ЗАТВЕРДЖЕНИЙ
АЧСА.32248356.00182-01 96 01-ЛУ

Ключ електронний "Secure Token-337F"

Програмне забезпечення.
Утиліти
"CryptoFlashManager"
і "CryptoFlash"

АЧСА.32248356.00182-01 96 01

Настанова користувача

Аркушів 25

2014

Зміст

1. Вступ

Документ містить опис управляючого програмного забезпечення - утиліт "CryptoFlashManager" і "CryptoFlash", для експлуатації носіїв криптографічної інформації - ключів електронних "Secure Token-337F" (далі - "Secure Token-337F").

1.1 Призначення

Утиліти "CryptoFlashManager" і "CryptoFlash" призначені для управління доступом до даних, що знаходяться в FLASH-пам'яті "Secure Token-337F".

1.2 Сфера застосування

Утиліти "CryptoFlashManager" і "CryptoFlash" працюють на персональних комп'ютерах з операційною системою Windows XP[1]/7/8/8.1 і Windows Server 2000/2003/2008/2012.

1.3 Визначення і скорочення

- НКІ – носій ключової інформації;
- ПК – персональний комп'ютер;
- ЕЦП - електронний цифровий підпис;
- АЦСК – акредитований центр сертифікації ключів;
- ОС - операційна система.

2. Опис "Secure Token-337F"

Електронний ключ "SecureToken-337F" — це два пристрої в одному корпусі: електронний ключ "Secure Token-337" і FLASH-пам'ять з логічними дисками для зберігання будь-яких даних користувача.

"SecureToken-337F", як носій ключової інформації, повністю сумісний з електронним ключем "SecureToken-337", застосовується для захищеного зберігання і використання ключів електронного цифрового підпису (ЕЦП) податкової служби України, ключів акредитованих центрів сертифікації ключів (АЦСК) державних і інших організацій, в банківських і корпоративних системах, інтернет-банкінгу і тому подібне. Виконує функції формування і перевірки електронного цифрового підпису, шифрування, автентифікації, зберігання секретної (ключової) інформації.

[1] Для роботи програмного забезпечення CryptoFlash під ОС Windows XP необхідний .Net Framework 3.5. За відсутності .Net Framework 3.5 програмне забезпечення CryptoFlash видає повідомлення "Помилка при ініціалізації додатка (0xc0000135)". Для установки .Net Framework 3.5 використовуйте посилання: http://www.microsoft.com/ru-ru/download/details.aspx?id=21

"SecureToken-337F", як пристрій зі вбудованою FLASH-пам'ятью, може використовуватися для зберігання будь-яких даних користувача із захистом від несанкціонованого доступу. Підтримує два типи дискових масивів – відкритий і захищений, загальним об'ємом до 32 Гбайт. Усі дані на захищеному носієві зберігаються в зашифрованому вигляді.

Для зберігання ключів і виконання криптографічних операцій в електронному ключі "SecureToken-337F" використовується смарт-чип P5CC037 компанії NXP Semiconductors . (Сертифікований в ДССЗЗІ України, експертний висновок №05/02/02-810 від 11.03.2013 р.).

2.1 Технічні характеристики "Secure Token-337"

- Генерація і зберігання ключової інформації згідно ДСТУ 4145-2002 (довжина ключа – 163-509 біт) і RSA (довжина ключа – 512-2048 біт);
- Шифрування/розшифрування електронних документів згідно з ДСТУ ГОСТ 28147-2009, DES, 3-DES, AES;
- Формування і перевірка ЕЦП згідно з ДСТУ 4145-2002 (довжина ключа – 163-509 біт) і RSA (довжина ключа – 512-2048 біт);
- Обчислення геш-кодування-функцій згідно з ГОСТ 34.311-95, MD5, SHA;
- Реалізація схеми автентифікації згідно з ISO 9798-3;
- Об'єм пам'яті 36 Кбайт.

2.2 Технічні характеристики FLASH-пам'яті

- Об'єм пам'яті: 4, 8, 16 або 32 Гбайт;
- Швидкість читання/запису даних на відкритому диску, не менше 5 Мбайт/с;
- Швидкість читання/запису даних на захищеному диску і алгоритми шифрування:

Алгоритм шифрування даних FLASH-пам'яті	ДСТУ ГОСТ 28147-2009	AES	RC5
Довжина ключа, біт	256	128	128
Швидкість читання/запису даних, не менше, Мбайт/с	0,4	0,8	1,7

2.3 Підтримувані інтерфейси і стандарти

- USB 2.0 High-speed;
- Windows PC/SC;
- Microsoft CCID;
- USB Mass Storage.

"SecureToken-337F" підтримує роботу з наступними операційними системами (ОС): Windows XP/2003/2008/Vista/7/8, Linux, Mac OS.

Вся FLASH-пам'ять пристрою "SecureToken-337F" ділиться на два логічні диски - відкритий диск і захищений диск.

Відкритий диск – це диск загального призначення, що використовується для зберігання даних у відкритому вигляді з можливістю установки обмеження на запис.

Захищений диск - це закритий диск користувача, дані на якому зберігаються в зашифрованому вигляді, а доступ організовується по паролю. У початковому стані захищений диск не створений (стан «витягнений») і, залежно від установок в ОС, може взагалі не відображуватися системою або відображуватися як порожній диск.

Створений захищений диск може знаходитися в одному з наступних станів: "витягнений" (стан за умовчанням, після підключення до ПК) або "підключений" (стан після правильного введення пароля). В стані "підключений" дані доступні для використання в звичайному режимі, аналогічно даним на інших логічних дисках.

В процесі ініціалізації захищеного диска активуються пароль і ключове слово і, випадковим чином, генерується секретний ключ для шифрування. Секретний ключ, пароль і ключове слово зберігаються у внутрішній пам'яті мікроконтроллера, що управляє, захищеній від зчитування зовнішніми засобами. Щоб уникнути підбору кодів доступу, кількість спроб введення пароля обмежена 10-ма спробами, кількість спроб введення ключового слова обмежена 5-ма спробами. Після вичерпання всіх спроб ключ, на якому шифруються дані в FLASH-пам'яті, видаляється, і доступ до диска блокується. Після цього, дані, що знаходилися в захищеній області диска, відновити неможливо.

Для зміни основних параметрів FLASH-пам'яті пристрою використовується утиліта "CryptoFlashManager".

Для створення і управління станами захищеного диска використовується утиліта "CryptoFlash".

