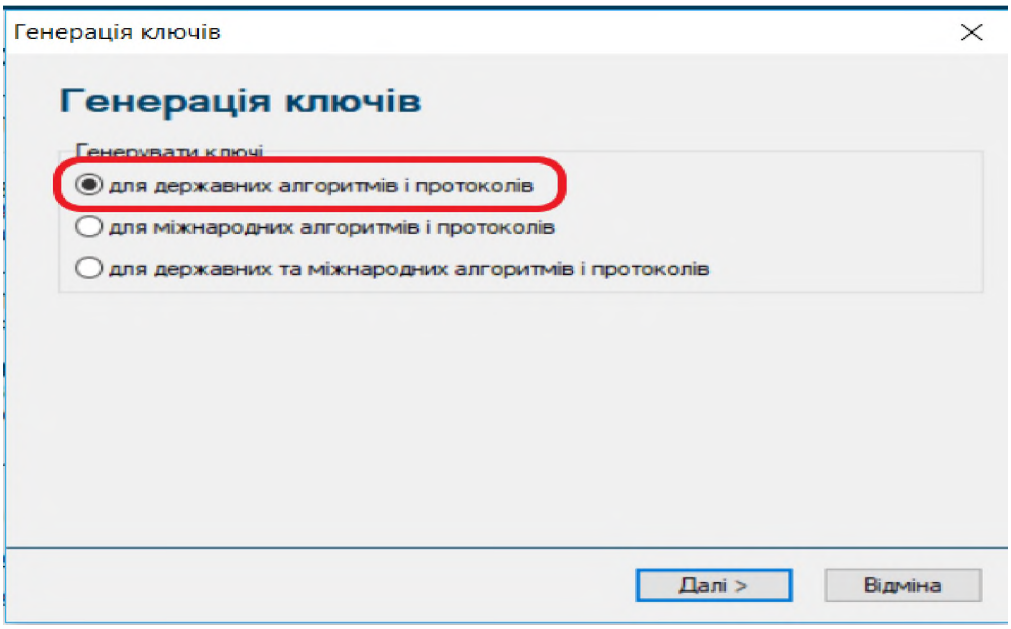


Рисунок 2.30

На наступній сторінці вказати параметри відповідно до (рис 2.30). Для продовження необхідно натиснути кнопку “Далі”.

Заборонено використовувати окремий ключ для протоколу розподілу та/або змінювати місце розміщення параметрів.

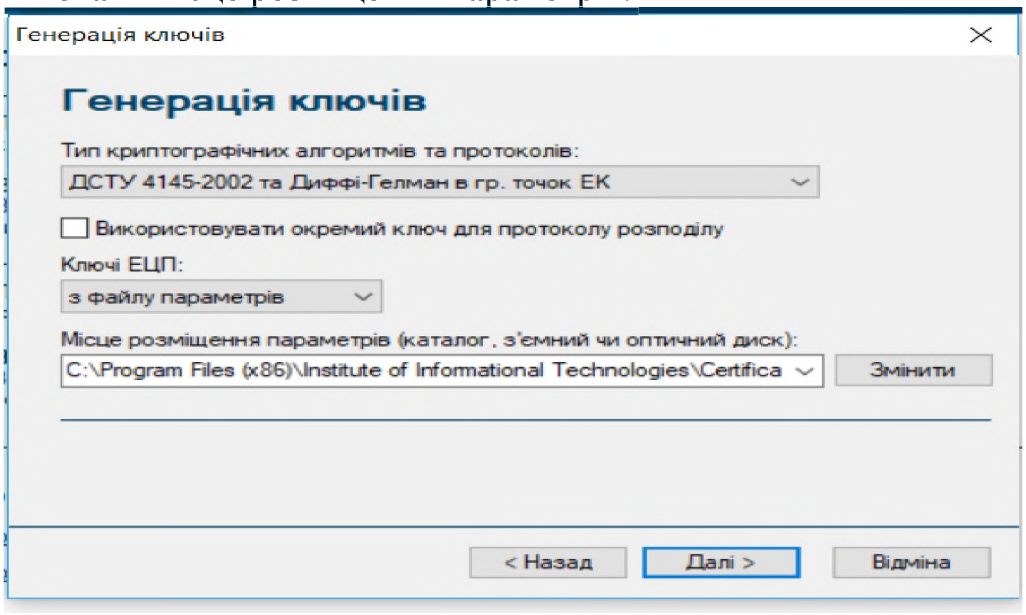


Рисунок 2.31

Далі необхідно встановити **ЗНОК** для запису особистого ключа електронної печатки у пристрій запису та на наступній сторінці майстра (рис. 2.32) вказати:

- тип ЗНОК;
- серійний номер ЗНОК;
- новий пароль доступу до ключового носія;
- попередньо від форматувати.

Генерація пари ключів електронної печатки здійснюється в режимі “Апаратний криптомодуль”.

Заборонено вибирати для генерації ключів електронної печатки типи носія ключової інформації “гнучкий диск”, “з’ємний диск”, “оптичний диск”, “файлова система” або тип носія з приміткою “(носій)”.

Пароль захисту особистого ключа повинен відповідати наступним вимогам:

- довжина - не менше 8 символів;
- не повинен містити однакові символи;
- не повинен містити підряд більше ніж 2 символи з розкладинки клавіатури;
- дозволені символи - 'a-z', 'A-Z', '0-9', '+', '-'.

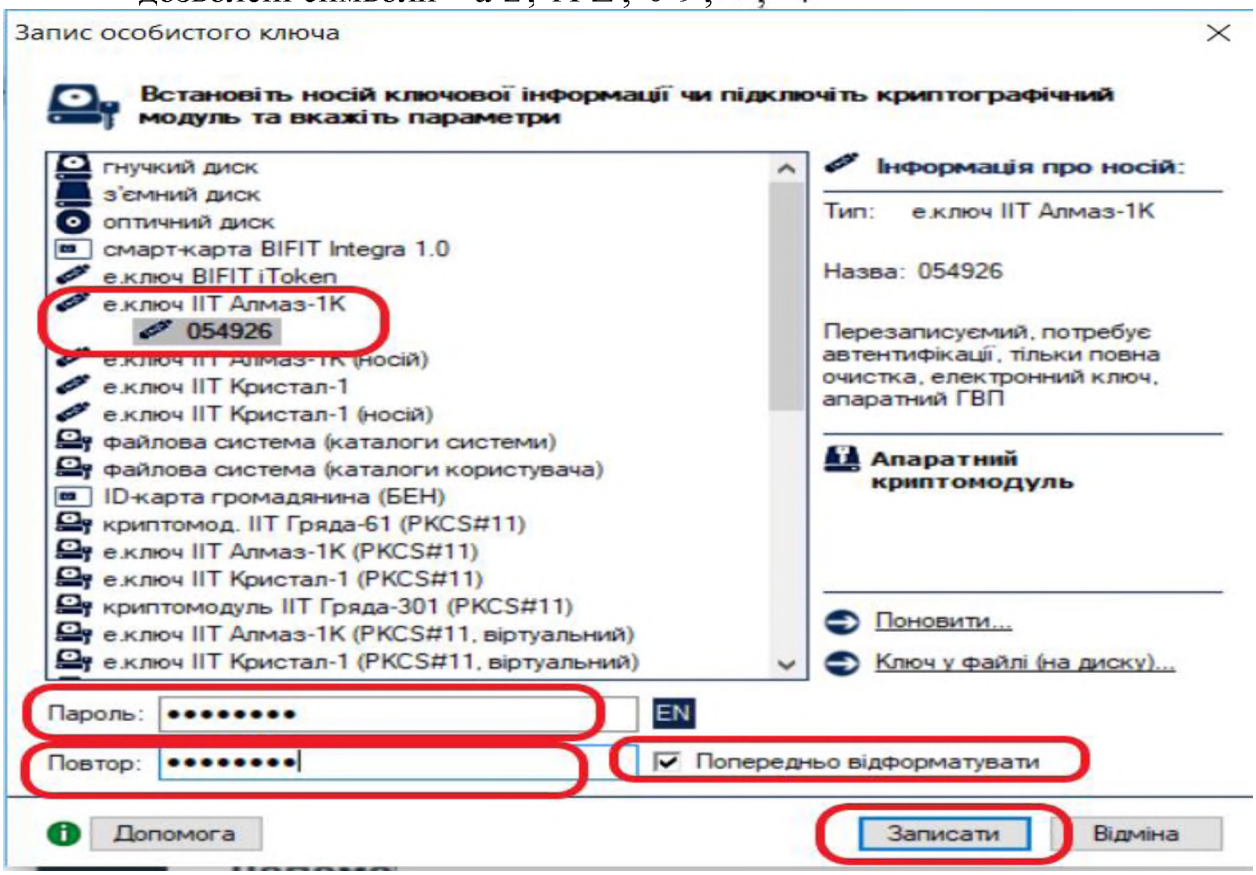


Рисунок 2.32

Після запису особистого ключа на ЗНОК, буде виведено вміст простого запиту на формування сертифікату з відкритим ключем ЕП для державних алгоритмів та протоколів (рис. 2.32), потрібно переконатись що особистий ключ згенеровано на ЗНОК, після перевірки вмісту простого запиту необхідно натиснути “ОК”. На наступній сторінці майстра (рис. 2.34) потрібно вказати

спосіб збереження запиту на формування сертифіката, обираємо **Зберегти у файл**.

