САЙФЕР
Системы защиты информации
Интернет-банкинг

САЙФЕР ПРО, ТОВ
04107, Київ, вул. Нагірна 25/27, 3-ій поверх

Тел.: +38 (044) 484-4612
Факс: +38 (044) 483-0322
E-mail: info@cipher.com.ua
Web: www.cipher.com.ua

Дата модифікації: 14.07.2021

42125815.001.IE.36

Система криптографічного захисту інформації "Шифр-X.509"

Модуль роботи з ключовим контейнером. Керівництво з експлуатації

Зміст

Список скорочень та умовних позначень

PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standards
PKCS#11	Cryptographic Token Interface Standard
PKI	Public-Key Infrastructure (Інфраструктура відкритих ключів)
TCP	Transmission Control Protocol
ЕП	Електронний підпис
МКМ	Мережний криптографічний модуль
МРКК	Модуль роботи з ключовим контейнером
ОС	Операційна система
ПЗ	Програмне забезпечення
ПТК	Програмно-технічний комплекс
СКЗІ	Система криптографічного захисту інформації
ЦЗО	Центральний засвідчувальний орган
ЦСК	Центр сертифікації ключів

Введення

Вступ

Даний документ є керівництвом користувача по роботі з Модулем роботи з ключовим контейнером, призначеного для роботи під управлінням ОС Windows 7 чи вище, у складі СКЗІ «Шифр-X.509» версія 2.

Системні вимоги

Апаратне забезпечення

Мінімальна апаратна конфігурація:

- Відповідає вимогам ОС Microsoft Windows 7.
- Вільного дискового простору: 20 Мб.
- Мережева карта: Fast Ethernet, IP v4.

Рекомендована апаратна конфігурація:

- Відповідає вимогам ОС Microsoft Windows 10.
- Вільного дискового простору: 1 Гб.
- Мережева карта: Gigabit Ethernet, IP v4.

Програмне забезпечення

Мінімальна конфігурація:

- Microsoft Windows 7.

Рекомендована конфігурація:

- Microsoft Windows 10.

Захищені ключові носії

Програма підтримує роботу із захищеними носіями, завдяки інтерфейсу PKCS#11, Таблиця 1.

Таблиця 1. Список підтримуваних захищених ключових носіїв

№	Виробник	Модель	Тип
1	ТОВ Автор, Україна	Author Secure Token-337	Token
2	ТОВ Автор, Україна	Author Secure SmartCard-336	SmartCard
3	ТОВ Мікрокрипт, Україна	Armorino	Token + Flash
4	Giesecke & Devrient, Німеччина	StarSign Crypto SmartCard	SmartCard
5	Giesecke & Devrient, Німеччина	StarSign Crypto USB Token	Token, Token + Flash
6	Технотрейд, Україна	uaToken	Token
7	ТОВ Авест Україна, Україна	Avest Key	Token
8	SafeNet, США	SafeNet Crypto eToken	Token
9	Gemalto, США	IDPrime Series	Token+SmartCard
10	ТОВ Ефіт технолоджіс, Україна	Efit Key	Token

Підготовка до роботи засобами Модуля роботи з ключовим контейнером

Попередні налаштування

У цьому розділі наведені обов'язкові та не обов'язкові дії для налаштування ОС перед встановленням основного ПЗ.

Встановлення ПЗ для роботи із захищеним носієм

Для роботи сервера із захищеними носіями, обов'язковим є встановлення драйвера захищеного ключового носія чи спеціального ПЗ користувача.

Після встановлення ПЗ для роботи із захищеними носіями, слід переконатися, що захищені носії знайдені ОС відображаються у «Диспетчере устройств». Для цього необхідно перейти «Пуск» -> «Control Panel» -> «Device Manager» -> «SmartCard Reader».

Якщо захищений носій не знайдений, слід звернутися до:

- Постачальника захищених носіїв.
- Розробника захищених носіїв.
- Розробника СКЗІ «Шифр-Х.509».

Подальша установка сервера можлива лише після повного усунення питань пов'язаних з коректною роботою захищених носіїв.

Встановлення

Для встановлення МРКК необхідно завершити всі невикористовувані задачі, після чого запустити файл **setup_CiX509_CtxViewer.exe** з інсталяційного носія та слідувати вказівкам програми зі встановлення.

Встановлення на сервер відбувається лише при наявності прав **Адміністратора домена** чи **Локального адміністратора**.

Після запуску **setup_CiX509_CtxViewer.exe**, з'являється стандартний діалог системи захисту ОС про дії, які можуть призвести до порушення функціонування ОС. Далі з'являється вікно з вибором мови для встановлення програмного забезпечення, у переліку мов доступні: українська та російська. У залежності від вибору мови, буде встановлено за замовчуванням мова при запуску Модуля роботи з ключовим контейнером, Рис. 1. За нагоди можна змінити у меню Сервіс – Мова інтерфейсу.

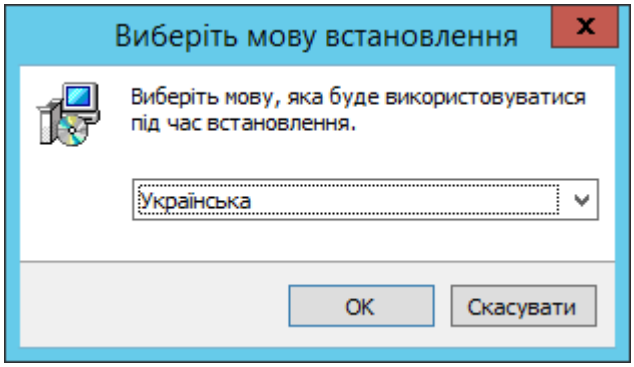

Рис. 1. Вибір мови встановлення

Слід обрати **Ок** для переходу до діалогу **Привітання**, Рис. 2.

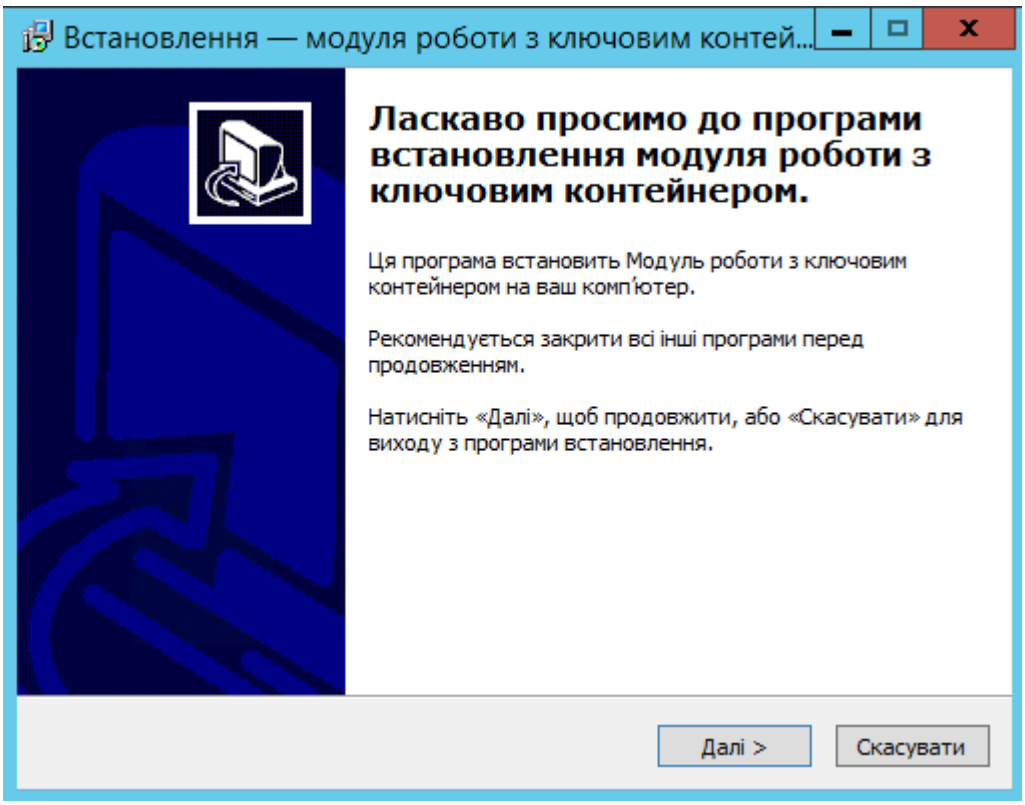

Рис. 2. Діалог Привітання

На діалозі **Привітання**, слід натиснути кнопку **Далі**, для переходу до наступного діалогу, Рис. 3, для ознайомлення з **Ліцензійна угода**, тобто з ліцензією про використання ПЗ. Для продовження установки слід прийняти дане погодження, явно указав **Я приймаю умови угоди**. Для переходу до наступного діалогу, необхідно натиснути кнопку **Далі**.

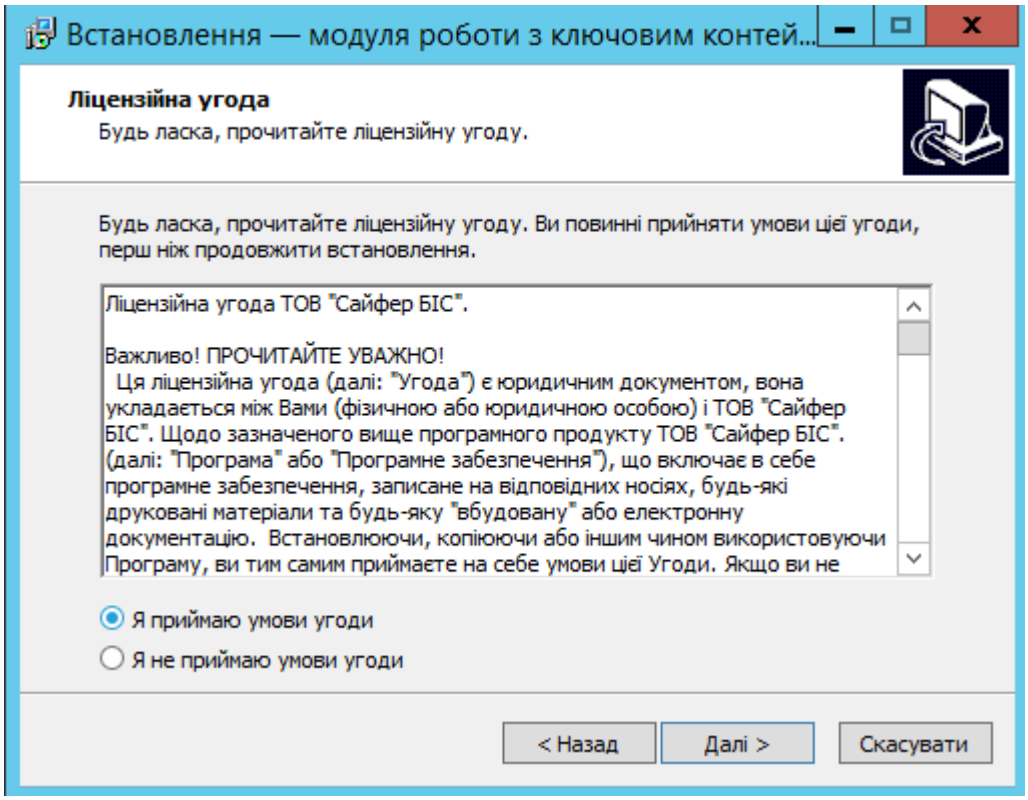

Рис. 3. Діалог з інформацією про ліцензії на використання ПЗ

Далі відображається діалог з пропозицією обрати **Вибір шляху встановлення**, куди буде встановлений МРКК, Рис. 4. Зараз під ОС Windows доступна лише 32-х розрядна версія МРКК.

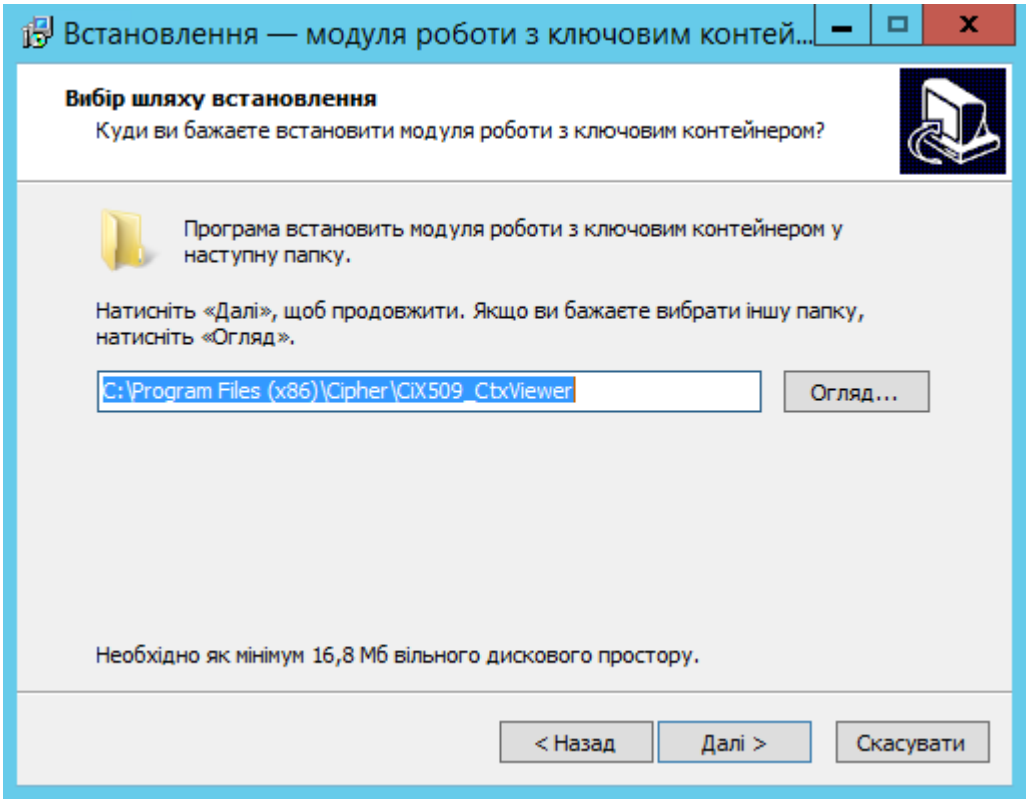

Рис. 4. Діалог вибору папки, для встановлення МРКК

Наступний діалог **Вибір папки в меню «Пуск»**, дозволить обрати в яку папку в меню «Пуск» будуть встановлені компоненти МРКК, Рис. 5.