3. Утиліта "CryptoFlashManager"

Для зміни основних параметрів FLASH-пам'яті пристрою "Secure Token-337F" використовується утиліта "CryptoFlashManager".

За допомогою утиліти можливе управління наступними параметрами:

- вибір мови інтерфейсу утиліт;
- вибір алгоритму шифрування даних на захищеному диску;
- розміри логічних дисків FLASH-накопичувача;
- установка захисту від перезапису відкритого диска.

3.1 Запуск утиліти "CryptoFlashManager"

Для запуску утиліти "CryptoFlashManager" необхідно встановити "Secure Token-337F" у вільний USB-порт. При цьому, в розділі "Мій комп'ютер" або "Цей комп'ютер" має бути виявлений новий дисковий пристрій - відкритий диск "UTILS ST-337F" (рисунок 1).

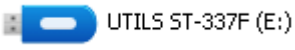


Рисунок 1

На відкритому дисковому пристрої "UTILS ST-337F" знаходяться утиліти для роботи з пристроєм. Для зміни параметрів "Secure Token-337F" необхідно відкрити дисковий пристрій "UTILS ST-337F", вибрати папку "ST337F" і запустити програму "CryptoFlashManager.exe" (рисунок 2).

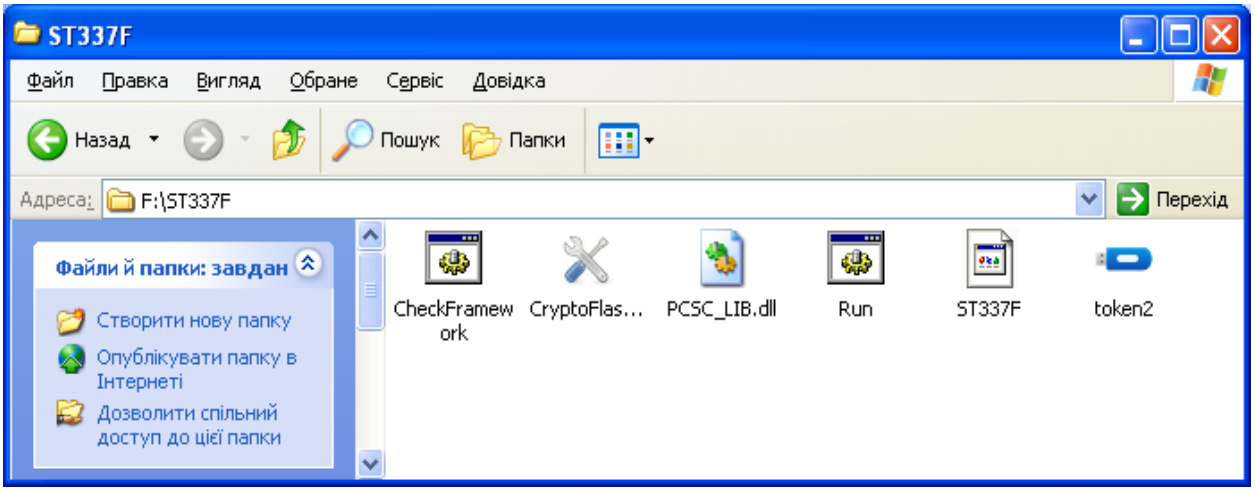


Рисунок 2

При запуску утиліти "CryptoFlashManager" виконується пошук пристрою "Secure Token-337F" і якщо, з якоїсь причини, пристрій не був виявлений, виводиться повідомлення (рисунок 3).

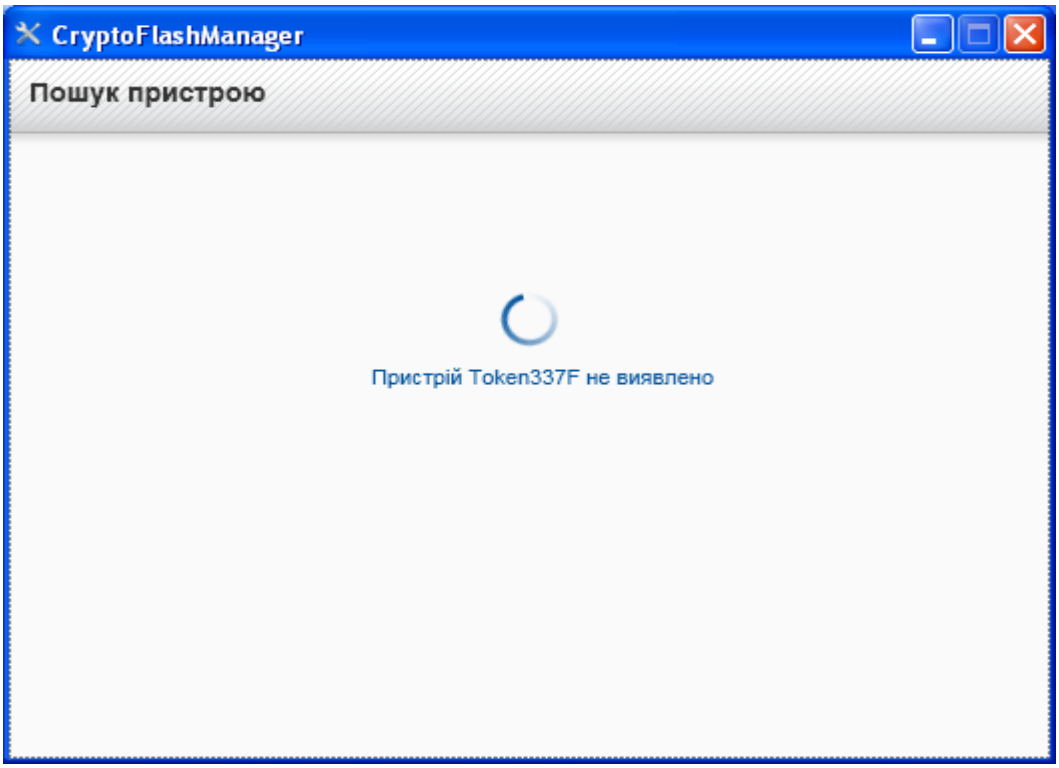


Рисунок 3

При успішному запуску утиліти "CryptoFlashManager" і виявленні пристрою "Secure Token-337F" отримуємо вікно налаштування дисків, рисунок 4.