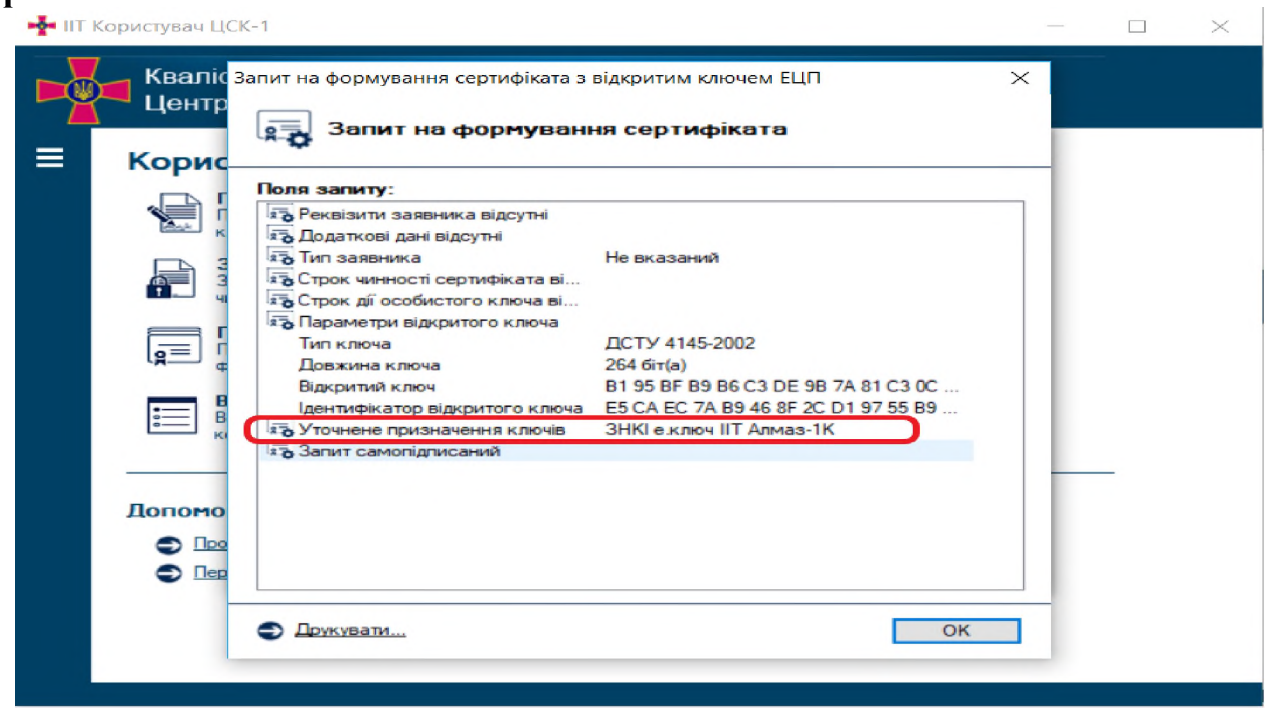


Рисунок 2.33

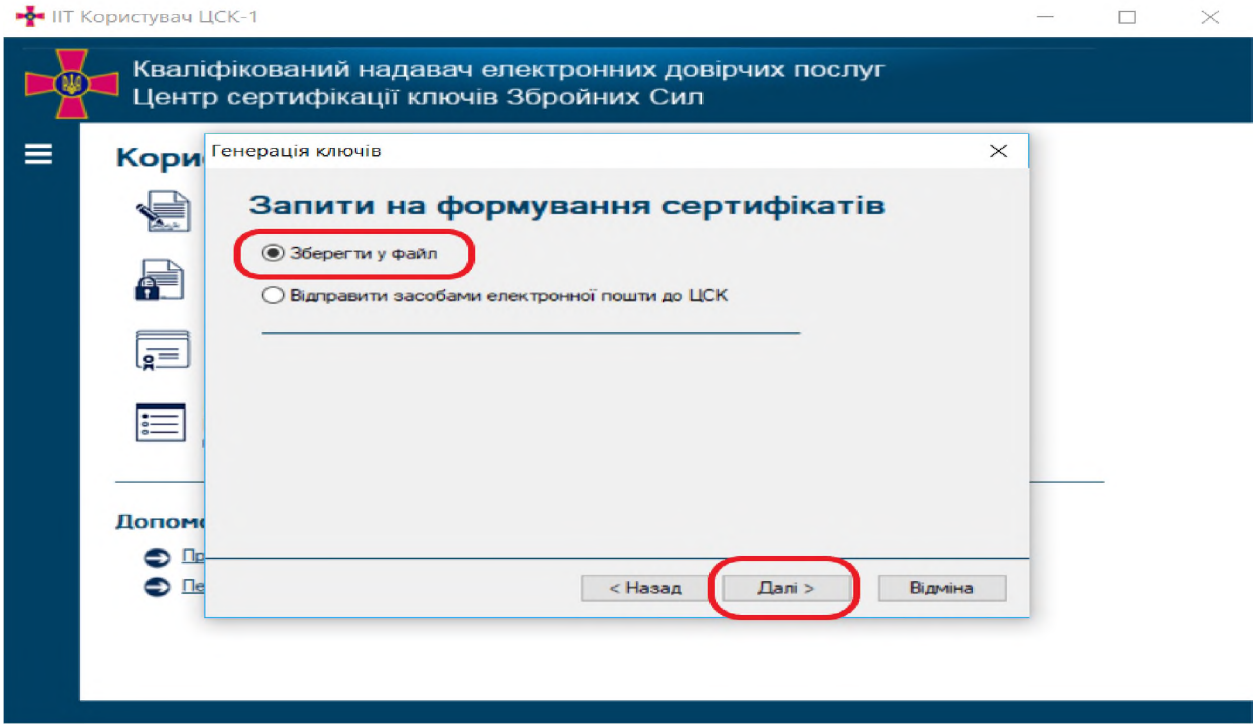


Рисунок 2.33

У наступному вікні (рис. 2.35) необхідно буде вказати ім’я файлу для запису запиту на формування сертифіката у файл. Запит повинен бути записаний на носій інформації чи на жорсткий диск. Після цього запит повинен бути переданий до КН або його ВПР для формування кваліфікованого сертифіката.

Увага! Для коректної ідентифікації запитів з відкритим ключем електронної печатки підписувача файл запиту на формування кваліфікованого сертифіката відкритого ключа обов’язково зберігатись з ім’ям у форматі **“EU-інд.p10”**, де:

інд – короткий ідентифікатор печатки або ПІБ створювача електронної печатки;

“EU” та “.p10”– ідентифікатор та розширення файлу запиту, що формується програмним забезпеченням за замовчуванням та повинно залишатись без змін.

Наприклад: **EU- печатка №1 А0000.p10.**

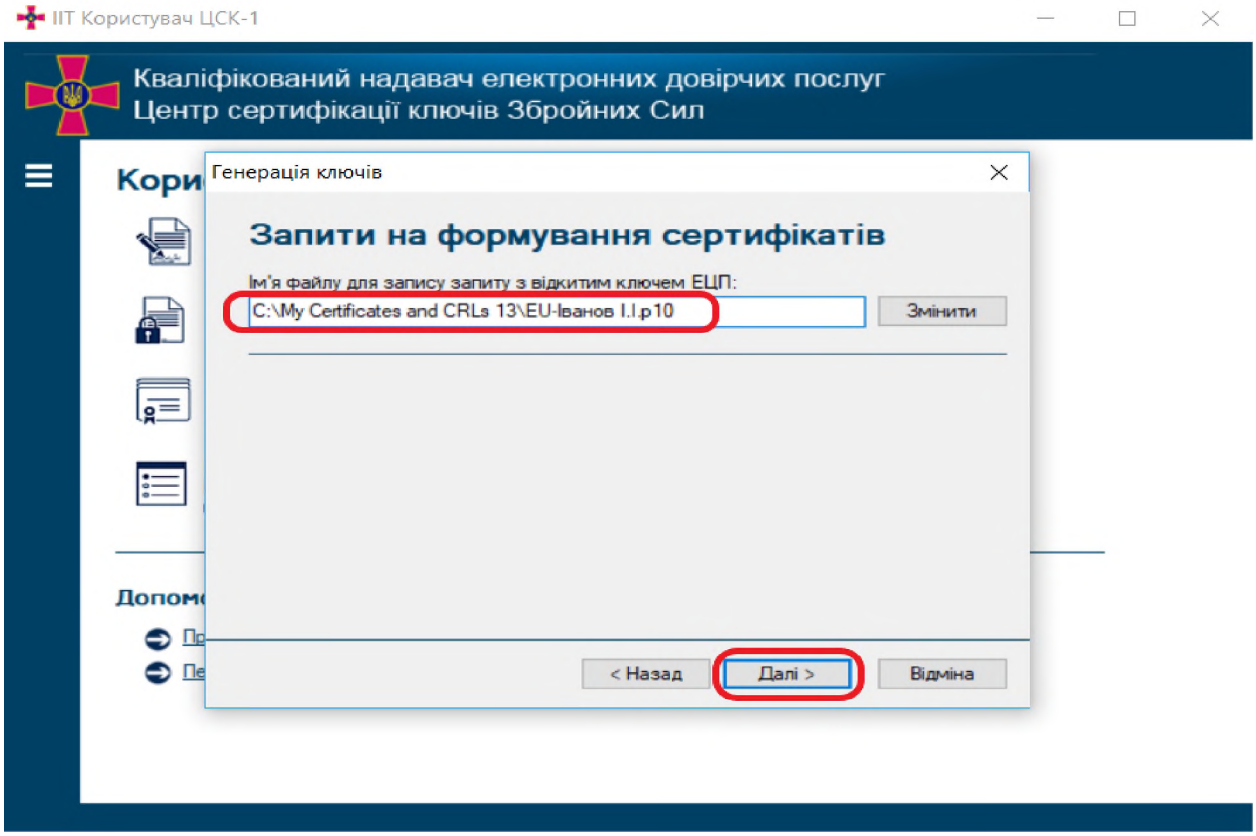


Рисунок 2.35

4.ЗАВАНТАЖЕННЯ КВАЛІФІКОВАНОГО СЕРТИФІКАТУ ВІДКРИТОГО КЛЮЧА.

Щоб завантажити кваліфікований сертифікат відкритого ключа через ПЗ необхідно обрати підпункт “Отримати з ЦСК…” в пункті меню “Сертифікати та СВС” (рис. 2.36).

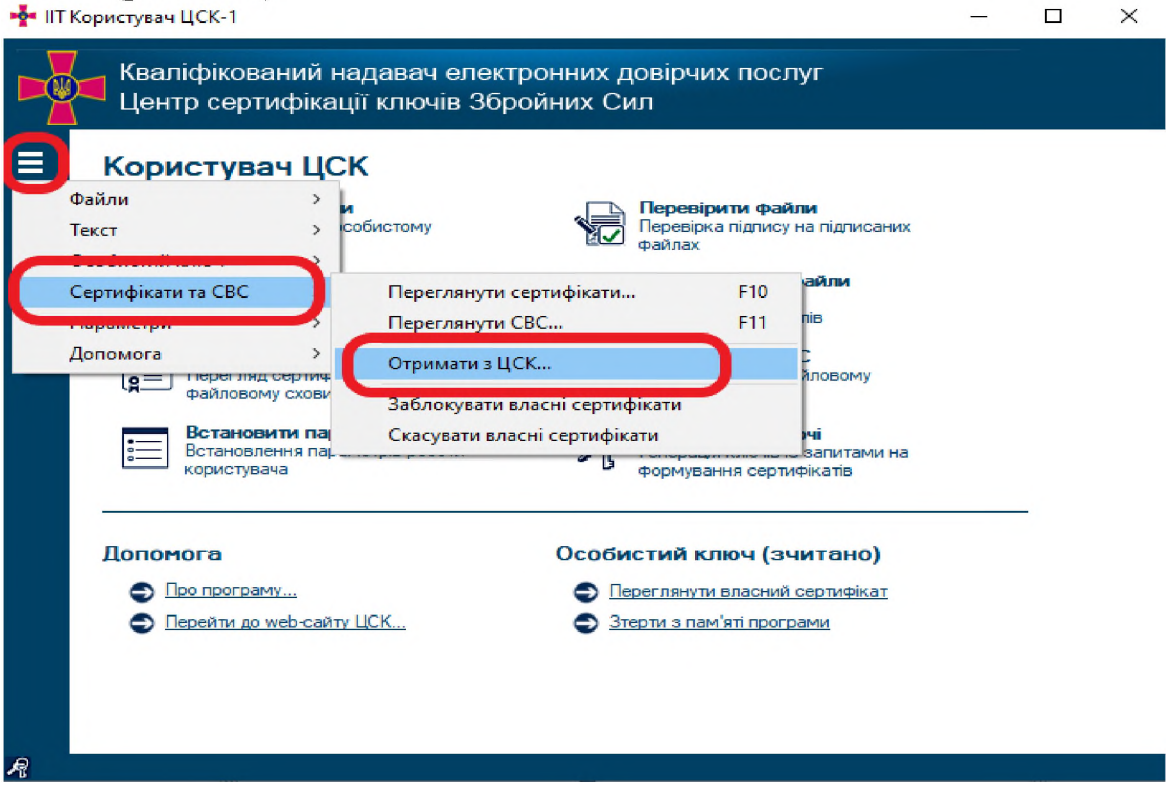


Рисунок 2.36

Для підтвердження отримання набору сертифікатів за особистим ключем чи власним сертифікатом з ЦСК натиснути кнопку “Да” (рис. 2.37).

