ІВК Користувач

(Версія 1.0.0…)

«Настанова користувача»

www.ivk.org.ua

2013

Анотація

Даний документ містить настанову користувача для роботи з програмним комплексом «ІВК Користувач» (далі – програма). Настанова містить відомості щодо послідовності особливостей інсталяції, встановлення параметрів роботи та використання програми.

Для роз’яснення порядку взаємодії з програмно-технічним комплексом ЦСК у додатку А наведена функціональна схема.

ЗМІСТ

1. Призначення

2. Умови виконання програми

3. Початок роботи з програмою

4. Підпис файлів

5. Шифрування файлів

6. Перевірка підпису користувача

7. Розшифрування

8. Завантаження програми через Інтеграцію з MS Word 2007

9. Підпис файлів

10. Захист

11. Відкрити та перевірити

12. Розшифрувати та перевірити

Перелік скорочень

Додаток А

1. ПРИЗНАЧЕННЯ ПРОГРАМИ

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

- підпис файлів;
- шифрування файлів;
- перевірка підпису;
- розшифрування файлів.

<<Назад

2. УМОВИ ВИКОНАННЯ ПРОГРАМИ

Програма може бути завантажена та виконана на ПЕОМ із 32-бітним або 64-бітним процесором з архітектурою Intel Architecture 32 (Intel, AMD, Cyrix та ін.) під керуванням ОС Microsoft Windows XP, Windows 2007 або Microsoft Windows 2003 Server та вище.

<<Назад

3. ПОЧАТОК РОБОТ З ПРОГРАМОЮ

3.1 Завантаження програми

Для завантаження програми необхідно в ПЕОМ вставити з'ємний диск з програмою «ІВК Користувач». Для завантаження програми необхідно на з'ємному диску запустити модуль «ІВК Користувач»(Рис.3.1), який знаходиться в папці IVKEndUser.

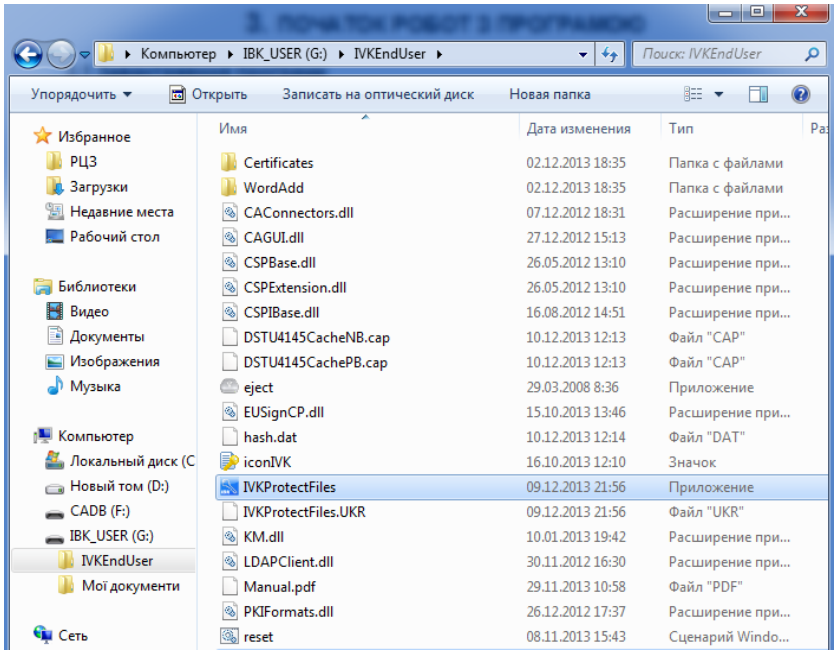


Рисунок 3.1 – Розташування програми

Після запуску програми, потрібно зберегти сертифікат користувача, для цього потрібно перетягнути на аркуш сертифікат, або в ручному режимі зберегти сертифікат на флешку до папки IVKEndUser/Certificates(Рис.3.1).

Для вводу паролю до ключа користувача потрібно натиснути на аркуш або перетягти файл на аркуш, щоб розпочати роботу ПЗ «ІВК Користувач».(Рис. 3.2)

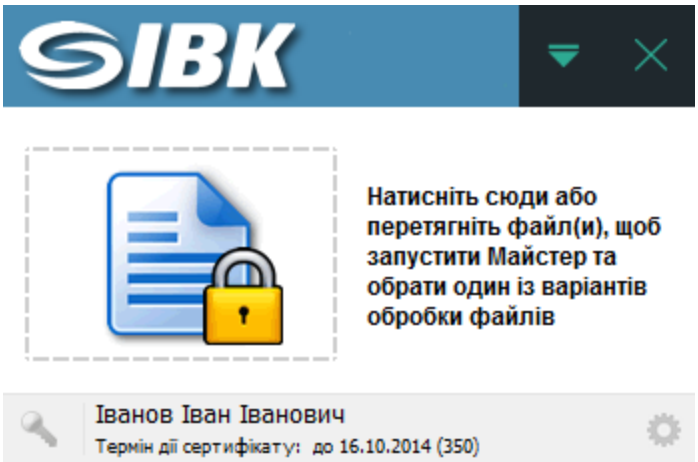


Рисунок 3.2 – Початок роботи програми

На наступній сторінці (Рис.3.3) необхідно вказати пароль доступу до особистого ключа та натиснути «Зчитати».

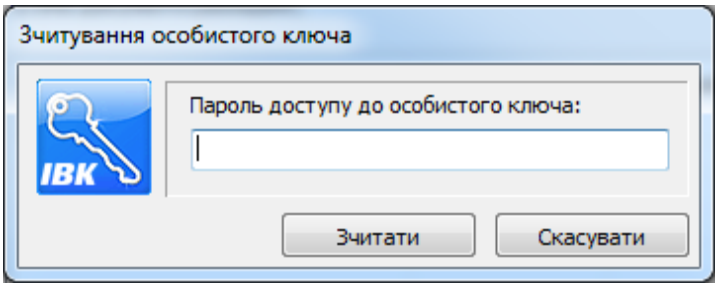


Рисунок 3.3 – Введення паролю доступу до особистого ключа

Пароль доступу потрібно вводити лише при першому запуску програми «ІВК Користувач» на ПЕОМ.

Програмне забезпечення «ІВК Користувач» сумісно з антивірусом «Касперського». При роботі з іншими антивірусами, можливі збої в роботі.

<<Назад

4. ПІДПИС ФАЙЛІВ

Для підпису файлів (накладання ЕЦП) необхідно натиснути на панелі «Підпис файлів» (Рис.4.1).

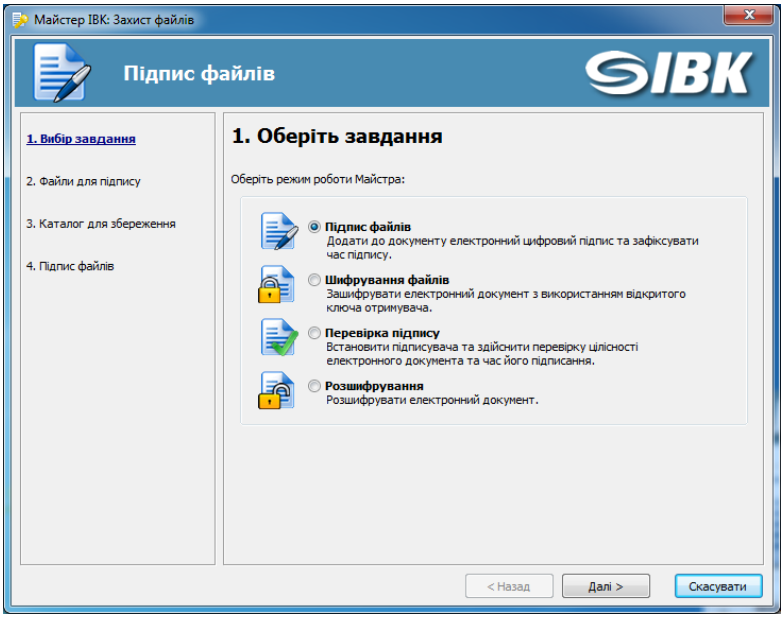


Рисунок 4.1 – Вибір режиму роботи

Натиснувши кнопку «Далі», переходимо до діалогового вікна вибору файлів підпису (Рис.4.2). Для додавання файлів необхідно натиснути «Додати…» або перетягнути файли з каталогу операційної системи в програму «ІВК Користувач».

Для видалення файлів зі списку необхідно обрати файл і натиснути «Видалити…».

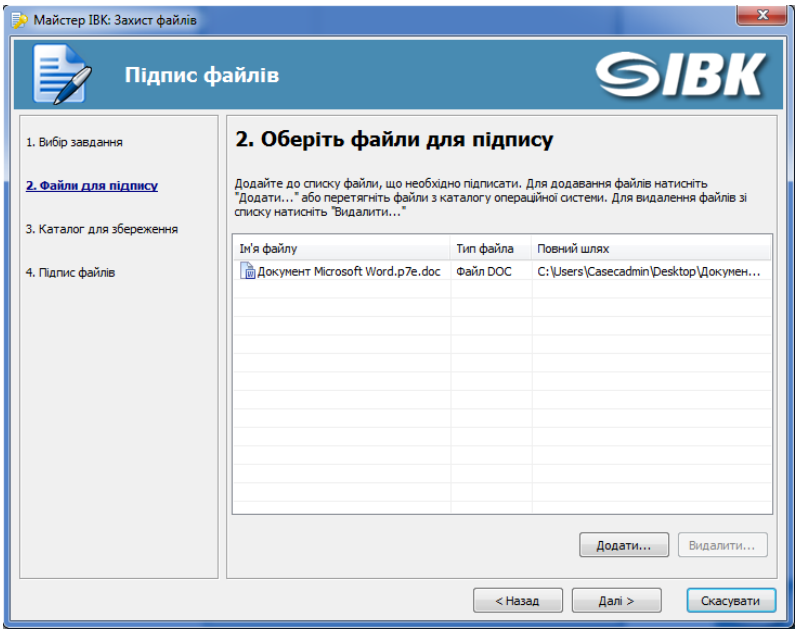


Рисунок 4.2 – Вибір файлів для підпису

Наступна сторінка майстра (Рис.4.3) дає можливість вказати каталог для збереження підписаних файлів. Для вибору каталогу слід натиснути «Огляд». За замовчуванням файли зберігаються до папки Мої документи\Захищені\ на з'ємному носії «ІВК Користувач».

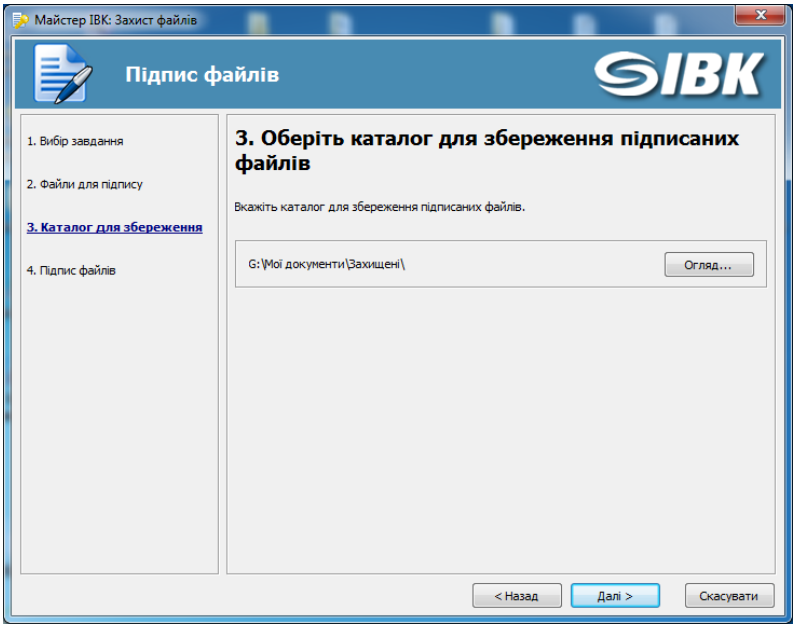


Рисунок 4.3 – Вибір каталогу для збереження підписаних файлів

Наступна сторінка майстра (Рис.4.4) здійснює підпис файлу. Для підпису файлів натисніть «Підписати».

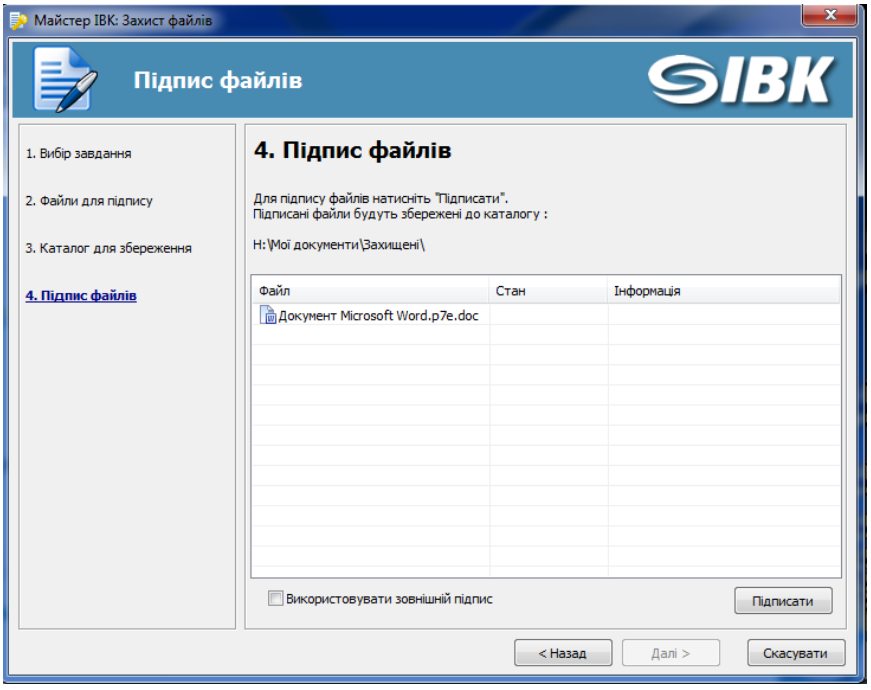


Рисунок 4.4 – Підпис файлів

Підпис здійснюється (Рис.4.5) на основі особистого ключа користувача. Доступ до ключа користувача здійснюється після вводу паролю доступу. Ввівши пароль потрібно натиснути «Зчитати».

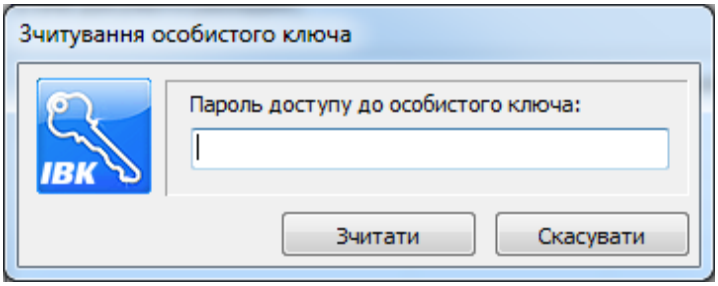


Рисунок 4.5 – Зчитування особистого ключа

У разі вдалого підписання (Рис.4.6) в таблиці навпроти файлу буде вказано статус файлу «Підписано». У разі помилки в підписі, відповідна інформація буде відображена в таблиці стану файлу.

Підписані файли будуть збережені до обраного каталогу (Рис.4.7). Для перегляду каталогу з підписаними файлами, потрібно натиснути кнопку «Завершити», після чого відкривається каталог з підписаними файлами. Також є можливість використання зовнішнього підпису. Використання зовнішнього підпису передбачає запис ЕЦП в окремий файл з розширенням “.p7s” без включення вмісту файлу що підписується. За замовчуванням використовується внутрішній підпис. Запис ЕЦП до зовнішнього файлу потрібен у випадку необхідності доступу до структури (вмісту) файлу без зняття з нього ЕЦП.