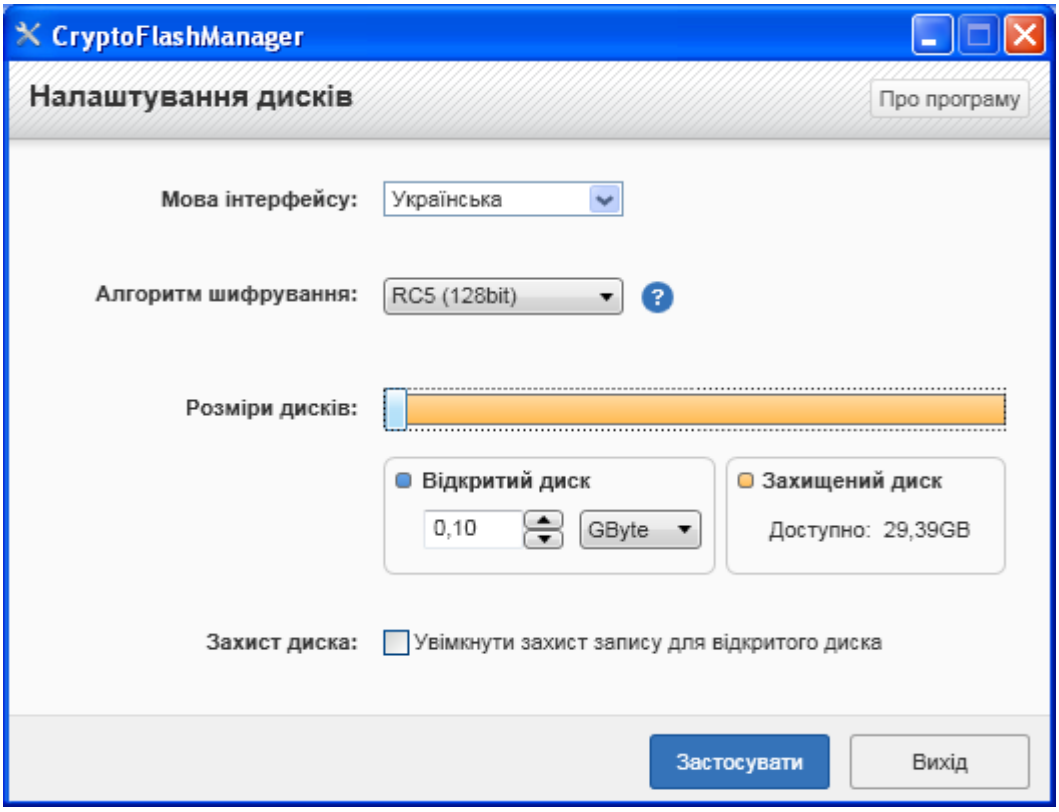
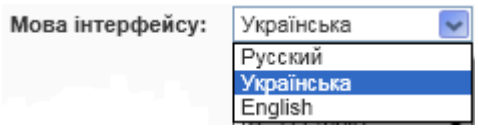


Рисунок 4

3.2 Робота з утилітою "CryptoFlashManager"

З мов інтерфейсу доступні: Українська, Російська, Англійська.



Для створення захищеного диска може бути використаний один з трьох алгоритмів шифрування даних: RC5, AES, GOST.

RC5 – найшвидший з підтримуваних алгоритмів шифрування, у той же час досить крипостійкий алгоритм з довжиною ключа 128 біт.

AES (Advanced Encryption Standard) — алгоритм шифрування прийнятий як стандарт шифрування урядом США. У даному виробі AES використовується з довжиною ключа 128 біт.

GOST (ДСТУ ГОСТ 28147:2009) .— алгоритм шифрування прийнятий як стандарт шифрування в Україні з довжиною ключа 256 біт.

Flash-пам'ять, вбудована в пристрій "Secure Token-337F", за умовчанням розбита на два логічні диски "Відкритий диск" і "Захищений диск".

Користувач має можливість змінювати розміри "Відкритого диска" і "Захищеного диска" за допомогою повзунка "Розміри дисків". Мінімальний розмір "Відкритого диска" або "Захищеного диска" не може бути менше 5 Мбайт, рисунок 5.

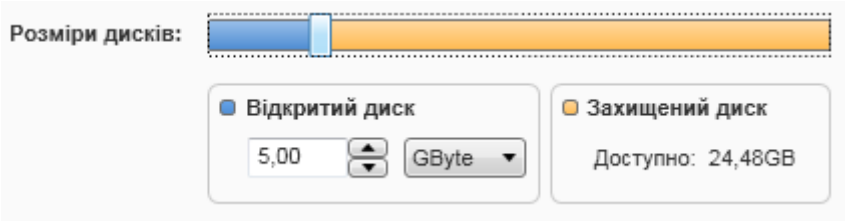


Рисунок 5

Для точного задання розмірів дисків необхідно вибрати розмірність відкритого диска GByte (Гігабайти) або MByte (Мегабайти), за умовчанням GByte, кликнути курсором на полі введення розміру відкритого диска, вручну ввести потрібне значення і натиснути клавішу «Enter», рисунок 6.

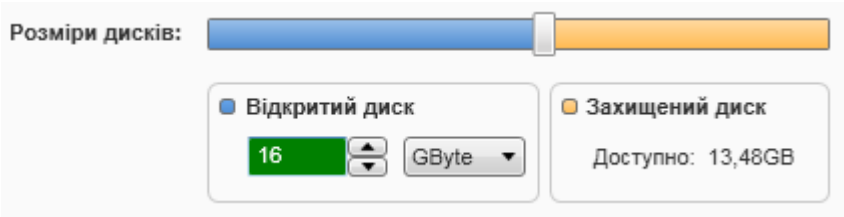


Рисунок 6

Якщо користувачеві не потрібний відкритий диск, а необхідний лише захищений диск на весь об'єм FLASH-пам'яті, то розмір відкритого диска задається як 0 Мбайт, повзунок "Розміри дисків" в крайньому лівому положенні (рисунок 7).

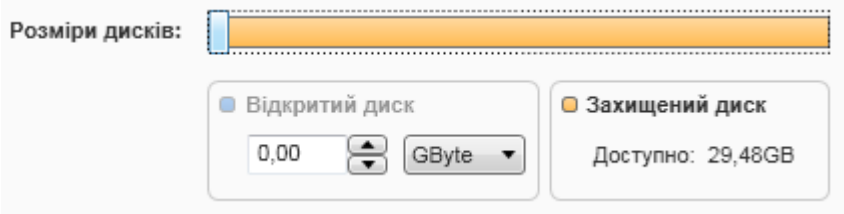


Рисунок 7

Якщо користувачам в роботі не потрібний захищений диск, вони можуть створити лише відкритий диск на весь об'єм FLASH-пам'яті; для цього повзунок "Розміри дисків", необхідно перевести в крайнє праве положення (рисунок 8).

