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.34

Система криптографічного захисту інформації "Шифр-X.509"

Модуль генерації ключів. Керівництво з експлуатації

Зміст

Список скорочень та умовних позначень

LDAP	Lightweight Directory Access Protocol
PIN	Personal Identification Number
TCP	Transmission Control Protocol
АРМ	Автоматизоване робоче місце
БД	База даних
ЕП	Електронний підпис
МГК	Модуль генерації ключів
ОС	Операційна система
ПЕМВ	Побічні електромагнітні випромінювання
ПЗ	Програмне забезпечення
ПТК	Програмно-технічний комплекс
СВС	Список відкликаних сертифікатів
СКЗІ	Система криптографічного захисту інформації
СУБД	Система управлінням базами даних
ЦР	Центр реєстрації
ЦСК	Центр сертифікації ключів

Введення

Вступ

Даний документ є керівництвом Користувача по роботі з МГК у ЦР, призначеного для роботи під управлінням ОС Windows 7 та 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.

Рекомендована апаратна конфігурація

- Відповідає вимогам ОС Microsoft Windows 10.
- Вільного дискового простору: 1 Гб.

Програмне забезпечення

Мінімальна конфігурація:

- Microsoft Windows 7.

Рекомендована конфігурація

- Microsoft Windows 10.

Мережеве забезпечення

Для роботи застосування немає необхідності у мережевому підключенні.

Захищені ключові носії

Застосування підтримує роботу із захищеними ключовими носіями за інтерфейсом 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 Модуля генерації ключів

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-X.509».

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

Встановлення

Для встановлення МГК необхідно завершити всі невикористовувані задачі, після чого запустити файл **setup_CiX509_CHK.exe** з інсталяційного носія та слідувати вказівкам програми установки.

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

Після запуску **setup_CiX509_CHK.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 генерації ключів, Рис. 1. За нагоди можна змінити у меню Сервіс – Мова інтерфейсу.

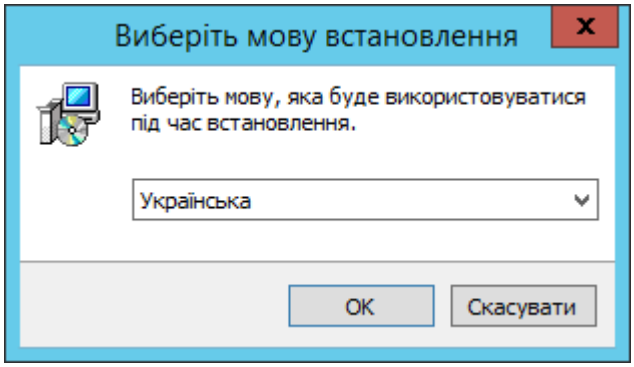

Рис. 1. Вибір мови встановлення

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

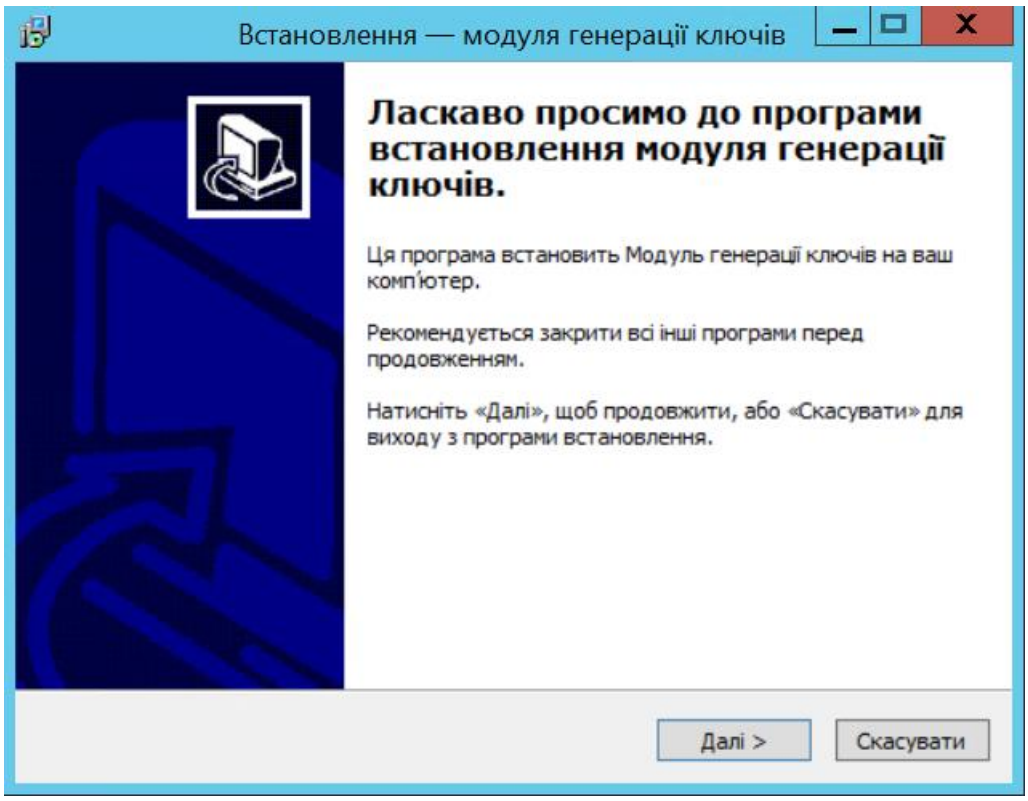

Рис. 2. Діалог Привітання

На діалозі **Привітання**, слід натиснути **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 вказавши, **Я приймаю угоду**. Для переходу до наступного діалогу, необхідно натиснути кнопку **Далі**.

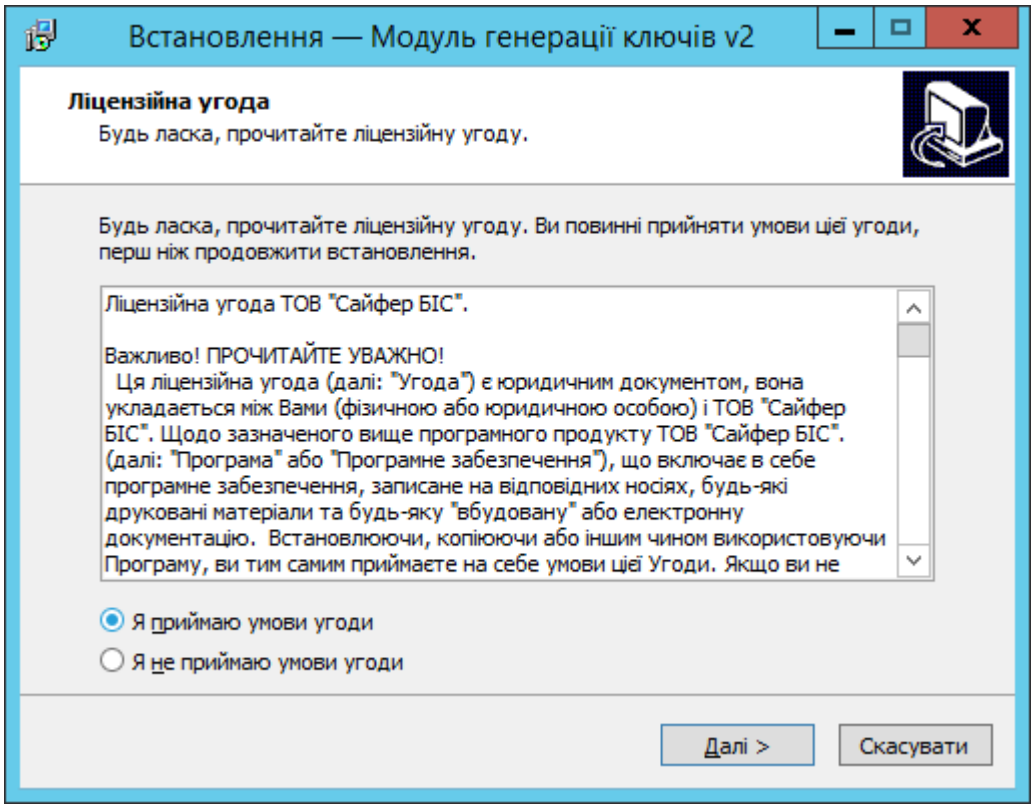

Рис. 3. Діалог з інформацією про ліцензію на використання ПЗ

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

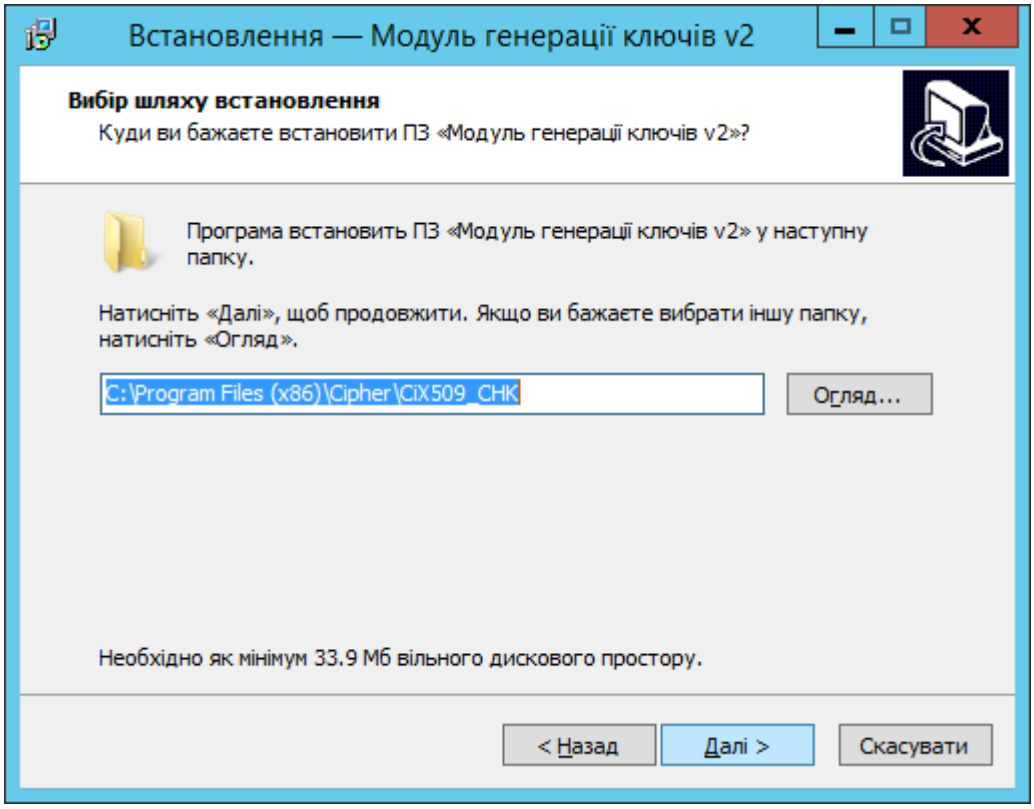

Рис. 4. Діалог вибору папки, куди буде встановлено МГК

Наступний діалог **Вибір папки в меню «Пуск»**, дозволить обрати до якої папки в меню «Пуск» будуть встановлені компоненти МГК, Рис. 5.

