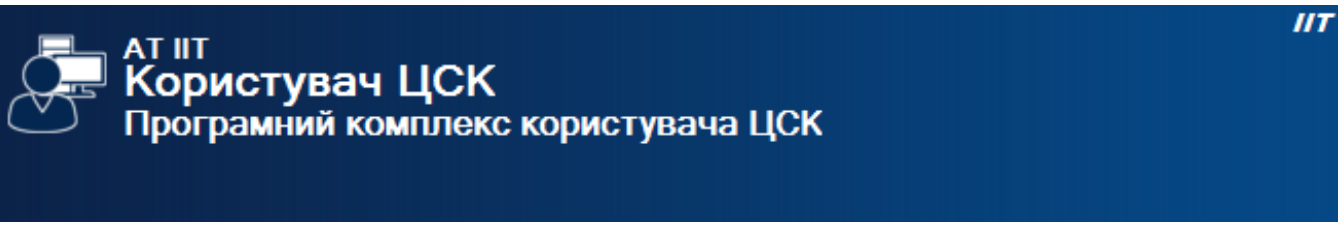
ЗАТВЕРДЖЕНИЙ
ЄААД.00021-13-ЛЗ



Підп. та дата	
Інв. № дубл	
Взам. інв. №	
Підп. та дата	
Інв. № ориг.	

Програмний комплекс користувача ЦСК (ОС Apple MAC OS X)

Версія 1.3.1

Настанова оператора

ЄААД.00021-13 34 30-3

Харків 2015 р.

АНОТАЦІЯ

Даний документ містить настанову оператора для роботи з програмним комплексом користувача центра сертифікації ключів (далі - програма). Настанова містить відомості щодо порядку використання програми.

Пор. № зміни	*Підпис відпов. особи*	*Дата внесення*

ЗМІСТ

Пор. № зміни	*Підпис відпов. особи*	*Дата внесення*

1 ПРИЗНАЧЕННЯ ПРОГРАМИ

Програма призначена для застосування на засобах ЕОТ користувача центра сертифікації ключів і виконує наступні функції:

- управління ключами користувача:
  - генерацію ключів користувача ЦСК, запис особистого ключа на НКІ та формування запита на формування сертифіката;
  - перевірку сформованого сертифіката користувача на відповідність запиту;
  - резервне копіювання особистого ключа з одного НКІ на інший;
  - зміну паролю захисту особистого ключа;
  - знищення особистого ключа на НКІ;
  - формування та передачу у ЦСК запита на блокування сертифіката користувача;
  - формування та передачу запита на формування нового сертифіката;
- доступ до сертифікатів ЦСК, серверів ЦСК, сертифікатів інших користувачів та СВС:
  - перегляд сертифікатів та СВС з файлового сховища;
  - пошук сертифікатів у файловому сховищі, LDAP-каталозі та за допомогою протоколу OCSP;
  - визначення статусу сертифікатів за допомогою СВС та за протоколом OCSP;
  - перевірку чинності та цілісності сертифікатів та ін.;
- захист файлів користувача:
  - підпис файлів;
  - перевірку файлів;
  - зашифрування файлів;
  - розшифрування файлів.

2 УМОВИ ВИКОНАННЯ ПРОГРАМИ

Програма може бути завантажена та виконана на ЕОМ під керуванням ОС Apple MAC OS X.

Примітка. Відомості щодо послідовності та особливостей інсталяції програми, а також встановлення параметрів роботи наведені в настанові системного програміста (ЄААД.00021-13 32 30-3).

3 УПРАВЛІННЯ СЕРТИФІКАТАМИ ТА СВС

3.1 Перегляд сертифікатів

Для перегляду сертифікатів що містяться у файловому сховищі необхідно обрати підпункт “Переглянути сертифікати...” в пункті меню “Сертифікати та СВС”. Вікно із сертифікатами наведене на рис. 3.1.

За допомогою даного вікна можна видаляти сертифікати з файлового сховища, перевіряти та переглядати сертифікати.

Сертифікати у вікні відсортовані за типами власників (тип власника обирається у верхній частині вікна у випадаючому списку):

- всі сертифікати;
- сертифікати центрів сертифікації ключів;
- сертифікати серверів ЦСК;
- сертифікати CMP-серверів;
- сертифікати TSP-серверів
- сертифікати OCSP-серверів
- сертифікати користувачів.

Для перегляду списку сертифікатів власника певного типу необхідно обрати відповідний тип власника у верхній частині вікна у списку що випадає.

Для перегляду сертифіката необхідно натиснути на відповідному записі про сертифікат у списку. Сертифікат буде відображено у вікні що наведене на рисунках 3.2 та 3.3.

Для видалення сертифікатів з файлового сховища необхідно виділити у списку відповідні записи про сертифікати та натиснути кнопку “Видалити”.

Для перевірки сертифіката необхідно виділити відповідний запис про сертифікат у списку та натиснути кнопку “Перевірити”. Перевірка сертифіката здійснюється відповідно до встановлених параметрів роботи - за допомогою СВС, OCSP-протоколу тощо. Результатом перевірки буде вікно що наведене на рис. 3.4. Якщо у цьому вікні натиснути “Сертифікат”, сертифікат буде відображений у вікні детального перегляду (рис. 3.2).

Для імпорту сертифіката до файлового сховища необхідно натиснути “Імпортувати”, та обрати потрібний сертифікат на будь-якому носії інформації.

Для експорту сертифіката з файлового сховища в інше місце (носій інформації тощо), необхідно натиснути “Експортувати”, та обрати інше місце розташування.