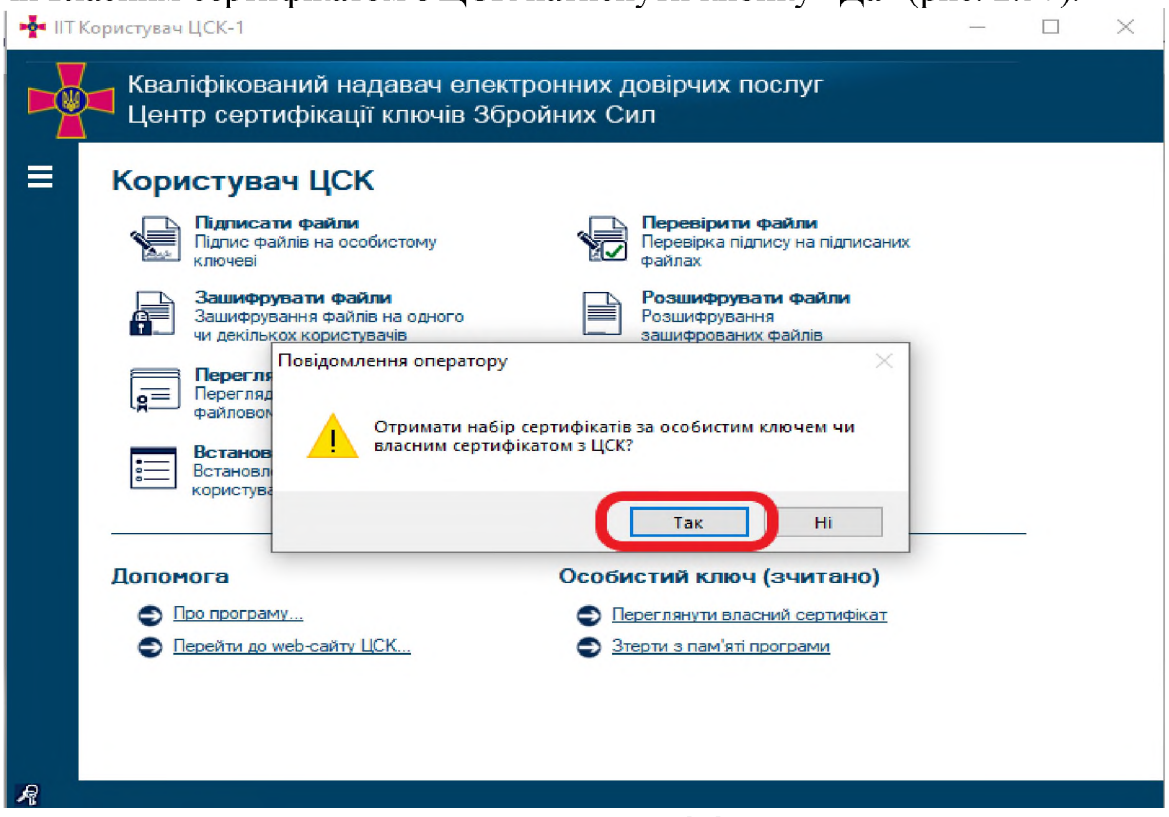


Рисунок 2.37

На наступній сторінці майстра Вам необхідно буде вибрати ЗНОК на який записаний особистий ключ КЕП та ввести пароль доступу до нього та зчитати його (рис. 2.38).

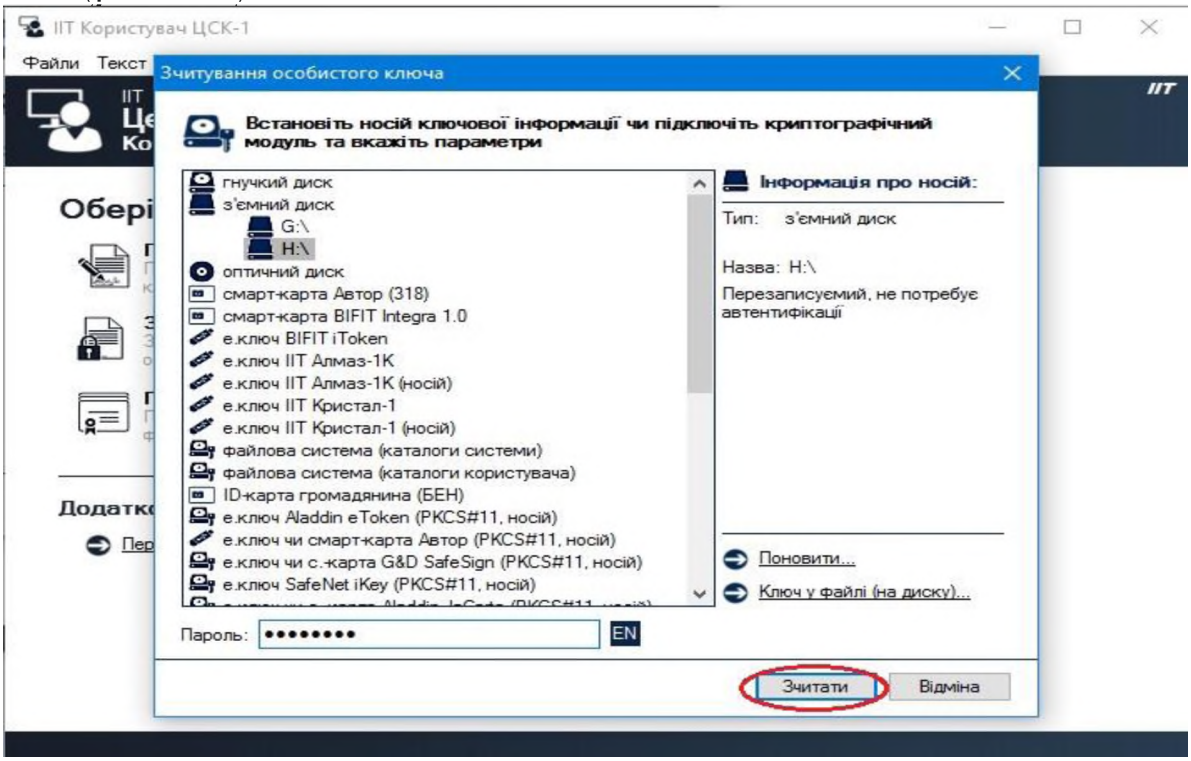


Рисунок 2.38

На наступній сторінці майстра Вам необхідно буде натиснути кнопку “Да” для інсталювання їх у файлове сховище сертифікатів (рис. 2.39).

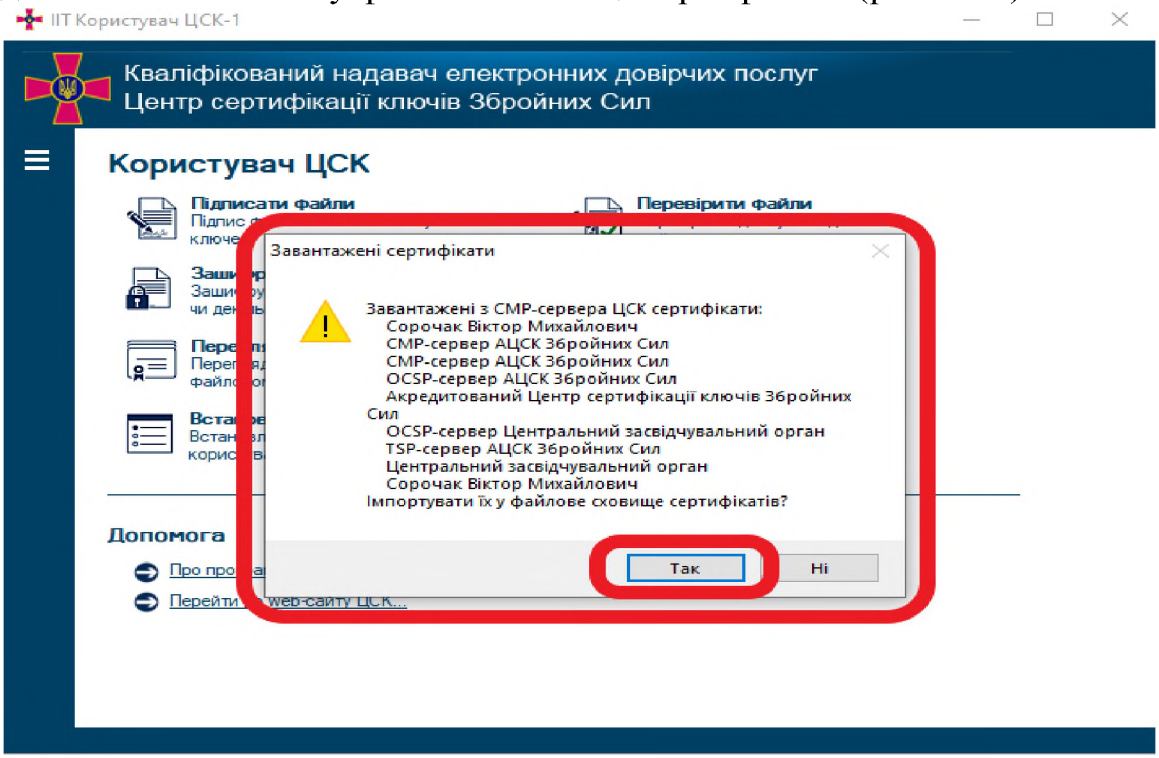


Рисунок 2.39

5. ЗЧИТУВАННЯ ОСОБИСТОГО КЛЮЧА

Зчитування особистого ключа може бути виконано шляхом вибору підпункту “Зчитати” в пункті меню “Особистий ключ” або шляхом натискання комбінації клавіш **Ctrl+K** (рис. 2.40).

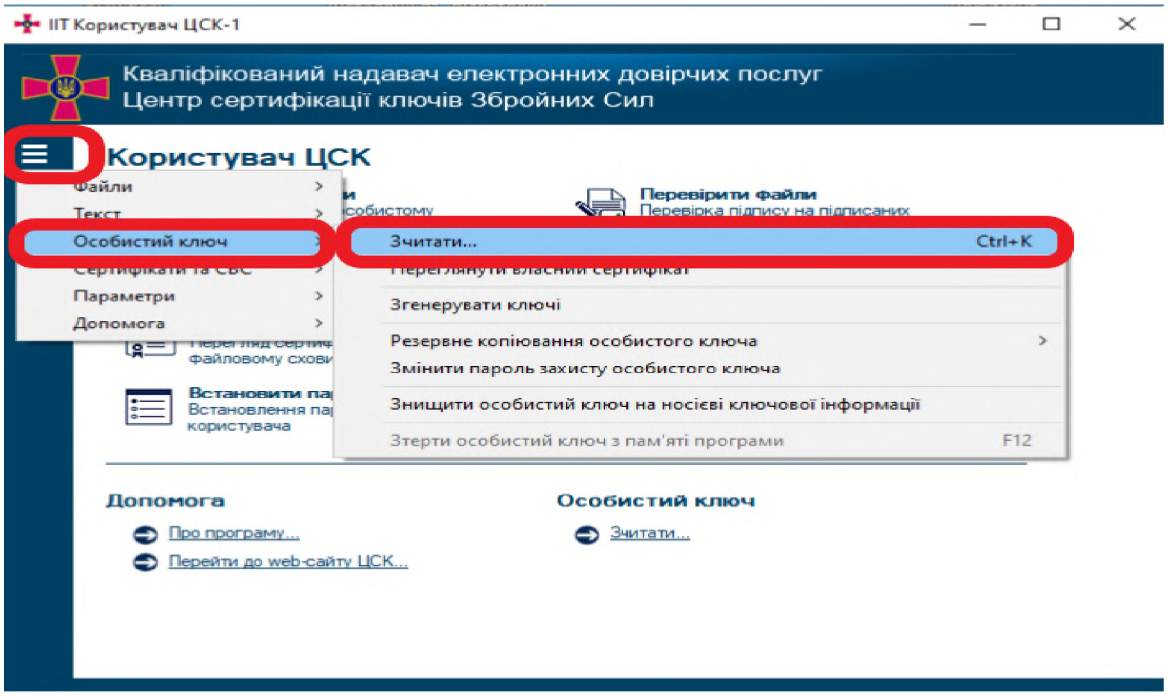


Рисунок 2.40

Після появи захищеного робочого столу (рис. 2.41), необхідно обрати з’ємний ЗНОК, ввести пароль захисту особистого ключа та натиснути кнопку “Зчитати”.

