

Інструкція

користувачеві програмного комплексу Користувач ЦСК (версія 1.3.1)

АНОТАЦІЯ

Даний документ містить настанову оператора для роботи з програмним комплексом користувача центра сертифікації ключів (далі — програма). Настанова містить відомості щодо послідовності та особливостей інсталяції, встановлення параметрів роботи та використання програми.

Оглавление

| 31 | МІСТ | Γ | | |
|----|----------------------|--|----|--|
| Π | ерелі | ік скорочень | 4 | |
| 1 | Призначення програми | | | |
| 2 | Ум | мови виконання програми | 4 | |
| 3 | Інс | сталяція програми | 4 | |
| 4 | По | очаток роботи з програмою | 7 | |
| | 4.1 | Завантаження програми | 7 | |
| | 4.2 | Встановлення параметрів роботи програми | 8 | |
| | 4.3 | Режими роботи програми | | |
| 5 | Уп | травління сертифікатами та CBC | | |
| | 5.1 | Отримання сертифікатів з ЦСК | 13 | |
| | 5.2 | Зчитування сертифікатів та СВС | | |
| | 5.3 | Перегляд сертифікатів | 13 | |
| | 5.4 | Перегляд СВС | 16 | |
| | 5.5 | Завантаження СВС | | |
| 6. | Упр | авління ключами | 19 | |
| | 6.1 | Генерація ключів | 19 | |
| | 6.2 | Встановлення сертифікатів особистого ключа ЕЦП | 23 | |
| | 6.3 | Зчитування особистого ключа | | |
| | 6.4 | Резервне копіювання особистого ключа | 27 | |
| | 6.5 | Зміна паролю захисту особистого ключа | | |
| 6 | 3az | хист файлів | | |
| | 7.1 | Підпис файлів | | |
| | 7.2 | Перевірка підпису файлів | | |
| | 7.3 | Зашифрування файлів | | |
| | 7.4 | Розшифрування файлів | | |
| 8 | До | овідкова система | | |
| | 8.1 | Контактні відомості для зв'язку | | |

| OC | Операційна система |
|------|--|
| EOT | Електронно-обчислювальна техніка |
| ЕЦП | Електронний цифровий підпис |
| K3I | Криптографічний захист інформації |
| ДКЕ | Довгостроковий ключовий елемент |
| CBC | Список відкликаних сертифікатів |
| ЦСК | Центр сертифікації ключів |
| HKI | Носій ключової інформації (особистого ключа) |
| ПЕОМ | Персональна електронно-обчислювальна машина |
| 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 |

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 HKI;
 - 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;
 - визначення статусу сертифікатів за допомогою СВС;
 - перевірку чинності та цілісності сертифікатів та ін.;
- захист файлів користувача:
 - підпис файлів;
 - перевірку файлів;
 - шифрування файлів;
 - розшифрування файлів.

2 УМОВИ ВИКОНАННЯ ПРОГРАМИ

Програма може бути завантажена та виконана на ПЕОМ під керуванням ОС Microsoft Windows версій 7, 8 або 10.

3 ІНСТАЛЯЦІЯ ПРОГРАМИ

Для інсталяції програми необхідно скачати і потім запустити програму інсталяції (майстер інсталяції) EUPravexBankInstall.exe з одного із сайтів Банку:

https://www.pravex.com.ua/korporativnym-klientam-bankam/vsi-poslugi/groshovi-perekazi

https://ca.pravex.com.ua/user-downloads або з іншого інсталяційного носія.

Після запуску програми інсталяції на першій сторінці (рис. 3.2) виводиться інформація про початок інсталяції. Для продовження інсталяції необхідно натиснути кнопку "Далі", а для завершення — "Скасувати".

| 🧰 Встановлення — Користу | вач ЦСК ПРАВЕКС БАНК | <u></u> | | × |
|---|--|--|--------------------------------|------|
| ПРАВЕКС БАНК Центр сертифікації ключів | Ласкаво просимо , встановлення Кор ПРАВЕКС БАНК. | до про истува | грами ч ЦСН | 1 |
| Користувач ЦСК | Ця програма встановить IIT Кори ваш комп'ютер. Рекомендусться закрити всі інші п продовженням. Натисніть «Далі», щоб продовжи виходу з програми встановлення. | стувач ЦСК-: програми пер ги, або «Ска | 1.3 (1.3.1) ед сувати» д |) на |
| | | Далі > | Скасу | вати |

Рисунок 3.2

На наступній сторінці майстра (рис. 3.3) за необхідністю можна вказати каталог на диску до якого буде встановлено програму. Для продовження інсталяції необхідно натиснути кнопку "Далі".

| 🔟 Встановлення — Користувач ЦСК ПРАВЕКС БАНК — 🛛 🗙 |
|---|
| Вибір шляху встановлення Куди ви бажаєте встановити Користувач ЦСК ПРАВЕКС БАНК? |
| Програма встановить Користувач ЦСК ПРАВЕКС БАНК у наступну папку. |
| Натисніть «Далі», щоб продовжити. Якщо ви бажаєте вибрати іншу папку, натисніть «Огляд». |
| tute of Informational Technologies\Certificate Authority-1.3\End User Огляд |
| |
| |
| |
| Необхідно як мінімум 33,7 Мб вільного дискового простору. |
| < Назад Далі > Скасувати |

Рисунок 3.3

На наступній сторінці майстра (рис. 3.4) за необхідністю можна вказати розділ меню "Пуск" до якого буде встановлено значки запуску та деінсталяції програми. Для продовження інсталяції необхідно натиснути кнопку "Далі".

| 🧰 Встановлення — Користувач ЦСК ПРАВЕКС БА | нк | — | | × |
|---|---------------------|---------|--------|-------|
| Вибір папки в меню «Пуск» | | | | |
| Де ви бажаєте створити ярлики? | | | | 100 |
| Програма встановлення створить ярлики | и наступній папці і | иеню «Г | lуск». | |
| Натисніть «Далі», щоб продовжити. Якщо ви бах натисніть «Огляд». | каєте вибрати інш | у папку | , | |
| IIT\Користувач ЦСК-1.3 | | 0 | сляд | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| < ! | <u>І</u> азад Далі | > | Скасу | /вати |

Рисунок 3.4

На наступній сторінці майстра (рис. 3.5) необхідно вказати каталог до якого будуть завантажуватись та зберігатися сертифікати і СВС. У параметрах роботи самої програми даний каталог визначається як "Каталог з сертифікатами та СВС" у параметрах файлового сховища (див. п. 4.2.2). Для зміни каталогу необхідно натиснути кнопку "Змінити" та обрати існуючий каталог чи створити новий. Для продовження інсталяції необхідно натиснути кнопку "Далі". Рекомендується залишити цей параметр без змін.

| 🔟 Встановлення — Користувач ЦСК ПРАВЕКС БАНК | _ | | | × |
|---|-----|--------------|-------|------|
| Вкажіть каталог для сертифікатів та СВС | | | | |
| Де створити каталог для сертифікатів та СВС? | | | ſ | INN |
| Вкажіть каталог для сертифікатів та СВС, натисніть Далі. Для вибс каталогу, натисніть Змінити. | ору | іншого |) | |
| C:\CACertificates | | О <u>г</u> л | яд | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| < <u>Н</u> азад Далі | > | | Скасу | вати |
| | | | | |

Рисунок 3.5

На наступній сторінці майстра (рис. 3.6) потрібно встановити признаки необхідності виконання майстром додаткових завдань — створення значку запуску програми на робочому столі та запуску програми після завершення інсталяції. Для продовження інсталяції необхідно натиснути кнопку "Далі".

| 🚾 Встановлення — Користувач ЦСК ПРАВЕКС БАНК — 🛛 📉 🗙 |
|--|
| Вибір додаткових завдань |
| Які додаткові завдання ви бажаєте виконати? |
| Виберіть додаткові завдання які програма встановлення Користувач ЦСК ПРАВЕКС БАНК повинна виконати, потім натисніть «Далі». |
| Додаткові значки: |
| Створити значок на робочому столі |
| Інші завдання: |
| Завантажити програму після інсталяції |
| |
| |
| |
| |
| |
| |
| < <u>Н</u> азад Далі > Скасувати |
| |

Рисунок 3.6

На наступній сторінці майстра (рис. 3.7) буде виведено інформацію про операції, що будутьвиконані майстром. Для виконання інсталяції необхідно натиснути кнопку "Встановити".

| 🔟 Встановлення — Користувач ЦСК ПРАВЕКС БАНК — | × |
|---|---------|
| Усе готово до встановлення Програма готова розпочати встановлення Користувач ЦСК ПРАВЕКС БАНК на ваш комп'ютер. | ักกกิ |
| Натисніть «Встановити» для продовження встановлення, або «Назад», якщо ви бажаєте переглянути або змінити налаштування встановлення. | |
| Шлях встановлення: C:\Program Files (x86)\Institute of Informational Technologies\Certificate Auth Папка в меню «Пуск»: IIT\Користувач ЦСК-1.3 | ^ |
| Додаткові завдання: Додаткові значки: Створити значок на робочому столі | |
| < > | ~ |
| < Назад Встановити Ска | асувати |

Рисунок 3.7

Після інсталяції програми, майстер завершує свою роботу.

