ЗАТВЕРДЖУЮ
Командир військової частини А0136
полковник

Віталій КІНЧЕВСЬКИЙ
"02" 03 2026 року

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

Київ 2026

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

АСУ	–	Автоматизована система управління
ВПР	–	Відокремлений пункт реєстрації
ЕНІ	–	Електронний носій інформації типу жорсткий магнітний диск, USB флеш-носій тощо
ЗС України	–	Збройні Сили України
ЗКЕП	–	Засіб кваліфікованого електронного підпису чи печатки
ІКС	–	Інформаційно-комунікаційна система
ІСД	–	Інформаційна система даних
КЕП	–	Кваліфікований електронний підпис чи печатка
КНЕДП ЗС України	–	Кваліфікований надавач електронних довірчих послуг “Центр сертифікації ключів Збройних Сил України”
ПЗ	–	Програмне забезпечення “ІІТ Користувач ЦСК-1”
ПК	–	Персональний комп’ютер
СВС	–	Список відкликаних сертифікатів

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Ця Настанова, щодо порядку використання програмного забезпечення ІІТ "Користувач ЦСК-1" (далі – Інструкція) узагальнює вимоги щодо порядку генерації пари ключів (особистого та відповідного йому відкритого ключа) КЕП в установах, що відносяться до сфери управління Міністерства оборони України та/або підпорядковані (придані) військовому командуванню Збройних Сил України з метою подальшого отримання кваліфікованих електронних довірчих послуг (формування, перевірки та підтвердження чинності сертифіката КЕП) в **Кваліфікованого надавача електронних довірчих послуг "Центр сертифікації ключів Збройних Сил України".**

Терміни в цій Інструкції застосовуються у значеннях, наведених в Законі України "Про електронну ідентифікацію та електронні довірчі послуги", постанові Кабінету Міністрів України від 01.08.2023 № 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 КНЕДП ЗС України) 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 ЗС України № 11).

Генерація пари ключів КЕП повинна здійснюватись особисто підписувачем чи створювачем (уповноваженим представником створювача)[1] кваліфікованої електронної печатки за допомогою ЗКЕП. *(стаття 20 Закону України "Про електронну ідентифікацію та електронні довірчі послуги")*

Підписувачі КНЕДП ЗС України здійснюють генерацію пар ключів КЕП особисто за допомогою **Комплексу програмного користувача центру сертифікації ключів "ІІТ Користувач ЦСК-1"** (Експертний висновок Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 27.02.2024 № 04/05/02-50/ВС1).

Надання допомоги підписувачам під час генерації пар ключів здійснює відповідальний підрозділ (відповідальна особа) за організацію використання кваліфікованих електронних довірчих послуг в установі *(пункт 6 ПКМУ 798, п 2.2 Наказ ГК ЗС України № 11).*

Генерація пар ключів для технічних та/або програмних засобів, обслуговуючого персоналу, інформаційних, комунікаційних, інформаційно-комунікаційних систем та/або засобів (систем) криптографічного захисту інформації, а також мережевих ресурсів (поштових серверів, вебсайтів, тощо) здійснюється визначеними наказом керівника установи особами, відповідальними за криптографічні ключі (представниками підрозділу з кіберзахисту (служби

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

захисту інформації), криптографічного захисту інформації). Генерація здійснюється відповідно до вимог інструкцій зі складу документації комплексних систем захисту інформації, затверджених у встановленому 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" (далі – Наказ НГШ ЗС України № 266)).*

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

ВАЖЛИВО! 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 КНЕДП ЗС України за посиланням http://ca.mil.gov.ua у розділі **ЗАВАНТАЖИТИ.**

Далі здійснити інсталяцію ПЗ виконавши наступні дії:

1.1. Запускаємо інсталятор ПЗ – EUInstall.exe (рис. 2.1).

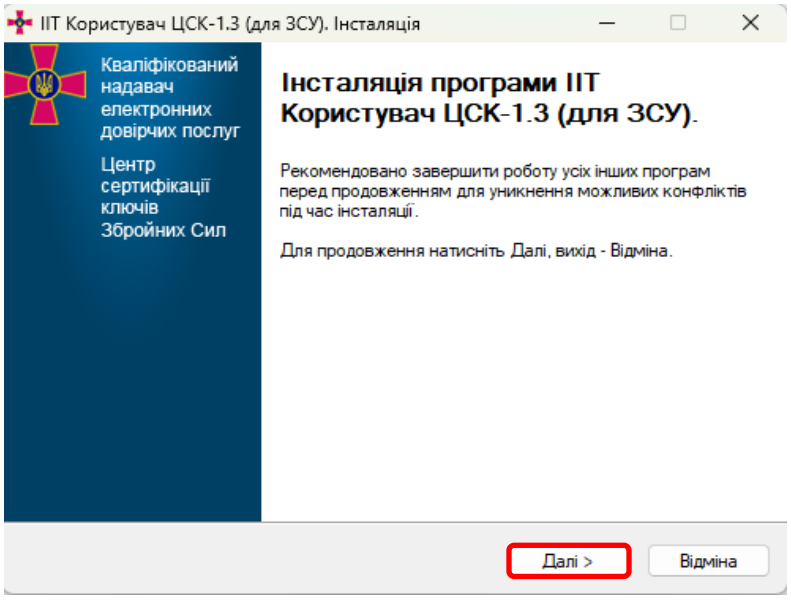

Рисунок 2.1

1.2. Ознайомлюємось з ліцензійною угодою та погоджуємось з її умовами, для продовження інсталяції натискаємо кнопку “Далі” (рис. 2.2).

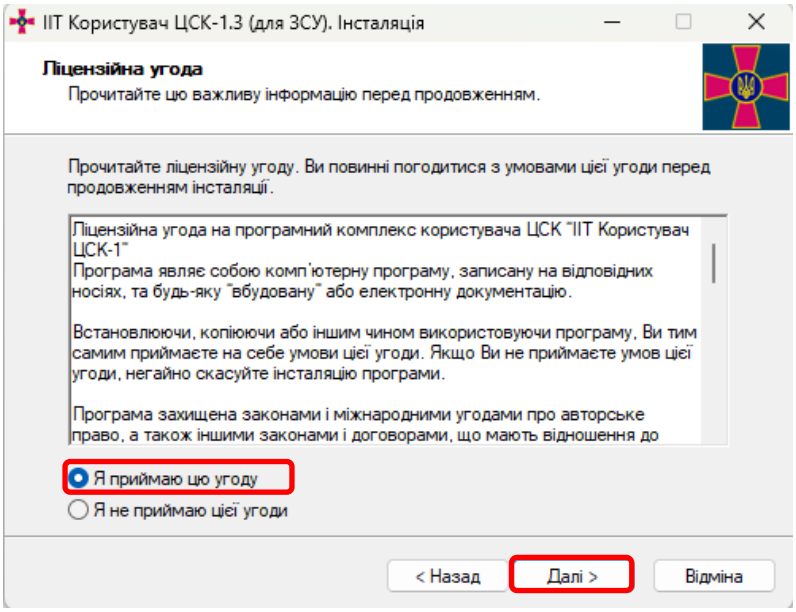

Рисунок 2.2

1.3. Каталог ПЗ у меню “Пуск” створюється автоматично, змінювати його не рекомендується, натискаємо кнопку “Далі” (рис. 2.3).

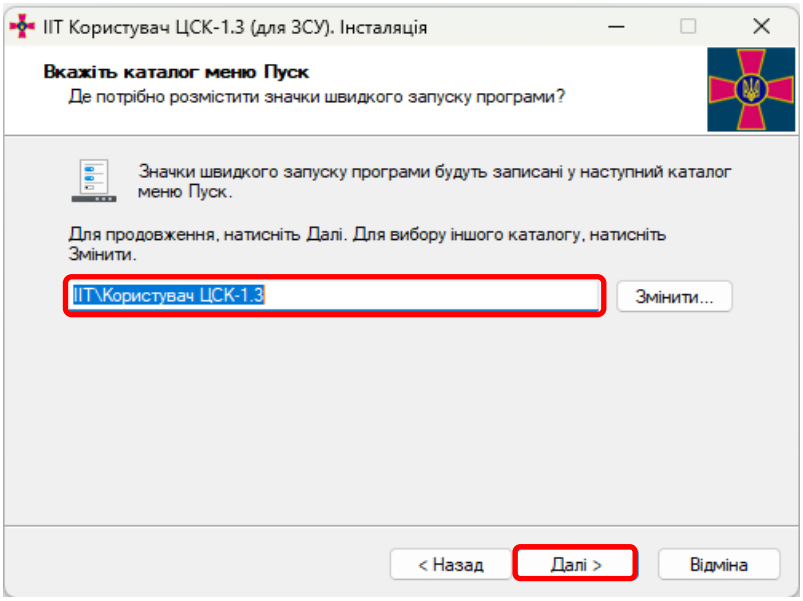

Рисунок 2.3

1.4. Під час встановлення ПЗ файлове сховище (локальний каталог, призначений для зберігання сертифікатів та СВС) створюється в розділі C:\My Certificates and CRLs 13 автоматично. Для зміни розташування файлового сховища необхідно натиснути кнопку “Змінити” та обрати відповідний каталог. Для продовження інсталяції натискаємо кнопку “Далі” (рис. 2.4).

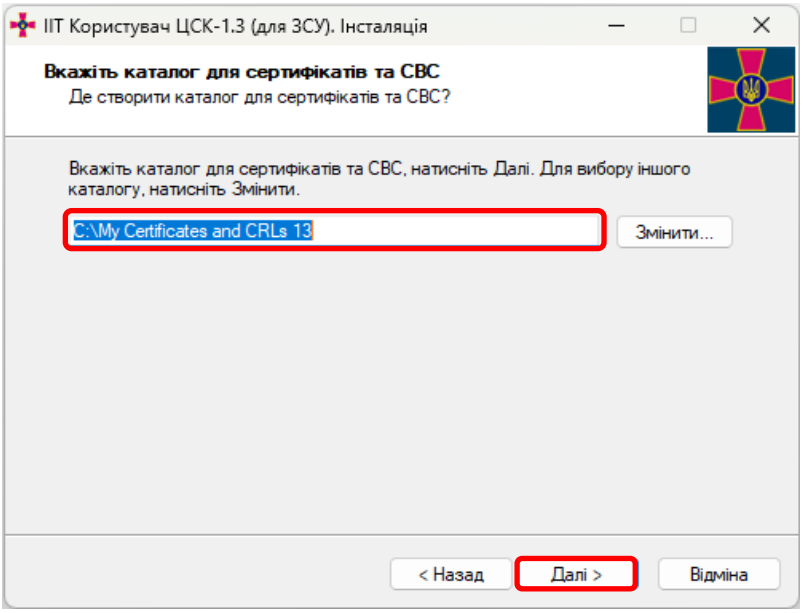

Рисунок 2.4

1.5. За необхідності можна створити ярлик на робочому столі та запустити ПЗ після завершення його інсталяції. Для цього необхідно проставити відповідні позначки (рис. 2.5). Для продовження інсталяції натискаємо кнопку “Далі”.

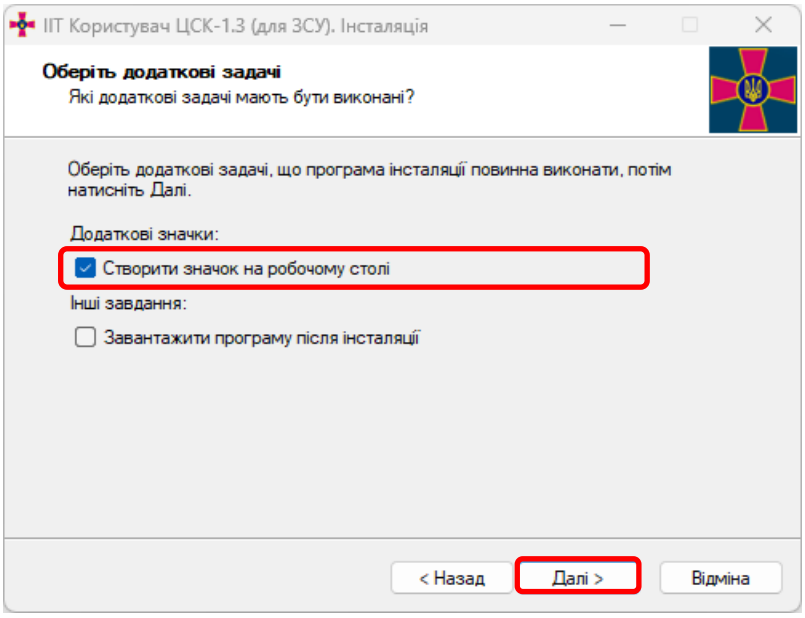

Рисунок 2.5

1.6. У вікні готовності до інсталяції натискаємо кнопку “Встановити” (рис. 2.6). Якщо параметри інсталяції не задовольняють підписувача, їх можна змінити натиснувши кнопку “Назад”. Для виходу з ПЗ без інсталяції необхідно натиснути “Відміна”.

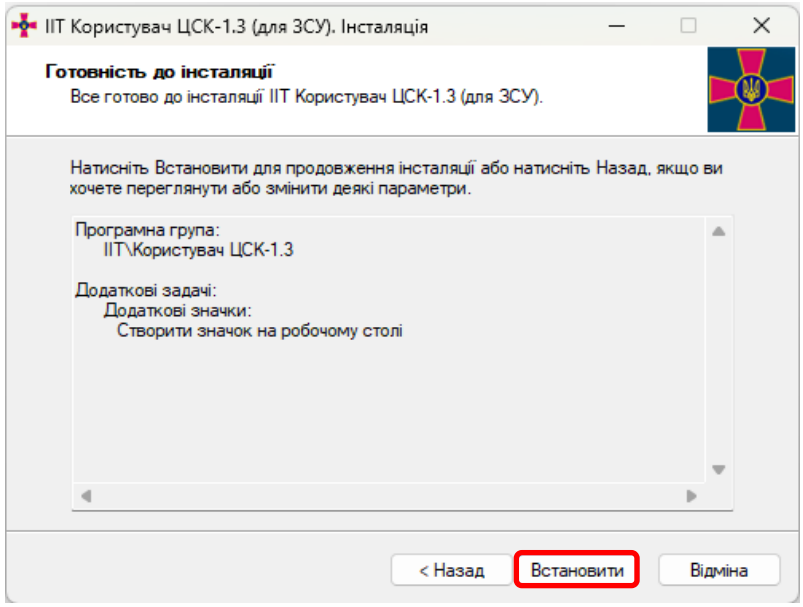

Рисунок 2.6

1.7. Після завершення інсталяції запущена ПЗ має вигляд як зображено на рис. 2.7. Перед використанням програму необхідно налаштувати.

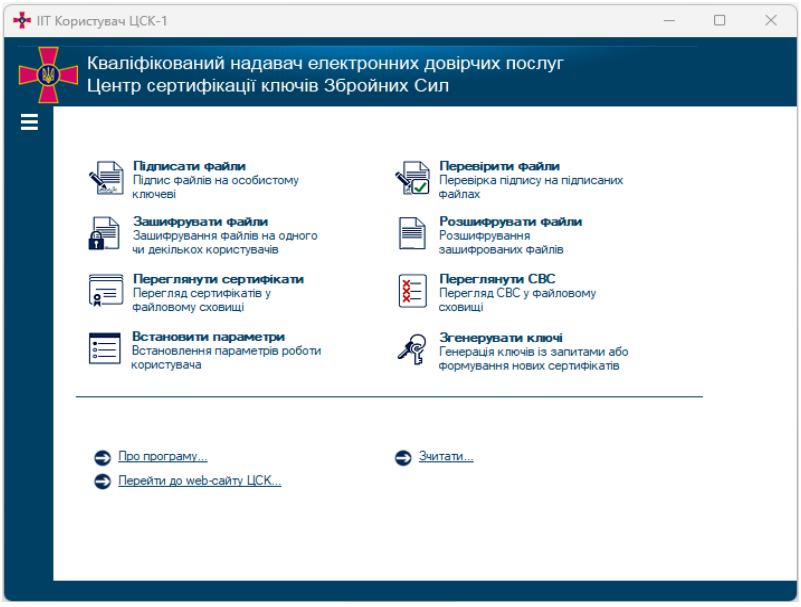

Рисунок 2.7

1.8. У зв’язку з відсутністю в ПЗ функції автоматичного оновлення версій, подальше його обслуговування здійснюється шляхом розміщення на вебсайті КНЕДП ЗС України (https://ca.mil.gov.ua) оновленого файлу з інсталяційним пакетом в розділі **ЗАВАНТАЖИТИ**. Про оновлення інсталяційного пакету ПЗ буде завчасно сповіщатись на вебсайті КНЕДП ЗС України за посиланням https://ca.mil.gov.ua в розділі **НОВИНИ**.