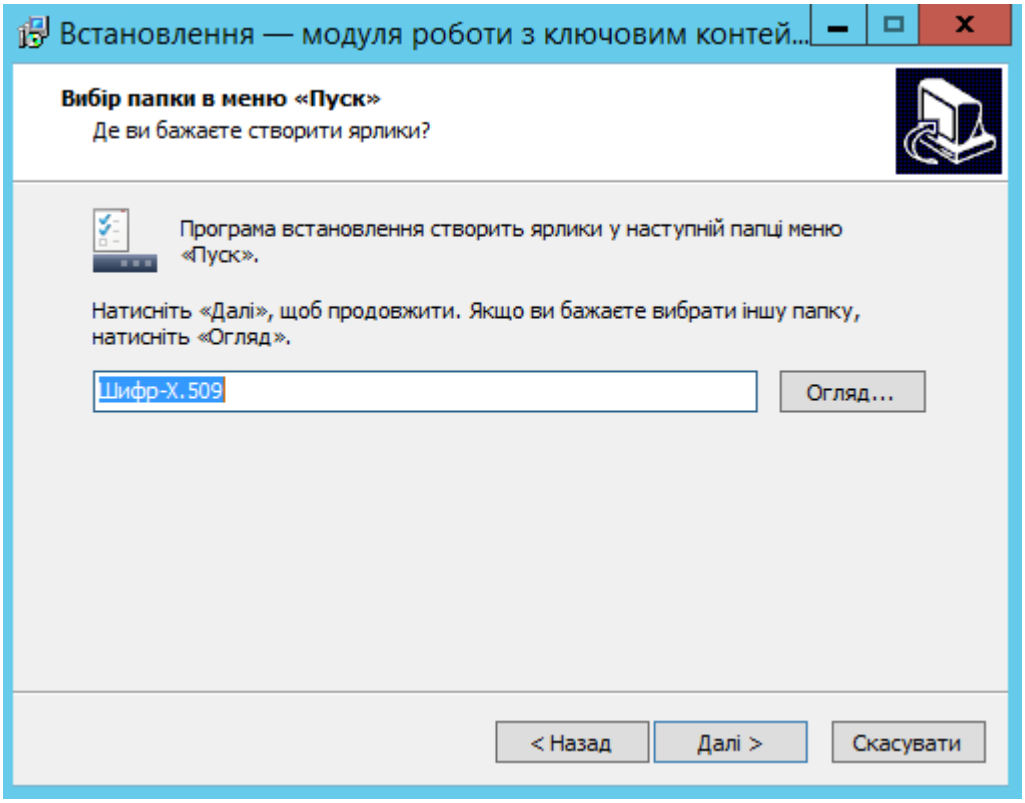

Рис. 5. Діалог вибору папки в меню «Пуск», для встановлення компонент МРКК

Наступний діалог **Вибір додаткових завдань**, дозволяє вказати, чи слід створювати ярлики застосування на робочому столі та створити файлові асоціації, Рис. 6.

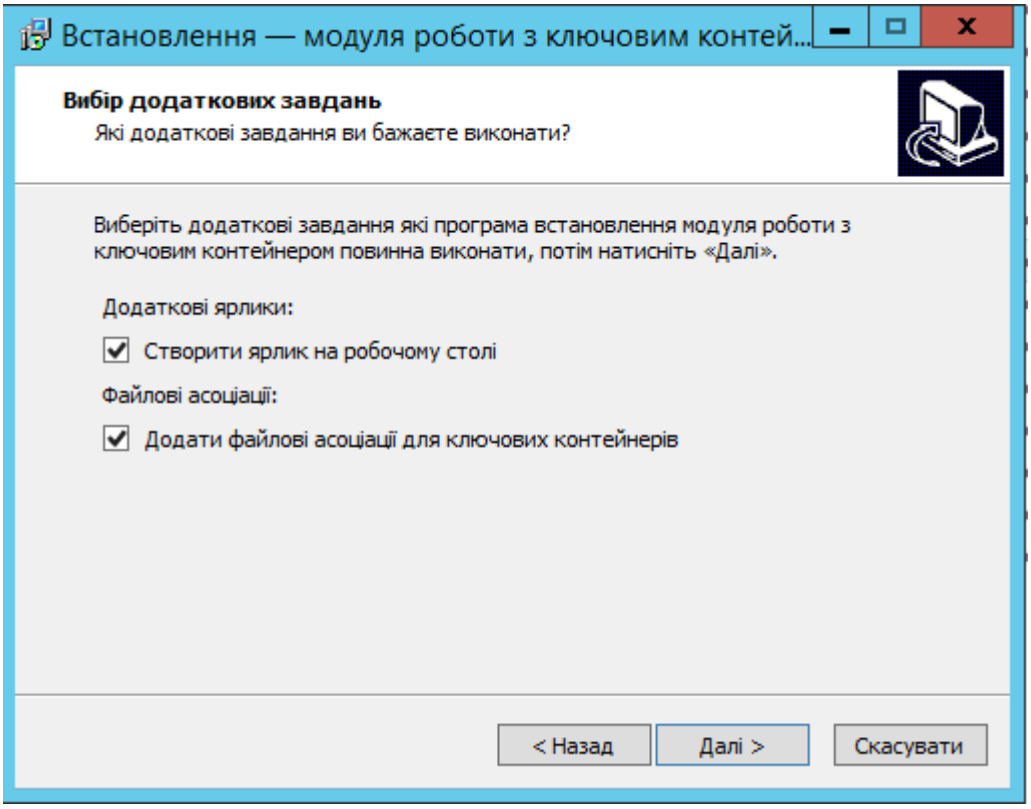

Рис. 6. Діалог вибору додаткових задач

Наступний діалог **Усе готово до встановлення**, дозволяє в одному місці побачити всі налаштування та безпосередньо приступити до копіювання файлів, Рис. 7, для початку встановлення слід натиснути кнопку **Встановити**.

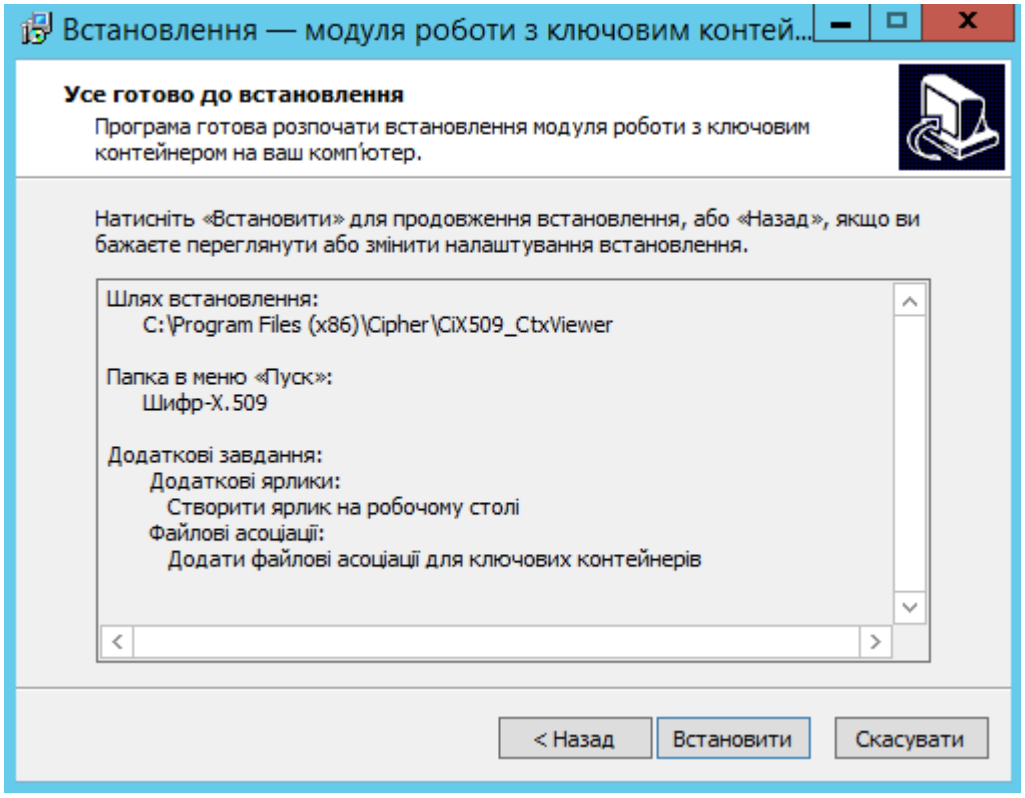

Рис. 7. Діалог перегляду налаштувань встановлення

Наступний діалог **Встановлення**, дозволяє продемонструвати процес копіювання файлів у систему користувача та налаштування застосування, Рис. 8. Процес встановлення можна перервати натисканням кнопки **Скасувати**.

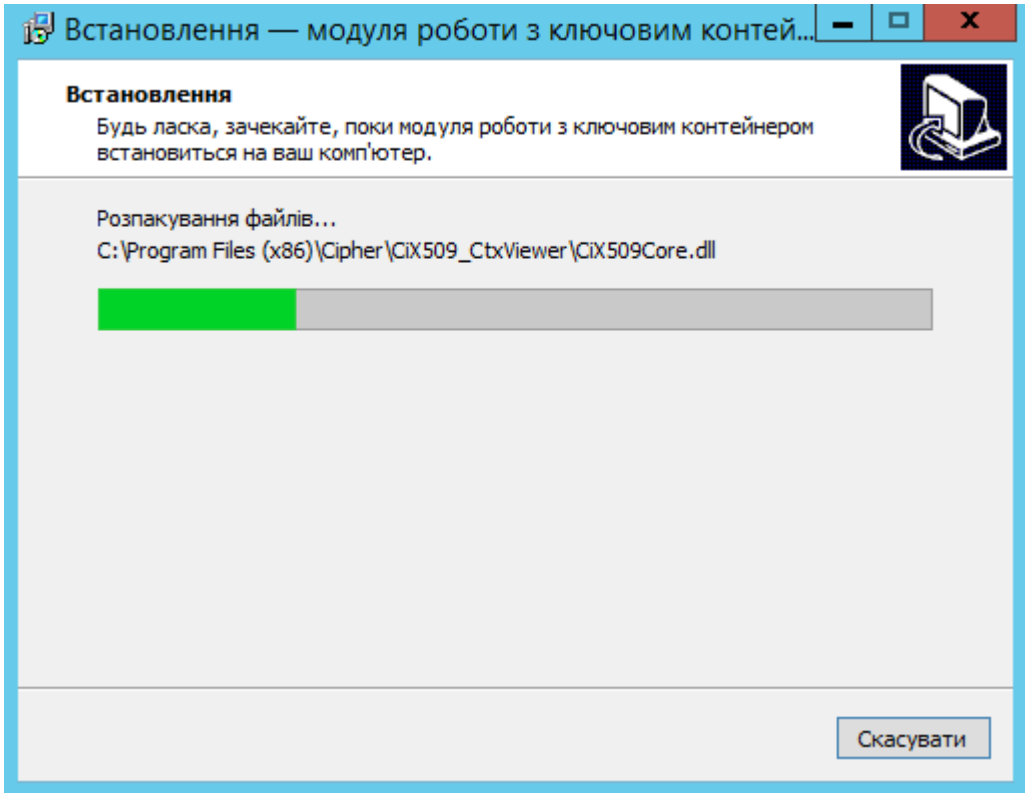

Рис. 8. Діалог відображення процесу встановлення МРКК

Після успішного копіювання файлів МРКК та наступного налаштування його для роботи в ОС, відображається діалог, з пропозицією провести запуск МРКК, Рис. 9.

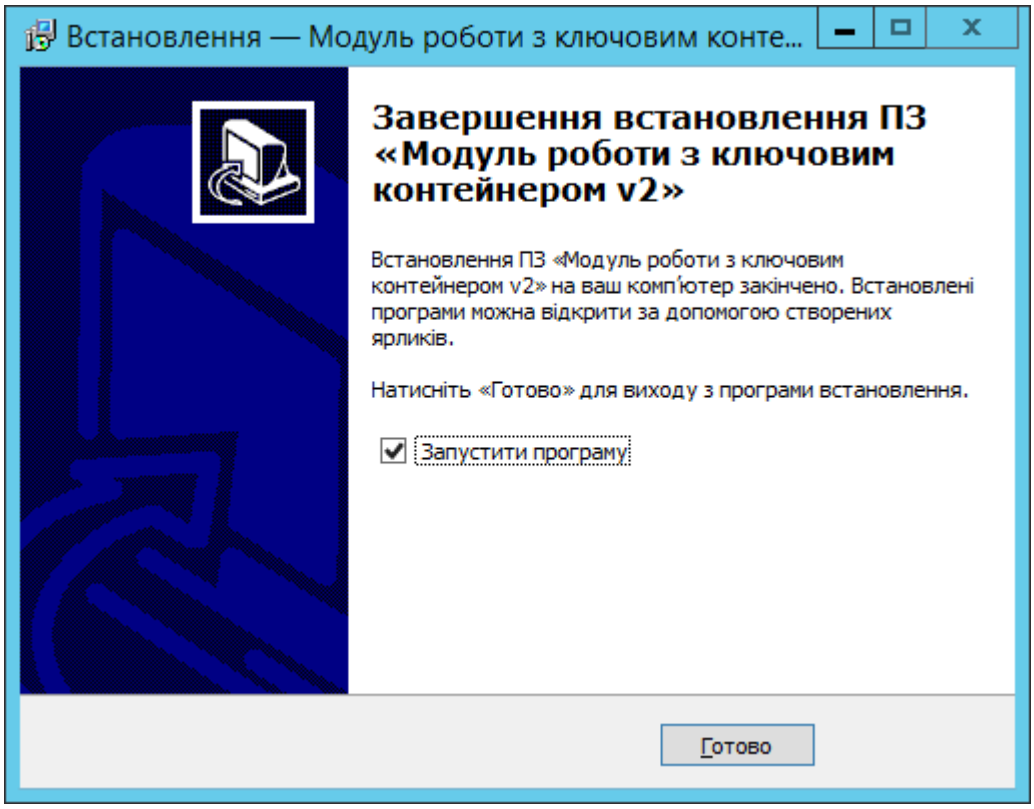

Рис. 9. Діалог завершення установки

Наявність необхідних даних перевіряється безпосередньо МРКК у процесі запуску, у випадку відсутності будь-яких налаштувань та відмові користувача виконувати дії для їх встановлення, програма припиняє свою роботу.

Робота з програмою

Запуск

Запуск МРКК здійснюється з меню «Пуск->Шифр-X.509->Модуль роботи з ключовим контейнером», Рис. 10.

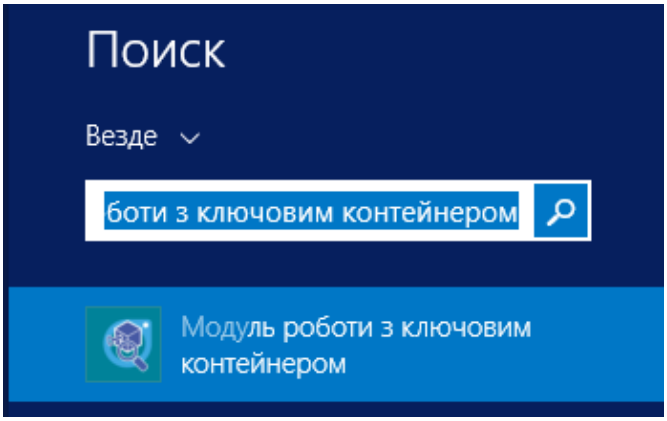

Рис. 10. Запуск модуля з меню «Пуск»

Після запуску Модуля, відображається діалог ключового контейнера та введення паролю для доступу до особистого ключа, Рис. 11.

Модуль дозволяє працювати, як з файловим ключовим контейнером, так із апаратним захищеним ключовим носієм та МКМ Шифр-HSM, реалізуючи інтерфейс PKCS#11.

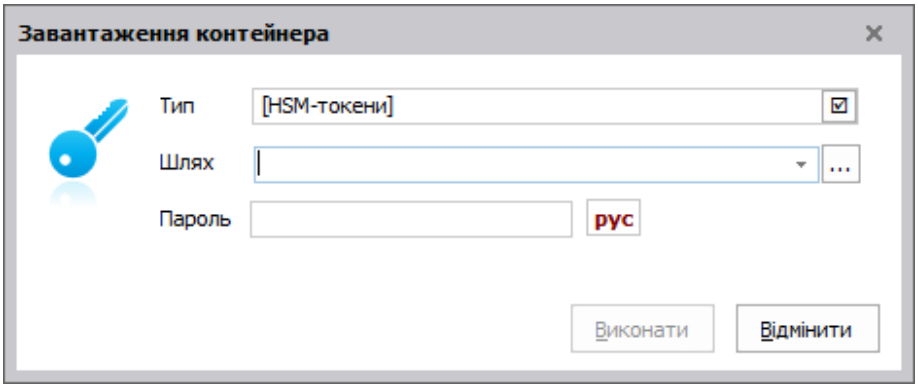

Рис. 11. Діалог вказівки типу ключового носія, а також введення паролю для доступу до особистого ключа

HSM-токени

За замовчуванням, завжди обраний тип ключового контейнера «HSM-токени», де ключовий контейнер знаходиться на МКМ Шифр-HSM, Рис. 12.