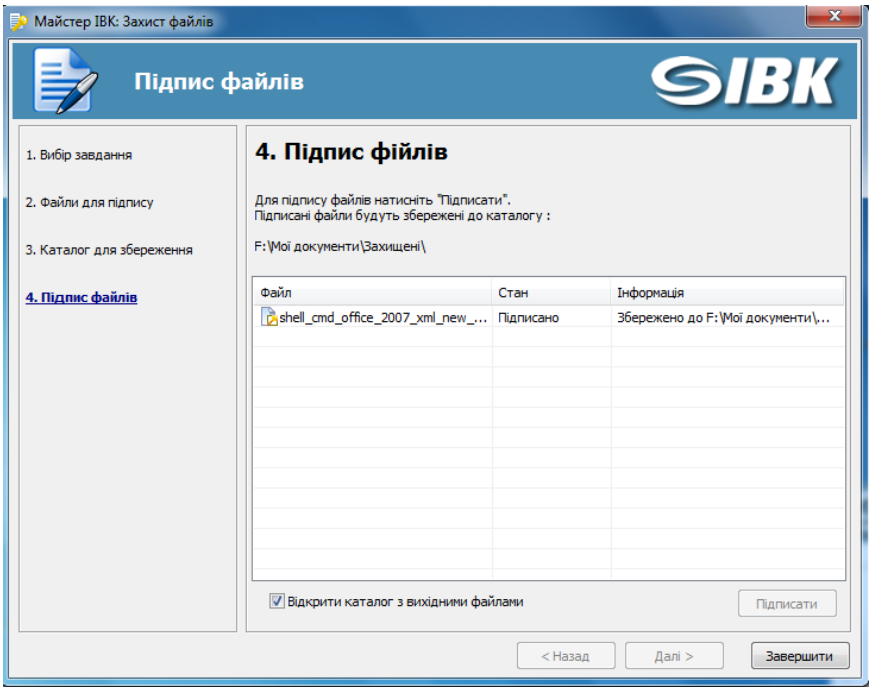


Рисунок 4.6 – Стан підписаного файлу

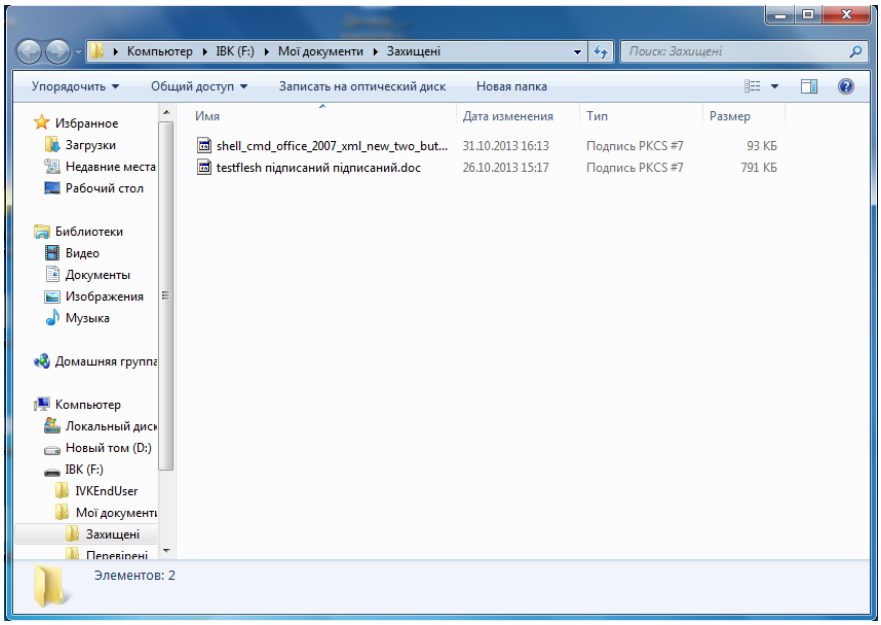


Рисунок 4.7 – Каталог з підписаними файлами

<<Назад

5. ШИФРУВАННЯ ФАЙЛІВ

Для шифрування файлу необхідно вибрати режим роботи «Шифрування файлів»(Рис.5.1).

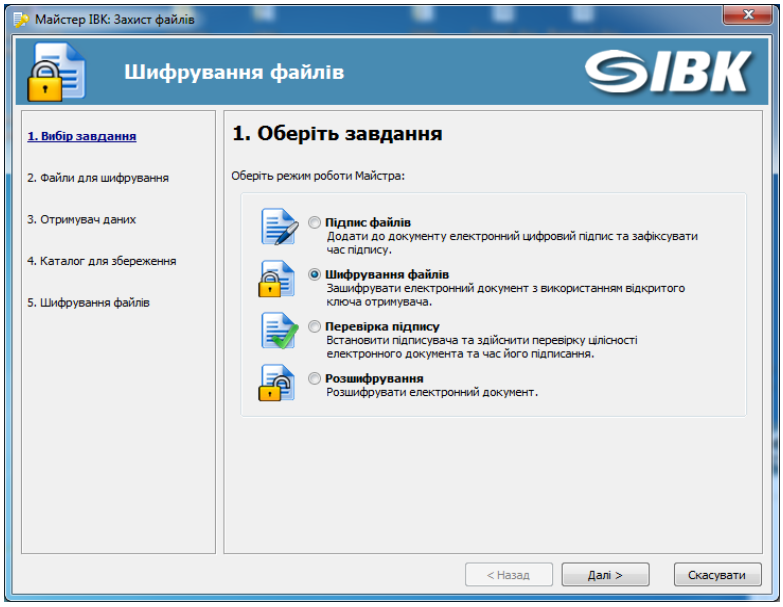


Рисунок 5.1 – Вибір режиму роботи

Натиснувши кнопку «Далі», переходимо до діалогового вікна з файлами, які необхідно зашифрувати (Рис.5.2). Для додавання файлів необхідно натиснути «Додати…» або перетягнути файли з каталогу операційної системи в програму «ІВК Користувач».

Для видалення файлів зі списку необхідно обрати файл і натиснути «Видалити…».

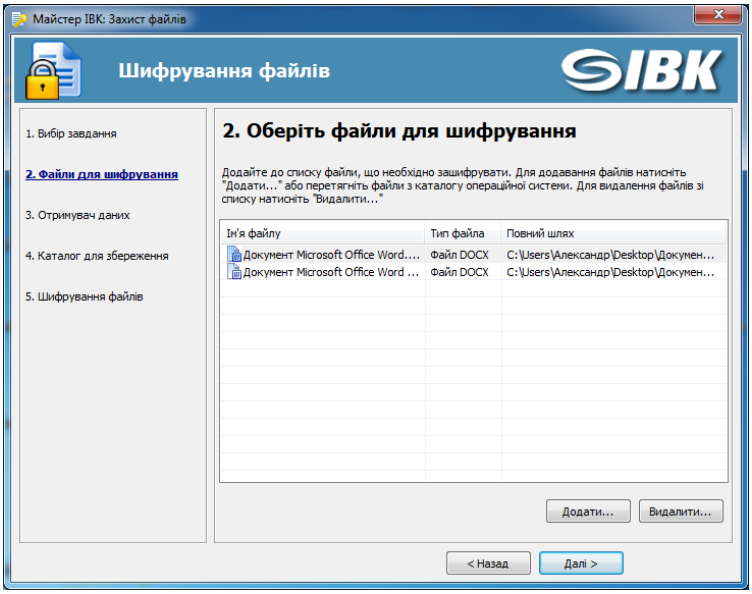


Рисунок 5.2 – Вибір файлу для шифрування

Для перевірки чинності сертифікату необхідно вибрати сертифікат зі списку та натиснути «Перевірити» (Рис.5.3). Якщо обраний сертифікат діючий, біля назви файлу з'явиться зелений трикутник. В протилежному випадку, якщо сертифікат не діючий, біля назви файлу з'явиться червоний круг. Після вибору сертифіката одержувача потрібно натиснути "Далі".

Для зашифровування файлів використовується особистий ключ користувача що виконує зашифровування та сертифікат(и) користувача(ів) для якого(их) зашифровується файл.

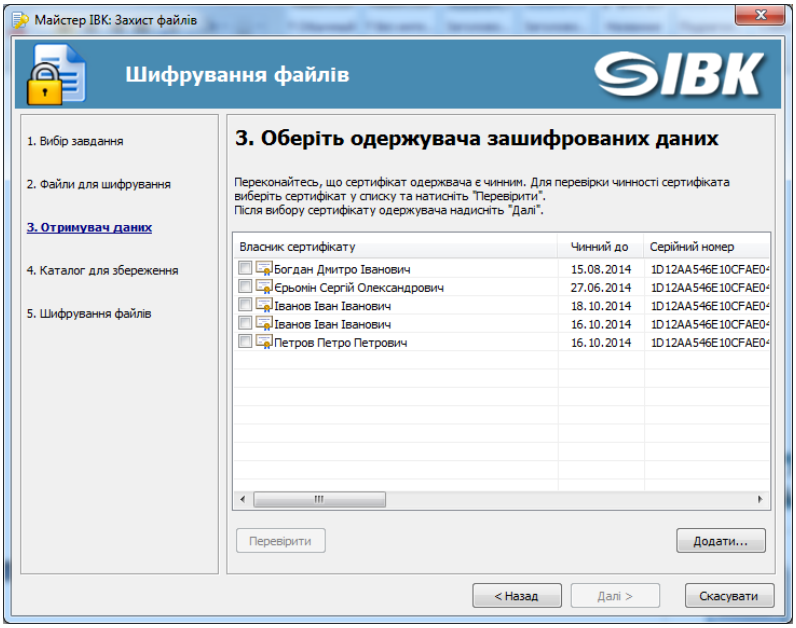


Рисунок 5.3 – Вибір одержувача зашифрованих даних

Наступна сторінка майстра (Рис.5.4) дає можливість вказати каталог для збереження зашифрованих файлів. Для вибору каталогу слід натиснути «Огляд». За замовчуванням файли зберігаються до папки Мої документи\Захищені\ на з'ємному носії «ІВК Користувач».

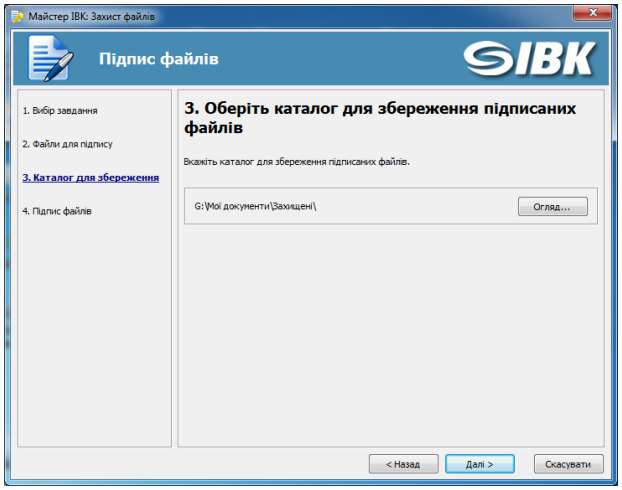


Рисунок 5.4 – Вибір каталогу для збереження підписаних файлів

Наступна сторінка майстра (Рис.5.5.) дає можливість додатково підписати обрані файли «Додатково підписати». За замовчуванням здійснюється лише зашифровування кожного файлу. Вихідні зашифровані файли мають розширення “.p7e”. Зашифровані файли будуть збережені до обраного вами каталогу. Для шифрування потрібно натиснути “Зашифрувати”.

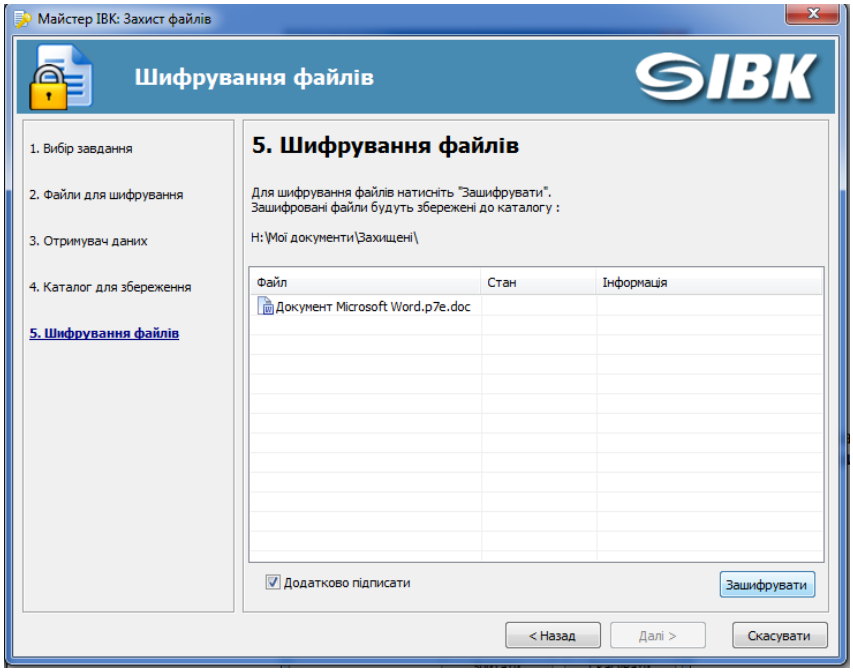


Рисунок 5.5 – Шифрування файлів

Шифрування здійснюється (Рис.5.6) на основі особистого ключа користувача. Доступ до ключа користувача здійснюється після вводу паролю доступу. Ввівши пароль потрібно натиснути «Зчитати».

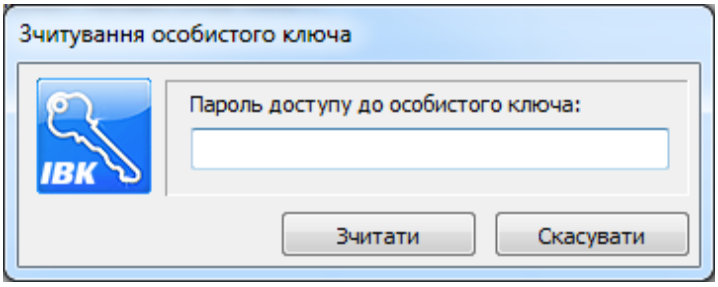


Рисунок 5.6 – Зчитування особистого ключа

Зашифровані файли будуть збережені до обраного каталогу. У разі вдалого шифрування (Рис.5.7) в таблиці навпроти файлу буде вказано статус файлу «Зашифровано». У разі помилки зашифровування, відповідна інформація буде відображена в таблиці стану документу.