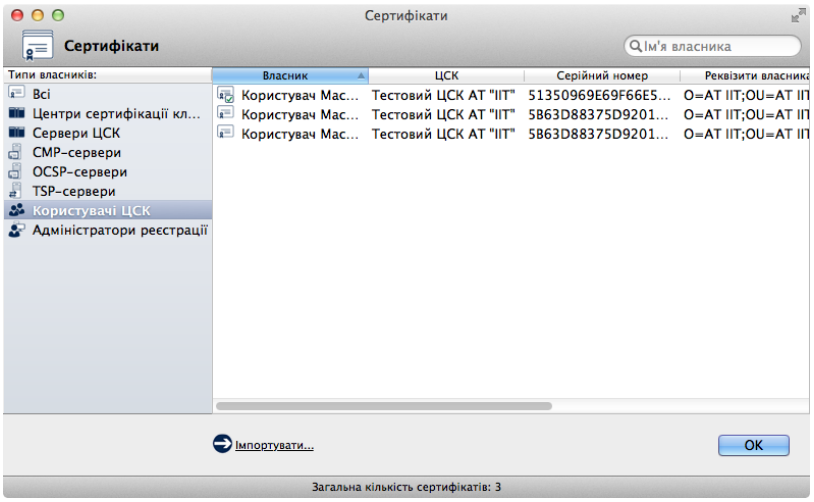


Рисунок 3.1

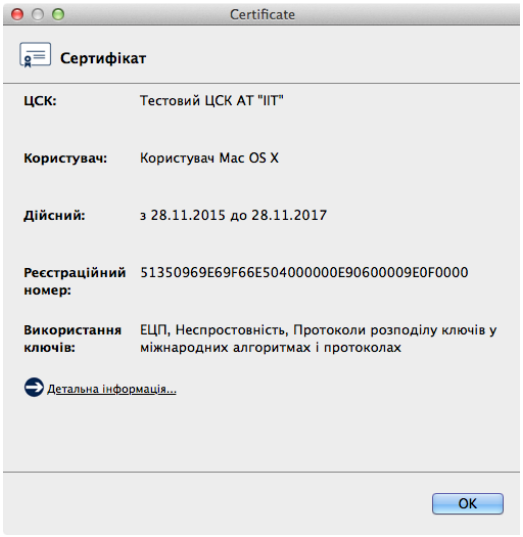


Рисунок 3.2

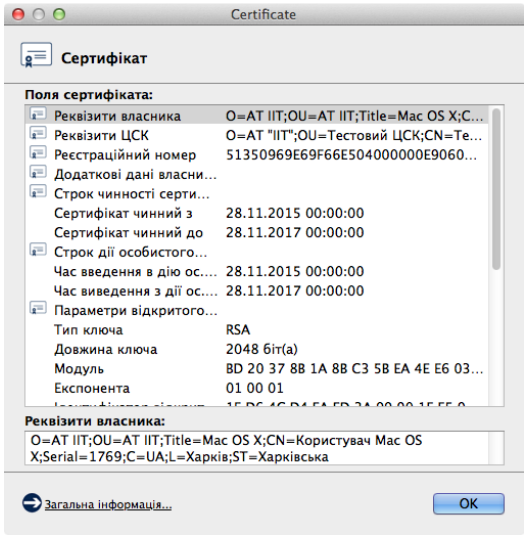


Рисунок 3.3

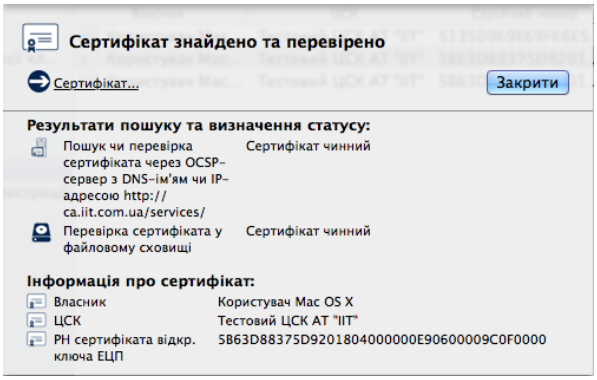


Рисунок 3.4

3.2 Перегляд СВС

Для перегляду списків відкликаних сертифікатів (СВС) необхідно натиснути підпункт “Переглянути СВС...” в пункті меню “Сертифікати та СВС”. Вікно із списками відкликаних сертифікатів наведене на рис. 3.5.

Вікно перегляду СВС дозволяє видаляти СВС з файлового сховища, переглядати СВС та завантажувати СВС з web-сервера ЦСК.

Пор. № зміни	*Підпис відпов. особи*	*Дата внесення*

Для перегляду СВС необхідно натиснути на відповідному записі про СВС у списку. СВС буде відображено у вікні що наведене на рисунках 3.6 та 3.7.

Для видалення файлу СВС з файлового сховища необхідно виділити відповідний запис про СВС у списку та натиснути кнопку “Видалити”.

Для імпорту СВС до файлового сховища необхідно натиснути “Імпортувати”, та обрати потрібний СВС на будь-якому носії інформації.

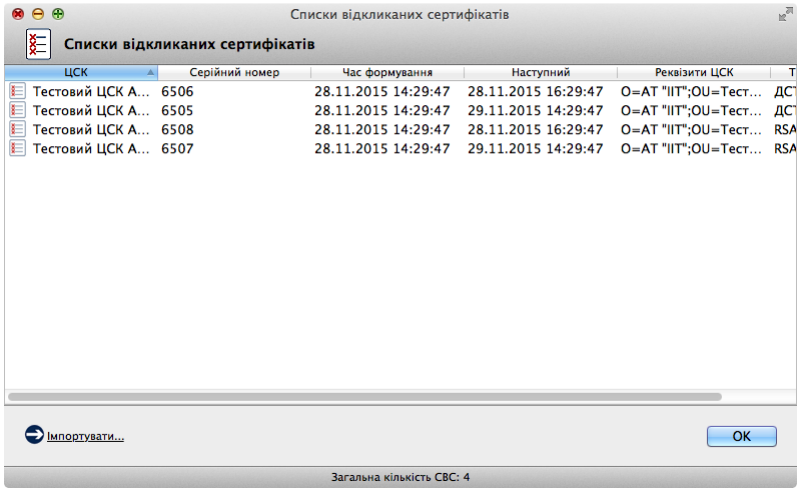


Рисунок 3.5

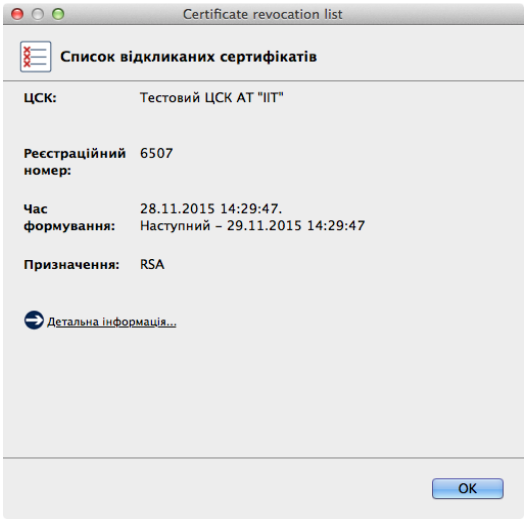


Рисунок 3.6

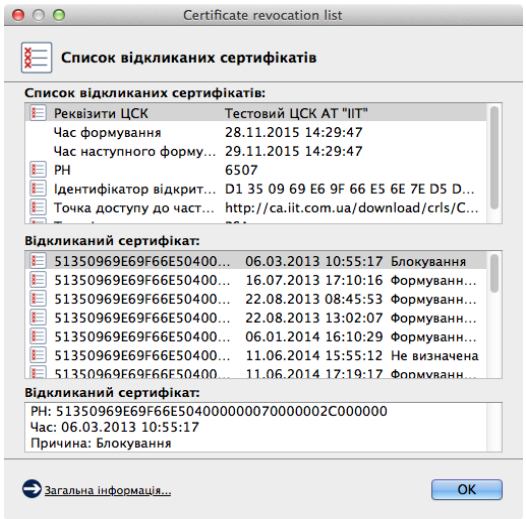


Рисунок 3.7

Пор. № зміни	*Підпис відпов. особи*	*Дата внесення*

4 УПРАВЛІННЯ КЛЮЧАМИ

4.1 Зчитування особистого ключа

Для роботи з більшістю функцій програми (захисту файлів та ін.) необхідне попереднє зчитування особистого ключа користувача. Ініціювання зчитування особистого ключа може бути виконане автоматично при виборі певної функції програми чи виконане шляхом вибору підпункту “Зчитати ...” в пункті меню “Особистий ключ”.