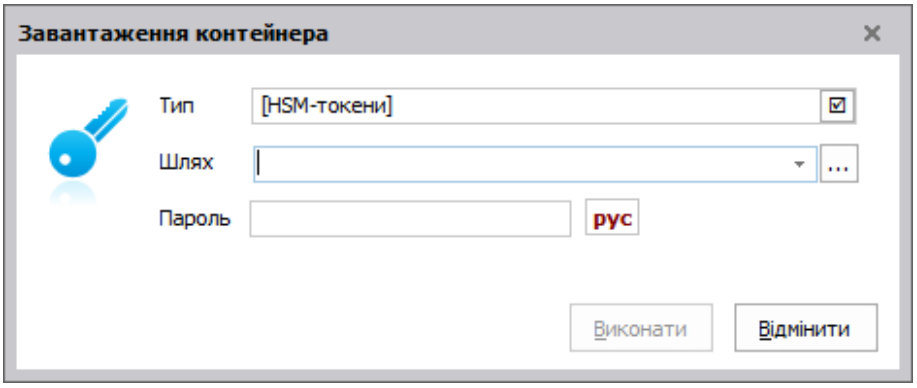

Рис. 12. Завантаження контейнера

Шлях до ключового контейнеру обирається через кнопку «…», далі відображається діалог вибору носія, Рис. 13.

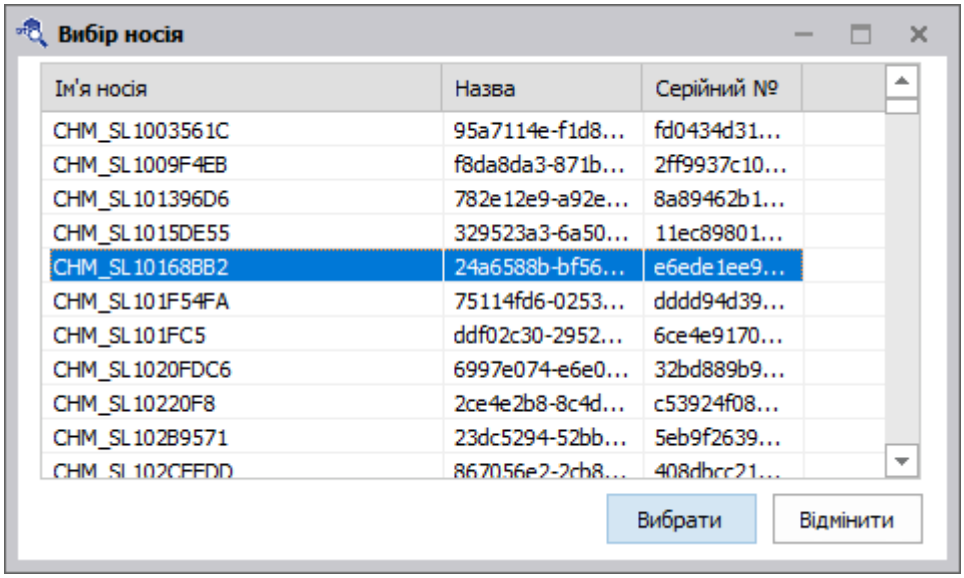

Рис. 13. Вибір носія

У пункті Шлях фіксується адреса слоту, **Рис. 14**.

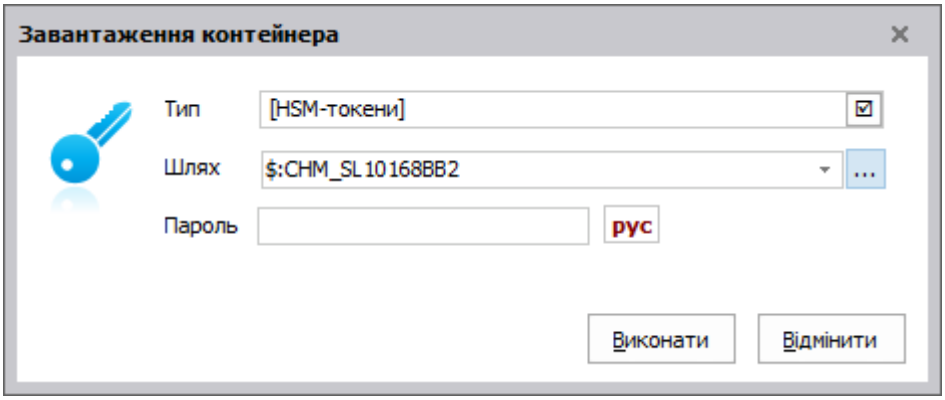

Рис. 14. Шлях до контейнеру

Вказівка пінкоду до ключового контейнеру, **Рис. 15**.

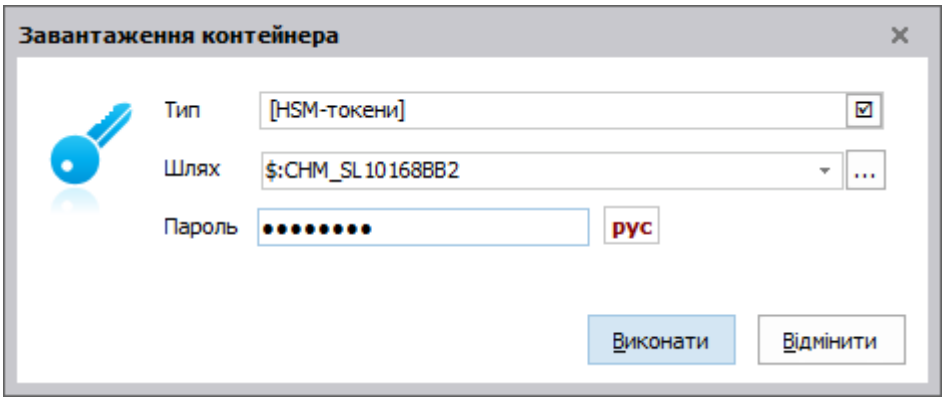

Рис. 15. Заповнення пінкоду до контейнеру

Після успішного заповнення полів, натискаємо на кнопку «Виконати» та отримуємо доступ до повної інформації, яка містить у контейнері, яку можна переглянути у короткому та докладному форматах, Рис. 16-Рис. 17.

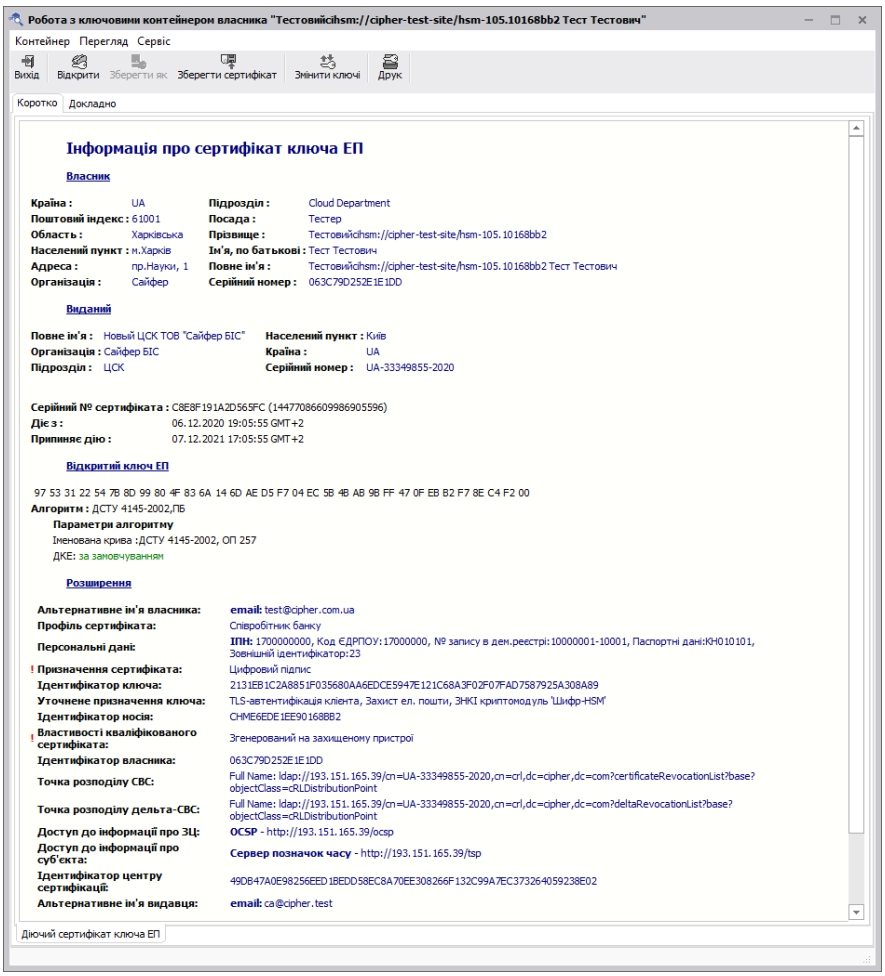

Рис. 16. Короткий опис

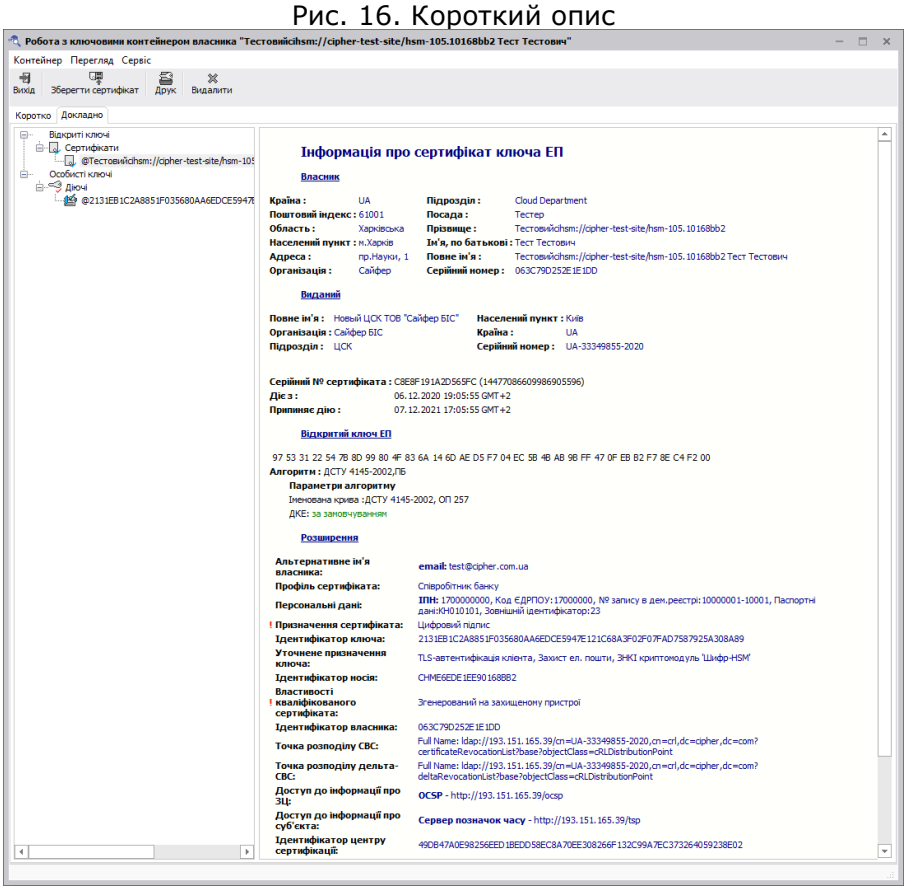

Рис. 17. Докладний опис

Активні/Пасивні PKCS#11-носії

Тип «Активні/Пасивні PKCS#11-носії», де розміщення ключового контейнеру безпосередньо на захищеному носії, який згенеровано в активному чи пасивному режимі, **відповідно, Рис. 18.**

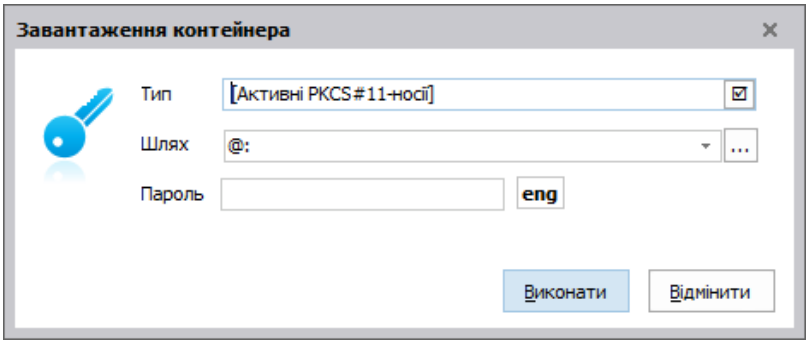

Рис. 18. Завантаження контейнера

Шлях до ключового контейнеру обирається через кнопку «…», далі відображається діалог вибору файлу, Рис. 19.

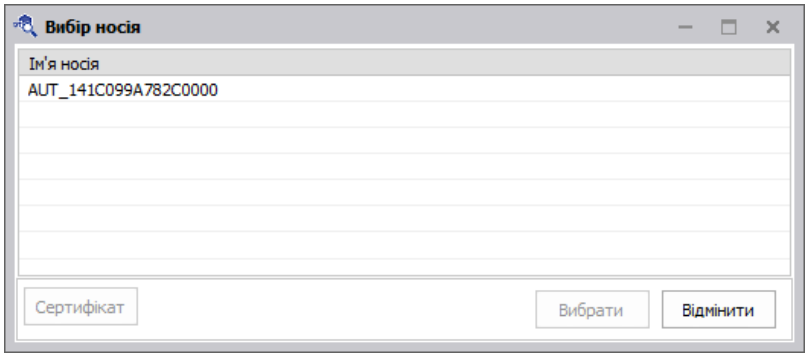

Рис. 19. Вибір носія

У пункті Шлях фіксується адреса слоту, Рис. 20.

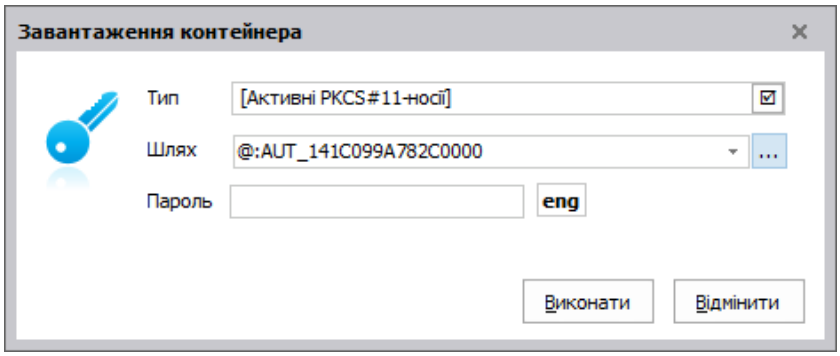

Рис. 20. Шлях до контейнеру

Вказівка пінкоду до ключового контейнеру, Рис. 21.

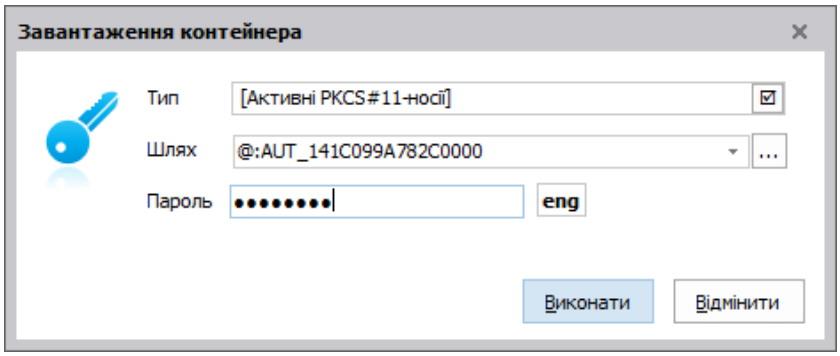

Рис. 21. Заповнення пінкоду до контейнеру

Після успішного заповнення полів, натискаємо на кнопку «Виконати» та отримуємо доступ до повної інформації, яка містить у контейнері, яку можна переглянути у короткому та докладному форматах, Рис. 22-Рис. 23.