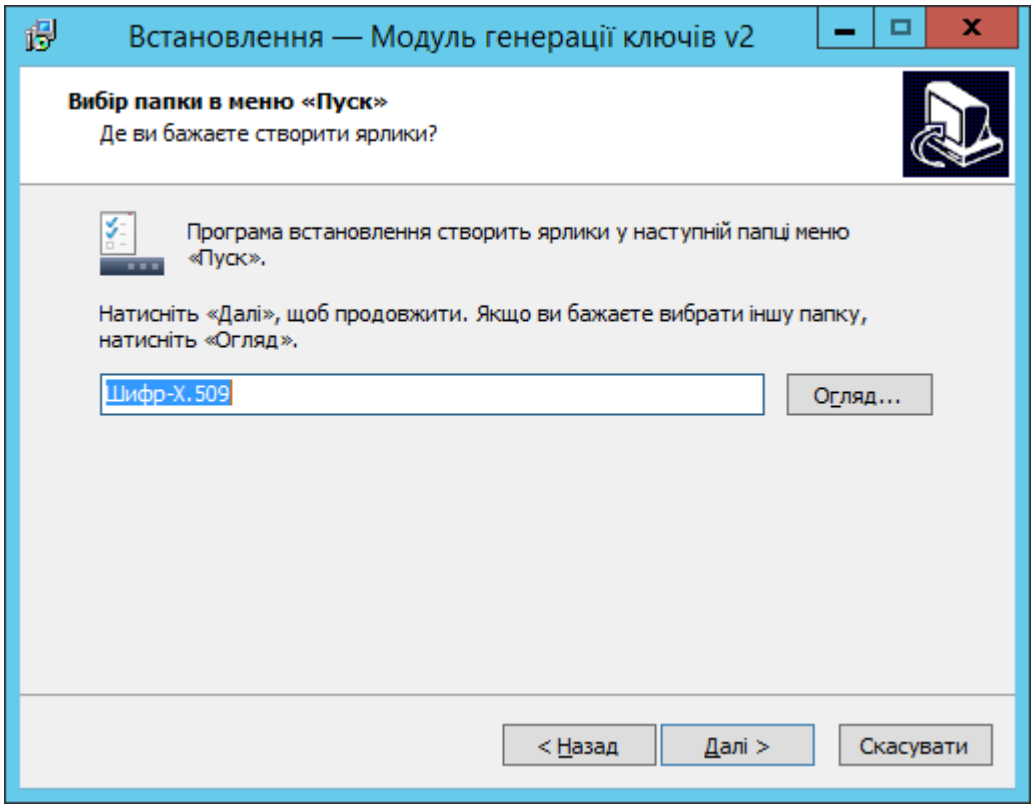

Рис. 5. Діалог вибору папки в меню «Пуск», для встановлення компонент МГК

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

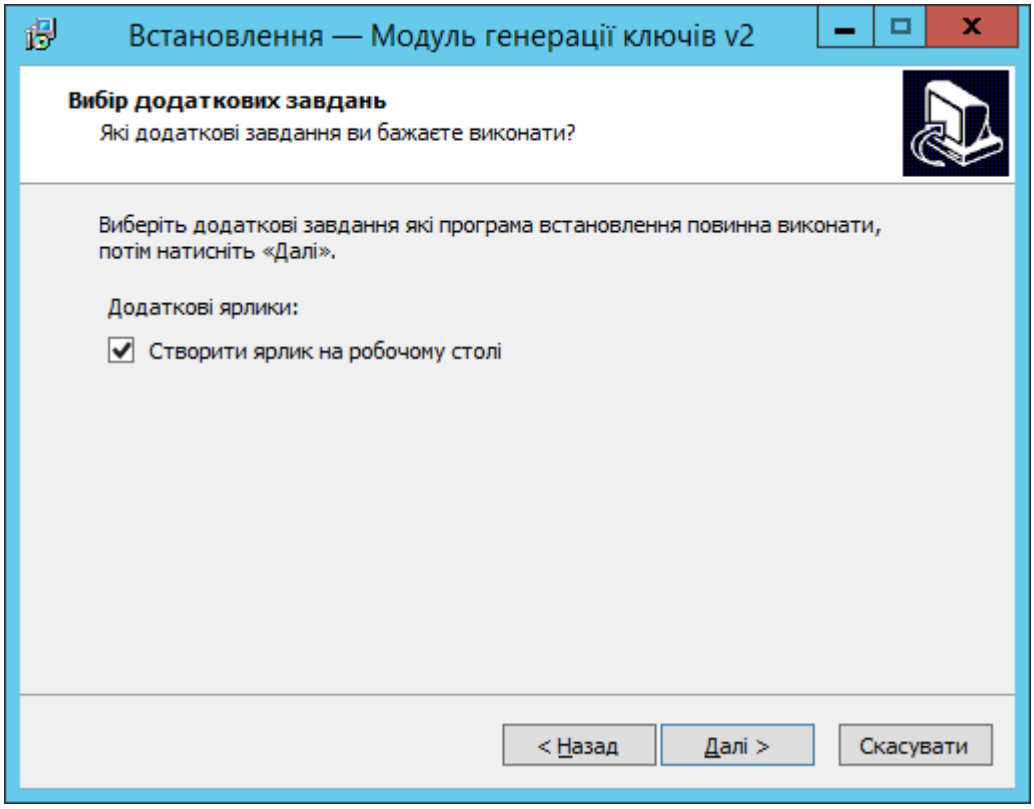

Рис. 6. Діалог вибору додаткових задач

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

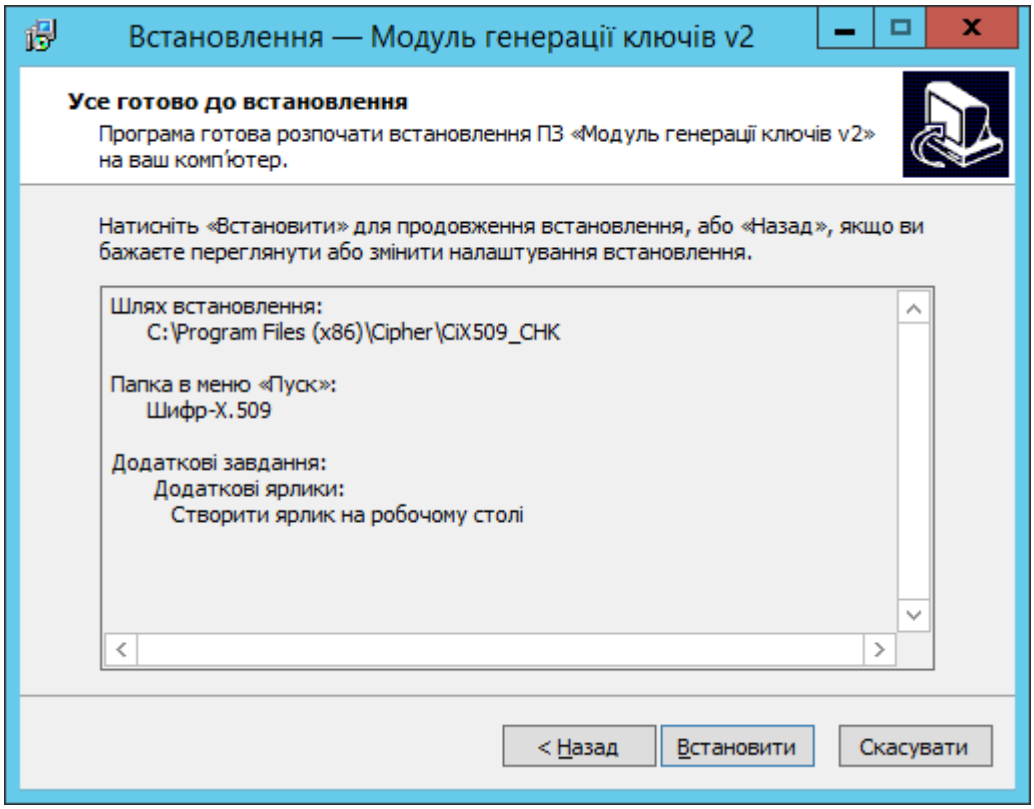

Рис. 7. Діалог перегляду налаштувань встановлення

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

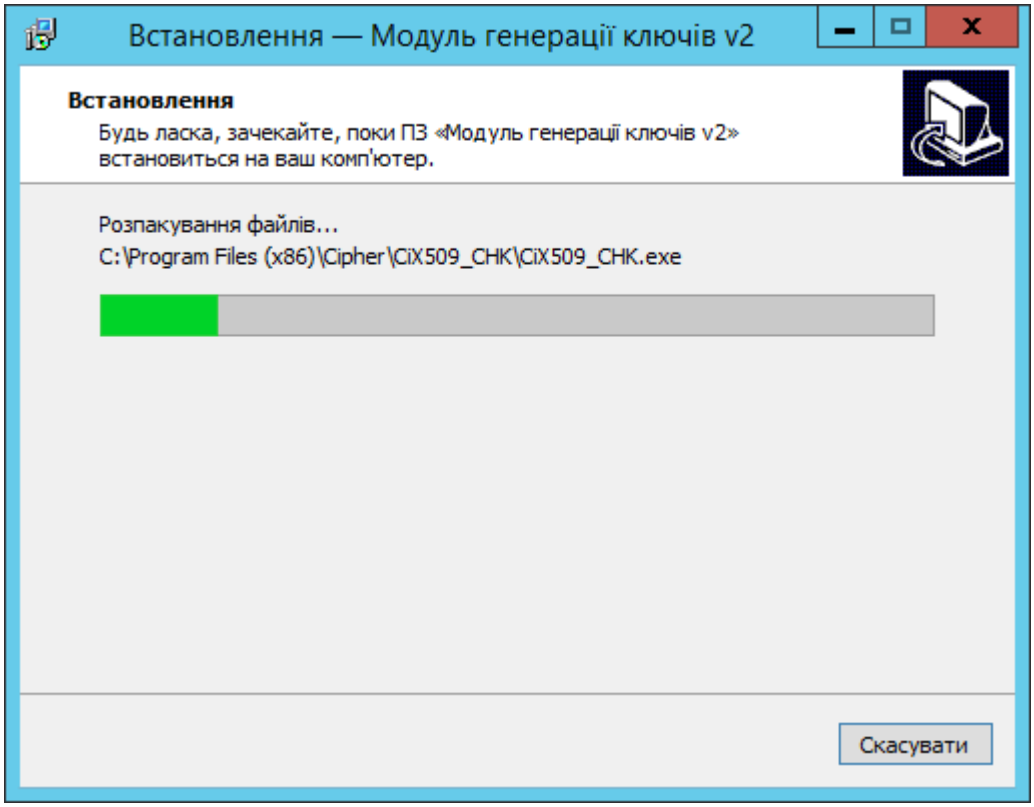

Рис. 8. Діалог відображення процесу встановлення МГК

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

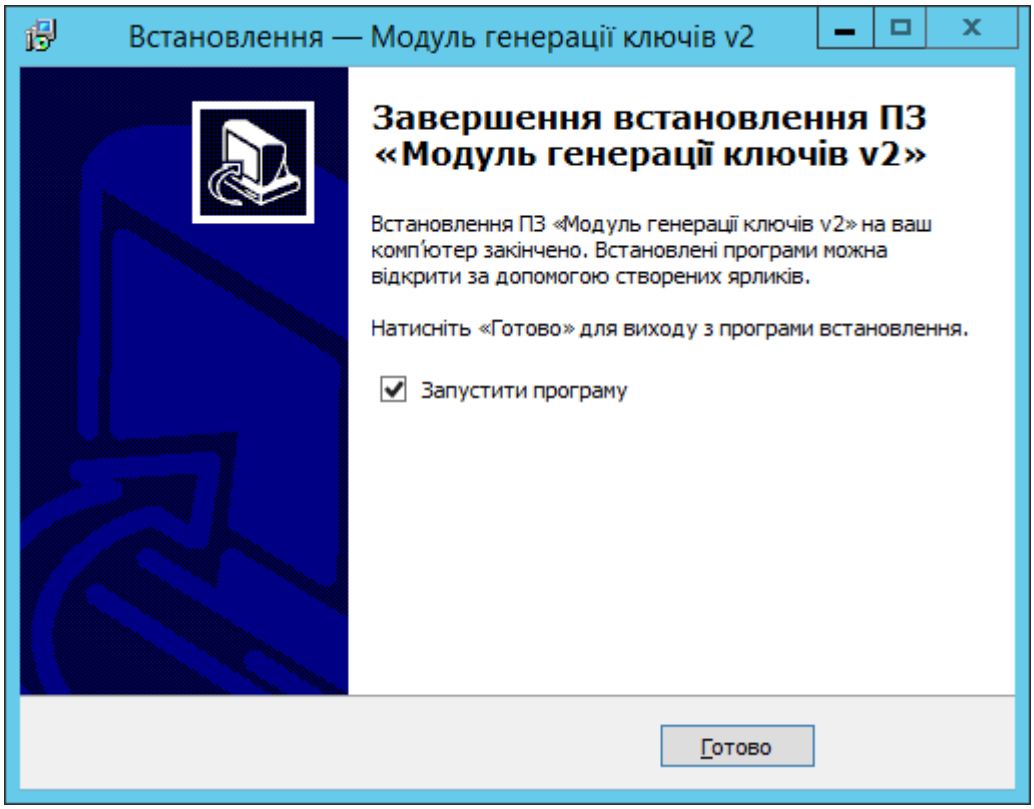

Рис. 9. Діалог завершення установки

Робота з програмою

Введення

МГК призначений для генерації робочих ключів користувачів у плановому режимі на спеціалізованому захищеному від ПЕМВ виконаних з використанням апаратних датчиків випадкових послідовностей чисел. У ключовому контейнері зберігаються стартові ключів, зі строком дії 2 тижні. Протягом 2-тижнів користувачу слід надіслати (передати) запит на сертифікат у ЦР ЦСК та у відповідь, отримати сертифікат та ввести у дію свої ключі.