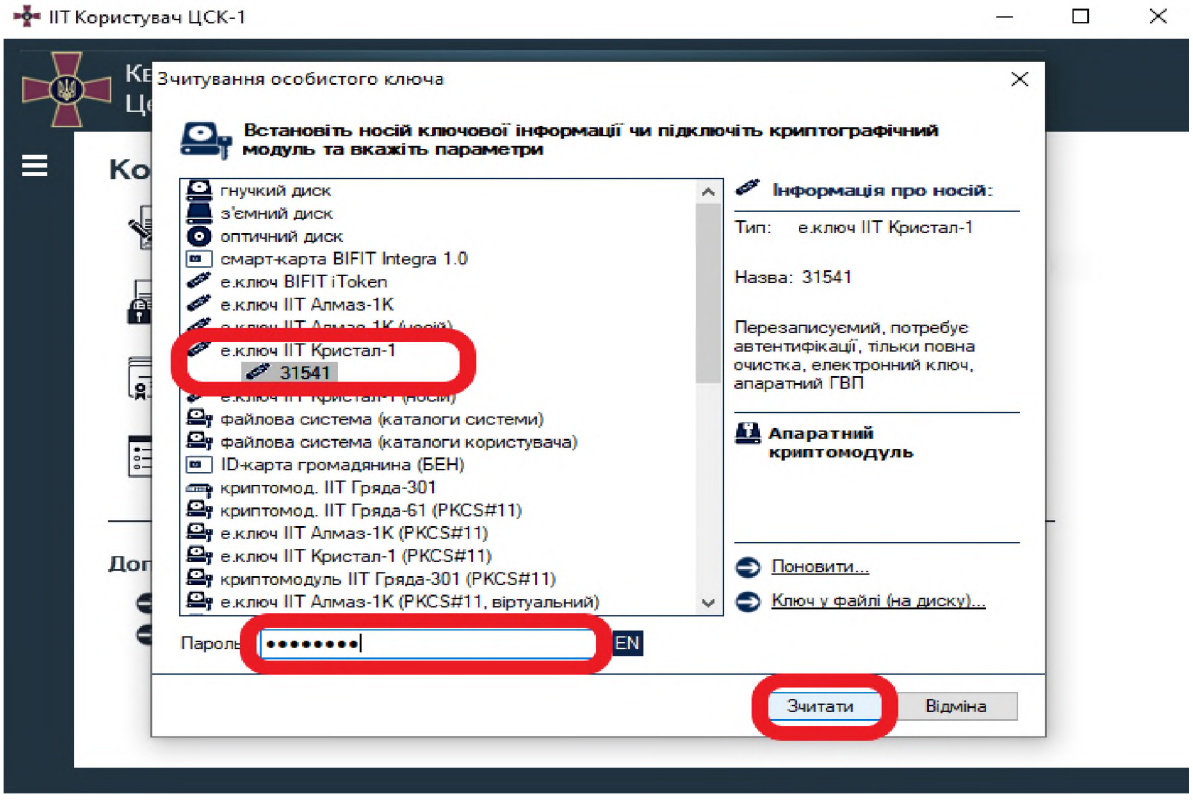


Рисунок 2.41

Інформація про те, що особистий ключ зчитаний та знаходиться в пам’яті ПК відображається у панелі стану вікна (рис. 2.42).

Рисунок 2.42

6. ЗМІНА ПАРОЛЮ ЗАХИСТУ ОСОБИСТОГО КЛЮЧА

Для зміни паролю захисту особистого ключа необхідно обрати підпункт “Змінити пароль захисту особистого ключа” у пункті меню “Особистий ключ” (рис. 2.43).

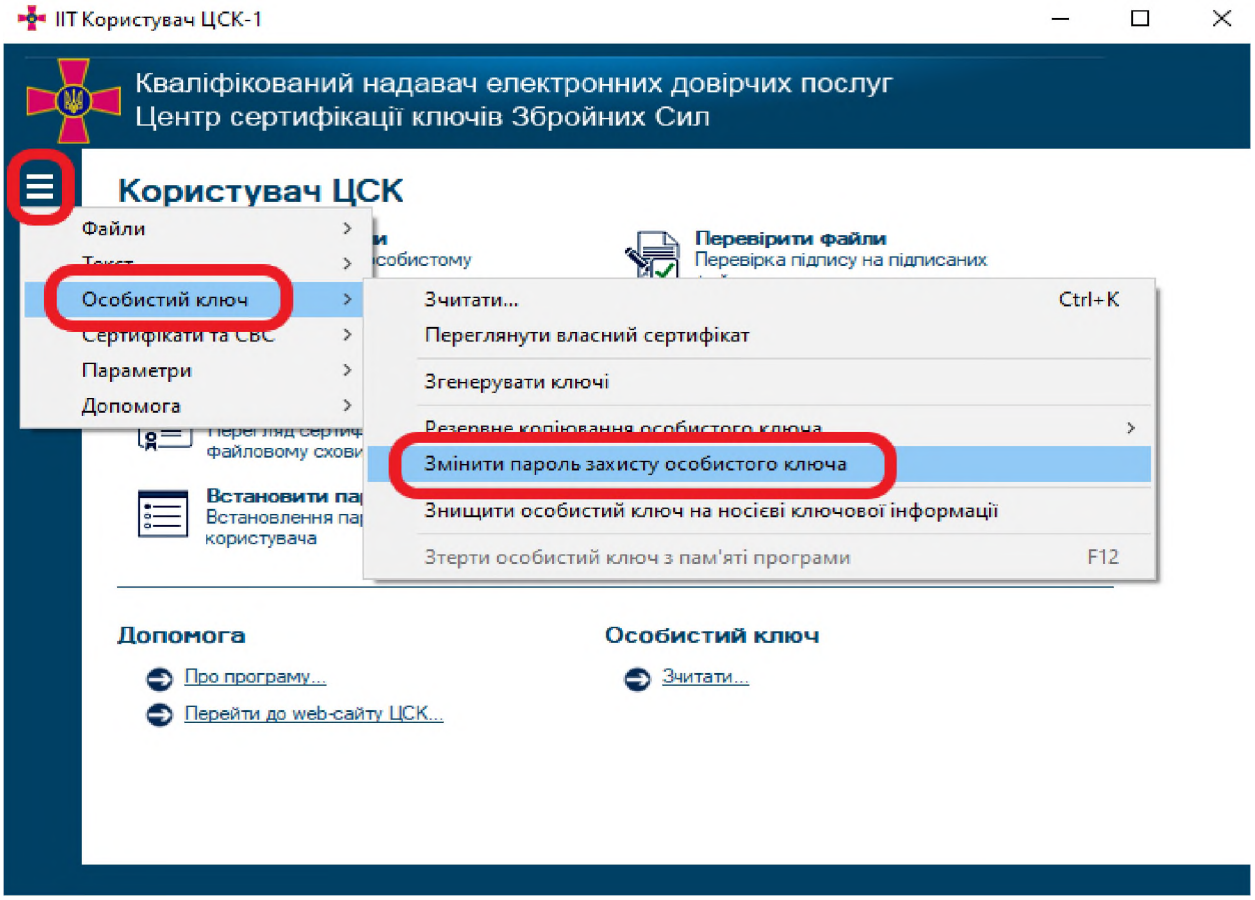


Рисунок 2.43

Далі необхідно встановити ЗНОК та на наступній сторінці майстра (рис. 2.44) вказати:

– тип ЗНОК;
– серійний номер ЗНОК;
– пароль захисту особистого ключа;
– новий пароль захисту особистого ключа (з підтвердженням).

Новий пароль повинен відповідати наступним вимогам:

– довжина – не менше 8 символів;
– не повинен містити однакові символи;
– не повинен містити підряд більше ніж 2 символи з розкладинки клавіатури;
– дозволені символи - 'a-z', 'A-Z', '0-9', '+', '-'.

Примітка. Такі вимоги носять рекомендаційний характер.