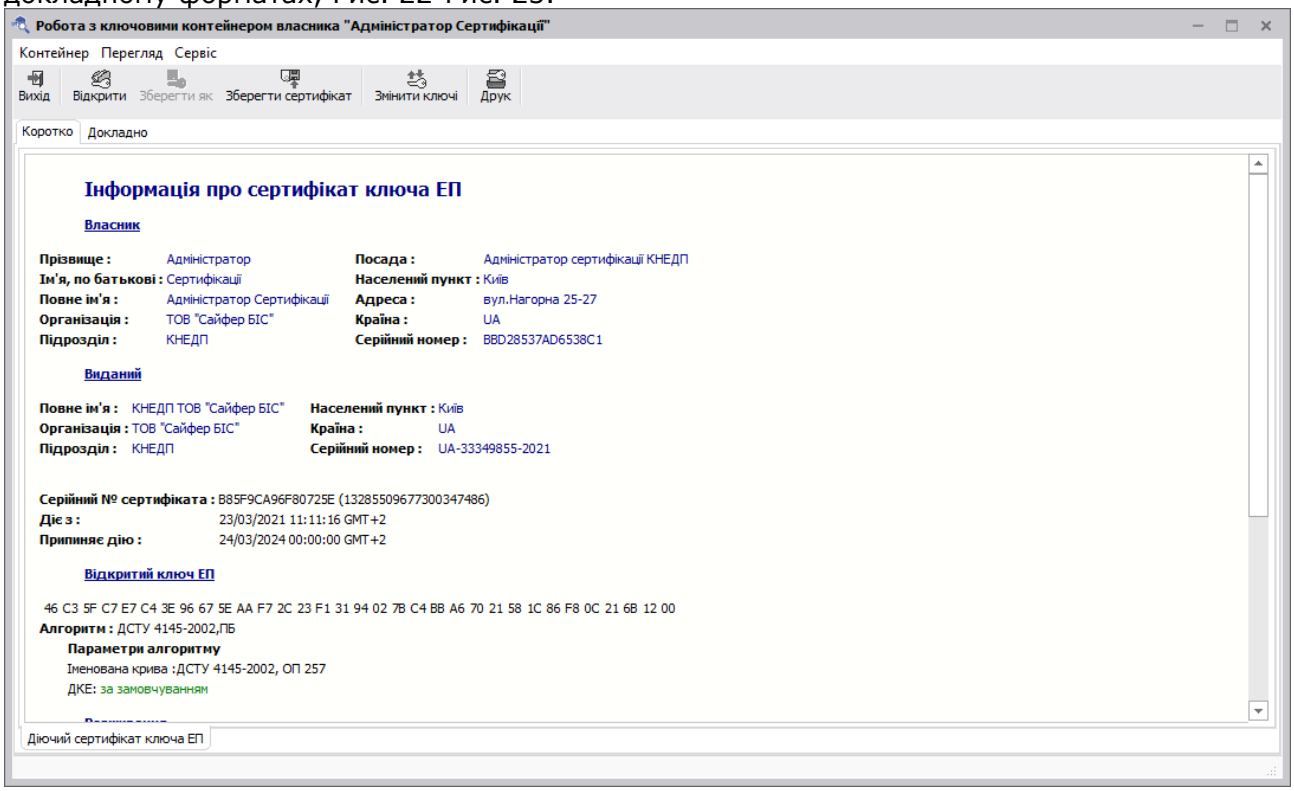

Рис. 22. Короткий опис

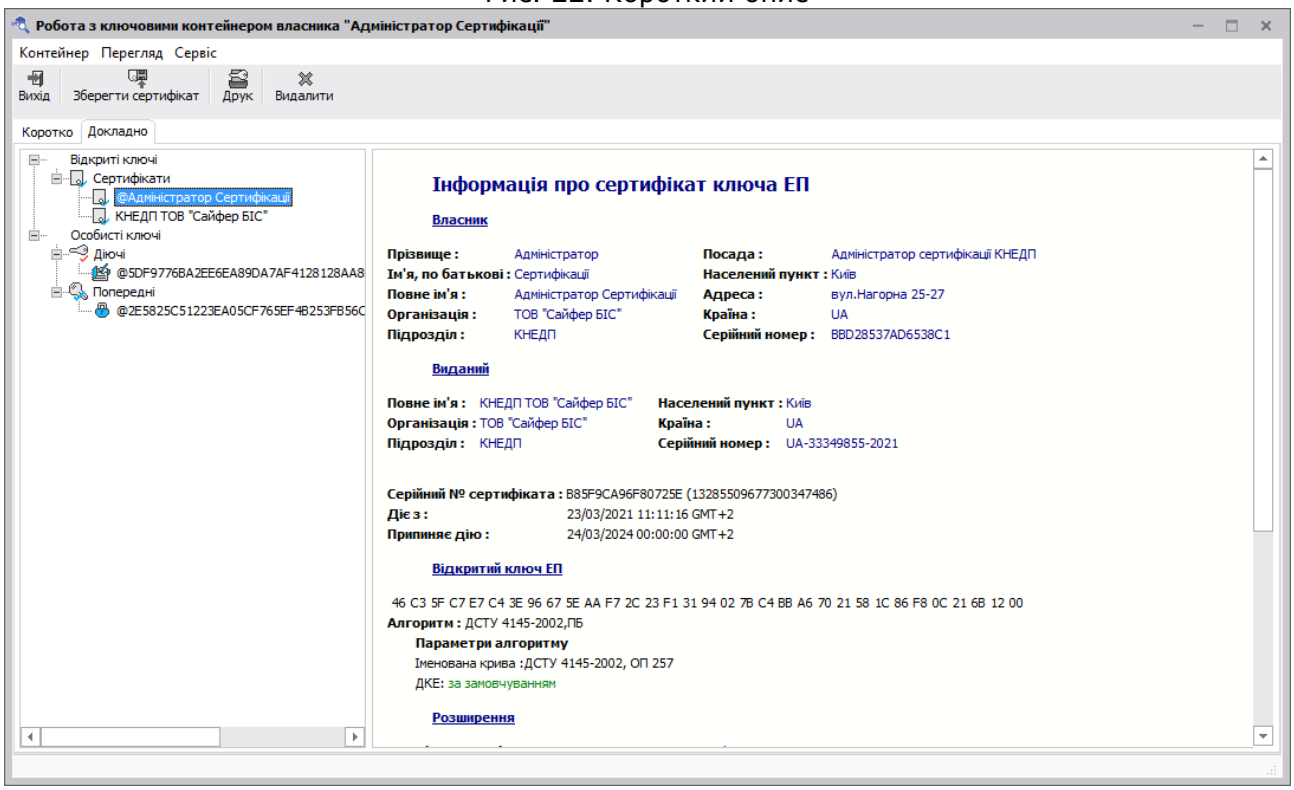

Рис. 23. Докладний опис

Для визначення, у якому режимі згенеровано ключ на захищений носій, звертаємо увагу на символ:

- Символ @ - означає активний режим.
- Символ # - означає пасивний режим.

Якщо ж символів немає, це є файловий контейнер.

Починаючи з версії 1.3.18.97 є можливість переглянути серійний номер захищеного носія на який записано даний контейнер.

Файл на диску

Тип «Файл на диску», де розміщення ключового контейнеру на диску комп'ютера чи на іншому (не захищеному) пристрої, Рис. 24.

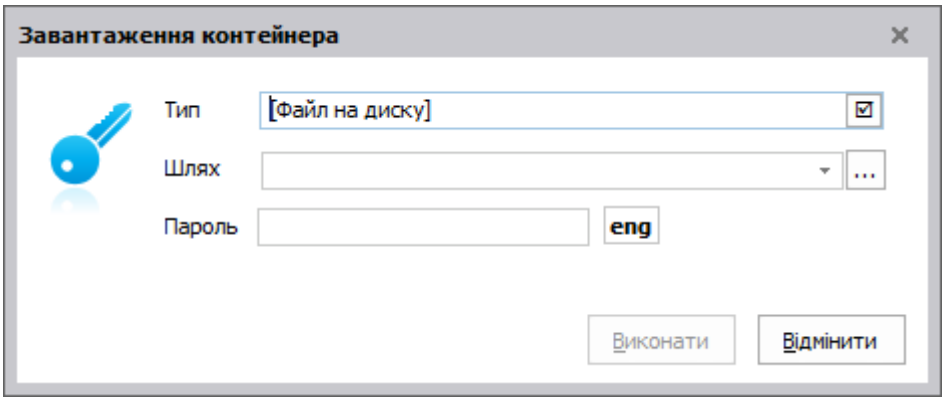

Рис. 24. Завантаження контейнера

Шлях до ключового контейнеру обирається через кнопку «…», далі відображається діалог вибору файлу, Рис. 25.

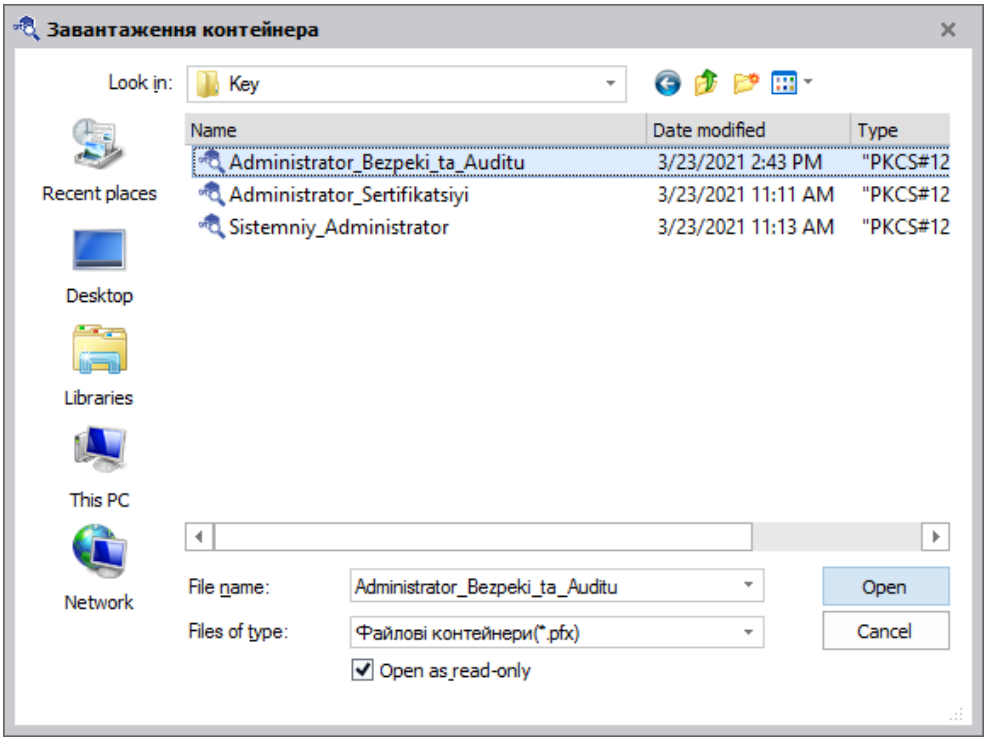

Рис. 25. Вибір файлового контейнера

У пункті Шлях фіксується адреса місцезнаходження файлового контейнеру, Рис. 26.

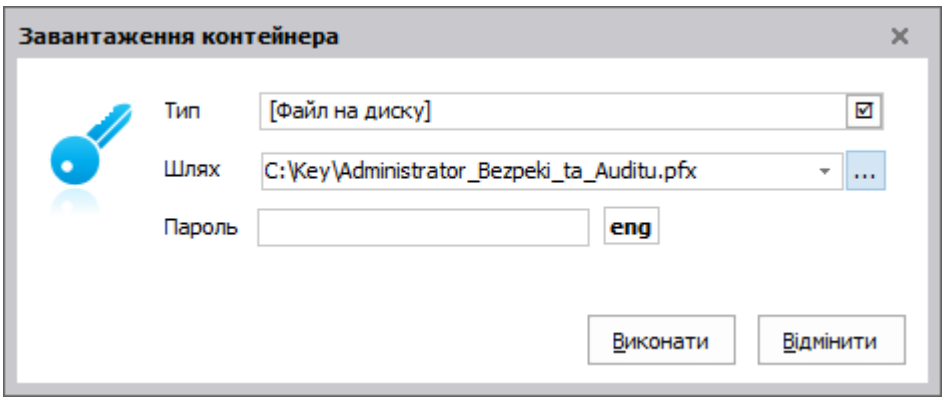

Рис. 26. Шлях до конетейнеру

Вказівка пінкоду до ключового контейнеру, Рис. 27.

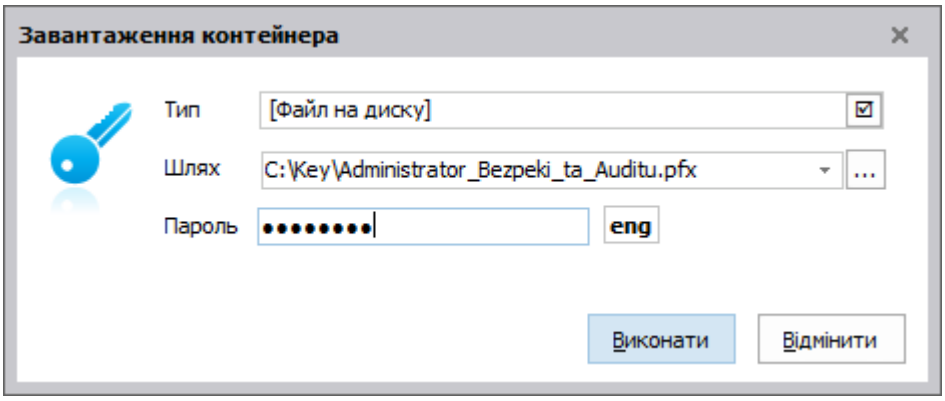

Рис. 27. Заповнення пінкоду до контейнеру

Після успішного заповнення полів, натискаємо на кнопку «Виконати» та отримуємо доступ до повної інформації, яка містить у контейнері, яку можна переглянути у короткому та докладному форматах, Рис. 28-Рис. 29.