4 ПОЧАТОК РОБОТИ З ПРОГРАМОЮ

4.1 Завантаження програми

Для початку роботи програми у каталозі із сертифікатами та СВС обов'язково повинні бути записані:

- сертифікат ЦСК;
- діючі СВС.

Інформативно: сертифікати ЦСК, серверів ЦСК та СВС необхідно записати у відповідний каталог, отримавши їх від співробітників Банку разом з інсталяційним пакетом або завантажити з офіційного сайту ЦСК ca.pravex.com.ua.

Для завантаження програми необхідно запустити модуль EU.exe через файловий менеджер OC або через меню "Пуск", обравши у розділі "IIT\Користувач ЦСК-1" підпункт "Користувач ЦСК ПРАВЕКС БАНК" чи за допомогою значку на робочому столі. Після запуску на екрані буде відображене головне вікно програми, що наведене на рис. 4.1.

| 🔟 Користувач ЦСК ПРАВЕКС БАНК — 🗆 | | | | | | |
|-----------------------------------|--|--|---|--|--|--|
| ітіі. Пен | ІРАВЕКС БАНК Ітр сертифікації ключів | | | | | |
| = | | | | | | |
| | Підписати файли Підпис файлів на особистому ключеві Підпис файлив на особистому ключеві | | | | | |
| | Зашифрувати файли Зашифрувати файлів на одного чи декількох користувачів Розшифрування зашифрованих файлів | | | | | |
| | Переглянути сертифікати Перегляд сертифікатів у файловому сховищі | | | | | |
| | Встановити параметри Встановлення параметрів роботи користувача Згенерувати ключів із запитами на формування сертифікатів | | | | | |
| | | | _ | | | |
| | Про програму Перейти до web-сайту ЦСК | | | | | |
| | | | | | | |
| | | | | | | |

Рисунок 4.1

4.2 Встановлення параметрів роботи програми

Програма інсталяції під час свого виконання встановлює параметри роботи програми зазамовчанням. Параметри встановлені для онлайн режиму, тобто потребується доступ до сайту ca.pravex.com.ua.

Інформативно: для роботи в офф-лайн режимі (без взаємодії з ЦСК) необхідно в меню обрати пункт «Параметри», після чого натиснути «Перейти в режим off-line (не взаємодіяти з ЦСК)» або натиснути комбінаціїю клавіш Ctrl+O. Для роботи в off-line режимі у файловому сховищі повинні бути сертифікати ЦСК, користувача та списки відкликаних сертифікатів (CBC, або CRL). Усе це можна завантажити з веб-сайту ЦСК.

Для встановлення чи зміни параметрів роботи програми необхідно обрати підпункт "Встановити" впункті меню "Параметри" (рис. 4.1). Вікно встановлення параметрів наведене на рис. 4.2.

| Файлове сховище | Файлове сховище сертифікатів та |
|--------------------|---|
| Ргоху-сервер | Параметри Файлового сховища |
| TSP-сервер | Каталог з сертифікатами та СВС: |
| | C:\CACertificates 3мінит |
| ОСЅР-сервер | Автоматично перечитувати при виявленні змін |
| LDAP-cepsep | 3берігати сертифікати, що отримані з OCSP-, LDAP- чи CMP-серверів |
| СМР-сервер | Час зберігання стану перевіреного сертифіката, с: 3600 |
| | ✓ Перевіряти СВС —————————————————————————————————— |
| Ссобистий ключ | Тільки свого ЦСК |
| Сертифікати та СВС | Завантажувати автоматично |
| Реєстрація подій | |
| | |

Рисунок 4.2

4.2.1 ФАЙЛОВЕ СХОВИЩЕ

Для настроювання параметрів файлового сховища сертифікатів та СВС необхідно перейти дозакладки "Файлове сховище". Вікно "Параметри роботи" із сторінкою "Файлове сховище" наведене на рис. 4.2.

На цій сторінці встановлюються наступні параметри роботи програми:

 – "Каталог з сертифікатами та СВС". Даний параметр встановлює каталог файлового сховища для зберігання сертифікатів та СВС. Всі сертифікати та СВС, що завантажуються не засобами програми повинні записуватися у даний каталог.

Інформативно: необхідно перевіряти правильність вказаного каталогу. Він повинен збігатися з тим, що був вказаний при інсталяції.

- "Автоматично перечитувати файлове сховище при виявлені змін". Даний параметр визначає необхідність автоматичного перечитування каталогу файлового сховища програмою привнесенні будь-яких змін до цього каталогу (запису нового сертифіката чи СВС у каталог чи видалення файлу з сертифікатом або СВС). Якщо параметр не встановлено необхідно виконувати повторне зчитування файлового сховища після внесення змін. Для цього необхідно обрати підпункт "Зчитати сертифікати та СВС" в пункті меню "Сертифікати та СВС" або натиснути клавішу "F9" у головному вікні програми.
- "Використовувати СВС". Параметр вказує на необхідність використання СВС в якості засобу перевірки статусу сертифікатів відкритих ключів що використовуються.
- "Тільки свого ЦСК". Даний параметр визначає необхідність використовувати при перевірці сертифікатів СВС лише свого ЦСК у ланцюжку. Для цього повинен бути зчитаний особистий ключ користувача, оскільки ЦСК користувача визначається за допомогою параметрів особистого ключа.

Для збереження внесених змін необхідно натиснути кнопку "Застосувати".

4.2.2 PROXY-CEPBEP

У випадку, якщо комп'ютер користувача підключений до мережі інтернет через proxy-сервер, то для настроювання параметрів необхідно перейти до закладки "Proxy-сервер" у вікні що наведене на рисунку 4.3. Поставити «галочку» навпроти пункту «Підключатися через proxy-сервер» та у відповідних полях прописати параметри цього сервера.

У випадку, якщо комп'ютер має пряме підключення до мережі інтернет, настроювати даний пунк не треба.

| Параметри роботи | | Х |
|--------------------|---------------------------------|-----|
| Файлове сховище | Ргоху-сервер | |
| Ргоху-сервер | Підключатися через ргоху-сервер | |
| ТSР-сервер | | |
| ОСSР-сервер | | |
| LDAP-сервер | | |
| СМР-сервер | | |
| УССОБИСТИЙ КЛЮЧ | | |
| Сертифікати та СВС | | |
| Реєстрація подій | | |
| | | |
| | ОК Відміна Застосув | ати |
| | | |

Рисунок 4.3

Для збереження внесених змін необхідно натиснути кнопку "Застосувати".

4.2.3 TSP-CEPBEP

Для настроювання параметрів TSP-сервера необхідно перейти до закладки "TSP-сервер" у вікні що наведене на рисунку 4.4.

| Параметри роботи | × |
|--------------------|---|
| Файлове сховище | При тур-сервер ЦСК |
| Ргоху-сервер | Отримувати позначки часу |
| С ТSP-сервер | DNS-ім'я чи IP-адреса сервера: са pravex.com.ua |
| ОСЅР-сервер | ТСР-порт: 80 З сертифіката 🔻 |
| LDAP-сервер | |
| СМР-сервер | |
| 餐 Особистий ключ | |
| Сертифікати та СВС | |
| Реєстрація подій | |
| | |
| | |
| | ОК Бідміна Застосувати |

Рисунок 4.4 10

Для збереження внесених змін необхідно натиснути кнопку "Застосувати".