Передача запиту на сертифікат у ЦР ЦСК здійснюється у ручному режимі, так як користувач передає Оператору реєстрації чи Адміністратору реєстрації носій з файлом-запитом на сертифікат.

Запуск

Запуск Модулю генерації ключів відбувається з меню «Пуск->Шифр-X.509->Модуль генерації ключів», Рис. 10.

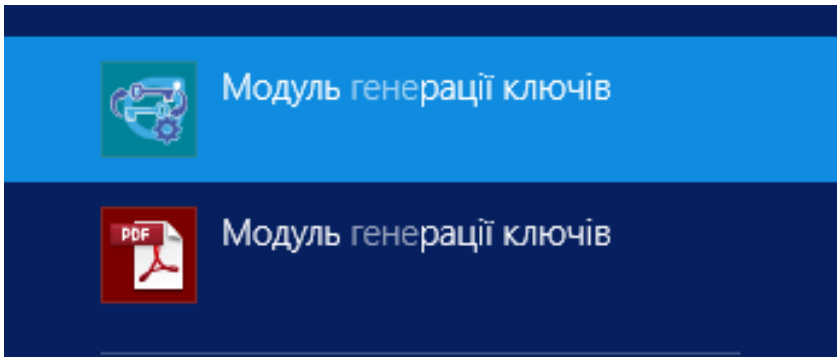

Рис. 10. Запуск Модуля генерації ключів з меню «Пуск»

МГК виконаний у вигляді майстра, кожну необхідну дію користувача передує детальний опис.

Далі з’являється головне вікно програми із пропозицією почати процедуру заміни стартових ключів на робочі (генерація робочої ключової пари).

Перервати роботу майстра можливо на будь-якому кроці, однак зміни завантаженого контейнеру **відмінити неможливо.**

Дії користувача на зміну ключів розбиті на три основних кроки.

Для початку генерації ключів, користувачу слід натиснути кнопку «Почати», після чого він переходить до кроків генерації, згаданих раніше, Рис. 11.

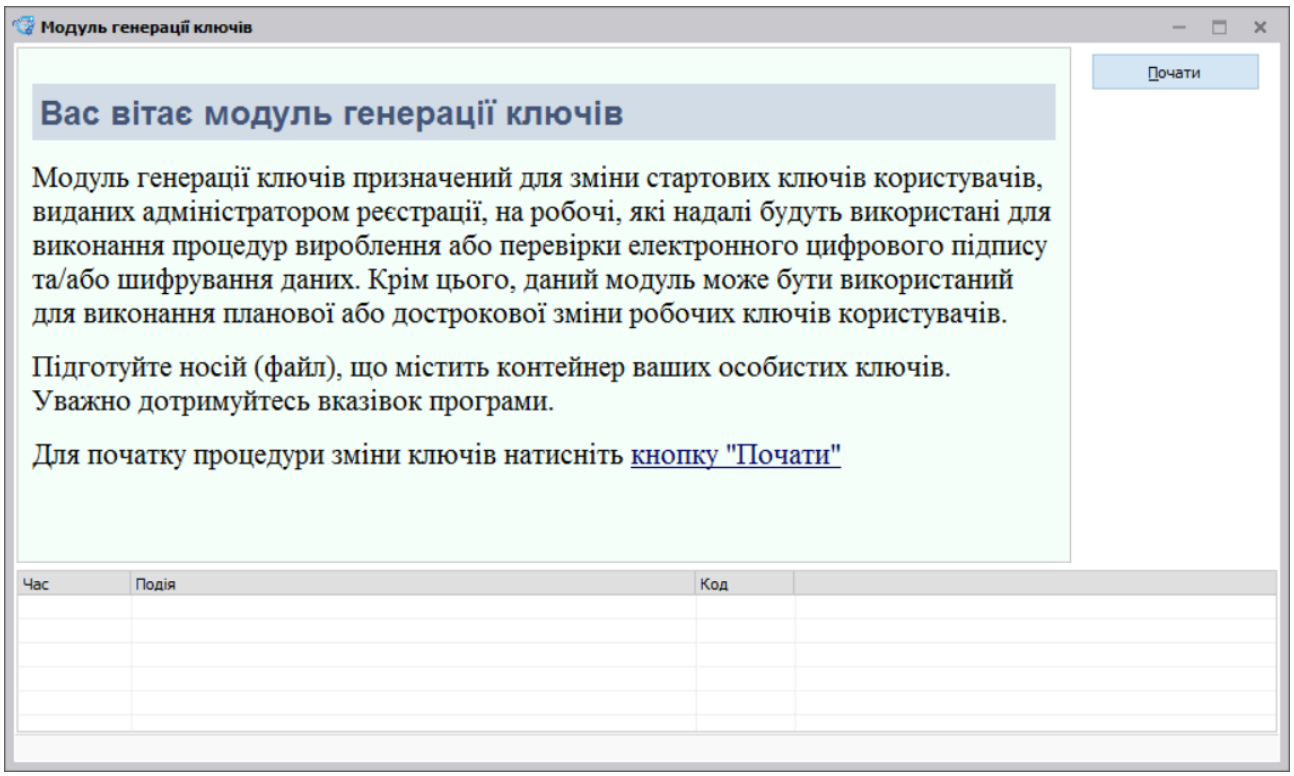

Рис. 11. Головне вікно програми

Крок 1. Завантаження контейнера з особистими ключами

На першому кроці завантаження ключового контейнеру зі стартовими ключами, Рис. 12.