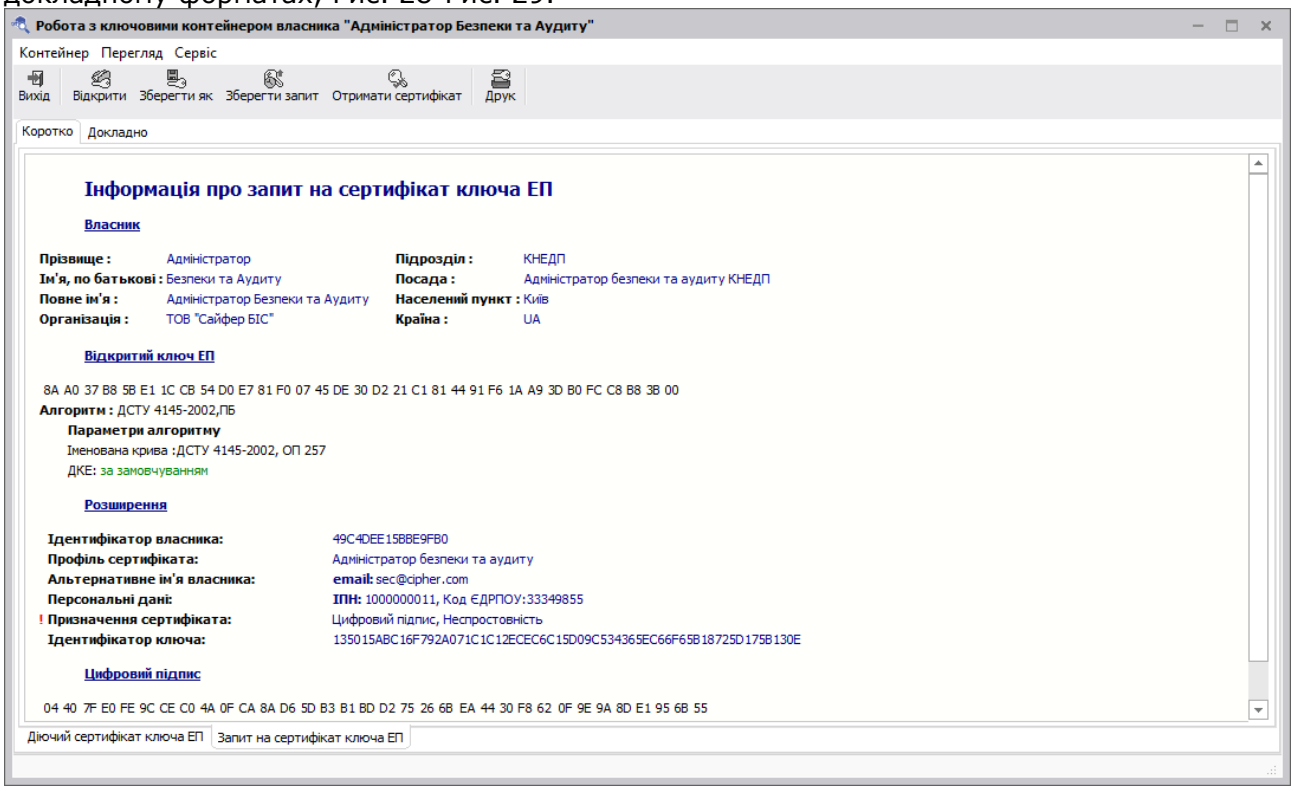

Рис. 28. Короткий опис

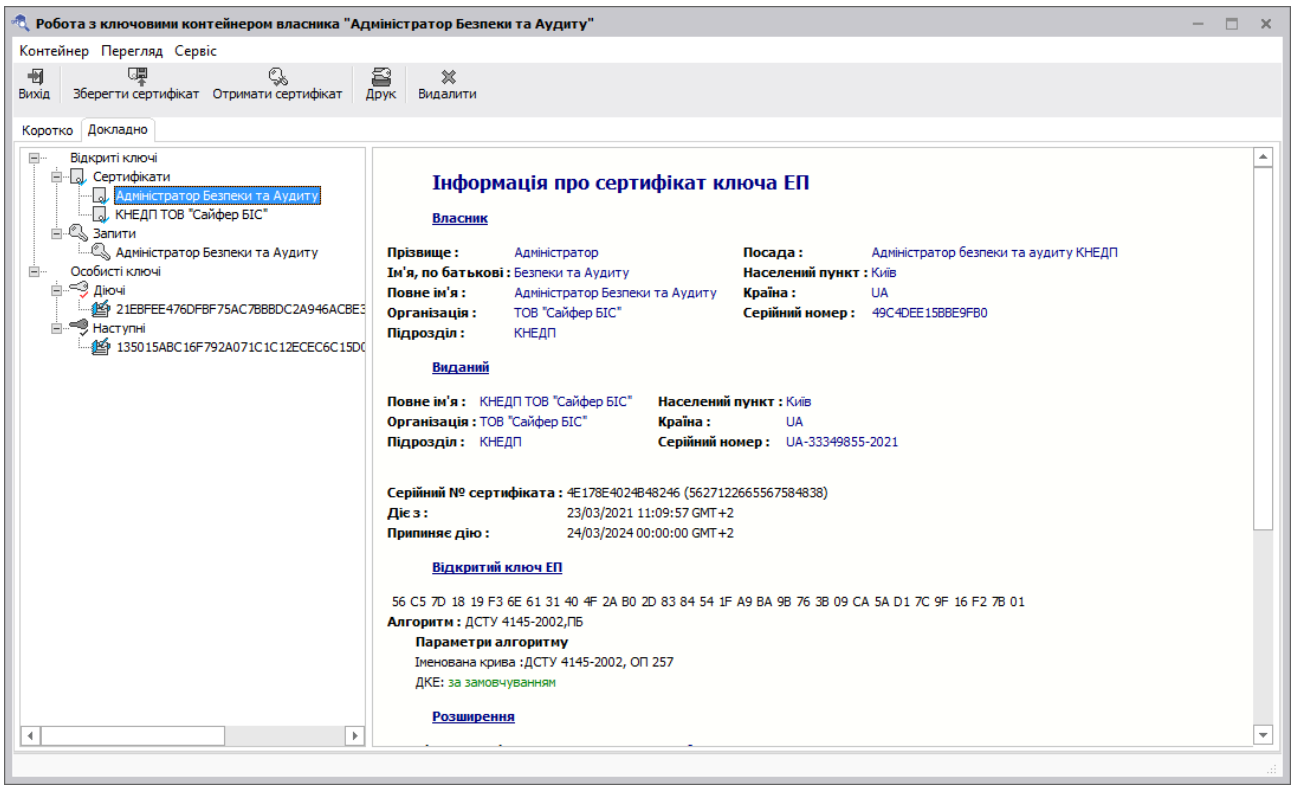

Рис. 29. Докладний опис

Функції застосування

МРКК виконує наступні функції:

- Перегляд всіх сертифікатів та запитів на сертифікат, які знаходяться у ключовому контейнері.
- Запис обраного сертифіката та запиту на сертифікат, який знаходиться у ключовому контейнері, на файловому носії.
- Зміна паролю для доступу до файлового ключового контейнера.
- Збереження з ключового контейнера, обраного сертифіката чи запиту на сертифікат у файл.
- Перетворення діючого сертифіката у запит на сертифікат та збереження його у файл.
- Реєстрація виданого у ЦЗО сертифіката у ключовому контейнері, із заміною попереднього сертифіката, перевіркою ключових полів та завантаженням повного ланцюга засвідчення нового сертифіката.
- Реєстрація нового сертифіката у ключовий контейнер.
- Видалення обраного сертифіката, запиту на сертифікат чи особистого ключа з контейнера.
- Збереження обраного сертифіката чи запиту на сертифікат з ключового контейнера у HTML- файл.
- Друк обраного сертифіката чи запиту на сертифікат на принтері.

Кожну з наведених функцій розглянемо окремо.

Перегляд вмісту ключового контейнера

Для перегляду вмісту ключового контейнера необхідно виконати запуск модуля роботи з ключовим контейнером, чи, якщо модуль вже запущений, обрати в меню «Контейнер», потім «Відкрити», див. Рис. 30.

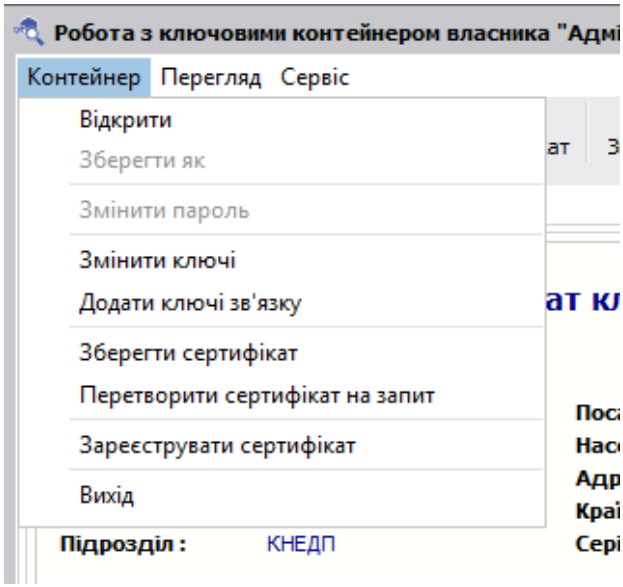

Рис. 30. Відкриття ключового контейнера для перегляду його вмісту

Режим короткого відображення

Даний режим є активним, за замовчування, після завантаження модулем ключового контейнера. У цьому режимі відображається вікно з інформацією про діючий чи стартовий сертифікат, чи у запиті на сертифікат, Рис. 31.

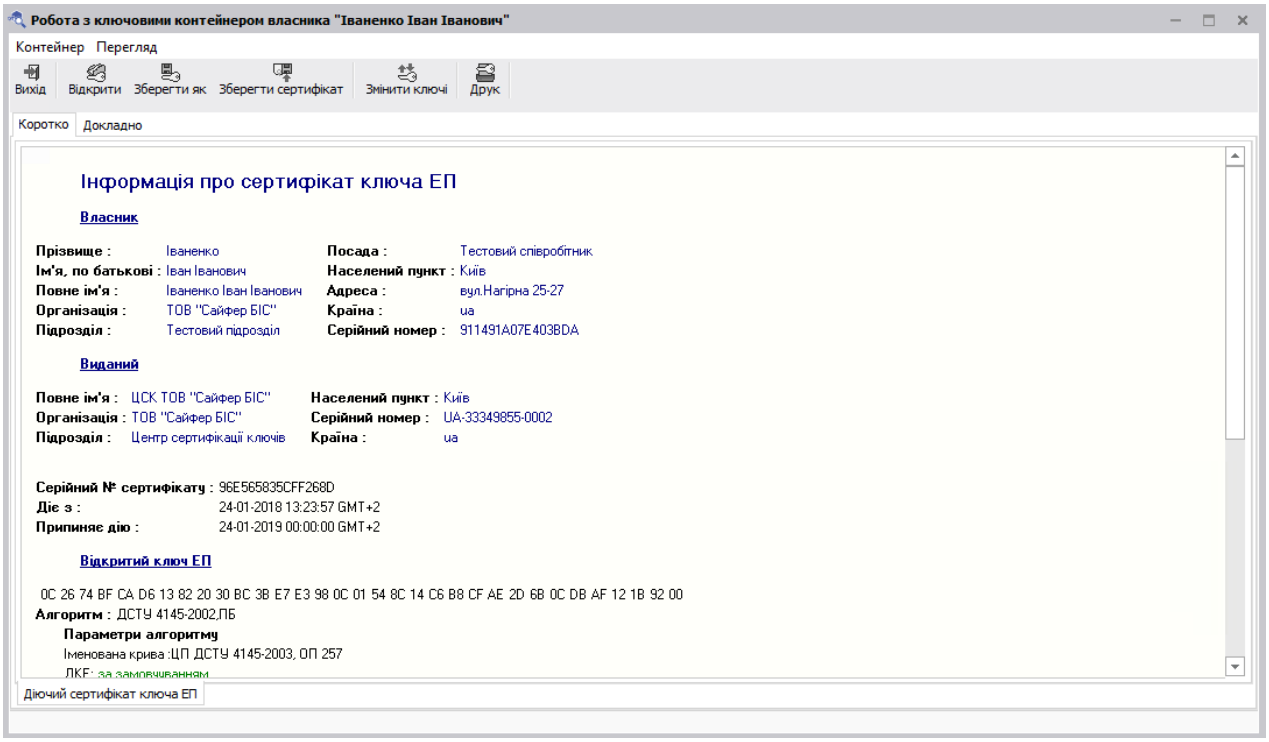

Рис. 31. Перегляд вмісту сертифікату у режимі "Коротко"

Режим детального відображення

Для активації даного режиму слід обрати «Докладно», що знаходиться під панеллю інструментів.

У даному режимі будуть відображені наступні гілки дерева, у залежності від наявності у контейнері:

- Сертифікати.
- Запит на сертифікат.
- Діючі особисті ключі.
- Чергові особисті ключі.
- Попередні особисті ключі.

При виборі будь-якого зі списку сертифіката, буде відображено вміст сертифіката, при виборі запиту – запиту на сертифікат, а при виборі особистих ключів – пов'язаний з ними PKI-об'єкт (сертифікат чи запит на сертифікат). У випадку відсутності відповідного об'єкта, наприклад, сертифікат, був видалений з ключового контейнера, жодної інформації не буде відображатися, що він дійсно був у ключовому контейнері, Рис. 32.

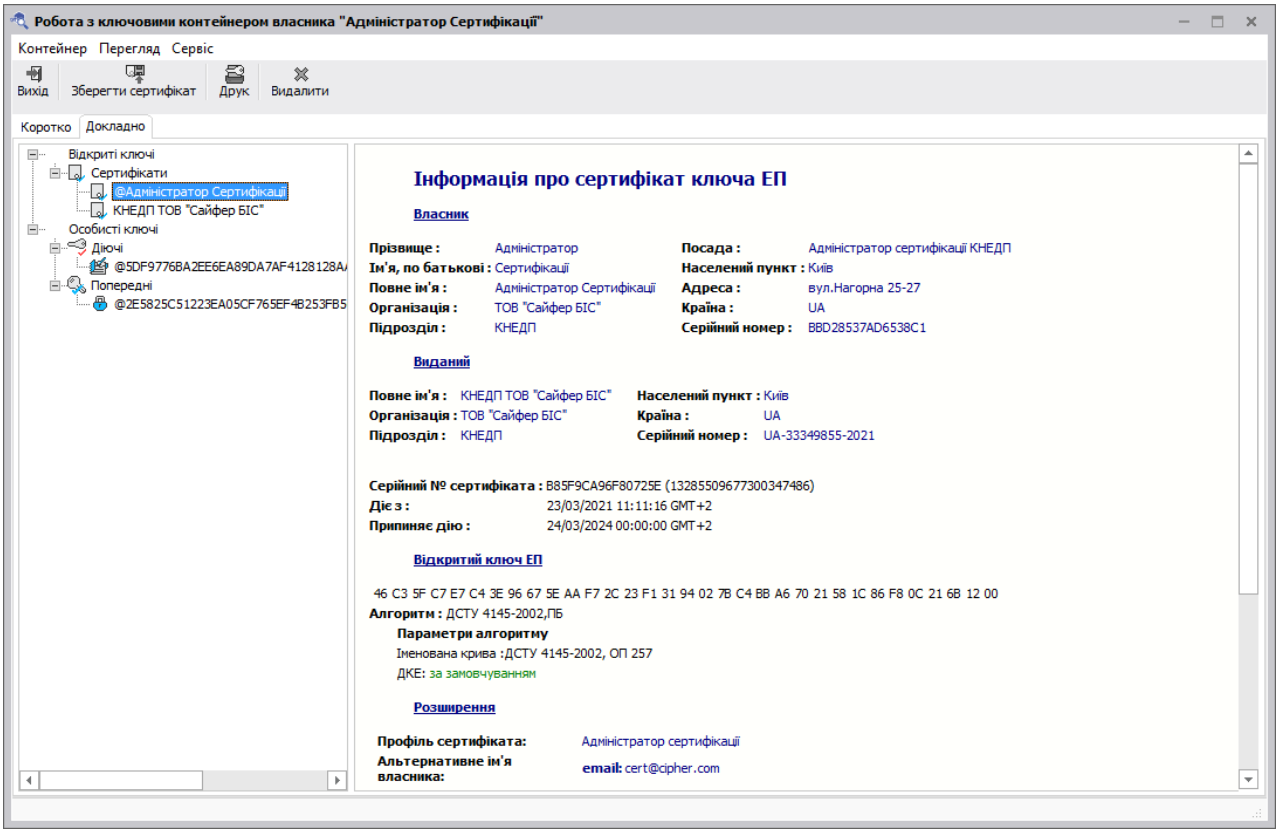

Рис. 32. Відображення сертифікату при виборі особистих ключів у режимі «Докладно»

Збереження ключового контейнера

Дана функція дозволяє виконати запис вмісту ключового контейнера у інший файл чи на захищений ключовий носій, але тільки при завантаженому сертифікаті типу [Файл на диску]. Це може бути корисно при резервному копіюванні ключового контейнера. Для цього необхідно обрати у меню «Контейнер», а потім «Зберегти як», після чого буде відображено діалог, для вказівки, куди саме слід зберегти вміст ключового контейнера, Рис. 33.