У вікні, що з’явиться (рис. 4.1) необхідно вказати:

- тип НКІ з особистим ключем;
- назву носія;
- пароль доступу до носія та захисту особистого ключа.

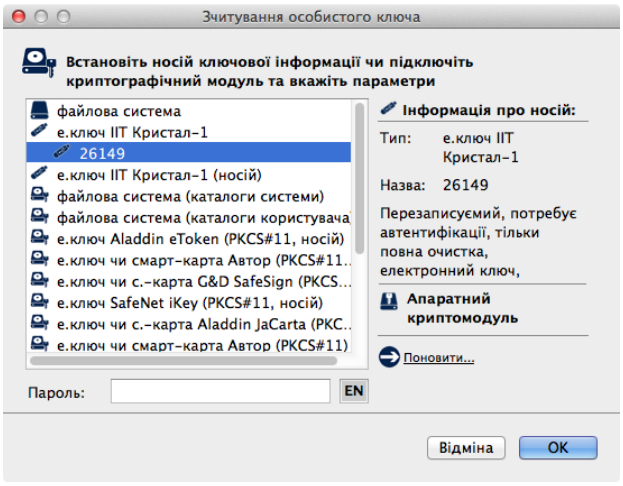


Рисунок 4.1

Після введення параметрів необхідно натиснути кнопку “OK”.

Інформація про те, що особистий ключ зчитаний та знаходиться в пам’яті ПЕОМ відображається до панелі стану вікна, як наведено на рисунку 4.2.

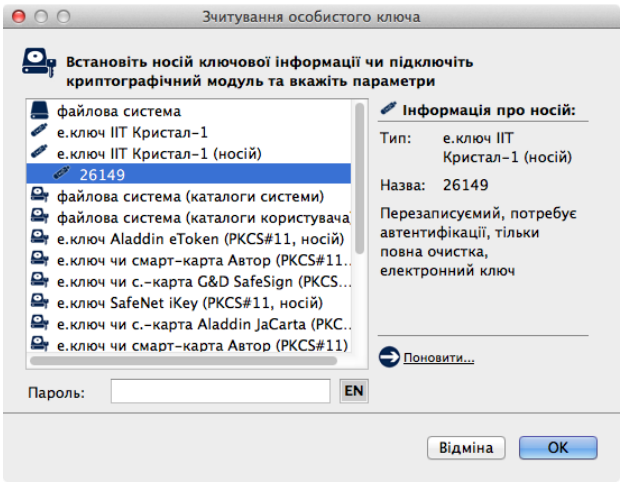


Рисунок 4.2

4.2 Резервне копіювання особистого ключа

Для резервного копіювання особистого ключа з одного НКІ на інший необхідно обрати підпункт “Резервне копіювання особистого ключа” в пункті меню “Особистий ключ”.

Під час резервного копіювання особистий ключ зчитується за допомогою вікна що наведене на рисунку 4.3. Під час резервного копіювання пароль захисту особистого ключа не вказується, та змінити його не можливо.

Пор. № зміни	*Підпис відпов. особи*	*Дата внесення*

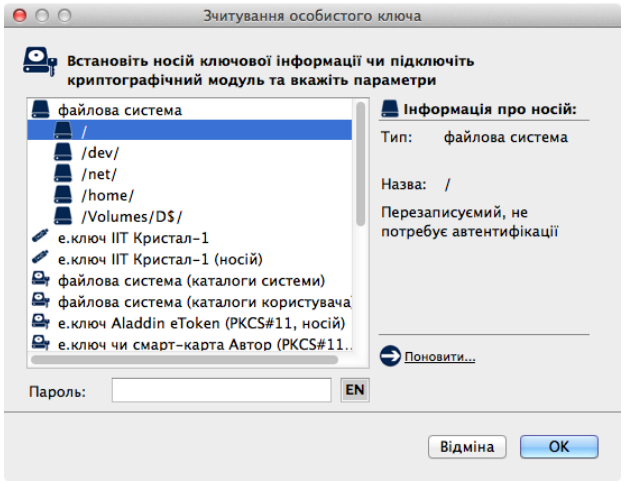


Рисунок 4.3

Після зчитування особистий ключ записується до резервного носія за допомогою вікна що наведене на рисунку 4.4.

Примітка. Якщо в якості засобу зберігання особистого ключа використовується електронний ключ “Кристал-1” в апаратному режимі роботи, резервна копія ключа не створюється, оскільки такі засоби не передбачають функції резервного копіювання ключів. Резервну копію особистого ключа можливо створити, якщо особистого ключа зберігається у електронному ключу “Кристал-1” в режимі роботи носій. При цьому під час запису особистого ключа вказується пароль, що був використаний під час зчитування особистого ключа.

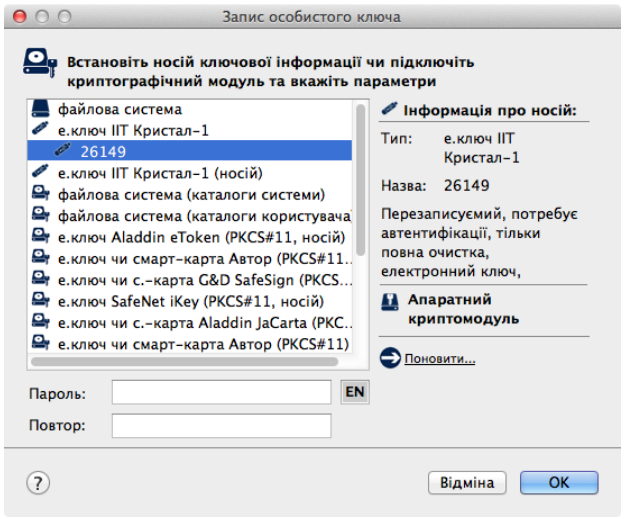


Рисунок 4.4

4.3 Зміна паролю захисту особистого ключа

Для зміни паролю захисту особистого ключа необхідно обрати підпункт “Змінити пароль захисту особистого ключа” в пункті меню “Особистий ключ”. Вікно зміни паролю захисту особистого ключа наведене на рис. 4.5. У вікні необхідно вказати:

- тип НКІ;
- назву носія;
- пароль доступу до носія та захисту особистого ключа;
- новий пароль захисту особистого ключа (з підтвердженням).