3. ГЕНЕРАЦІЯ ПАР КЛЮЧІВ

Для генерації особистих та відкритих ключів КЕП на ПК підписувача застосовується комплекс програмного користувача центру сертифікації ключів “ІІТ Користувач ЦСК-1”.

Генерація пар ключів може бути здійснена виключно на засіб кваліфікованого електронного підпису чи печатки (ЗКЕП), при чому особисті ключі КЕП автоматично захищаються паролем.

ВАЖЛИВО! Відповідальність за забезпечення конфіденційності особистого ключа КЕП та паролю до нього несе підписувач. У разі передачі ЗКЕП з особистим ключем КЕП та пароля до нього **сторонній особі ключ вважається скомпрометованим**.

Для генерації пар ключів у ПЗ необхідно обрати один з двох доступних способів:

1. Обрати меню, в ньому пункт “Особистий ключ” та підпункт “Згенерувати ключі” як зображено на рис. 3.1;

2. В стартовому вікні ПЗ обрати пункт “Згенерувати ключі” відповідно до рис. 3.2. Далі обрати “Згенерувати ключі та сформувати запити на сертифікати” та натиснути “ОК” (рис. 3.3).

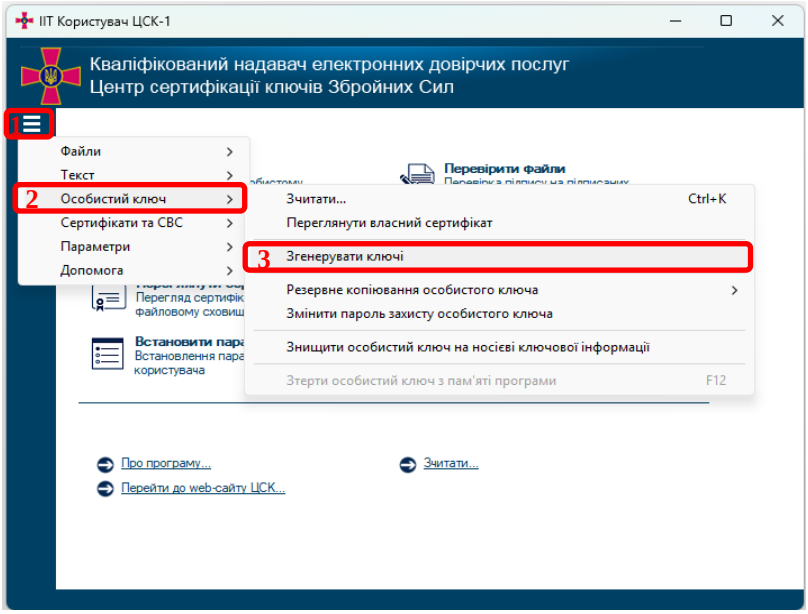

Рисунок 3.1

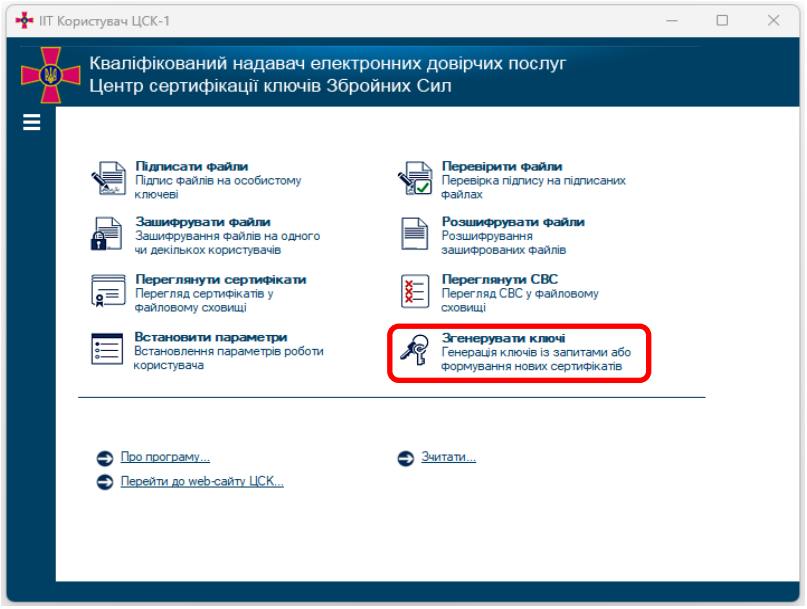

Рисунок 3.2

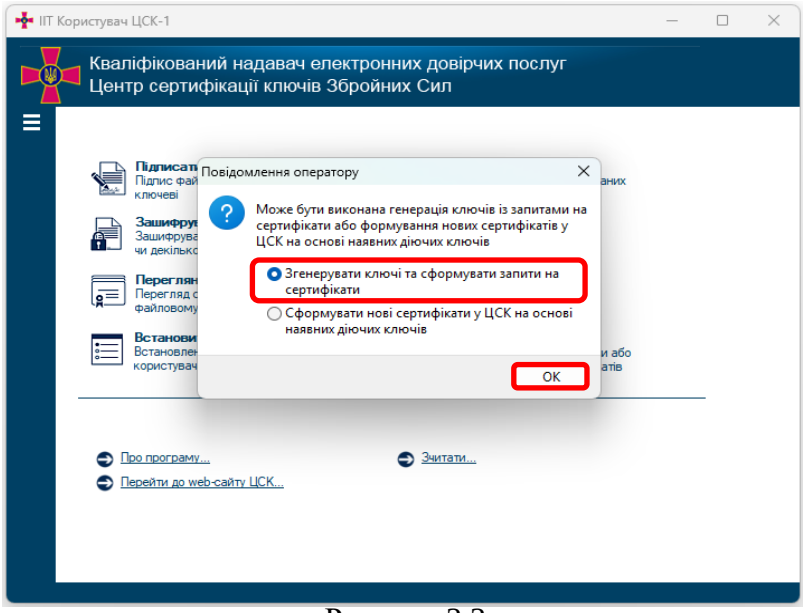

Рисунок 3.3

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

Файли відкритих ключів, разом з комплектом реєстраційних документів, можуть подаватись до КНЕДП ЗС України або його ВПР підписувачем або відповідальною особою у відповідності до пункту 4.1 Додатку 2 до Регламенту роботи КНЕДП ЗС України та особою, відповідальною за криптографічні ключі відповідно до Наказу НГШ ЗС України № 266 для формування кваліфікованих сертифікатів.

3.1. Генерація пар ключів для роботи за державними алгоритмами та протоколами на засіб кваліфікованого електронного підпису чи печатки (ЗКЕП)

Для того щоб згенерувати особистий ключ та файли запитів на сертифікати **“для державних алгоритмів і протоколів”** потрібно обрати відповідний параметр генерації ключів як зображено на рис. 3.4.

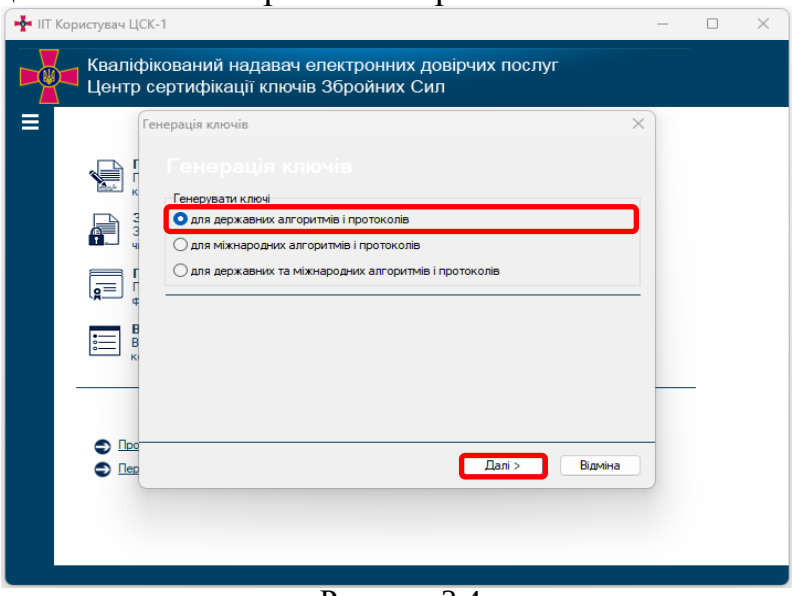

Рисунок 3.4

На наступній сторінці має бути обраний тип криптографічних алгоритмів та протоколів за ДСТУ 4145-2002 та Диффі-Гелман в гр. точок ЕК з ГОСТ 34.311, та параметр **“Використовувати окремий ключ для протоколу розподілу”**, інші параметри відповідно до рис. 3.5. 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 “Далі”.

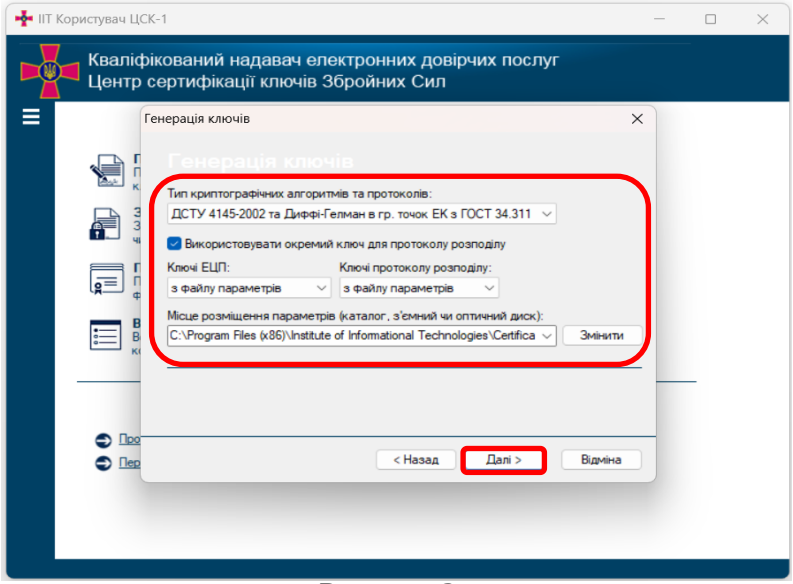

Рисунок 3.5

Далі необхідно встановити ЗКЕП для запису особистого ключа у пристрій запису та на наступній сторінці (рис. 3.6) вказати (обрати):

– тип ЗКЕП;
– серійний номер ЗКЕП;
– пароль доступу до особистого ключа;
– обрати попередньо відформатувати;
– повторити пароль доступу до особистого ключа.

Генерація пари ключів КЕП здійснюється в режимі “Апаратний криптомодуль”.

НЕ ДОПУСКАЄТЬСЯ вибирати для генерації ключа типи носія “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 розкладки клавіатури;
– дозволені символи – 'a-z', 'A-Z', '0-9', '+', '-'.

Примітка: такі вимоги до паролю носять рекомендаційний характер.

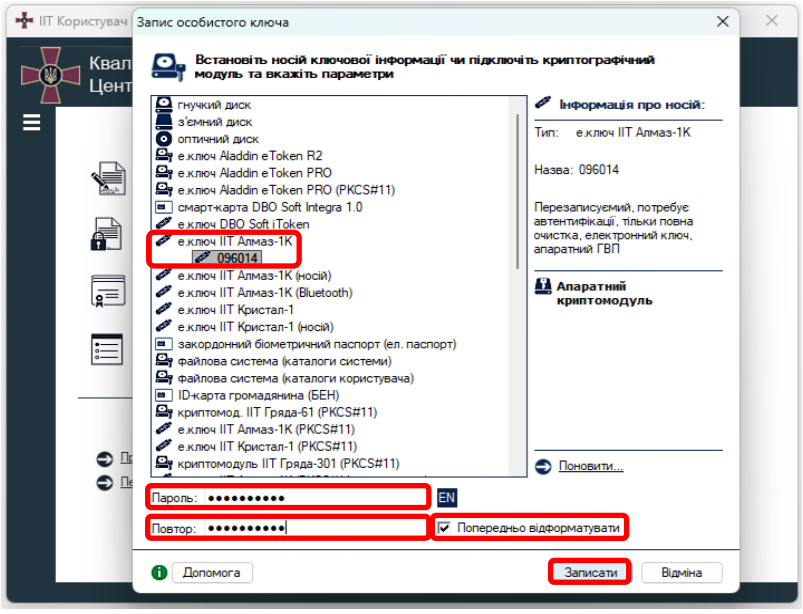

Рисунок 3.6

Після форматування (знищення всіх ключів, що зберігались на ЗКЕП) та запису особистого ключа на ЗКЕП, буде виведено вміст простих запитів на формування сертифікату з відкритим КЕП та запит на формування сертифіката з відкритим ключем протоколу розподілу для державних алгоритмів та протоколів (рис. 3.7 та рис. 3.8 відповідно). Потрібно переконатись, що особистий ключ згенеровано на ЗКЕП (в полі запиту уточнене призначення ключів) та обрано алгоритм підпису за ДСТУ 4145-2002, а алгоритм гешування за ГОСТ 34.311. Після перевірки вмісту простих запитів необхідно натиснути “ОК”.

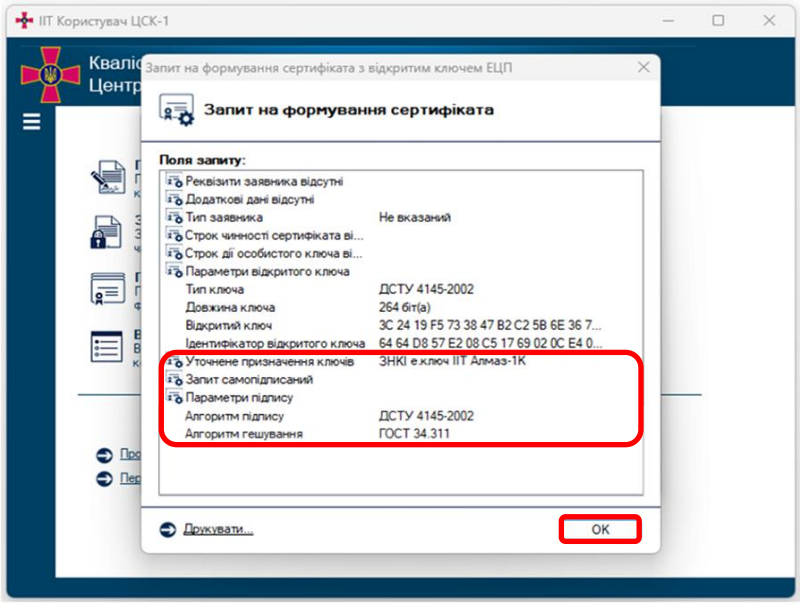

Рисунок 3.7

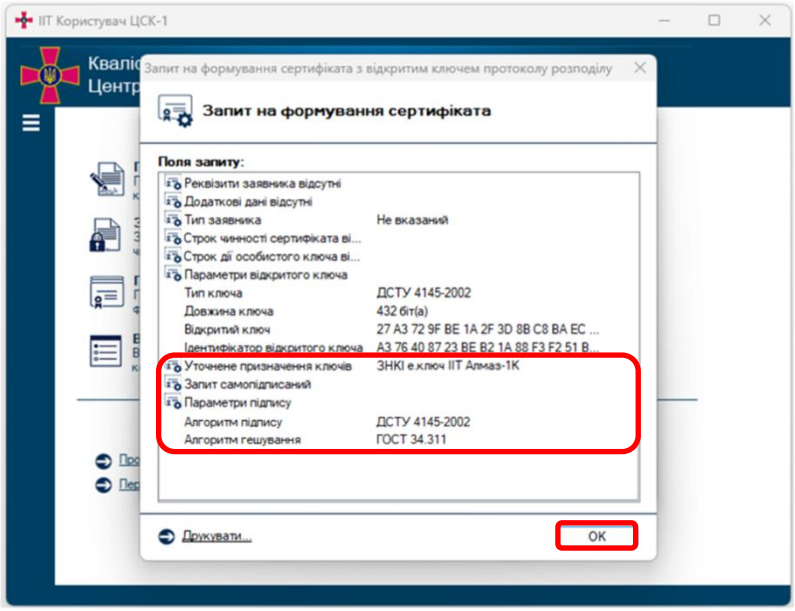

Рисунок 3.8

На наступній сторінці майстра (рис. 3.9) потрібно вказати спосіб збереження запитів на формування сертифікатів. Обираємо “Зберегти у файл” та натискаємо “Далі”.