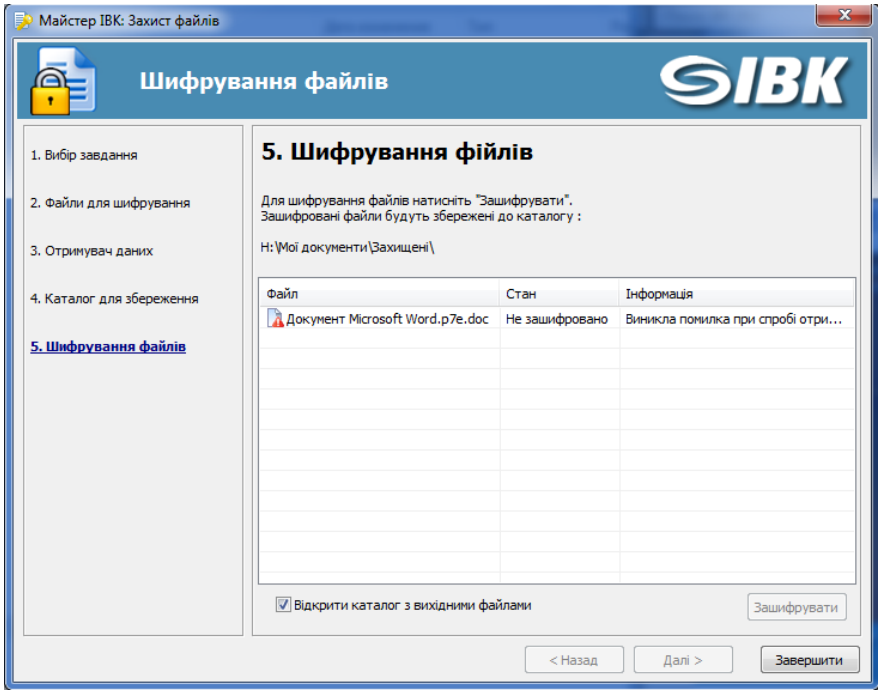


Рисунок 5.7 – Стан зашифрованого файлу

Для перегляду каталогу з зашифрованими файлами (Рис.5.8), потрібно натиснути кнопку «Завершити», після чого відкриється каталог з зашифрованими файлам.

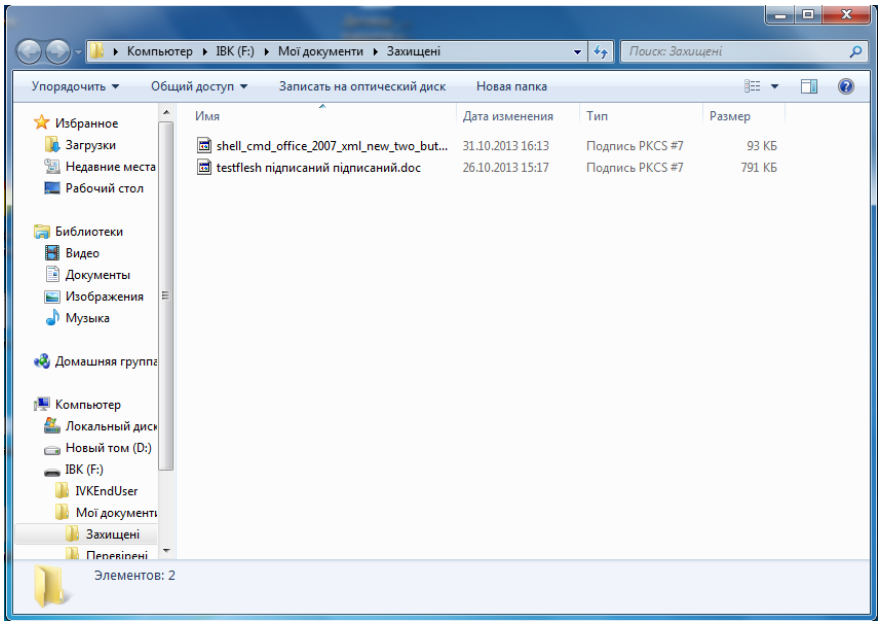


Рисунок 5.8 – Каталог з зашифрованими файлами

<<Назад

6. ПЕРЕВІРКА ПІДПИСУ КОРИСТУВАЧА

Для перевірки підпису користувача, потрібно в головному вікні програми вибрати режим роботи «Перевірка підпису» (Рис. 6.1).

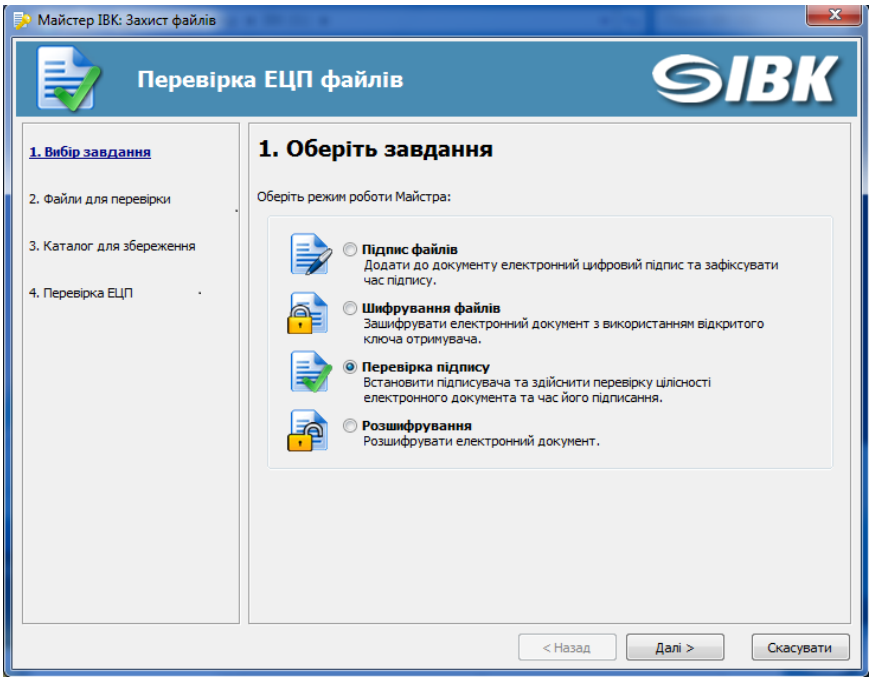


Рисунок.6.1 – Вибір режиму роботи

Натиснувши кнопку «Далі», переходимо до діалогового вікна, в якому необхідно додати до списку підписані файли (Рис.6.2). Для додавання файлів необхідно натиснути «Додати…» або перетягнути файли з каталогу операційної системи в програму «ІВК Користувач».

Для видалення файлів зі списку необхідно обрати файл і натиснути «Видалити…».

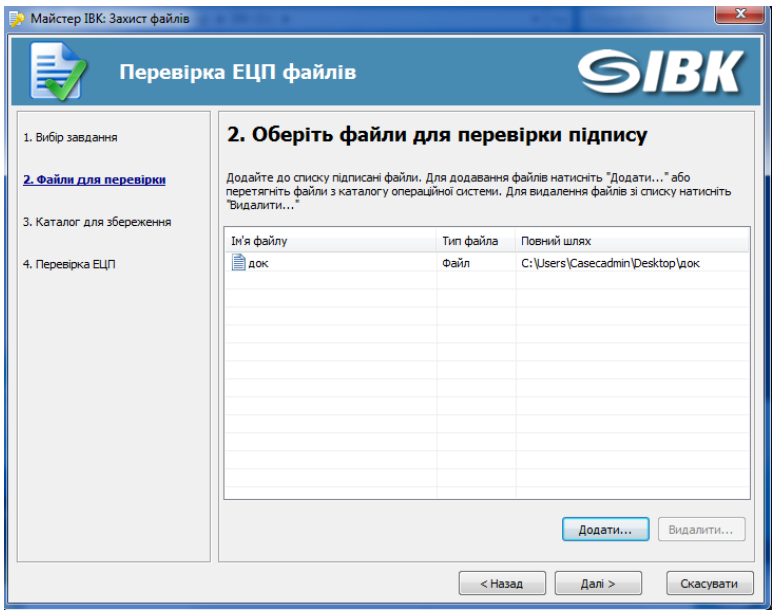


Рисунок 6.2 – Вибір файлу для перевірки підпису

Наступна сторінка майстра (Рис.6.3) дає можливість вказати каталог для збереження перевірених файлів. Для вибору каталогу слід натиснути «Огляд». За замовчуванням файли зберігаються до папки Мої документи\Перевірені\ на з'ємному носії «ІВК Користувач».

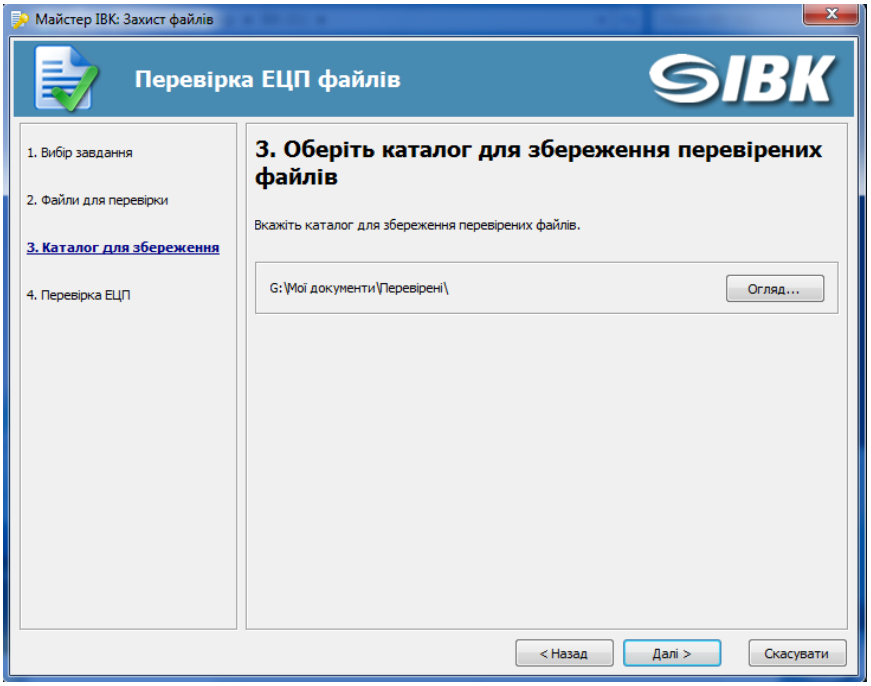


Рисунок 6.3 – Вибір каталогу для збереження перевірених файлів

На наступній сторінці (Рис.6.4) необхідно натиснути «Перевірити». Після перевірки підпису файли будуть збережені до обраного каталогу.

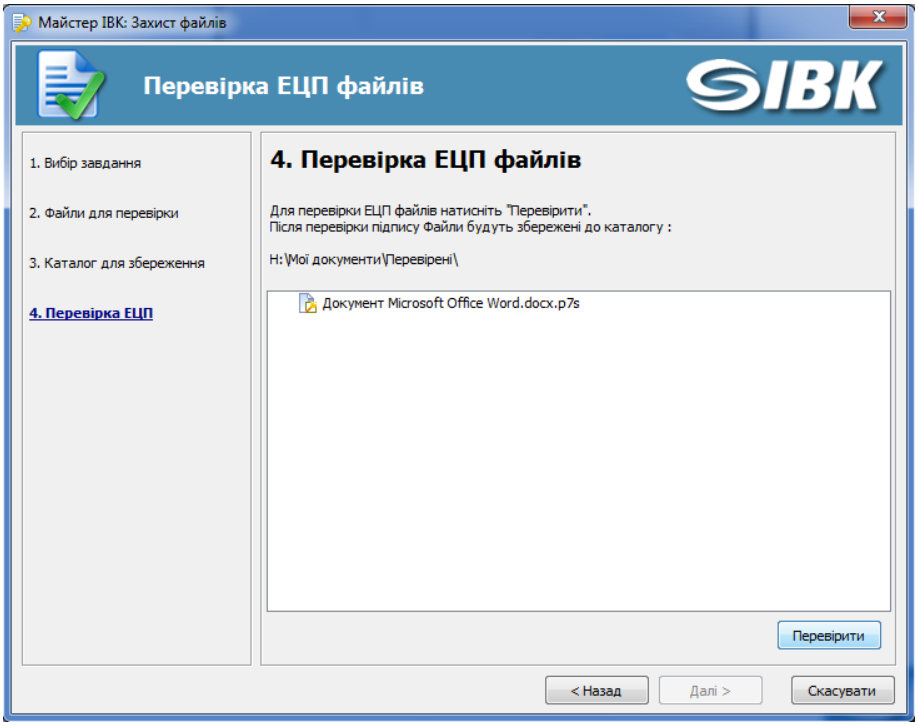


Рисунок 6.4 – Перевірка ЕЦП файлів

Для перевірки ЕЦП файлів необхідно натиснути сноПку «Перевірити». Після перевірки підпису файли будуть збережені до каталогу Мої документи\Перевірені\ на з'ємному носії «ІВК Користувач».

Для відкриття перевіреного файлу, потрібно його вибрати та натиснути кнопку «Відкрити» (Рис.6.5), після чого відкривається вікно з інформацією про підпис файлу(Рис.6.6).

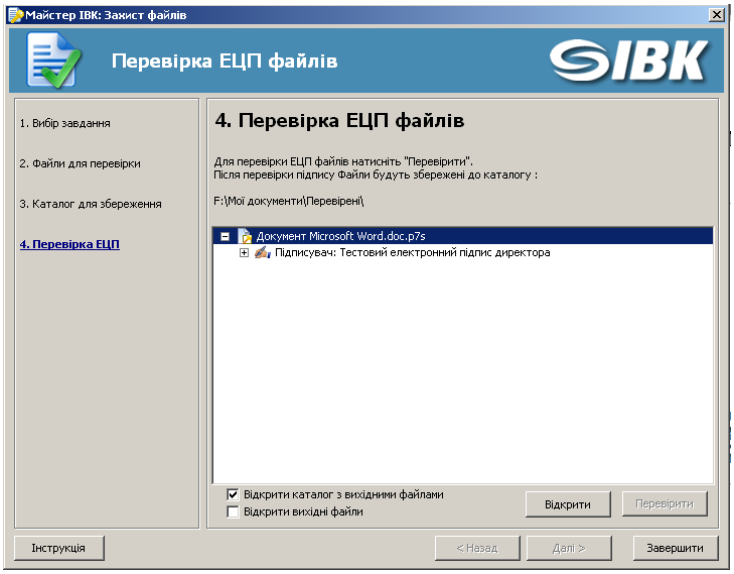


Рисунок 6.5 – Відкриття перевіреного файлу

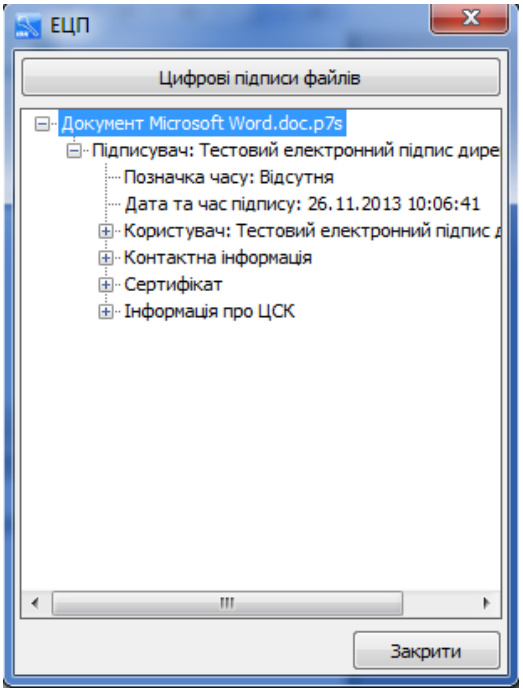


Рисунок 6.6 – Інформація про підпис файлу

Для перегляду каталогу з перевіреними файлами(Рис.6.7), потрібно натиснути кнопку «Завершити», після чого відкриється каталог з перевіреними файлам.