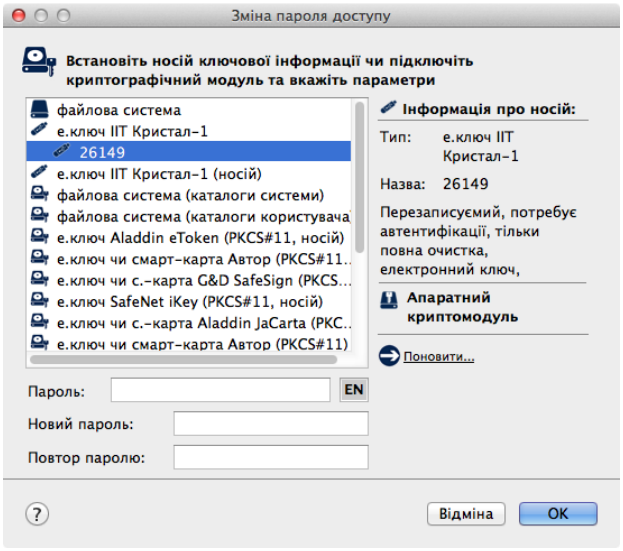


Рисунок 4.5

4.4 Знищення особистого ключа на носієві

Особистий ключ на НКІ повинен знищуватись спеціальними засобами, які вбудовані у програму, що забезпечують його гарантоване знищення.

Для знищення особистого ключа необхідно обрати підпункт “Знищити особистий ключ на носієві ключової інформації” в пункті меню “Особистий ключ”. Вікно знищення особистого ключа наведене на рис. 4.6. У вікні необхідно вказати тип та назву НКІ і натиснути кнопку “Виконати”.

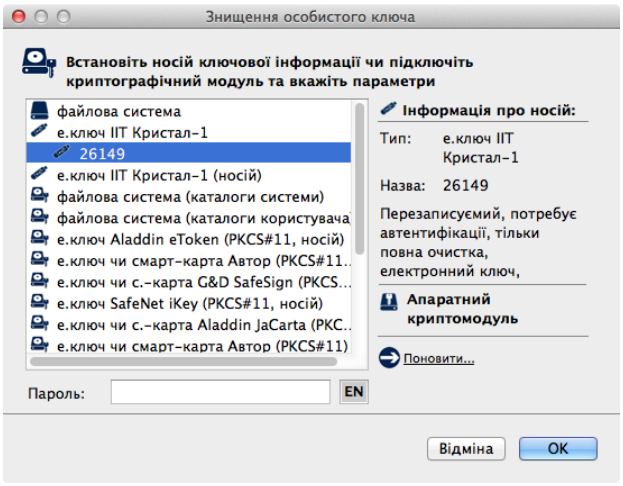


Рисунок 4.6

4.5 Знищення особистого ключа в пам’яті

Якщо необхідно знищити ключ з пам’яті не виходячи з програми необхідно обрати підпункт “Знищити особистий ключ у пам’яті” в пункті меню “Особистий ключ”.

4.6 Перегляд власного сертифіката

Після зчитування особистого ключа користувач може переглянути власний сертифікат. Для перегляду власного сертифіката необхідно обрати підпункт “Переглянути власний сертифікат” в пункті меню “Особистий ключ”. Сертифікат буде відображено до вікон що наведені на рисунках 3.2, 3.3.

Пор. № зміни	*Підпис відпов. особи*	*Дата внесення*

5 ЗАХИСТ ФАЙЛІВ

5.1 Підпис файлів

Для підпису файлів (накладання ЕЦП) необхідно натиснути на панелі “Підписати файли” у головному вікні програми, або обрати підпункт “Підписати” у пункті меню “Файли. Якщо особистий ключ ще не було зчитано, відбувається його зчитування відповідно до п. 4.1.

Вікно підпису файлів наведене на рис. 5.1. Вікно містить наступні параметри:

- список файлів, які необхідно підписати;
- признак запису ЕЦП у зовнішній файл;
- признак запису підписаних файлів чи файлів з ЕЦП у окремий каталог;
- ім’я каталогу для запису підписаних даних чи файлів з ЕЦП.

Список файлів містить імена файлів що необхідно підписати. Файли додаються до списку за допомогою кнопки “Додати” та стандартного діалогового вікна вибору файлів ОС. Для видалення файлів зі списку необхідно виділити відповідні файли у списку та натиснути кнопку “Видалити”.

Признак запису ЕЦП у зовнішньому файлі встановлює необхідність запису ЕЦП у окремий файл з розширенням “.p7s” без включення вмісту файлу що підписується. За замовчанням підпис записується до вихідного файлу та до розширення файлу додається суфікс “.p7s”. Запис ЕЦП до зовнішнього файлу потрібен у випадку, коли файл підписується декількома користувачами, або при необхідності доступу до структури (вмісту) файлу без зняття з нього ЕЦП.

Признак запису підписаних файлів у окремий каталог встановлює необхідність запису підписаних файлів або файлів з ЕЦП до окремого каталогу що задається параметром “Каталог для запису підписаних даних чи файлів з ЕЦП ”. Якщо признак не встановлено підписані файли чи файли з ЕЦП будуть записуватися у каталог з вихідними файлами.

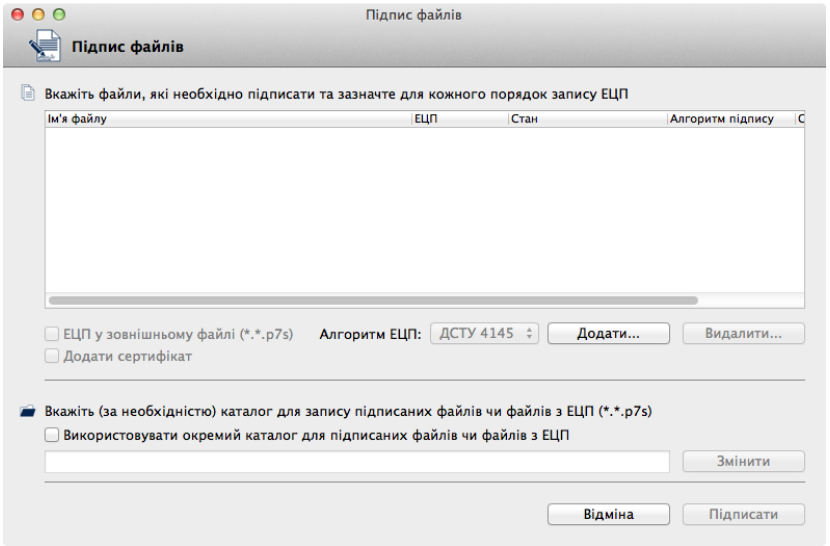


Рисунок 5.1

Після встановлення значень параметрів вікно може мати вигляд як наведено на рис. 5.2.

