ТОВ «САЙФЕР ПРО»
Адреса: 04107, Київ, вул. Нагірна, 25-27
Тел.: +38 044 484 46 12, 484 46 17
E-mail: info@cipher.com.ua

Системи захисту інформації
www.cipher.com.ua

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 (МРКК), призначеного для роботи під управлінням ОС Windows 10 чи вище, у складі СКЗІ «Шифр-X.509» версія 2.

Системні вимоги

Апаратне забезпечення

Мінімальна апаратна конфігурація:

- Відповідає вимогам ОС Microsoft Windows 10.
- Вільного дискового простору: 40 Мб.
- Мережева карта: Fast Ethernet, IP v4.

Рекомендована апаратна конфігурація:

- Відповідає вимогам ОС Microsoft Windows 11.
- Вільного дискового простору: 1 Гб.
- Мережева карта: Gigabit Ethernet, IP v4.

Програмне забезпечення

Мінімальна конфігурація:

- Microsoft Windows 10.

Рекомендована конфігурація:

- Microsoft Windows 11.

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	Avtor Secure Token-337/338 Series	Token
2	ТОВ Автор, Україна	Avtor Secure SmartCard-337/338	SmartCard
3	ТОВ Пластик Карта, Україна	PlasticCard TEllipse 3/4	SmartCard
4	ТОВ Авест Україна, Україна	AvestKey UA	Token
5	Thales, США	Thales I Gemalto I SafeNet I Aladdin eToken	Token
6	ТОВ Ефіт технолоджіс, Україна	EfitKey	Token
7	АТ ІІТ, Україна	Кристал-1	Token
8	АТ ІІТ, Україна	Алмаз-1К	Token

Підготовка до роботи засобами Модуля роботи з ключовим контейнером

Попередні налаштування

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

Встановлення ПЗ для роботи із захищеним носієм

Для роботи із захищеними носіями, обов'язковим є встановлення драйвера захищеного ключового носія або спеціального призначеного для користувача ПЗ.
Після встановлення програмного забезпечення(або драйвера), щоб переконатися у можливості використання захищеного носія, необхідно запустити «Диспетчер пристроїв». Для цього натисніть і утримуйте клавішу «Windows» і «X», після чого з'явиться меню у якому необхідно обрати і натиснути «Диспетчері пристроїв».
Якщо захищений носій визначився ОС, його буде відображено у вікні диспетчера пристроїв. У протилежному випадку, якщо носій ОС невиявлений, слід звернутися до:

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

Подальше продовження встановлення «АРМ адміністратора сертифікації» можливе лише після повного усунення питань пов'язаних з коректною роботою захищених носіїв.

Встановлення

Для встановлення МРКК необхідно завершити всі невикористовувані завдання, після чого запустити файл **setup_CiX509_CtxViewer.exe** з інсталяційного носія і слідувати вказівкам програми встановлення. Встановлення можливо лише за наявності прав **Адміністратора.**
Після запуску **setup_CiX509_CtxViewer.exe** буде відображений стандартний діалог системи захисту. ОС запитає дозвіл програмі на внесення змін, Рис. 1(якщо службу захисту користувачів (UAC) вимкнено відобразиться діалог Рис. 2).

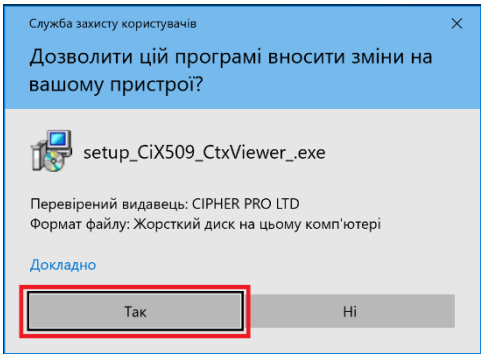

Рис. 1. Діалог системи захисту ОС

Слід вибрати **Так**, для переходу до діалогу вибору мови, яка буде використовуватися під час встановлення ПЗ, Рис. 2.

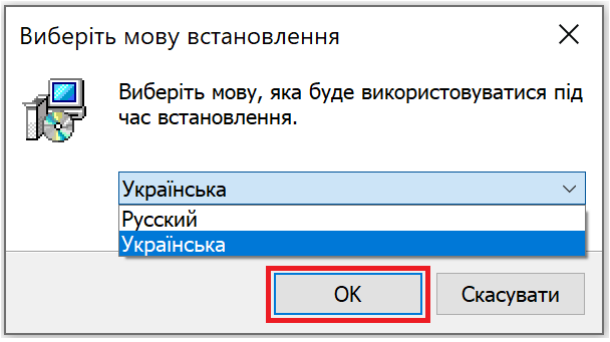

Рис. 2. Діалог вибору мови

Після вибору мови встановлення ПЗ натискаємо **Ок,** наступний діалог, Рис. 3. Після ознайомлення з **Ліцензійною угодою ТОВ "САЙФЕР ПРО"**, тобто з ліцензією по використанню ПЗ, для продовження встановлення слід прийняти умови угоди, явно вказавши **Я приймаю умови угоду** та натиснути кнопку **Далі**.

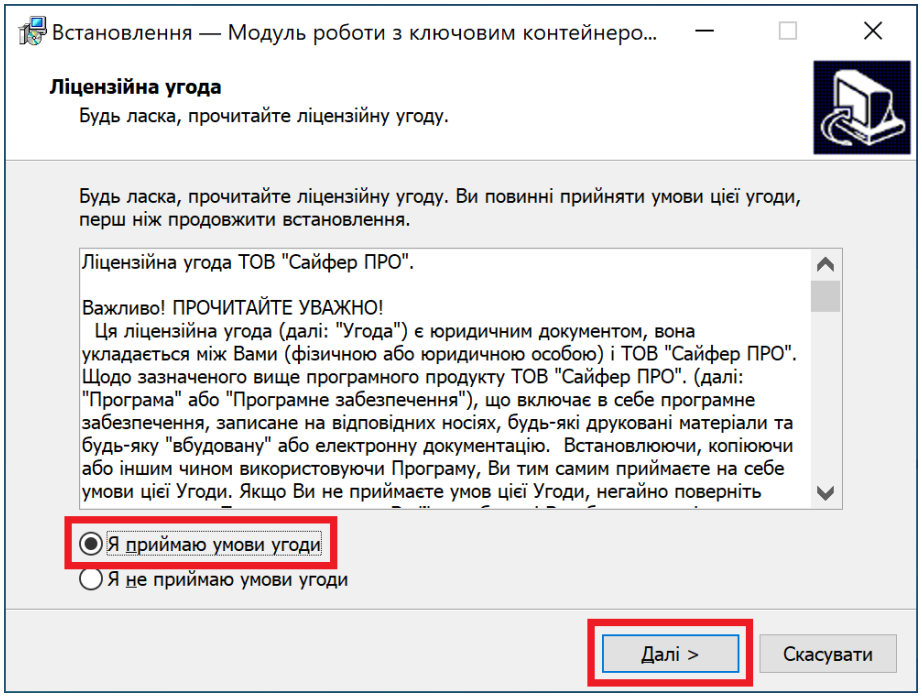

Рис. 3. Діалог з інформацією про ліцензію на використання ПЗ

Далі відображається діалог **Вибір шляху для встановлення**, куди буде встановлено МРКК, Рис. 4 *(зараз під ОС Windows доступна лише 32-х розрядна версія).*

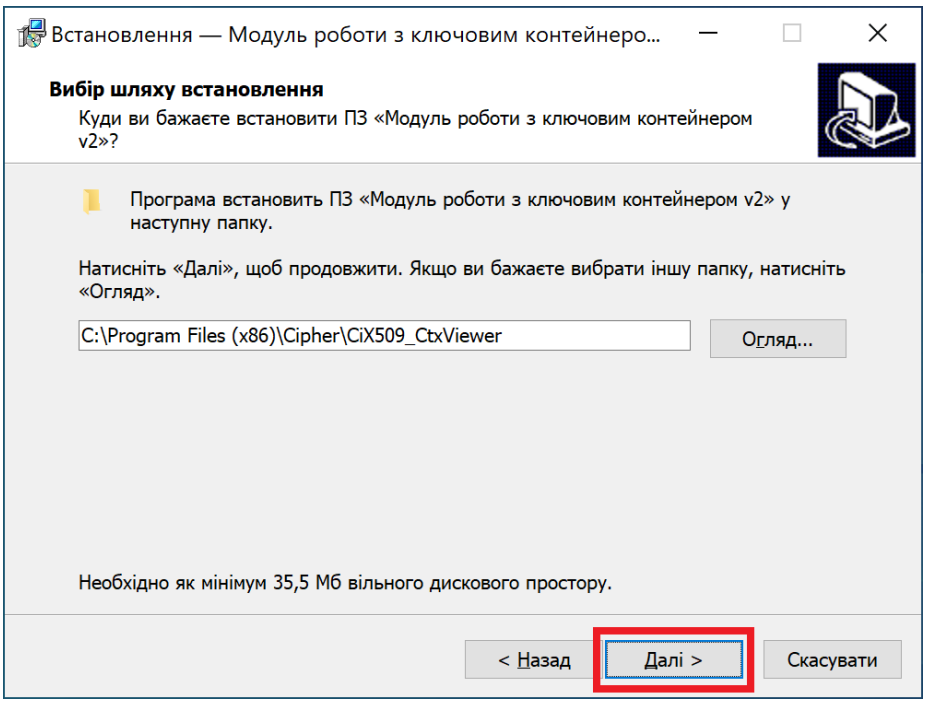

Рис. 4. Діалог вибору шляху до папки, куди буде встановлено МРКК

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

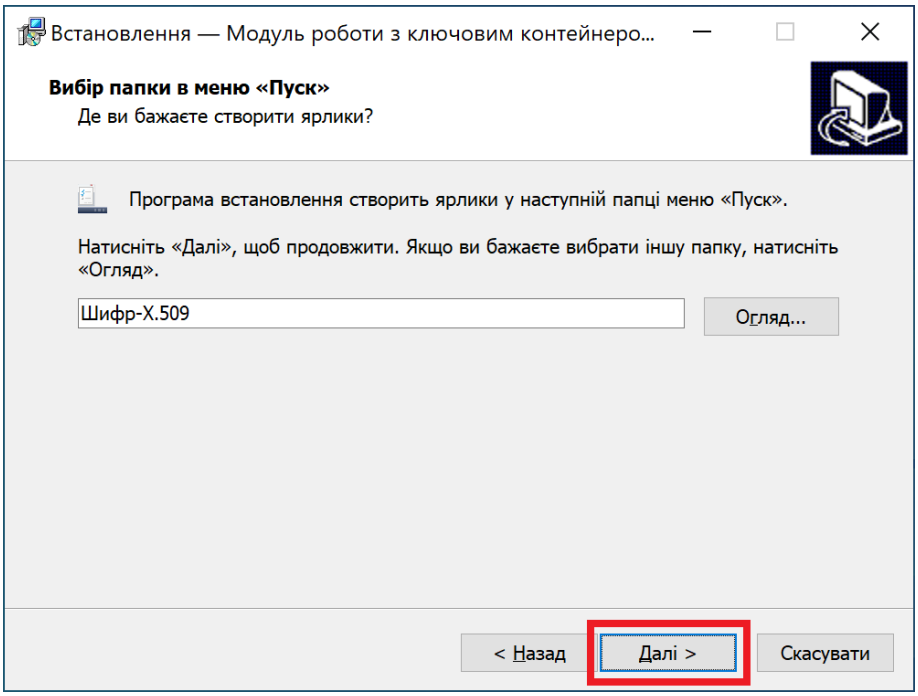

Рис. 5. Діалог вибору папки в меню «Пуск», для встановлення ярлика запуску МРКК

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

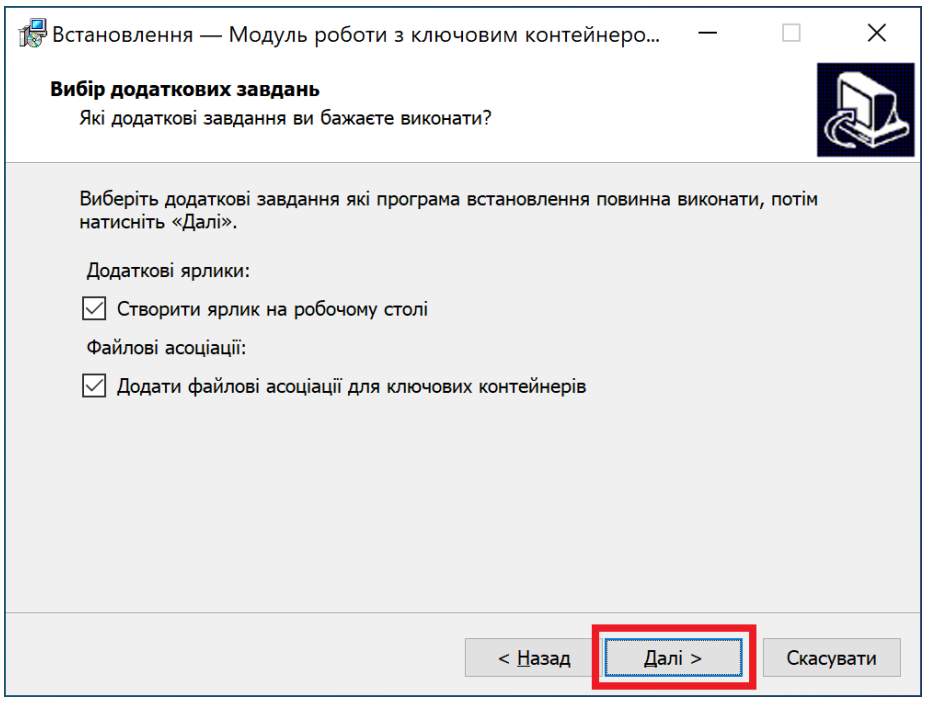

Рис. 6. Діалог вибору додаткових задач

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**.