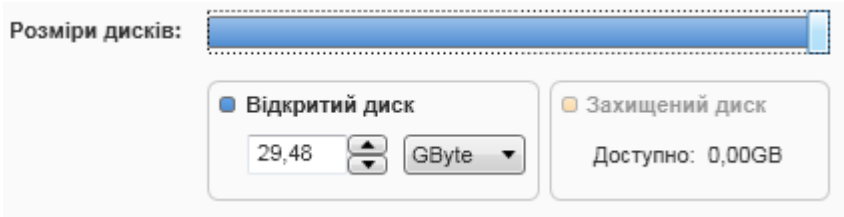


Рисунок 8

Якщо у користувача є необхідність в захисті відкритого диска від запису/зміни/видалення файлів, то користувач повинен установити прапорець на розділі "Захист диска", рисунок 9. Це дозволяє захистити дані від шкідливої дії вірусів, наприклад у випадках, коли пристрій використовується на "чужому" комп'ютері.

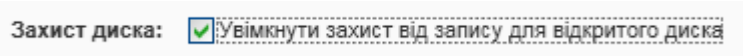


Рисунок 9

3.3 Застосування параметрів утиліти «CryptoFlashManager»

Для збереження змінених параметрів пристрою "Secure Token-337F" необхідно натиснути на кнопку "Застосувати". Пристрій збереже у внутрішній пам'яті управляючого мікроконтроллера змінені параметри і, якщо необхідно, буде запропоновано відключити пристрій від USB (рисунок 10) для вживання нових параметрів.

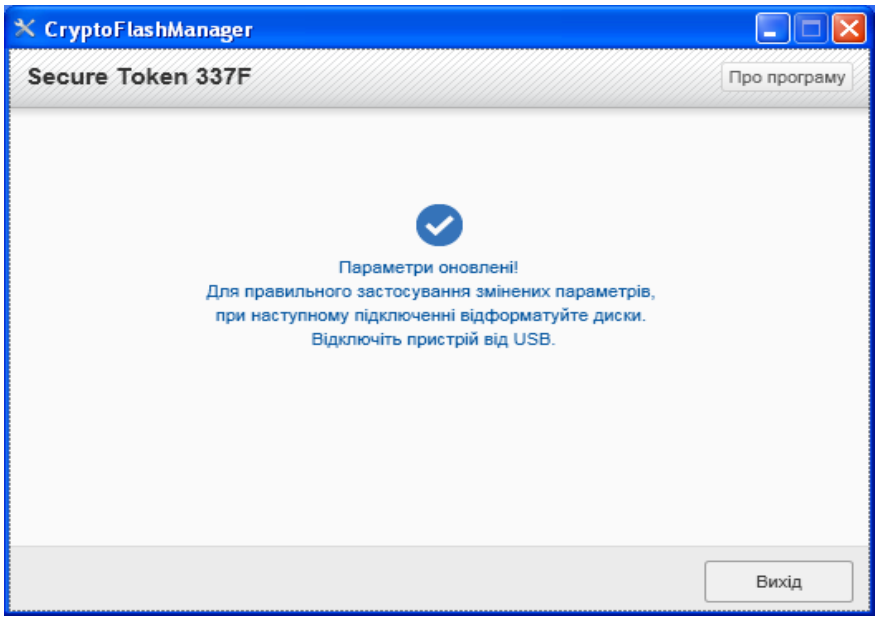


Рисунок 10

Після повторного підключення пристрою необхідно відформатувати відкритий диск "UTILS ST-337F", заздалегідь при цьому зберегти з нього всю інформацію.

УВАГА! Після зміни розмірів відкритого і захищеного диска пристрою "Secure Token-337F" Windows неправильно визначатиме розмір відкритого диска до його переформатування. Windows орієнтується на розмір диска по його попередньому форматуванню.

Форматувати відкритий диск допустимо в будь-якій файловій системі (FAT, FAT32, NTFS, extFAT), за умовчанням FAT32, рекомендуємо вказати мітку тому і вибрати спосіб форматування "Швидке", рисунок 11.

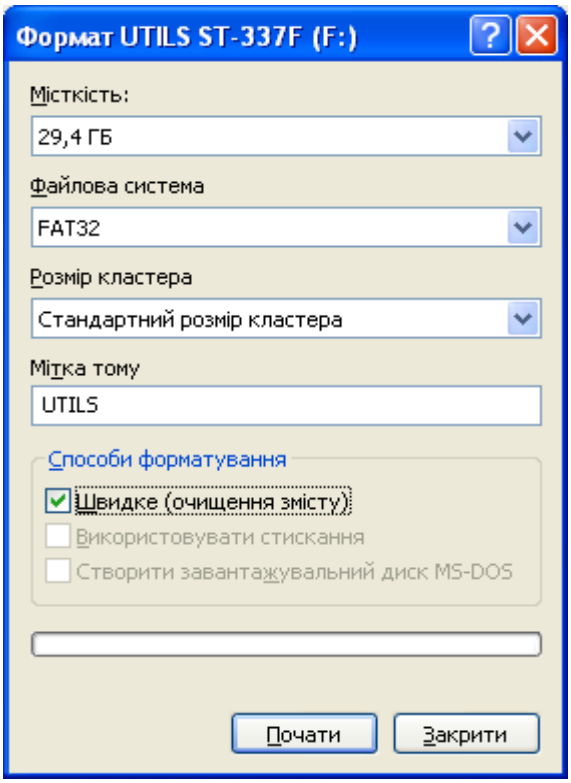


Рисунок 11

Після форматування, для зручності використання утиліт, рекомендуємо відновити дані на відкритому диску "UTILS ST-337F"

3.4 Інформація про утиліту

Аби отримати відомості про утиліту і версію прошивки "Secure Token-337F" (рисунок 12), необхідно натиснути кнопку «Про програму».