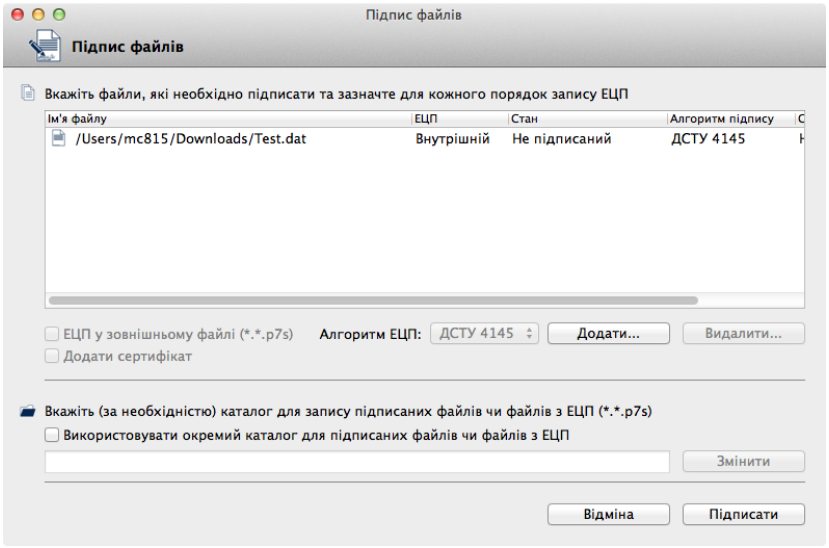


Рисунок 5.2

Для підпису файлів необхідно натиснути кнопку “Підписати”.

Після здійснення підпису файлів вікно буде містити інформацію про результати підпису (рис. 5.3).

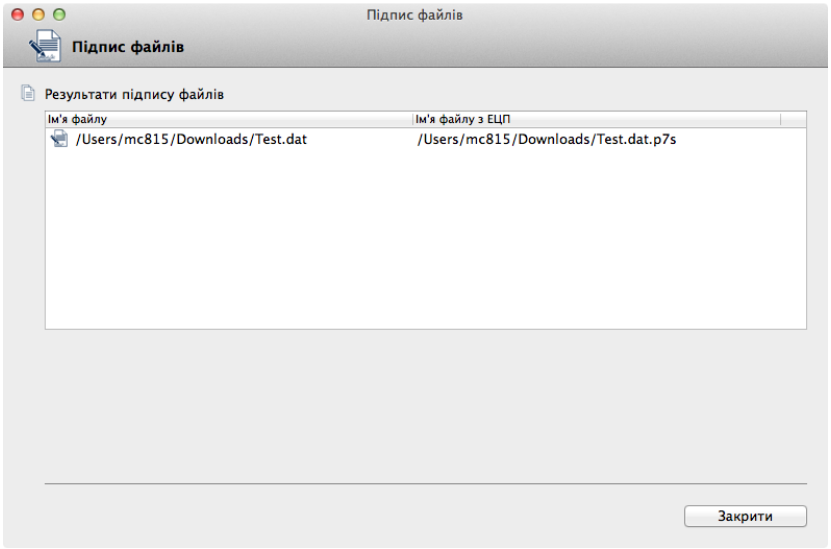


Рисунок 5.3

5.2 Перевірка файлів

Для перевірки підпису (ЕЦП) файлів необхідно натиснути на панелі “Перевірити файли” у головному вікні програми або обрати підпункт “Перевірити підпис” у пункті меню “Файли”.

Вікно перевірки файлів наведене на рис. 5.4. Вікно містить наступні параметри:

- список файлів, які необхідно перевірити;
- признак запису файлів без ЕЦП у окремий каталог;
- ім’я каталогу для запису файлів без ЕЦП.

Список файлів містить імена файлів що необхідно перевірити. Файли додаються до списку за допомогою кнопки “Додати” та стандартного діалогового вікна вибору файлів ОС. Для видалення файлів зі списку необхідно виділити відповідні файли у списку та натиснути кнопку “Видалити”.

Признак запису файлів без ЕЦП у окремий каталог встановлює необхідність запису файлів після зняття ЕЦП у окремий каталог що задається параметром “Каталог для запису файлів без ЕЦП ”. Якщо признак не встановлено файли без ЕЦП будуть записуватися у каталог з підписаними файлами.

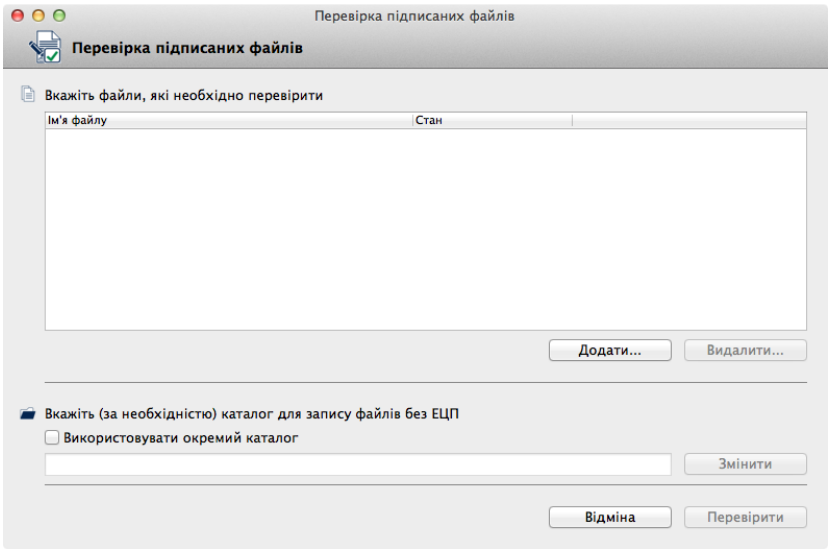


Рисунок 5.4

Після встановлення значень параметрів вікно може мати вигляд як наведено на рис. 5.5.