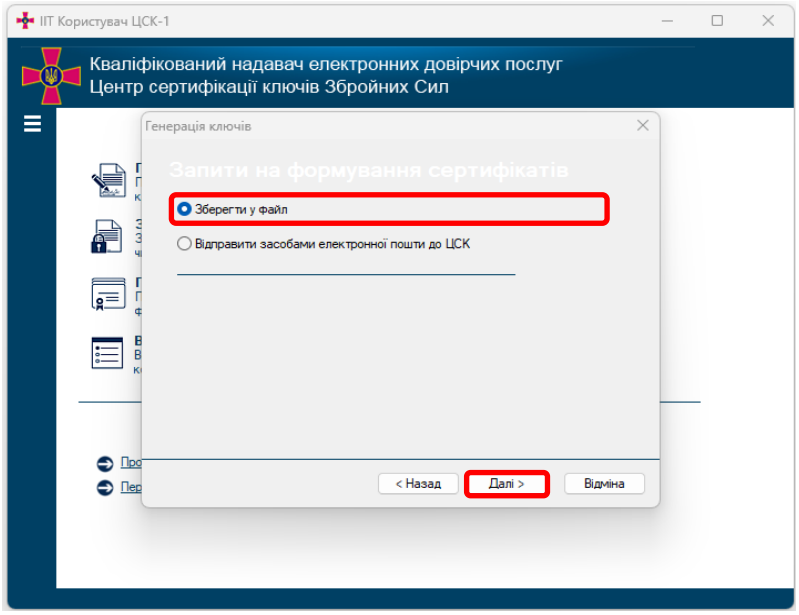

Рисунок 3.9

У наступному вікні (рис. 3.10) необхідно буде вказати ім’я файлів для запису запитів на формування сертифікатів у файл. Запити повинні бути записані на зареєстрований ЕНІ.

ВАЖЛИВО! Для коректної ідентифікації запитів на формування кваліфікованих сертифікатів вони мають 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 ініціали підписувача, що є власником особистого ключа.

“EU-” та “EU-KEP-” та “*.p10” – ідентифікатори та розширення файлів запитів, що формується ПЗ за замовчуванням та повинні залишатись без змін.

Наприклад: **EU-Петренко П.П.p10, EU-KEP-Петренко П.П.p10.**

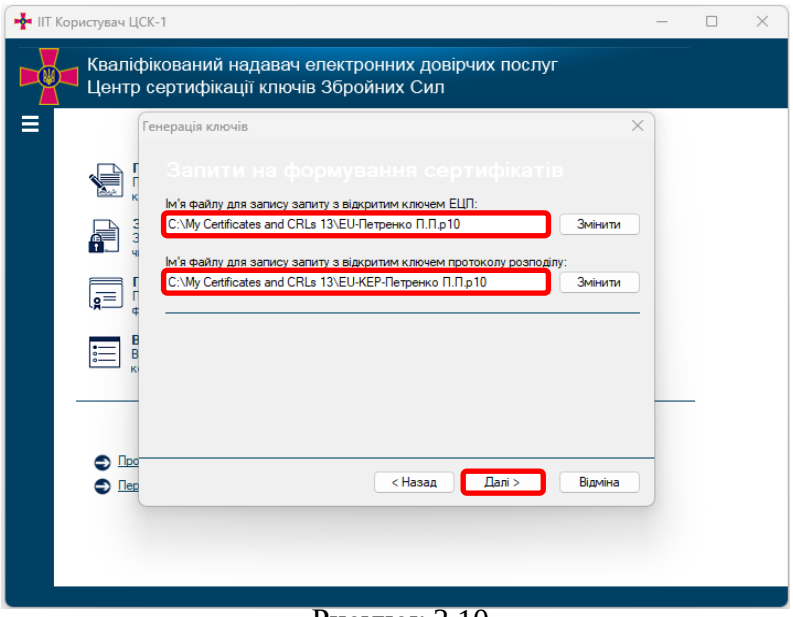

Рисунок 3.10

У наступному вікні (рис. 3.11) необхідно обрати завершити генерацію ключів. Сформовані файли запитів на формування сертифікатів можна буде знайти за посиланням, яке було вказано під час генерації (рис. 3.10).

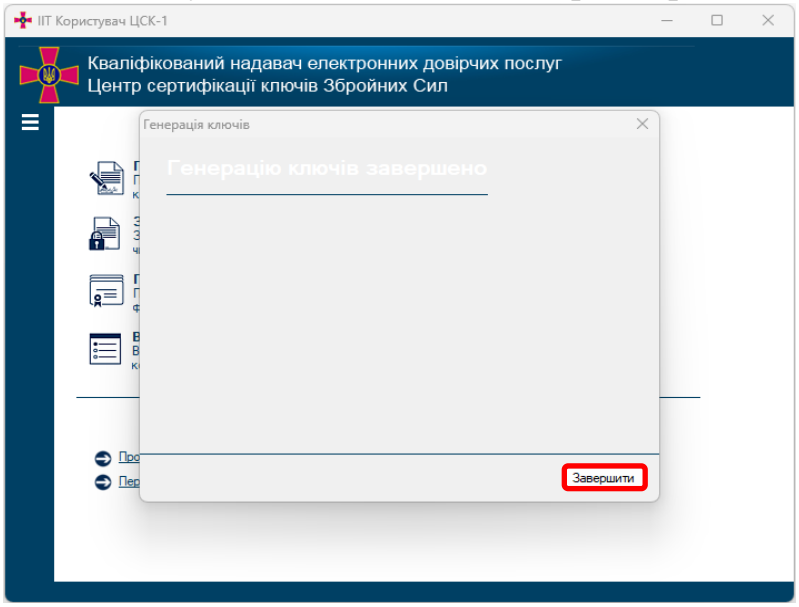

Рисунок 3.11

Файли відкритих ключів, разом з комплектом реєстраційних документів, можуть подаватись до КНЕДП ЗС України або його ВПР підписувачем або відповідальною особою у відповідності до пункту 4.1 Додатку 2 до Регламенту роботи КНЕДП ЗС України та особою, відповідальною за криптографічні ключі відповідно до Наказу НГШ ЗС України № 266 для формування кваліфікованих сертифікатів.

3.2. Генерація пар ключів для роботи за державними та міжнародними алгоритмами та протоколами на засіб кваліфікованого електронного підпису чи печатки (ЗКЕП)

Щоб згенерувати особистий ключ потрібно вказати параметри генерації ключів **“для державних та міжнародних алгоритмів і протоколів** та обрати параметри міжнародних алгоритмів: тільки RSA чи RSA та ECDSA (рис. 3.12).

ВАЖЛИВО! Додаткова генерація пар ключів за міжнародними алгоритмами RSA, ECDSA або RSA та ECDSA здійснюється виключно шляхом скасування чинних сертифікатів та формуванням нових пар ключів за державними та міжнародними алгоритмами і протоколами відповідно до цього пункту Інструкції.

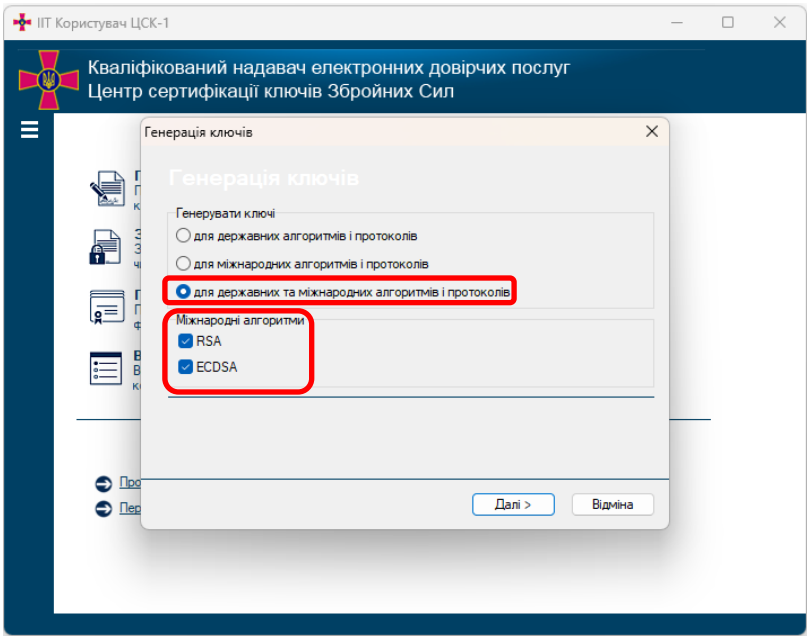

Рисунок 3.12

На наступній сторінці має бути обраний тип криптографічних алгоритмів та протоколів за ДСТУ 4145-2002 та Диффі-Гелман в гр. точок ЕК з ГОСТ 34.311, та параметр **“Використовувати окремий ключ для протоколу розподілу”**, інші параметри відповідно до рис. 3.13. Для продовження генерації ключа необхідно натиснути “Далі”.

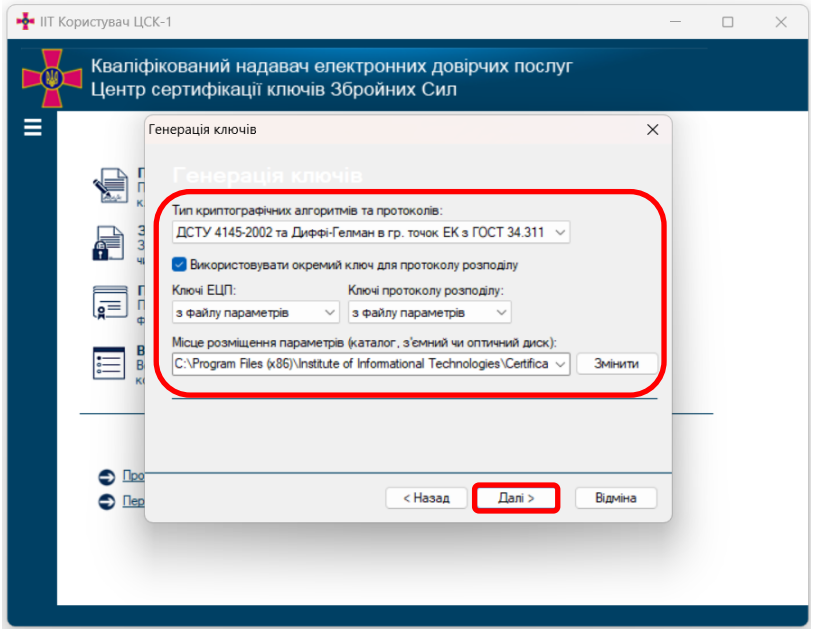

Рисунок 3.13

На наступній сторінці обрати параметри генерації ключів за RSA алгоритмами та протоколами відповідно до рис. 3.14. В разі генерації ключів за ECDSA алгоритмами та протоколами вибрати параметри відповідно до рис. 3.15. Для продовження генерації ключів необхідно натиснути “Далі”.

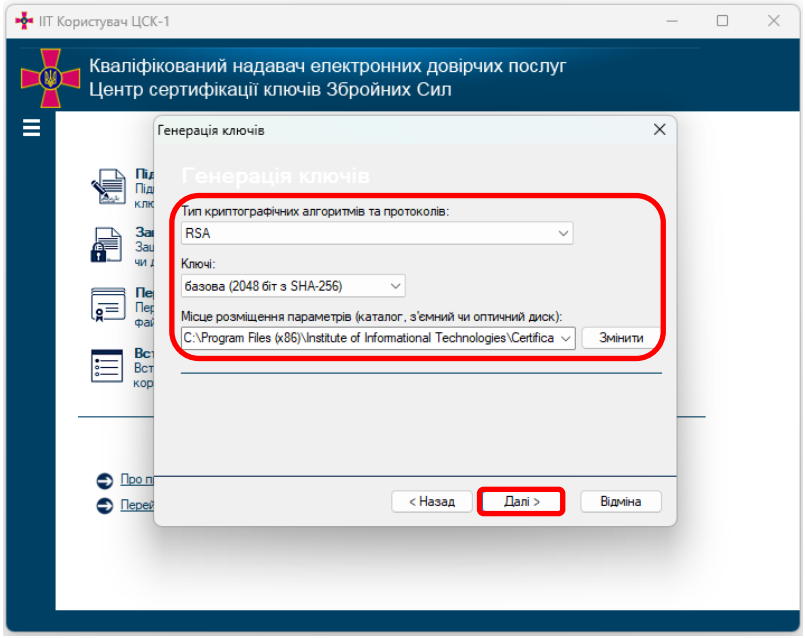

Рисунок 3.14

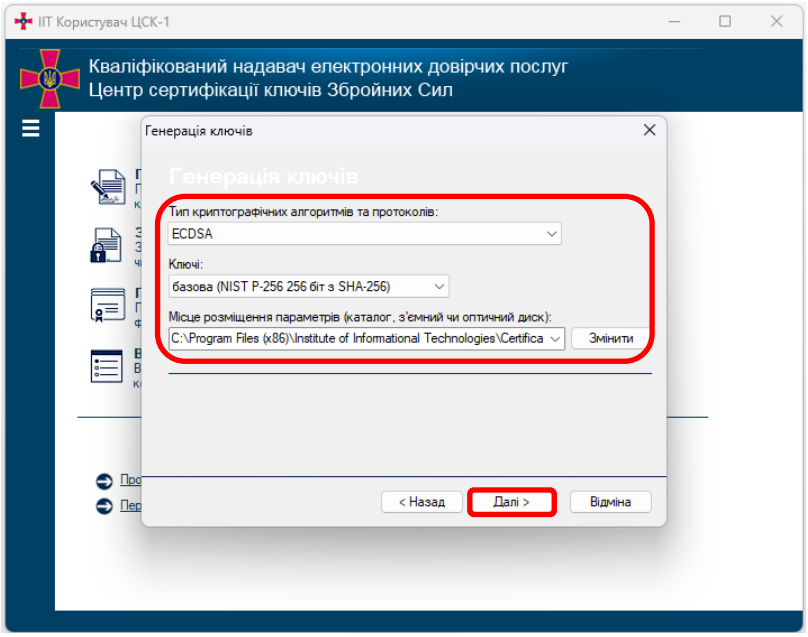

Рисунок 3.15

Далі необхідно встановити ЗКЕП для запису особистого ключа у пристрій запису та на наступній сторінці (рис. 3.16) вказати (обрати):

– тип ЗКЕП;
– серійний номер ЗКЕП;
– пароль доступу до особистого ключа;
– обрати попередньо відформатувати;
– повторити пароль доступу до особистого ключа.

Генерація пари ключів КЕП здійснюється в режимі “Апаратний криптомодуль”.

НЕ ДОПУСКАЄТЬСЯ вибирати для генерації ключа типи носія “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 розкладки клавіатури;
– дозволені символи – 'a-z', 'A-Z', '0-9', '+', '-'.

Примітка: такі вимоги до паролю носять рекомендаційний характер.