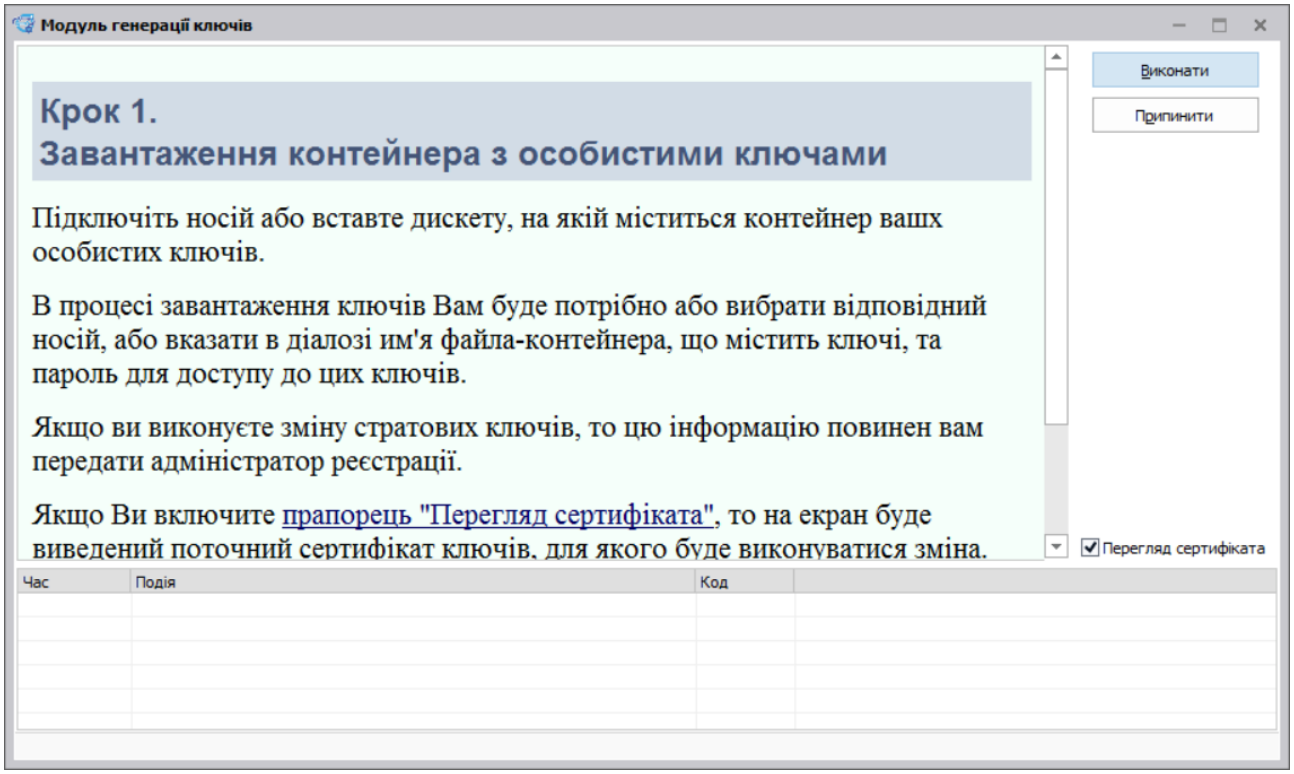

Рис. 12. Діалог «Крок 1» Майстра генерації ключів

Для цього необхідно підключити до комп'ютера ключовий носій і натиснути кнопку «Виконати». Після чого відображається діалог обрання типу ключового носія та контейнеру, Рис. 13.

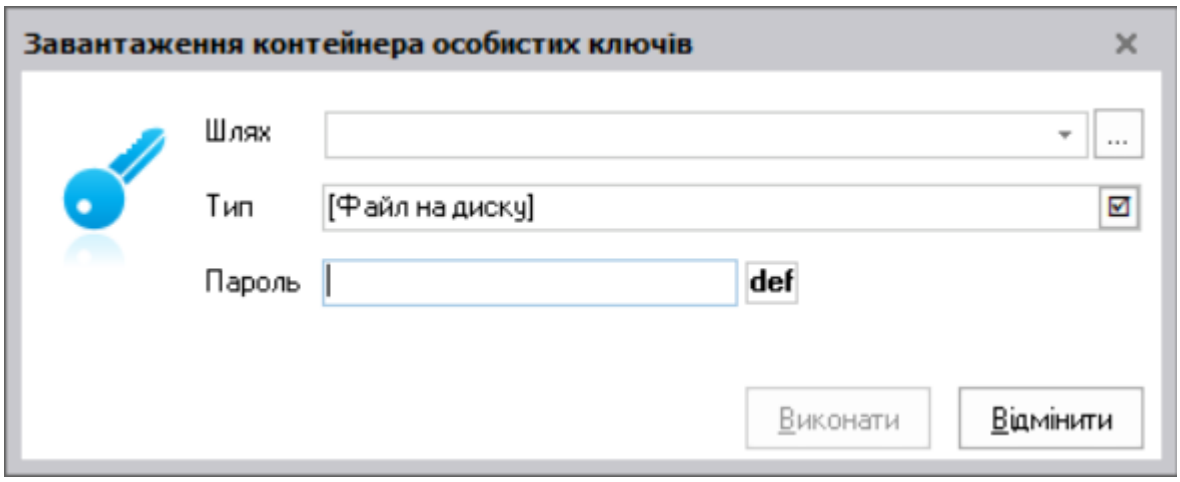

Рис. 13. Діалог обрання ключового носія та введення паролю

Для роботи з носієм, необхідно у поле «Тип» вказати «Файл на диску», для роботи із захищеним носієм, слід вказати «Активні PKCS#11-носії» чи «Пасивні PKCS#11-носії», якщо ключ знаходиться на у хмарі «HSM-токени».

Для файлового контейнеру, необхідно у поле «Шлях» вказати повний шлях, де розміщується файл-контейнеру. Для цього слід натиснути на кнопку «…», яка розміщена поруч, після чого буде відображено діалог вибору файлу, Рис. 14.

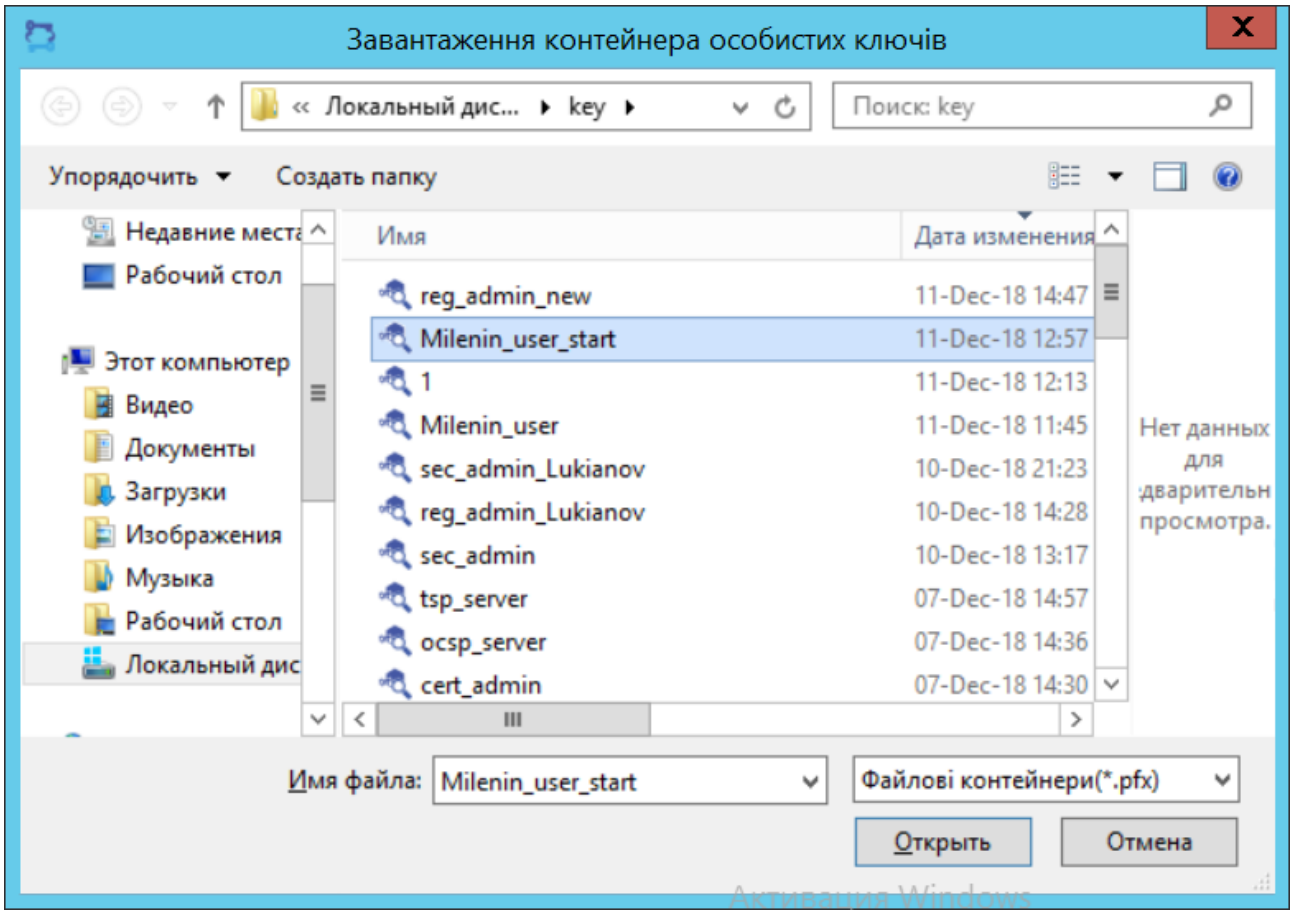

Рис. 14. Діалог вибору файлу-ключового контейнеру

За замовчування, відображаються лише файли з типом ключового контейнеру, з розширенням «*.pfx».