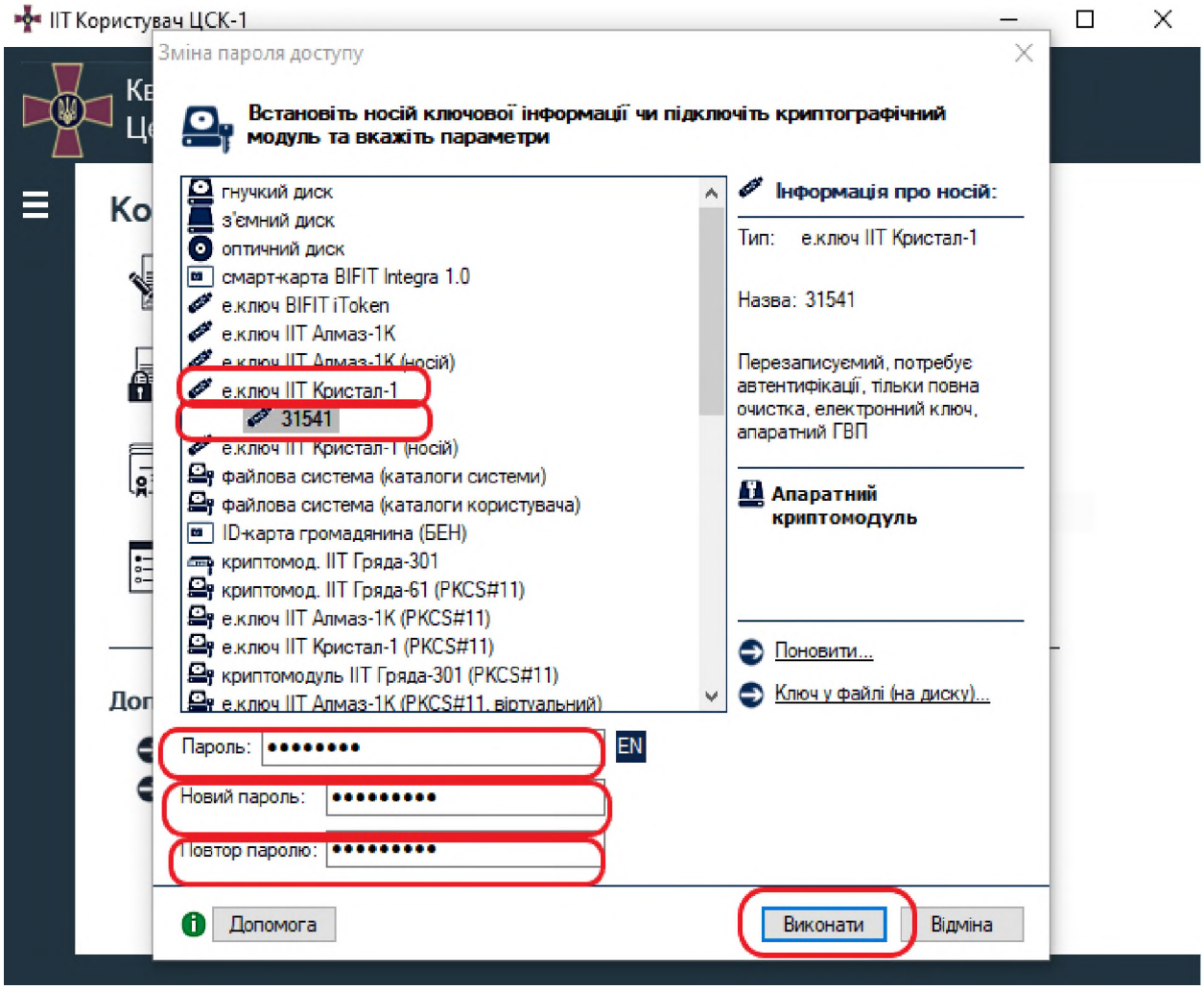

ІІТ Користувач ЦСК-1
Зміна пароля доступу
Встановіть носій ключової інформації чи підключіть криптографічний модуль та вкажіть параметри
гнучкий диск
з'ємний диск
оптичний диск
смарт-карта BIFIT Integra 1.0
е.ключ BIFIT iToken
е.ключ ІІТ Алмаз-1К
е.ключ ІІТ Кристал-1
31541
е.ключ ІІТ Кристал-1 (носій)
файлова система (каталоги системи)
файлова система (каталоги користувача)
ID-карта громадянина (БЕН)
криптомод. ІІТ Гряда-301
криптомод. ІІТ Гряда-61 (PKCS#11)
е.ключ ІІТ Алмаз-1К (PKCS#11)
е.ключ ІІТ Кристал-1 (PKCS#11)
криптомодуль ІІТ Гряда-301 (PKCS#11)
Інформація про носій:
Тип: е.ключ ІІТ Кристал-1
Назва: 31541
Перезаписуємий, потребує автентифікації, тільки повна очистка, електронний ключ, апаратний ГВП
Апаратний криптомодуль
Поновити...
Ключ у файлі (на диску)...
Пароль:
EN
Новий пароль:
Повтор паролю:
Допомога
Виконати
Відміна

Рисунок 2.44

7. БЛОКУВАННЯ КВАЛІФІКОВАНОГО СЕРТИФІКАТА ВІДКРИТОГО КЛЮЧА

Під блокуванням кваліфікованого сертифіката розуміється тимчасове зупинення чинності кваліфікованого сертифіката.

Увага! Для здійснення блокування кваліфікованого сертифікату необхідно підключення робочого місця на якому установлено ПЗ до мережі ІСД “Інтернет” або АСУ ЗСУ “Дніпро”.

Після блокування кваліфікованого сертифіката, підписувач може протягом тридцяти календарних днів поновити строк чинності кваліфікованого сертифіката. Блокований кваліфікований сертифікат буде автоматично скасований КН, якщо протягом зазначеного строку підписувач не поновить його чинність.

Для блокування кваліфікованого сертифіката у ПЗ необхідно обрати підпункт “Заблокувати власний сертифікат” в пункті меню “Сертифікати та СВС” (рис. 2.45).

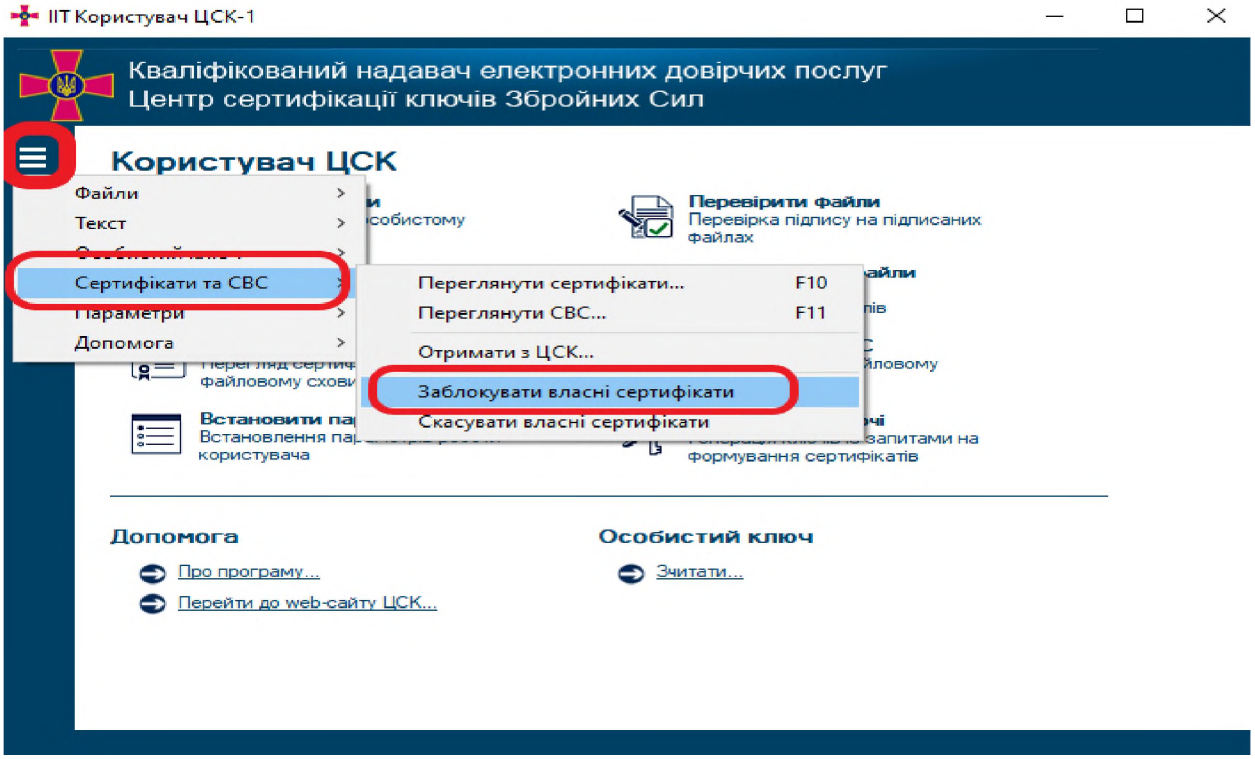


Рисунок 2.45

Після появи захищеного робочого столу необхідно обрати ЗНОК та ввести пароль захисту особистого ключа (рис. 2.46).

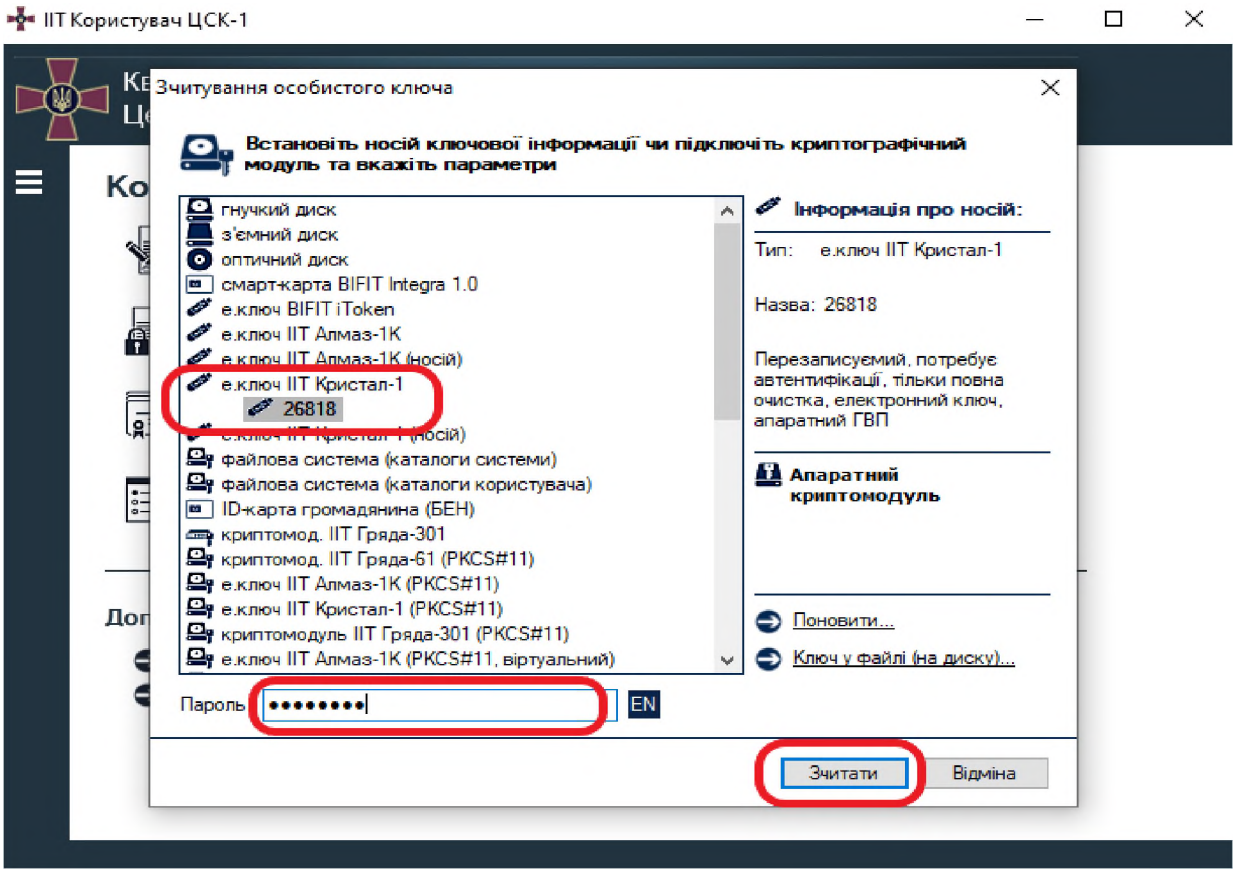


Рисунок 2.46

Далі з'являється повідомлення щодо підтвердження блокування кваліфікованого сертифіката, для підтвердження блокування натискаємо "Так" (рис. 2.47).