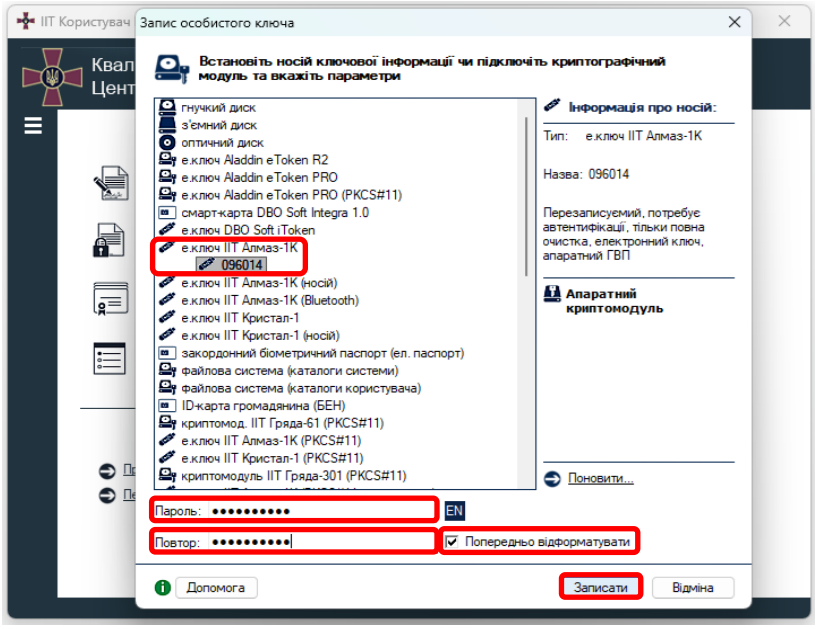

Рисунок 3.16

Після форматування (знищення всіх ключів, що зберігались на ЗКЕП) та запису особистого ключа на ЗКЕП, буде виведено вміст запитів на формування сертифікатів з відкритими ключами КЕП за державними та міжнародними алгоритмами та протоколами (рис. 3.17, 3.18, 3.19, 3.20). Далі потрібно переконатись, що особистий ключ згенеровано на ЗКЕП[2] та для запитів на формування сертифікату з відкритим КЕП та на формування сертифікату з відкритим ключем протоколу розподілу обрано алгоритм підпису за ДСТУ 4145-2002, а алгоритм гешування за ГОСТ 34.311. Після перевірки вмісту запитів необхідно натиснути ”ОК”.

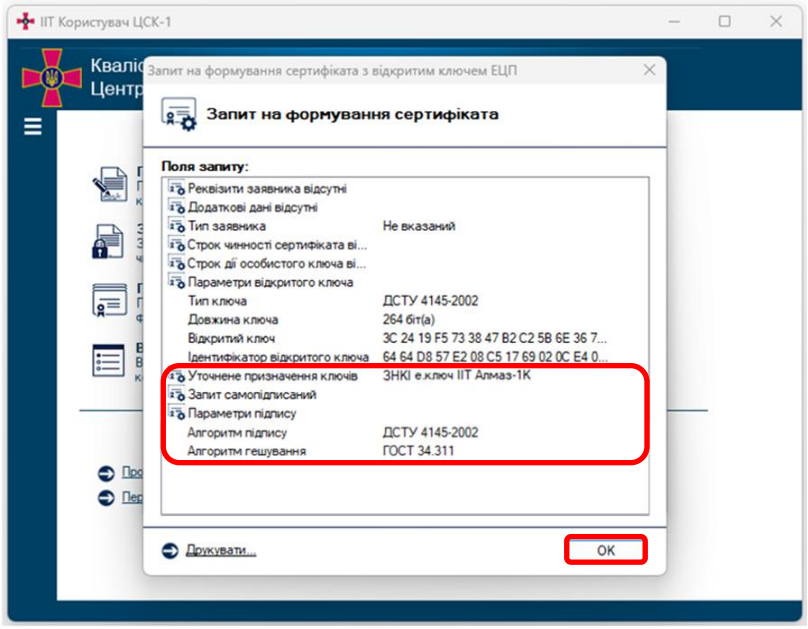

Рисунок 3.17

[2] Уточнене призначення для ключів RSA та ECDSA – відсутнє навіть при генерації на ЗКЕП.

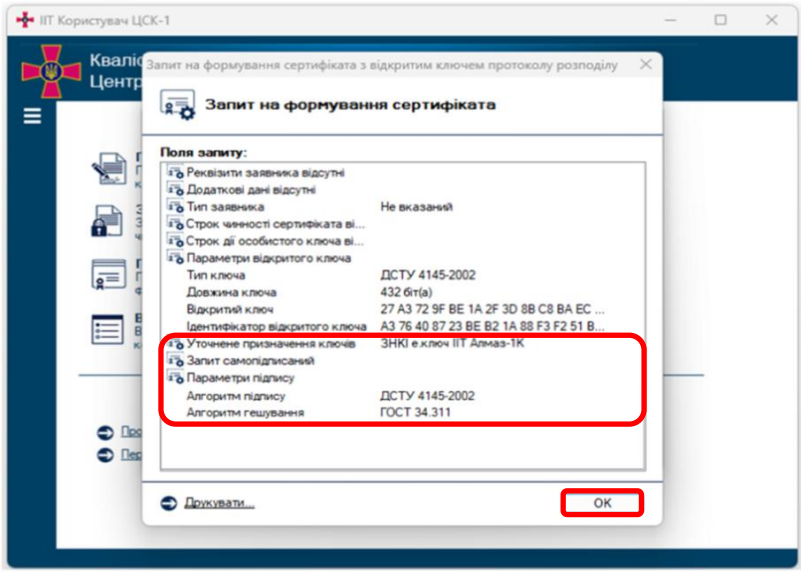

Рисунок 3.18

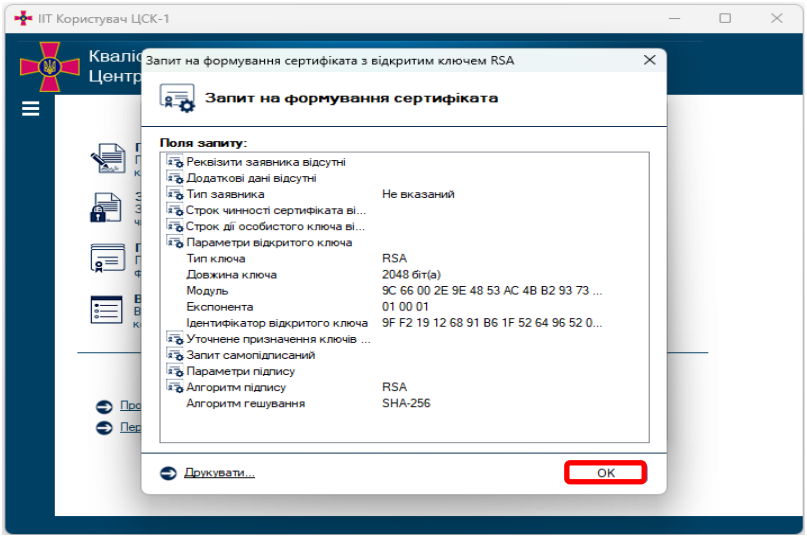

Рисунок 3.19

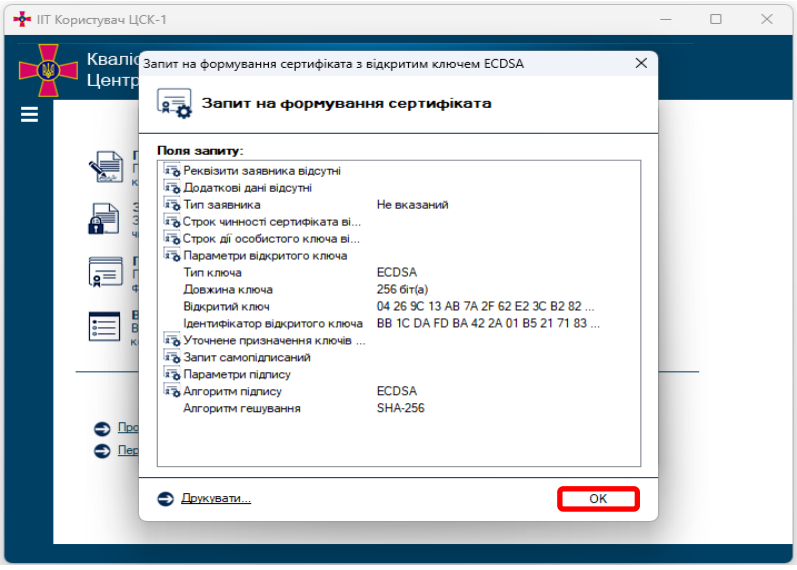

Рисунок 3.20

На наступній сторінці (рис. 3.21) потрібно обрати спосіб збереження запитів на формування сертифікатів. Обираємо “Зберегти у файл” та натискаємо “Далі”.

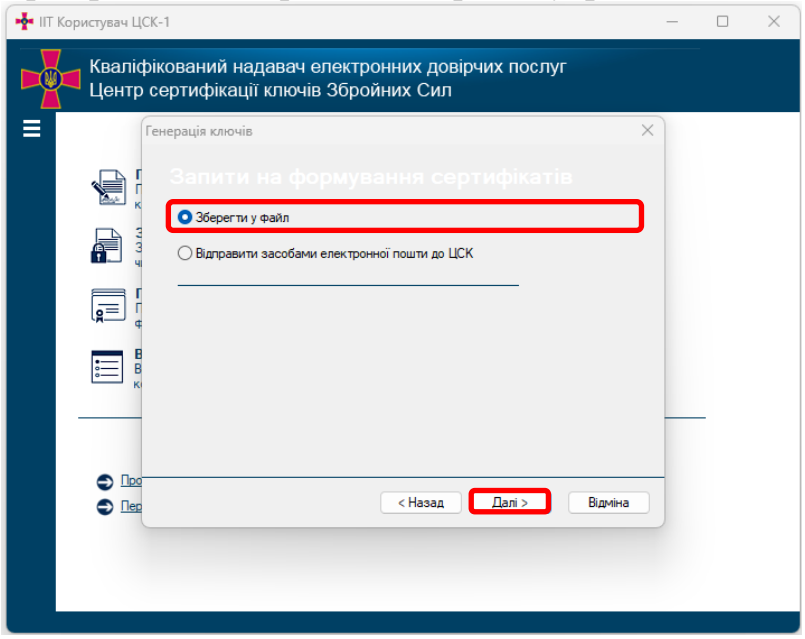

Рисунок 3.21

У наступному вікні (рис. 3.22) необхідно вказати ім’я файлів для запису запитів на формування сертифікатів у файл. Запити повинні бути записані на зареєстрований ЕНІ.

ВАЖЛИВО! Для коректної ідентифікації запитів на формування кваліфікованих сертифікатів вони мають обов’язково зберігатись з ім’ям у наступному форматі:

“EU-ПІБ.p10”;

“EU-KEP-ПІБ.p10”;

“EU-RSA-ПІБ.p10”,

“EU-ECDSA-ПІБ.p10”.

ПІБ – прізвище та ініціали підписувача, що є власником особистого ключа.

“EU-”, “EU-KEP-”, “EU-RSA-” “EU-ECDSA-” та “*.p10” – ідентифікатори та розширення файлів запитів, що формуються ПЗ за замовчуванням, та повинні залишатись без змін.

Наприклад: **EU-Петренко П.П.p10, EU-KEP-Петренко П.П.p10, EU-RSA-Петренко П.П.p10, EU-ECDSA-Петренко П.П.p10.**

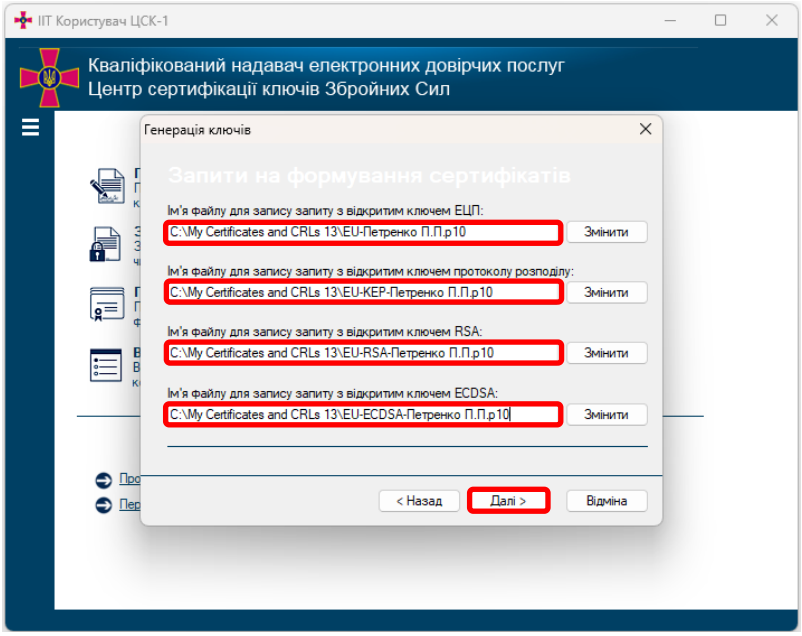

Рисунок 3.22

У наступному вікні (рис. 3.23) необхідно обрати завершити генерацію ключів. Сформовані файли запитів на формування сертифікатів можна буде знайти за посиланням, яке було вказано під час генерації ключів (рис. 3.22).

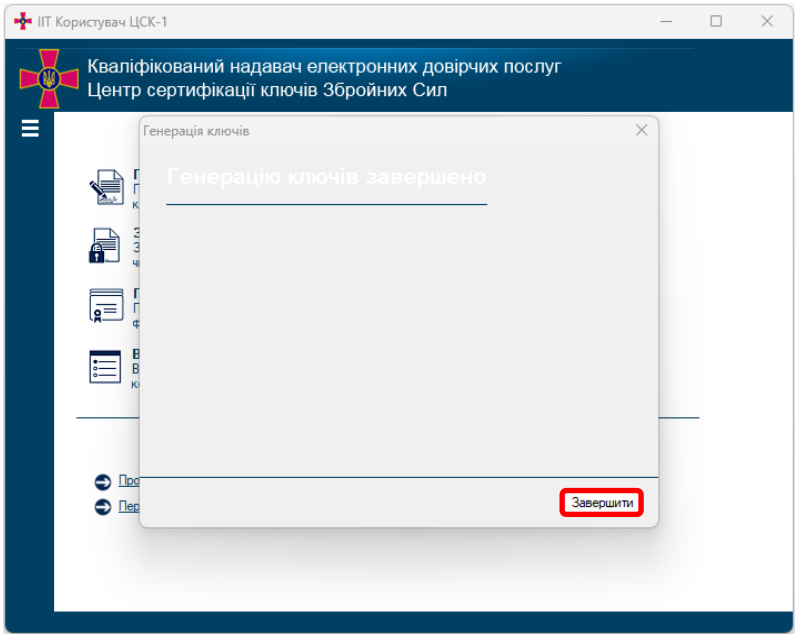

Рисунок 3.23

Файли відкритих ключів, разом з комплектом реєстраційних документів, можуть подаватись до КНЕДП ЗС України або його ВПР підписувачем або відповідальною особою у відповідності до пункту 4.1 Додатку 2 до Регламенту роботи КНЕДП ЗС України та особою, відповідальною за криптографічні ключі відповідно до Наказу НГШ ЗС України № 266 для формування кваліфікованих сертифікатів.

3.3. Генерація пари ключів кваліфікованої електронної печатки на засіб кваліфікованого електронного підпису чи печатки (ЗКЕП)

Генерація пари кваліфікованої ключів електронної печатки здійснюється створювачем електронної печатки (особою відповідальною за електронну печатку установи) на ЗКЕП.

Щоб згенерувати пару ключів кваліфікованої електронної печатки потрібно вказати параметри генерації ключів **“для державних алгоритмів і протоколів”** (рис. 3.34).

