

Інструкція клієнта щодо аварійного відновлення роботи в СКБ та ключа(ів) ЕЦП (Web клієнт)

Інструкція клієнта щодо аварійного відновлення роботи в СКБ та ключа(ключів) ЕЦП визначає послідовність дій користувача, після отримання аварійних паролів в ПУБЛІЧНОМУ АКЦІОНЕРНОМУ ТОВАРИСТВІ «КРИСТАЛБАНК», далі - Банк, виконання запуску системи, генерації робочих ключів і сертифікатів.

Зміст

1. Налаштування та запуск системи.	1
2. Відновлення роботи в СКБ та ключа(ів) ЕЦП.	4
2.1. Створення та відправка запиту на новий сертифікат та ключі.....	4
2.2. Прийом і запис нових сертифікатів та ключів.....	8

1. Налаштування та запуск системи

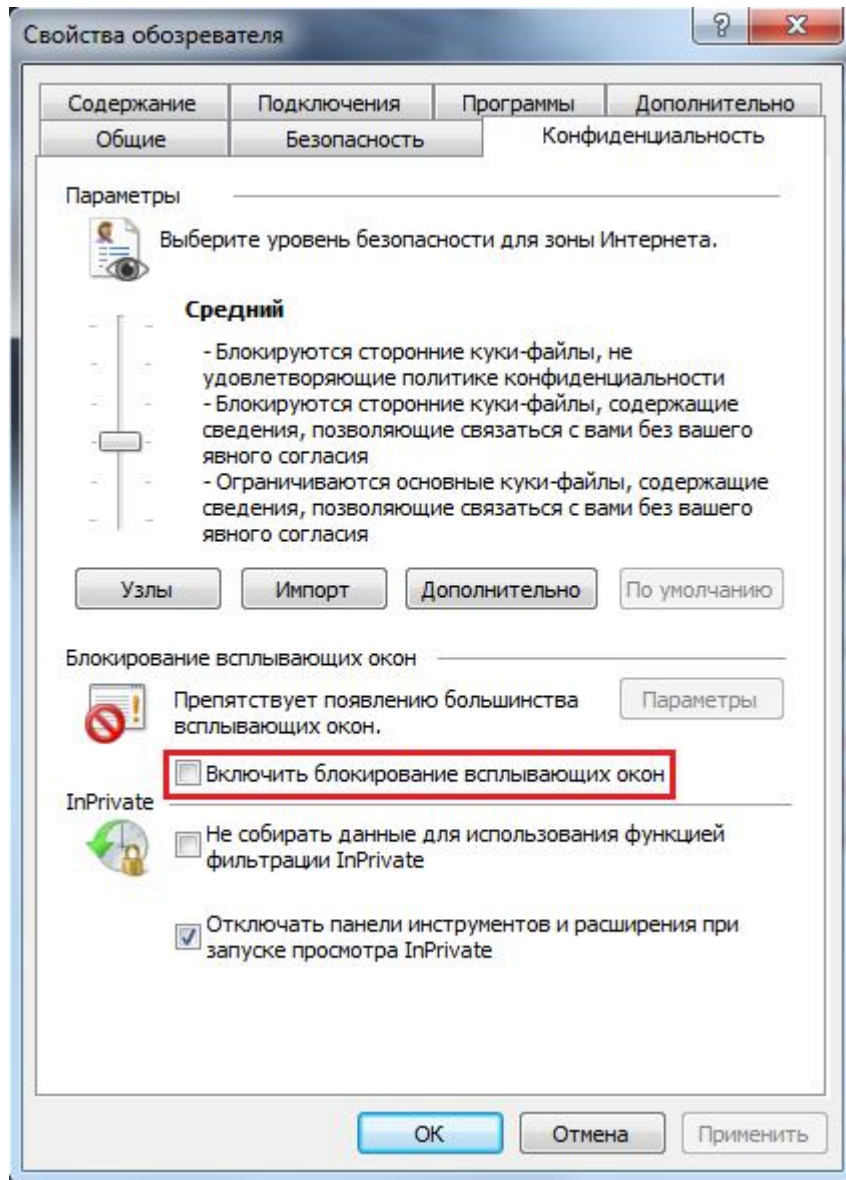
1.1. Вимоги до програмного забезпечення системи «Клієнт-банк» (Web-клієнт) на робочому місці користувача:

Операційна система	Інше ПЗ
Win2003/Vista/7	Microsoft Internet Explorer 9.0 + JRE 1.7 +

При використанні інших параметрів Банк не гарантує коректної роботи системи «Клієнт-банк».

1.2. Перед початком роботи в системі «Клієнт-банк» в браузері Internet Explorer необхідно відключити блокування спливаючих вікон. Для цього зробить наступне:

Відкрийте браузер Internet Explorer. Оберіть пункт меню «Сервіс (Сервис)»/«Властивості оглядача (Свойства обозревателя)». На закладці «Конфіденційність (Конфиденциальность)», необхідно зняти відмітку «Включити блокування спливаючих вікон (Включить блокирование всплывающих окон)», Мал. 1.



Мал.1

Натисніть кнопку «**ОК**».

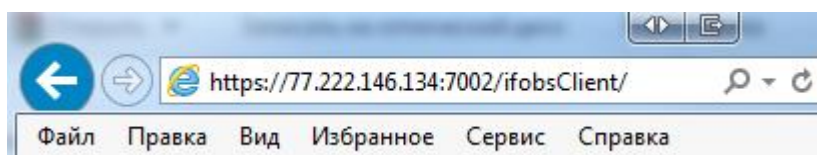
1.3. Вставте в комп'ютер зовнішній носій інформації, на якому будуть зберігатися файли ключів **(не зберігайте ключі на жорсткому диску, що є порушенням інформаційної безпеки та збереження засобів захисту інформації)**;

1.4. На зовнішньому носії інформації створіть теку, де будуть зберігатися файли ключів, наприклад: G:\Key\

Увага! Тека, в якій будуть зберігатись файли ключів, перед проведенням процедури відновлення має бути порожня.

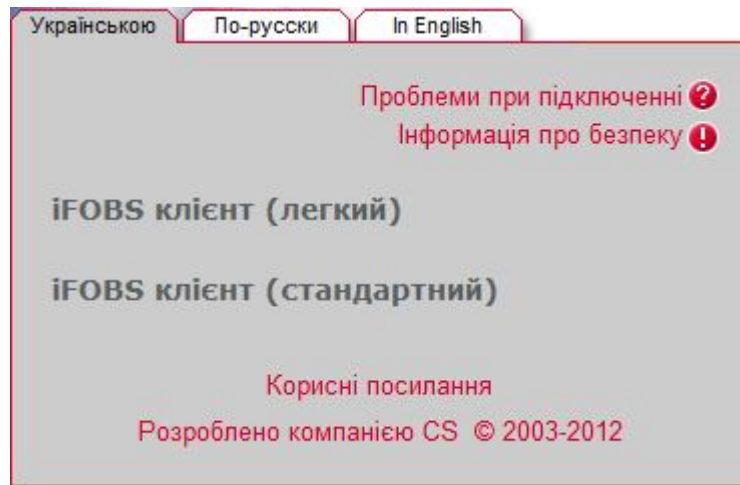
1.5. Перейдіть за посиланням, мал.2:

<https://77.222.146.134:7002/ifobsClient/>



Мал.2

1.6. Стартова сторінка виглядає наступним чином, оберіть пункт «**iFobs клієнт (стандартний)**».
мал 3:



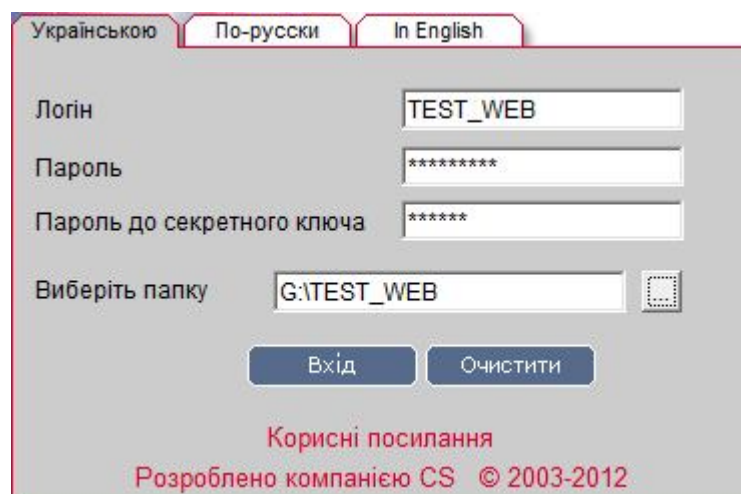
Мал.3

1.7. Якщо при цьому на екрані з'явиться повідомлення, мал. 4. Необхідно встановити відмітку на пункті «**Always trust content from this publisher**» та натиснути кнопку «**Yes**» чи «**Run**».



Мал.4

1.8. Заповніть екранну форму «**Реєстрація**», Мал.5:



Мал.5. Екранна форма «**Реєстрація**».

Якщо екранна форма «Реєстрація» не з'явилась (не відображуються поля для вводу логіна і паролей) значить на Вашому комп'ютері не встановлено (або встановлена застаріла версія) Java - [Java Runtime Environment \(JRE\)](#).

Увага! При введенні Логіну та паролів має бути встановлена англійська розкладка клавіатури і вимкнена клавіша "Caps Lock".

Введіть своє ім'я користувача в полі «Логін» (див. файл «RECOVERY.TXT»);

Введіть свій пароль на вхід в систему в полі «Пароль» (див. файл «RECOVERY.TXT»);

Введіть в полі «Пароль до секретного ключа» будь-яку послідовність символів (дані цього поля використані не будуть, необхідно наявність мінімум одного символу);

Вкажіть шлях до секретного ключа в полі «Виберіть папку». При необхідності змініть шлях до зовнішнього носія інформації, вказавши шлях вручну або за допомогою кнопки «...» для вибору зовнішнього пристрою, наприклад: G:\Key\.

Натисніть кнопку «Вхід».

2. Відновлення роботи в СКБ та ключа(ів) ЕЦП

2.1. Створення та відправка запиту на новий сертифікат та ключі

2.1.1. При наявності Аварійних паролів ви маєте змогу увійти в систему. Однак для подальшої роботи із системою вам необхідно буде відправити запит у Банк на одержання Робочих Ключів та Сертифікатів. Здійснивши вхід в систему на екрані з'явиться наступне вікно, мал. 6:

Аварійне відновлення ключів

Для поточного користувача було призначено аварійний пароль!

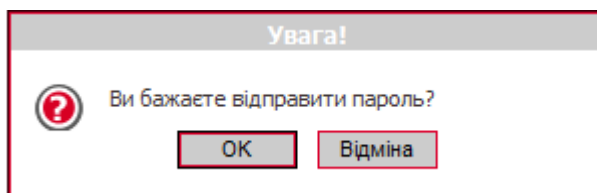
Подальша робота у звичайному режимі забороняється.

Будь ласка, зверніться до адміністратора системи.

Введіть аварійний пароль

Мал. 6.

2.1.2. Введіть **Аварійний пароль** в поле «Введіть аварійний пароль» (див. файл «RECOVERY.TXT»). Натисніть кнопку «Відправити», на екрані буде отримано повідомлення, мал. 7:



Увага!
Ви бажаєте відправити пароль?

Мал. 7.