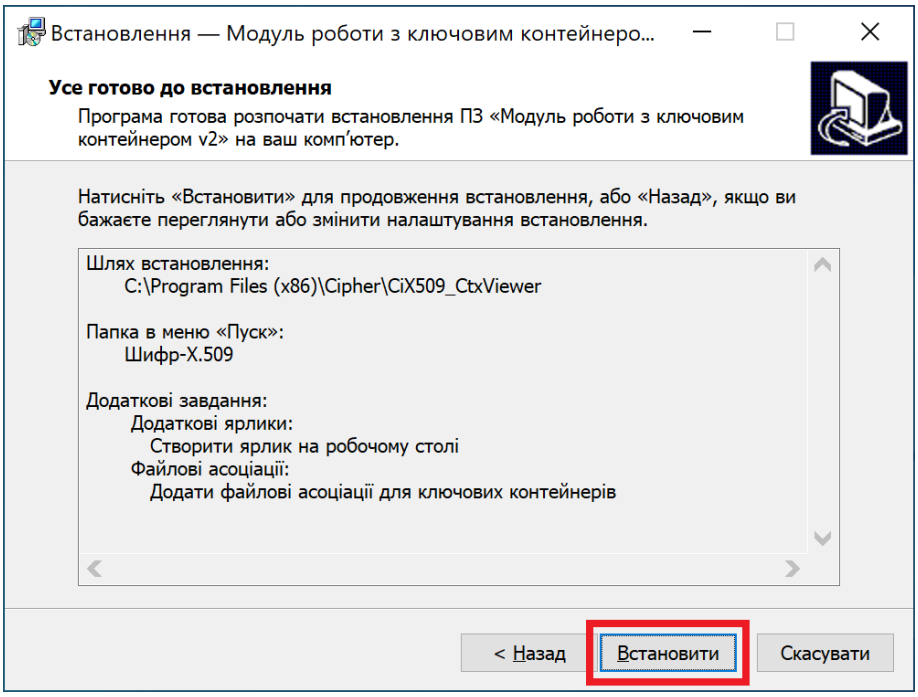

Рис. 7. Діалог перегляду налаштувань встановлення

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

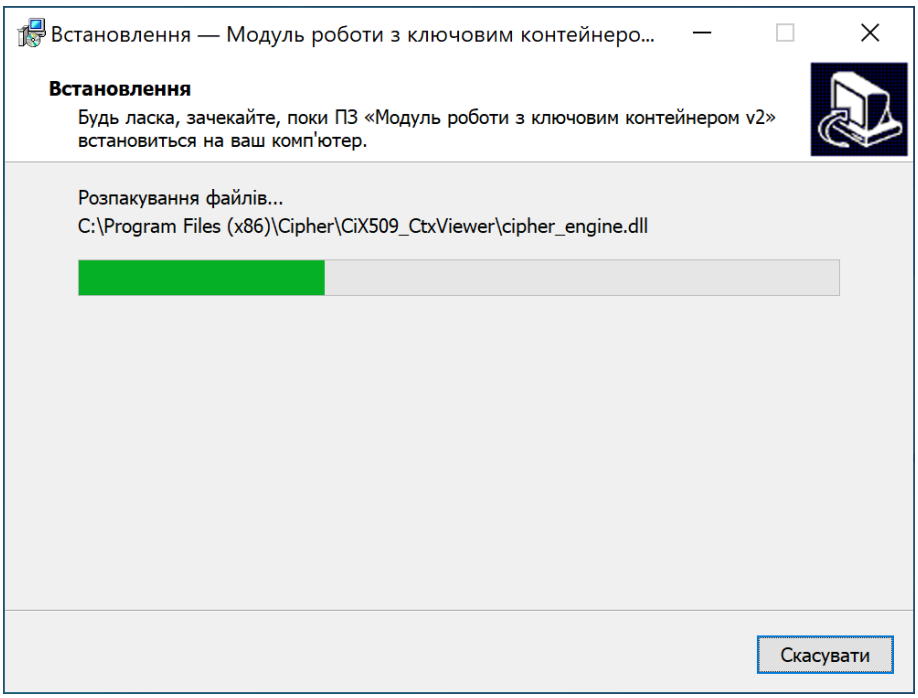

Рис. 8. Діалог відображення процесу встановлення МРКК

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

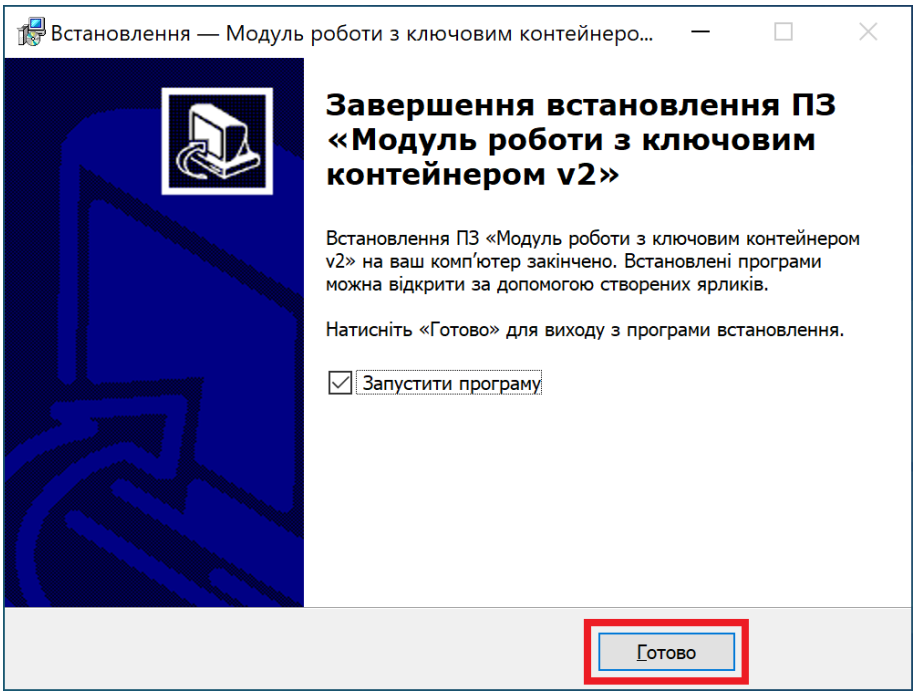

Рис. 9. Діалог завершення установки

Наявність необхідних даних перевіряється безпосередньо МРКК у процесі запуску, у випадку відсутності будь-яких налаштувань та відмови 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, або через ярлик застосування на «**Робочому столі**» Рис. 11.

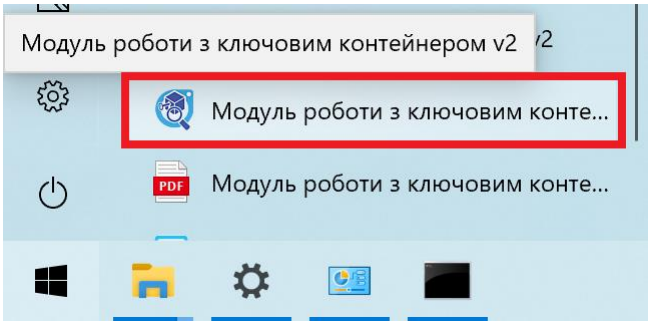

Рис. 10. Запуск модуля з меню «Пуск»

Рис. 11. Ярлик застосування на «Робочому столі»

Після запуску Модуля, відображається діалог ключового контейнера та введення паролю для доступу до особистого ключа, Рис. 12.

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

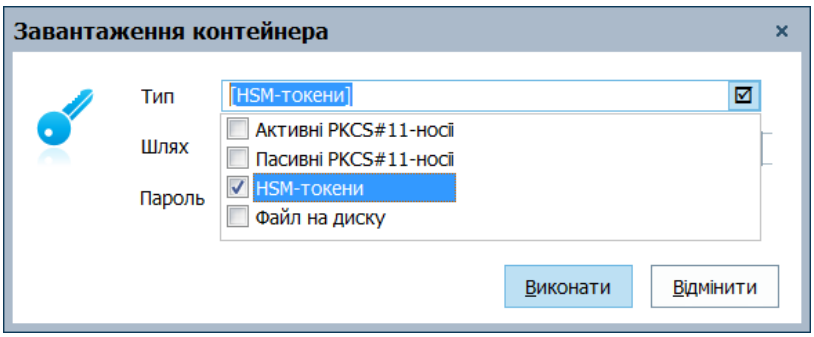

Рис. 12. Діалог вибору типу ключового носія, а також введення паролю для доступу до особистого ключа

HSM-токени

За замовчуванням, завжди обраний тип ключового контейнера «**HSM-токени**», де ключовий контейнер знаходиться на МКМ Шифр-HSM, Рис. 13.

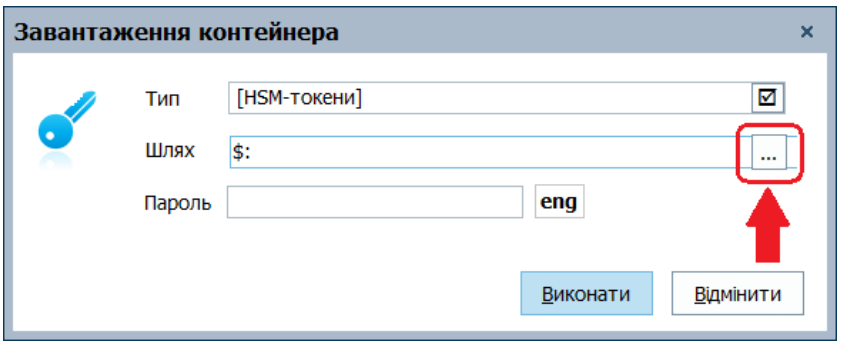

Рис. 13. Завантаження контейнера

Шлях до ключового контейнеру обирається через кнопку «...», далі відображається діалог вибору носія, Рис. 14.

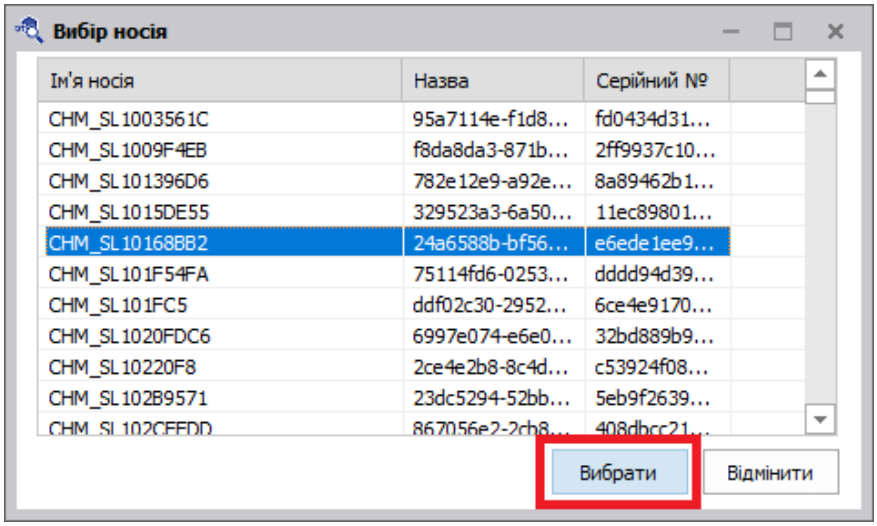

Рис. 14. Вибір носія

У пункті Шлях фіксується адреса слоту, Рис. 15.

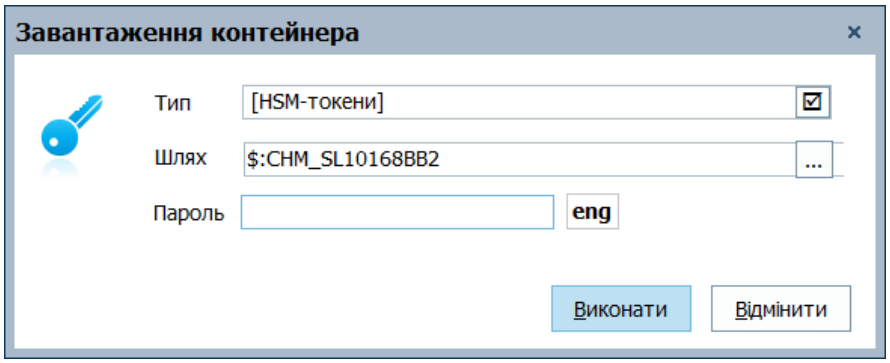

Рис. 15. Шлях до контейнеру

Вказівка пін коду до ключового контейнеру, Рис. 16.

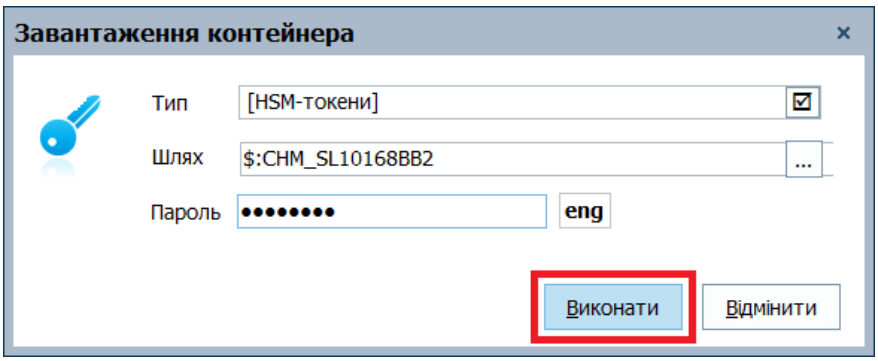

Рис. 16. Заповнення пін коду до контейнеру

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. 17-Рис. 18.