У поле «Пароль» необхідно ввести пароль доступу до ключового контейнеру. Пароль користувачу повідомить Оператор реєстрації чи Адміністратор реєстрації, який генерує

стартові ключів. Слід зауважити, що поруч з полем для введення паролю вводиться у скороченому вигляді поточної розкладки клавіатури.

Якщо у майстра встановлена позначка «Перегляд сертифіката», то у процесі завантаження контейнера, користувачу буде запропоновано переглянути сертифікат стартових ключів, Рис. 15.

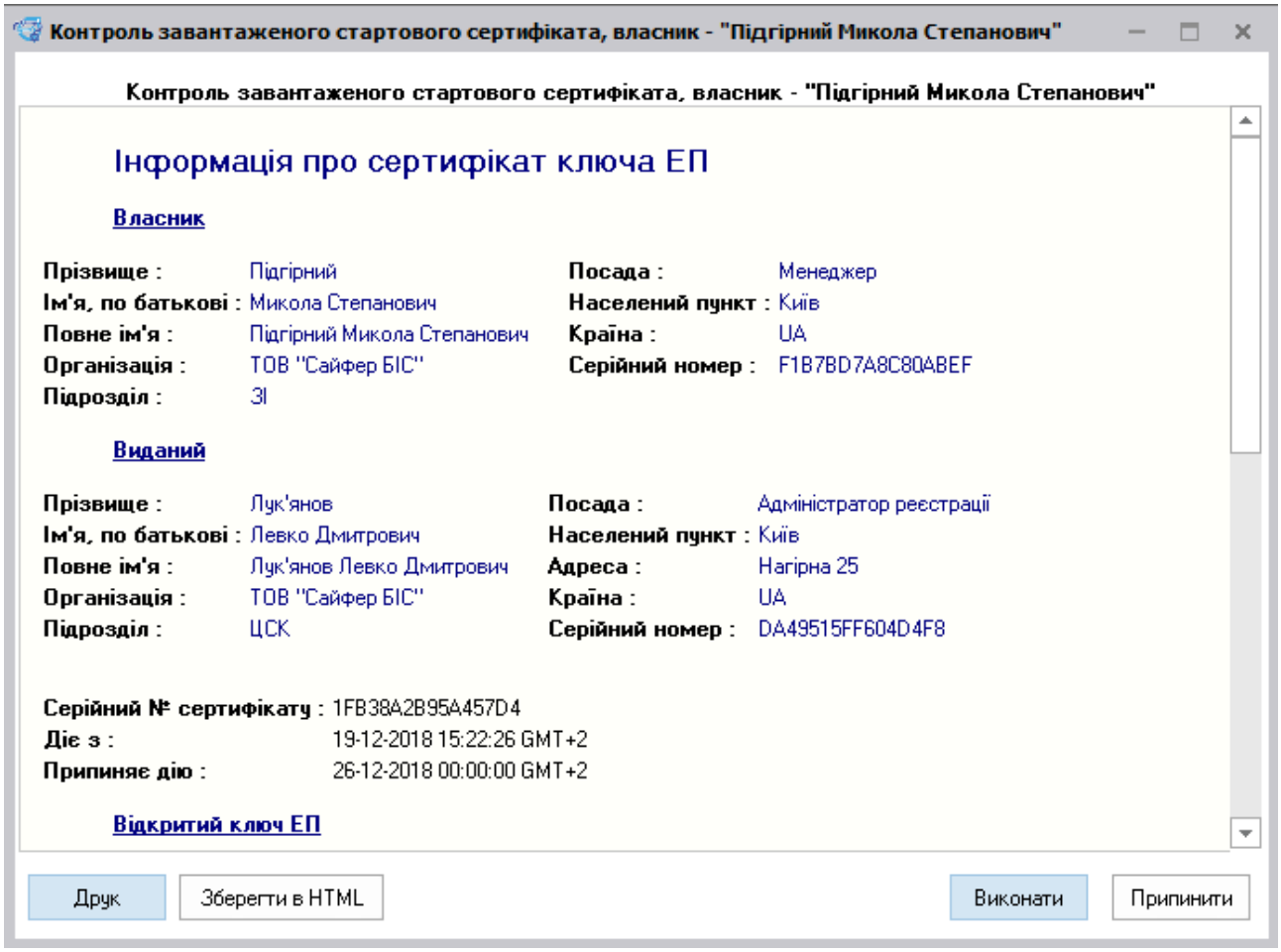

Рис. 15. Діалог з інформацією про стартовий сертифікат відкритого ключа

Слід зауважити, що у процесі завантаження контейнера ключів, МГК проаналізує необхідність виконання замін ключів. Якщо у користувача у ключовому контейнері вже знаходяться робочі ключів, буде показано відповідний діалог та МГК зупинить свою роботу, Рис. 16.

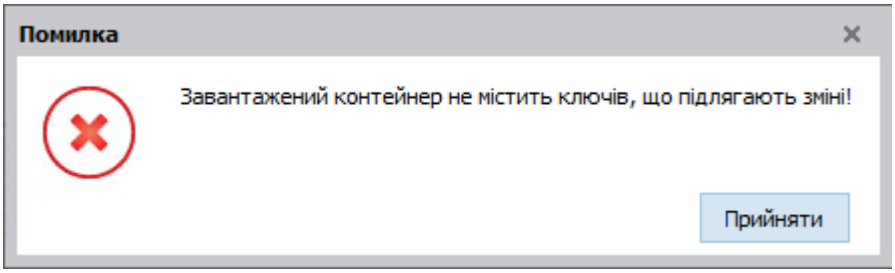

Рис. 16. Діалог з повідомленням про відсутність необхідності заміни ключів

Зауважимо, що у випадку вибору на першому кроці ключового контейнеру, який вже містить робочі ключів та запит на сертифікат відкритого ключа, то Модуль автоматично перейде до третього кроку – реєстрація запиту на сертифікат.

Крок 2. Генерація робочих ключів

На другому кроці відбувається генерація робочих ключів у форматі PKCS#10, які замінять стартові ключів. На початку етапу генерації ключового контейнеру необхідно натиснути кнопку «Виконати», Рис. 17.

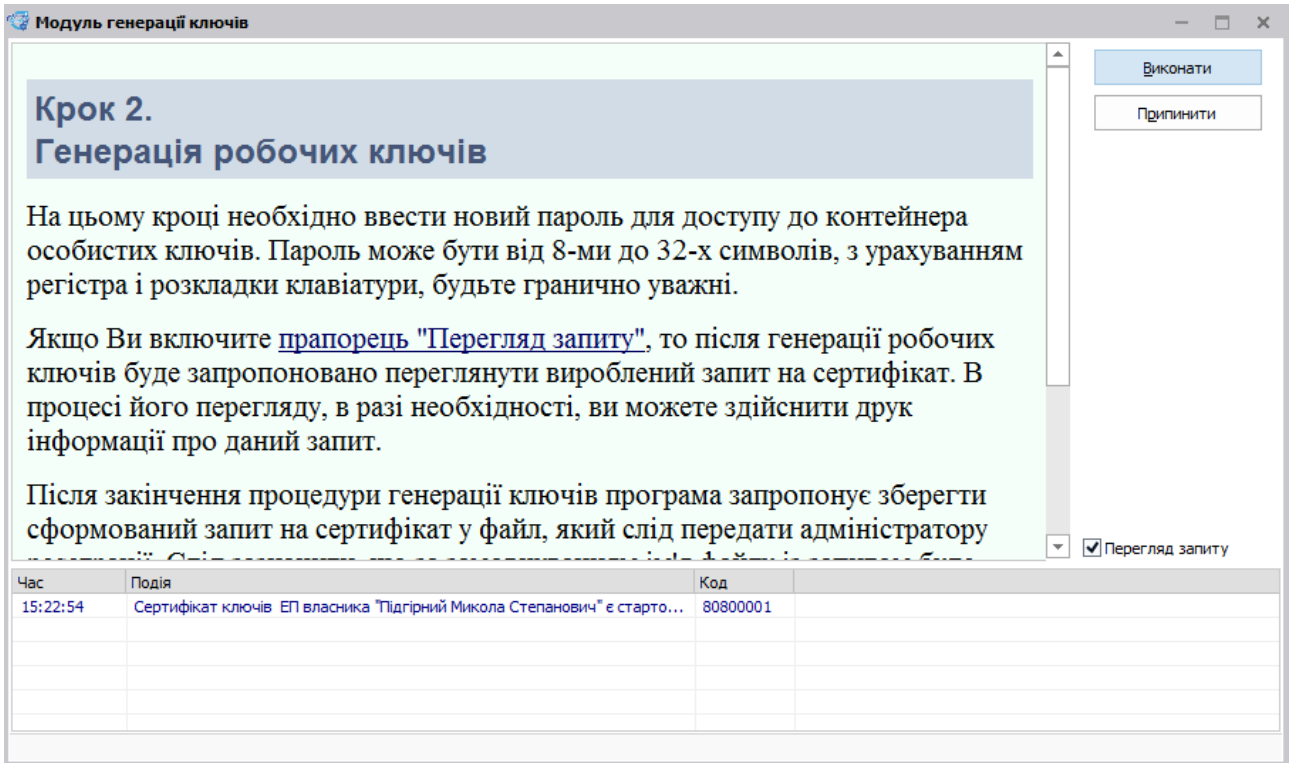

Рис. 17. Діалог «Крок 2» Майстра генерації ключів

На другому етапі відбувається заміна ключового контейнеру на робочий пароль, для цього відображається діалог, Рис. 18.