4.2.4 OCSP-CEPBEP

Для настроювання параметрів OCSP-сервера необхідно перейти до закладки "OCSP-сервер" у вікніщо наведене на рисунку 4.5.

| Параметри роботи | × |
|-------------------|---|
| Файлове сховище | 📙 ОСЅР-сервер ЦСК |
| Ргоху-сервер | Використовувати ОСЅР-сервер |
| TSP-сервер | DNS-ім'я чи IP-адреса сервера: са.pravex.com.ua |
| ОСЅР-сервер | ТСР-порт: 80 З сертифіката 🔻 |
| LDAP-сервер | Перевіряти до перевірки у Файловому сховищі |
| СМР-сервер | Використовувати точки доступу до OCSP-серверів |
| 🔊 Особистий ключ | |
| ертифікати та CBC | |
| Реєстрація подій | |
| | |
| | |
| | ОК Відміна Застосувати |

Рисунок 4.5

Для збереження внесених змін необхідно натиснути кнопку "Застосувати".

4.2.5 LDAP-CEPBEP

Для настроювання параметрів LDAP-сервера перейти до закладки "LDAP-сервер" у вікні щонаведене на рисунку 4.6.

Зазвичай LDAP-сервер не використовується.

| Параметри роботи | X | (|
|---|---|---|
| Файлове сховище Proxy-сервер TSP-сервер OCSP-сервер LDAP-сервер CMP-сервер Особистий ключ Сертифікати та СВС Реєстрація подій | ■ LDAP-сервер ЦСК Використовувати LDAP-сервер | |
| | ОК Відміна Застосувати | |

Рисунок 4.6

Для збереження внесених змін необхідно натиснути кнопку "Застосувати".

4.3 Режими роботи програми

Для встановлення режиму off-line роботи з ЦСК необхідно обрати підпункт меню "Перейти врежим offline (не взаємодіяти з ЦСК)/Перейти в режим on-line (взаємодіяти з ЦСК)" в пункті меню "Параметри".

Якщо програма працює у режимі off-line інформацію про це буде виведено до нижньої правої частини головного вікна програми (рис.4.7).

| 🔟 Користувач ЦСК ПРАВЕКС БАНК | - | | × |
|---|---|--------------|------|
| ПРАВЕКС БАНК Центр сертифікації ключів | | | |
| = | | | |
| Підписати файли Підпис файлів на особистому ключеві Підпис файлів на особистому | | | |
| Зашифрувати файли Зашифрування файлів на одного чи декількох користувачів | | | |
| Переглянути сертифікати Перегляд сертифікатів у файловому сковищі | | | |
| Встановити параметри Встановлення параметрів роботи користувача Ястановления сертифікатів | | | |
| | | _ | |
| Про програму Перейти до web-сайту ЦСК | | | |
| | | | |
| | C |)ff-line pex | им 🝶 |

Рисунок 4.7

5 УПРАВЛІННЯ СЕРТИФІКАТАМИ ТА СВС

5.1 Отримання сертифікатів з ЦСК

Набір сертифікатів отримується разом з програмним забезпеченням Банком після укладання всіх необхідних договорів.

До пакету сертифікатів входять сертифікат ЦСК та сертифікат користувача.

Для встановлення сертифікатів необхідно скопіювати їх з носія в папку, що зазначається при інсталяції (рисунок 3.5.).

У режимі on-line можна отримати набір сертифікатів за власним ключем:

| Файли Текст Особистий ключ | > 4 > 4 | обистому Гер файл | евірити фай вірка підпису нах | йли / на підлисаних | |
|-------------------------------------|------------------|--|-------------------------------------|-------------------------------|--|
| Сертифікати та СВС Параметри | > | Переглянути сертифікати Переглянути СВС | F10 F11 | айли | |
| Допомога | , | Отримати з ЦСК | | 118 | |
| (g=) Перегляд файловому встанови | скови | Заблокувати власні сертифікати Скасувати власні сертифікати | 1 | повому | |
| Встановле користувач | ння парам на | иетрів роботи Гене Форм | рація ключів і чування серті | із запитами на ифікатів | |
| | | | | | |
| Про програми | <u>veb-сайту</u> | Зчитати. | | | |

Рисунок 5.1

Потрібно зчитати власний ключ, після чого усі необхідні сертифікати будуть завантажені з веб-сайту ЦСК.

5.2 Зчитування сертифікатів та СВС

Програма автоматично виконує зчитування сертифікатів та СВС з файлового сховища при першій необхідності після свого запуску. При внесенні змін (запису чи видалення сертифікатів чи СВС) до файлового сховища під час роботи програми, якщо не встановлено параметр "Автоматично перечитувати файлове сховище при виявленні змін" (див п. 4.2.1), необхідно перечитати файлове сховище. Для цього необхідно обрати підпункт "Зчитати сертифікати та СВС" в пункті меню "Сертифікати та СВС" або натиснути клавішу F9.

5.3 Перегляд сертифікатів

Для перегляду сертифікатів що містяться у файловому сховищі необхідно обрати підпункт "Переглянути сертифікати…" в пункті меню "Сертифікати та СВС" або натиснути клавішу F10. Вікно із сертифікатами наведене на рис. 5.4.

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 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 5.5 та 5.6.

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 (див п. 4.2) - за допомогою CBC, OCSP-протоколу тощо. Результатом перевірки буде вікно що наведене на рис. 5.7. Якщо у цьому вікні натиснути "Сертифікат", сертифікат буде відображенийу вікні детального перегляду (рис. 5.6).

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 5.5

| тифікат Сертифікат | | > |
|--------------------------------|--------------------------------------|---|
| оля сертифіката: | | |
| 📧 Реквізити власника | О=Публічне акціонерне товариство к | ^ |
| 🖻 Реквізити ЦСК | О=Публічне акціонерне товариство к | |
| 📰 Реєстраційний номер | 0EB1A8661085F7CD02000000200000 | |
| 📧 Додаткові дані власника | | |
| Адреса | 01021, Україна, м. Київ, Кловський у | |
| Телефон | 0 800 500 450 | |
| DNS-ім'я чи інше технічного за | ca.pravex.com.ua | |
| Адреса електронної пошти | ca@pravex.ua | |
| 🖻 Строк чинності сертифіката | | |
| Сертифікат чинний з | 27.11.2017 00:00:00 | |
| Сертифікат чинний до | 27.11.2022 00:00:00 | |
| 💷 Строк дії особистого ключа | | |
| Особистий ключ діє з | 27.11.2017 00:00:00 | |
| Особистий ключ діє до | 27.11.2022 00:00:00 | |
| 📰 Параметри відкритого ключа | | |
| Тип ключа | ДСТУ 4145-2002 | |
| Довжина ключа | 264 біт(а) | |
| Відкритий ключ | CD 1E 4C 74 14 94 90 73 5C 14 A7 A9 | |
| Ідентифікатор відкритого ключа | 63 8A 4B DB 36 C7 C0 2C B6 B3 42 C9 | |
| Використання ключів | ЕЦП | ~ |

Рисунок 5.6

| Пошу | к та <mark>визначення статус</mark> | у се <mark>ртифік</mark> ат | а | × |
|---------|---|--|------------------------------------|--------------|
| | Сертифікат з | найдено | та перев <mark>і</mark> рено | |
| • | Сертифікат | | | ОК |
| Pe | зультати пошуку та в | изначення с | татусу: | |
| | Пошук чи перевірка сер через OCSP-сервер з D IP-адресою http://ca.pravex.com.ua/ | тифіката NS-ім'ям чи services/ocsr | Сертифікат чинний | |
| <u></u> | Перевірка сертифіката сховищі | у файловому | Сертифікат чинний | |
| Iн¢ | юрмація про сертифі | кат: | | |
| | Власник | СМР-сервер ПАТКБ "ПР. | О ЦЕНТР СЕРТИФІКАЦ АВЕКС-БАНК'' | ції КЛЮЧІВ |
| 1 | ЦСК | ЦЕНТР СЕР "ПРАВЕКС- | ТИФІКАЦІЇ КЛЮЧІВ П БАНК'' | АТКБ |
| 2= | РН сертифіката відкр. ключа ЕЦП | 0EB1A86610 | 085F7CD020000000200 | 000006000000 |

Рисунок 5.7

5.4 Перегляд СВС

Для перегляду списків відкликаних сертифікатів (СВС) необхідно натиснути підпункт "Переглянути СВС…" в пункті меню "Сертифікати та СВС" або натиснути клавішу F11. Вікно із списками відкликаних сертифікатів наведене на рис. 5.8.

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

Для перегляду CBC необхідно натиснути на відповідному записі про CBC у списку. CBC буде відображено у вікні що наведене на рисунках 5.9 та 5.10.