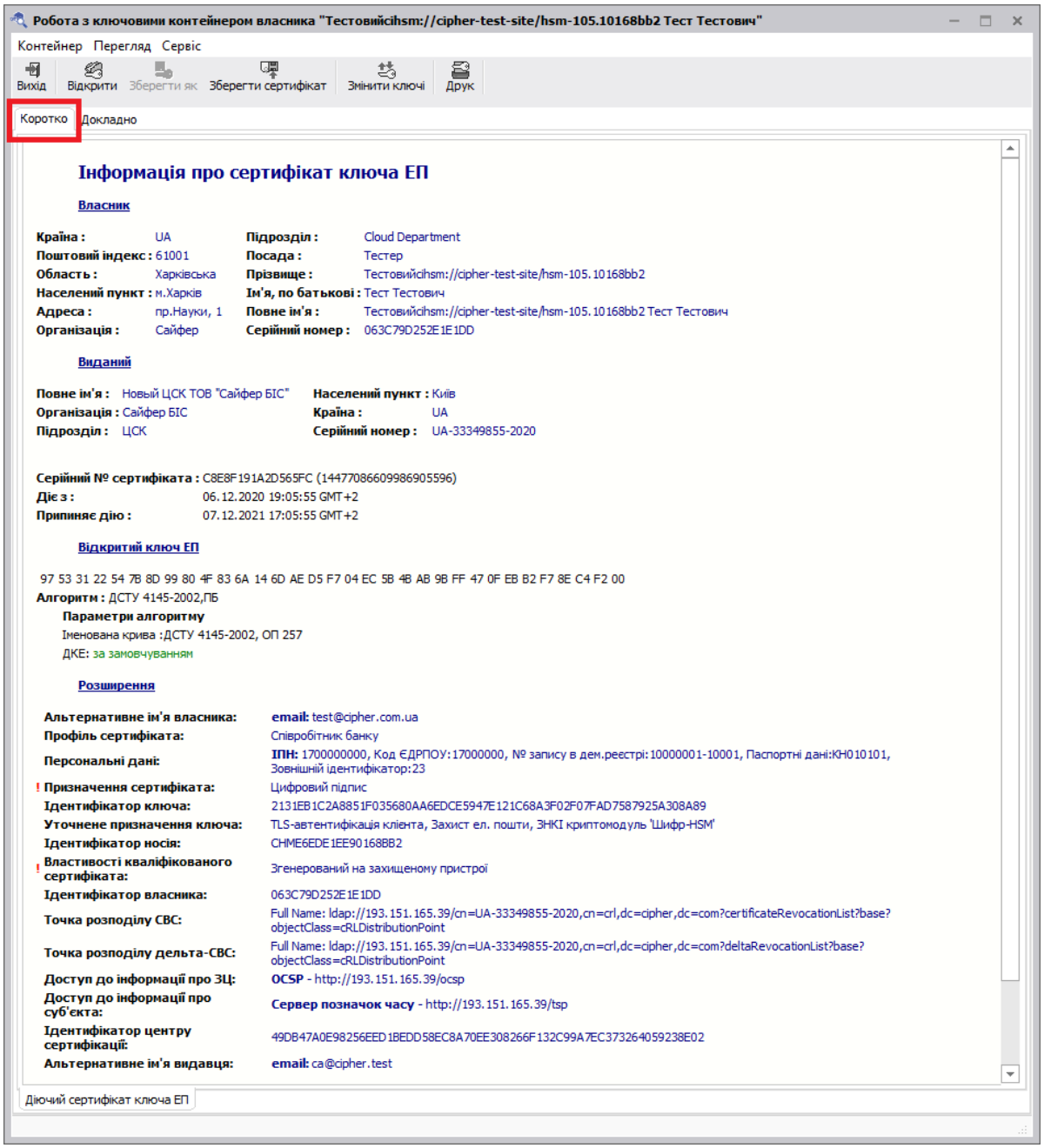

Рис. 17. Головне вікно МРКК, вкладка із коротким описом

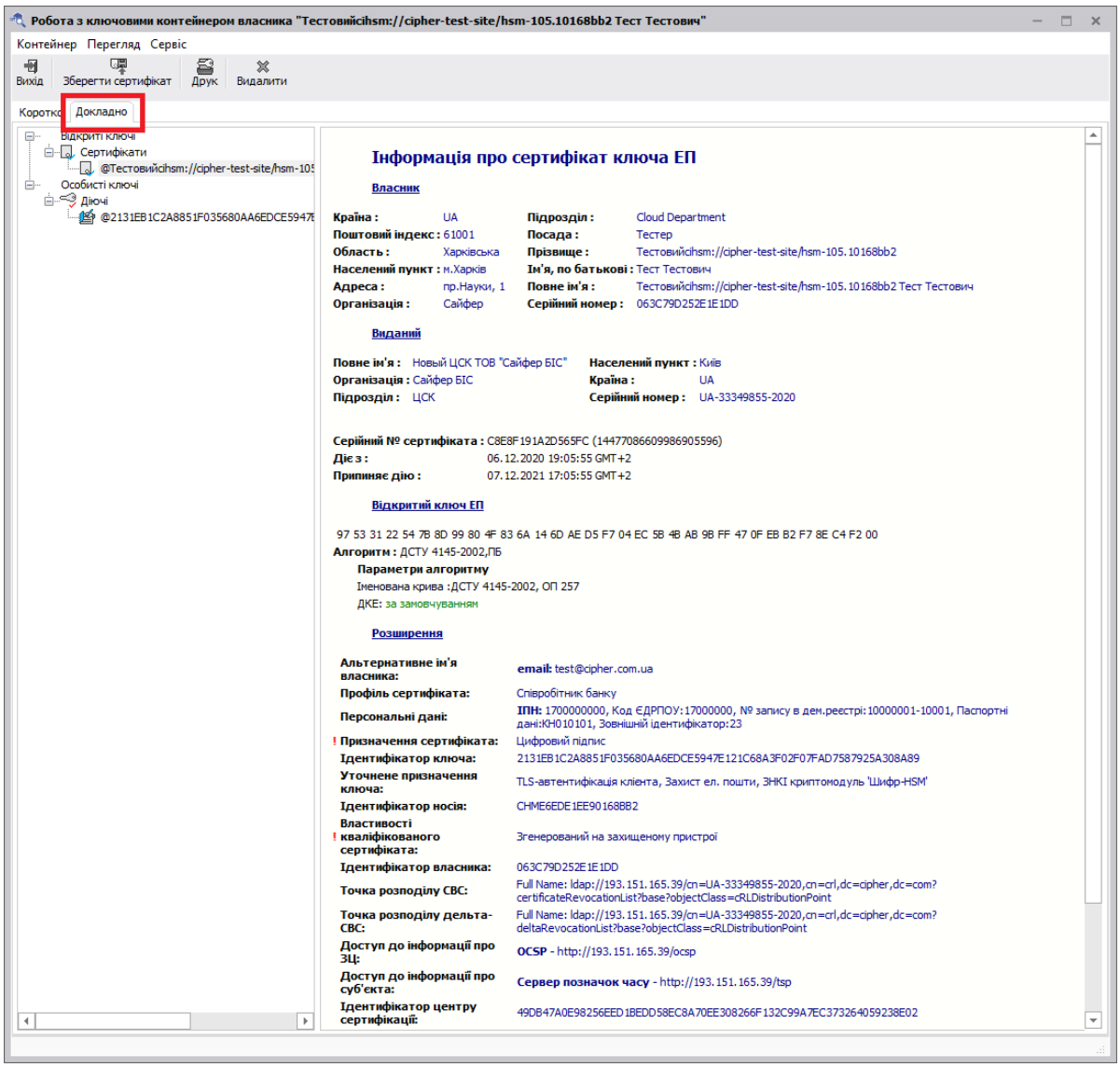

Рис. 18. Головне вікно МРКК, вкладка із докладним описом

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. 19.

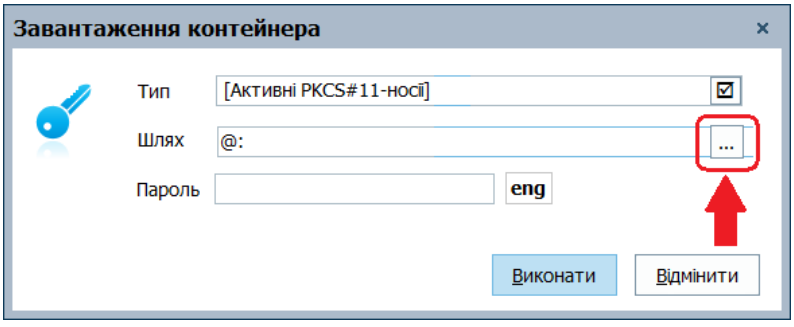

Рис. 19. Завантаження контейнера

Шлях до ключового контейнеру обирається через кнопку «...», далі відображається діалог вибору носія, Рис. 20.

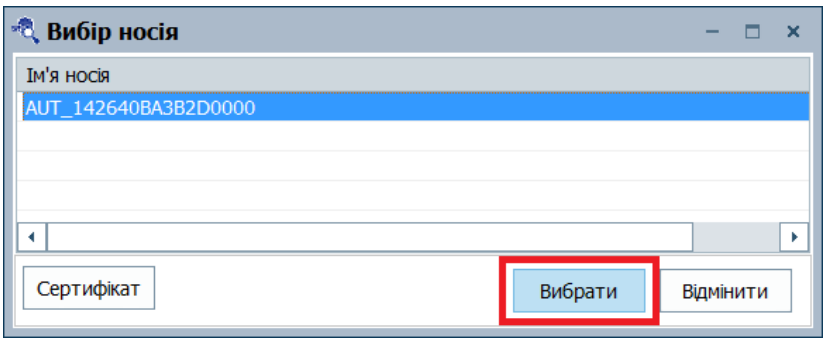

Рис. 20. Вибір носія

У пункті Шлях фіксується адреса слоту, Рис. 21.

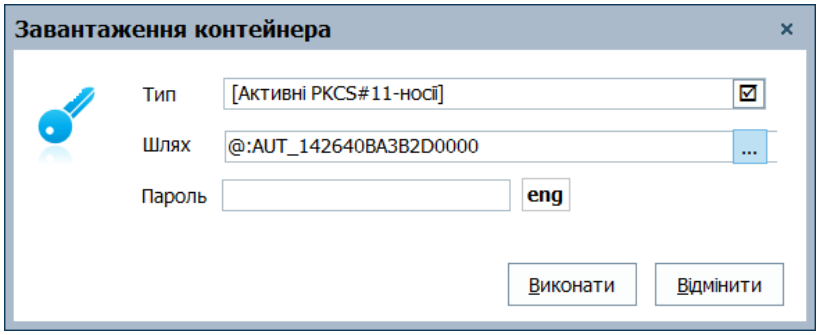

Рис. 21. Шлях до контейнеру

Введення «**Пароль**» (пін коду) до ключового контейнеру, Рис. 22.

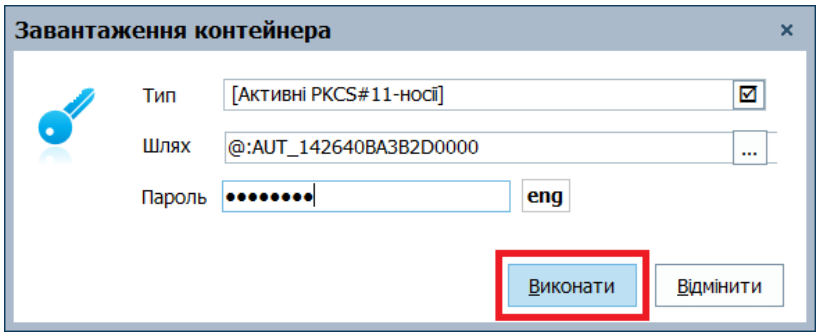

Рис. 22. Заповнення паролю (пін коду) до контейнеру

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. 23-Рис. 24.