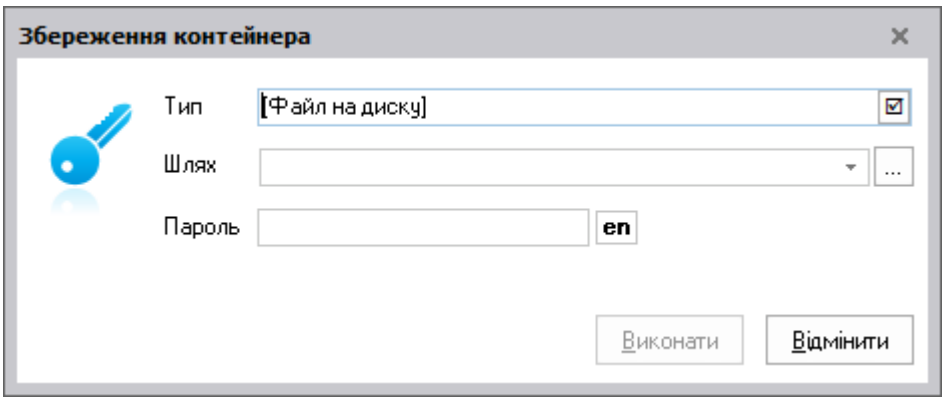

Рис. 33. Вибір носія для збереження ключового контейнера

Зміна паролю для поточного файлового контейнера

Для зміни паролю доступу до поточного (відкритого) ключового контейнера, необхідно обрати в меню «Контейнер», а потім «Змінити пароль», після чого буде відображено діалог для введення нового паролю та його підтвердження, Рис. 34. Слід звернути увагу на мову розкладки клавіатури, який розміщений нижче, для коректної зміни паролю.

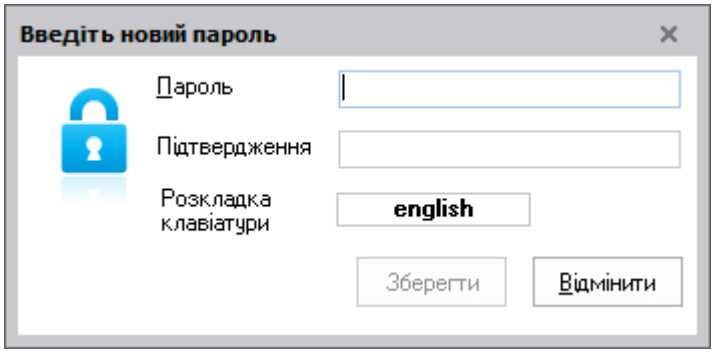

Рис. 34. Зміна паролю для обраного контейнера

Після успішної зміни паролю буде відображено відповідне повідомлення, Рис. 35.

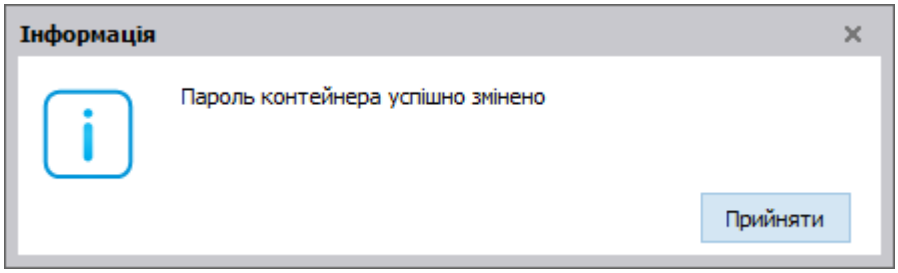

Рис. 35. Повідомлення про успішну зміну пароля до ключового контейнера

Запис сертифіката чи запиту на сертифікат у файл

У детальному режимі, є можливість обрати зі списку, будь-який сертифікат чи запит на сертифікат, і далі зберегти його у файл. Для цього необхідно, при обраному об’єкті PKI, обрати у меню «Контейнер», а далі «Зберегти запит»/«Зберегти сертифікат», Рис. 36 (у залежності від типу обраного об’єкту). Буде відображене вікно з пропозицією обрання місця, для збереження файлу (Рис. 37 чи Рис. 38), після чого файл буде збережено на диску. При спробі виконати збереження особистого ключа, буде відображено повідомлення з пропозицією зберегти відповідний йому чи сертифікат, чи запит на сертифікат.

Рис. 36. Діалог з пропозицією зберегти запит

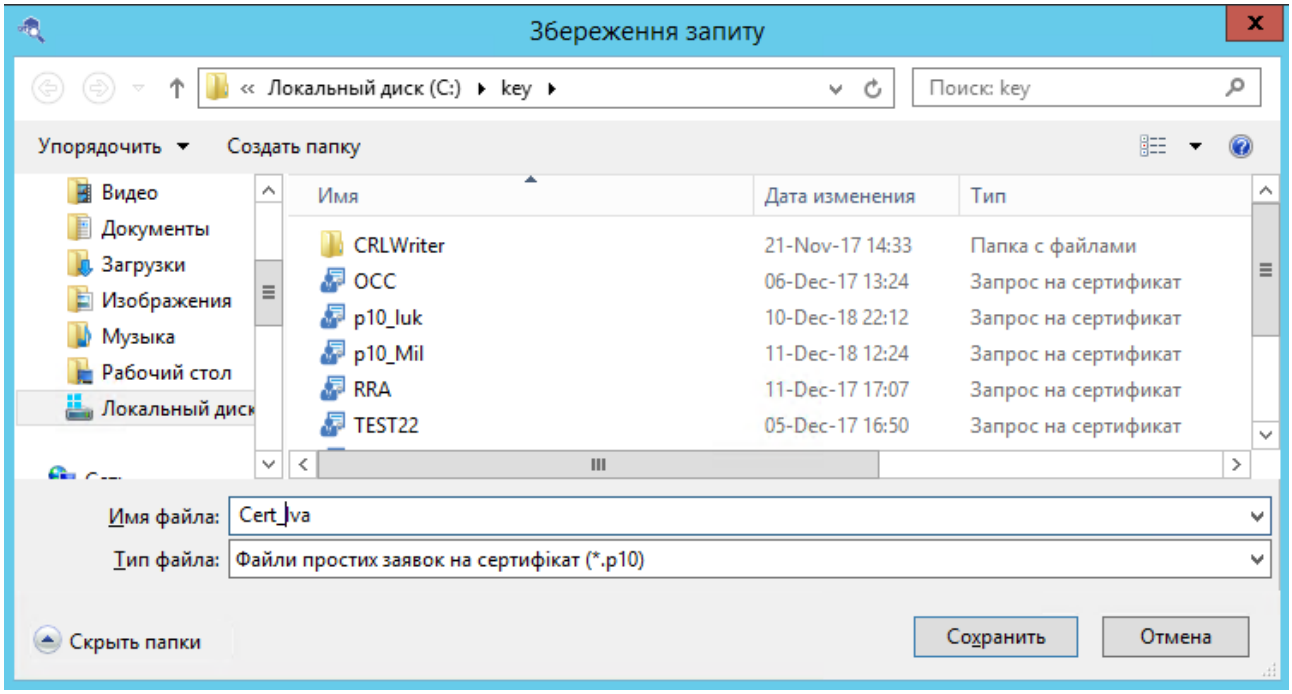

Рис. 37. Збереження запиту на сертифікат

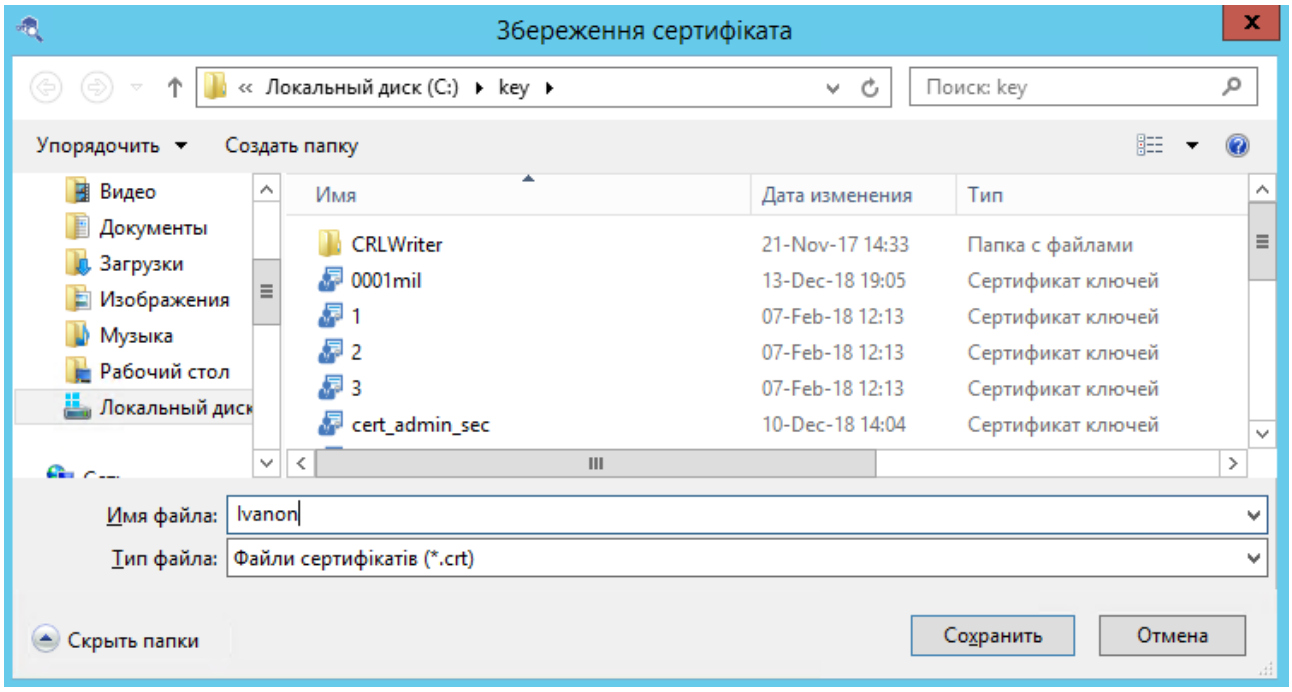

Рис. 38. Збереження сертифікату

Перетворення діючого сертифікату у запит на сертифікат та збереження його у файл

Для перевидачі сертифікату у ЦЗО, необхідно перетворити діючий сертифікат у запит на сертифікат, для подальшої відправки у ЦЗО.

Для виконання вказаного перетворення, необхідно обрати у меню «Контейнер», а потім «Перетворити сертифікати на запит», після чого буде відображено діалог формування нового запиту, Рис. 39. Після, є можливість зберегти перетворений у запит сертифікат, Рис. 40.

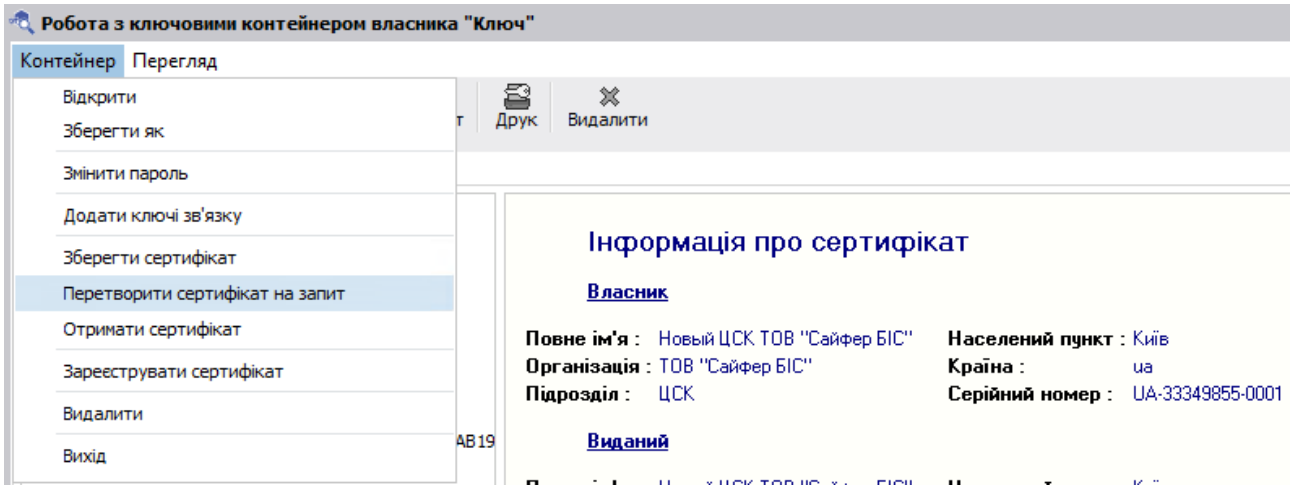

Рис. 39. Діалог «Перетворити сертифікат на запит»

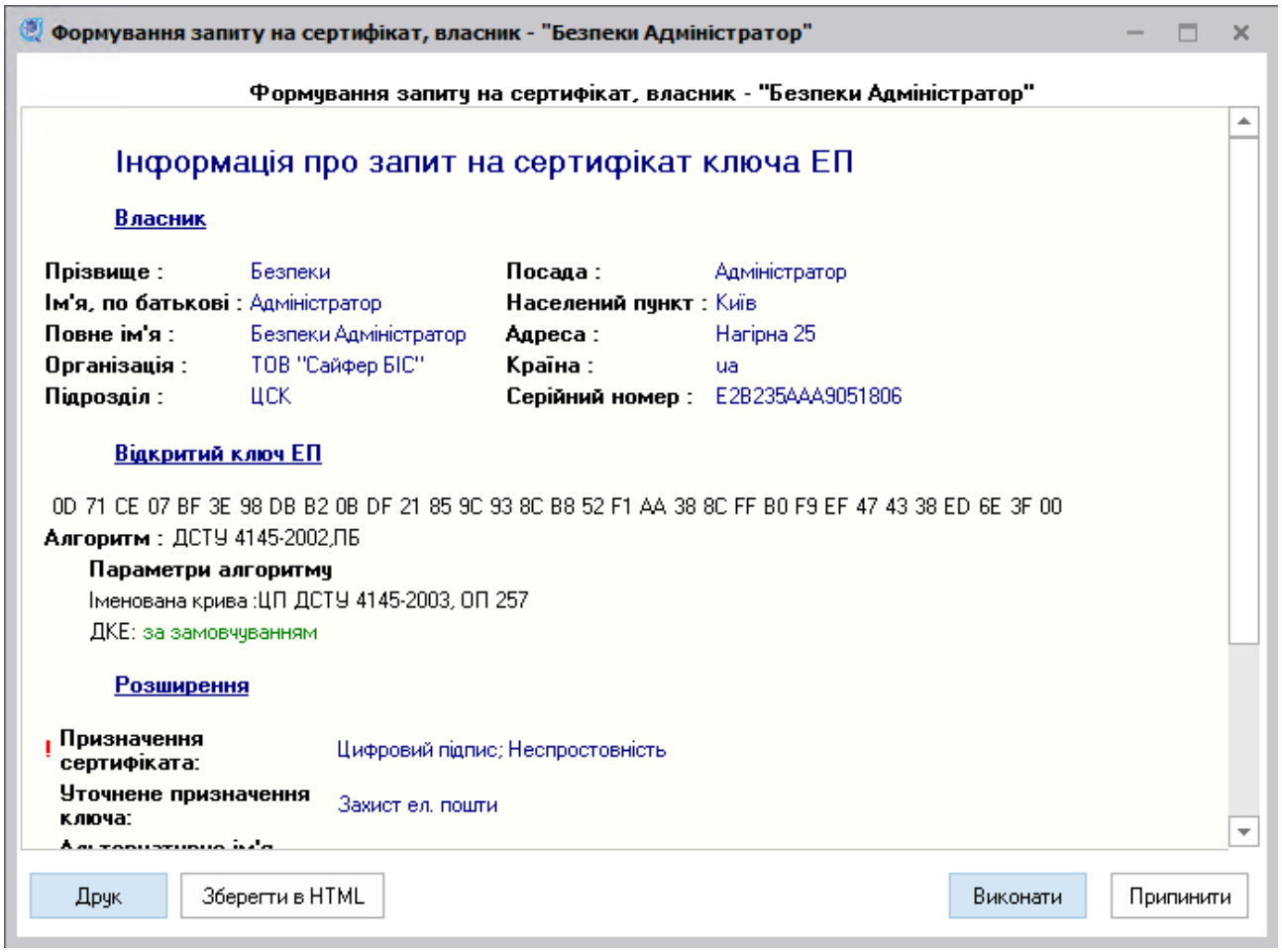

Рис. 40. Збереження перетвореного у запит сертифікату

Реєстрація виданого у ЦЗО сертифікату у ключовому контейнері

Для заміни існуючого сертифіката, виданого ЦСК, на сертифікат виданий іншим ЦСК, засвідчувальний центр чи ЦЗО, з послідовною реєстрацію повного ланцюга засвідчення, необхідно у меню «Контейнер», а потім «Зареєструвати сертифікат», і у діалозі, який з'явився вказати сертифікат, який необхідно перезаписати у контейнер, Рис. 41. Також слід вказати розташування сертифіката ЦЗО для додавання його у контейнер та послідовним формуванням ланцюга засвідчення.