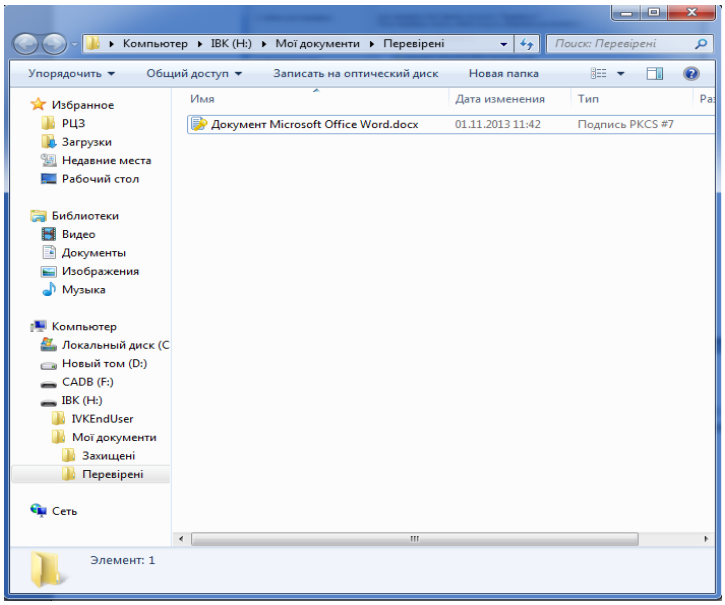


Рисунок 6.7 – Каталог з перевіреними файлами

<<Назад

7. РОЗШИФРУВАННЯ

Для розшифрування електронного документу, потрібно в головному вікні програми вибрати режим роботи «Розшифрування» (Рис. 7.1).

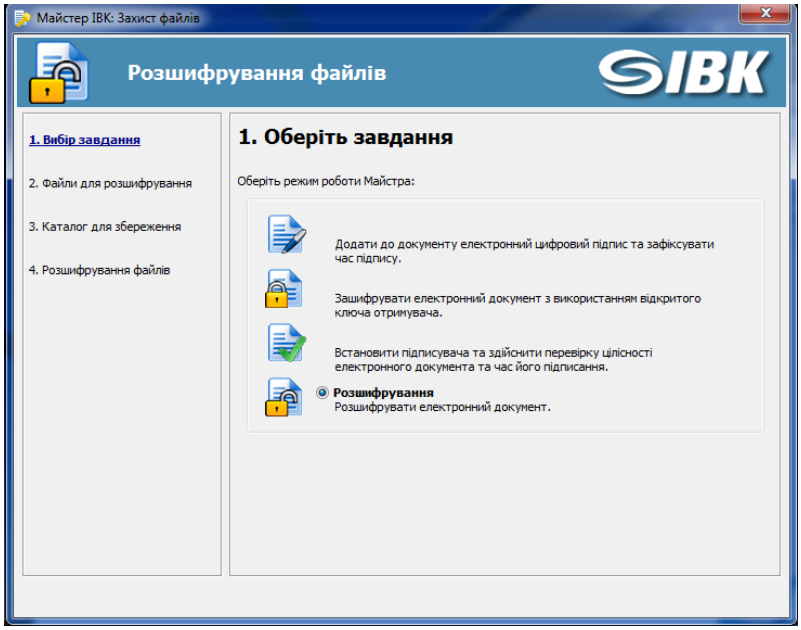


Рисунок 7.1 – Вибір режиму роботи

Натиснувши кнопку «Далі», переходимо до діалогового вікна, в якому необхідно додати до списку зашифровані файли (Рис.7.2). Для додавання файлів необхідно натиснути «Додати…» або перетягнути файли з каталогу операційної системи в програму «ІВК Користувач».

Для видалення файлів зі списку необхідно обрати файл і натиснути «Видалити…».

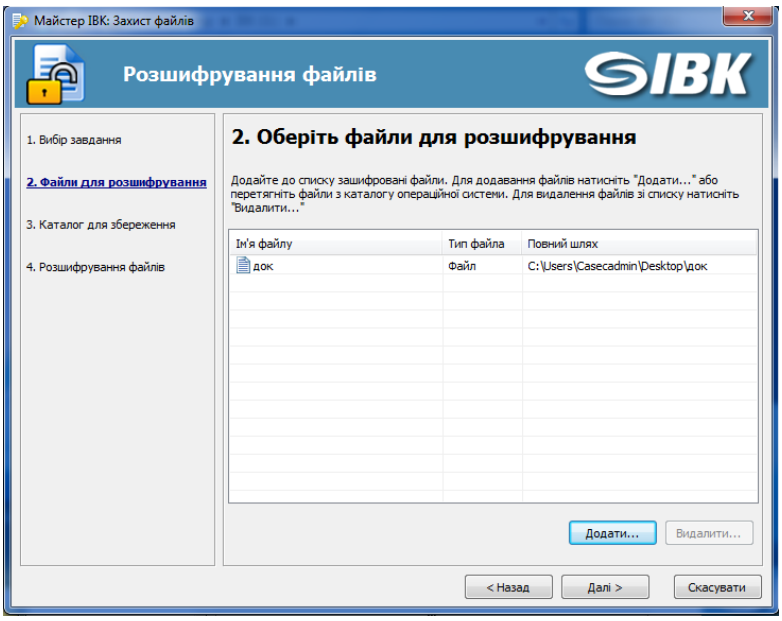


Рисунок 7.2 – Вибір файлів для розшифрування

Наступна сторінка майстра (Рис.7.3) дає можливість вказати каталог для збереження розшифрованих файлів. Для вибору каталогу слід натиснути «Огляд». За замовчуванням файли зберігаються до папки Мої документи\Перевірені\ на з'ємному носії «ІВК Користувач».

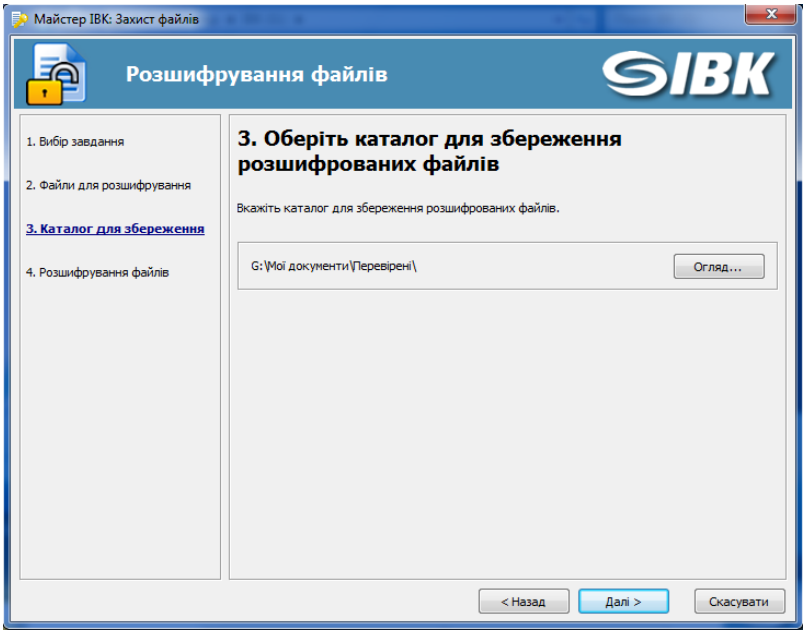


Рисунок 7.3 – Вибір каталогу для збереження розшифрованих файлів

На наступній сторінці (Рис.7.4) для розшифрування файлів необхідно натиснути «Розшифрувати». Розшифровані файли будуть збережені до обраного каталогу Мої документи\Перевірені\ на з'ємному носії «ІВК Користувач».

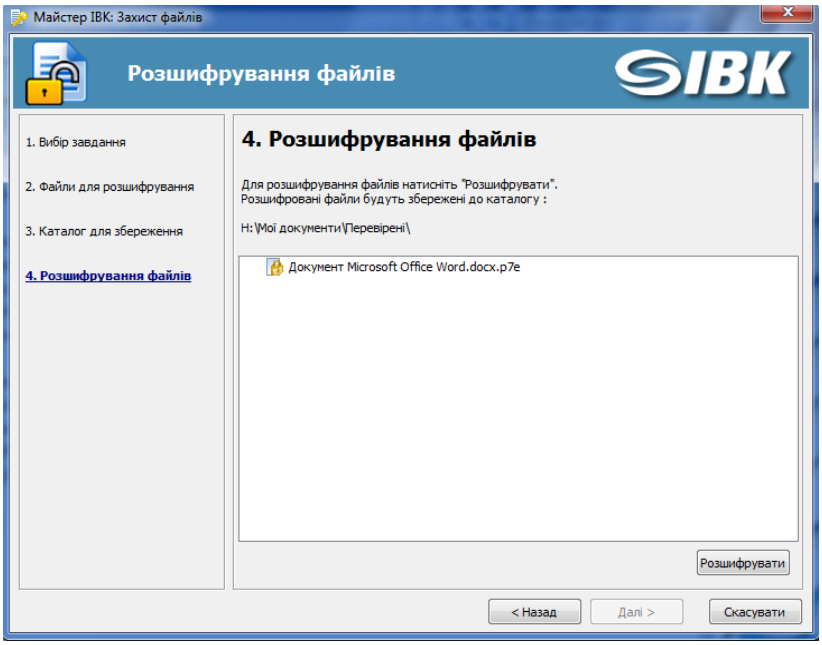


Рисунок 7.4 – Розшифрування файлів

Розшифрування файлу (Рис.7.5) здійснюється на основі особистого ключа користувача. Доступ до ключа користувача здійснюється після вводу паролю доступу. Ввівши пароль потрібно натиснути «Зчитати».

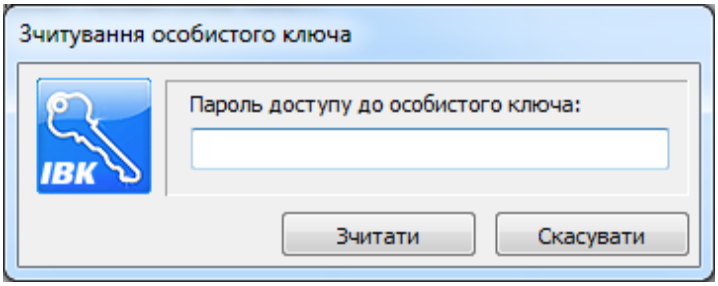


Рисунок 7.5 – Зчитування особистого ключа

Для перегляду каталогу з розшифрованими файлами, потрібно натиснути кнопку «Завершити»(Рис.7.6), після чого відкриється каталог з розшифрованими файлам(Рис.7.7).

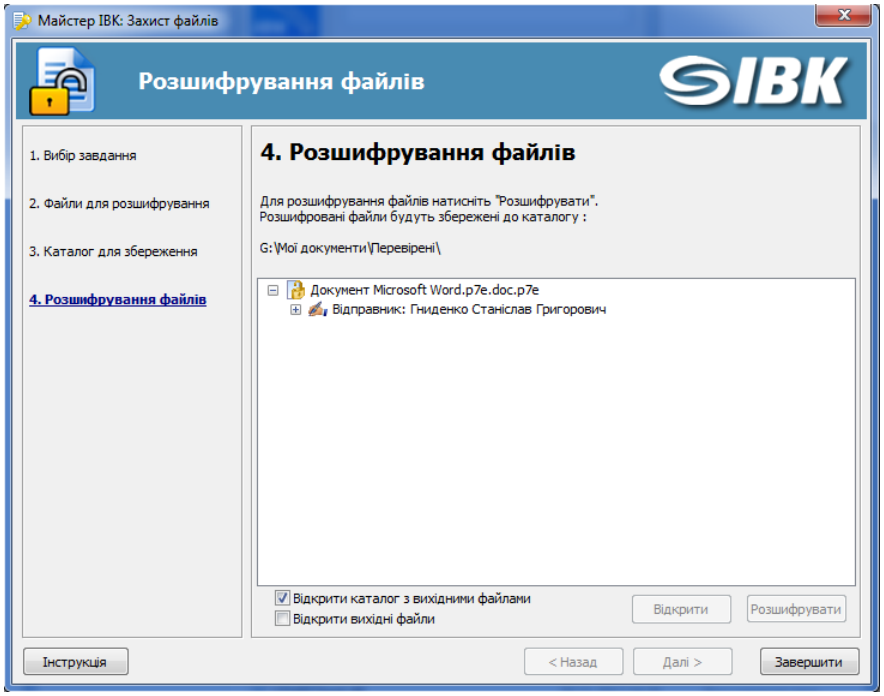


Рисунок 7.6 – Завершення розшифрування файлів

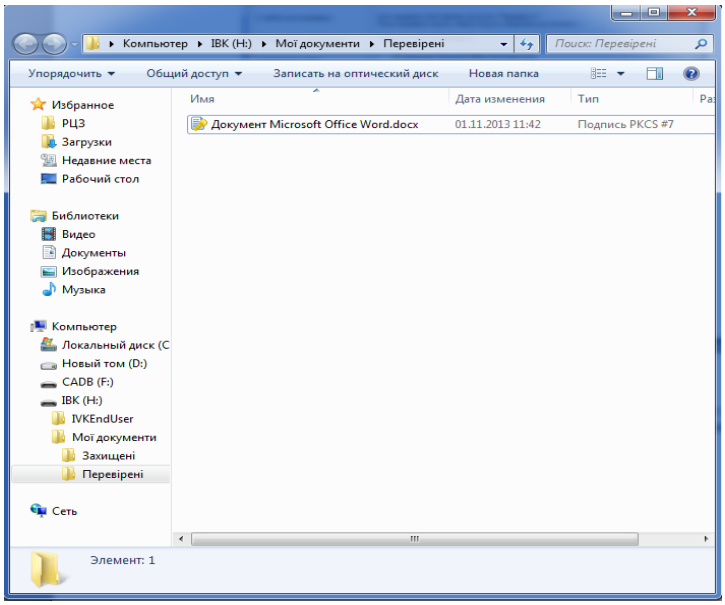


Рисунок 7.7 – Каталог з розшифрованими файлами

<<Назад

8. ЗАВАНТАЖЕННЯ ПРОГРАМИ ЧЕРЕЗ ІНТЕГРАЦІЮ С MS Word

Для завантаження програми необхідно в ПЕОМ вставити з'ємний диск з програмою «ІВК Користувач». Для завантаження програми необхідно на з'ємному диску запустити модуль «ІВК Користувач»(Рис.8.1) від імені адміністратора(Рис.8.2).

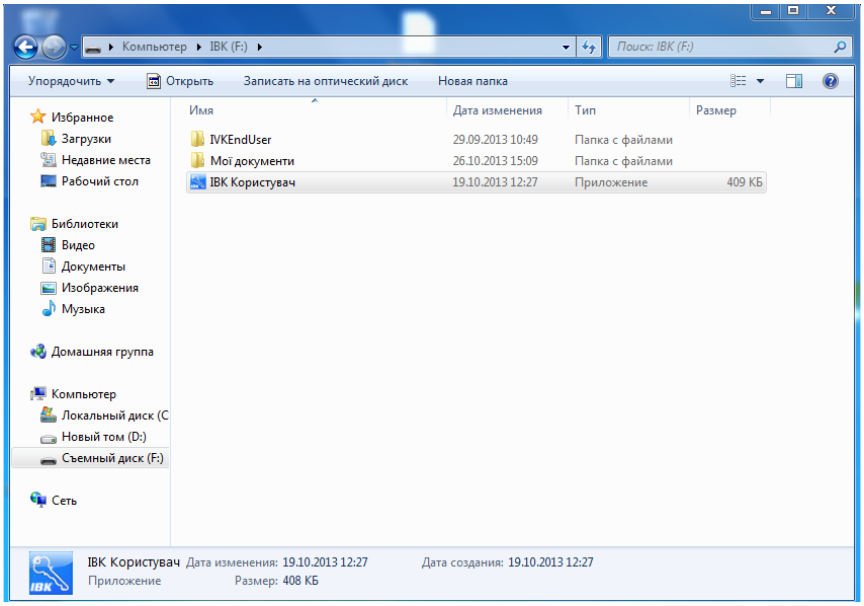


Рисунок 8.1 – Розташування програми

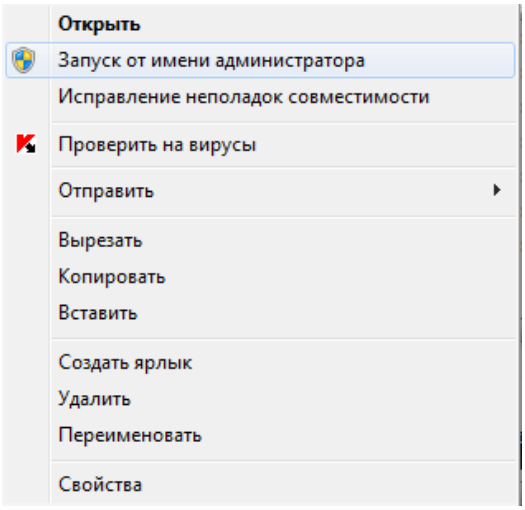


Рисунок 8.2 – Запуск програми від імені адміністратора

Потім потрібно відкрити вікно налаштувань програми (Рис.8.3) та вибрати відмітку «Інтеграція з MS Word 2007». Після натискання кнопки «Так», відкривається Документ Microsoft Word, в якому треба вибрати та натиснути кнопку «Параметри»(Рис.8.4). В наступному вікні(Рис.8.5) потрібно вибрати відмітку «Включить это содержимое» і натиснути кнопку «Ок».