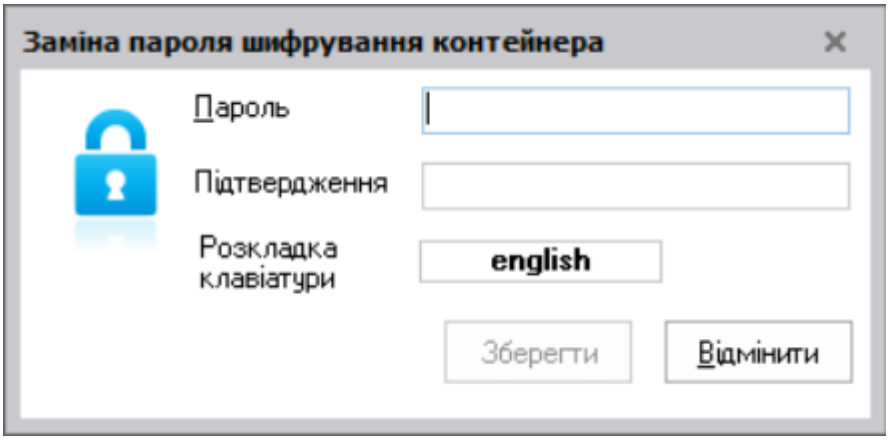

Рис. 18. Діалог введення нового паролю для доступу до ключового контейнеру та його підтвердження

Після чого, якщо раніше була встановлена позначка «Перегляд сертифіката», буде відображений діалог з інформацією про запит на сертифікат, Рис. 19.

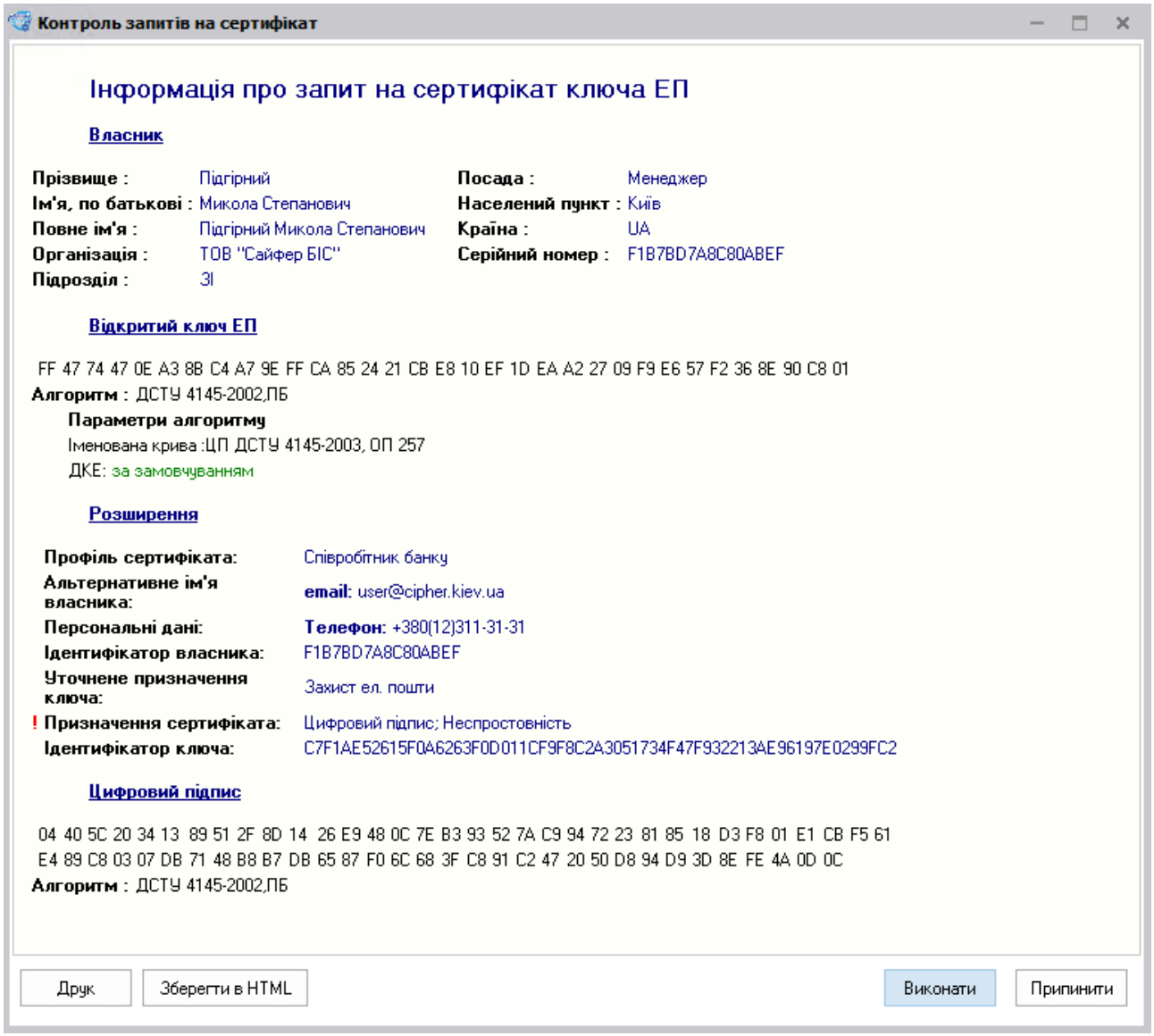

Рис. 19. Діалог перегляду інформації запиту на сертифікат відкритого ключа

Потім, МГК запропонує зберегти запит на заміну сертифіката у файл, Рис. 20. Зауважимо, що запит на сертифікат слід зберегти на файловий носій **відмінний** від того, на якому збережено ключовий контейнер.

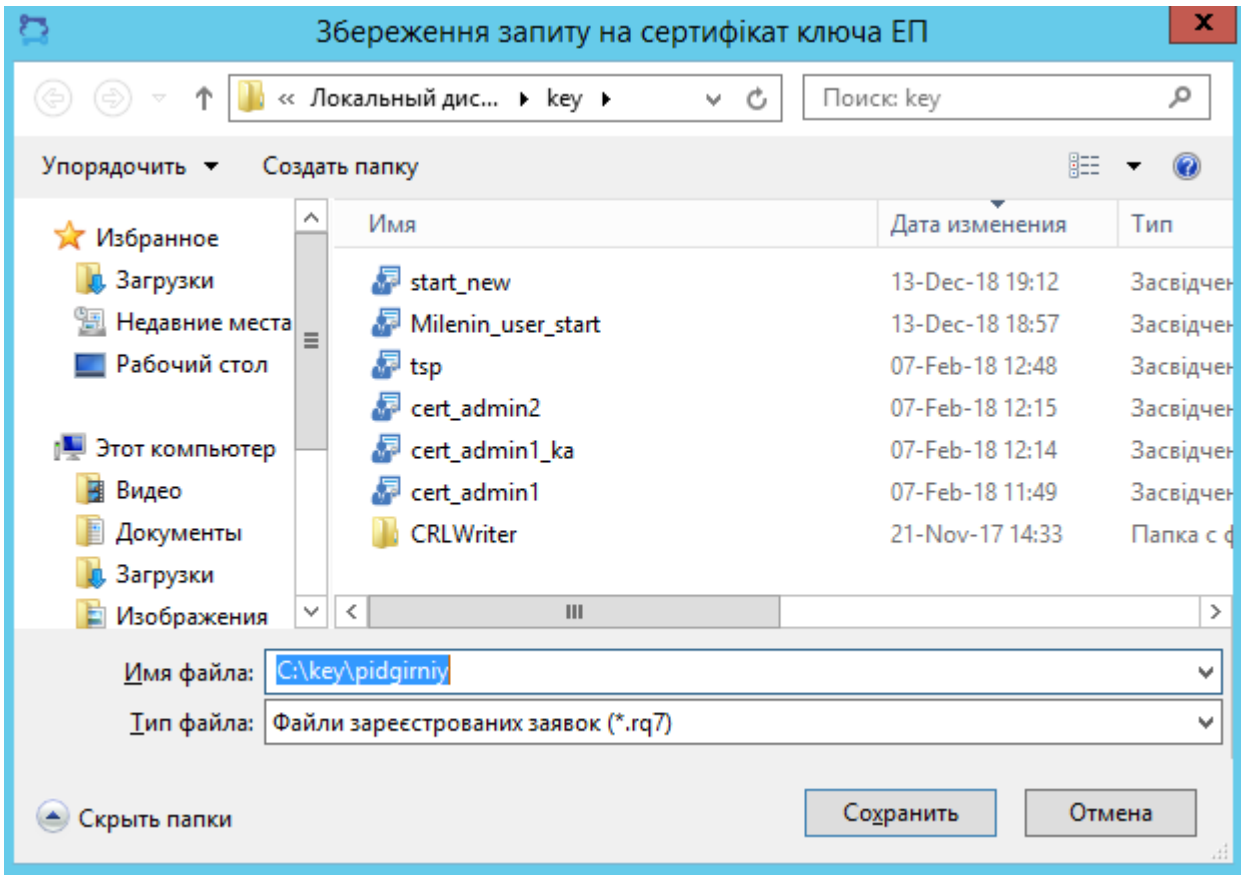

Рис. 20. Діалог вибору файлу для запису запиту на сертифікат у файл

Файловий носій із запитом на сертифікат слід передати Оператору реєстрації чи Адміністратору реєстрації ЦР, для послідовної реєстрації у БД ЦР.