Слід зауважити, що перезапис сертифіката дозволяється тільки для сертифікатів одного власника, а при перезаписі здійснюється перевірка співпадіння ключових полів обох сертифікатів. При спробі перезаписати сертифікат, власник якого відрізняється від поточного власника контейнера, буде відображено повідомлення про помилку, див. Рис. 42.

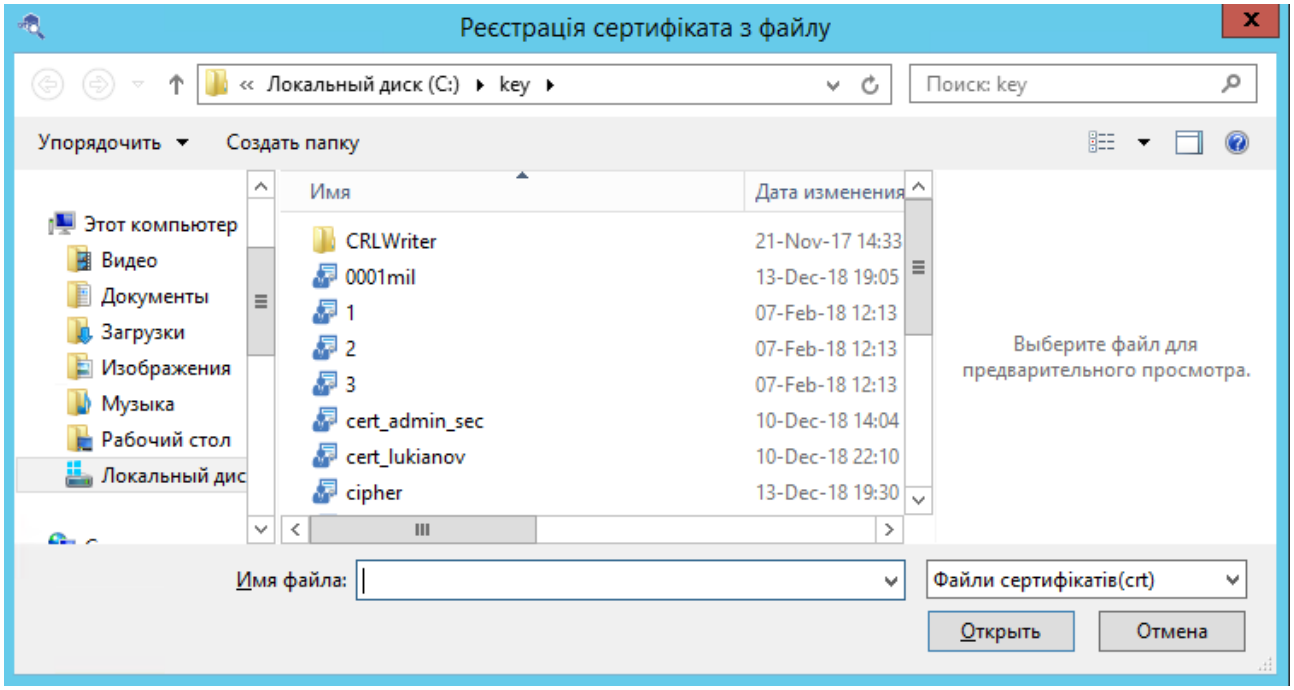

Рис. 41. Реєстрація підписаного у ЦЗО сертифікату для перезапису його у контейнері

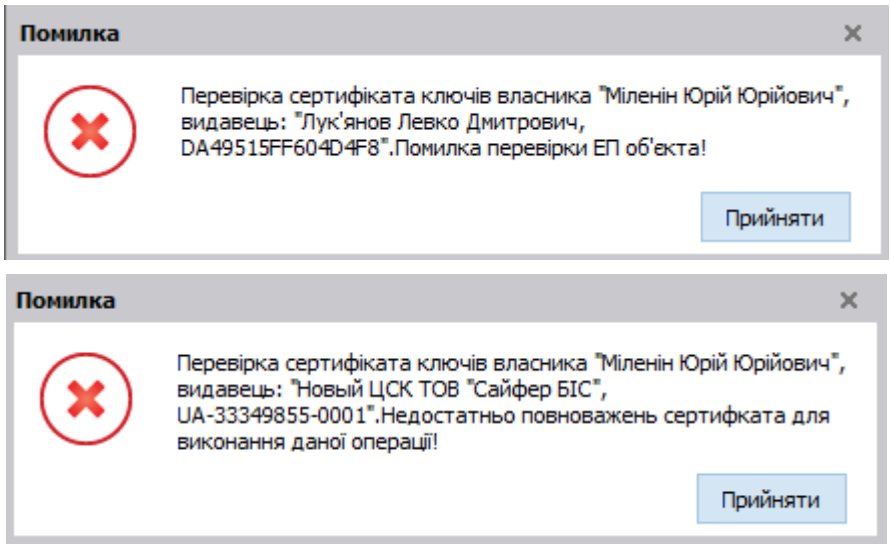

Рис. 42. Помилка при перезаписі сертифікату іншого власника у ключовий контейнер

Реєстрація нового сертифікату у ключовий контейнер

Для додавання нового сертифіката у ключовий контейнер необхідно обрати пункт меню «Контейнер», а потім «Зареєструвати сертифікат», після чого буде відображено діалог для вибору файлу сертифіката, який буде додано у контейнер, Рис. 43.

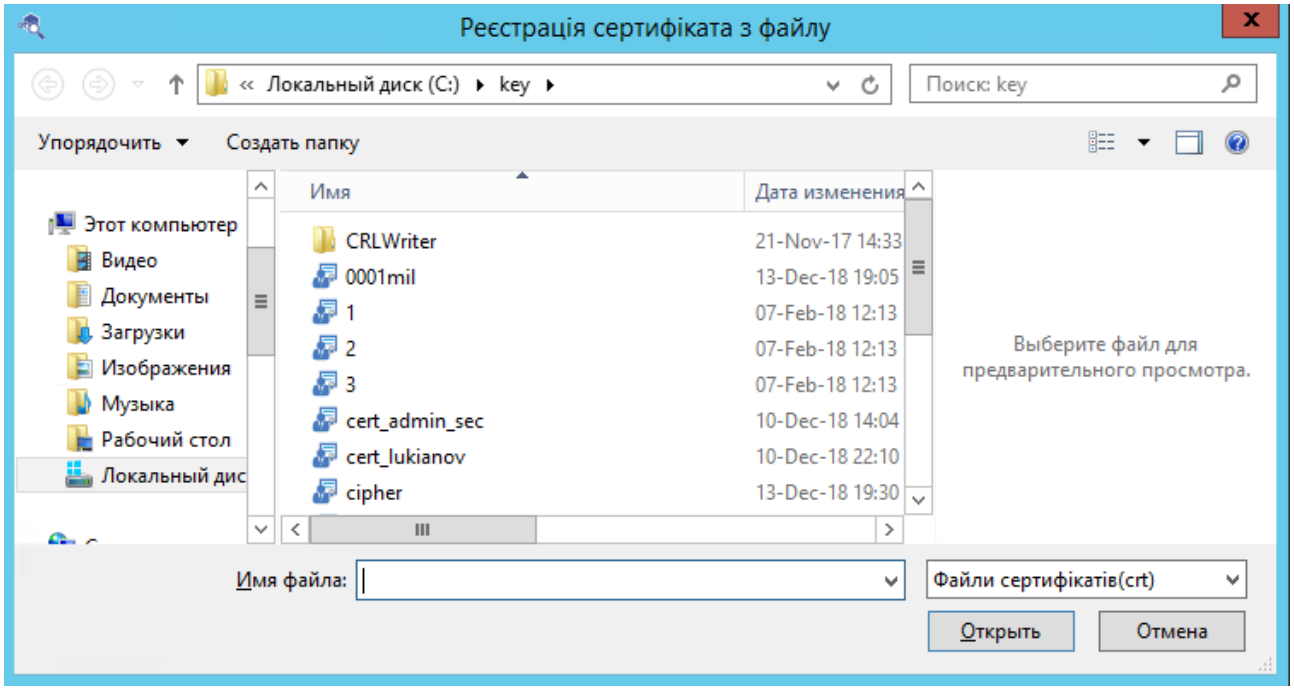

Рис. 43. Завантаження нового сертифікату до контейнера

Якщо сертифікат, який реєструється не належить власнику сертифікату поточного контейнера, то він буде доданий у контейнер та відображений у списку сертифікатів. Після успішної реєстрації сертифікації, буде відображено повідомлення, Рис. 44.

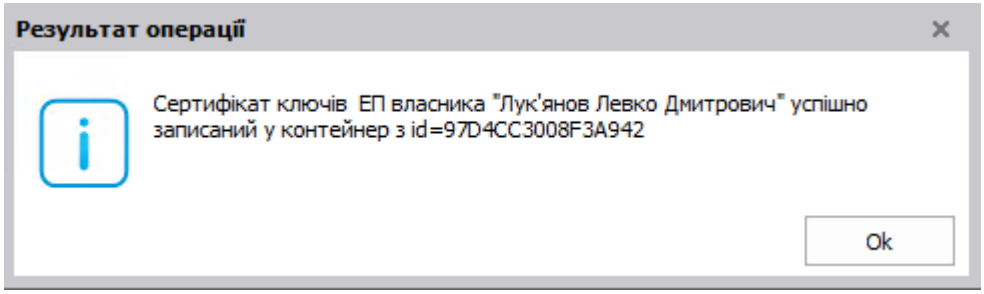

Рис. 44. Успішне завантаження сертифікату у контейнер

У випадку, якщо сертифікат, який реєструється належить власнику сертифіката поточного контейнера, то буде здійснена перевірка на необхідність введення у дію нових ключів.

Видалення обраного сертифікат, запиту на сертифікат чи особистого ключа з ключового контейнера

Дана функція доступна лише у режимі детального перегляду, при обраному об’єкту PKI.

Для управління вмістом ключового контейнера можна скористатися можливістю не лише реєстрації нових сертифікатів чи запитів, але і їх видалення. Крім цього, присутня можливість видалення і особистих ключів.

Для видалення обраного об’єкта PKI, необхідно у контекстному меню обрати «Видалити», чи у головному меню «Контейнер», потім «Видалити», Рис. 45, після чого буде показано запит на підтвердження обраного об’єкта, Рис. 46.

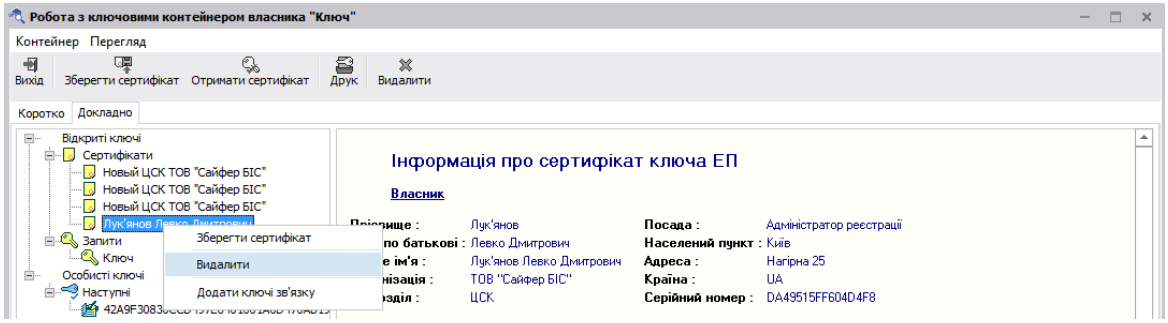

Рис. 45. Діалог видалення обраного об’єкта PKI

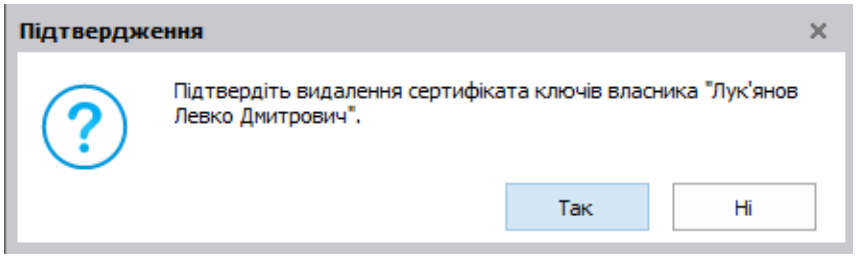

Рис. 46. Запит на підтвердження видалення об’єкта

При спробі видалення діючого сертифікату, Рис. 46, буде показане вікно, з пропозицією видалити також, запит на сертифікат та відповідний йому особистий ключ, Рис. 47, Рис. 48 та Рис. 49.

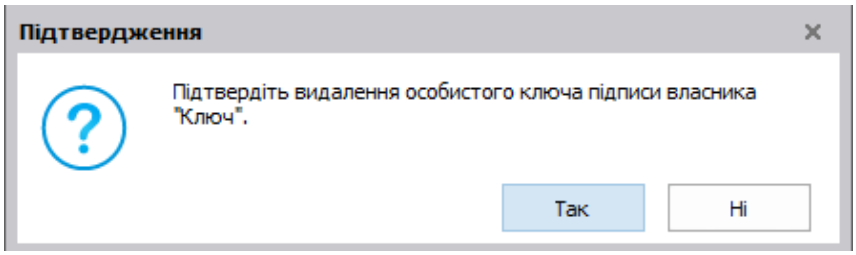

Рис. 47. Підтвердження про видалення сертифікату ключів власника

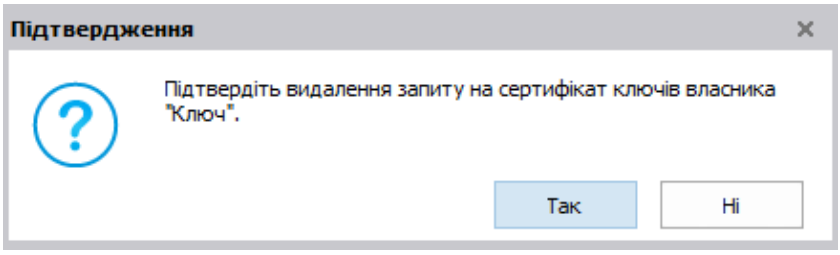

Рис. 48. Підтвердження про видалення запиту на сертифікат ключів власника

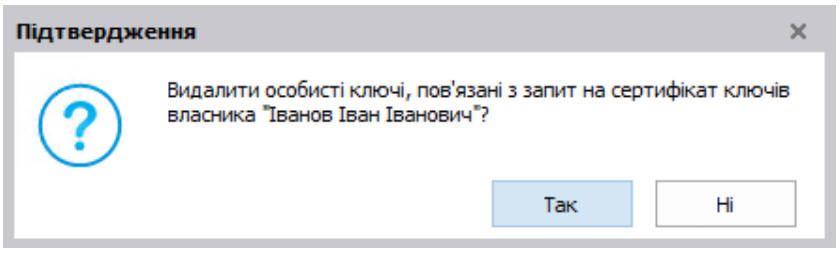

Рис. 49. Підтвердження про видалення особистого ключа, пов’язаного і із запитом на сертифікат ключів власника

Після успішного видалення сертифіката, запиту та ключів, буде показано відповідне повідомлення, Рис. 50 та Рис. 51.