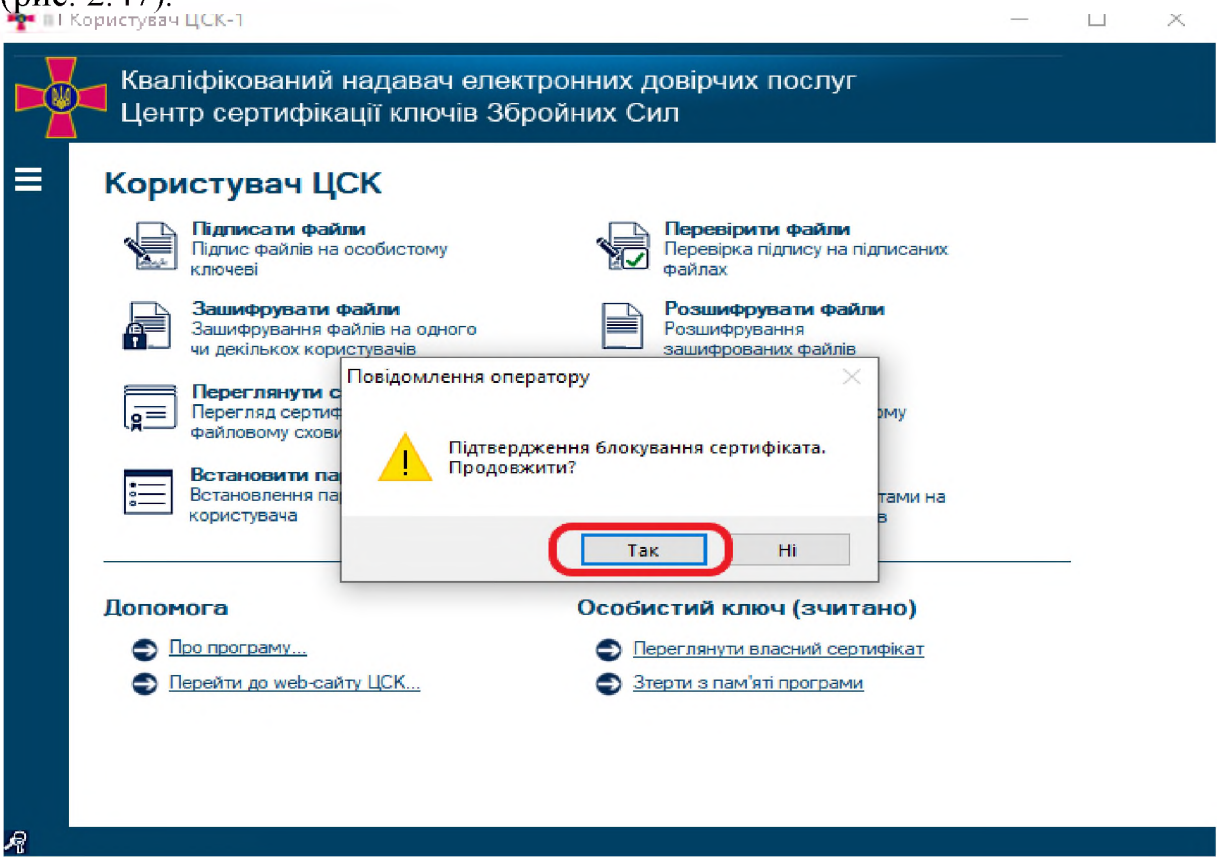


Рисунок 2.47

У наступному вікні майстра появиться результат обробки запиту. Натиснути “ОК” (рис. 2.48).

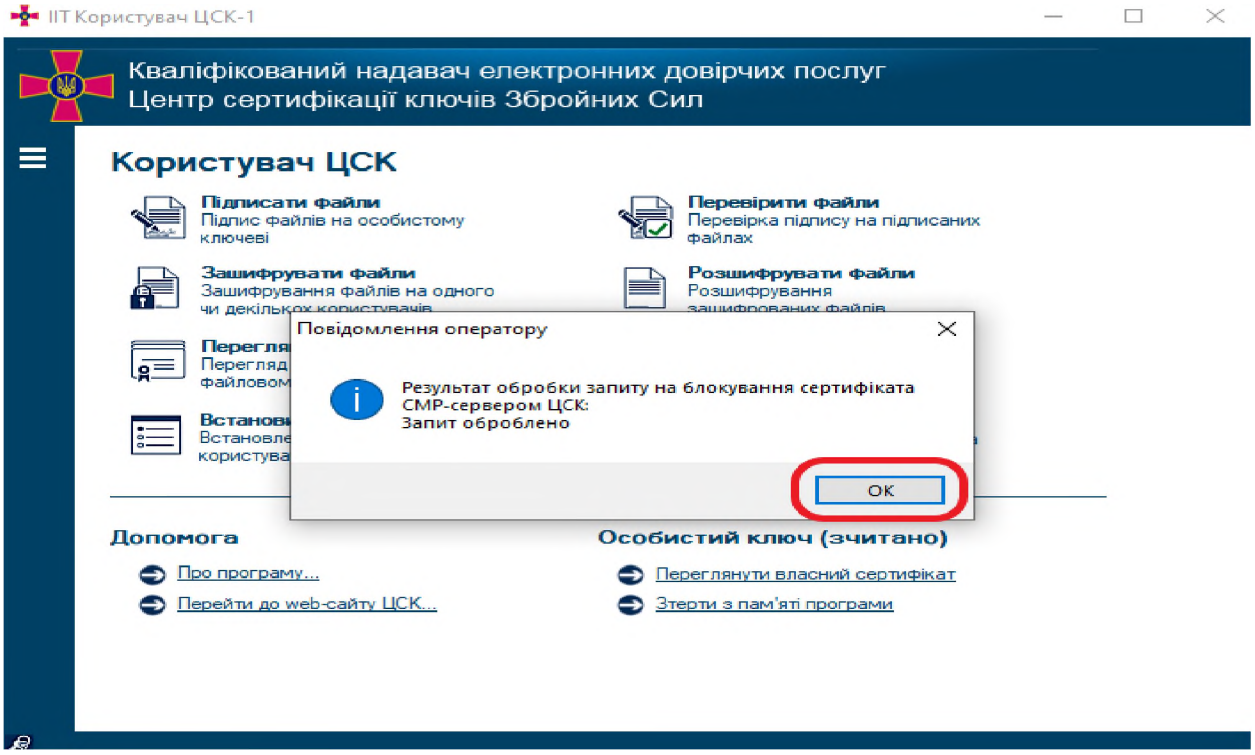


Рисунок 2.48

8. СКАСУВАННЯ КВАЛІФІКОВАНОГО СЕРТИФІКАТА ВІДКРИТОГО КЛЮЧА

Під скасуванням кваліфікованого сертифіката відкритого ключа розуміється зупинення чинності кваліфікованого сертифіката відкритого ключа.

Увага! Для здійснення скасування кваліфікованого сертифікату відкритого ключа необхідно підключення робочого місця на якому установлено ПЗ до мережі ІСД “Інтернет” або АСУ ЗСУ “Дніпро”.

Для скасування кваліфікованого сертифіката відкритого ключа у ПЗ необхідно обрати підпункт «Скасувати власні сертифікати» в пункті меню “Сертифікати та СВС” (рис. 2.49).

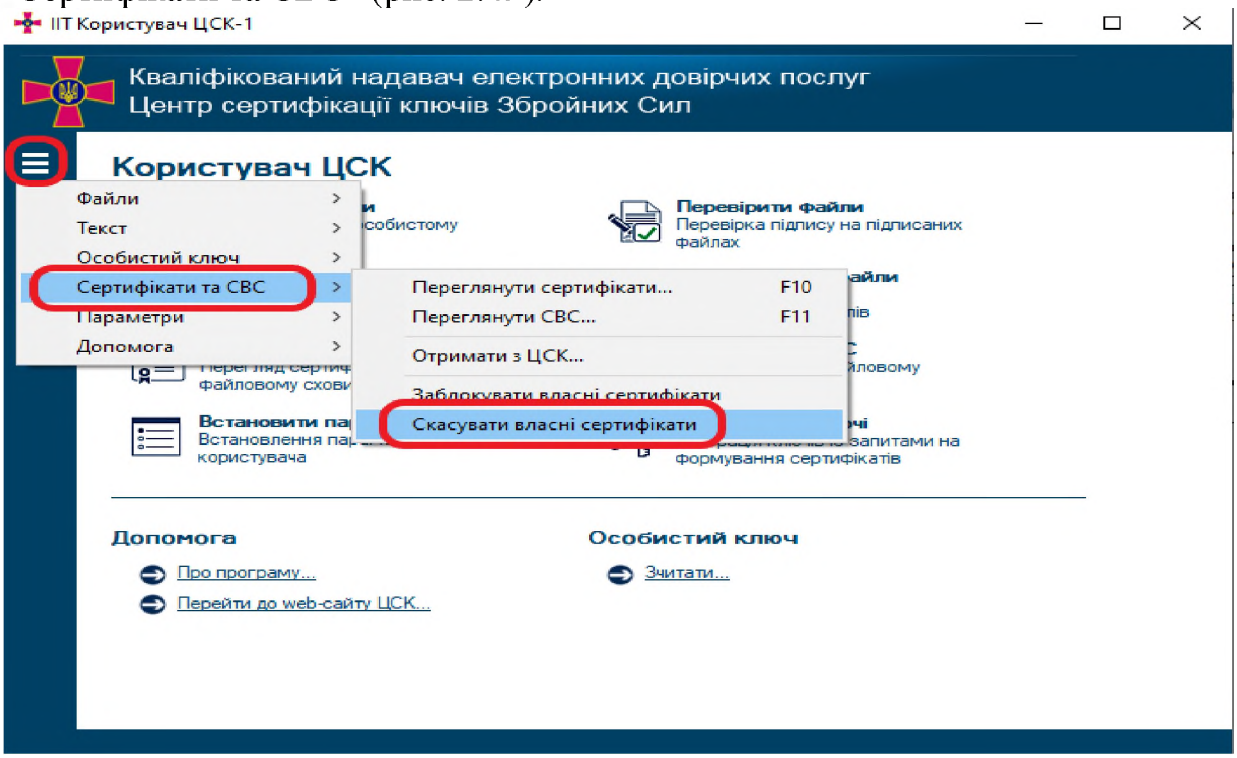


Рисунок 2.49

Для підтвердження скасування потрібно в наступному вікні майстра обрати “Так”(рис. 2.50).

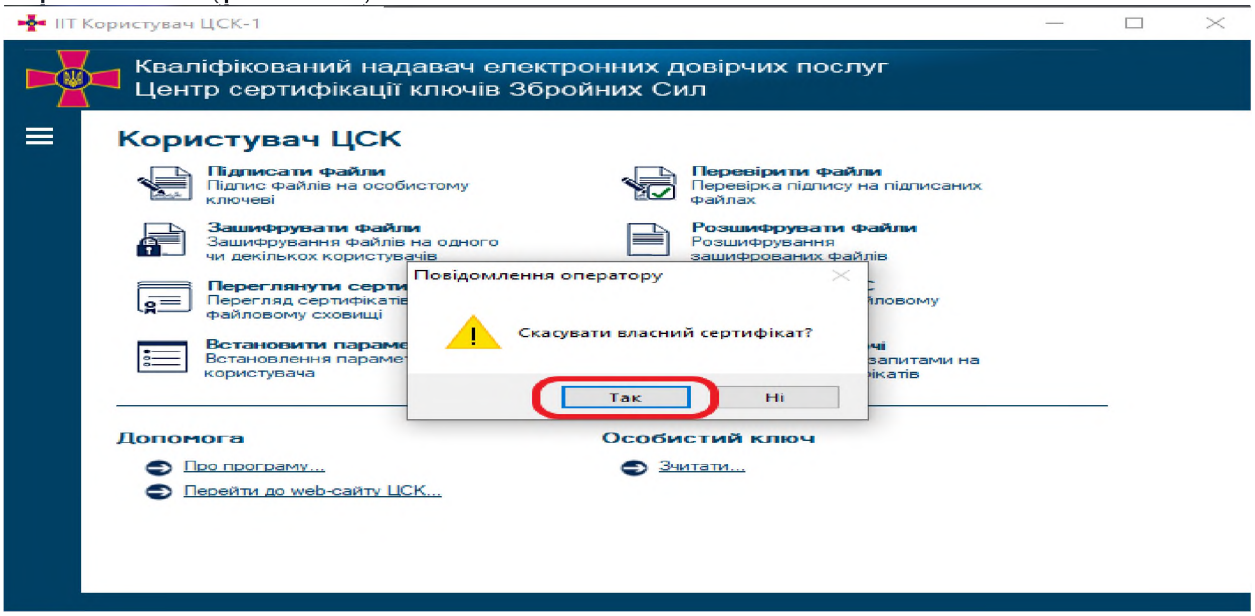


Рисунок 2.50

Після появи захищеного робочого столу необхідно обрати ЗНОК та ввести пароль захисту особистого ключа (рис. 2.51).