Для видалення файлу CBC з файлового сховища необхідно виділити відповідний запис про CBC у списку та натиснути кнопку "Видалити".

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

| Списки відкликаних сертифікатів | | | | × |
|--|----------------|--|--|------------------------|
| Списки відкликаних си Кількість: 2 | ертифікатів | | | |
| ЦСК 👻 | Серійний номер | Час формування | Наступний | Тип підлису |
| ЦЕНТР СЕРТИФІКАЦІЇ КЛЮЧІВ ЦЕНТР СЕРТИФІКАЦІЇ КЛЮЧІВ | 39BD 3A00 | 15.03.2021 17:52:51 17.03.2021 13:52:51 | 22.03.2021 17:57:51 17.03.2021 15:57:51 | ДСТУ 4145 ДСТУ 4145 |
| | | | | |
| | | | | |
| | | | | |
| < | | | | > |
| 🗢 Імпортувати | | | | ОК |

Рисунок 5.8

Список відкликаних сертифікатів

| LICK: | ЦЕНТР СЕРТИ | ФІКАЦІЇ КЛЮЧІВ ПАТКБ "П | РАВЕКС-БАНК" | |
|--|--|--|--|---|
| Реєстраційний номер: | 39BD | | | |
| Час | 15.03.2021 17:5 | 2. | | |
| формування: | наступнии - 22. | 03.2021 17:57 | | |
| призначення: | для використа | ння у державних алгоритма. | ктпротоколах | |
| Детальна інфо; | рмація | | | |
| | | | | |
| | | | | |
| | | | OK | |
| | _ | | | |
| | Dia | <u>רעט הע ה ע</u> | | |
| | Ри | сунок 5.9 | | |
| сок відкликаних се | Ри ертифікатів | сунок 5.9 | | |
| сок відкликаних се Список ві | Ри ертифікатів дкликаних | сунок 5.9 сертифікатів | | |
| сок відкликаних се Список ві агальна інформаі | Ри ертифікатів дкликаних ція: | сүнок 5.9 сертифікатів | | |
| сок відкликаних се Список ві агальна інформан Реквізити ЦСК | Ри ертифікатів дкликаних ція: | сунок 5.9 сертифікатів О=Публічне акціонерне | товариство к | 1 |
| сок відкликаних се Список ві агальна інформан Реквізити ЦСК Час формування | Ри ертифікатів дкликаних ція: | сертифікатів О=Публічне акціонерне 15.03.2021 17:52:51 | товариство к | , |
| сок відкликаних се Список ві агальна інформаі Реквізити ЦСК Час формування Час наступного ф | Ри ертифікатів дкликаних ція: рормування | сертифікатів О=Публічне акціонерне 15.03.2021 17:52:51 22.03.2021 17:57:51 | товариство к | , |
| сок відкликаних се Список ві агальна інформан Реквізити ЦСК Час формування Час наступного ф РН | Ри ертифікатів дкликаних ція: рормування | сертифікатів О=Публічне акціонерне 15.03.2021 17:52:51 22.03.2021 17:57:51 39BD | товариство к | , |
| сок відкликаних се Список ві агальна інформан Реквізити ЦСК Час формування Час наступного ф Рн Ідентифікатор від | Ри ертифікатів дкликаних ція: рормування критого клю | сертифікатів О=Публічне акціонерне 15.03.2021 17:52:51 22.03.2021 17:57:51 39BD 8E B1 A8 66 10 85 F7 CE | товариство к) 2E 37 D6 4D | |
| сок відкликаних се Список ві агальна інформан Реквізити ЦСК Час формування Час наступного ф РН Ідентифікатор від | Ри ертифікатів дкликаних ція: рормування коритого клю ок сертифікаті | сертифікатів О=Публічне акціонерне 15.03.2021 17:52:51 22.03.2021 17:57:51 39BD 8E B1 A8 66 10 85 F7 CE | товариство к) 2E 37 D6 4D | |
| сок відкликаних се Список ві агальна інформан Реквізити ЦСК Час формування Час наступного ф РН Центифікатор від писок відкликани 0EB1A8661085F7 | Ри артифікатів дкликаних ція: формування критого клю с сертифікаті СD030000002. | ССРНОК 5.9 Сертифікатів О=Публічне акціонерне 15.03.2021 17:52:51 22.03.2021 17:57:51 39BD 8E B1 A8 66 10 85 F7 CE ш | товариство к 0 2E 37 D6 4D Блокування | |
| сок відкликаних се Список ві агальна інформан Реквізити ЦСК Час формування Час наступного ф РН Центифікатор від писок відкликани 0EB1A8661085F7 0EB1A8661085F7 | Ри артифікатів дкликаних ція: формування критого клю ок сертифікаті СD030000002 СD030000002 | ССРНОК 5.9 Сертифікатів О=Публічне акціонерне 15.03.2021 17:52:51 22.03.2021 17:57:51 39BD 8E B1 A8 66 10 85 F7 CE . 17.04.2020 17:24:56 . 22.01.2021 21:00:00 | товариство к 0 2E 37 D6 4D (даниется у село Блокування Не визначена | |
| сок відкликаних се Список ві агальна інформан Реквізити ЦСК Час формування Час наступного ф РН Центифікатор від Писок відкликани ОЕВ 1А8661085F7 0EB 1A8661085F7 | Ри артифікатів дкликаних ція: формування критого клю ок сертифікаті СD030000002 СD030000002 | ССРНОК 5.9 Сертифікатів О=Публічне акціонерне 15.03.2021 17:52:51 22.03.2021 17:57:51 39BD 8E B1 A8 66 10 85 F7 CE . 17.04.2020 17:24:56 . 22.01.2021 21:00:00 . 17.04.2020 17:24:59 | товариство к 0 2E 37 D6 4D (да | |
| сок відкликаних се Список ві агальна інформан Реквізити ЦСК Час формування Час наступного ф РН Центифікатор від писок відкликани ОЕВ1А8661085F7 0ЕВ1А8661085F7 0ЕВ1А8661085F7 | Ри артифікатів дкликаних ція: формування критого клю ос сертифікаті СО030000002 СО030000002 СО030000002 | ССРНОК 5.9 Сертифікатів О=Публічне акціонерне 15.03.2021 17:52:51 22.03.2021 17:57:51 39BD 8E B1 A8 66 10 85 F7 CE 17.04.2020 17:24:56 22.01.2021 21:00:00 17.04.2020 17:24:59 22.01.2021 21:00:00 | товариство к 0 2E 37 D6 4D (да | |
| сок відкликаних се Список ві агальна інформан Реквізити ЦСК Час формування Час наступного ф РН Центифікатор від ОЕВ 1А8661085F7 0ЕВ 1А8661085F7 0ЕВ 1А8661085F7 0ЕВ 1А8661085F7 | Ри артифікатів дкликаних ція: формування критого клю с сертифікаті С D030000002 С D030000002 С D030000002 С D030000002 С D030000002 С D030000002 С D0300000002 | ССРНОК 5.9 Сертифікатів 0=Публічне акціонерне 15.03.2021 17:52:51 22.03.2021 17:57:51 39BD 8E B1 A8 66 10 85 F7 CE 17.04.2020 17:24:56 22.01.2021 21:00:00 17.04.2020 17:24:59 22.01.2021 21:00:00 16.11.2018 10:04:14 | товариство к 2 2E 37 D6 4D Э 2E 37 D6 4D Блокування Не визначена Блокування Не визначена Блокування | |
| сок відкликаних се Список ві агальна інформаі Реквізити ЦСК Час формування Час наступного ф РН Ідентифікатор від ОЕВ1А8661085F7 0ЕВ1А8661085F7 0ЕВ1А8661085F7 0ЕВ1А8661085F7 0ЕВ1А8661085F7 | Ри артифікатів дкликаних дкликаних ція: формування критого клю ссертифікаті СD030000002 CD030000002 CD030000002 CD030000002 CD030000003 CD030000003 | ССРНОК 5.9 Сертифікатів 0=Публічне акціонерне 15.03.2021 17:52:51 22.03.2021 17:57:51 39BD 8E B1 A8 66 10 85 F7 CD 17.04.2020 17:24:56 22.01.2021 21:00:00 17.04.2020 17:24:59 22.01.2021 21:00:00 16.11.2018 10:04:14 22.01.2021 21:00:00 | товариство к 2 2 2 37 D6 4D Блокування Не визначена Блокування Не визначена Блокування Не визначена Блокування Не визначена | |
| сок відкликаних се Список ві агальна інформан Реквізити ЦСК Час формування Час наступного ф РН Ідентифікатор від ОЕВ1А8661085F7 0ЕВ1А8661085F7 0ЕВ1А8661085F7 0ЕВ1А8661085F7 0ЕВ1А8661085F7 | Ри артифікатів дкликаних ція: рормування критого клю с сертифікаті (CD030000002 (CD030000002 (CD0300000002 (CD0300000003 (CD0300000003 | ССРНОК 5.9 Сертифікатів О=Публічне акціонерне 15.03.2021 17:52:51 22.03.2021 17:57:51 39BD 8E B1 A8 66 10 85 F7 CE . 17.04.2020 17:24:56 . 22.01.2021 21:00:00 . 16.11.2018 10:04:14 . 22.01.2021 21:00:00 | товариство к 2 2E 37 D6 4D Блокування Не визначена Блокування Не визначена Блокування Не визначена | |
| сок відкликаних се Список від агальна інформан Реквізити ЦСК Час формування Час наступного ф РН Ідентифікатор від тисок відкликани ОЕВ 1А8661085F7 ОЕВ 1А8661085F7 ОЕВ 1А8661085F7 ОЕВ 1А8661085F7 ВІА8661085F7 | Ри артифікатів дкликаних ція: рормування критого клю с сертифікатії СD030000002 (CD030000002 (CD0300000002 (CD0300000003 (CD0300000003 | СУНОК 5.9 Сертифікатів О=Публічне акціонерне 15.03.2021 17:52:51 22.03.2021 17:57:51 39BD 8E B1 A8 66 10 85 F7 CI 17.04.2020 17:24:56 22.01.2021 21:00:00 17.04.2020 17:24:59 22.01.2021 21:00:00 16.11.2018 10:04:14 22.01.2021 21:00:00 | товариство к 2 Е 37 D6 4D Блокування Не визначена Блокування Не визначена Блокування Не визначена Блокування Не визначена | |