Після передачі запиту на сертифікат, користувач очікує формування робочого сертифіката відкритого ключа. Після видачі сертифіката, користувачу слід ввести у дію робочу ключову пару.

Крок 3. Реєстрація сертифіката робочих ключів

На третьому кроці відбувається реєстрація сертифіката робочих ключів, які були отримані від Адміністратора реєстрації ЦР на файловому носії, Рис. 21.

Після того як, Адміністратор реєстрації отримає від Сервера застосувань ЦСК електронною поштою сформований сертифікат та внесе його у БД ЦР, Адміністратор реєстрації записує робочий сертифікат у вигляді файлу на носій користувача.

Користувач, отримавши файловий носій із файлом-сертифікатом, підключає його до комп'ютера на робочому місці генерації ключів. Та переходить до кроку 3 Майстра генерації ключів.

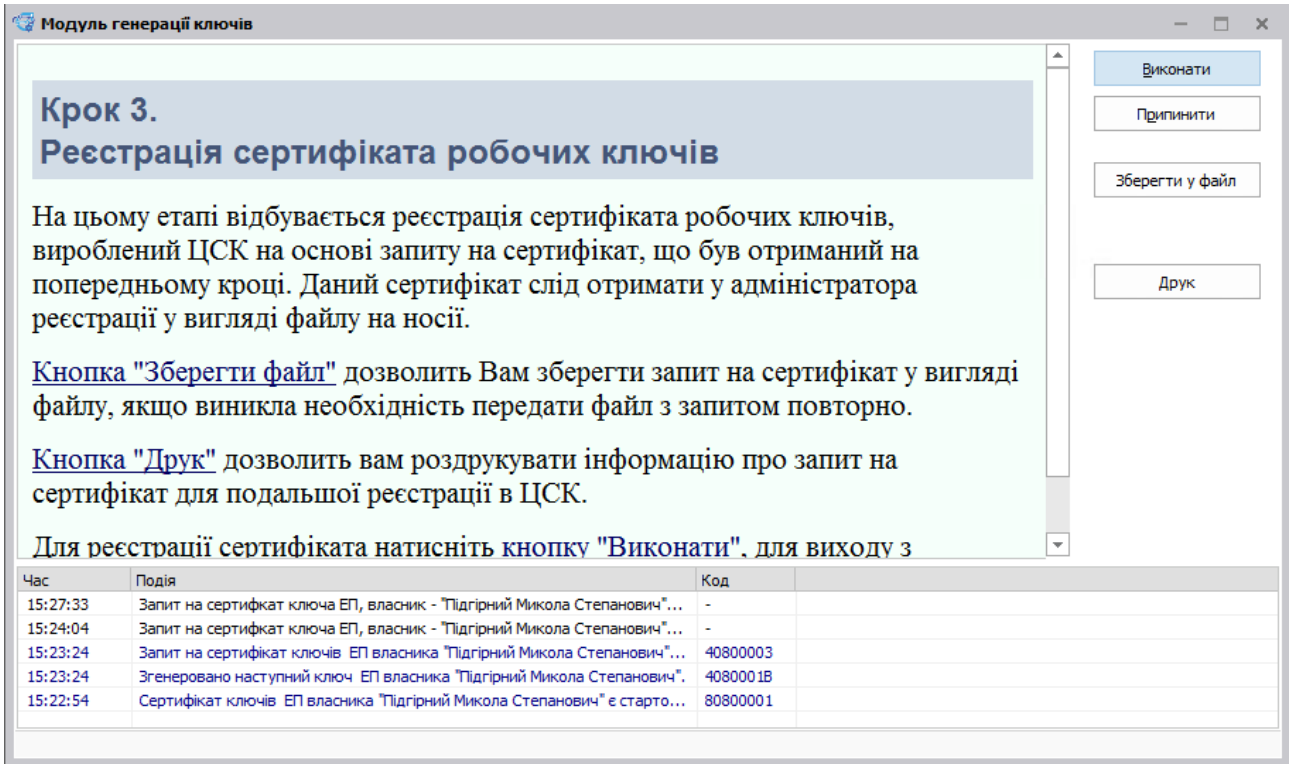

Рис. 21. Діалог «Крок 3» Майстра генерації ключів

Модуль генерації ключів запросить у користувача обрати файл із сертифікатом, Рис. 22.

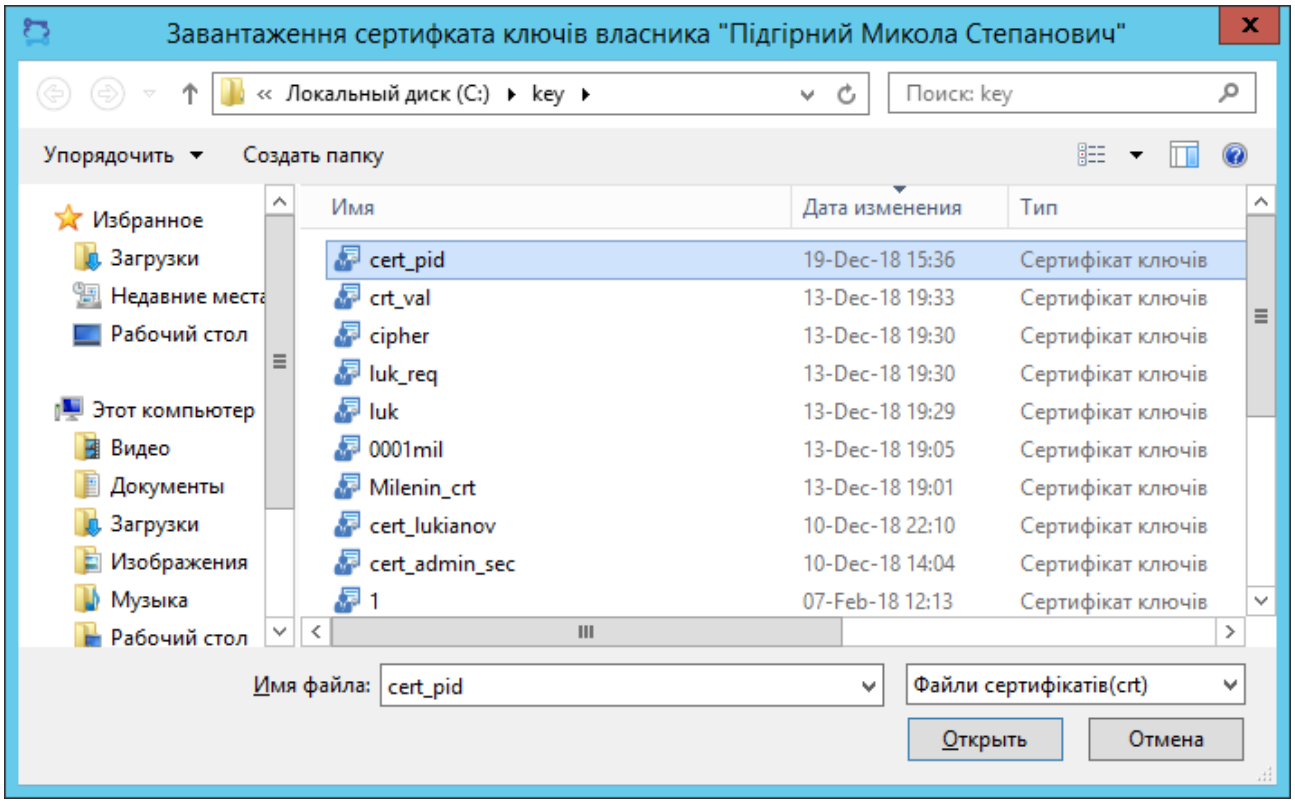

Рис. 22. Діалог обрання файлу із сертифікатом

Якщо сертифікат не відповідає згенерованим ключам, то Модуль видає повідомлення про помилку, Рис. 23.

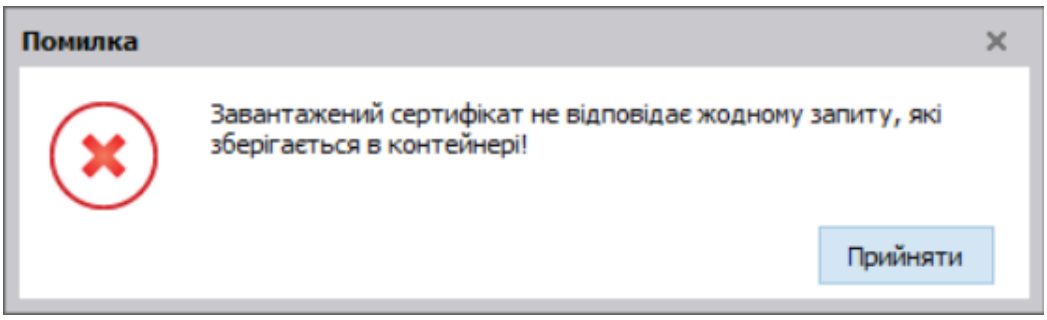

Рис. 23. Діалог з повідомленням про помилку

Якщо у Майстра встановлена позначка «Перегляд сертифікату», користувачу буде показана інформація із завантаженого знову виданого сертифіката, Рис. 24.