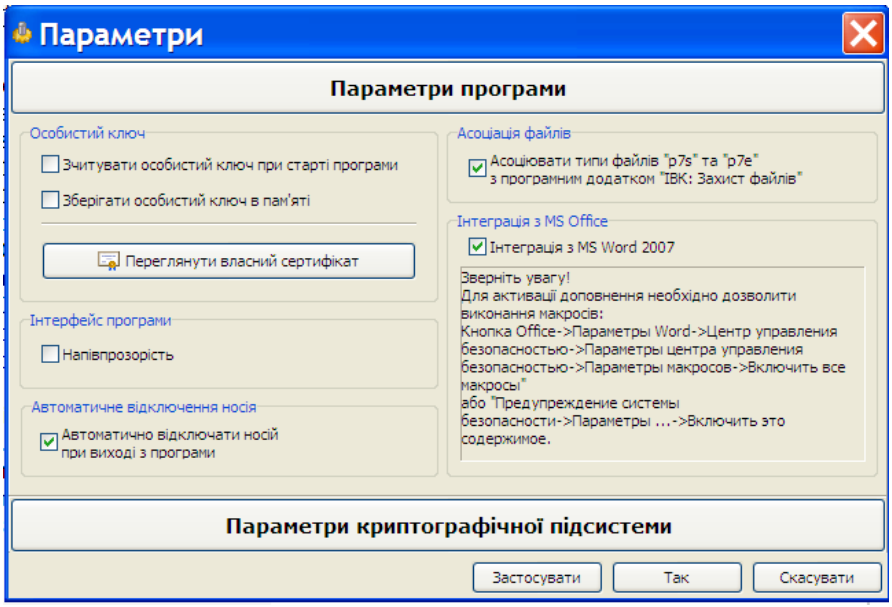


Рисунок 8.3 – Вікно налаштувань програми

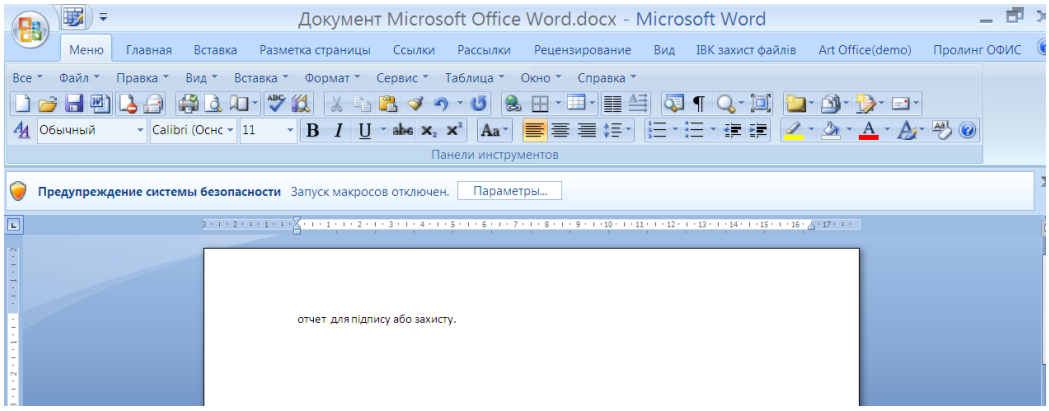


Рисунок 8.4 – Вибір параметрів

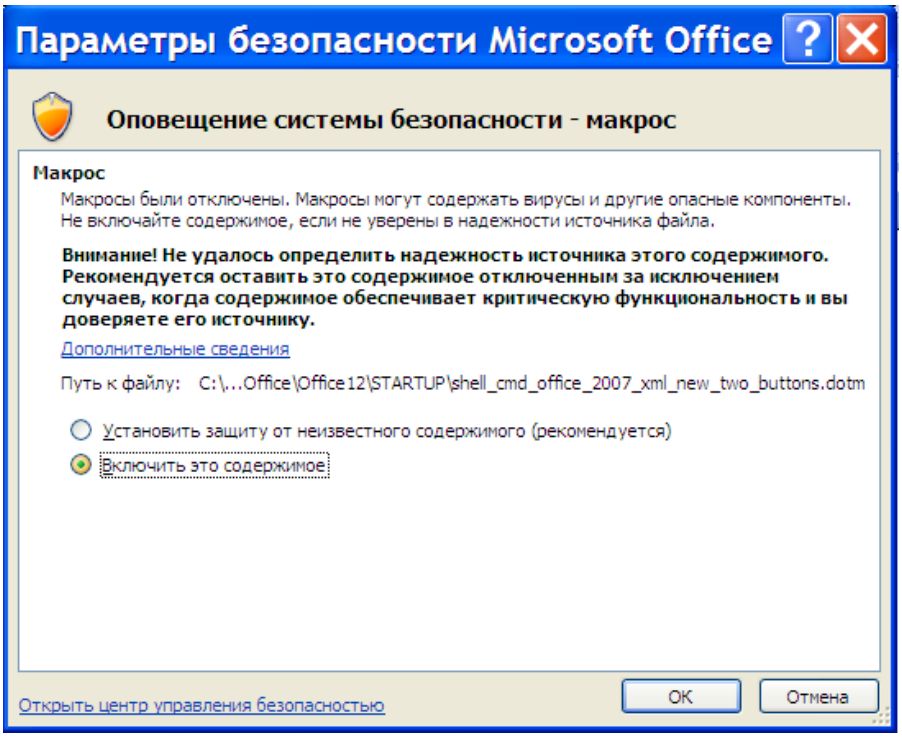


Рисунок 8.5 – Параметри безпеки Microsoft Office

<<Назад

9. ПІДПИС ФАЙЛІВ

При першій спробі підписати файл з’явиться вікно застереження. Якщо ви згодні натисніть «Ок

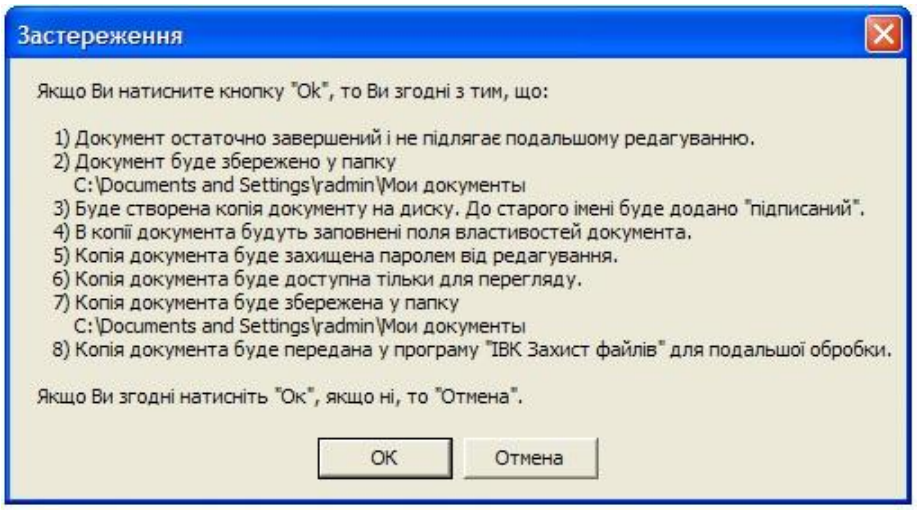


Рисунок 9.1 – Застереження

Для підпису файлів (накладання ЕЦП) необхідно натиснути на панелі «Підпис файлів» (Рис.9.2).

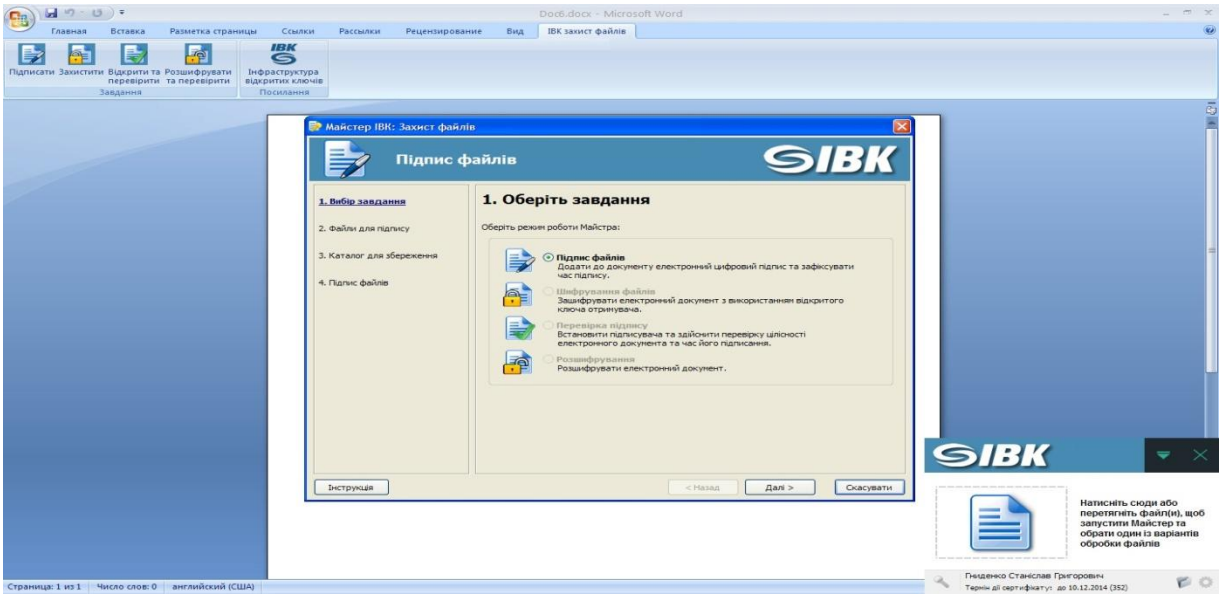


Рисунок 9.2 – Вибір режиму роботи

Натиснувши кнопку «Далі», переходимо до діалогового вікна вибору файлів підпису (Рис.9.3). Для додавання файлів необхідно натиснути «Додати…» або перетягнути файли з каталогу операційної системи в програму «ІВК Користувач».

Для видалення файлів зі списку необхідно обрати файл і натиснути «Видалити…».

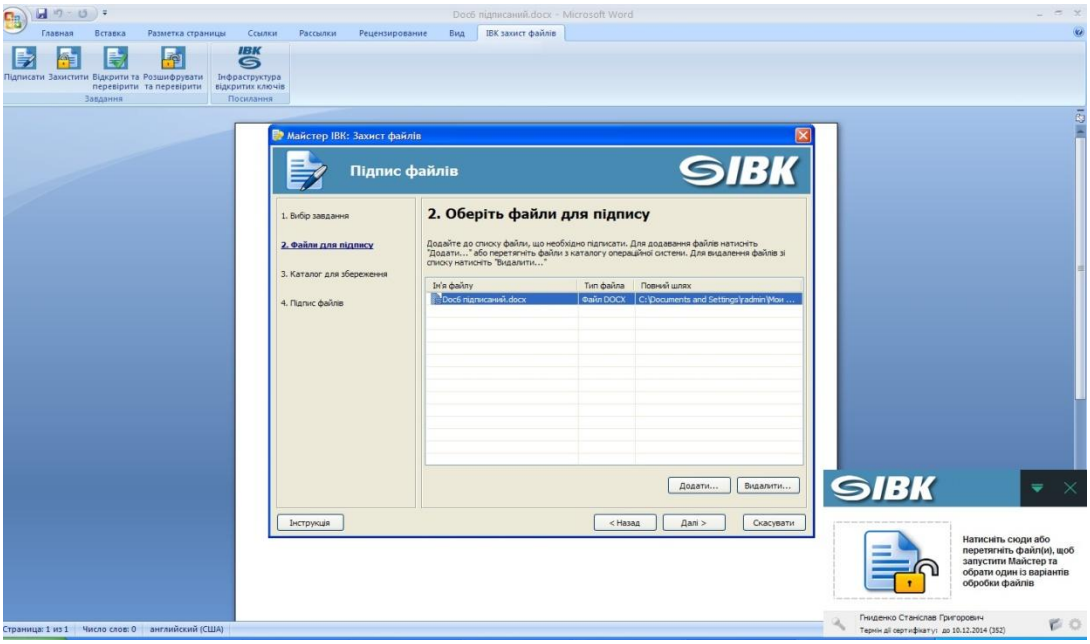


Рисунок 9.3 – Вибір файлів для підпису

Наступна сторінка (Рис.9.4) дає можливість вказати каталог для збереження підписаних файлів. Для вибору каталогу слід натиснути «Огляд». За замовчуванням файли зберігаються до папки C:\Мої документи\Захищені\

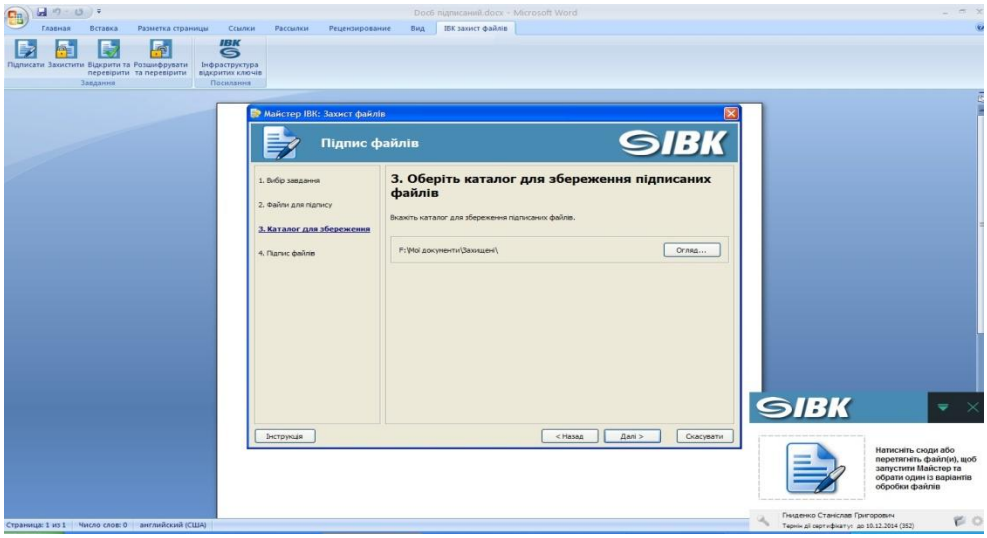


Рисунок 9.4– Вибір каталогу для збереження підписаних файлів

Наступна сторінка (Рис.9.5) здійснює підпис файлу. Для підпису файлів натисніть «Підписати».