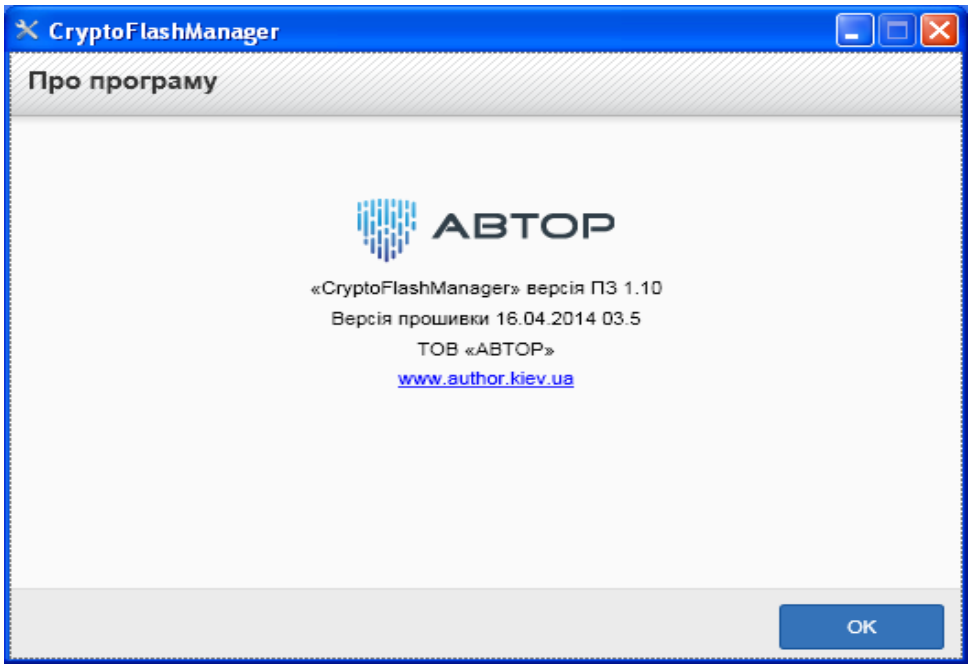


Рисунок 12

4. Утиліта "CryptoFlash"

Для управління станами "Secure Token-337F" використовується утиліта "CryptoFlash". Якщо у користувача нема необхідності в створенні захищеного диска, то використовувати утиліту "CryptoFlash" не потрібно. В цьому випадку "Secure Token-337F" працюватиме як звичайний USB-флеш-накопичувач, поєднаний з НКІ. Користувачеві буде доступний лише відкритий диск пристрою.

При використанні захищеного диска слід звернути увагу на те, що при втраті пароля і ключового слова до захищеного диска, **дані, що знаходилися на цьому диску, відновити неможливо**.

4.1 Запуск утиліти "CryptoFlash"

Для запуску утиліти "CryptoFlash" необхідно встановити "Secure Token-337F" у вільний USB-порт. При цьому, в розділі "Мій комп'ютер" або "Цей комп'ютер" має бути виявлений новий дисковий пристрій - відкритий диск "UTILS ST-337F" (рисунок 1).

Для створення захищеного диска необхідно відкрити дисковий пристрій "UTILS Token337F" і запустити програму "CryptoFlash.exe" (рисунок 13).

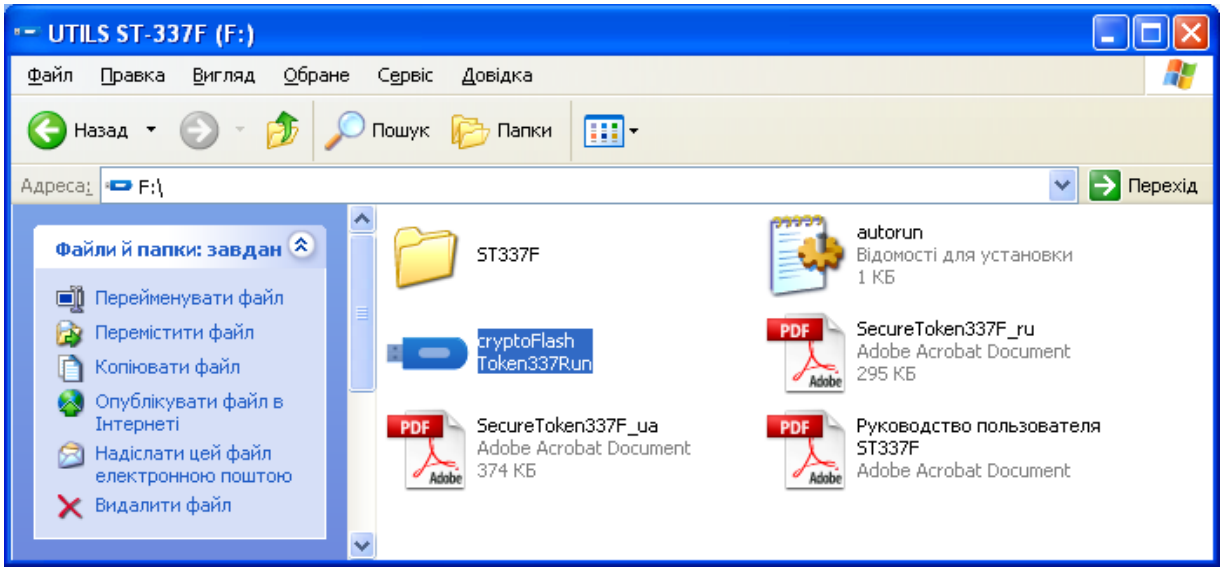


Рисунок 13

При запуску утиліти "CryptoFlash" виконується пошук "Secure Token-337F" і якщо, з якоїсь причини, пристрій не був виявлений, виводитися повідомлення (рисунок 14).

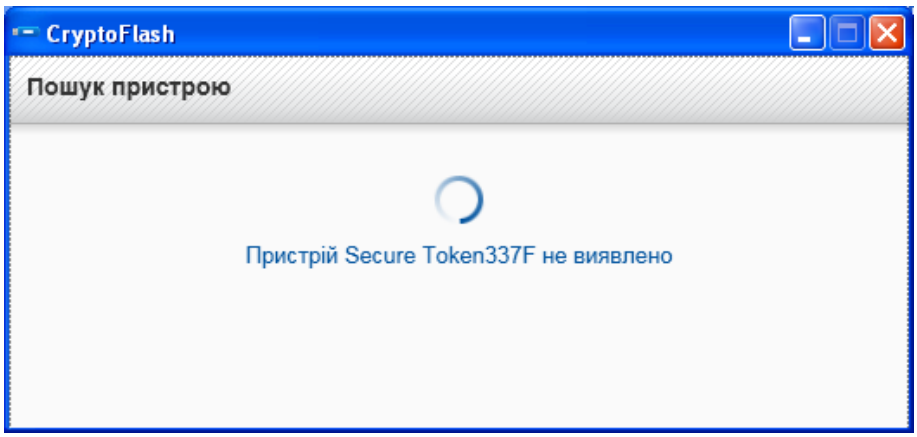


Рисунок 14

При виявленні "Secure Token-337F" на екран виводитися діалогове меню для створення захищеного (закритого) диска, див. Рисунок 15.