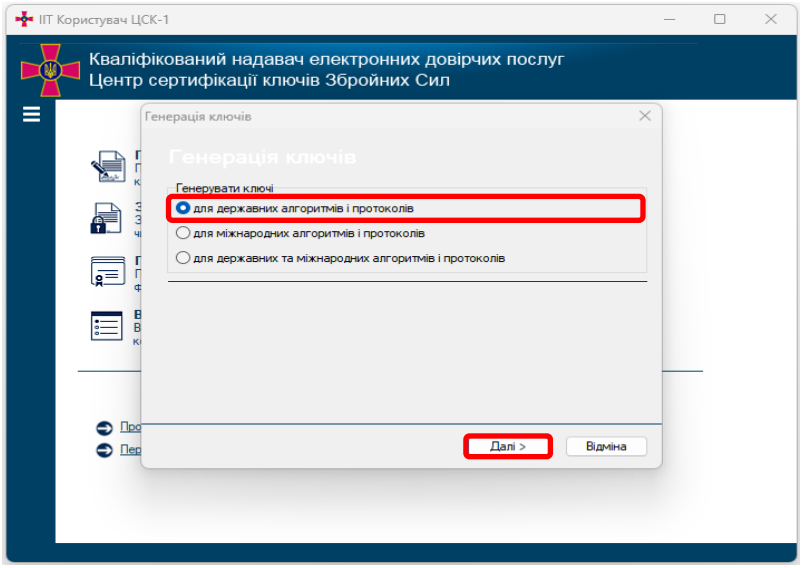

Рисунок 3.34

На наступній сторінці має бути обраний тип криптографічних алгоритмів та протоколів за ДСТУ 4145-2002 та Диффі-Гелман в гр. точок ЕК з ГОСТ 34.311, та **НЕ** має бути обрано параметру **“Використовувати окремий ключ для протоколу розподілу”,** інші параметри відповідно до рис. 3.35. Для продовження необхідно натиснути “Далі”.

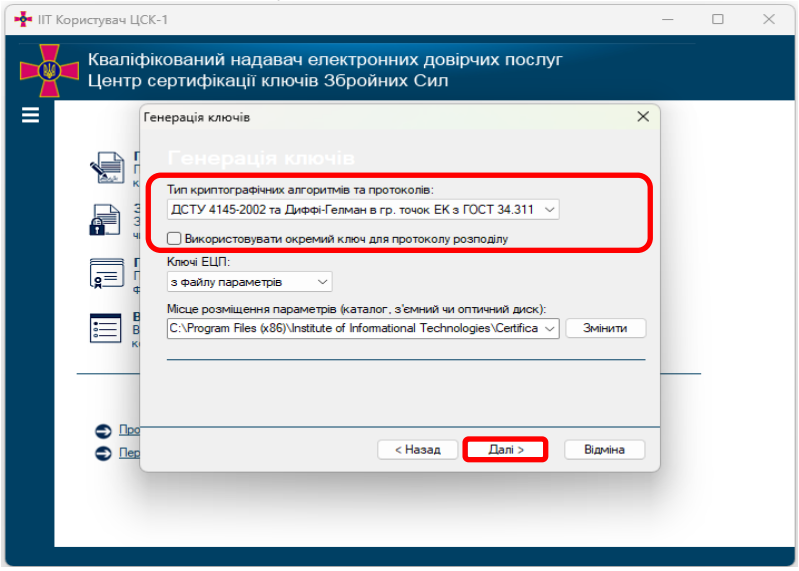

Рисунок 3.35

Наступним кроком необхідно встановити ЗКЕП для запису особистого ключа електронної печатки та на наступній сторінці (рис. 3.36) вказати (обрати):

– тип ЗКЕП;
– серійний номер ЗКЕП;
– пароль доступу до особистого ключа;
– обрати попередньо відформатувати;
– повторити пароль доступу до особистого ключа.

Генерація пари ключів КЕП здійснюється в режимі “Апаратний криптомодуль”.

НЕ ДОПУСКАЄТЬСЯ вибирати для генерації ключа типи носія “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 розкладки клавіатури;
– дозволені символи – 'a-z', 'A-Z', '0-9', '+', '-'.

Примітка: такі вимоги до паролю носять рекомендаційний характер.

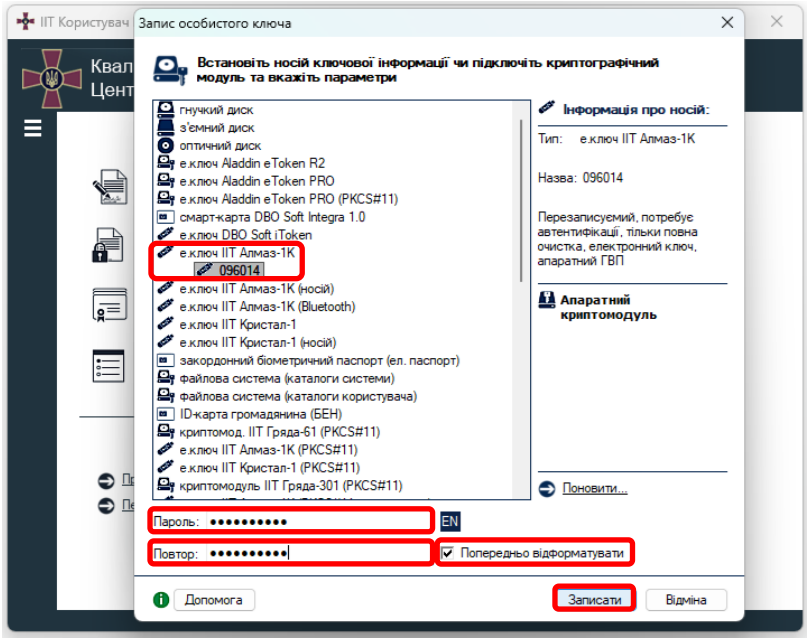

Рисунок 3.36

Після запису особистого ключа на ЗКЕП, буде виведено вміст запиту на формування сертифікату з відкритим ключем КЕП (рис. 3.37). Потрібно переконатись, що особистий ключ згенеровано на ЗКЕП (в полі запиту уточнене призначення ключів) та обрано алгоритм підпису за ДСТУ 4145-2002. Після перевірки вмісту простого запиту необхідно натиснути “ОК”.

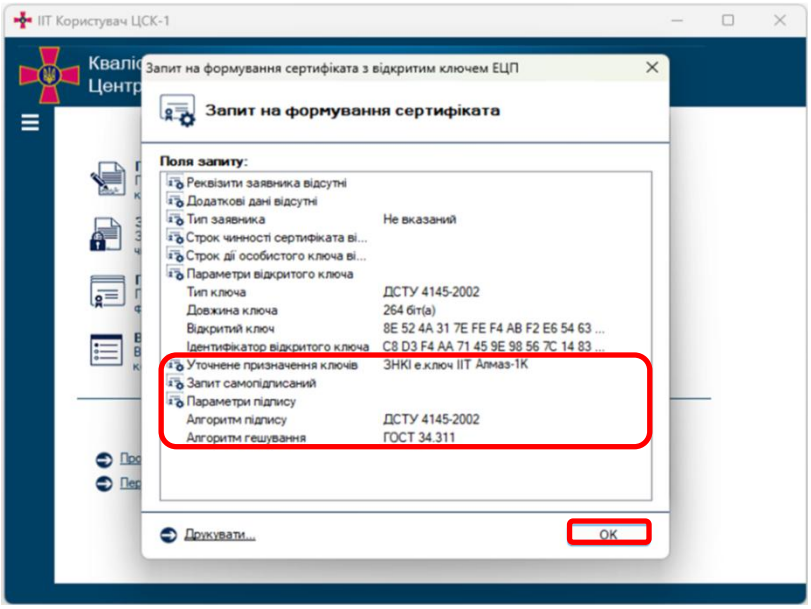

Рисунок 3.37

На наступній сторінці майстра (рис. 3.38) потрібно вказати спосіб збереження запиту на формування сертифіката. Обираємо “Зберегти у файл” та натиснути “Далі”.

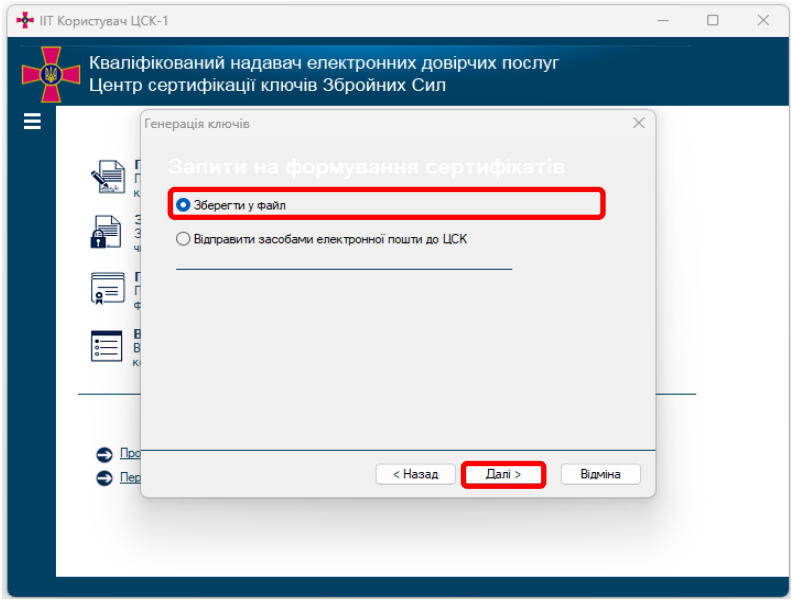

Рисунок 3.38

У наступному вікні (рис. 3.39) необхідно буде вказати ім’я файлу для запису запиту на формування сертифіката у файл. Запит повинен бути записаний на зареєстрований ЕНІ.

ВАЖЛИВО! Для коректної ідентифікації запиту з відкритим ключем КЕП на формування кваліфікованого сертифіката він обов’язково має зберігатись з ім’ям у наступному форматі: **“EU-Назва.p10”**, де: **Назва** – найменування установи та її печатки.

“EU-” та “.p10”– ідентифікатори та розширення файлу запиту, що формується ПЗ за замовчуванням, та повинно залишатись без змін.

Наприклад: **EU-печатка №1 A0000.p10.**

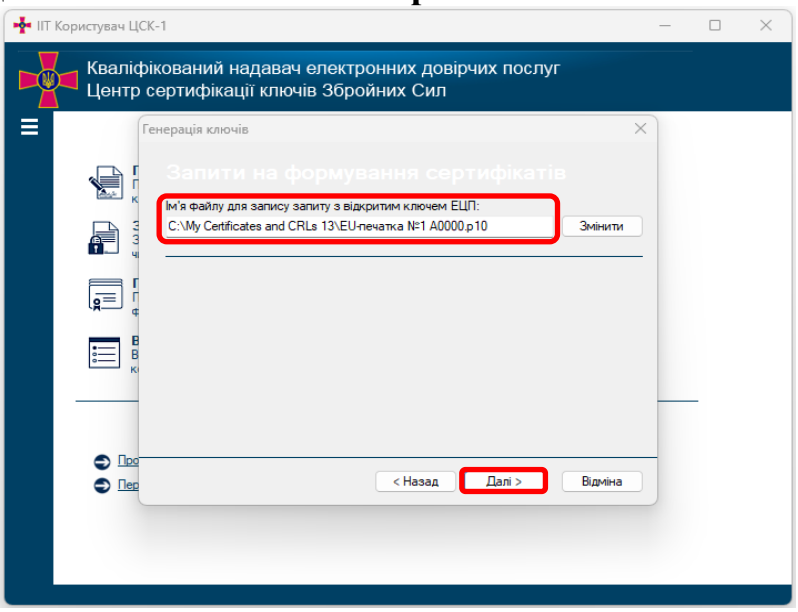

Рисунок 3.39

У наступному вікні (рис. 3.40) необхідно завершити генерацію ключів. Сформований файл запиту на формування сертифікатів можна знайти за посиланням, яке було вказано при генерації (рис. 3.39).

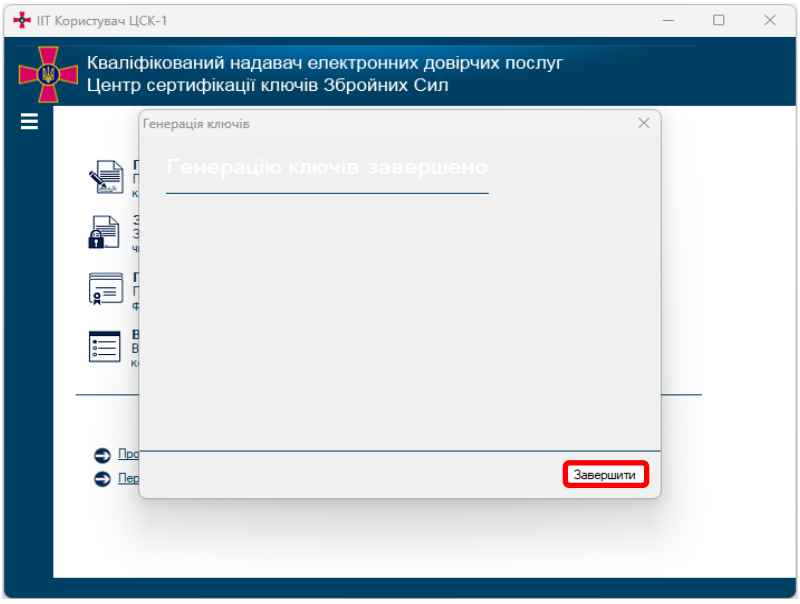

Рисунок 3.40

Файл відкритого ключа, разом з комплектом реєстраційних документів, може подаватись до КНЕДП ЗС України або його ВПР підписувачем або відповідальною особою у відповідності до пункту 4.1 Додатку 2 до Регламенту роботи КНЕДП ЗС .

4. ЗАВАНТАЖЕННЯ КВАЛІФІКОВАНИХ СЕРТИФІКАТІВ ВІДКРИТИХ КЛЮЧІВ

Щоб завантажити кваліфіковані сертифікати відкритих ключів через ПЗ необхідно обрати меню, в ньому пункт **“**Сертифікати та СВС**”** та підпункт **“**Отримати з ЦСК…**”** (рис. 4.1).

ВАЖЛИВО! Для завантаження кваліфікованих сертифікатів необхідно підключення робочого місця на якому установлено ПЗ до мережі ІСД “Інтернет” або АСУ ЗС України “Дніпро”.

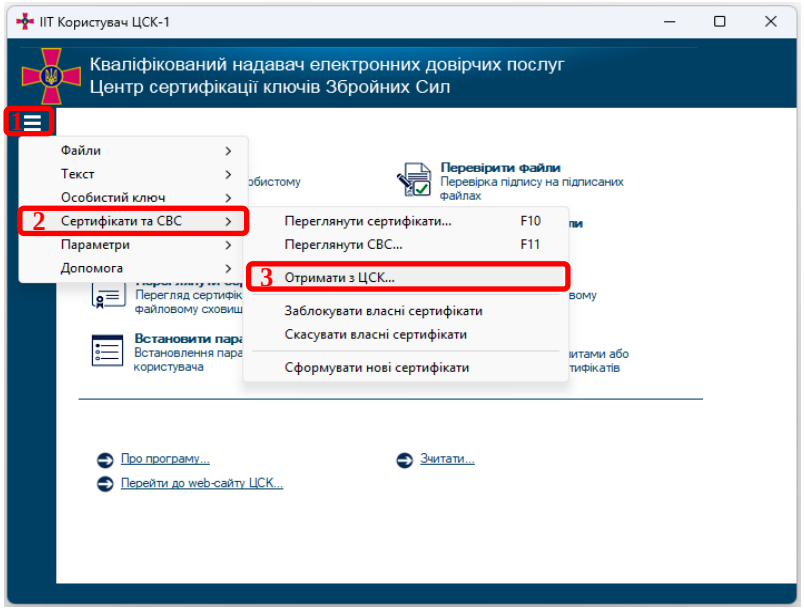

Рисунок 4.1

Для підтвердження отримання набору сертифікатів за особистим ключем чи власним сертифікатом з ЦСК натиснути “Так” (рис. 4.2).