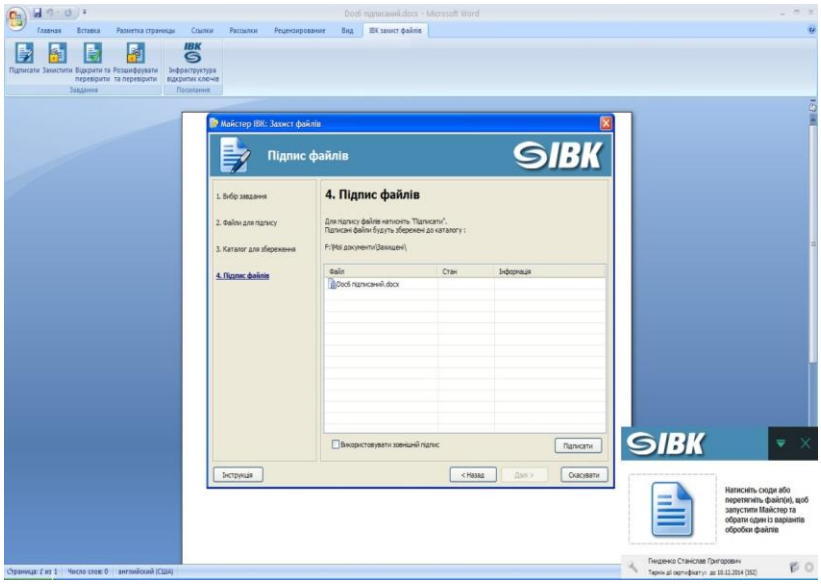


Рисунок 9.5 – Підпис файлів

На наступній сторінці (Рис.9.6) необхідно вказати пароль доступу до особистого ключа та натиснути «Зчитати».

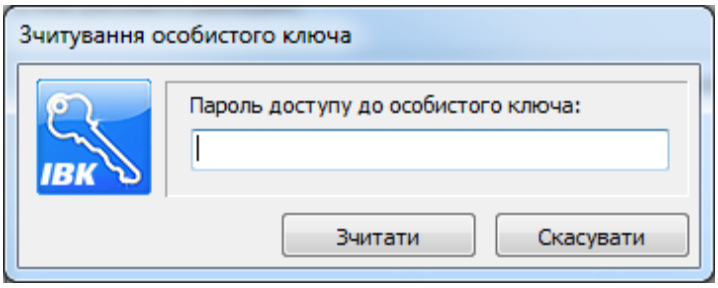


Рисунок 9.6 – Введення паролю доступу до особистого ключа

У разі вдалого підписання (Рис.9.7) в таблиці навпроти файлу буде вказано статус файлу «Підписано». У разі помилки в підписі, відповідна інформація буде відображена в таблиці стану файлу.

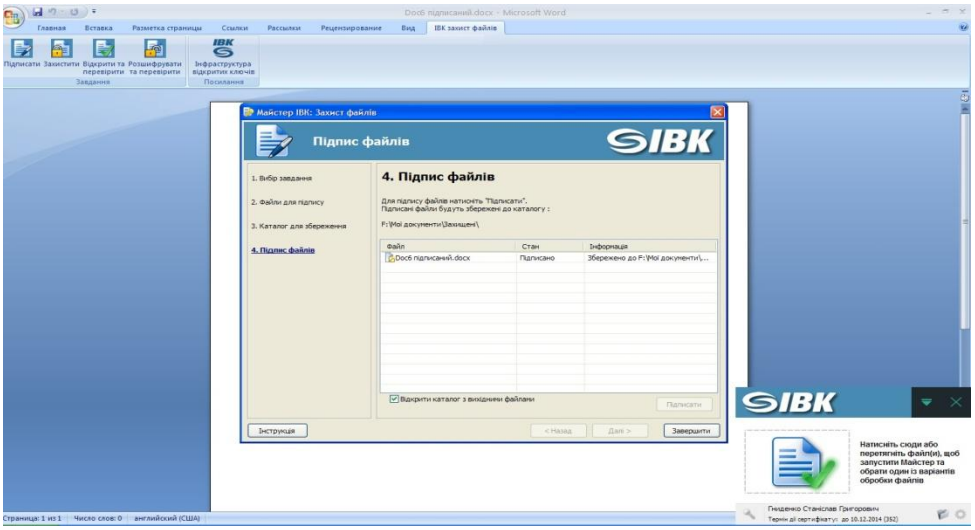


Рисунок 9.7 – Стан підписаного файлу

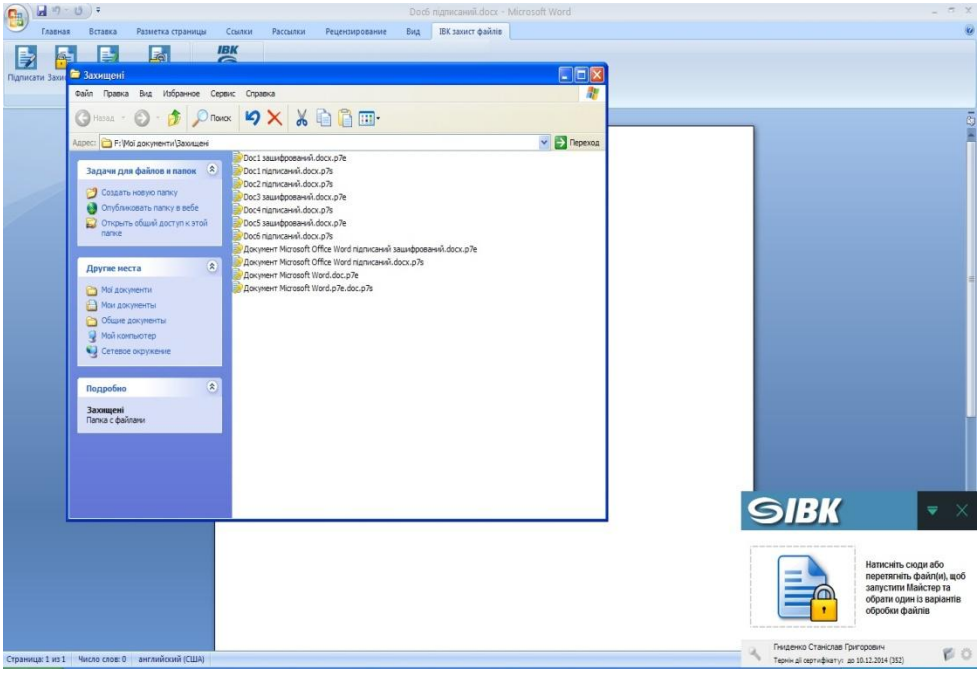


Рисунок 9.8 – Каталог з підписаними файлами

<<Назад

10. ЗАХИСТ

Для шифрування файлу необхідно вибрати режим роботи «Шифрування файлів»(Рис.10.1).

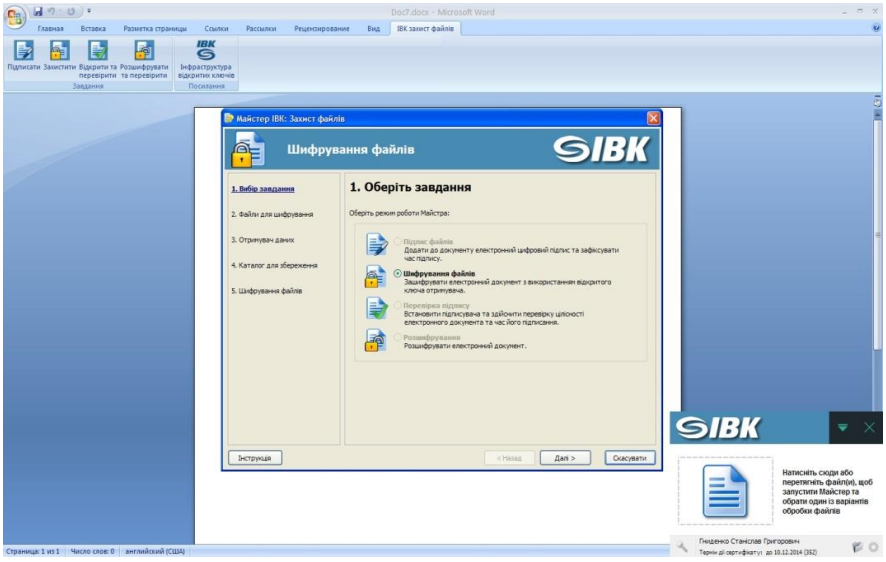


Рисунок 10.1 – Вибір режиму роботи

Натиснувши кнопку «Далі», переходимо до діалогового вікна з файлами, які необхідно зашифрувати (Рис.10.2). Для додавання файлів необхідно натиснути «Додати…» або перетягнути файли з каталогу операційної системи в програму «ІВК Користувач».

Для видалення файлів зі списку необхідно обрати файл і натиснути «Видалити…».

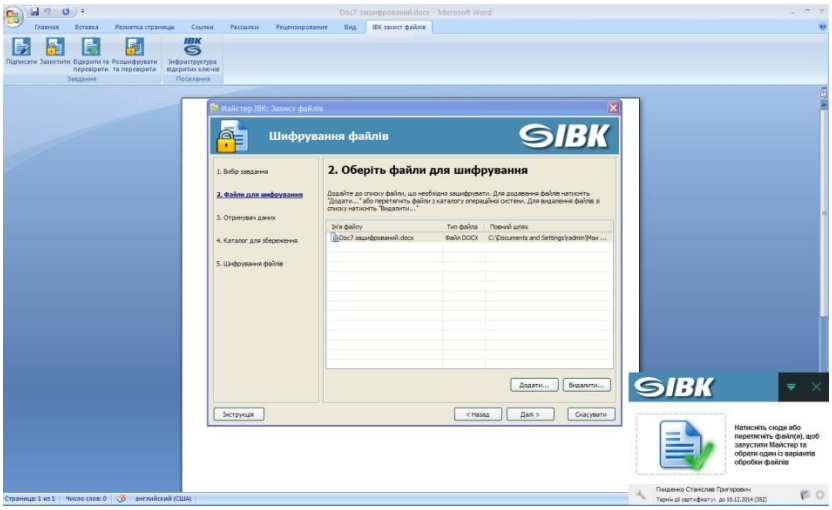


Рисунок 10.2 – Вибір файлу для шифрування

Для перевірки чинності сертифікату необхідно вибрати сертифікат зі списку та натиснути «Перевірити» (Рис.10.3). Якщо обраний сертифікат діючий, біля назви файлу з'явиться зелений трикутник. В протилежному випадку, якщо сертифікат не діючий, біля назви файлу з'явиться червоний круг. Після вибору сертифіката одержувача потрібно натиснути "Далі".

Для зашифровування файлів використовується особистий ключ користувача що виконує зашифровування та сертифікат(и) користувача(ів) для якого(их) зашифровується файл.

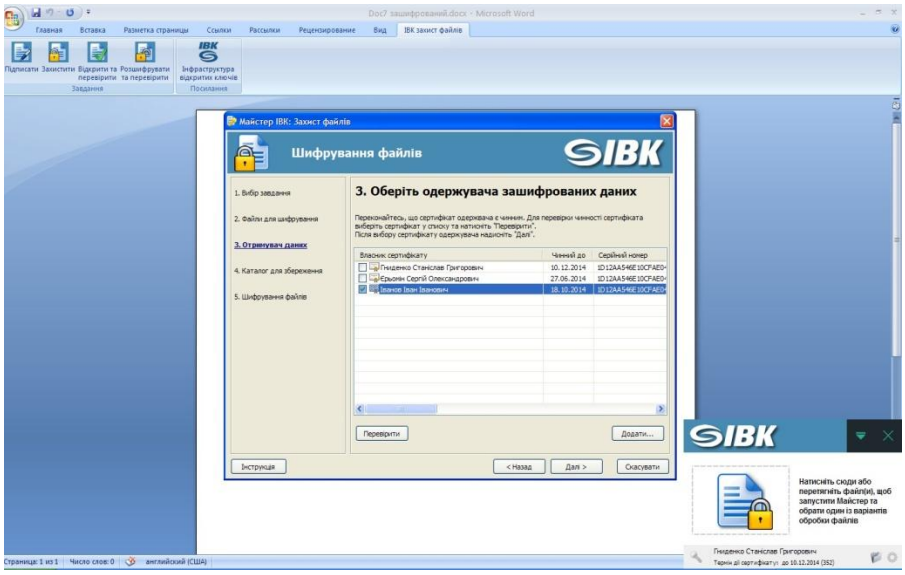


Рисунок 10.3 – Вибір одержувача зашифрованих даних

Наступна сторінка (Рис.10.4) дає можливість вказати каталог для збереження зашифрованих файлів. Для вибору каталогу слід натиснути «Огляд». За замовчуванням файли зберігаються до папки C:\Мої документи\Захищені\

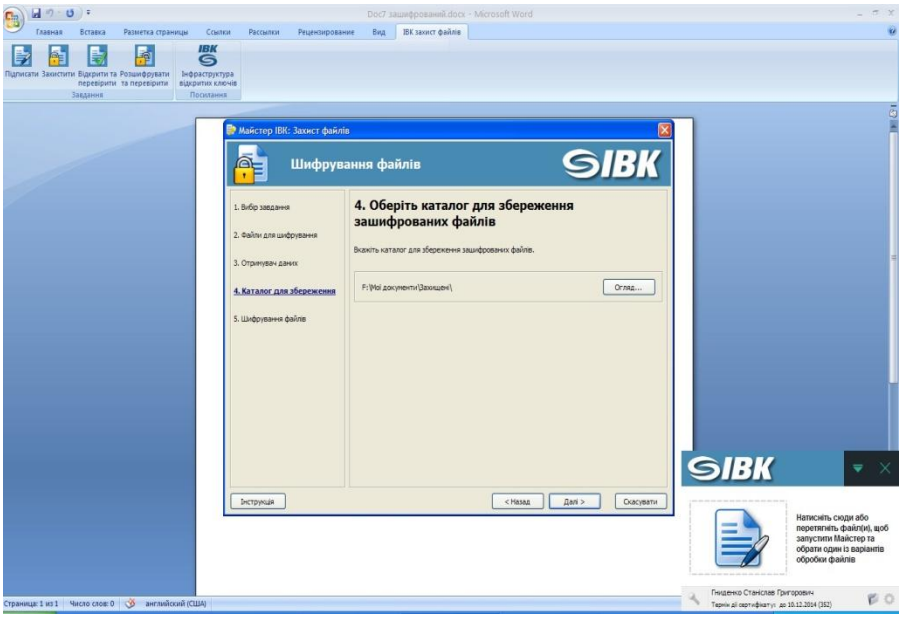


Рисунок 10.4 – Вибір каталогу для збереження підписаних файлів

Наступна сторінка (Рис.10.5.) дає можливість додатково підписати обрані файли «Додатково підписати». За замовчуванням здійснюється лише зашифровування кожного файлу. Вихідні зашифровані файли мають розширення “.p7e”. Зашифровані файли будуть збережені до обраного вами каталогу. Для шифрування потрібно натиснути “Зашифрувати”.