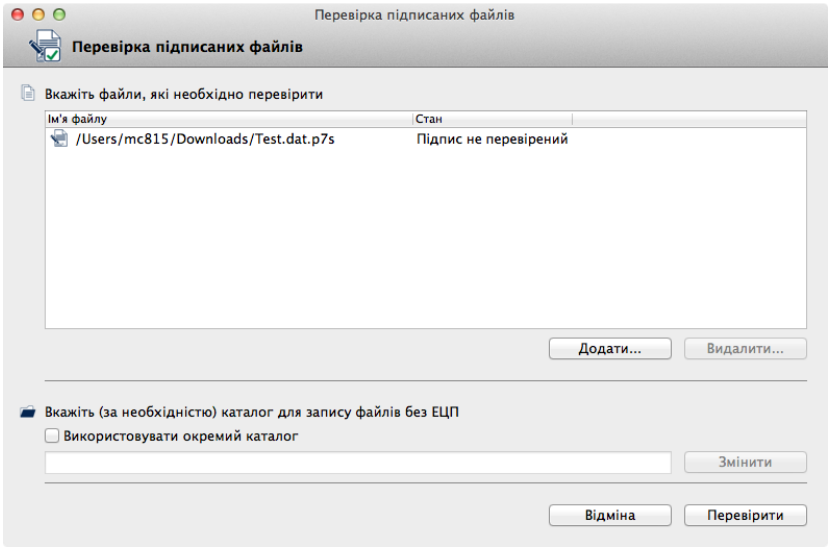


Рисунок 5.5

Для перевірки файлів необхідно натиснути кнопку “Перевірити”.

Після здійснення перевірки файлів вікно буде містити інформацію про результати підпису (рис. 5.6).

В разі вдалої перевірки можна також переглянути інформацію про підписаний файл (для цього необхідно натиснути на відповідний запис про файл). Вікно наведене на рис. 5.7.

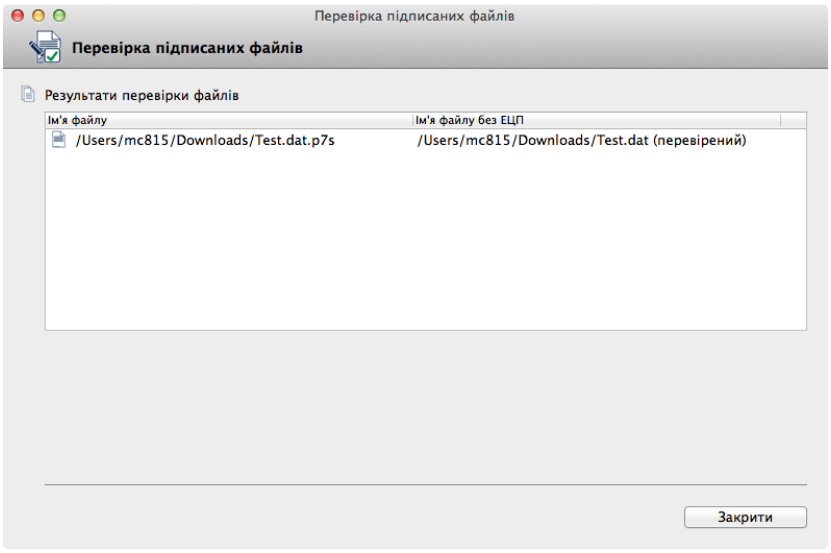


Рисунок 5.6

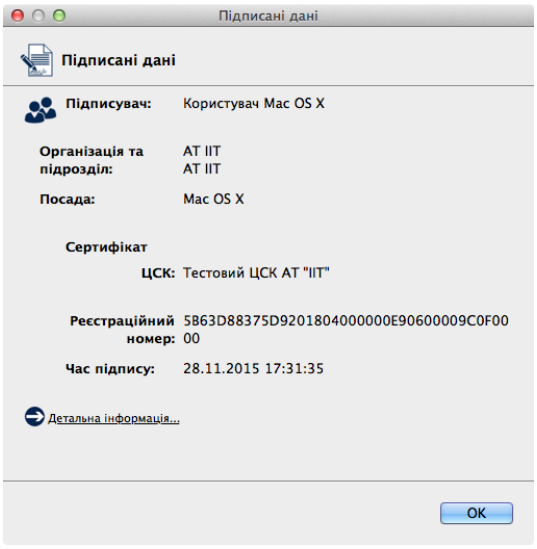


Рисунок 5.7

У детальній інформації наводиться сертифікат користувача що підписав файл.

Якщо ЕЦП містився в файлі з даними, при перевірці підпису буде створено копію файлу без підпису без розширення “.p7s”. За замовчанням (якщо не встановлено окремого каталогу для файлів без підпису) файл буде записаний до того ж каталогу у якому знаходився підписаний файл.

5.3 Зашифрування файлів

Для зашифрування файлу необхідно натиснути на панелі “Зашифрувати файли” у головному вікні програми, або обрати підпункт “Зашифрувати” у пункті меню “Файли”.

Вікно зашифрування файлів наведене на рис. 5.8. Вікно містить наступні параметри:

- список файлів, які необхідно зашифрувати;
- признак необхідності додаткового підпису файлу;
- признак запису зашифрованих файлів у окремий каталог;
- ім’я каталогу для запису зашифрованих файлів.

Список файлів містить імена файлів що необхідно зашифрувати. Файли додаються до списку за допомогою кнопки “Додати” та стандартного діалогового вікна вибору файлів ОС. Для видалення файлів зі списку необхідно виділити відповідні файли у списку та натиснути кнопку “Видалити”.

Признак додаткового підпису файлів (“Додатково підписати”) встановлює необхідність підпису файлу. За замовчанням здійснюється лише зашифрування кожного файлу.

Вихідні зашифровані файли мають розширення “.p7e”.

Признак запису зашифрованих файлів у окремий каталог встановлює необхідність запису зашифрованих файлів до окремого каталогу що задається параметром “Каталог для запису зашифрованих файлів”.

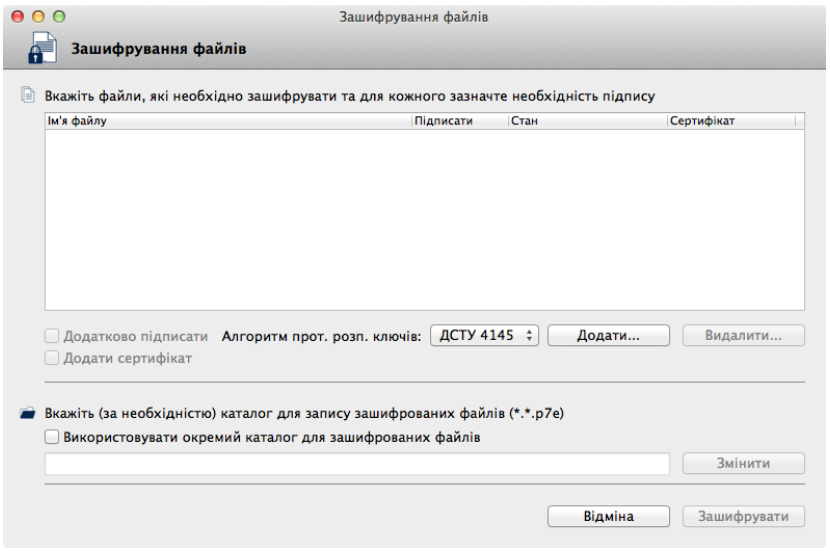


Рисунок 5.8

Після встановлення значень параметрів, вікно може мати вигляд як наведено на рис. 5.9. Для виконання зашифрування необхідно натиснути кнопку “Зашифрувати”.