2.1.3. Натисніть кнопку «ОК». На екрані з'явиться форма зміни сертифікату, мал. 8:

На поточній формі ви можете згенерувати новий сертифікат, зберегти секретний ключ на диск..

Зміна сертифікату ?

Введіть пароль до секретного ключа

Новий пароль до секретного ключа

Повторіть введення пароля

Ключі будуть збережені в ...

Заповніть параметри сертифіката

Місто

Ел. адреса

Згенеруйте випадкове число, переміщуючи випадковим чином курсор в ділянці нижче

83 %

Натисніть кнопку 'Створити' для створення запиту на сертифікат

Натисніть кнопку 'Відправити' для відправлення запиту на сертифікат в банк

Мал. 8

Заповніть всі поля форми.

Увага! При введенні паролів необхідно дотримуватися правил:

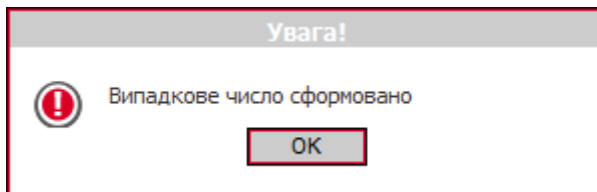
- англійська розкладка клавіатури і вимкнена клавіша "Caps Lock";
- новий пароль повинен бути розміром не менше восьми (8) символів (максимально до 15), формуватися з латинських літер та службових символів (-, %, *, ?, _), цифр;
- не повинен повторювати попередній пароль.
-

Опис полів форми «Зміна сертифіката»

Найменування поля	Вміст поля
Новий пароль до секретного ключа	Вкажіть новий пароль до секретного ключа
Повторіть введення пароля	Повторіть введення нового пароля до секретного ключа
Далі йде ряд інформаційних полів параметрів сертифіката. Інформація буде використана системою для формування запиту на сертифікат.	
Місто	Місто, у якому зареєстрована організація
Електронна адреса	Електронна адреса Вашої організації

ПРИМІТКА. Поля виділені червоним кольором – обов'язкові для заповнення.

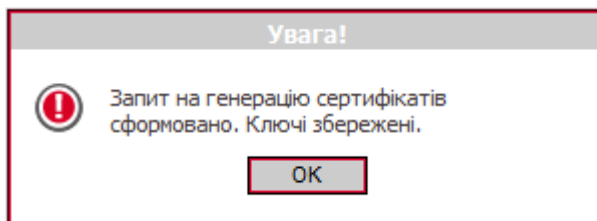
2.1.4. Згенеруйте випадкове число, переміщуючи випадковим чином курсор в затемненій ділянці форми досягнувши 100% виконання. В результаті успішного виконання на екрані буде отримано повідомлення, мал. 9:



Мал. 9

Натисніть кнопку «ОК».

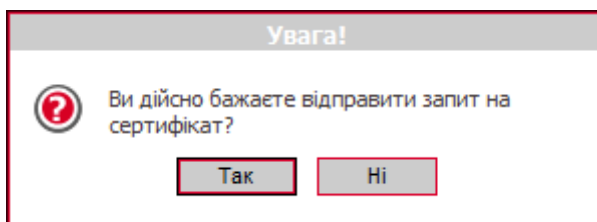
2.1.5. Для генерації запиту на сертифікат натисніть кнопку «Створити», на екрані буде отримано повідомлення, мал. 10:



Мал. 10

Натисніть кнопку «ОК».

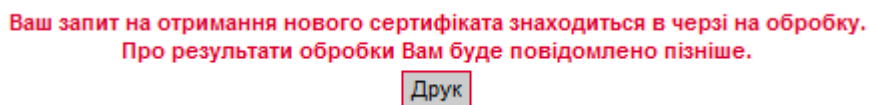
2.1.6. Для відправлення запиту на сертифікат в банк натисніть кнопку «Відправити», на екрані буде отримано повідомлення, мал. 11:



Мал. 11

Натисніть кнопку «Так».