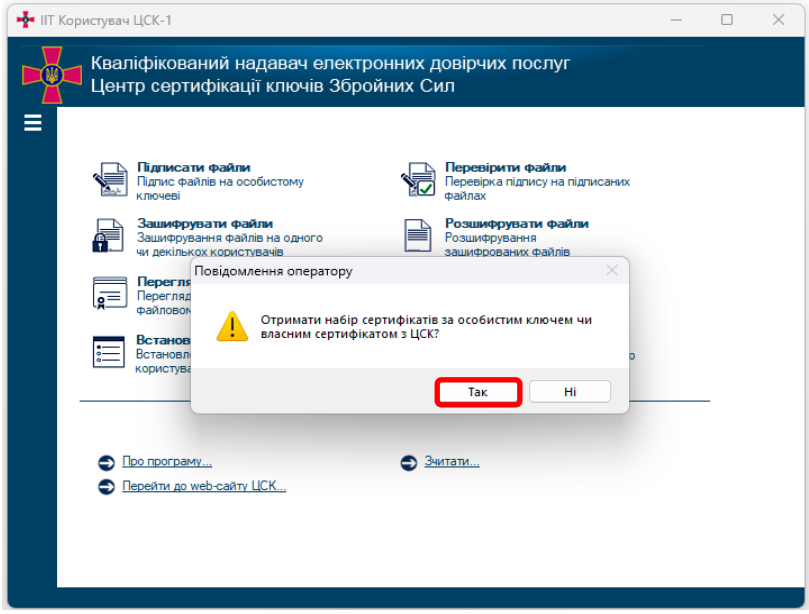

Рисунок 4.2

На наступній сторінці необхідно обрати ЗКЕП, на який записаний особистий ключ КЕП, ввести пароль доступу до нього та зчитати його (рис. 4.3).

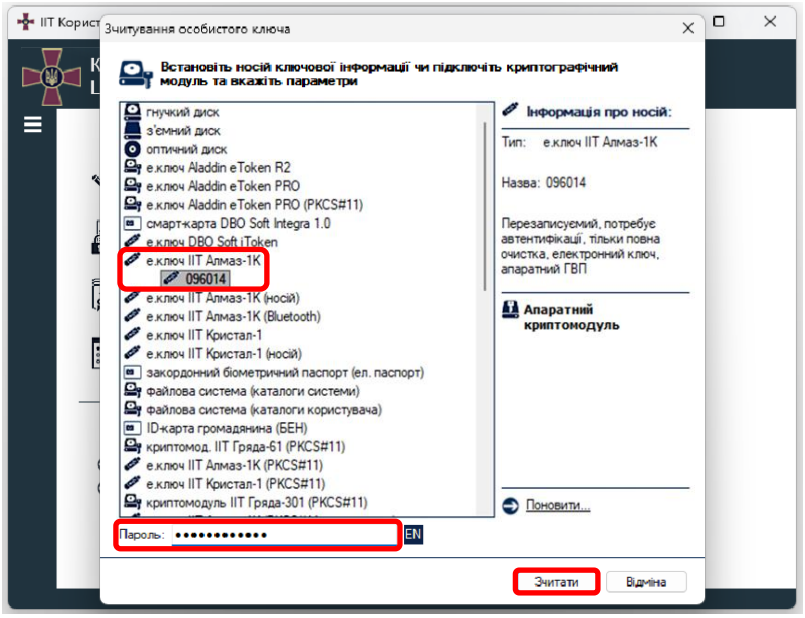

Рисунок 4.3

На наступній сторінці система запропонує завантажити сертифікати та інсталювати їх у файлове сховище сертифікатів на ПК, необхідно обрати “Так” (рис. 4.4).

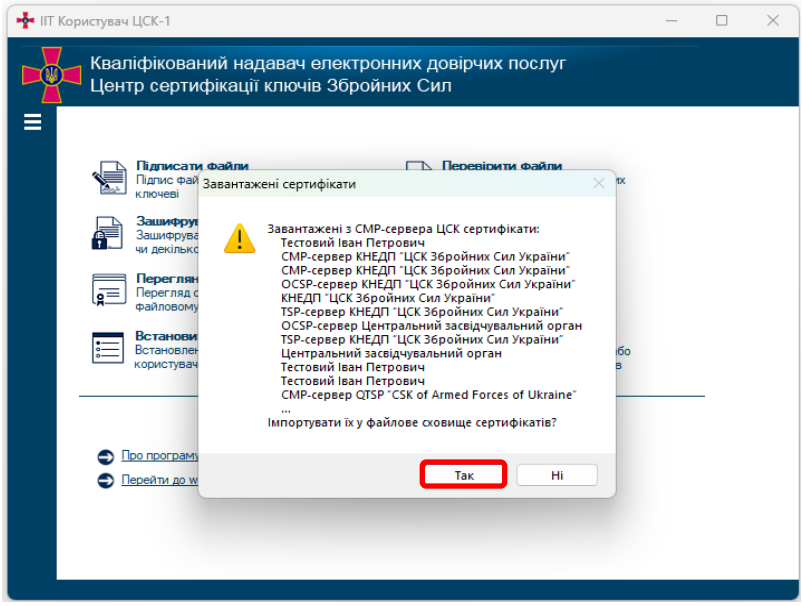

Рисунок 4.4

5. ЗЧИТУВАННЯ ОСОБИСТОГО КЛЮЧА

Зчитування особистого ключа може бути виконано шляхом вибору пункту “Зчитати” в стартовому меню ПЗ (рис. 5.1) або вибору в пункті меню “Особистий ключ” підпункту “Зчитати” (рис. 5.2).

ВАЖЛИВО! Для зчитування особистого ключа необхідно підключення робочого місця на якому установлено ПЗ до мережі ІСД “Інтернет” або АСУ ЗС України “Дніпро”.

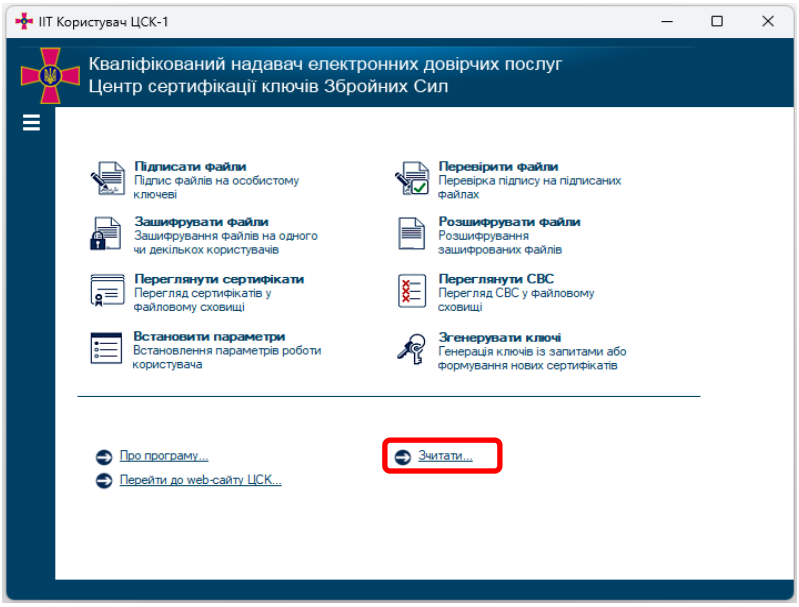

Рисунок 5.1

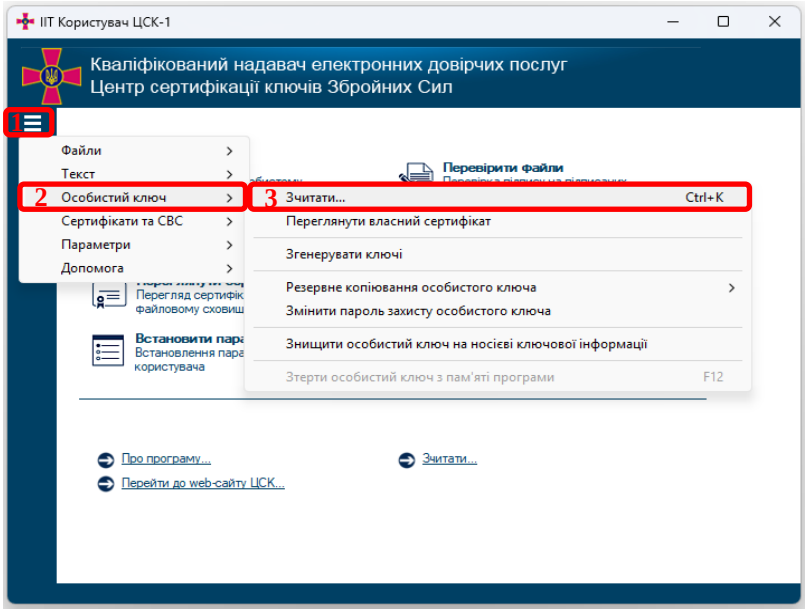

Рисунок 5.2

Після появи захищеного робочого столу (рис. 5.3), необхідно обрати ЗКЕП, ввести пароль захисту особистого ключа та натиснути “Зчитати”.

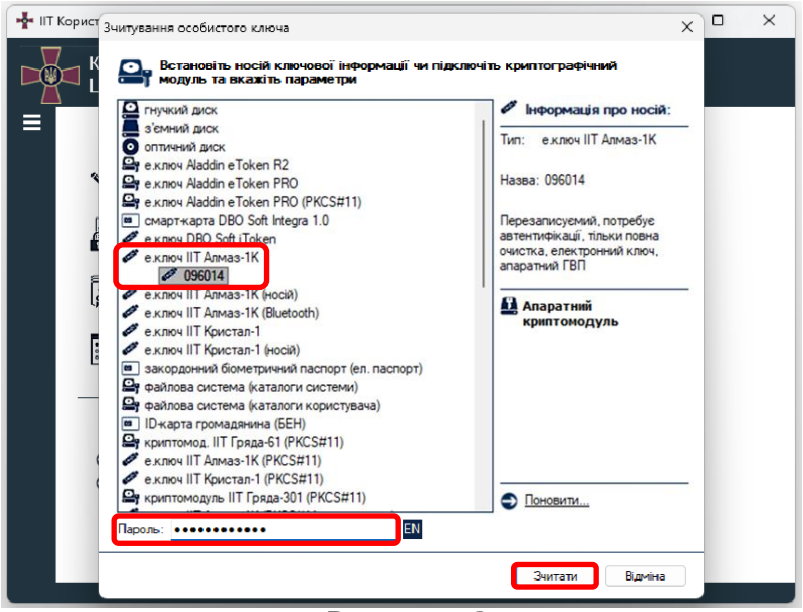

Рисунок 5.3

Інформація про те, що особистий ключ зчитаний та знаходиться в пам’яті ПК відображається внизу на панелі стартового меню ПЗ (рис. 5.4).

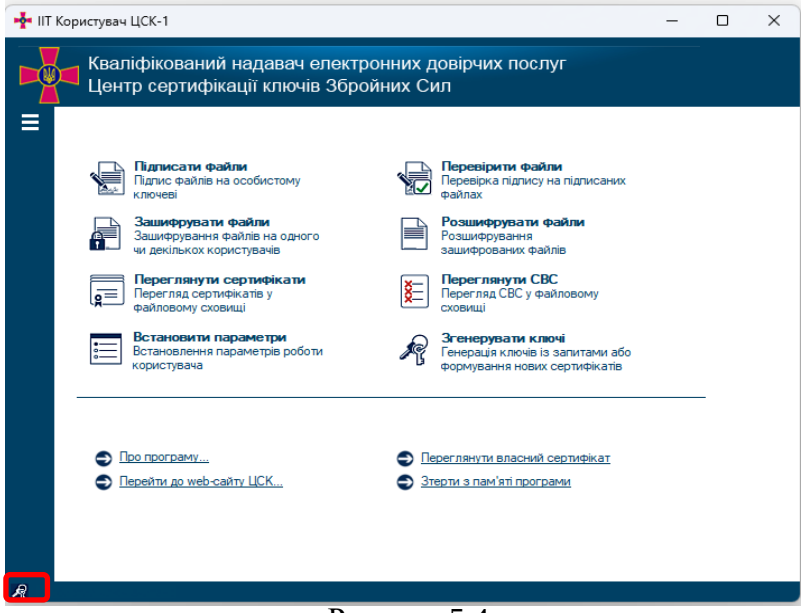

Рисунок 5.4

За необхідності підписувач може переглянути власні сертифікати та інформацію, що в них міститься. Для цього необхідно обрати пункт “Переглянути власний сертифікат” (рис. 5.5 та рис. 5.6).

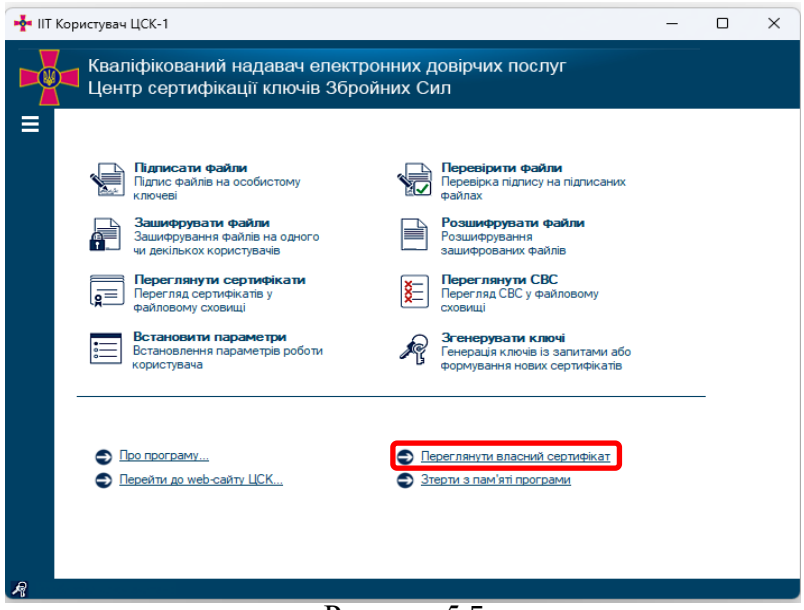

Рисунок 5.5

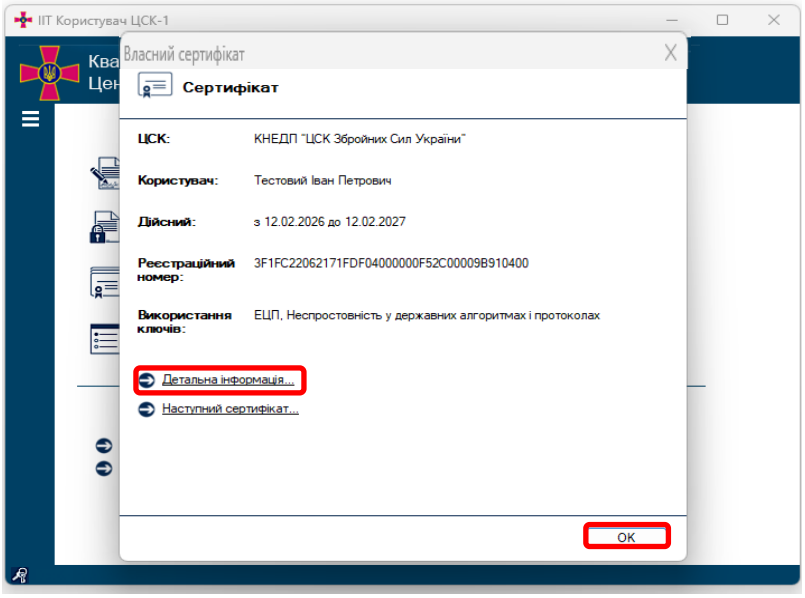

Рисунок 5.6

6. ЗМІНА ПАРОЛЮ ЗАХИСТУ ОСОБИСТОГО КЛЮЧА

Для зміни паролю захисту особистого ключа на ЗКЕП необхідно обрати меню, в ньому пункт “Особистий ключ” та підпункт “Змінити пароль захисту особистого ключа” (рис. 6.1).