 \times

Рисунок 5.10

5.5 Завантаження СВС

Автоматичне завантаження списку відкликаних сертифікатів з web-сервера ЦСК в оффлайн-режимі необхідно відключати, знявши відповідну позначку ("Завантажувати автоматично") у вікні параметрів, що наведене на рис. 4.2.

В онлайн-режимі СВС завантажуються автоматично.

6. УПРАВЛІННЯ КЛЮЧАМИ

6.1 Генерація ключів

1. На робочому столі необхідно знайти значок «Користувач ЦСК ПРАВЕКС БАНК» (Рис. 6.1):





2. Після запуску програми необхідно обрати підпункт "Згенерувати ключі" (Рис. 6.2).

| 🔟 Кори | стувач ЦСК ПРАВЕКС БАНК | - | | × |
|--------------|---|---|---|---|
| ि ∏] Цент | РАВЕКС БАНК р сертифікації ключів | | | |
| ≡ | | | | |
| | Підписати файли Підпис файлів на особистому ключеві | | | |
| | Зашифрувати файли Зашифрувания файлів на одного чи декількох користувачів Розшифрувания зашифрованих файлів | | | |
| | Переглянути сертифікати Перегляд сертифікатів у файловому сховищі | | | |
| | Встановити параметри Встановлення параметрів роботи користувача Згенерувати ключів із запитами на формування сертифікатів | > | | |
| | | | - | |
| | Поо програму Переглянути власний сертифікат Перейти до web-сайту ЦСК Зтерти з пам'яті програми | | | |
| | | | | |
| | Рис. 6.2 | | | |

3. На сторінці майстра (Рис. 6.3), що відкрилась, необхідно вибрати пункт «для державних алгоритмів і протоколів» і натиснути "Далі".

| Генерація ключів | × |
|---|---|
| | |
| Генераци клонь | |
| Генерувати ключі | |
| Для державних алгоритмів і протоколів | |
| О для міжнародних алгоритмів і протоколів | |
| Одля державних та міжнародних алгоритмів і протоколів | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| Далі > Відміна | |
| Рис 63 | _ |

4. На другій сторінці майстра за необхідністю можна вказати тип криптографічних алгоритмів та протоколів, та місце розміщення файлів з параметрами обраних криптографічних алгоритмів та протоколів.

| енерація ключів | | \times |
|--------------------------------|--|----------|
| | | |
| Тип криптографічних алгор | итмів та протоколів: | |
| ДСТУ 4145-2002 та Дифф | i-Гелман в гр. точок ЕК 🛛 🗸 🗸 | |
| 🗹 Використовувати окрем | ий ключ для протоколу розподілу | |
| Ключі ЕЦП: | Ключі протоколу розподілу: | |
| з файлу параметрів | ✓ з файлу параметрів ✓ | |
| Місце розміщення парамет | прів (каталог, з'ємний чи оптичний диск): | |
| C:\Program Files (x86)\Institu | te of Informational Technologies\Certifica 🗸 Змінити | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | < Назад Далі > Відміна | |
| | D C A | |

Рис. 6.4

Для переходу до наступної сторінки необхідно натиснути кнопку "Далі".

5. На наступній сторінці майстра (Рис. 6.5) необхідно вказати тип носія -- як приклад, вказано токен Aladdin eToken Pro.

Пароль доступу до носія та захисту особистого ключа рекомендовано повинен відповідати наступним вимогам:

- довжина не менше 8 символів;
- не повинен містити однакові символи;

- не повинен містити підряд більше ніж 2 символи з розкладинки клавіатури;
- дозволені символи 'a-z', 'A-Z', '0-9', '+', '-'.

| гнучкий диск | А Информація про носій |
|--|--|
| з'ємний диск | |
| оптичний диск | Iип: е.ключ Aladdin e loker PRO (PKCS#11) |
| 🗭 е.ключ Aladdin e Token R2 | Pho (PRC3#11) |
| 🖉 е.ключ Aladdin e Token PRO | Hassa: 47e4ae14 |
| 🕐 е.ключ Aladdin e Token PRO (PKCS#11) | |
| 47e4ae14 | Перезаписуємий, потребує |
| смарт-карта BIFIT Integra 1.0 | автентифікації, електронний |
| 🗭 е.ключ BIFIT iToken | ключ |
| 🥙 е.ключ IIT Алмаз-1К | |
| 🗭 е.ключ IIT Алмаз-1К (носій) | |
| 🗭 е.ключ IIT Алмаз-1К (через ВТ-адаптер) | |
| 🗭 е.ключ IIT Кристал-1 | |
| 🕫 е.ключ IIT Кристал-1 (носій) | |
| закордонний біометричний паспорт (ел. паспорт | (тс |
| у файлова система (каталоги системи) | |
| у файлова система (каталоги користувача) | |
| ID-карта громадянина (БЕН) | Поновити |
| р криптомод. IIT Гряда-301 | Ключ у файлі (на диску) |
| | 284 |
| ароль: | EN . |
| | |

6. Після введення паролю для запису особистого ключа необхідно натиснути кнопку «Записати».

Якщо на носії вже знаходиться попередньо отриманий електронний ключ, то з'явиться вікно (Рис. 6.6), в якому необхідно натиснути «Да».



Рис. 6.6

7. На наступній сторінці майстра (Рис. 6.7) буде відображено два запити на формування сертифікату.

| Запит на формування сертифіката з відкритим ключем ЕЦП 🛛 🗙 | Запит на формування сертифіката з відкритим ключем протоколу розподілу 🛛 🗙 |
|--|--|
| 🖳 Запит на формування сертифіката | и Запит на формування сертифіката |
| Поля запиту: ☐ Реквізити заявника відсутні ☐ Додаткові дані відсутні ☐ Додаткові дані відсутні ☐ Строк чинності сертифіката ві ☐ Параметри відкритого ключа Тип ключа ДСТУ 4145-2002 Довжина ключа ДСТУ 4145-2002 Довжина ключа ДСТУ 4145-2002 Довжина ключа АР 77.84 80 CE 33 86 80 8F 92 F0 2D Цантифікатор відкритого ключа С5 69 EA 06 11 F9 A5 7E C9 C2 F2 31 ☐ Уточнене призначення ключів ☐ Залит самопідписаний | Поля запиту: Поля заявника відсутні Додаткові дані відсутні По заявника — Не вказаний Строк чинності сертифіката ві Строк ції особистого ключа ві Параметри відкритого ключа Довжина ключа ДСТУ 4145-2002 Довжина ключа 432 біт(а) Відкритий ключ FA 5C F1 A3 78 C2 78 62 3C 64 4F B5 8 Ідентифікатор відкритого ключа б4 47 CE 91 81 02 67 B6 E5 6F 10 49 7 Уточнене призначення ключів Запит самопідлисаний |
| ОК | • Друкувати ОК |