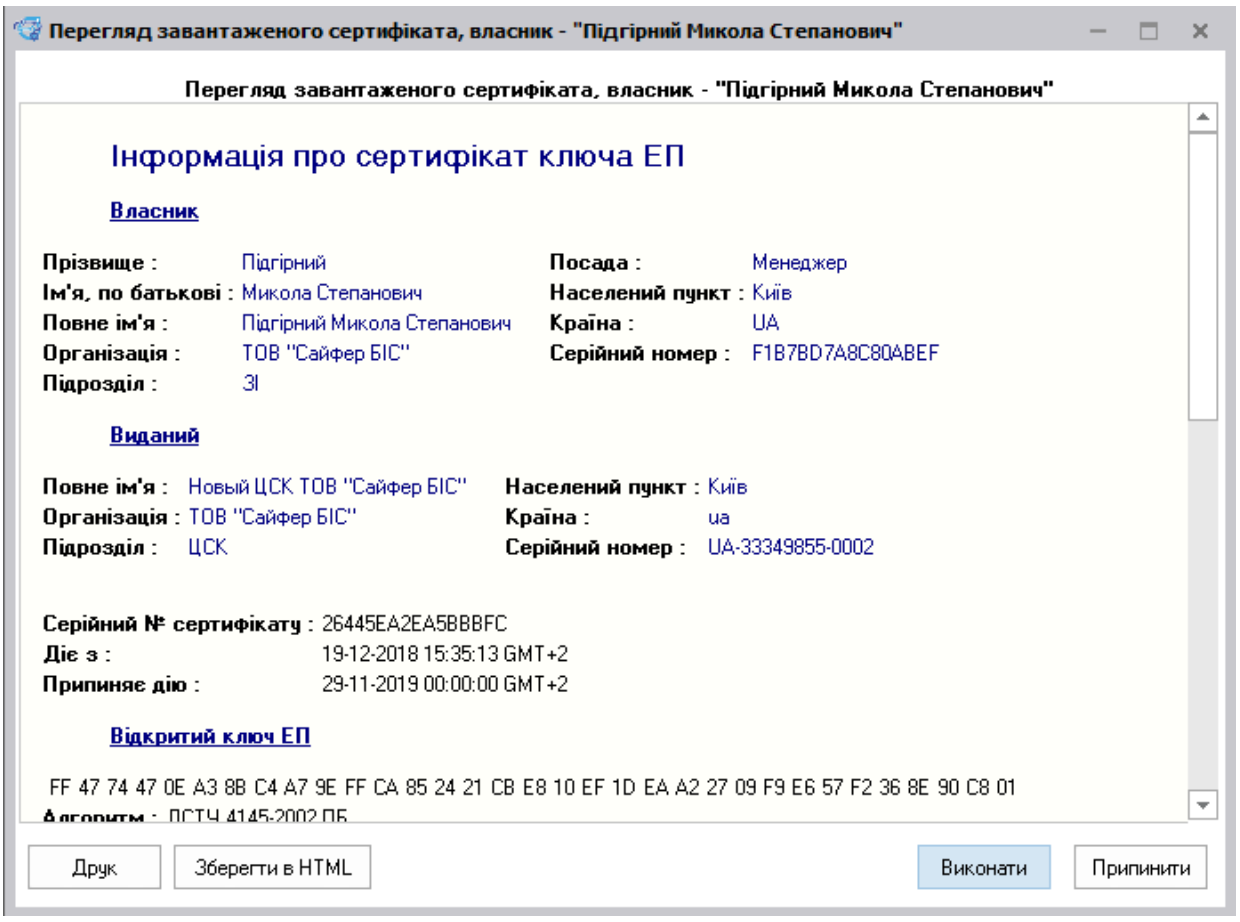

Рис. 24. Діалог з інформацією про робочий сертифікат

Друк

Після натискання на кнопку, відображається діалог налаштування та друку інформації, що міститься у самому сертифікаті, у якому можна обрати принтер, вказати кількість екземплярів та орієнтацію сторінки.

Зберегти в HTML

Після натискання на кнопку відображається діалог обрання файлу, який слід у форматі HTML зберегти інформацію, що міститься у завантаженому сертифікаті.

Припинити

Після натискання на кнопку припиняється процес завантаження сертифіката.

Виконати

Після натискання на кнопку у ключовий контейнер буде записано сертифікат робочих ключів чи видалений запит на сертифікат.

Інформація про завантажений сертифікат можна зберегти у HTML-файлі, для цього необхідно натиснути кнопку «Зберегти в HTML», Рис. 25.

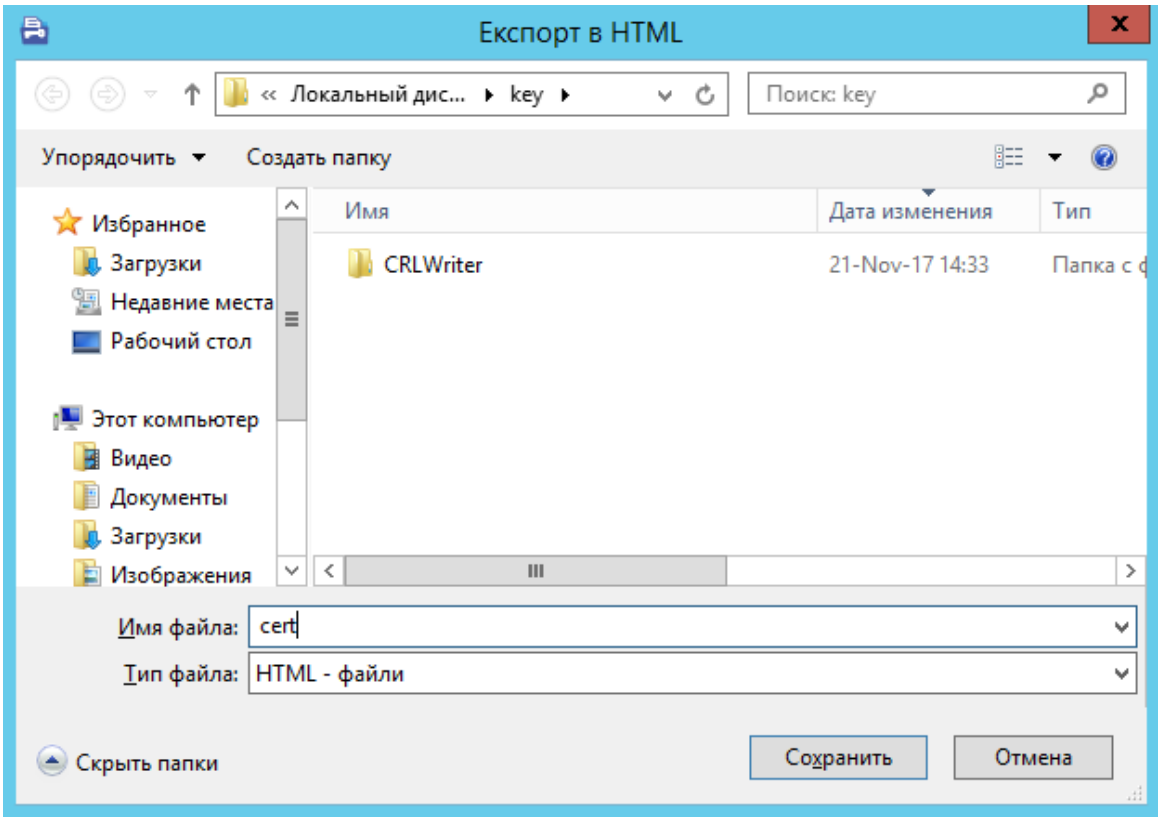

Рис. 25. Діалог збереження інформації про завантажений сертифікат у форматі HTML

Далі, Модуль генерації зберігає робочий сертифікат у ключовий контейнер та видає у дію робочі ключі, про це буде повідомлено у фінальному діалозі Майстра, Рис. 26.

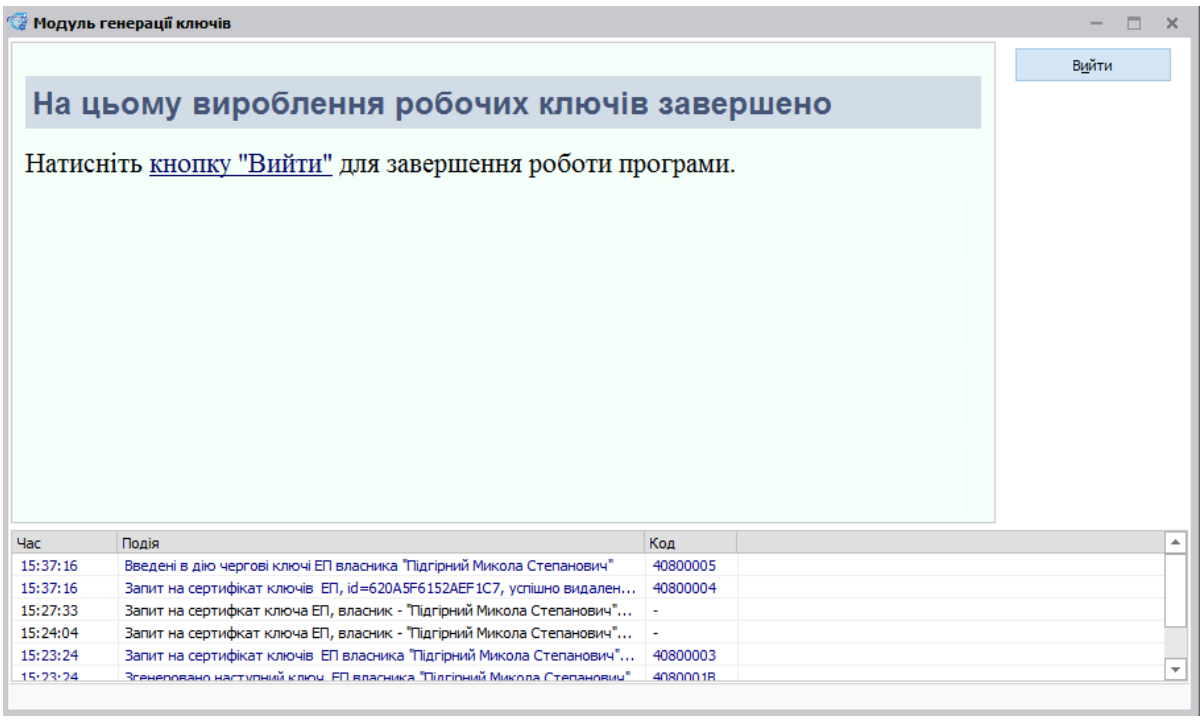

Рис. 26. Діалог з інформацією про успішну генерацію та зміну стартових ключів на робочі, Модуля генерації ключів