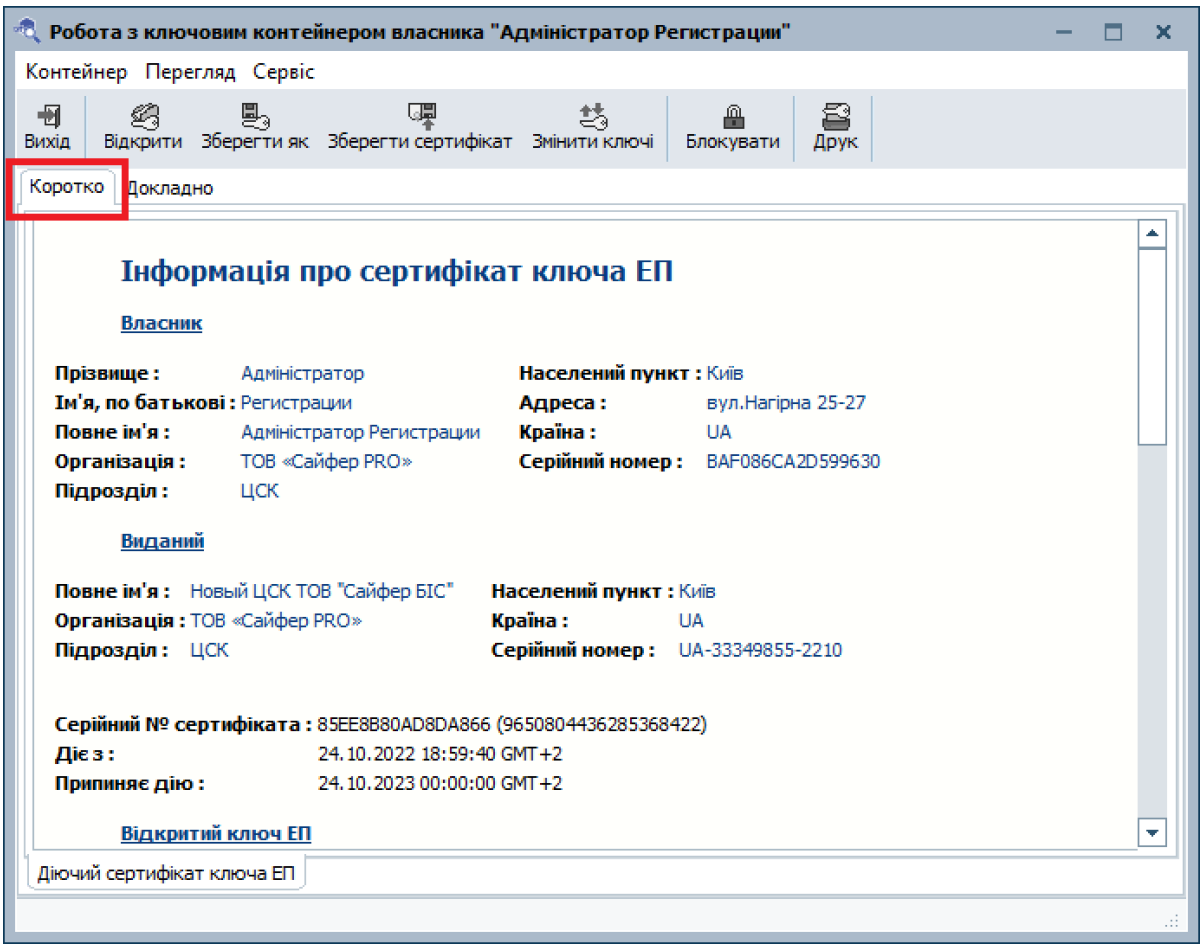

Рис. 23. Короткий опис

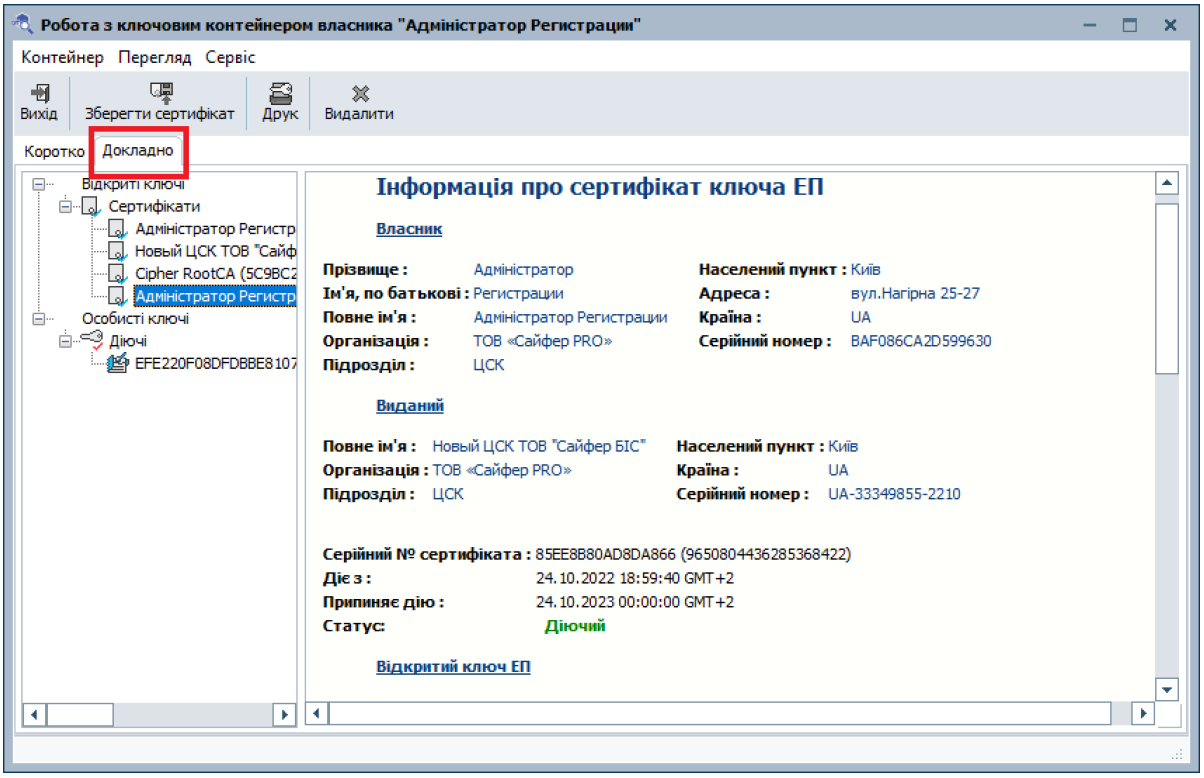

Рис. 24. Докладний опис

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. 25.

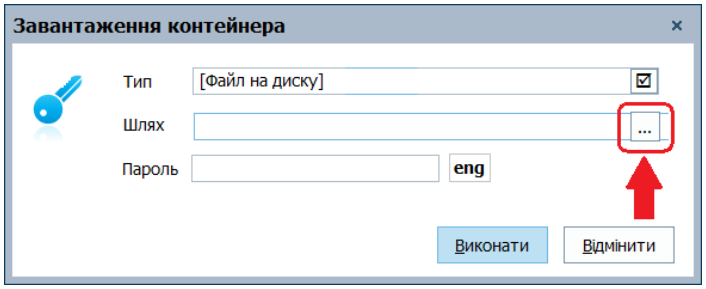

Рис. 25. Завантаження контейнера

Шлях до ключового контейнеру обирається через кнопку «**...**», далі відображається діалог вибору файлу, Рис. 26.

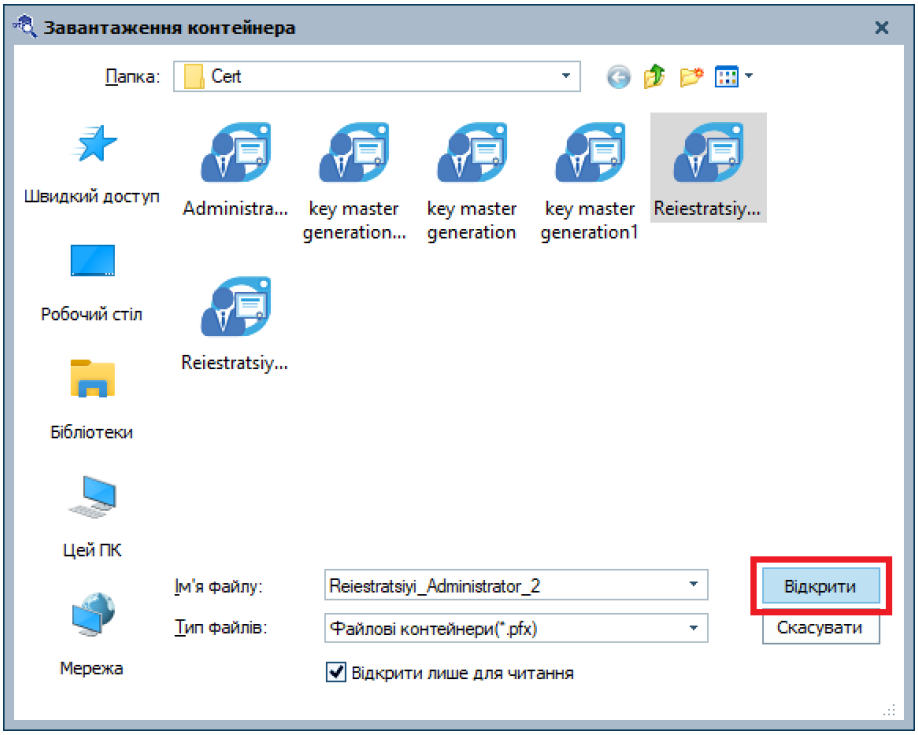

Рис. 26. Вибір файлового контейнера

У пункті Шлях фіксується адреса місцезнаходження файлового контейнеру, Рис. 27.

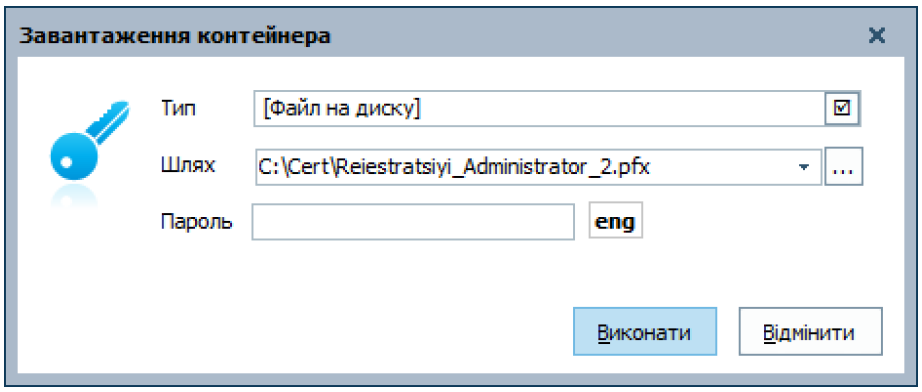

Рис. 27. Шлях до файлового контейнеру

Вказівка пін-коду до ключового контейнеру, Рис. 28.

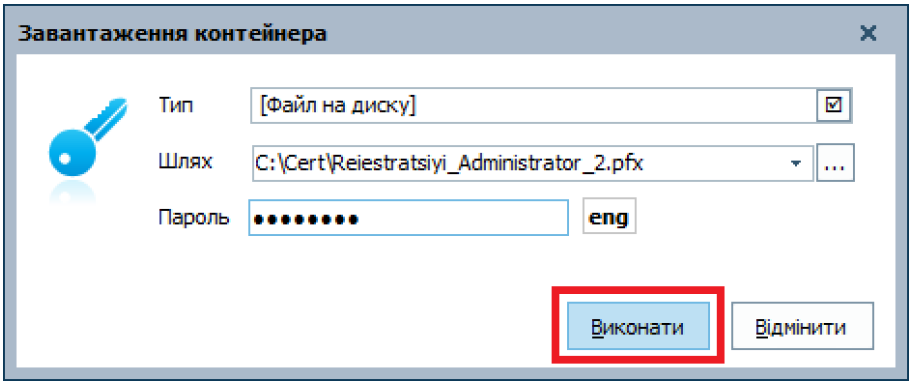

Рис. 28. Заповнення пін-коду до контейнеру

Після успішного заповнення полів, натискаємо на кнопку «**Виконати**» та отримуємо доступ до інформації, яка містить у контейнері. Інформацію можна переглянути у короткому та докладному форматах, Рис. 29-Рис. 30.

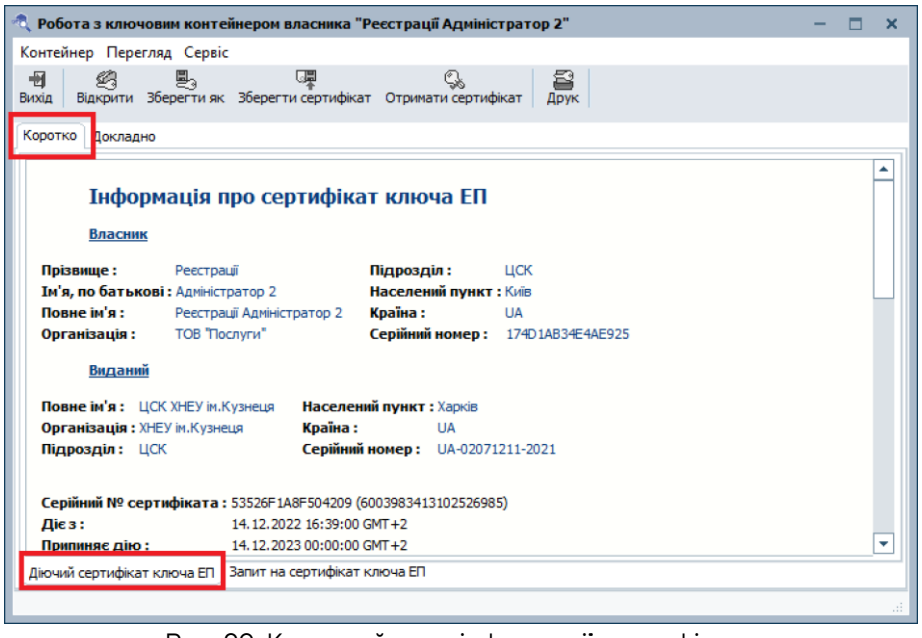

Рис. 29. Короткий опис інформації сертифіката

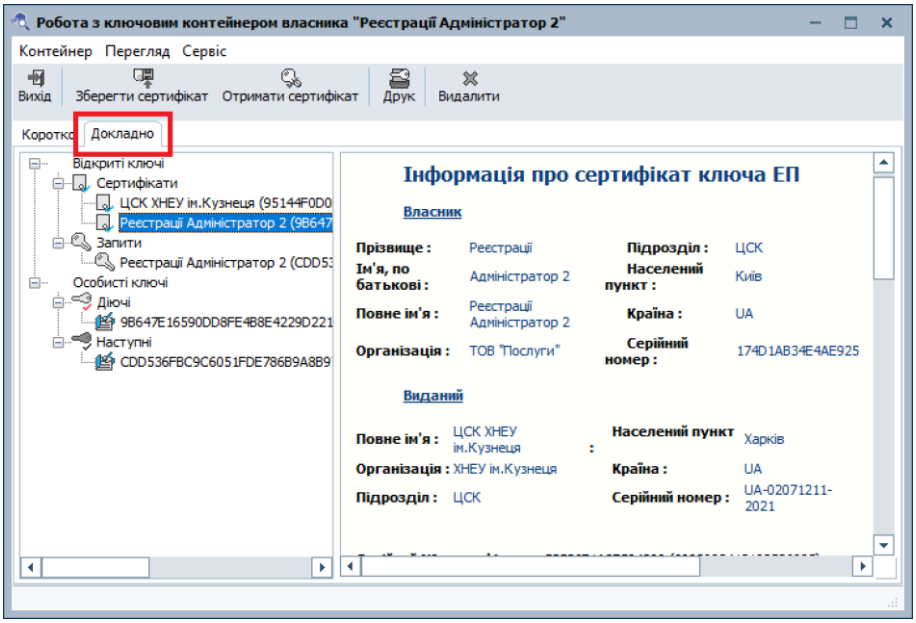

Рис. 30. Докладний опис інформації сертифіката

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.
- Надсилання запиту на сертифікат особистого ключа безпосередньо на jCMP-службу сертифікатів.
- Отримання сертифіката особистого ключа безпосередньо із jCMP-службу сертифікатів.

Кожну з наведених функцій розглянемо окремо.

Контейнер

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. 31.