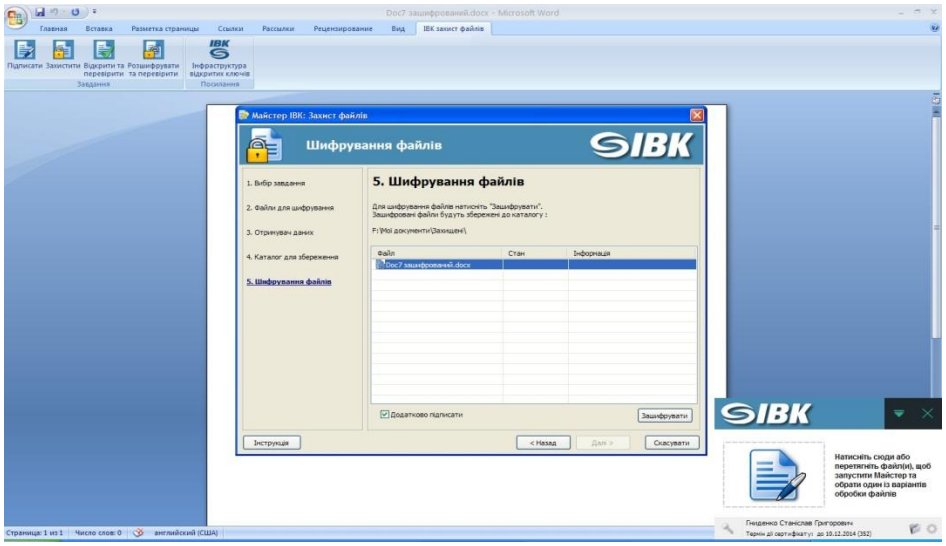


Рисунок 10.5 – Шифрування файлів

Шифрування здійснюється (Рис.10.6) на основі особистого ключа користувача. Доступ до ключа користувача здійснюється після вводу паролю доступу. Ввівши пароль потрібно натиснути «Зчитати».

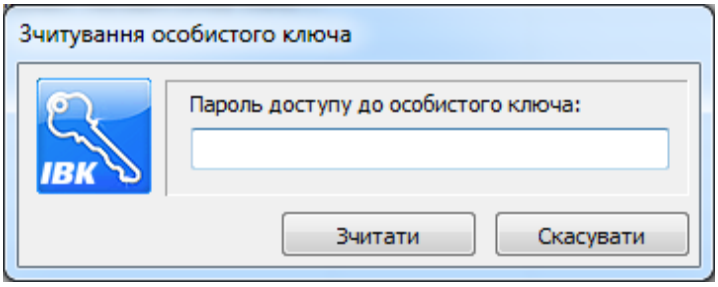


Рисунок 10.6 – Зчитування особистого ключа

Зашифровані файли будуть збережені до обраного каталогу. У разі вдалого шифрування (Рис.10.7) в таблиці навпроти файлу буде вказано статус файлу «Зашифровано». У разі помилки зашифровування, відповідна інформація буде відображена в таблиці стану документу.

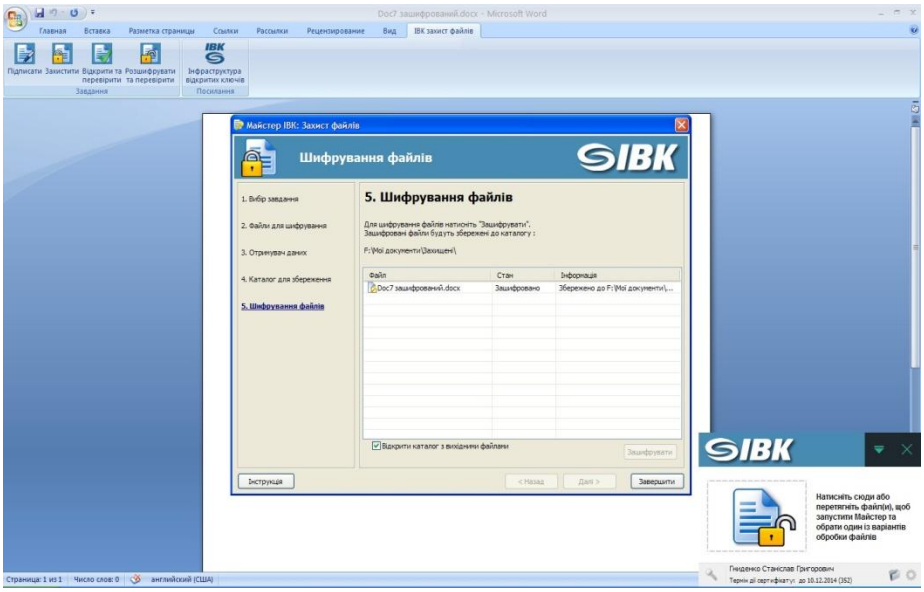


Рисунок 10.7 – Стан зашифрованого файлу

Для перегляду каталогу з зашифрованими файлами (Рис.10.8), потрібно натиснути кнопку «Завершити», після чого відкриється каталог з зашифрованими файлам.

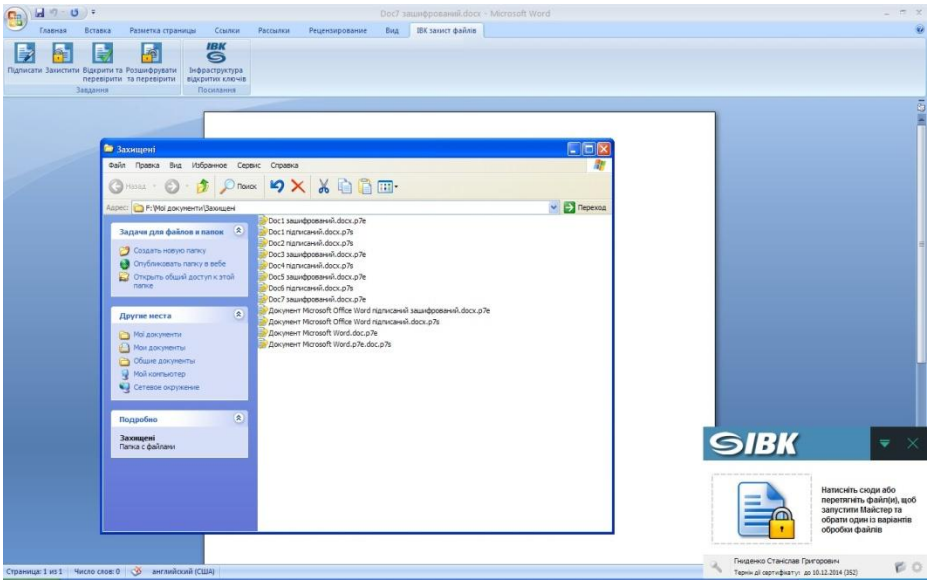


Рисунок 10.8 – Каталог з зашифрованими файлами

<<Назад

11. ВІДКРИТИ ТА ПЕРЕВІРИТИ

В каталозі «Захищені» обираємо зашифрований файл (Рис. 11.1)

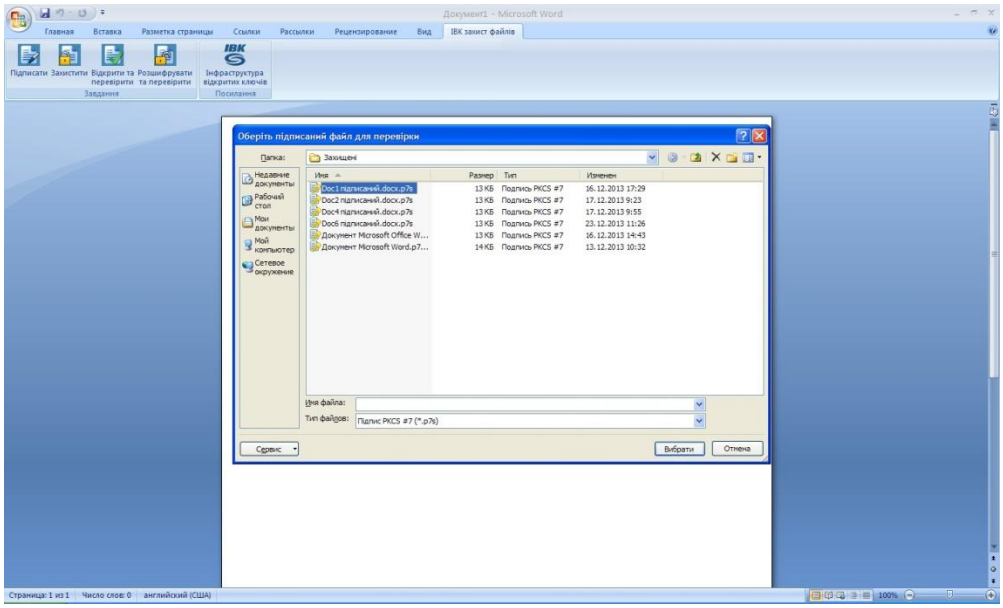


Рисунок 11.1 – Каталог з зашифрованими файлами

На наступній сторінці погоджуємось з повідомленням (Рис. 11.2)

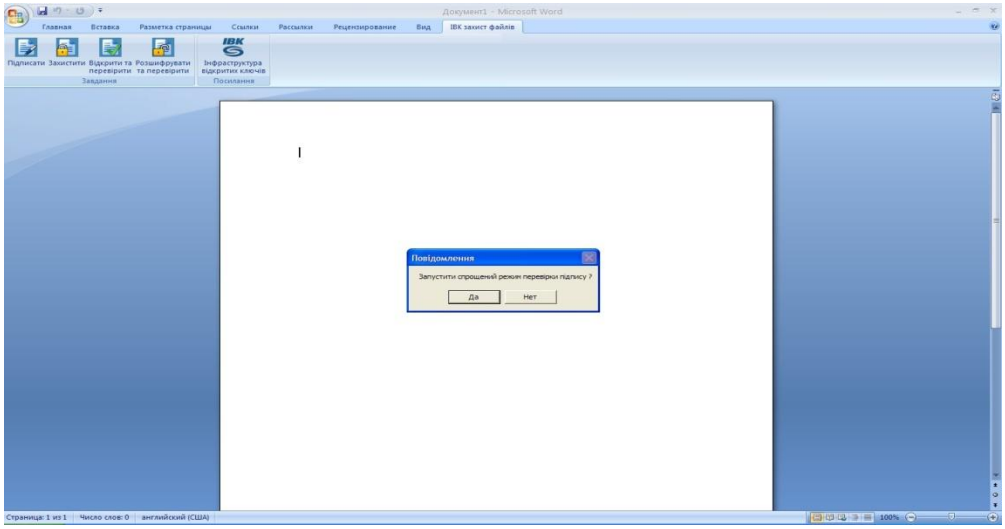


Рисунок 11.2 – Вибір спрощеного режиму перевірки підпису

На наступній сторінці (Рис.11.3) необхідно натиснути «Перевірити». Після перевірки підпису файли будуть збережені до обраного каталогу.

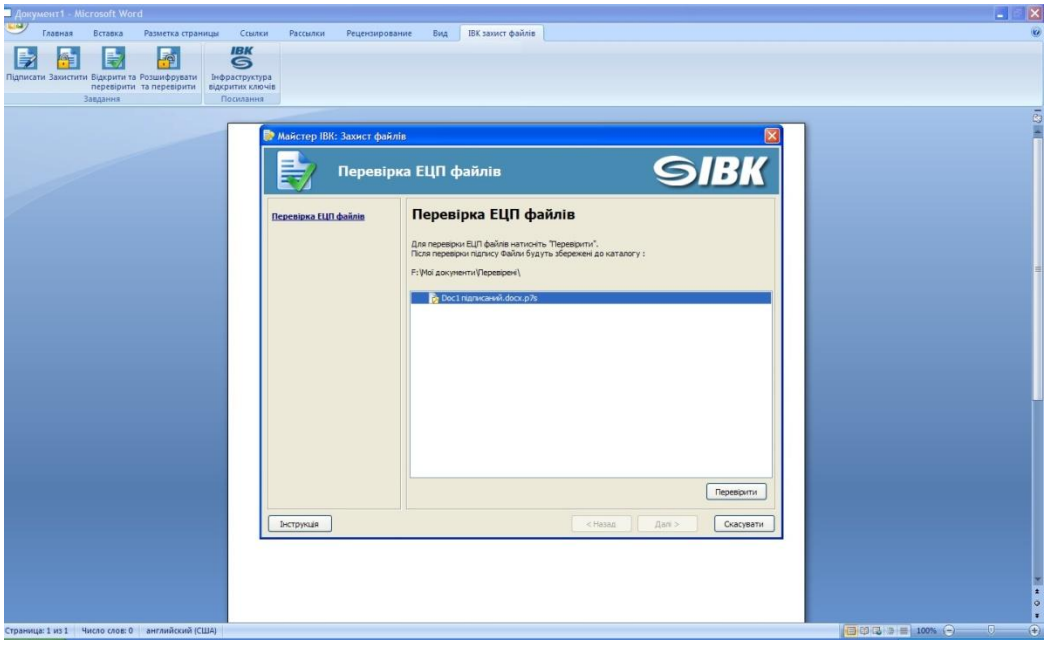


Рисунок 11.3 – Перевірка ЕЦП файлів

Для перевірки ЕЦП файлів необхідно натиснути кнопку «Перевірити». Після перевірки підпису файли будуть збережені до каталогу Мої документи\Перевірені\

Для відкриття перевіреного файлу, потрібно його вибрати та натиснути кнопку «Відкрити» (Рис.11.4)

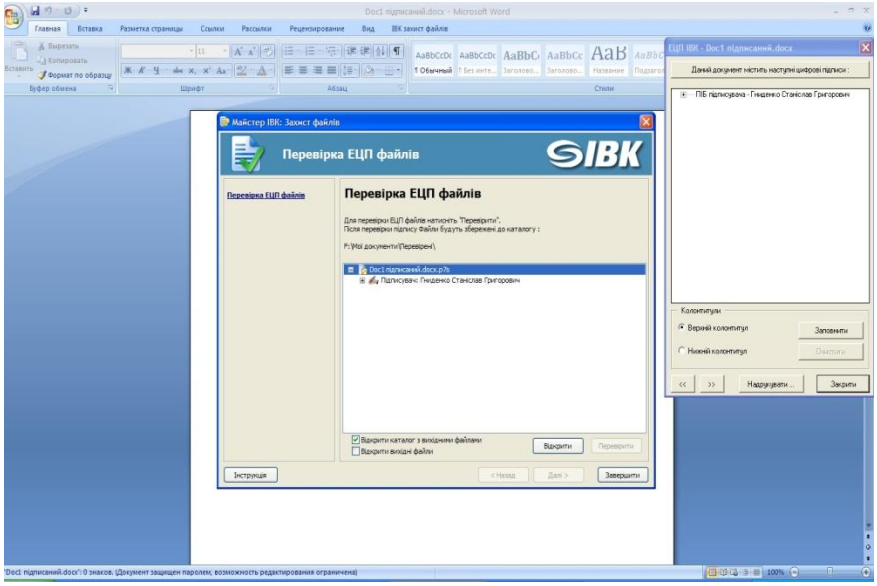


Рисунок 11.4 – Відкриття перевіреного файлу

Вікно зображене на (Рис. 11.5) містить інформацію про підписувача, надає можливості обирати колонтитули