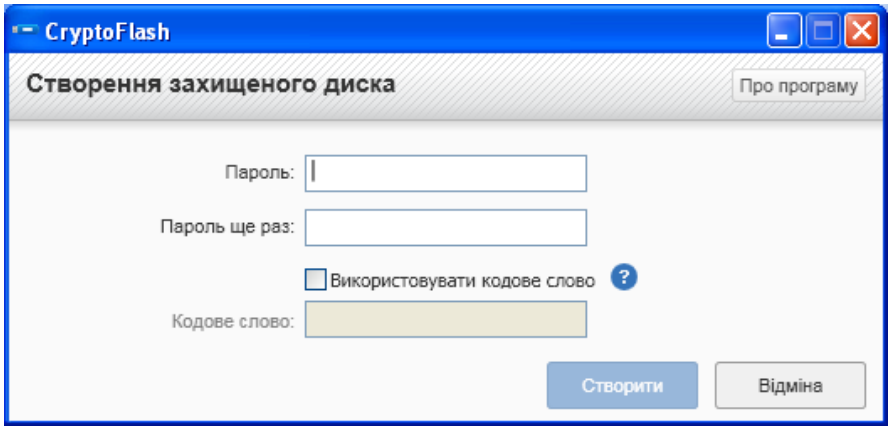


Рисунок 15

4.2 Створення захищеного диска

Для створення захищеного (закритого) диска необхідно задати пароль завдовжки 4-16 символів в полі "Пароль". Цей пароль буде необхідний для доступу до даних на закритому диску після його створення. Пароль може складатися з цифр, символів і букв будь-якого алфавіту доступного на даному ПК. Після введення пароля його необхідно підтвердити, для цього треба ввести його ще раз в полі "Пароль ще раз".

Для можливості відновлення пароля, в разі його втрати, рекомендується скористатися додатковою опцією "Кодове слово"(рисунок 16). По кодовому слову або фразі, при блокуванні диска із-за вичерпання спроб введення пароля, з'являється можливість створити

новий пароль і відновити доступ до даних на захищеному диску. Якщо кодове слово не вводилося і число спроб введення пароля вичерпалося, то дані на захищеному диску будуть безповоротно загублені.

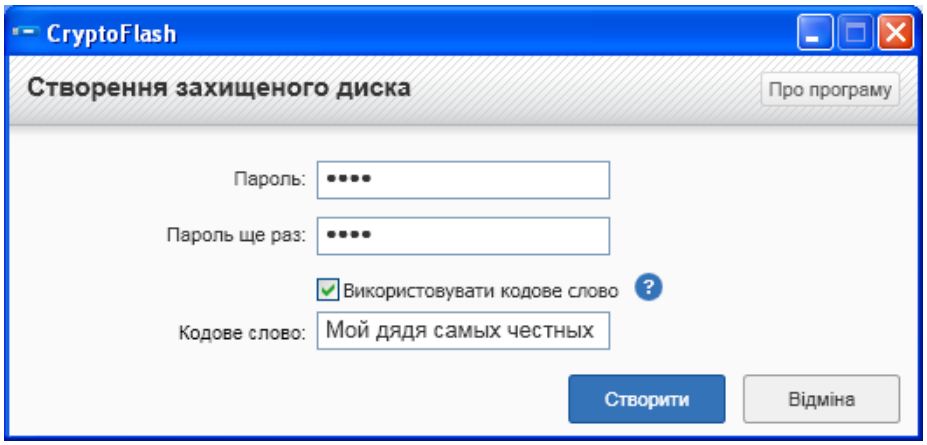


Рисунок 16

Після натискання кнопки "Створити" з'явиться повідомлення про успішне створення захищеного диска (рисунок 17), або про помилку, у випадку неправильної довжини використовуваного пароля (рисунок 18), або про помилку в його підтвердженні (рисунок 19).