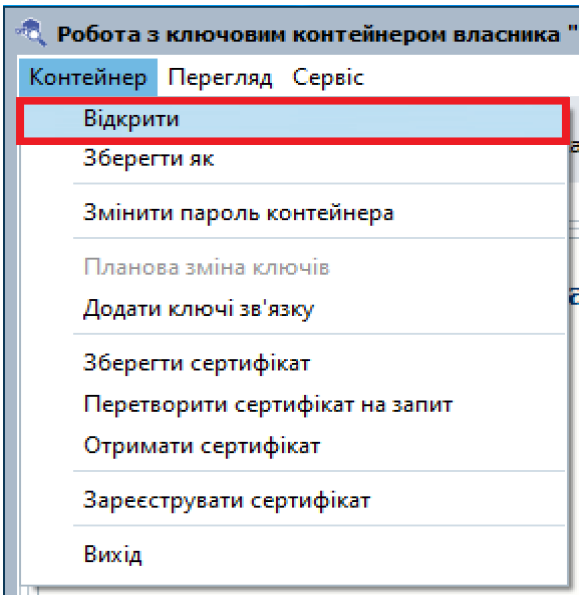

Рис. 31. Відкриття ключового контейнера для перегляду його вмісту

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 запит на сертифікат, Рис. 32.

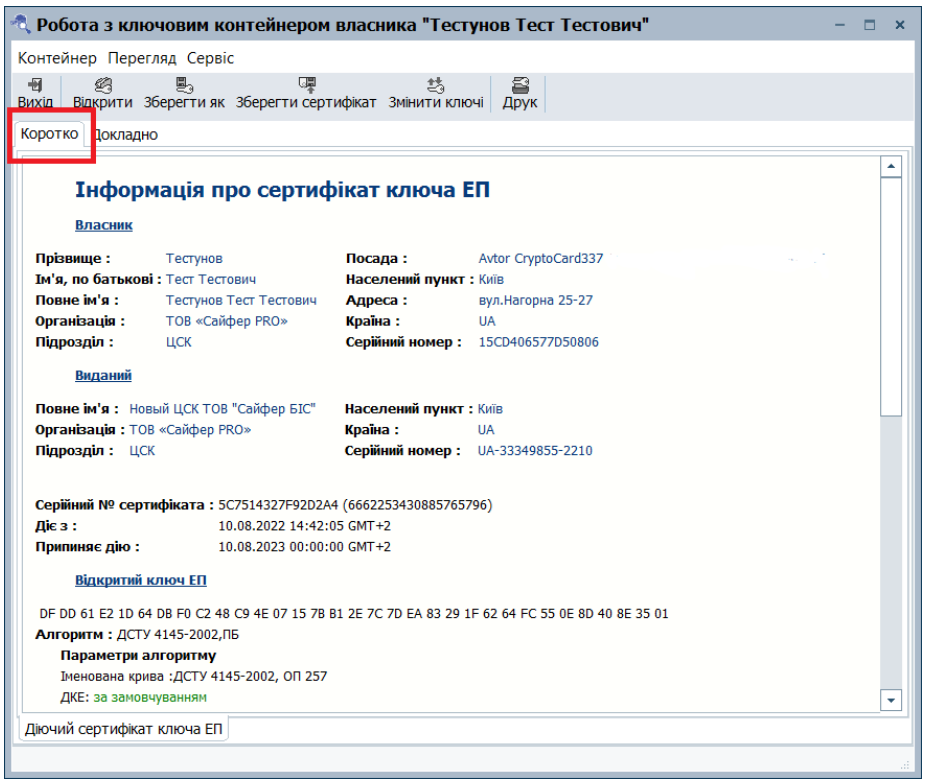

Рис. 32. Перегляд вмісту сертифікату у режимі "Коротко"

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. 33.

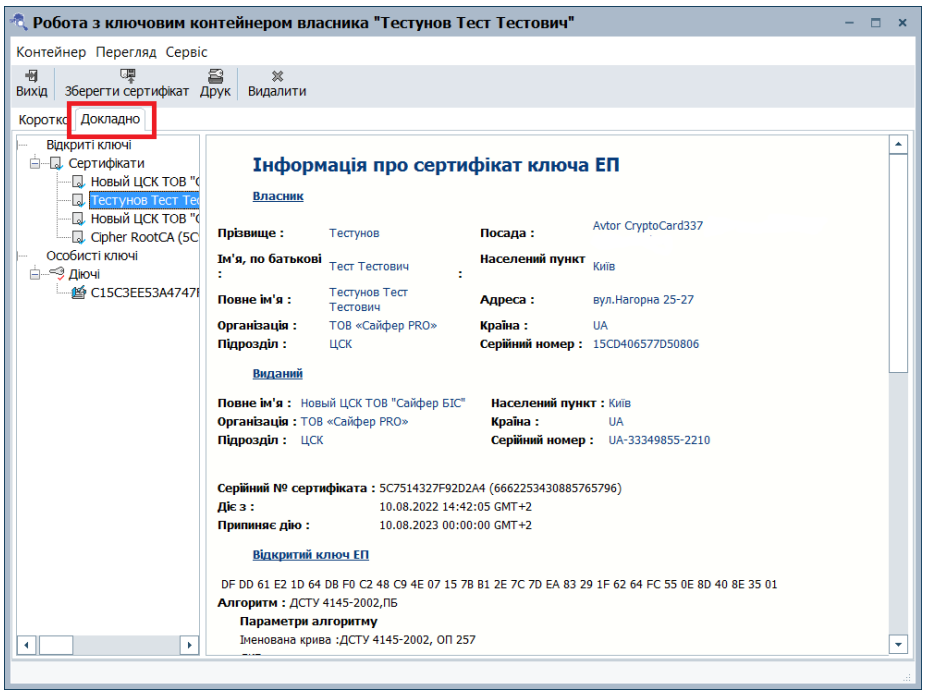

Рис. 33. Відображення сертифікату при виборі особистих ключів у режимі «Докладно»

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. 34.

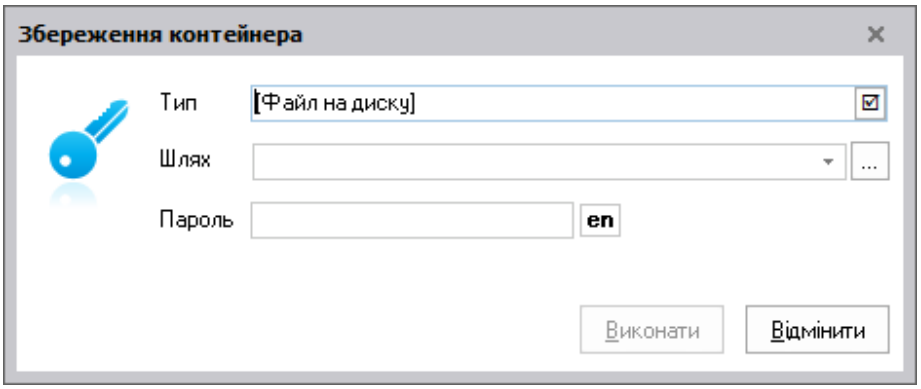

Рис. 34. Вибір носія для збереження ключового контейнера

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. 35. Слід звернути увагу на мову розкладки клавіатури, який розміщений нижче, для коректної зміни паролю.

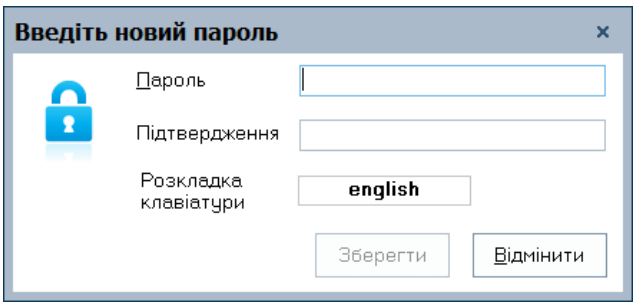

Рис. 35. Зміна паролю для обраного контейнера

Після успішної зміни паролю буде відображено відповідне повідомлення, Рис. 36.

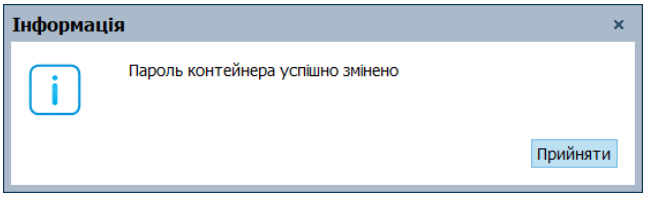

Рис. 36. Повідомлення про успішну зміну пароля до ключового контейнера

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. 37 (у залежності від типу обраного об'єкту). Буде відображене вікно з пропозицією обрання місця, для збереження файлу (Рис. 38 чи Рис. 39), після чого файл буде збережено на диску. При спробі виконати збереження особистого ключа, буде відображено повідомлення з пропозицією зберегти відповідний йому сертифікат, або запит на сертифікат.

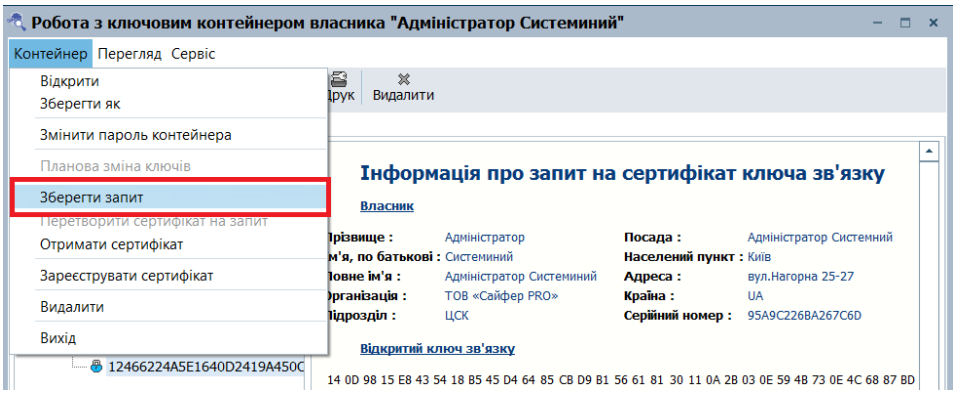

Рис. 37. Діалог з пропозицією зберегти запит

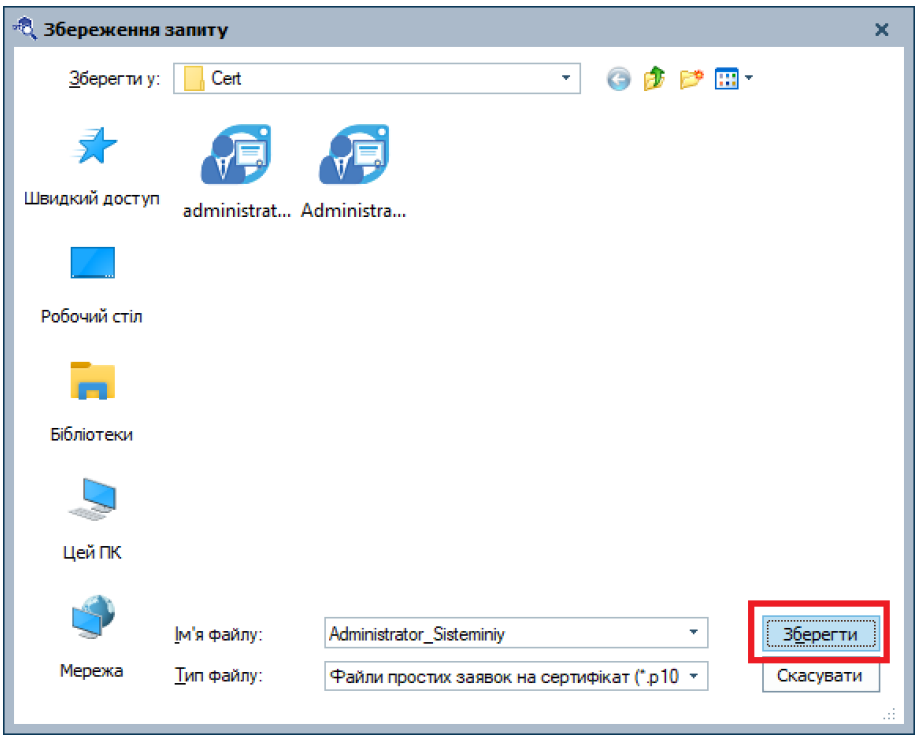

Рис. 38. Збереження запиту на сертифікат

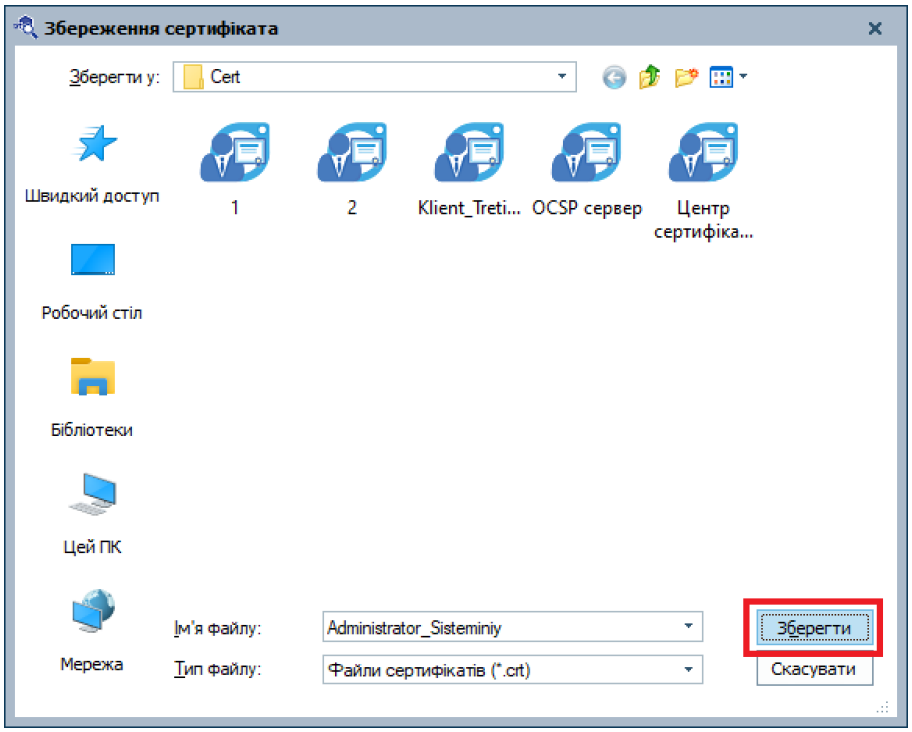

Рис. 39. Збереження сертифікату

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. 40. Після, є можливість зберегти перетворений у запит сертифікат, Рис. 41.