8. На наступній сторінці майстра (Рис. 6.8) необхідно поставити позначку на «Зберегти у файл» та натиснути «Далі».

| Генерація ключів | | > |
|-------------------------|-------------------------|--------------|
| | | |
| Эберегти у файл | | |
| 🔘 Відправити засобами е | лектронної пошти до ЦСК | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | < Назад Далі > | Відміна |
| | | Crage in rea |

Рис. 6.8

9. На наступній сторінці майстра (Рис. 6.9) створюються два файли запиту на сертифікацію. Це файли, які згодом потрібно відправити в центр сертифікації.

| нерація ключів | | | > |
|-------------------------------------|-------------------|--------|-----------|
| | | | |
| | | | |
| Ім'я файлу для запису запиту з відн | критим ключем ЕЦ | Π: | |
| C:\CACertificates\EU-B253D235.p10 |) | | Змінити |
| | | | |
| Ім'я файлу для запису запиту з від | критим ключем RS. | A: | |
| C:\CACertificates\EU-RSA-521C090 | 0.p10 | | Змінити |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | (Haaaa | | Distaires |
| | < пазад | далі > | ыдміна |
| | < Назад | Далі > | Відміна |

Рис. 6.9

10. Після виконання всіх дій майстер завершує свою роботу (Рис. 6.10).

| Генерація ключів | \times |
|------------------|----------|
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| 3a | вершити |

Рис. 6.10

Необхідно натиснути «Завершити».

- 11. Запити на формування сертифікатів сформовано, програму «Користувач ЦСК ПРАВЕКС БАНК» необхідно закрити.
- Сформовані (згідно пункту 9) два файли запиту, що знаходяться у папці C:\CACertificates, з розширенням
 *.p10, необхідно засобами електронної пошти відправити адміністратору сертифікації (адреса вказана на офіційному сайті ЦСК у розділі «Контакти» -- https://ca.pravex.com.ua/contacts).
- 13. Після отримання письмової відповіді від адміністратора сертифікації, необхідно виконати наступний розділ даної інструкції (встановити сертифікати).

6.2 Встановлення сертифікатів особистого ключа ЕЦП

1. Сертифікати власного ключа ЕЦП встановлюються (копіюються в папку C:\CACertificates) на кожну робочу станцію, де буде працювати користувач і використовувати в своїй роботі ЕЦП.

2. Зазначена нижче процедура виконується на кожній робочій станції у повному обсязі один раз після проведення генерації особистого ключа ЕЦП користувача до наступного сеансу зміни особистого ключа ЕЦП.

3. Процедура проводиться особисто користувачем, якому був виданий особистий ключ ЕЦП.

4. На робочому столі своєї робочої станції знайти ярлик програми «Користувач ЦСК ПРАВЕКС БАНК» (Рис. 6.11):



Рис. 6.11

5. Після запуску програми відкриється вікно, що зображене на Рис. 6.12



Рис. 6.12

6. У цьому вікні необхідно у меню обрати пункт «Сертифікати та CBC», далі з випадаючого меню обрати пункт «Отримати з ЦСК» (Рис. 6.13).

| Користувач ЦСК ПРАВЕКС БАНК ПРАВЕКС БАНК Центр сертифікації кл | ючів | | - | | × |
|--|---|--|--------------|---|---|
| Файли > Текст > Особистий ключ > | и собистому Герее файла | в ірити файли ірка підпису на підп х | исаних | | |
| Сертифікати та СВС 🔷 🔶 | Переглянути сертифікати | F10 айли | | | |
| Параметри > | Переглянути СВС | F11 nis | | | |
| Допомога > | Отримати з ЦСК | | | | |
| Перетляд сертиф файловому схови Встановлити пај Встановлення пар користувача Про програму Перейти до web-сайт | Заблокувати власні сертифікати Скасувати власні сертифікати аметрів роботи 🖋 Генер форму • <u>Эчитати</u> | иловон заця ключів із запит вання сертифікатів | му ами на | _ | |

Рис. 6.13

7. У вікні «Повідомлення оператору» (Рис. 6.14) натиснути «Да».

Повідомлення оператору

Отримати набір сертифікатів за особистим ключем чи власним сертифікатом з ЦСК? Да Нет \times

Рис. 6.14

8. Після цього з'являється вікно, що зображене на Рис. 6.15.



Рис. 6.15

Необхідно вказати тип носія, та у вікні «Пароль» ввести пароль носія.
 Після введення паролю для запису особистого ключа необхідно натиснути кнопку «Зчитати».
 У вікні «Завантажені сертифікати» (Рис. 6.22) натисніть «Да».

| Завантажені з СМР-сервера ЦСК сертифікати: |
|--|
| СМР-сервер ЦЕНТР СЕРТИФІКАЦІЇ КЛЮЧІВ ПАТКБ |
| СМР-сервер ЦЕНТР СЕРТИФІКАЦІЇ КЛЮЧІВ ПАТКБ |
| "ПРАВЕКС-БАНК" |
| ТЅР-сервер ЦЕНТР СЕРТИФІКАЦІЇ КЛЮЧІВ ПАТКБ |
| |
| "ПРАВЕКС-БАНК" |
| ЦЕНТР СЕРТИФІКАЦІЇ КЛЮЧІВ ПАТКБ "ПРАВЕКС-БАНК" |
| Імпортувати їх у файлове сховище сертифікатів? |
| |

Рис. 6.22

15. Процедура встановлення сертифікатів особистого ключа ЕЦП на робочій станції завершена, програму «Користувач ЦСК ПРАВЕКС БАНК» необхідно закрити.

6.3 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" або шляхом натискання комбінації клавіш Ctrl+K.

У вікні, що з'явиться (рис. 6.7) необхідно вказати:

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

| | T |
|---|-----------------------------|
| | PRO (PKCS#11) |
| | 110 (1103#11) |
| | Назва: 47е4ае14 |
| | |
| | Перезаписуємий, потребує |
| | автентифікації, електронний |
| | ключ |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | • • |
| | С Поновити |
| ~ | Ключ у файлі (на диску)… |
| | |
| | |
| | > |

Рисунок 6.7

Після введення параметрів необхідно натиснути кнопку "Зчитати".

Інформація про те, що особистий ключ зчитаний та знаходиться в пам'яті ПЕОМ відображається до панелі стану вікна, як наведено на рисунку 6.8.



6.4 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 6.9. Під час резервного копіювання пароль захисту особистого ключа не вказується, та змінити його не можливо.

| Зчитування особистого ключа | X |
|--|---|
| 🤻 Встановіть носій ключової інформ криптографічний модуль та вкажі | нації чи підключіть іть параметри |
| 📇 гнучкий диск | 📇 Інформація про носій: |
| 🚑 А:\ 🚑 з'ємний диск | Тип: гнучкий диск |
| e ключ Aladdin eToken B2 | Назва: А:\ |
| еключ Aladdin eToken PR0 еключ Aladdin eToken PR0 еключ Aladdin eToken PR0 еключ IIT Грядь61 еключ IIT Кристал-1 еключ IIT Кристал-2 еключ IIT Кристал-2 | Перезалисуємий, не потребує автентифікації |
| 📹 е.ключ Технотрейд uaToken | 🜍 Поновити |
| Пароль: | EN |
| | Зчитати Відміна |

Рисунок 6.9

Після зчитування особистий ключ записується до резервного носія за допомогою вікна що наведене на рисунку 6.10.

| Запис особистого ключа | × |
|--|--|
| Встановіть носій ключової інформації криптографічний модуль та вкажіть па | чи підключіть араметри |
| 📇 гнучкий диск | 🔠 Інформація про носій: |
| 🚑 А.\ 🚑 з'ємний диск | Тип: гнучкий диск |
| e к доу Aladdin eToken B2 | Назва: А:\ |
| е.ключ Aladdin eToken PR0 е.ключ Aladdin eToken PR0 (PKCS) криттомод. IIT Града-61 е.ключ IIT Кристал-1 е.ключ IIT Кристал-1 (носій) е.ключ IIT Калина-1ЕК криттомод. IIT Града-301 е.ключ ICL Almaz S е.ключ Технотрейд uaToken | Перезаписуємий, не потребує автентифікації |
| Пароль: | N. Contraction of the second sec |
| 🕦 Допомога | Записати Відміна |