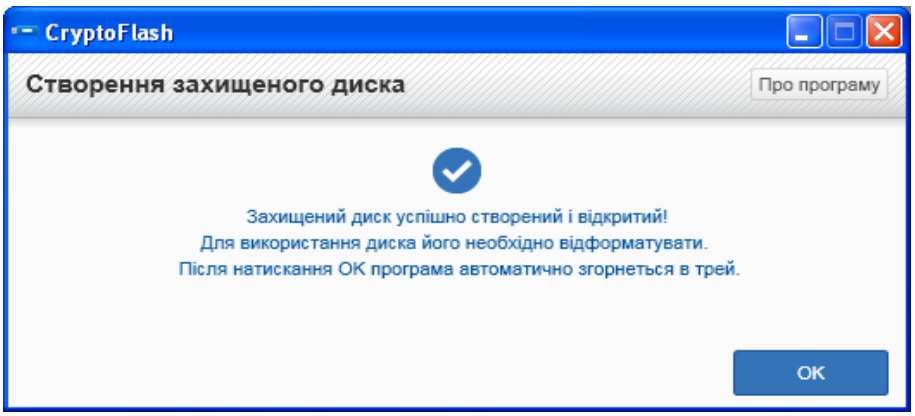


Рисунок 17

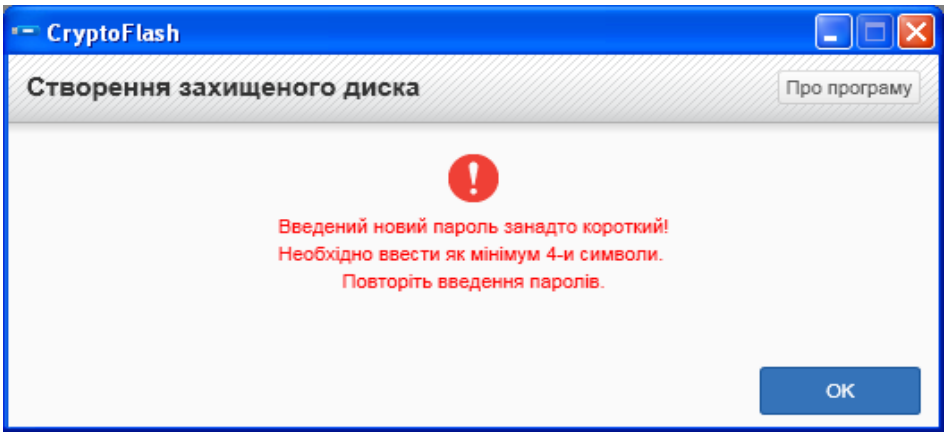


Рисунок 18

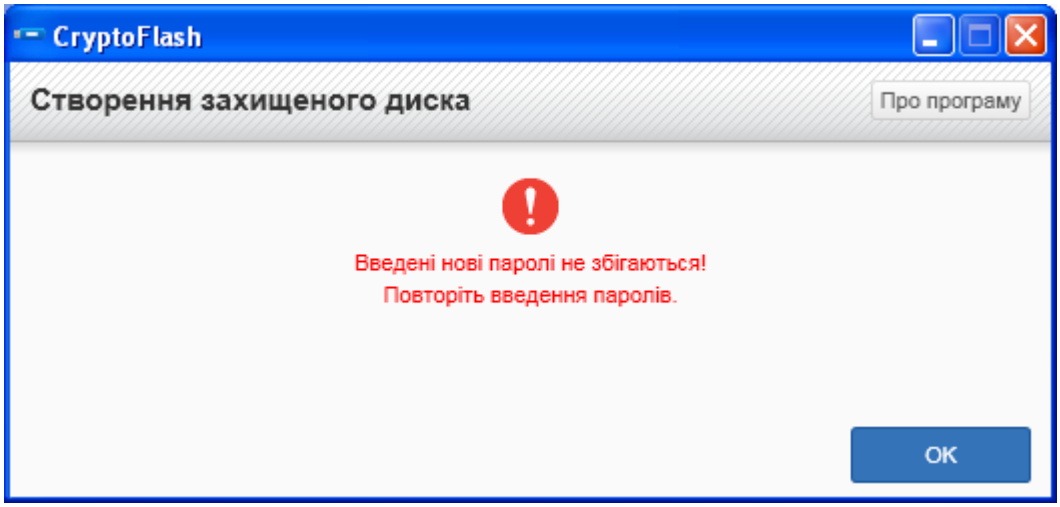


Рисунок 19

При створенні захищеного диска, генерується унікальний ключ для шифрування даних на диску. Після успішного створення захищеного диска операційна система запропонує провести його форматування (рисунок 20).

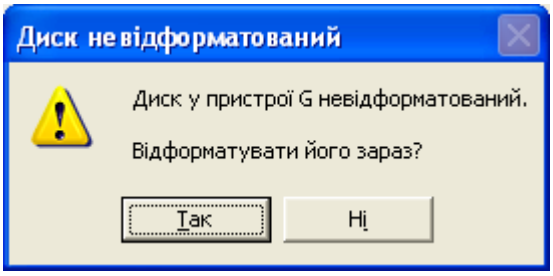


Рисунок 20

Захищений диск необхідно відформатувати в потрібній користувачеві файловій системі FAT, FAT32, NTFS, exFAT. За умовчанням використовується FAT32.

Рекомендується прописати мітку тому і вибрати спосіб форматування "Швидке" (рисунок 21).

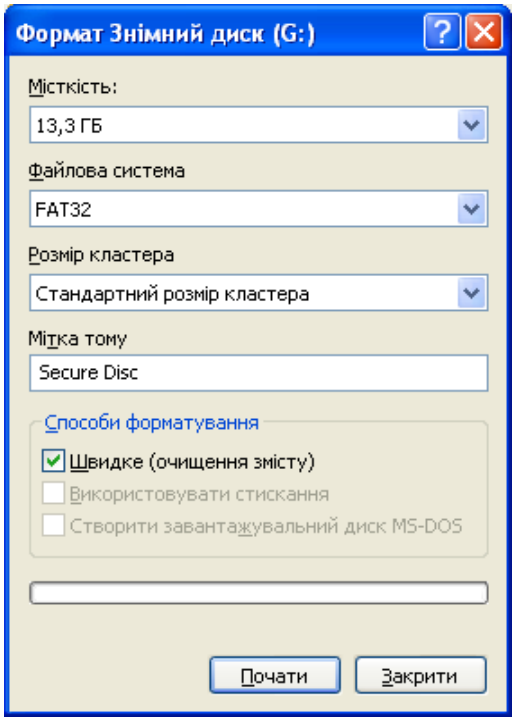


Рисунок 21

Після форматування в системі з'явиться порожній захищений диск.

4.3 Отримання доступу до захищеного диска

При підключенні до ПК пристрою "Secure Token-337F" із створеним захищеним диском необхідно ввести пароль для отримання доступу до захищеного диска (Рисунок 22).

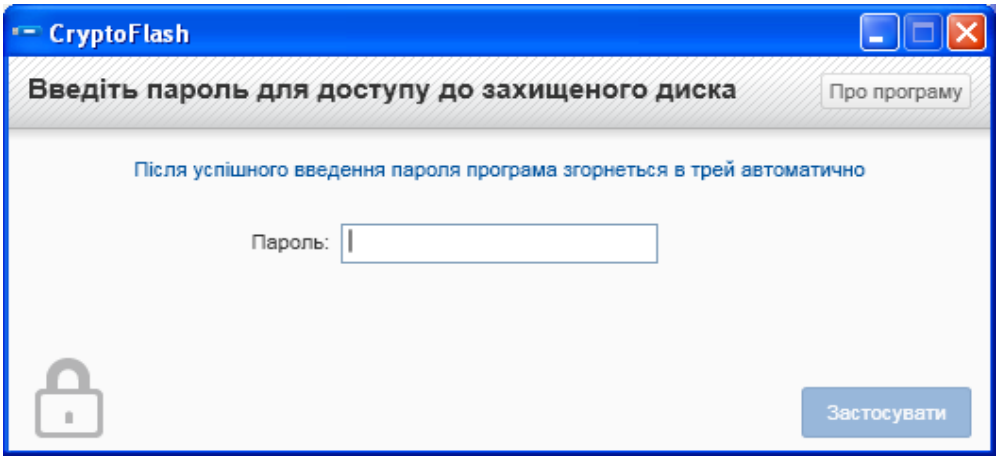


Рисунок 22

При невірному введенні пароля кількість спроб зменшиться (рисунок 23). Після досягнення ліміту спроб неправильного введення пароля, поведінка пристрою визначається пунктом 4.7