2.1.7. Система відправить у Банк запит на створення Робочого Сертифіката. На екрані буде виведене повідомлення, Мал.12:



Мал. 12

2.1.8. Натисніть кнопку «Друк». На екрані з'явиться наступне вікно, Мал. 13:

Інформація про відкриті ключі користувача (сертифікати)

Користувач: TEST_WEB

П.І.Б.: Test Web

Хеш відкритого ключа RSA

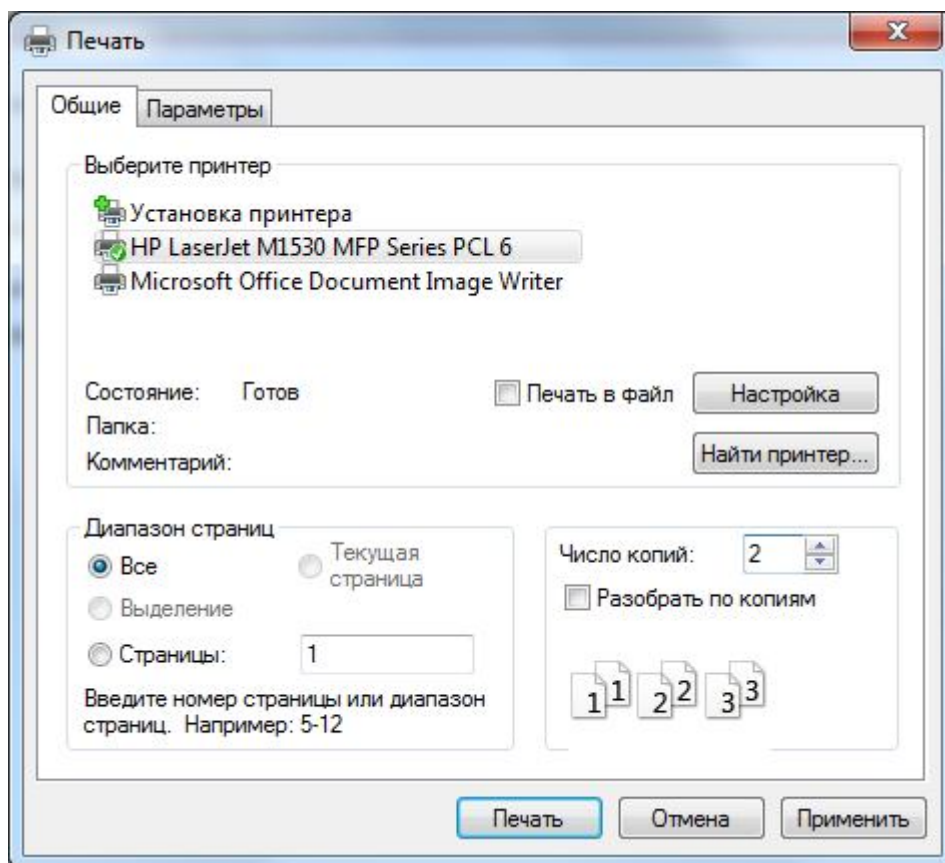
351C 9148 B4BA 4E32 1584 BBE7 06DA 1DBB 0227 2BCB

Друк

Повернутися

Мал. 13

2.1.9. Натисніть кнопку «Друк» та оберіть підключений до вашого ком'ютера принтер, мал.14:



Мал. 14

Роздрукуйте в 2-х примірниках інформацію про відкриті ключі користувача. Після роздрукування натисніть кнопку «Вихід».

2.1.10. Роздруковані примірники необхідно засвідчити підписом та печаткою відповідно до картки із зразками підписів та відбитка печатки, що знаходиться в Банку.

2.1.11. Оформлені паперові носії запиту надаються Клієнтом у відділення Банку, де обслуговується Клієнт. Один примірник з відміткою Банку повертається Клієнту.