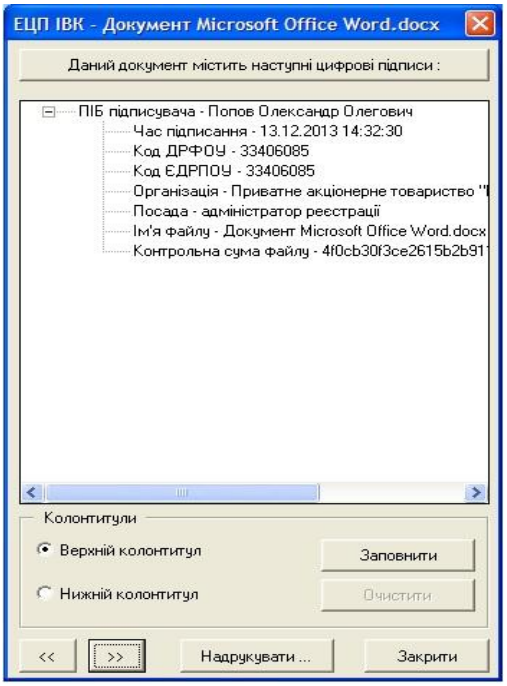


Рисунок 11.5 – Інформація про підписувача

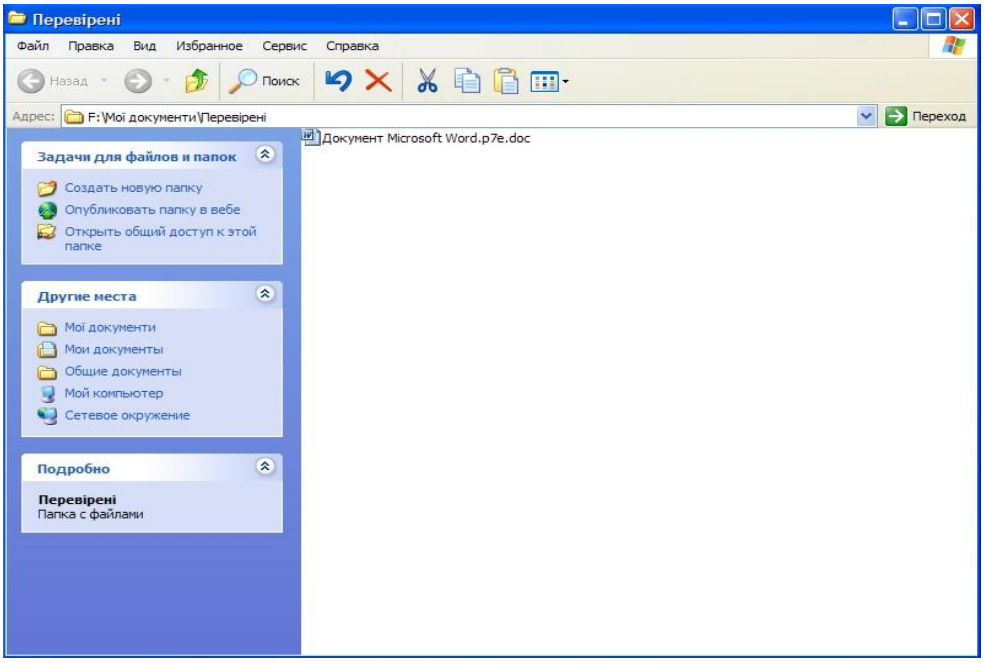


Рисунок 11.5 – Каталог з перевіреними файлами

<<Назад

12. РОЗШИФРУВАТИ ТА ПЕРЕВІРИТИ

В каталозі «Захищені» обираємо зашифрований файл (Рис.12.1)

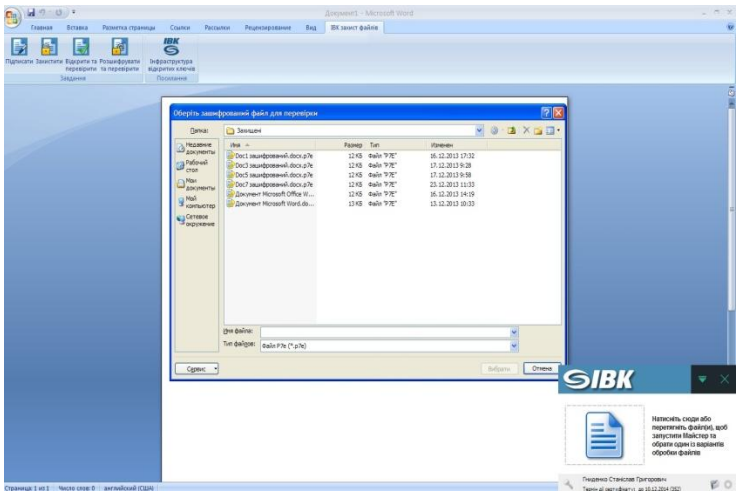


Рисунок 12.1 – Каталог з зашифрованими файлами

На наступній сторінці погоджуємось з повідомленням (Рис. 12.2)

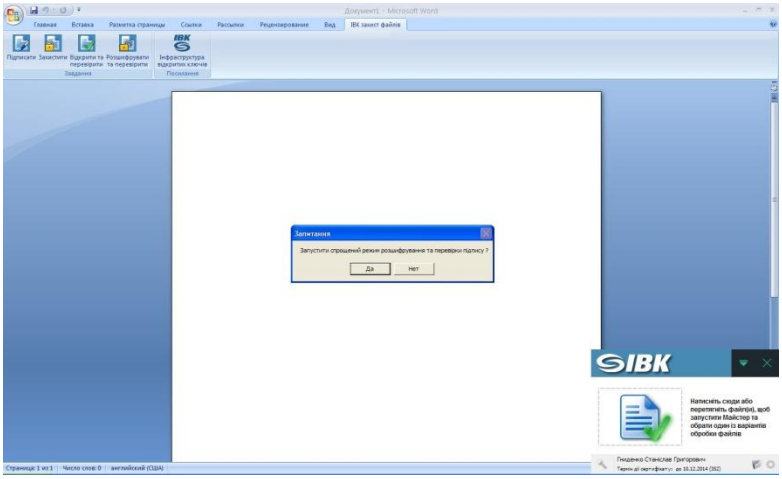


Рисунок 12.2 – Вибір спрощеного режиму перевірки підпису

На наступній сторінці (Рис.12.3) для розшифрування файлів необхідно натиснути «Розшифрувати». Розшифровані файли будуть збережені до обраного каталогу Мої документи\Перевірені\

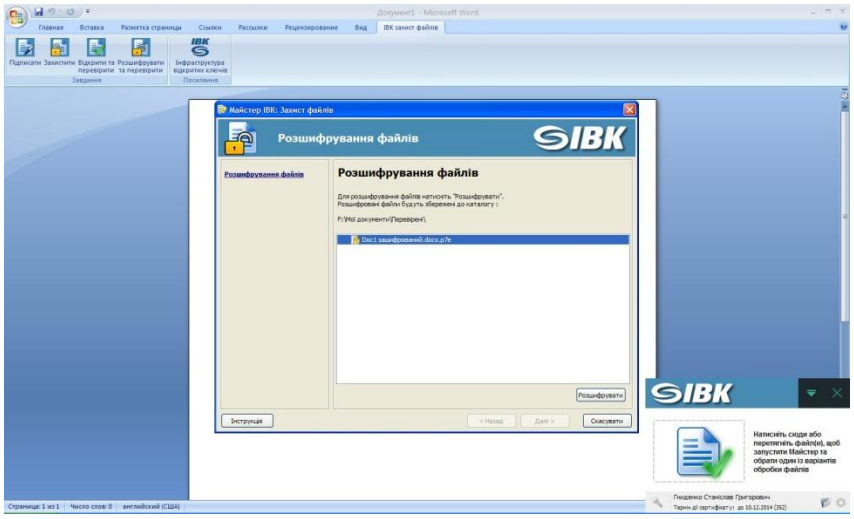


Рисунок 12.3 – Розшифрування файлів

Розшифрування файлу (Рис.12.4) здійснюється на основі особистого ключа користувача. Доступ до ключа користувача здійснюється після вводу паролю доступу. Ввівши пароль потрібно натиснути «Зчитати».

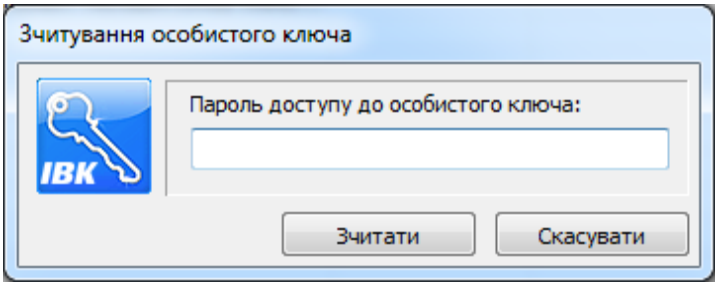


Рисунок 12.4 – Зчитування особистого ключа

Для перегляду каталогу з розшифрованими файлами, потрібно натиснути кнопку «Завершити»(Рис.12.5), після чого відкриється каталог з розшифрованими файлам(Рис.12.6).

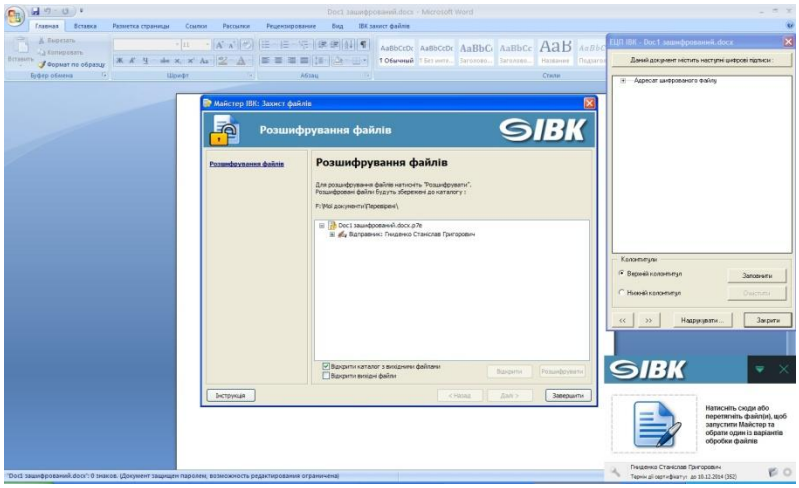


Рисунок 12.5 – Завершення розшифрування файлів

Вікно зображене на (Рис. 12.6) містить інформацію про підписувача, надає можливості обирати колонтитули

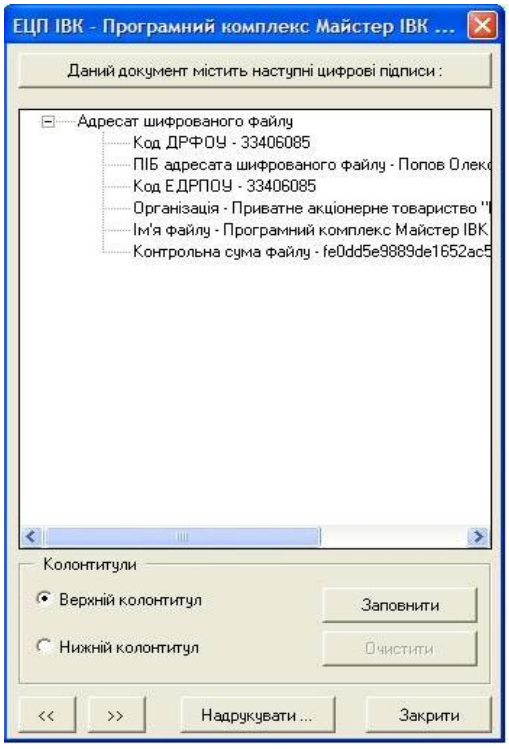


Рисунок 12.6 – Інформація про підписувача

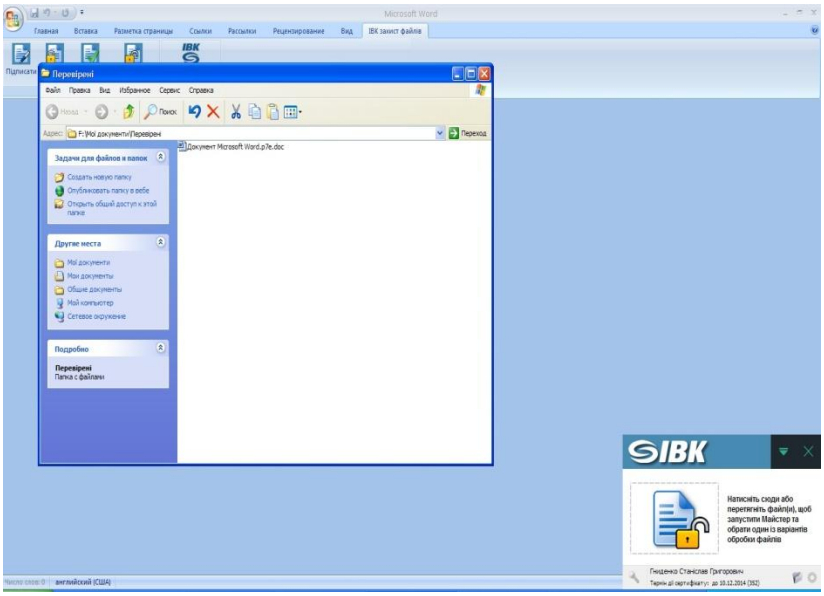


Рисунок 12.6 – Каталог з розшифрованими файлами

<<Назад

ПЕРЕЛІК СКОРОЧЕНЬ

ОС	Операційна система
ЕОТ	Електронно-обчислювальна техніка
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
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

<<Назад

ДОДАТОК А

функціональна схема взаємодії з програмно-технічним комплексом цск

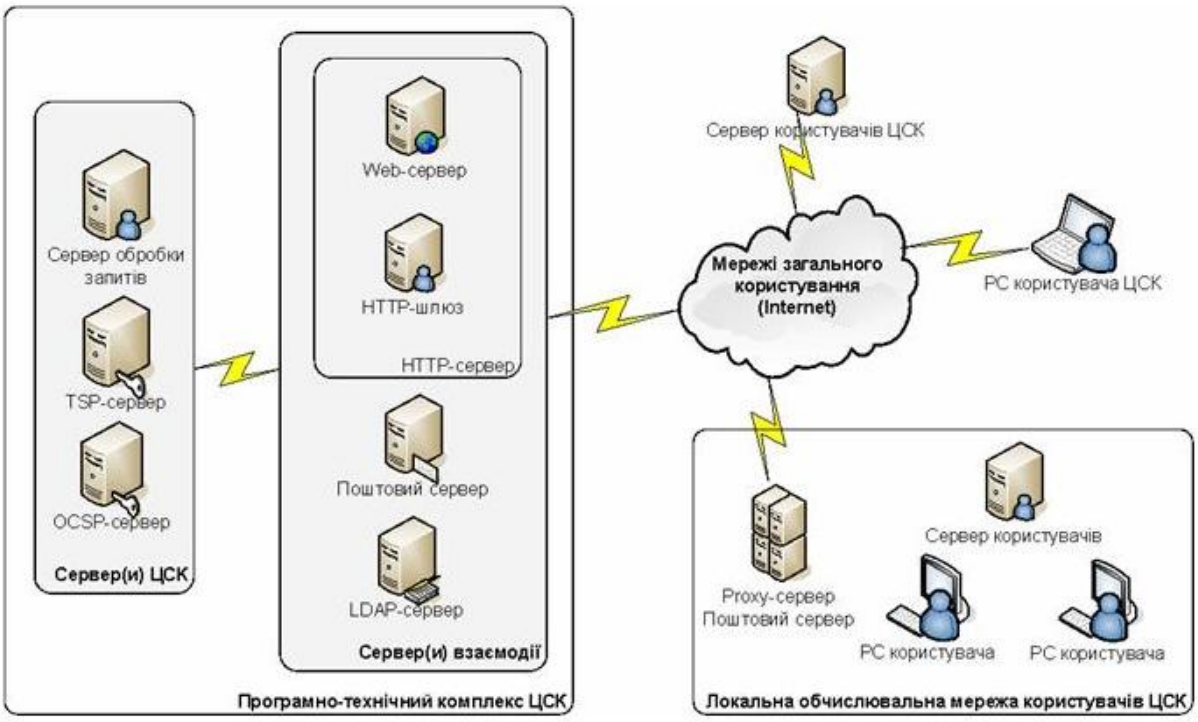


Схема А1

<<Назад