Рисунок 6.10

6.5 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 ключанаведене на рис. 6.11. У вікні необхідно вказати:

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

Після введення параметрів необхідно натиснути кнопку "Виконати".

| Зміна пароля доступу | X |
|--|-----------------------------|
| Встановіть носій ключової інформації ч криптографічний модуль та вкажіть па | ии підключіть раметри |
| 📇 гнучкий диск | 📇 Інформація про носій: |
| A:\ | T |
| 🚑 з'ємний диск | тип: гнучкии диск |
| 👝 оптичний диск | |
| 🖙 е.ключ Aladdin eToken R2 | Назва: А:\ |
| 🖙 е.ключ Aladdin eToken PRO | Перезаписуємий, не потребує |
| 📹 е.ключ Aladdin eToken PHU (PKCS) | автентифікаці |
| 🔤 криптомод. III Гряда-61 | |
| е.ключи п кристал-и кана с кана III Кристал-и (чесій) | |
| еключит кристалят (носи) | |
| | |
| 🛲 е к оку СС Аlmaz S | |
| 🚛 е.ключ Технотрейд uaToken | |
| · · · · | 🕑 Поновити |
| Пароль: •••••• | l |
| Новий пароль: | |
| Повтор паролю: | |
| 🕦 Допомога | Виконати Відміна |

Рисунок 6.11

6 ЗАХИСТ ФАЙЛІВ

7.1 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", або натиснути клавішу F5. Якщо особистий ключ ще не було зчитано, відбувається його зчитування відповідно до п. 6.2.

Вікно підпису файлів наведене на рис. 7.1. Вікно містить такі 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.

| 🔟 Користувач ЦСК ПРАВЕКС БАНК | | | | _ | | × |
|---|-------------------|----------------------|--------------------|-------------|-------|------|
| Підпис файлів | | | | | | |
| Вкажіть файли, які необхідно підписати | та зазначте для к | ожного порядок за | апису підпису | | | |
| Ім'я файлу | | ЕЦП | Стан | Алгоритм пі | дпису | Фор |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| < | | | | | | > |
| Підлис у зовнішньому файлі (*.*.p7s) | Алгоритм ЕЦП: | ДСТУ 4145 🔍 | | Додати | Видал | ити |
| Додати сертифікат | Формат ЕЦП: | базовий | | \sim | | |
| 葿 Вкажіть (за необхідністю) каталог для з | апису підписаних | файлів чи файлів з | підписом (*.*.p7s) | | | |
| Використовувати окремий каталог д | иля підписаних фа | йлів чи файлів з під | лисом | | | |
| | | | | | Змін | ити |
| Для підпису файлів натисніть кнопку "П | ідлисати" | | | Відміна | Підпи | сати |
| - | | | | | | |

Рисунок 7.1

Після встановлення значень параметрів вікно може мати вигляд як наведено на рис. 7.2.

| Користувач ЦСК ПРАВЕКС БАНК | | | | - | | > |
|--|---|---|-----------------------------|------------|---------------|------------------|
| Підлис файлів | | | | | | |
| Вкажіть файли, які необхідно підписат | и та зазначте для ко: | жного порядок заг | пису підпису | | | |
| Ім'я файлу | | ЕЦП | Стан | Алгоритм п | ідпису | Фо |
| D:\Users\e2008006\Documents\E | JRegistration.txt | Внутрішній | Не підписаний | ДСТУ 4145 | j | баз |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| ٢ | | | | | | |
| < Підлис у зовнішньому файлі (*.*.р.7s |) Алгоритм ЕЦП: | дсту 4145 🗸 | | Додати | Видал | пити |
| Підлис у зовнішньому файлі (*.*.р7sДодати сертифікат |) Алгоритм ЕЦП: Формат ЕЦП: | ДСТУ 4145 — V базовий | (| Додати | Видал | : |
| Підпис у зовнішньому файлі (*.*, р7s Додати сертифікат |) Алгоритм ЕЦП: Формат ЕЦП: запису гіописаних п | ДСТУ 4145 — базовий айлів чи файлів в Г | ілписом (** o.7s) | Додати | Видал | пити |
| Підлис у зовнішньому файлі (*.*.р7в Додати сертифікат Вкажіть (за необхідністю) каталог для | Элгорити ЕЦП: Формат ЕЦП: запису підписаних фай | ДСТУ 4145 ∨ базовий айлів чи файлів з пілг | і́дписом (*.*.р7s) | Додати | Видал | анти |
| Підпис у зовнішньому файлі (*.*.р7s Додати сертифікат Вкажіть (за необхідністю) каталог для Використовувати окремий каталог |) Алгоритм ЕЦП: Формат ЕЦП: запису підписаних ф для підписаних файл | ДСТУ 4145 — базовий айлів чи файлів з г тів чи файлів з підг | ідлисом (*.*,р7s) іисом | Додати | Видал | |
| Підпис у зовнішньому файлі (*.*.р.7s Додати сертифікат Вкажіть (за необхідністю) каталог для Використовувати окремий каталог |) Алгоритм ЕЦП: Формат ЕЦП: запису підписаних ф для підписаних файл | ДСТУ 4145 | підписом (*,*,р7s) Ійсом | Додати | Видал Змін | : лити ити |

Рисунок 7.2

Для підпису файлів необхідно натиснути кнопку "Підписати".

Після здійснення підпису файлів вікно буде містити інформацію про результати підпису.

7.2 Перевірка підпису 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", або натиснутиклавішу F6.

Вікно перевірки файлів наведене на рис. 7.4. 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.

| 🔟 Користувач ЦСК ПРАВЕКС БАНК | | _ | |
|--|----------------|---------|------------|
| Перевірка підписаних файлів | | | |
| Вкажіть файли, які необхідно перевірити | | | |
| ім'я файлу | Стан | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | Додати | Видалити |
| 🖀 Вкажіть (за необхідністю) каталог для запису о | файлів без ЕЦП | | |
| Використовувати окремий каталог | | | |
| | | | Змінити |
| Для перевірки файлів натисніть кнопку "Перек | вірити" | Відміна | Перевірити |

Рисунок 7.4

Після встановлення значень параметрів вікно може мати вигляд як наведено на рис. 7.5.

| 🔟 Користувач ЦСК ПРАВЕКС БАНК | - 🗆 X |
|--|--|
| Перевірка підписаних файлів | |
| ист В Вкажіть файли, які необхідно перевірити | |
| Iм'я файлу Стан ₩D:\Users\e2008006\Documents\container.p7s Підпис не пер | реврений |
| Вкажіть (за необхідністю) каталог для запису файлів без ЕЦП Використовувати окремий каталог Для перевірки файлів натисніть кнопку "Перевірити" | Додати Видалити Змінити Відчіна Перевірити |

Рисунок 7.5

Для перевірки файлів необхідно натиснути кнопку "Перевірити".

Якщо під час перевірки виникає помилка:

| Пошук та визначення статусу | сертифіката | | | × |
|---|-----------------------------------|---|--|--|
| Сертифікат мо | ожливо не й. Викори | е чинн истати | ий або йог його? | то стат у с |
| Сертифікат | | | Так | Hi |
| Результати пошуку та ви | значення с | татусу: | | |
| Пошук чи перевірка серт через OCSP-сервер з DN IP-адресою http://czo.gov.ua/services | ифіката IS-ім'ям чи s/ocsp/ | Сертиф скасова виникла перевір | ікат ОСЅР-серв аний чи заблоко а помилка при й ці у файловому | ера ований або його пошуку та сховищі |
| Перевірка сертифіката у сховищі | файловому | Один з знайден | сертифікатів у л но | панцюжку не |
| Інформація про сертифік | ат: | | | |
| 📰 Власник | TSP-сервер | АЦСК ор | ганів юстиції Ун | країни |
| E LICK | Центральни | й засвідч | увальний орган | 1 |
| РН сертифіката відкр. ключа ЕЦП | 3DB73E7BF | 0D575B20 | 0200000001000 | 000AE000000 |

Це може означати, що у файловому сховищі відсутні необхідні сертифікати (підписувача, центру сертифікації або серверів центру сертифікації – зазвичай їх можна завантажити с офіційного сайту відповідного центру сертифікації) або відсутній мережевий доступ до веб-сайту центру сертифікації.