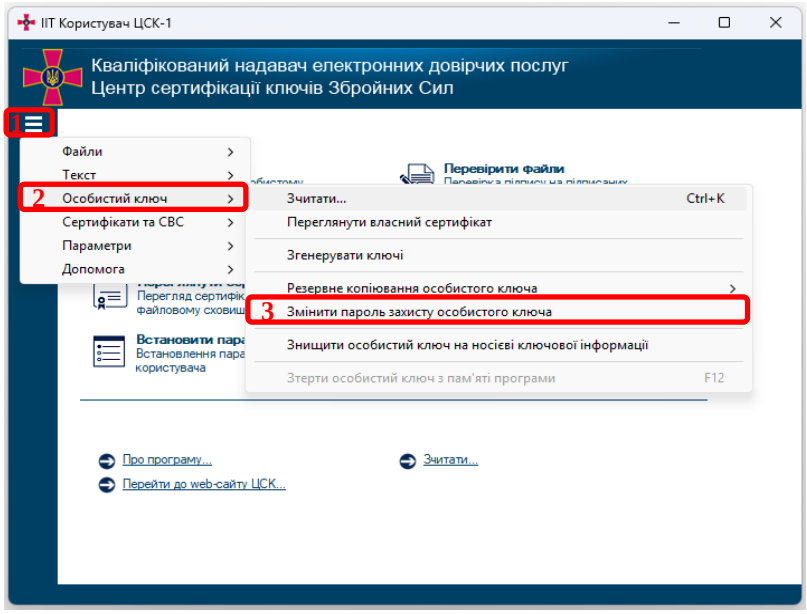

Рисунок 6.1

Далі необхідно встановити ЗКЕП та на наступній сторінці (рис. 6.2) вказати (обрати):

– тип ЗКЕП;

– серійний номер ЗКЕП;

– існуючий пароль захисту особистого ключа;

– новий пароль захисту особистого ключа (з підтвердженням).

Зміна паролю захисту особистого ключа КЕП здійснюється в режимі “Апаратний криптомодуль”.

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 розкладки клавіатури;

– дозволені символи – 'a-z', 'A-Z', '0-9', '+', '-'.

Примітка: такі вимоги носять рекомендаційний характер.

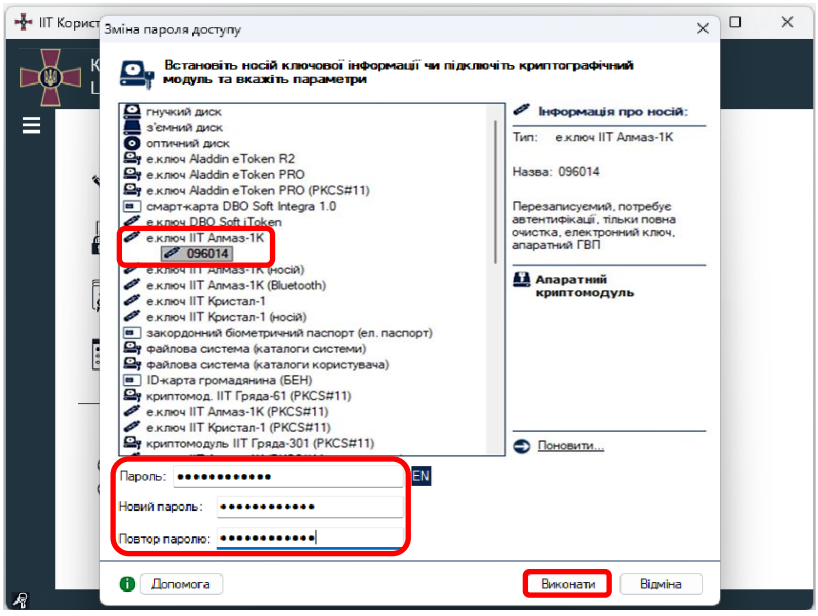
Зміна пароля доступу
Встановіть носій ключової інформації чи підключіть криптографічний модуль та вкажіть параметри
гнучкий диск
з'ємний диск
оптичний диск
е.ключ Aladdin eToken R2
е.ключ Aladdin eToken PRO
е.ключ Aladdin eToken PRO (PKCS#11)
смарт-карта DBO Soft Integra 1.0
е.ключ DBO Soft iToken
е.ключ IIT Алмаз-1K
096014
е.ключ IIT Алмаз-1K (носій)
е.ключ IIT Алмаз-1K (Bluetooth)
е.ключ IIT Кристал-1
е.ключ IIT Кристал-1 (носій)
закордонний біометричний паспорт (ел. паспорт)
Файлова система (каталоги системи)
Файлова система (каталоги користувача)
ID-карта громадянина (БЕН)
криптомод. IIT Гряда-61 (PKCS#11)
е.ключ IIT Алмаз-1K (PKCS#11)
е.ключ IIT Кристал-1 (PKCS#11)
криптомодуль IIT Гряда-301 (PKCS#11)
Інформація про носій:
Тип: е.ключ IIT Алмаз-1K
Назва: 096014
Перезаписуємий, потребує автентифікації, тільки повна очистка, електронний ключ, апаратний ГВП
Апаратний криптомодуль
Поновити...
EN
Пароль:
Новий пароль:
Повтор паролю:
Допомога
Виконати
Відміна

Рисунок 6.2

7. БЛОКУВАННЯ КВАЛІФІКОВАНИХ СЕРТИФІКАТІВ ВІДКРИТИХ КЛЮЧІВ

Під блокуванням кваліфікованих сертифікатів розуміється тимчасове призупинення їх чинності. Після блокування кваліфікованих сертифікатів, підписувач може протягом 30 календарних днів поновити свої кваліфіковані сертифікати. Блоковані кваліфіковані сертифікати будуть автоматично скасовані ІКС КНЕДП ЗС України, якщо протягом зазначеного строку підписувач не поновить їх чинність.

ВАЖЛИВО! Для здійснення блокування кваліфікованих сертифікатів необхідно підключення робочого місця на якому установлено ПЗ до мережі ІСД “Інтернет” або АСУ ЗСУ “Дніпро”.

Щоб заблокувати кваліфіковані сертифікати у ПЗ необхідно обрати меню, в ньому пункт **“**Сертифікати та СВС**”** та підпункт “Заблокувати власний сертифікат” (рис. 7.1).

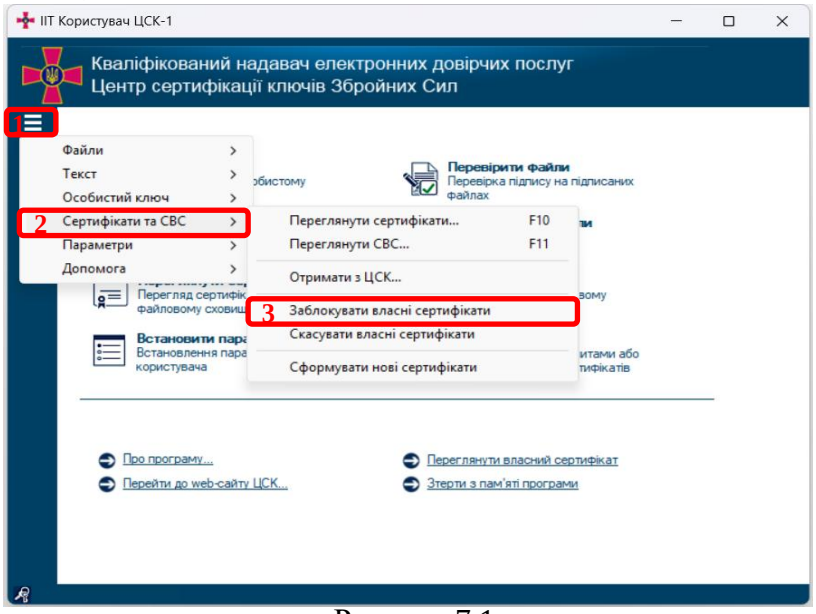

Рисунок 7.1

В наступному вікні надійде повідомлення про блокування кваліфікованих сертифікатів. Для підтвердження блокування натискаємо “Так” (рис. 7.2).

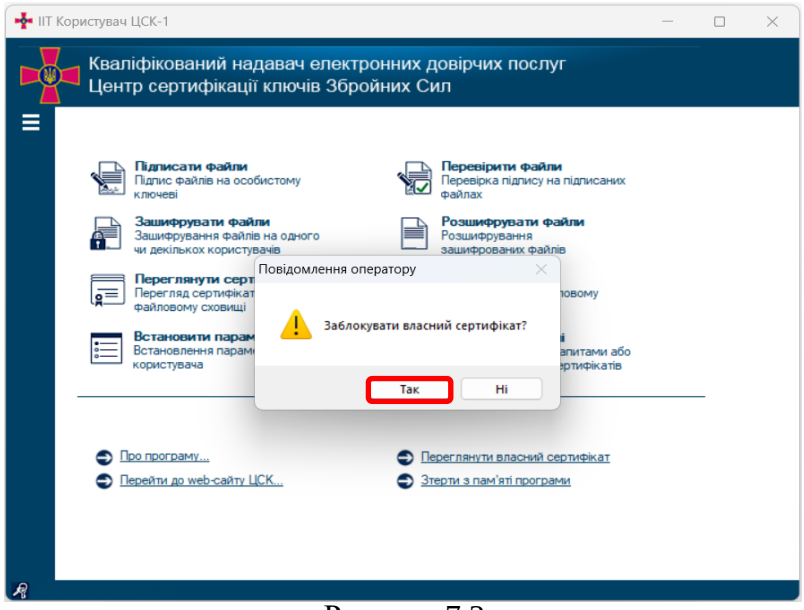

Рисунок 7.2

Після появи захищеного робочого столу необхідно обрати ЗКЕП та ввести пароль захисту до особистого ключа (рис. 7.3).

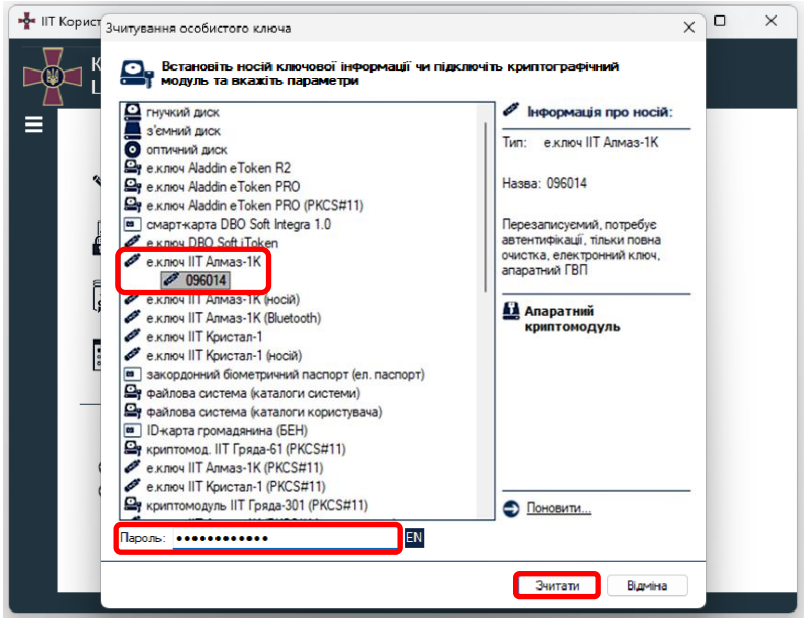

Рисунок 7.3

В наступному вікні отримаємо повідомлення з запитом про підтвердження блокування кваліфікованих сертифікатів відкритих ключів. Для підтвердження блокування натискаємо “Так” (рис. 7.4).

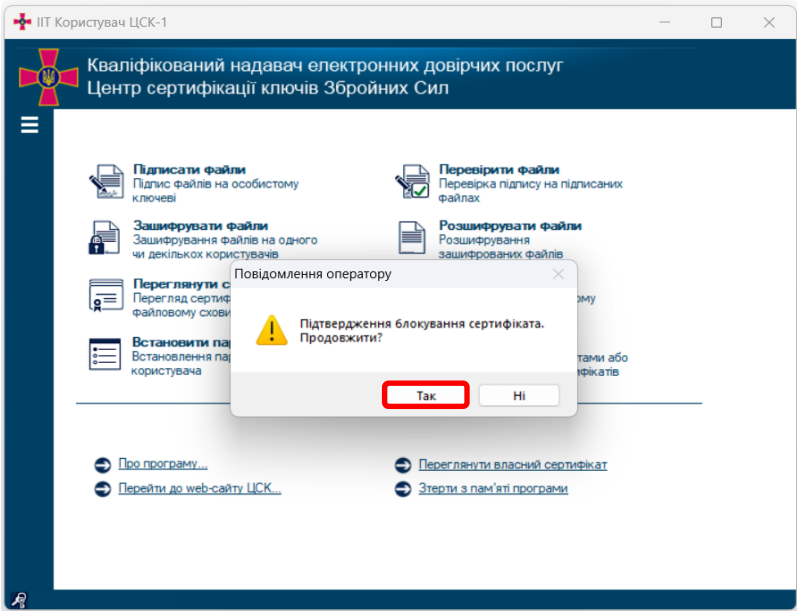

Рисунок 7.4

На наступній сторінці надійде повідомлення, що запит оброблено, кваліфіковані сертифікати відкритих ключів заблоковано. Треба натиснути “ОК” (рис. 7.5).

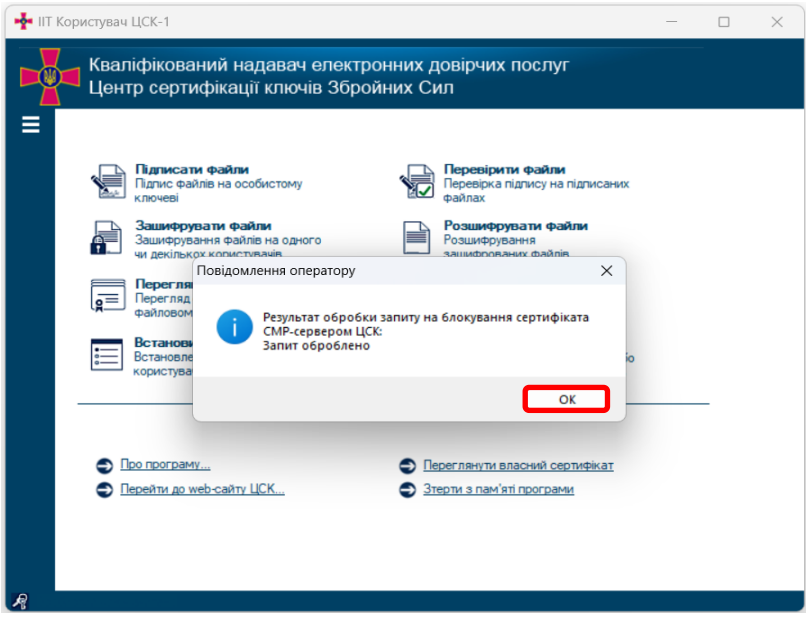

Рисунок 7.5

8. СКАСУВАННЯ КВАЛІФІКОВАНИХ СЕРТИФІКАТІВ ВІДКРИТИХ КЛЮЧІВ

Під скасуванням кваліфікованих сертифікатів відкритих ключів розуміється зупинення їх чинності.

ВАЖЛИВО! Для здійснення скасування кваліфікованих сертифікатів відкритих ключів необхідно підключення робочого місця на якому установлено ПЗ до мережі ІСД “Інтернет” або АСУ ЗС України “Дніпро”.

Для скасування кваліфікованих сертифікатів відкритих ключів у ПЗ необхідно обрати меню, в ньому пункт “Сертифікати та СВС” та підпункт “Скасувати власні сертифікати”(рис. 8.1).