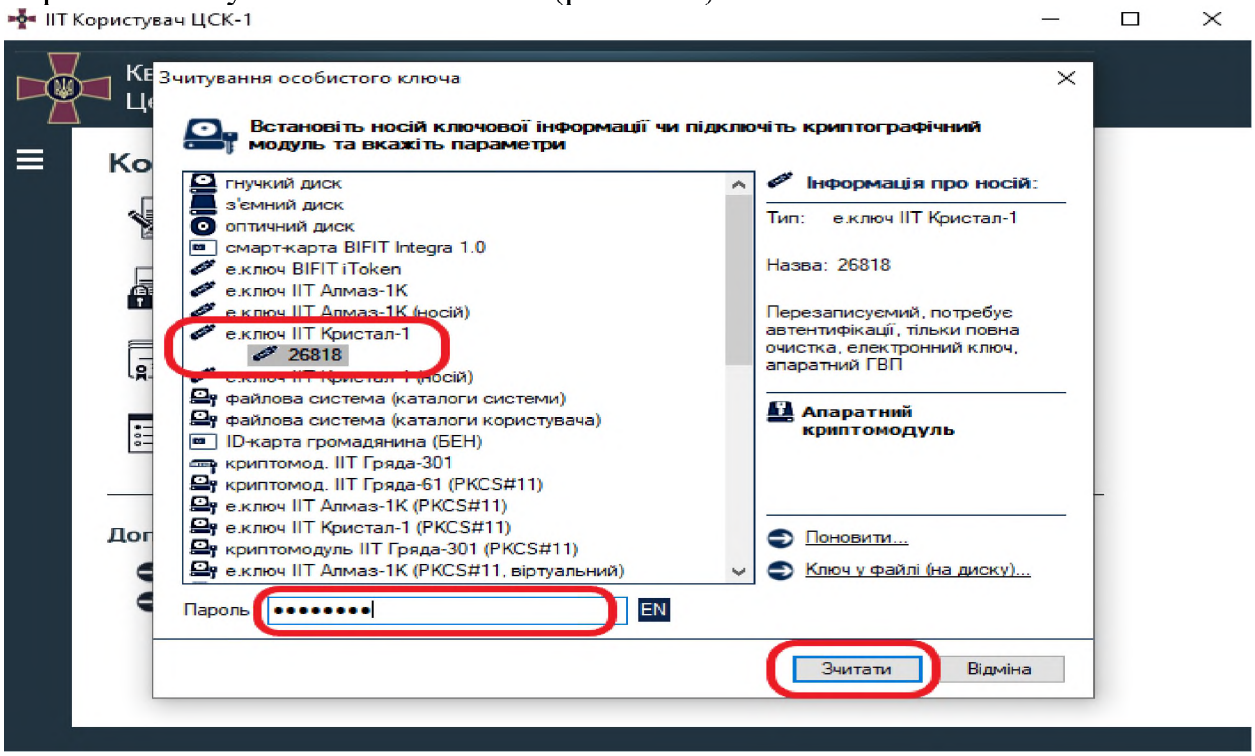


Рисунок 2.51

Далі з’являється повідомлення щодо підтвердження скасування кваліфікованого сертифіката, для підтвердження скасування натискаємо “Так” (рис. 2.52).

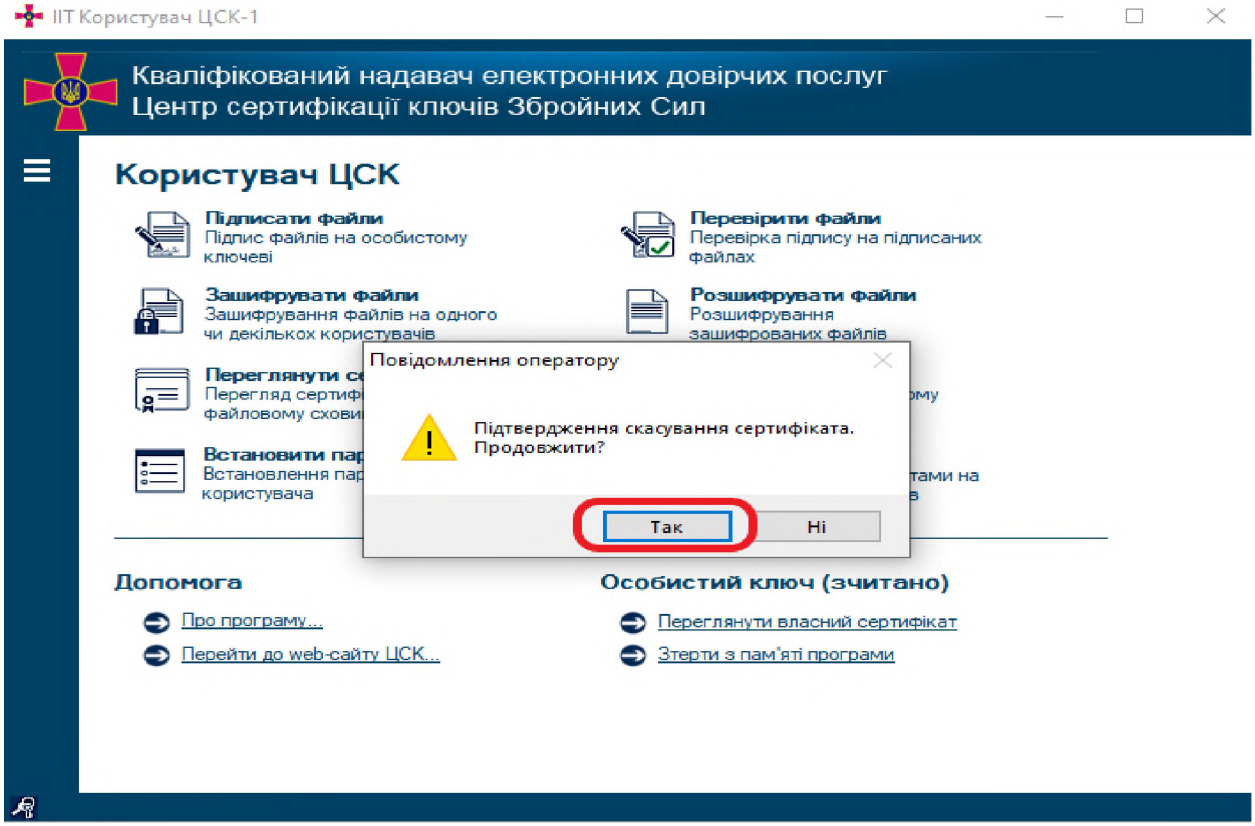


Рисунок 2.52

У наступному вікні майстра появиться результат обробки запиту. Натиснути “ОК” (рис. 2.52).

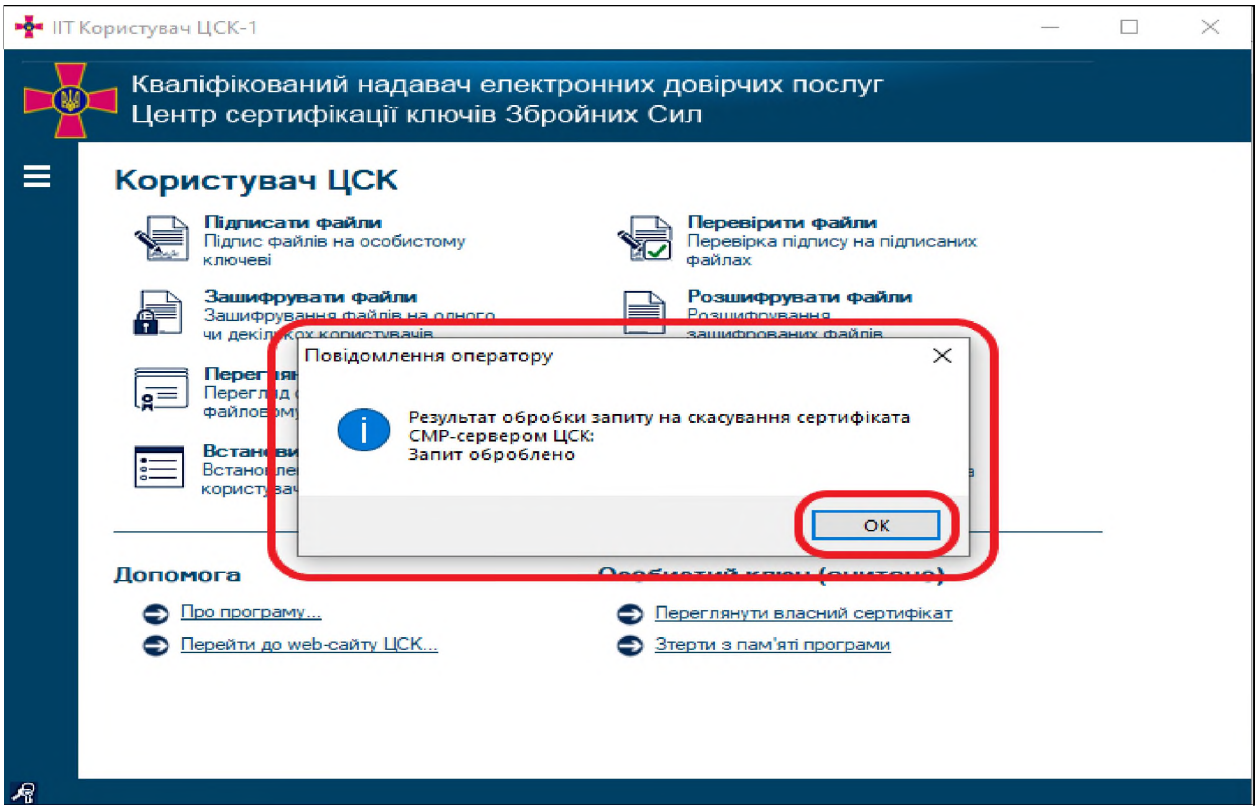
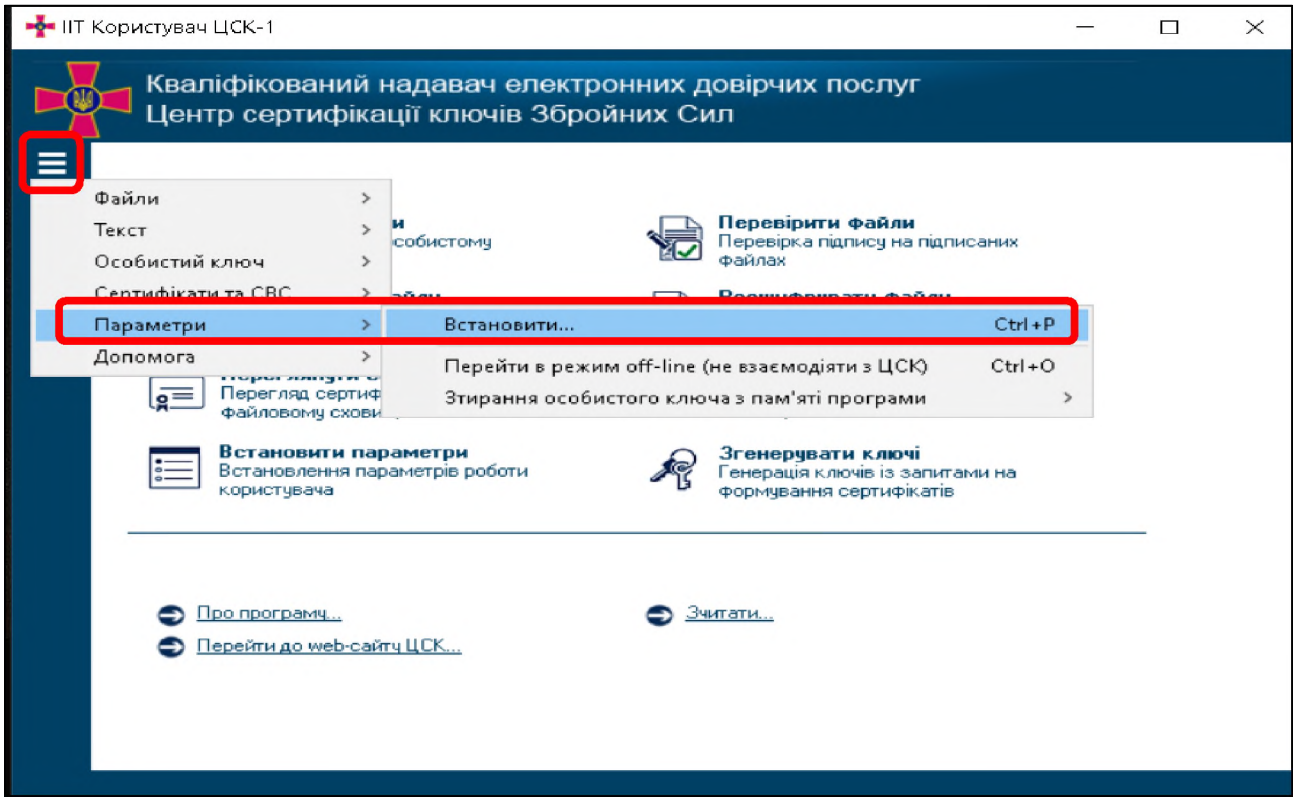