Увага! Авторизація Клієнта в системі «Клієнт-Банк» відбувається тільки за умови надання Клієнтом до відділення Банку інформації про відкриті ключі користувача на паперовому носії, завіреному належним чином.

Авторизація нових ключів Клієнта для роботи в системі «Клієнт-Банк» проводиться після звірки поданого запиту (сертифіката ключів).

ПРИМІТКА:

- Якщо Клієнт подав запит у відділення до 14:00 годин, то з 09:00 наступного дня Клієнт може користуватися системою. При вході в СКБ необхідно натиснути кнопку «F5» «Синхронізувати усі дії з Банком»
- Якщо запит до відділення Банку подано після 14:00, то користування системою можливо після 14:00 наступного робочого дня.

2.2. Прийом і запис нових сертифікатів та ключів

2.2.1. Ввійдіть в систему використовуючи форму «Реєстрація» (Мал. 15) з наступними даними:


Мал. 15

Увага !!! При введенні Логіну та паролів має бути встановлена англійська розкладка клавіатури і вимкнена клавіша "Caps Lock".

Введіть Логін користувача в полі «Логін» (див. файл «RECOVERY.TXT»);

Введіть свій пароль на вхід в систему в полі «Пароль» (див. файл «RECOVERY.TXT»);

Введіть в полі «Пароль до секретного ключа» будь-яку послідовність символів (дані цього поля використані не будуть, необхідно наявність мінімум одного символу). Новий пароль, заданий вами при створенні запиту в п.п. 2.1.3, буде введений в дію лише після авторизації користувача і отримання ним нового сертифікату з Банку;

Вкажіть шлях до секретного ключа в полі «Виберіть папку». При необхідності змініть шлях до зовнішнього носія інформації, вказавши шлях вручну або за допомогою кнопки  для вибору зовнішнього пристрою, наприклад: G:\Key\.

Увага !!! Шлях необхідно вибрати той самий що був вказаний Вами при створенні запиту на сертифікат та ключі.

Натисніть кнопку «Вхід».

2.2.2. У випадку якщо Ваш запит на генерацію нового Сертифіката ще не був оброблений Банком, система видає повідомлення, Мал.16. У цьому випадку необхідно, **натиснути кнопку «Вихід» та зателефонувати до Адміністратора захисту інформації Банку з проханням прискорити авторизацію сертифікату** (контактна інформація вказана, також, в кінці документу).

Аварийное восстановление ключей

Ожидайте, Ваш запрос на восстановление сертификата находится в очереди на рассмотрение в банке.

Если Вы хотите отправить новый запрос на восстановление сертификата в банк:

- 1) Введите аварийный пароль.
- 2) Пройдите процедуру восстановления. Ключи следует сохранить в новую папку.

Введите аварийный пароль

Мал. 16.

2.2.3. Якщо Ваш запит на генерацію нового Сертифіката був оброблений Банком, система видає повідомлення, Мал.17:

Аварійне відновлення ключів

Ваш запит на відновлення сертифікатів оброблено.

Нові сертифікати готові до передачі.

Для встановлення нових сертифікатів введіть аварійний пароль.


Введіть аварійний пароль

Мал. 17.

Введіть **Аварійний пароль** в поле **«Введіть аварійний пароль»** (див. файл **«RECOVERY.TXT»**).

2.2.4. Натисніть кнопку **«Відправити»**, на екрані буде отримано повідомлення, мал. 18:

Увага!

 Ви бажаєте відправити пароль?

Мал. 18

2.2.5. Натисніть кнопку **«ОК»**. На екрані буде отримано повідомлення, мал. 19:

Ваш запит на відновлення сертифікатів оброблено.

Нові сертифікати готові до передачі.