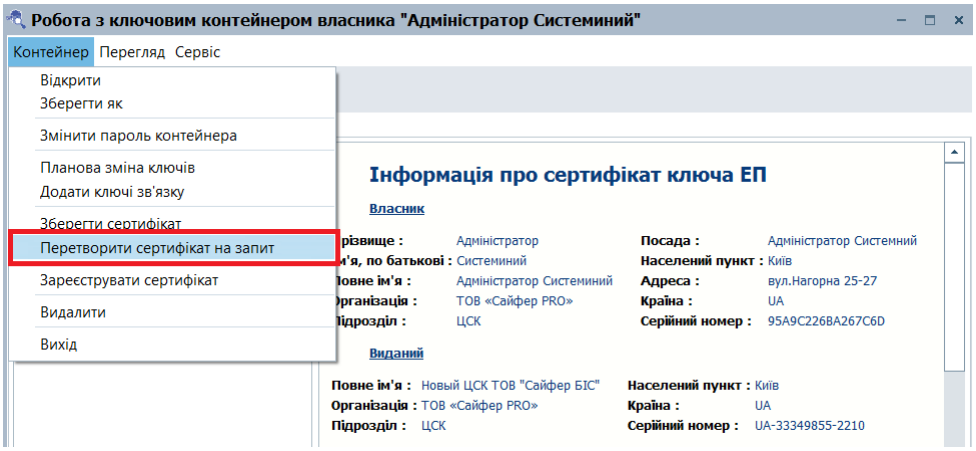

Рис. 40. Діалог «Перетворити сертифікат на запит»

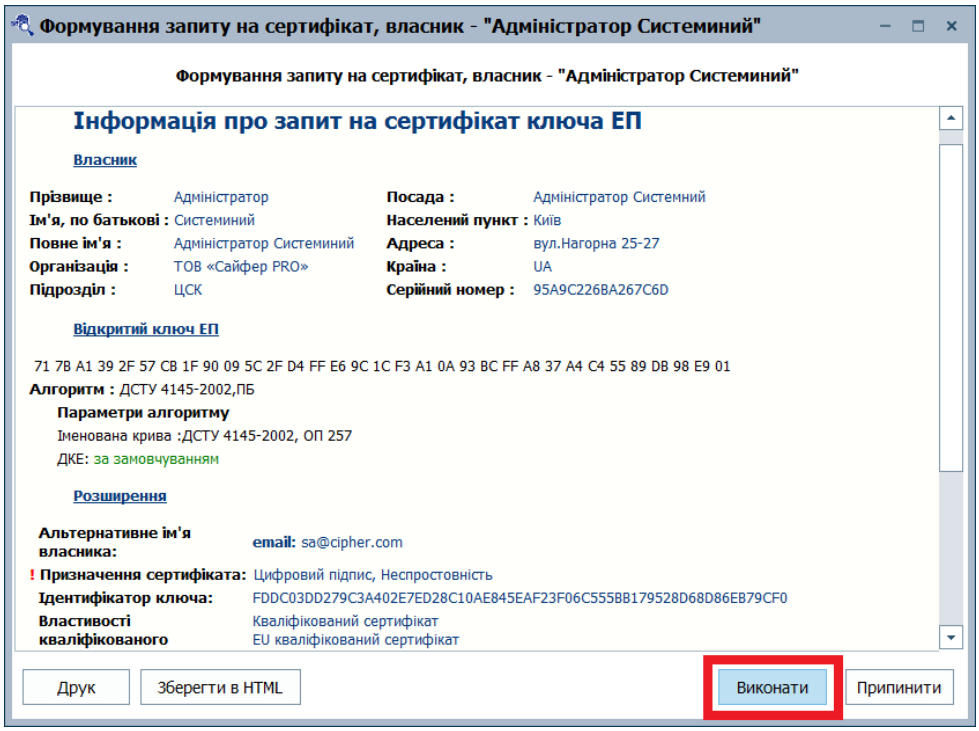

Рис. 41. Збереження перетвореного у запит сертифікату

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. 42. 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. 44,

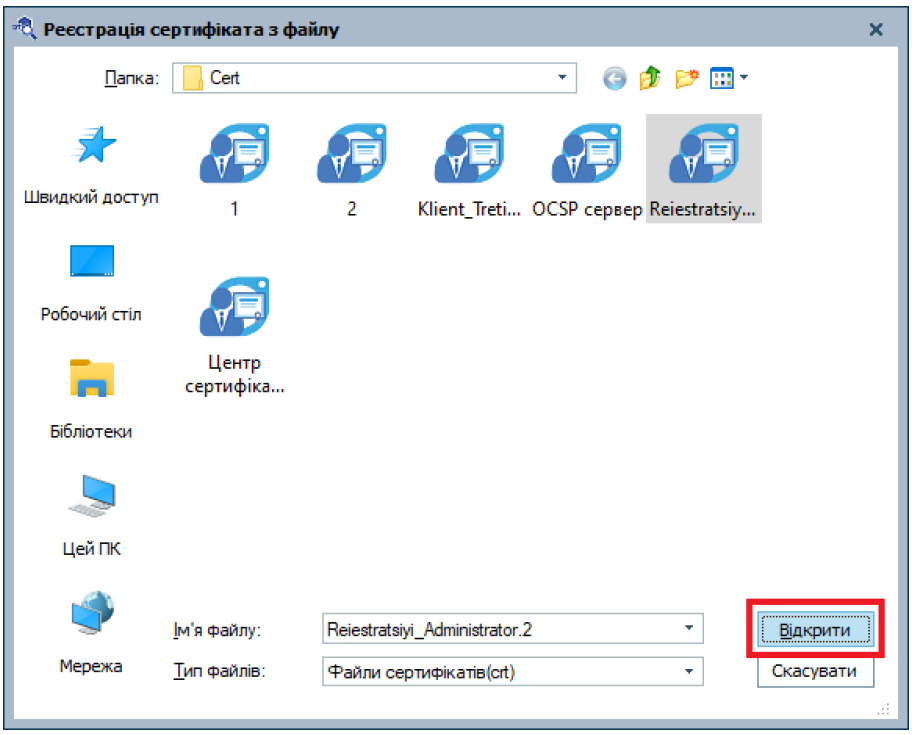

Рис. 42. Реєстрація підписаного у ЦЗО сертифікату для перезапису його у контейнері

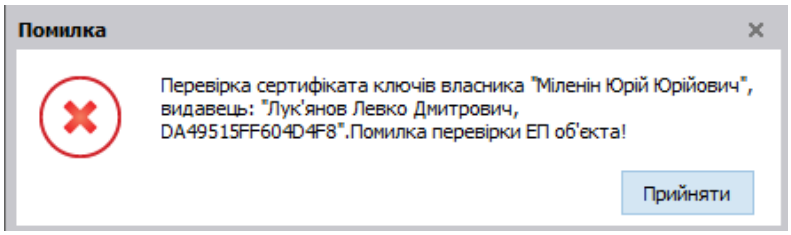

Рис. 43. Помилка при перезаписі сертифікату іншого власника у ключовий контейнер

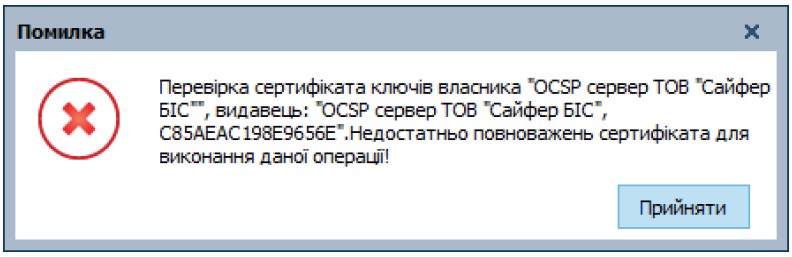

Рис. 44. Помилка при перезаписі іншого сертифікату

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. 45.

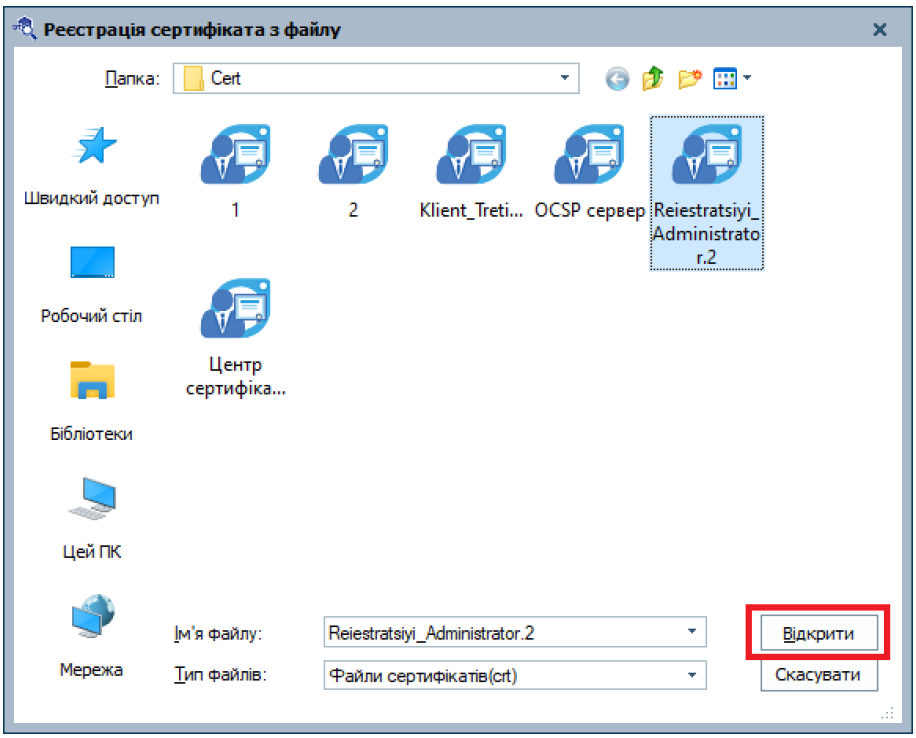

Рис. 45. Завантаження нового сертифікату до контейнера

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. 46.

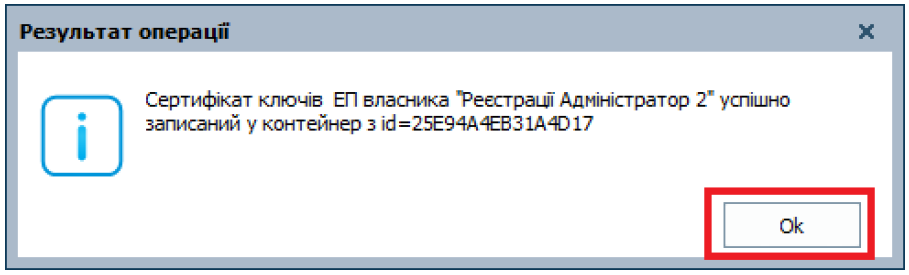

Рис. 46. Успішне завантаження сертифікату у контейнер

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

Видалення обраного сертифікату, 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. 47, після чого буде показано запит на підтвердження видалення обраного об'єкта, Рис. 48.

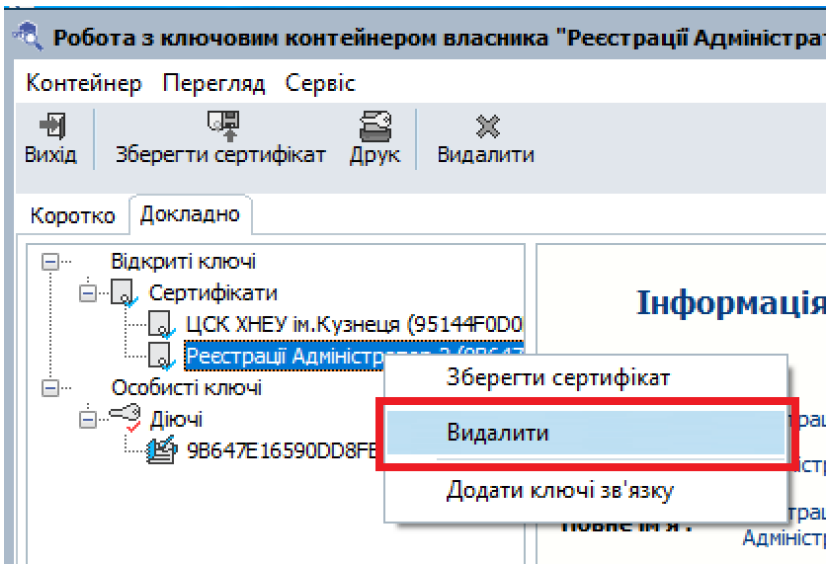

Рис. 47. Діалог видалення обраного об'єкта PKI

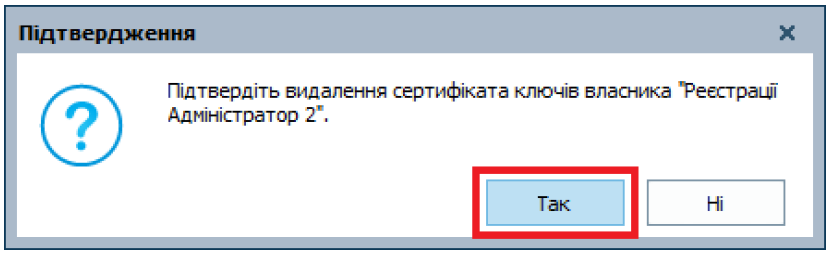

Рис. 48. Запит на підтвердження видалення об'єкта

При спробі видалення діючого сертифікату, Рис. 49, буде показане вікно, з пропозицією видалити також, запит на сертифікат та відповідний йому особистий ключ, Рис. 50 та Рис. 51.