Рисунок 2.52

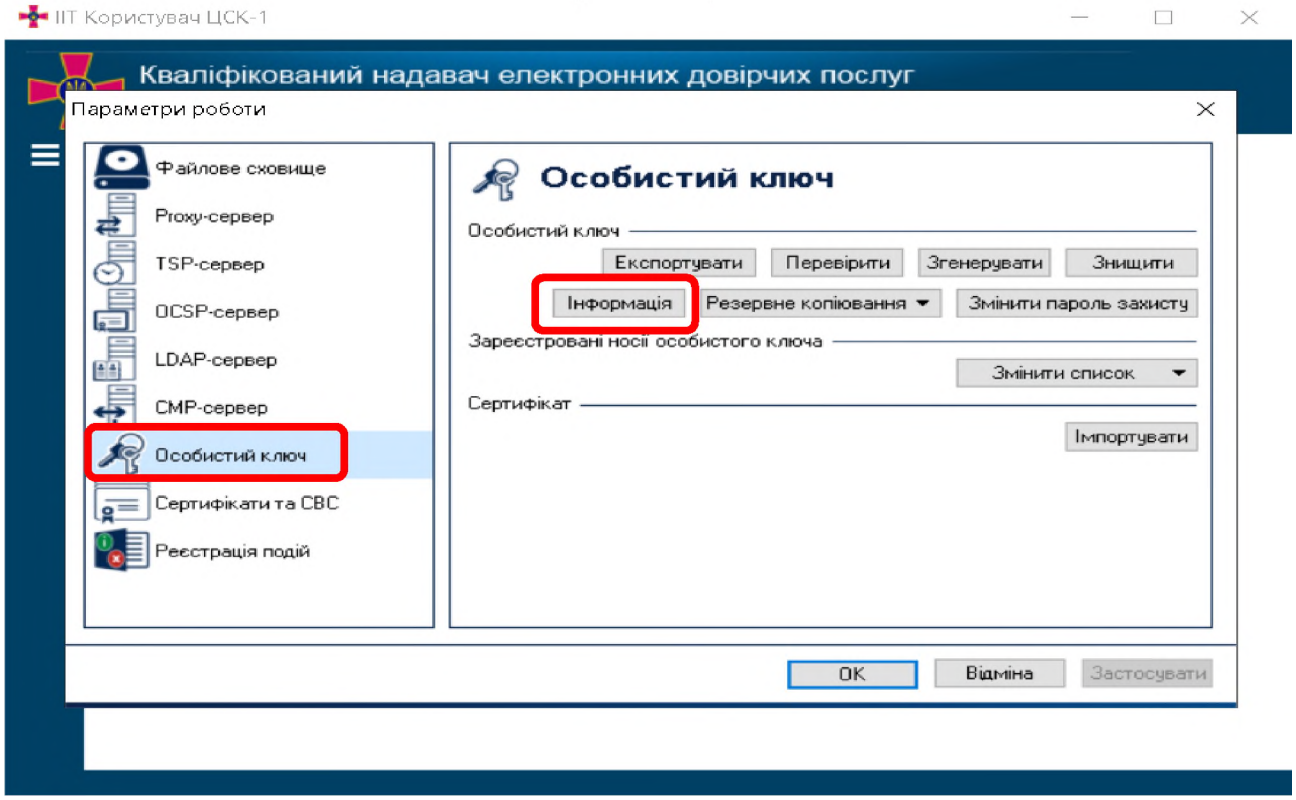
9. ПЕРЕВІРКА НАЯВНОСТІ ОСОБИСТИХ КЛЮЧІВ НА ЗНОК

Для перевірки наявності ключової інформації на захищеному носії необхідно натиснути меню(рис 2.53), потім “Параметри ” і “Встановити”.



Рисунок(2.53)

Далі необхідно обрати розділ “Особистий ключ” та натиснути “Інформація” (рис 2.54).



Рисунок(2.54)

Після виконання попередніх кроків, з'явиться вікно у якому необхідно обрати тип ЗНОК та ввести пароль(рис 2.55).

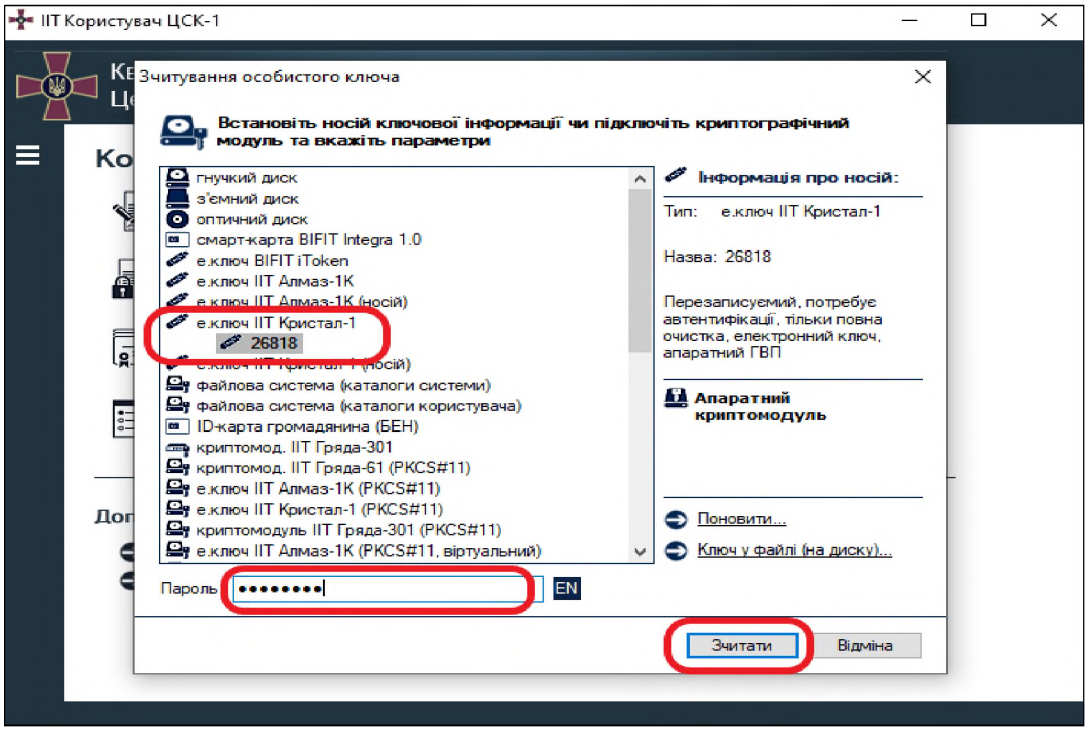
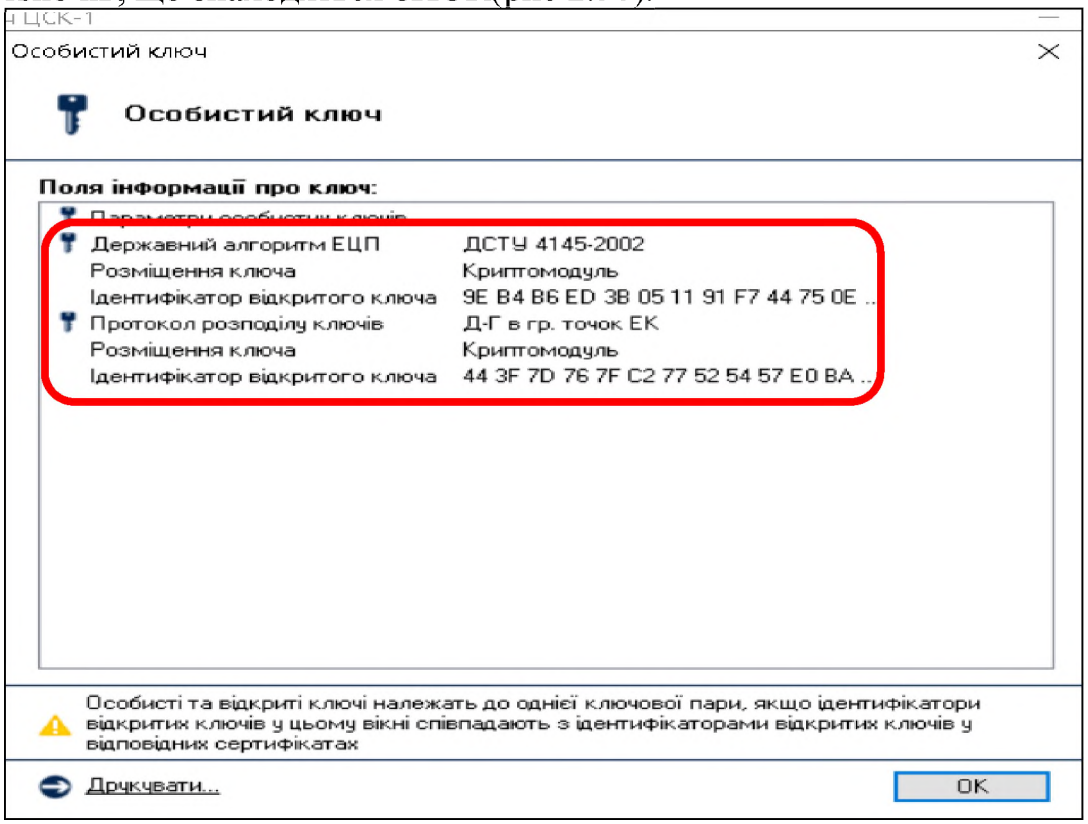


Рисунок 2.55

Якщо пароль введено вірно, то на екрані з'явиться перелік особистих ключів, що знаходяться ЗНОК(рис 2.56).



Начальник центру сертифікації ключів військової частини А0136
підполковник Володимир СОРОЧАК