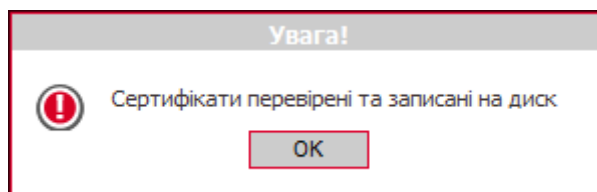
Для продовження роботи з системою необхідно встановити нові сертифікати.

Новий пароль	<input type="password" value="*****"/>
Ключі будуть збережені в	G:\TEST_WEB
	<input type="button" value="Записати файли"/>

Мал.19

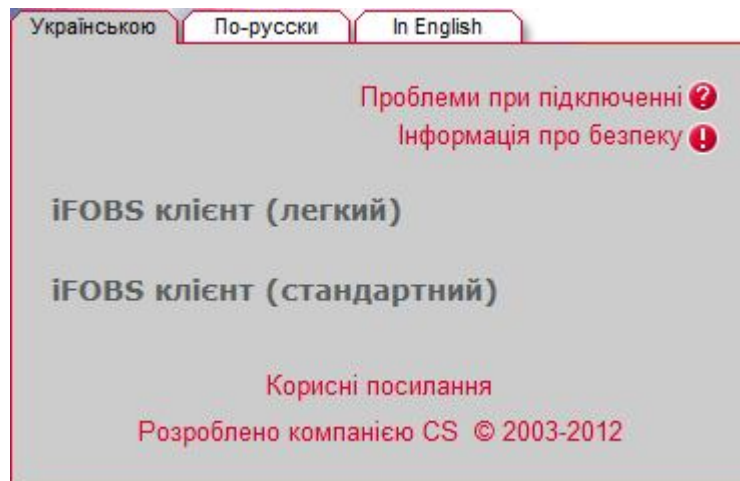
Вкажіть новий пароль до секретного ключа що був заданий Вами при створенні запиту в п.п.2.1.3, для підтвердження того, що Ключ отримуєте саме Ви.

2.2.6. Натисніть кнопку «**Записати файли**». На екрані буде отримано повідомлення, мал. 20:



Мал.20

2.2.7. Натисніть кнопку «**Ок**», при цьому Ви будете переміщені на стартову сторінку програми, мал. 21:



Мал.21

2.2.8. Оберіть пункт «**iFobs клієнт (стандартний)**» та увійдіть в систему використовуючи наступні дані, мал. 22:

Мал.22

Введіть Логін користувача в полі «Логін» (див. файл «RECOVERY.TXT»);

Введіть свій пароль на вхід в систему в полі «Пароль» (див. файл «RECOVERY.TXT»);

Введіть новий пароль до секретного ключа що був заданий Вами при створенні запиту в п.п.2.1.3 в полі «Пароль до секретного ключа».

Натисніть кнопку «Вхід».

2.2.9. На екрані відкриється форма зміни пароля для входу в систему, Мал. 23:

Мал.23

Введіть пароль на вхід в систему в полі «Поточний пароль» (див. файл «RECOVERY.TXT»);

Задайте новий пароль, та підтвердіть новий пароль.

Увага! При введенні паролів необхідно дотримуватися правил:

- англійська розкладка клавіатури і вимкнена клавіша "Caps Lock";
- Новий пароль повинен бути розміром не менше восьми (8) символів (максимально до 15), формуватися з латинських літер та службових символів (-, %, *, ?, _), цифр;
- не повинен повторювати попередній пароль.

2.2.10. Натисніть кнопку «Застосувати». На екрані буде отримано повідомлення, мал. 24:

Мал.24

2.2.11. Натисніть кнопку «ОК», при цьому Ви будете переміщені на стартову сторінку програми.

Подальший вхід в систему «Клієнт-банк» можна виконувати використовуючи новий **пароль на вхід в систему** та новий **пароль до секретного ключа**.

Система «Клієнт-Банк» готова до роботи.

Бажаємо успіхів і висловлюємо надію на подальшу співпрацю.

З повагою, ПАТ "КРИСТАЛБАНК"