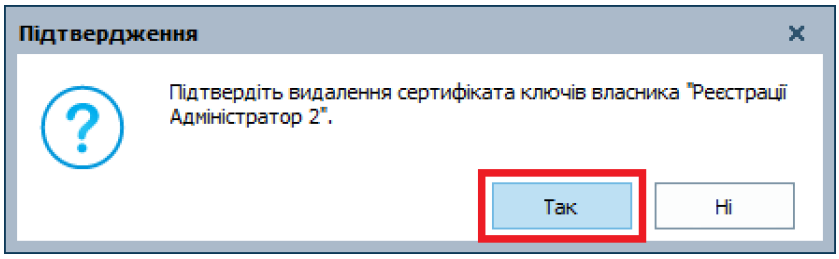

Рис. 49. Підтвердження про видалення сертифікату ключів власника

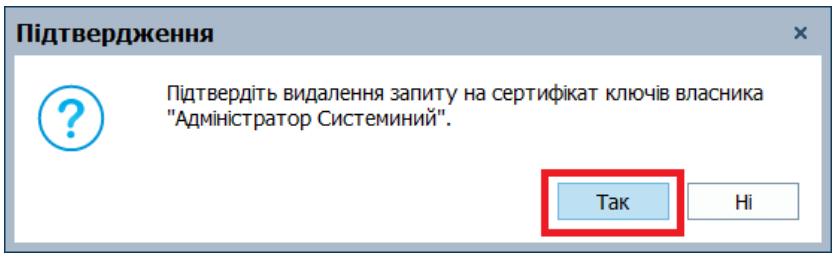

Рис. 50. Підтвердження про видалення запиту на сертифікат ключів власника

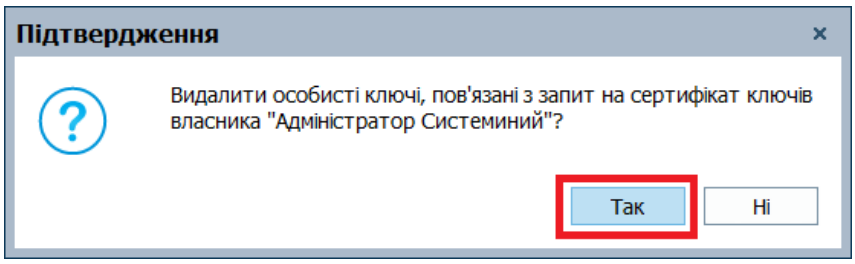

Рис. 51. Підтвердження про видалення особистого ключа, пов'язаного і із запитом на сертифікат ключів власника

Після успішного видалення сертифіката, запиту та ключів, буде показано відповідне повідомлення, Рис. 52 та Рис. 53.

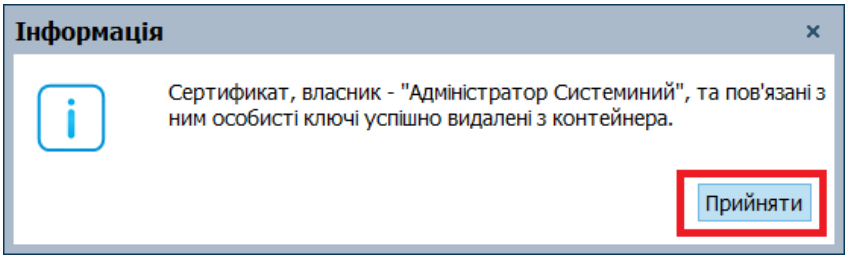

Рис. 52. Повідомлення про успішне видалення сертифіката і ключа власника

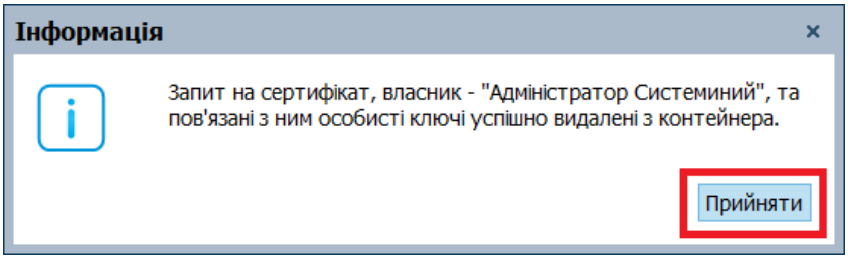

Рис. 53. Повідомлення про успішне видалення запиту на сертифікат ключів власника

Перегляд

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. 54. 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).

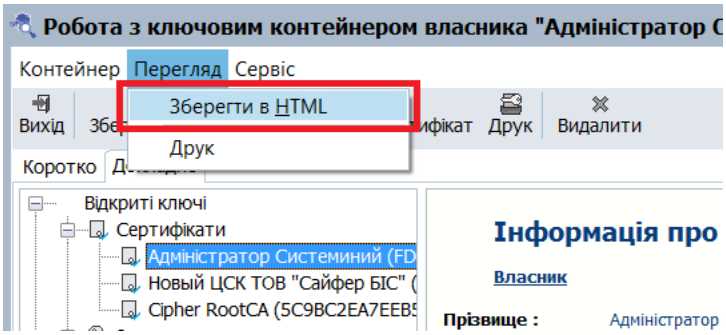

Рис. 54. Діалог збереження у HTML-файлі

Після вибору меню «**Зберегти в HTML**», буде відображено вікно, з пропозицією вказати, куди слід зберегти HTML-файл, Рис. 55.

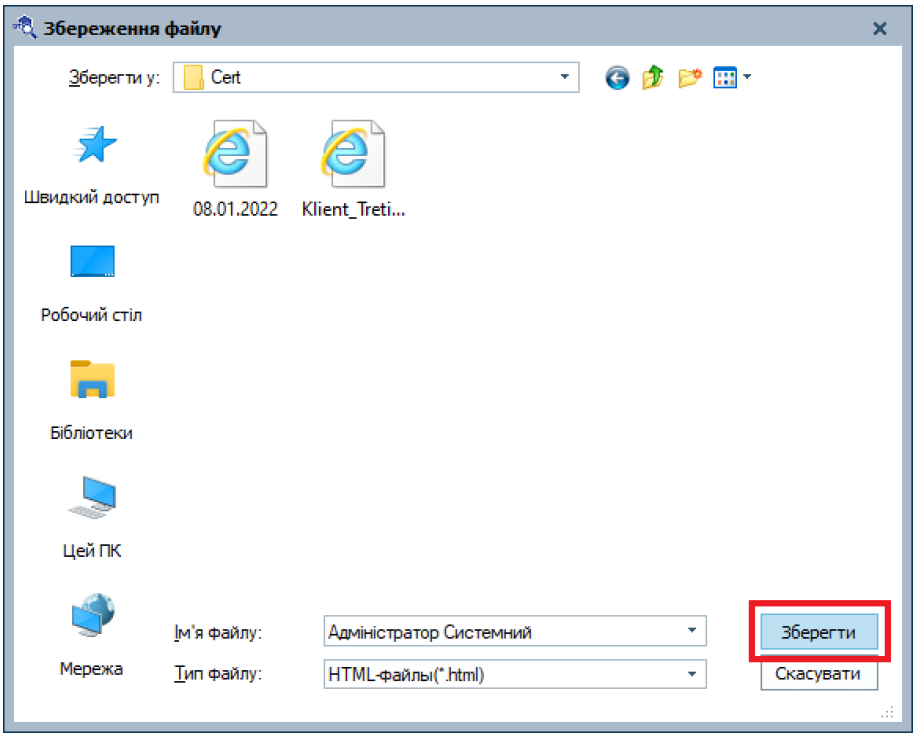

Рис. 55. Збереження обраного сертифікату у форматі HTML

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. 56.

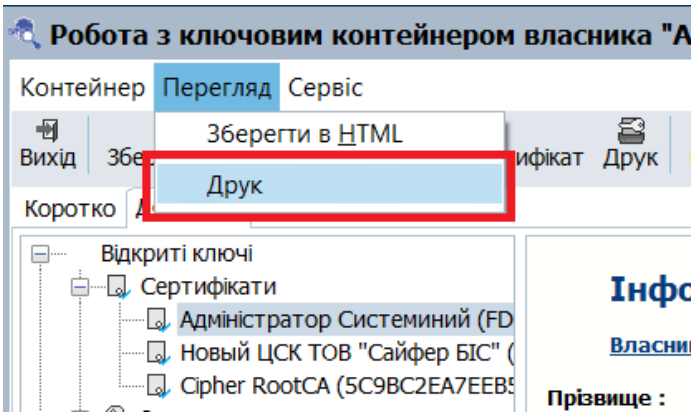

Рис. 56. Діалог вибору інформації про сертифікат для друку

За допомогою діалогу друку, можна обрати принтер для друку, кількість копій і т.д., Рис. 57.

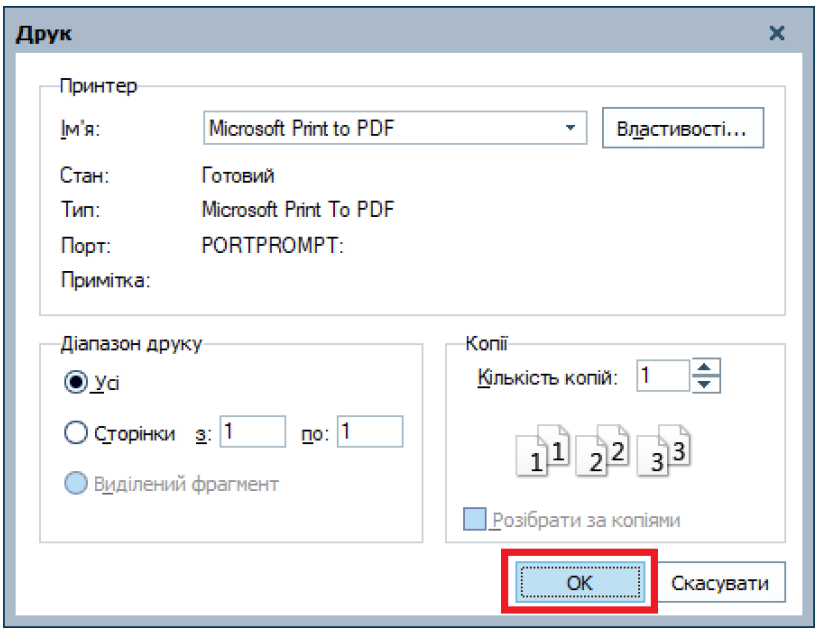

Рис. 57. Друк обраного сертифікату

Сервіс

Параметри «Налаштування»

Налаштування цих параметрів дає змогу програмі взаємодіяти з jCMP-службою, HSM-модулем, та увімкнути контроль джерела точного часу Для виклику вікна діалогу необхідно обрати в меню «**Сервіс**», потім «**Налаштування**».

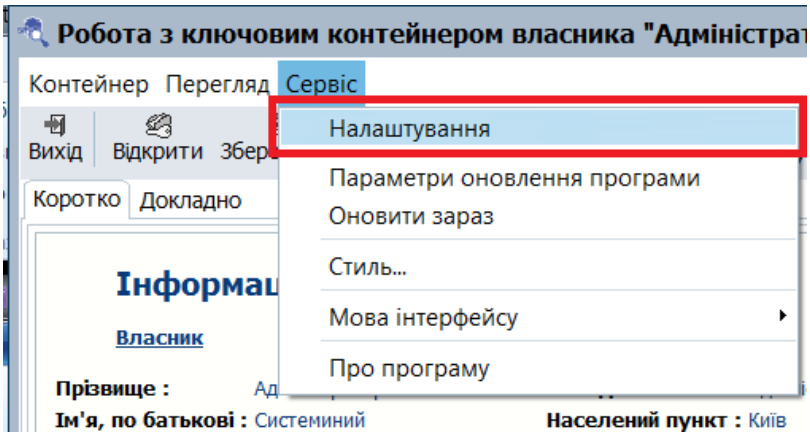

Рис. 58. Виклик вікна діалогу «Налаштування» МРКК

Вкладка «Параметри»

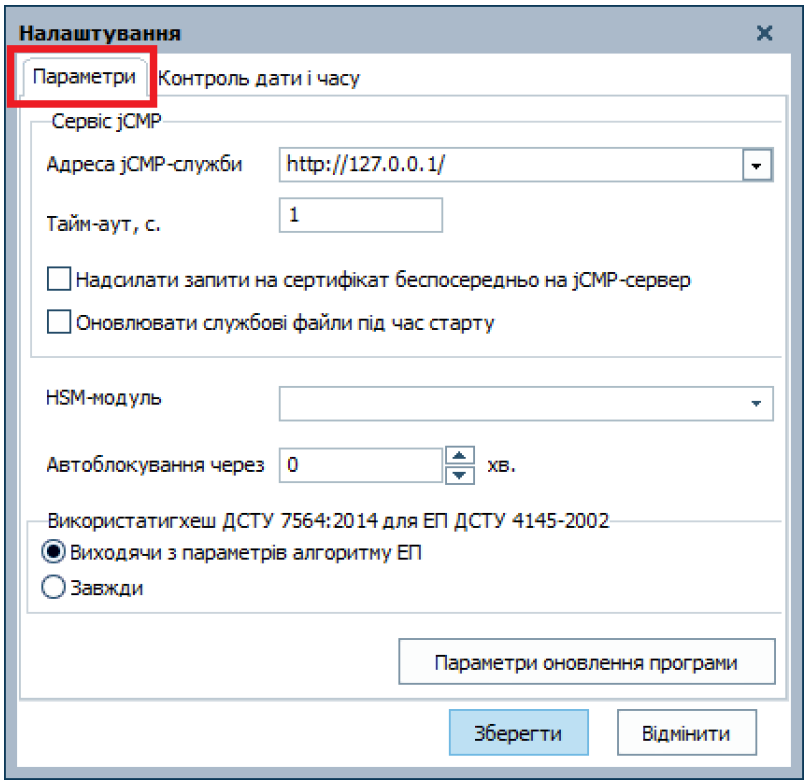

Рис. 59. Діалог вікна налаштувань, вкладка Параметри

Група «Сервіс jCMP»

Адреса jCMP-служби

Адреса, за якою програма звертатиметься до функцій jCMP-служби, має формат «http://IP-адреса (або DNS имя серверу jCMP-служби)/». Наприклад «http://192.168.37.1/»

Тайм-аут

Тайм-аут очікування відгуку служби у секундах.