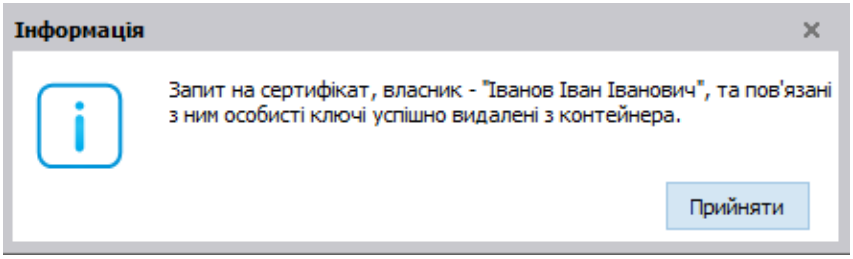

Рис. 50. Повідомлення про успішне видалення

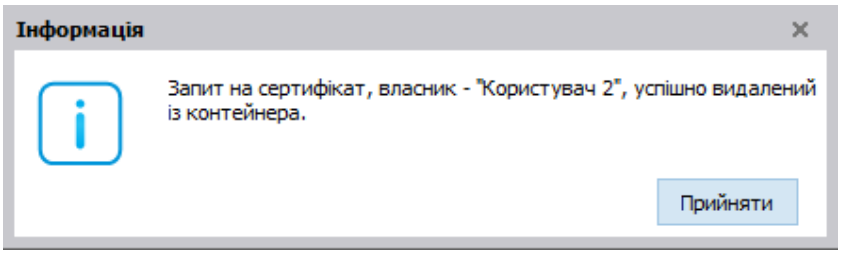

Рис. 51. Повідомлення про успішне видалення

Збереження обраного сертифіката чи запиту на сертифікат у HTML-файл

Дана функція дозволяє зберегти вміст обраного сертифіката чи запиту на сертифікат у HTML-файл.

Для цього необхідно обрати сертифікат чи запит на сертифікат та обрати меню «Перегляд», а потім «Зберегти в HTML», Рис. 52. Слід зауважити, що дана функція працює тільки для сертифікатів та запитів на сертифікат, у випадку вибору особистих ключів (стартових, діючих чи чергових) у файл буде збережено вміст відповідного PKI-об'єкта (сертифікатів чи запитів на сертифікат).

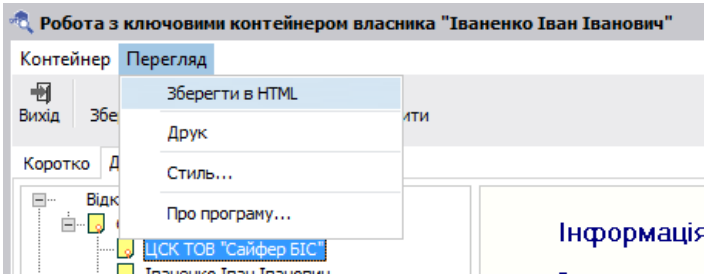

Рис. 52. Діалог збереження у HTML-файлі

Після вибору меню «Зберегти в HTML», буде відображено вікно, з пропозицією вказати, куди слід зберегти HTML-файл, Рис. 53.

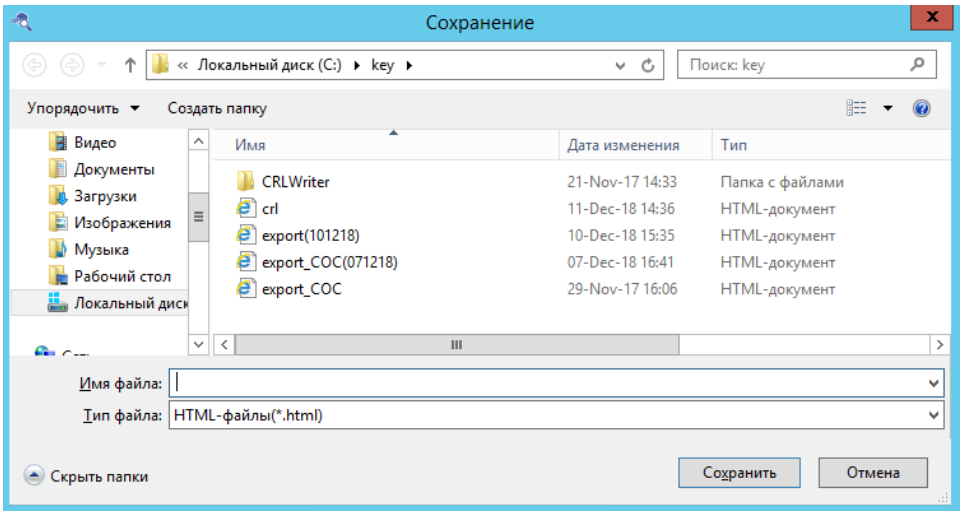

Рис. 53. Збереження обраного сертифікату у форматі HTML

Друк обраного сертифіката чи запиту на сертифікат на принтер

Дана функція дозволяє здійснити друк обраного сертифіката чи запиту на сертифікат на принтер.

Для вибору даної функції необхідно обрати сертифікат чи запит на сертифікат, потім обрати у контекстному меню «Друк», чи обрати у головному меню «Перегляд», а потім «Друк», після чого буде відображено діалог друку, Рис. 54.

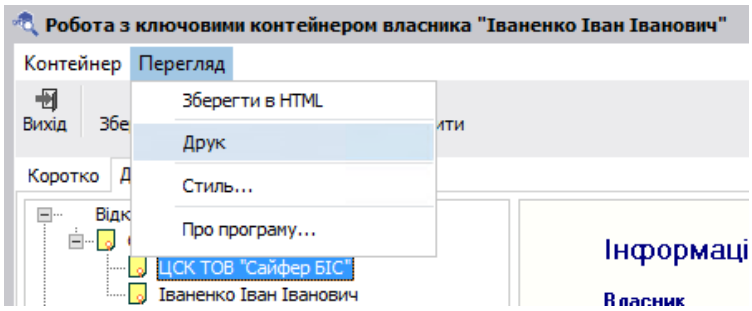

Рис. 54. Діалог вибору друку інформації про сертифікат

За допомогою діалогу друку, можна обрати принтер для друку, кількість копій і т.д., Рис. 55.

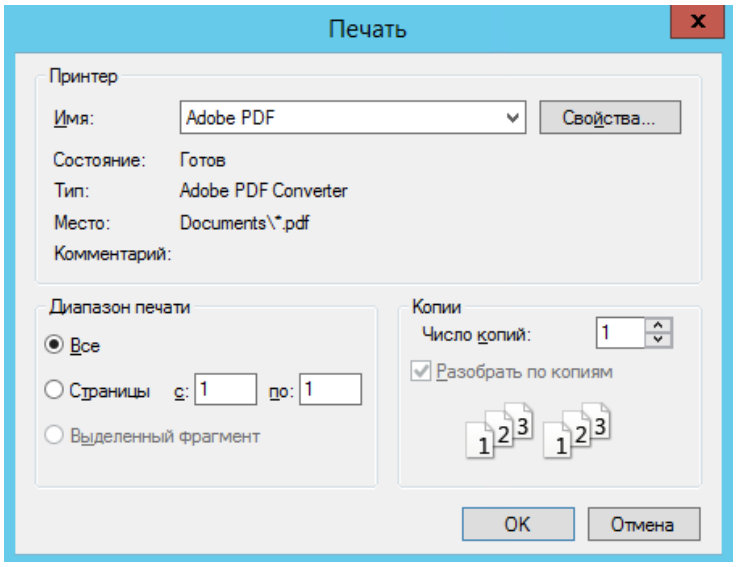

Рис. 55. Друк обраного сертифікату

Коротка характеристика команд меню головного вікна

Нижче, у Таблиця 2 наведені команди меню головного вікна МРКК.

Таблиця 2. Перелік функцій доступних через головне меню

Підменю	Пункт меню	Опис
Контейнер	Відкрити	Дозволяє відкрити вікно для вибору файлового чи апаратного ключового носія та введення паролю.
	Зберегти як	Дозволяє зберегти поточний ключовий контейнер у файл чи на захищений ключовий носій.
	Змінити пароль	Дозволяє змінити пароль до обраного файлового контейнера.
	Зберегти запит/ сертифікат	Дозволяє зберегти сертифікат чи запит на сертифікат у файл.
	Додати ключі зв'язку	Дозволяє додати ключі зв'язку, якщо вони

Підменю	Пункт меню	Опис
		відсутні.
	Перетворити сертифікат на запит	Дозволяє перетворити діючий сертифікат у запит на сертифікат для подальшої його відправки у засвідчувальний центр чи ЦЗО.
	Зареєструвати сертифікат	Дозволяє зареєструвати у ключовому контейнері сертифікат, виданий засвідчувальним центром чи ЦЗО.
	Зареєструвати сертифікат	Дозволяє додати новий сертифікат у ключовий контейнер.
	Видалити	Дозволяє видалити зазначений сертифікат, запит на сертифікат чи особистий ключ, з ключового контейнера.
	Вихід	Завершає роботу програми.
Перегляд	Зберегти в HTML	Дозволяє зберегти зазначений сертифікат чи запит на сертифікат у HTML-файл.
	Друк	Дозволяє виконати друк обраного сертифікату чи запиту на сертифікат.
Опції	Стиль	Дозволяє обрати та встановити стиль оформлення вікон застосування.
	Параметри оновлення програми	Дозволяє здійснити налаштування оновлень. Редагуючи Адресу сервера оновлень, періодичність перевірки та параметри проксі сервера (за необхідності).
	Оновити зараз	Дозволяє здійснити перевірку оновлень та оновити застосування.
	Про програму	Дозволяє отримати детальну інформацію про застосування, версію та розробника.

Централізоване оновлення застосування

Слід звернути увагу, що з версії 1.3.18.96 з'явилась можливість централізовано оновлювати Модуль роботи з ключовим контейнером. Даний функціонал допомагає оновлювати застосування без обов'язкового перевстановлення, таким чином зберігає час, забезпечує від можливих збоїв та повідомляє, про можливі нові оновлення.
Для здійснення оновлення, необхідно перейти в меню «Опції» - «Оновити зараз», Рис. 56.

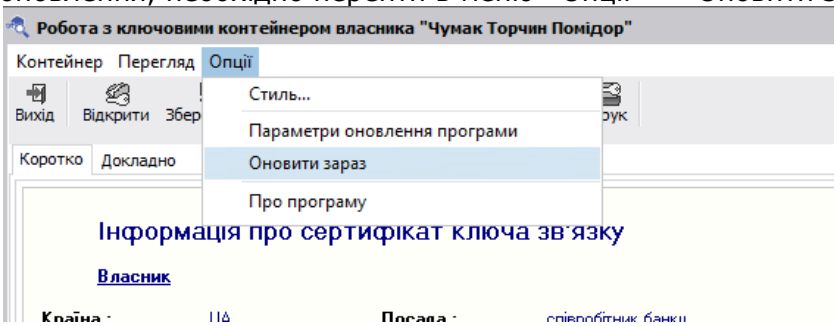

Рис. 56. Пункт меню «Оновити зараз»

Якщо оновлення наявні, з'являється повідомлення про те, що оновлення вже завантаженні, але для введення їх в дію, необхідно перезавантажити програму. У подіях вказано, де файл взято та куди збережено, Рис. 57.

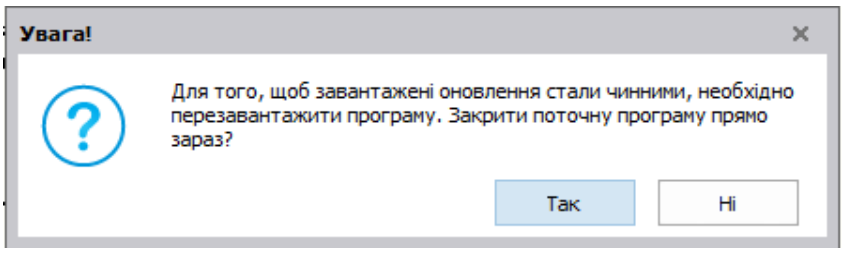

Рис. 57. Інформація про оновлення програми

Після повторного відкриття вже оновленої програми, можна знову перейти у меню «Опції» - «Оновити зараз», якщо повідомлення не з'являється, отже встановлено останню версію застосування.

В меню «Опції» - «Параметри оновлення програми» можна здійснити налаштування, Рис. 58.

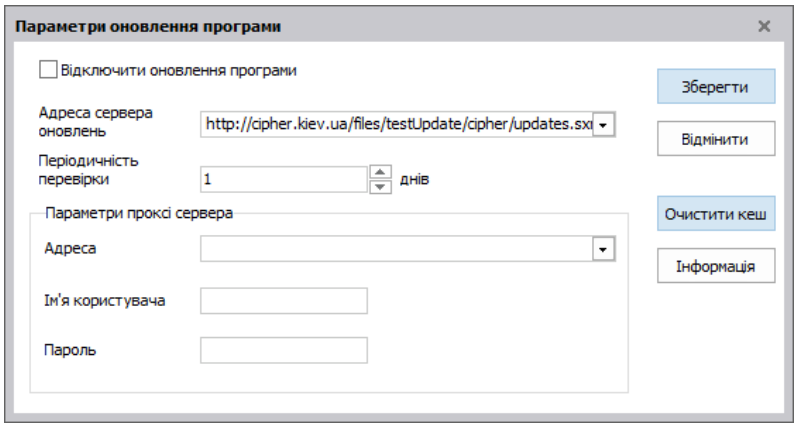

Рис. 58. Меню «Параметри оновлення програми»

Вказавши позначку «Відключити оновлення програми» - дає можливість не перевіряти оновлення при старті та встановити нові оновлення не буде можливості.

«Адреса сервера оновлень» – дозволяє вказати розміщення файлу з оновленнями.

«Періодичність перевірки» – дозволяє вказати як часто здійснювати перевірку на наявність оновлень. Якщо вказати 0, то перевірка буде здійснюватися автоматично при кожному запуску застосування, Рис. 59. Якщо вказати 1, то перевірка буде здійснюватися щодня, відповідно, якщо 2, то раз у два дні.

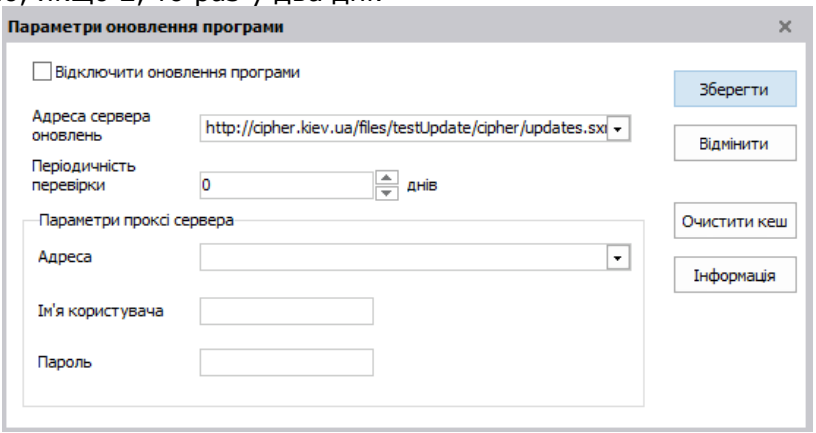

Рис. 59. Меню «Параметри оновлення програми»