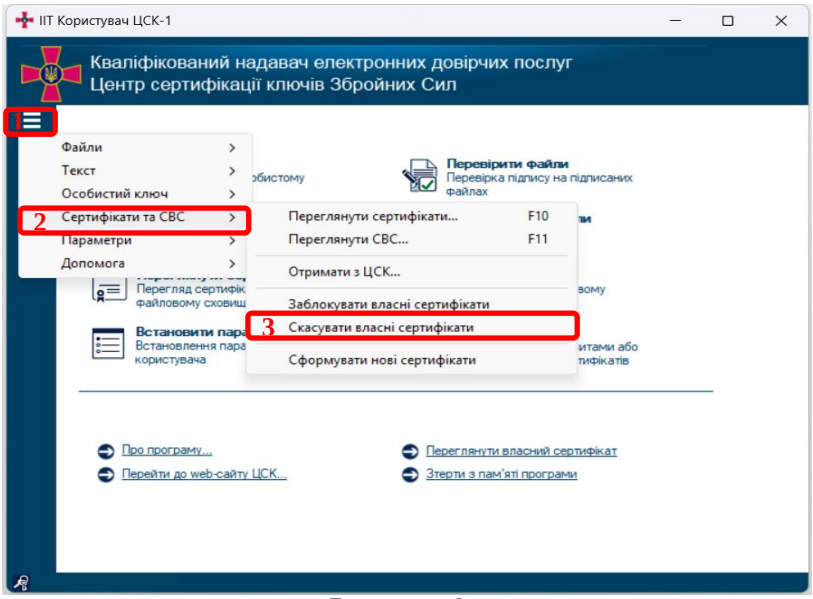

Рисунок 8.1

В наступному вікні надійде повідомлення щодо скасування кваліфікованих сертифікатів. Для підтвердження скасування натискаємо “Так” (рис. 8.2).

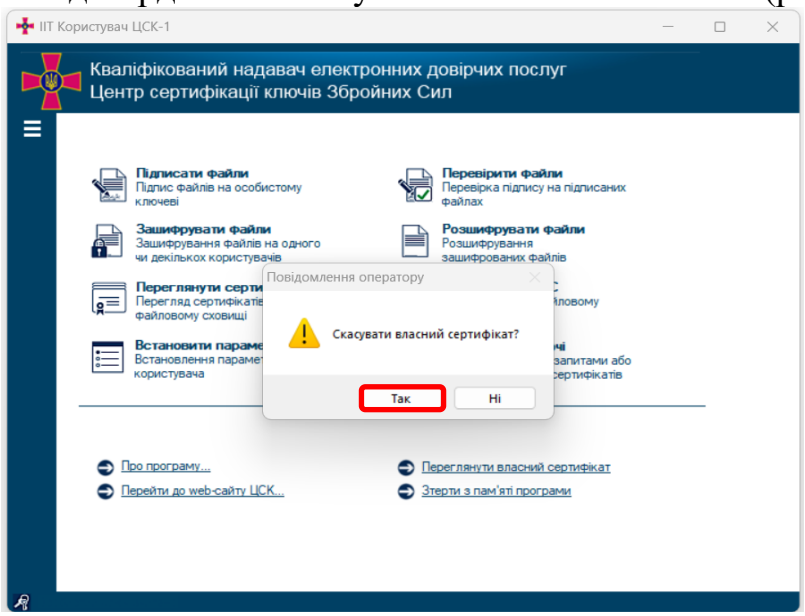

Рисунок 8.2

Після появи захищеного робочого столу необхідно обрати ЗКЕП та ввести пароль захисту до особистого ключа (рис. 8.3).

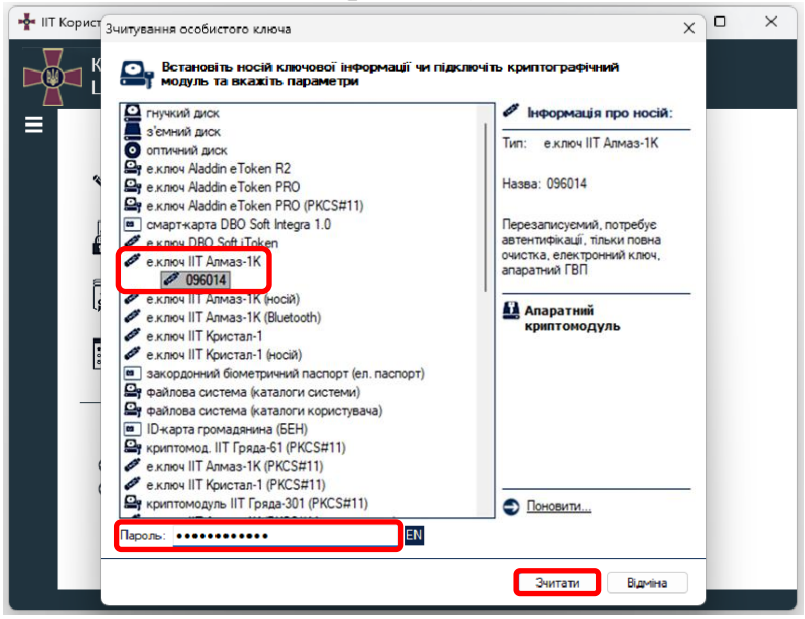

Рисунок 8.3

В наступному вікні отримаємо повідомлення з запитом про підтвердження скасування кваліфікованих сертифікатів відкритих ключів. Для підтвердження скасування натискаємо “Так” (рис. 8.4).

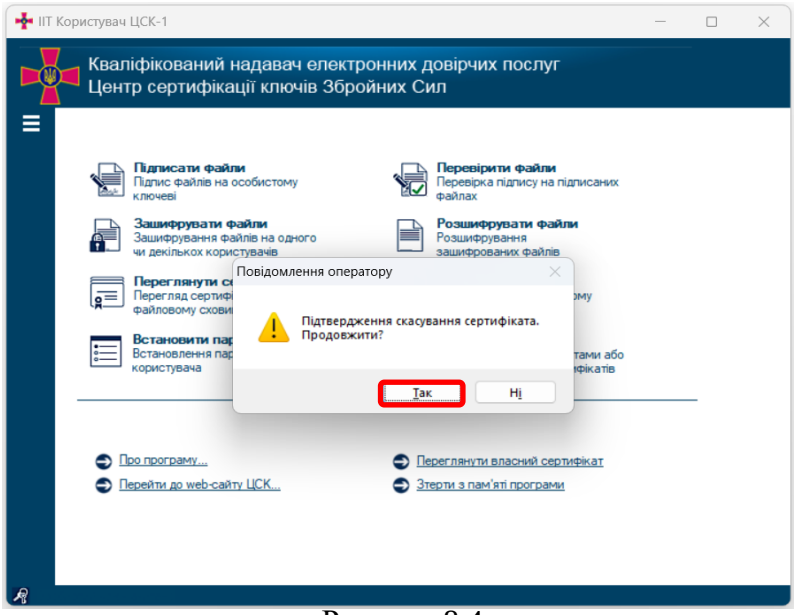

Рисунок 8.4

На наступній сторінці отримаємо повідомлення, що запит оброблено, кваліфіковані сертифікати відкритих ключів скасовано. Треба натиснути “ОК” (рис. 8.5).

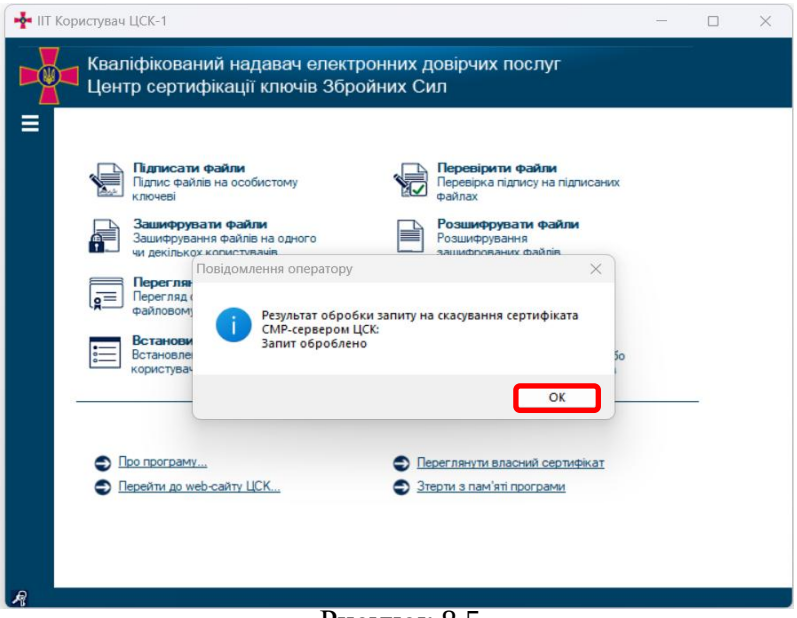
ІІТ Користувач ЦСК-1
Кваліфікований надавач електронних довірчих послуг
Центр сертифікації ключів Збройних Сил
Підписати файли
Підпис файлів на особистому ключеві
Перевірити файли
Перевірка підпису на підписаних файлах
Зашифрувати файли
Зашифрування файлів на одного чи декількох користувачів
Розшифрувати файли
Розшифрування зашифрованих файлів
Повідомлення оператору
Результат обробки запиту на скасування сертифіката СМР-сервером ЦСК:
Запит оброблено
OK
Про програму...
Перейти до web-сайту ЦСК...
Переглянути власний сертифікат
Зтерти з пам'яті програми

Рисунок 8.5

9. ПЕРЕВІРКА НАЯВНОСТІ ОСОБИСТИХ КЛЮЧІВ

Для перевірки наявності ключової інформації на ЗКЕП необхідно обрати меню, в ньому пункт “Параметри” та підпункт “Встановити” (рис. 9.1).

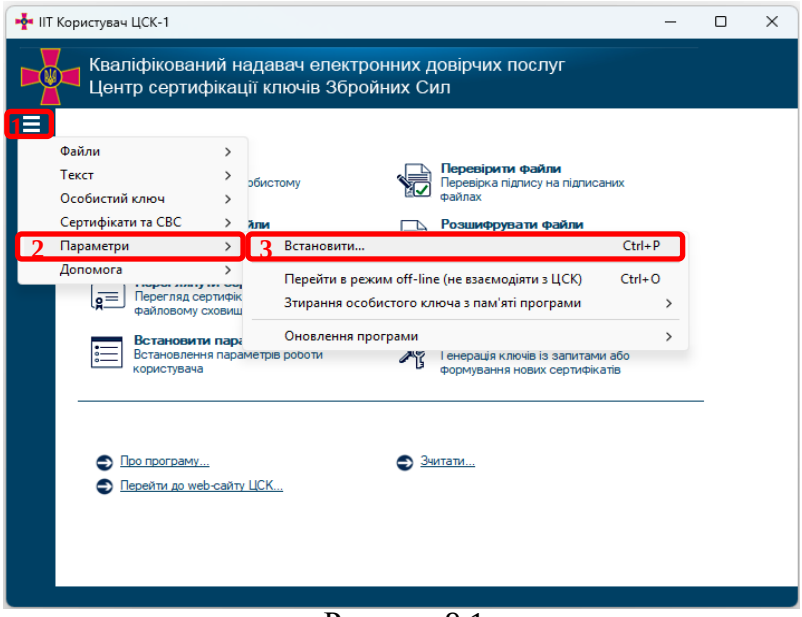

Рисунок 9.1

Далі необхідно обрати розділ “Особистий ключ” та натиснути “Інформація” (рис. 9.2).

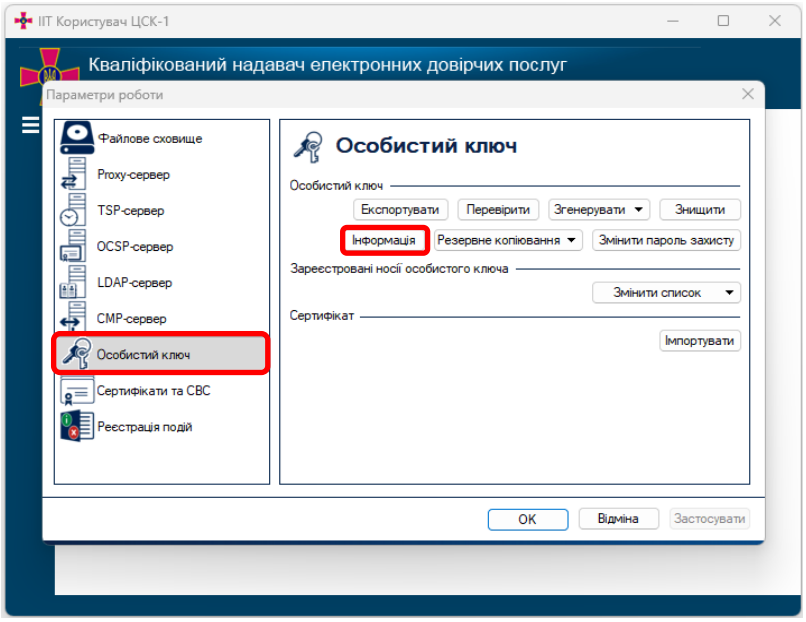

Рисунок 9.2

Після виконання попередніх кроків зявиться захищений робочий стіл на якому необхідно обрати ЗКЕП та ввести пароль захисту до особистого ключа (рис. 9.3).

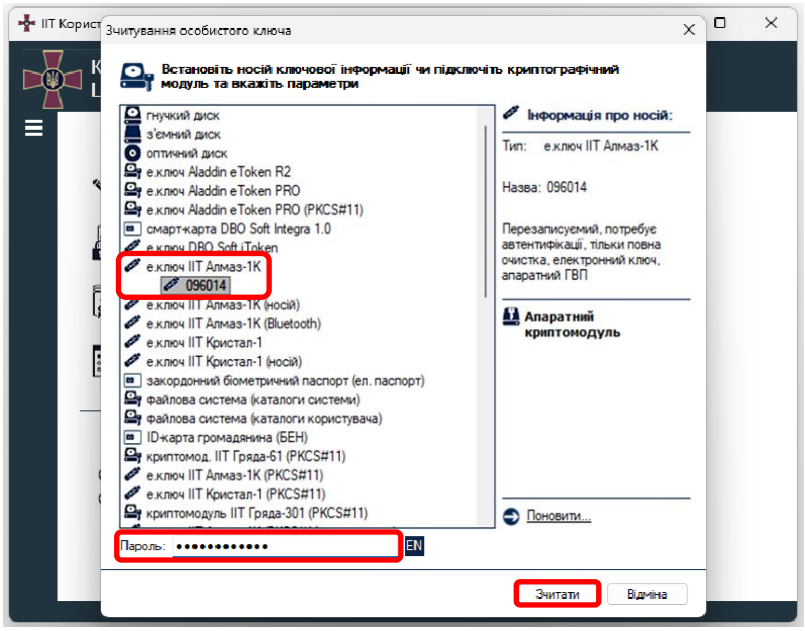

Рисунок 9.3

Якщо особистий пароль введено вірно, то на екрані з'явиться перелік особистих ключів, що знаходяться на ЗКЕП (рис. 9.4).

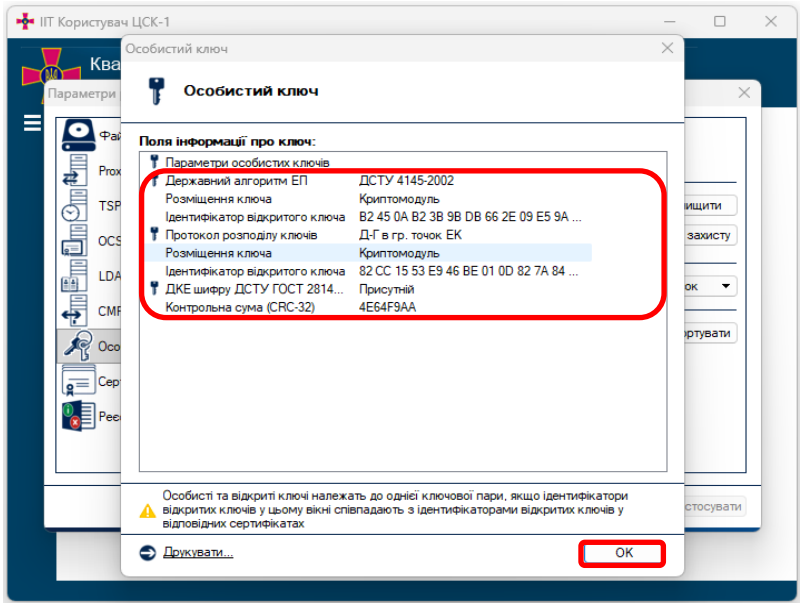

Рисунок 9.4

Начальник центру сертифікації ключів військової частини А0136
підполковник Володимир СОРОЧАК