Після здійснення перевірки файлів вікно буде містити інформацію про результати підпису (рис. 7.6)

В разі вдалої перевірки можна також переглянути інформацію про підписаний файл (для цього необхідно натиснути на відповідний запис про файл). Вікно наведене на рис. 7.7.



Рисунок 7.6

| Підписувач | test1 |
|------------------------------|--|
| Організація та підрозділ: | AT ПРАВЕКС БАНК test |
| Посада: | test 1 |
| Сертифікат | |
| LICK: | ЦЕНТР СЕРТИФІКАЦІЇ КЛЮЧІВ ПАТКБ "ПРАВЕК |
| Реєстраційний номер: | 0EB1A8661085F7CD04000000561B0000FB4A0000 |
| Позначка часу: | 10.12.2020 13:21:51 |

Рисунок 7.7

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.

7.3 Зашифрування файлів

Для зашифрування файлу необхідно натиснути на панелі "Зашифрувати файли" у головному вікні програми, або обрати підпункт "Зашифрувати" у пункті меню "Файли", або натиснути клавішу F7.



Рисунок 7.8

Вікно зашифрування файлів наведене на рис. 7.9. 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.

| IN A CODY | | Підписати | Стан | Сертифікат | |
|-------------------|----------------------------|----------------|-------------------|------------|--------|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | Протокол розподілу ключів: | ДифГелм. в гр. | точок EK $ \sim $ | Додати | Видали |
| Додати сертифікат | | | | | |

Рисунок 7.9

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. Для того, щоб пункт «додатково підписати» став активним, необхідно виділити файл лівою клавішою миші.

Інформативно: Для надання інформації в Банк необхідно обов'язково підписувати файли.

| Documents\test keys\прод 1.3.1\te | Тадлисати Так | Стан Не зашифрований | Не додавати | |
|-------------------------------------|-------------------|-------------------------|-------------|--------|
| JOCUMENTA VESK KEYS VIDUL 1.3. I VE | Tax. | пе зашичровании | пе додавани | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| Протокол розподілу ключів: [| ІифГелм. в гр. то | чок ЕК 🗸 | Додати | Видали |
| Протокол разподілу ключів: 👖 | ифГелм. в гр. то | чок ЕК ~ . | Додати | Видали |
| Протокол розподілу ключів: [| ифГелм. в гр. то | чок ЕК 🗸 | Додати | Видали |
| | | | | |

Рисунок 7.11

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".

Після встановлення значень параметрів, вікно може мати вигляд як наведено на рис. 7.12. Для виконання зашифрування необхідно натиснути кнопку "Зашифрувати".

| Вкажіть файли, які необхі | | зазначте необхід | ність підпису | | |
|--|-----------------------------------|------------------|-----------------|-------------|---------|
| Ім'я файлу | | Підписати | Стан | Сертифікат | |
| D:\Users\e2008006\0 | Documents/test keys/прод 1.3.1/te | Так | Не зашифрований | Не додавати | |
| | | | | | |
| Додатково підписати | Протокол розподілу ключів: | ДифГелм, в гр. | точок ЕК 🗸 🤳 | Додати | Видалит |
| Додатково підписати □ Додати сертифікат | Протокол розподілу ключів: | Диф-Гелм, в гр. | точок ЕК 🗸 🧾 | Додати | Видалит |

Рисунок 7.12

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. 7.13 необхідно обрати користувачів для яких виконується зашифрування файлу. Зашифрований файл може бути відкритим лише користувачем для якого виконувалось зашифрування.

Під час шифрування здійснюється перевірка параметрів ключових даних користувачів що були обрані у списку (рис 7.13). У списку присутні тільки ті користувачі, чиї сертифікати присутні у файловому сховищі, та параметри яких співпадають з параметрами ключа, яким шифруються файли (якщо шифрування ДСТУ, розшифрувати можна тільки ключем ДСТУ).

| Cep | тифікати | | | × |
|-----|--------------------------------------|---------------------------------------|--|---------------|
| (| Сертифікати користу Кількість: 1 | увачів-отр иму вачів | Пошук за влас | ником: |
| E | Власник ▼ ☑ ॡॊ Малишко Антон Тест | LICK QTSP of the "PRAVEX BANK" JSC | Серійний номер 68FABF8C256890310400000CD2900003379000 | Тип) D RSA |
| | мпортувати | | ОК Ві | > ұміна |

Рисунок 7.13

Після здійснення зашифрування файлів буде виведене наступне вікно (рис. 7.14) з інформацією про результати зашифрування.

| cramithh25aunin daning | |
|--------------------------------|------------------------------|
| Результати зашифрування файлів | |
| Ім'я файлу | Ім'я зашифрованого файлу |
| D:\TEST\test.txt | D:\TEST\test.txt.p7e (з ЕЦП) |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| • | |

Рисунок 7.14

Інформативно: В колонці «Ім'я зашифрованого файлу» в дужках повинен обов'язково бути присутній напис «(з ЕЦП)», що свідчить про накладання на файл, що зашифрований, електронного цифрового підпису.

7.4 Розшифрування файлів

Перед розшифруванням файлів необхідно зчитати ключ, сертифікат якого було вказано у списку сертифікатів отримувачів зашифрованого файлу при зашифруванні (див. рис. 7.13).

Для розшифрування файлів необхідно натиснути на панелі "Розшифрувати файли" у головному вікні програми, або пункт меню "Розшифрувати" у розділі меню "Файли", або натиснути клавішу F8. Вікно розшифрування файлів наведене на рис. 7.15. Форма містить такі 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".

| Б | ристувач ЦСК ПРАВЕКС БАНК | | | - | | \times |
|----------|--|------------|------|-------|----------------------|----------|
| | Розшифрування зашифрованих файлів | | | | | |
| 0 | Вкажіть файли, які необхілно розшифоувати | | | | | |
| | | | | | | |
| | Ім'я файлу | Стан | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | Дол | ати | Видали | ти |
| | Вкажіть (за необхідністю) каталог для запису розшифрован | них файлів | | | | |
| - | Використовувати окремий каталог | | | | | |
| | | | | | Змінит | и |
| | | | | | | |
| ۲ | Для розшифрування файлів натисніть кнопку "Розшифрува | "ити | Відм | iна I | ^о озшифру | вати |
| | | | | | | |

Рисунок 7.15

Після встановлення значень параметрів, вікно розшифрування файлів може мати вигляд, як наведено на рис. 7.16.

| 🔟 Користувач ЦСК ПРАВЕКС БАНК | _ | | × |
|---|----------|----------|------|
| Розшифрування зашифрованих файлів | | | |
| ∎∎ Вкажіть файли, які необхідно розшифрувати | | | |
| Iм'я файлу Стан ∰ С∴САСеttificates\CA-0EB1A8661085F7CD0400000CD2 Не розшифрований | | | |
| | | | |
| | | | |
| | Полати | Ruppo | 1714 |
| Вкажіть (за необхідністю) каталог для запису розшифрованих файлів Використовувати окремий каталог | ацида In | Зицали | |
| | | Зміни | ти |
| Для розшифрування файлів натисніть кнопку "Розшифрувати" | Відміна | Розшифру | вати |

Рисунок 7.16

Для розшифрування файлів необхідно натиснути кнопку "Розшифрувати". Після розшифрування буде виведено інформацію про результати розшифрування (рис. 7.17).

В разі вдалого розшифрування є можливість переглянути інформацію про розшифровані файли (рис. 7.18), для чого необхідно натиснути на запис про відповідний файл.

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



Рисунок 7.17

| ифровані дані | : |
|------------------------------|--|
| Зашифрован | і дані |
| Відправник: | Малишко Антон Тест |
| Організація та підрозділ: | Фізична особа Фізична особа |
| Посада: | Фізична особа |
| Сертифікат | |
| LICK: | ЦЕНТР СЕРТИФІКАЦІЇ КЛЮЧІВ ПАТКБ "ПРАВЕКС-БАН |
| Реєстраційний номер: | 0EB1A8661085F7CD04000000CD29000032790000 |
| Час підпису: | Підлис відсутній |
| | |
| | |
| Детальна інформація | OK |

Рисунок 7.18

8 ДОВІДКОВА СИСТЕМА

8.1 Контактні відомості для зв'язку

Телефон, за яким необхідно звертатись в разі виникнення питань по ЦСК вказані на офіційному сайті ЦСК у розділі «Контакти» (<u>https://ca.pravex.com.ua/contacts</u>) або написавши листа на адресу <u>ca@pravex.ua</u>