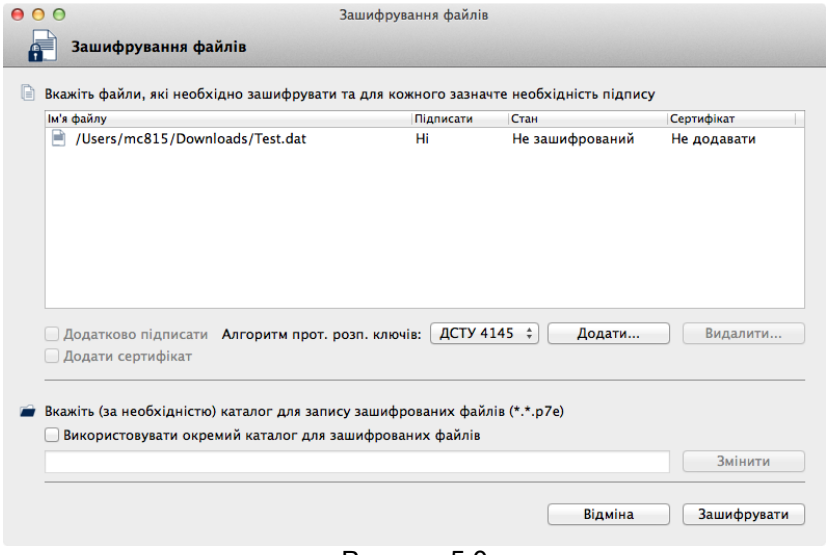


Рисунок 5.9

Для зашифрування файлів використовується особистий ключ користувача що виконує зашифрування та сертифікат(и) користувача(ів) для якого(их) зашифровується файл. Тому у вікні що наведене на рис. 5.10 необхідно обрати користувачів для яких виконується зашифрування файлу. Зашифрований файл може бути відкритим лише користувачем для якого виконувалось зашифрування.

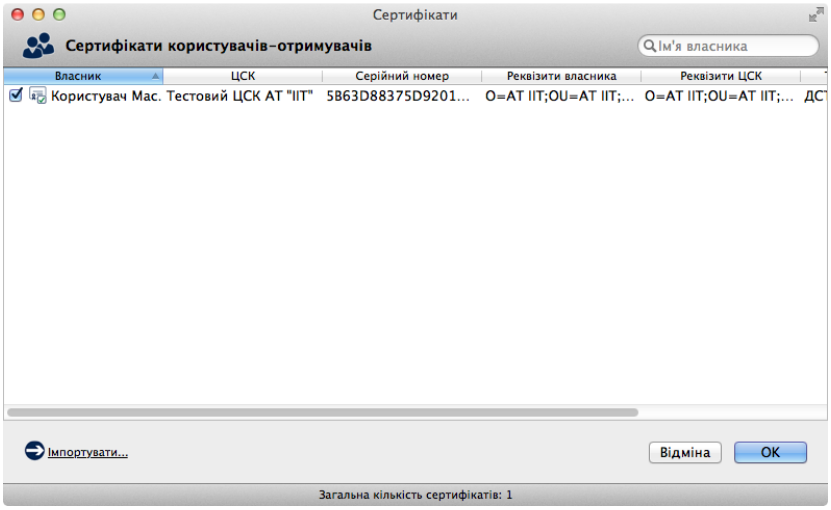


Рисунок 5.10

Під час шифрування здійснюється перевірка параметрів ключових даних користувачів що були обрані у списку (рис 5.10). Якщо параметри ключів користувачів для яких виконується шифрування будуть відрізнятись від параметрів ключів користувача що виконує шифрування, користувачу буде видане повідомлення про неможливість виконування шифрування у зв'язку з відмінністю параметрів та процес шифрування буде припинено. Для запобігання цього слід переглянути сертифікат користувача на адресу якого виконується шифрування та перевірити відповідність параметрів власних ключів параметрам ключів цього користувача.

Після здійснення зашифрування файлів буде виведене наступне вікно (рис. 5.11) з інформацією про результати зашифрування.

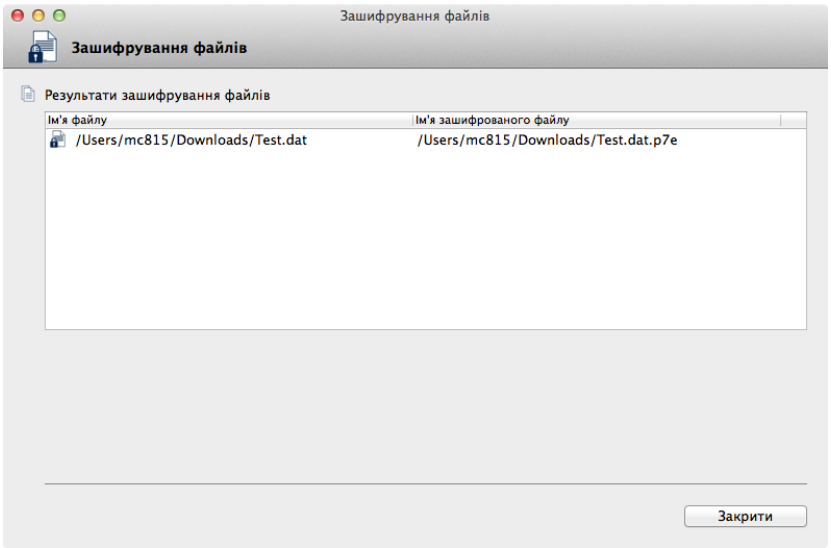


Рисунок 5.11

5.4 Розшифрування файлів

Для розшифрування файлів необхідно натиснути на панелі "Розшифрувати файли" у головному вікні програми, або пункт меню "Розшифрувати" у розділі меню "Файли". Вікно розшифрування файлів наведене на рис. 5.12. Форма містить наступні параметри:

- список зашифрованих файлів, які необхідно розшифрувати;
- признак запису розшифрованих файлів у окремий каталог;
- ім'я каталогу для запису розшифрованих файлів.

Список файлів містить імена файлів що необхідно розшифрувати. Файли додаються до списку за допомогою кнопки "Додати" та стандартного діалогового вікна вибору файлів ОС. Для видалення файлів зі списку необхідно виділити відповідні файли у списку та натиснути кнопку "Видалити".

Признак запису розшифрованих файлів у окремий каталог встановлює необхідність запису розшифрованих файлів у окремий каталог що задається параметром “Каталог для запису розшифрованих файлів”.