Надсилати запит на сертифікат безпосередньо на jCMP-сервер

При зміні ключів запит на сертифікат буде не у файл, а безпосередньо надсилається на сервер jCMP-служби сертифікатів. При цьому можливе отримання сертифіката безпосередньо із служби.

Оновлювати службові файли під час старту

У процесі старту здійснюватиметься перевірка на наявність оновлень службових файлів програми (XCGF тощо) та їх завантаження.

HSM-модуль

Адреса HSM-модулю, до якого планується здійснювати підключення.

Адреса має бути вказана саме у такому форматі, «tcp://IP-адреса модулю : порт»

Наприклад: «tcp://192.168.0.136:2345»

Автоблокування через « » хв.

Автоматичне блокування програми з вимогою пароля. Як пароль використовується пароль шифрування поточного особистого ключа.

Група «Використати геш ДСТУ 7564:2014 для ЕП ДСТУ 4145-2002»

Підтримка зв'язку нової функція гешування, затвердженої наказом Міністерства економічного розвитку і торгівлі України. Може приймати значення:

- Виходячи з параметрів алгоритму ЕП.
- Завжди.

«Параметри оновлення програми»

Дивись розділ «**Централізоване оновлення застосування**», Рис. 63-Рис. 64

«Контроль дати і часу»

На Рис. 60 наведений діалог параметрів «**Контроль дати та часу**». Дане налаштування необхідне з огляду на можливу відмінність часу робочої станції, на якій встановлено МРКК, від часу, яке використовує Сервер застосувань ЦСК. Зупинимося на описі параметрів даної вкладки.

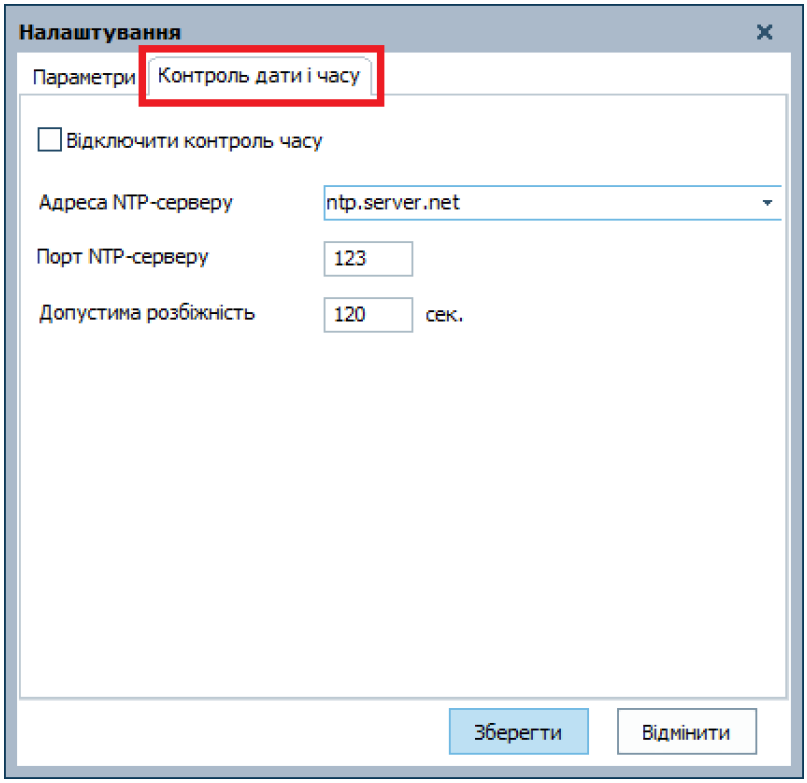

Рис. 60. Вкладка «Контроль дати і часу»

Відключити контроль часу

У випадку активної даної позначки, МРКК буде використовувати системний час машина, на якій він встановлений в якості джерела точного часу.

Якщо дана позначка не активна, буде використовуватись джерело точного часу згідно вказаних нижче налаштувань.

Адреса NTP-серверу

Вказується IP-адреса чи DNS ім'я Сервера точного часу. Рекомендується обрати єдине джерело точного часу для всього ЦСК, котрий може бути, як публічним NTP-сервером, доступним з мережі Інтернет, так і внутрішнім сервером доступним в рамках мережі організації.

Порт NTP-серверу

Порт підключення, за замовчуванням вказується, як 123. Порт може бути змінений на стороні NTP-сервера, що спричинить необхідність зміни його на всіх робочих місцях, в тому числі і в налаштуваннях МРКК.

Допустима розбіжність

Вказується допустиме розходження часу, використовуваного МРКК від часу, отримуваного від NTP-сервер. При підвищені розходження більш, ніж вказано у даному пункті, буде здійснена автоматична синхронізація часу.

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 «**Сервіс**» - «**Оновити зараз**», Рис. 61.

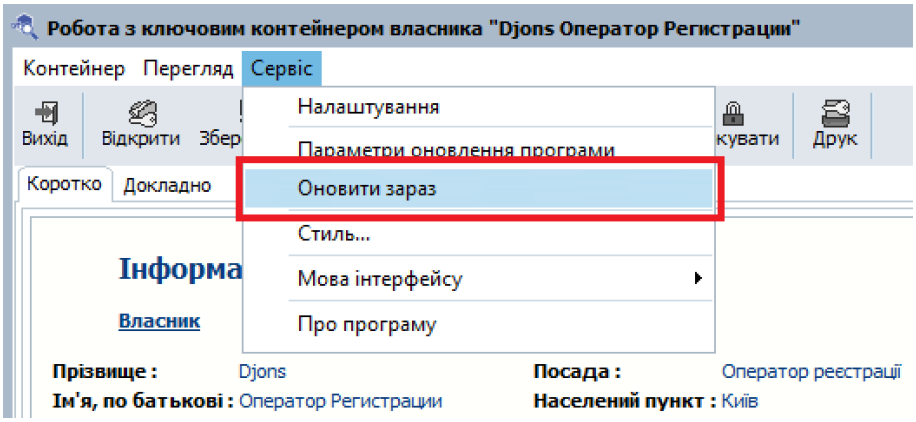

Рис. 61. Пункт меню «Оновити зараз»

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. 62.

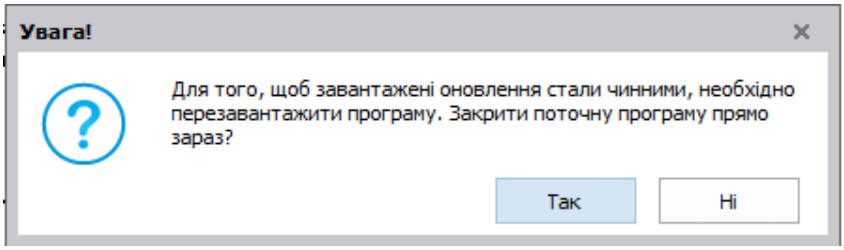

Рис. 62. Інформація про оновлення програми

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

В меню «**Сервіс**» - «**Параметри оновлення програми**» можна здійснити налаштування, Рис. 63.

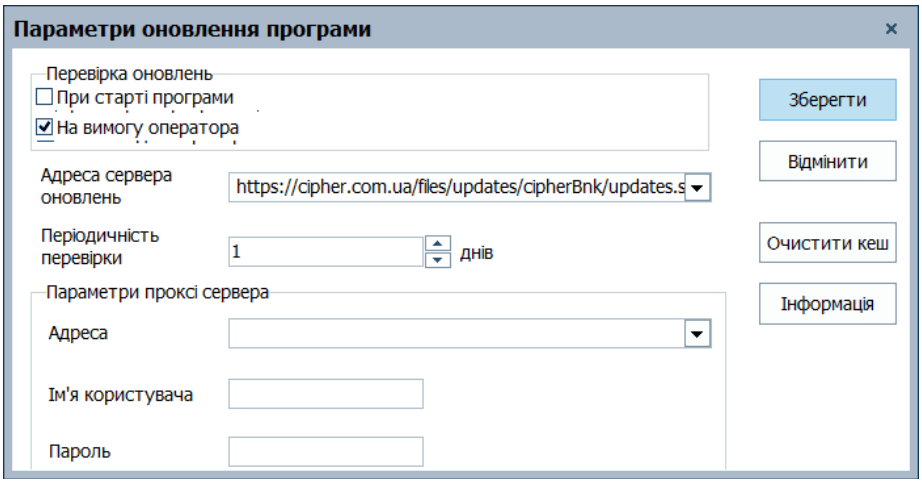

Рис. 63. Меню «Параметри оновлення програми»

Вказавши позначку «**При старті програми**» - дає можливість перевіряти оновлення при старті та встановити нові оновлення.

«**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. 64. Якщо вказати **1**, то перевірка буде здійснюватися щодня, відповідно, якщо **2**, то раз у два дні.

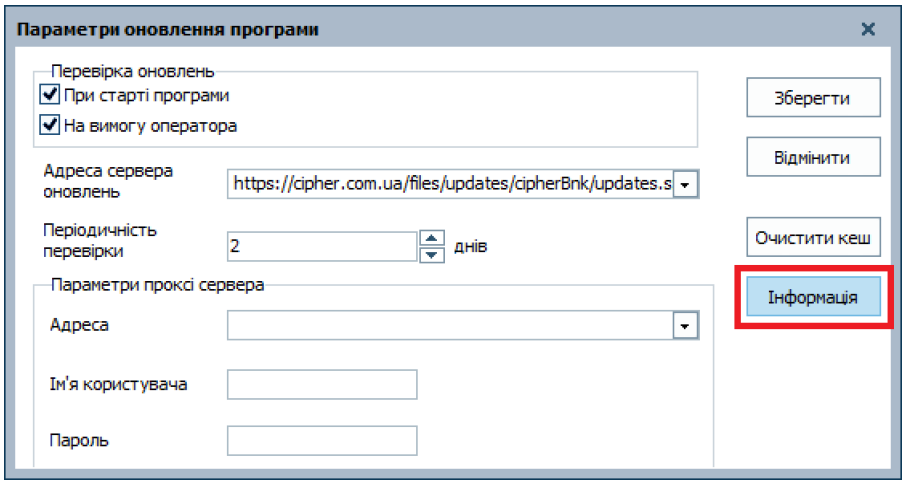

Рис. 64.Кнопка виклику діалогу «Інформація» вікна «Параметри оновлення програми»

Для перегляду інформації щодо останнього оновлення програми необхідно натиснути кнопку «**Інформація**». Буде виведено детальну інформацію щодо дати та часу оновлення, де були внесені зміни та їх редакція/версія, Рис. 65.

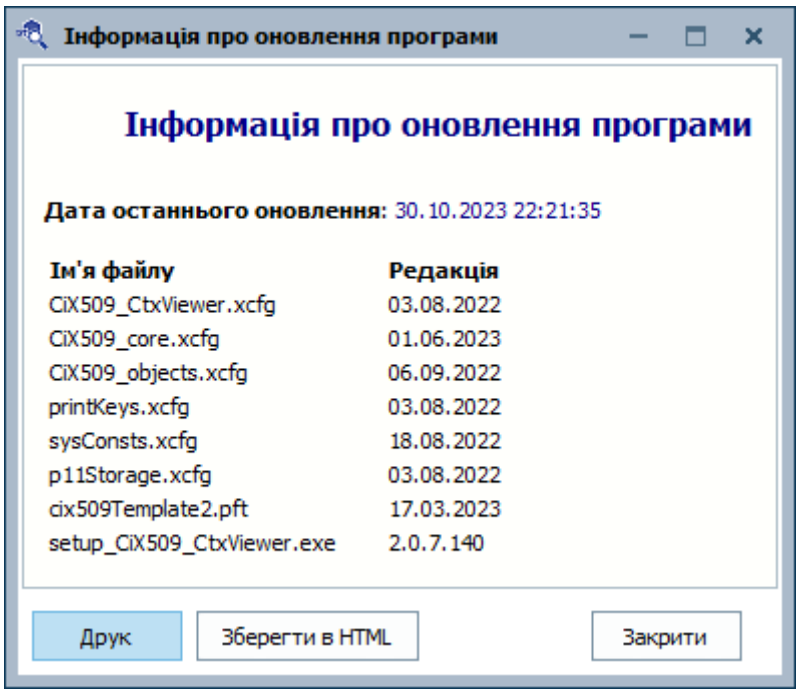

Рис. 65. Інформація про дату останнього оновлення та редакції файлів

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 контейнера	Дозволяє змінити пароль до обраного файлового контейнера.
	Планова зміна ключів	Дозволяє згенерувати запит на сертифікат ключа, термін сертифікату якого незабаром сплине.
	Змінити ключі	Дозволяє примусово, достроково згенерувати новий ключ і запит на сертифікат.
	Додати ключі зв'язку	Дозволяє додати ключі зв'язку, якщо вони відсутні.
	Зберегти запит/ сертифікат	Дозволяє зберегти сертифікат чи запит на сертифікат у файл.
	Перетворити сертифікат на запит	Дозволяє перетворити діючий сертифікат у запит на сертифікат для подальшої його відправки у засвідчувальний центр чи ЦЗО.
	Отримати сертифікат	Дозволяє завантажити сертифікат виданий засвідчувальним центром чи ЦЗО
	Зареєструвати сертифікат	Дозволяє зареєструвати у ключовому контейнері сертифікат, виданий засвідчувальним центром чи ЦЗО, або 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.
Сервіс	Налаштування	Дозволяє здійснити налаштування параметрів програми: зміна адреси та налаштувань роботи з jCMP-службою, увімкнути контроль джерела точного часу
	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.
	Стиль	Дозволяє обрати та встановити стиль оформлення вікон застосування.
	Мова інтерфейсу	Дозволяє змінити мову інтерфейсу. Доступні Українська чи Російська. Зміни вступають в силу після перезавантаження застосування
	Про програму	Дозволяє отримати детальну інформацію про застосування, версію та розробника.