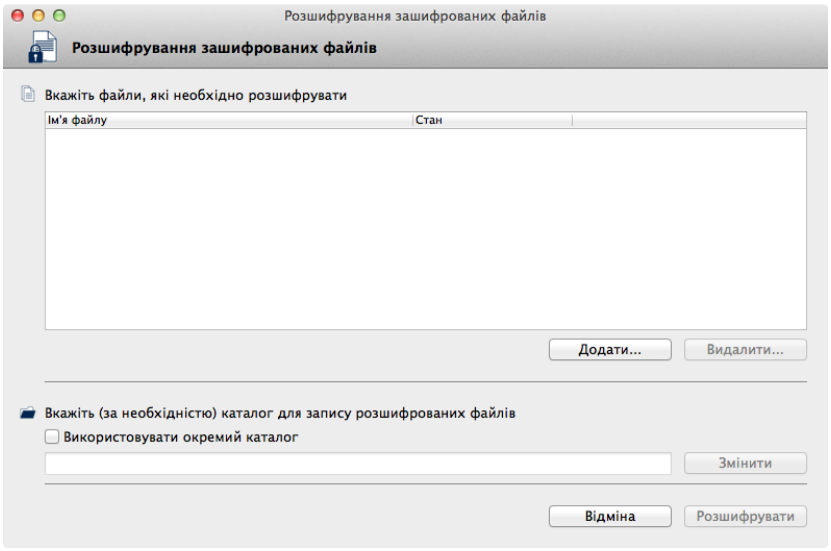


Рисунок 5.12

Після встановлення значень параметрів, вікно розшифрування файлів може мати вигляд як наведено на рис. 5.13.

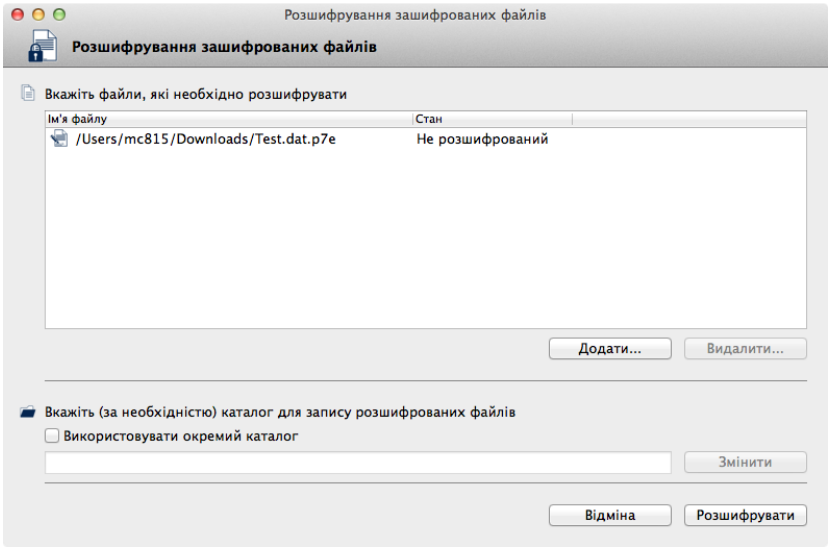


Рисунок 5.13

Для розшифрування файлів необхідно натиснути кнопку “Розшифрувати”. Після розшифрування буде виведено інформацію про результати розшифрування (рис. 5.14).

В разі вдалого розшифрування є можливість переглянути інформацію про розшифровані файли (рис. 5.15), для чого необхідно натиснути на запис про відповідний файл.

За замовчанням (якщо не встановлено окремого каталогу для розшифрованих файлів) розшифровані файли будуть записані до того ж каталогу у якому знаходилися зашифровані.

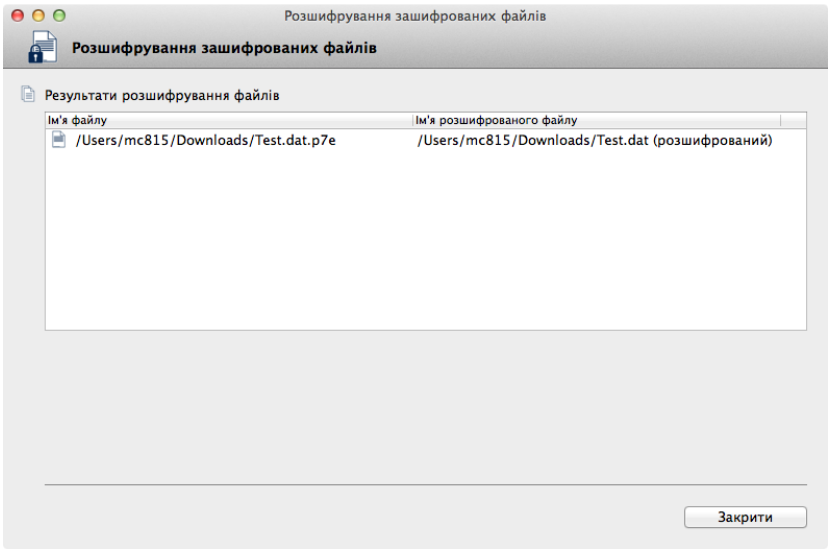


Рисунок 5.14

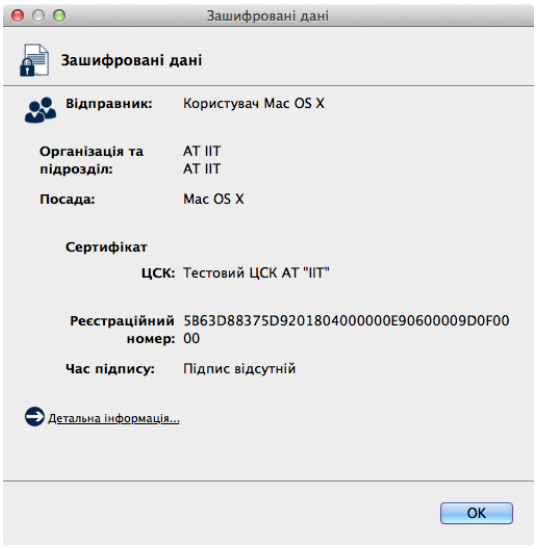


Рисунок 5.15

ПЕРЕЛІК СКОРОЧЕНЬ

ОС	Операційна система
ЕЦП	Електронний цифровий підпис
КЗІ	Криптографічний захист інформації
ДКЕ	Довгостроковий ключовий елемент
СВС	Список відкликаних сертифікатів
ЦСК	Центр сертифікації ключів
НКІ	Носій ключової інформації (особистого ключа)
ПЕОМ	Персональна електронно-обчислювальна машина
CMP	Certificate Management Protocol (протокол управління обслуговуванням сертифікатів)
OCSP	Online Certificate Status Protocol (протокол визначення статусу сертифіката)
LDAP	Lightweight Directory Access Protocol (протокол доступу до каталогу)
TSP	Time-Stamp Protocol (протокол отримання позначок часу)
HTTP	Hyper Text Transfer Protocol