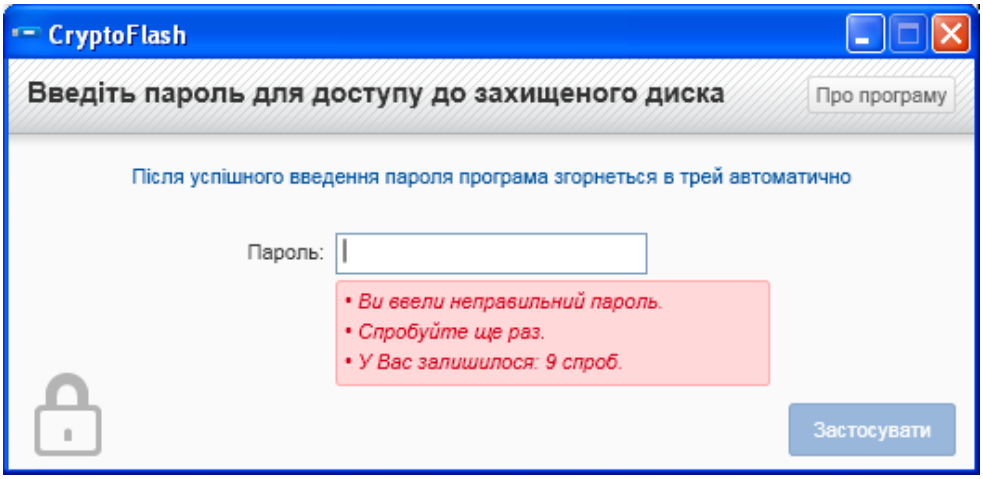


Рисунок 23

Після успішного введення пароля і відкриття захищеного диска з'являється меню «Робота із захищеним диском» (рисунок 24). Це меню дозволяє виконувати операції закриття диска, зміни пароля доступу до захищеного диска, видалення захищеного диска.

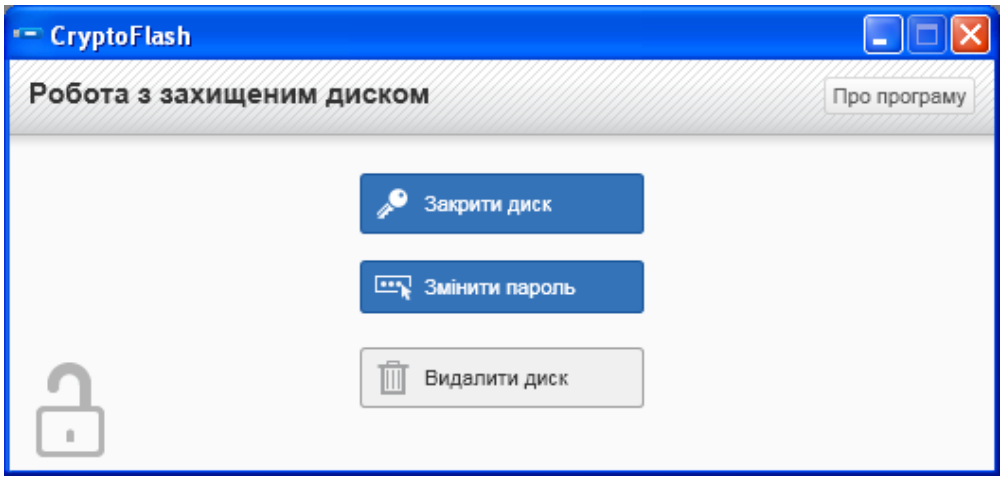


Рисунок 24

4.4 Закриття доступу до захищеного диска

Після завершення роботи із захищеним диском, його можна закрити для доступу (рисунок 24, кнопка "Закрити диск"). З'явиться повідомлення про закриття диска (рисунок 25). При цьому диск або зникне з системи, або відображуватиметься як "порожній" (стан

"Витягнений"). У такому режимі доступ до даних на диску неможливий. Для отримання доступу до диска необхідно повторно ввести пароль (рисунок 22) і натиснути на кнопку "Застосувати".

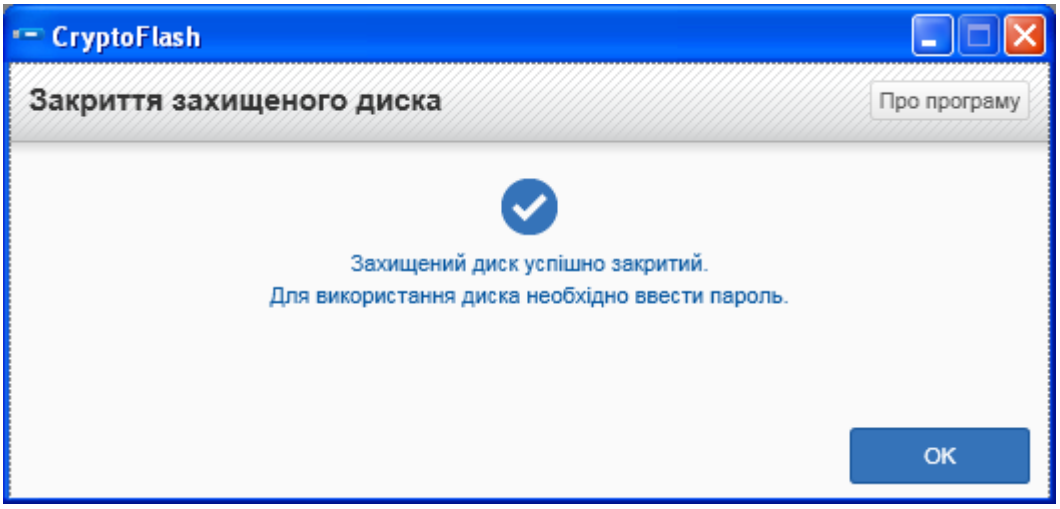


Рисунок 25

Примітка. Витягання пристрою "Secure Token-337F" з USB-порту ПК, не виконавши заздалегідь процедуру закриття захищеного диска, приведе до його автоматичного закриття.

4.5 Зміна пароля доступу до захищеного диска

Існує можливість зміни пароля доступу до захищеного диска (рисунок 24, кнопка "Змінити пароль"). Для цього потрібно ввести старий пароль і новий з підтвердженням (рисунок 26).

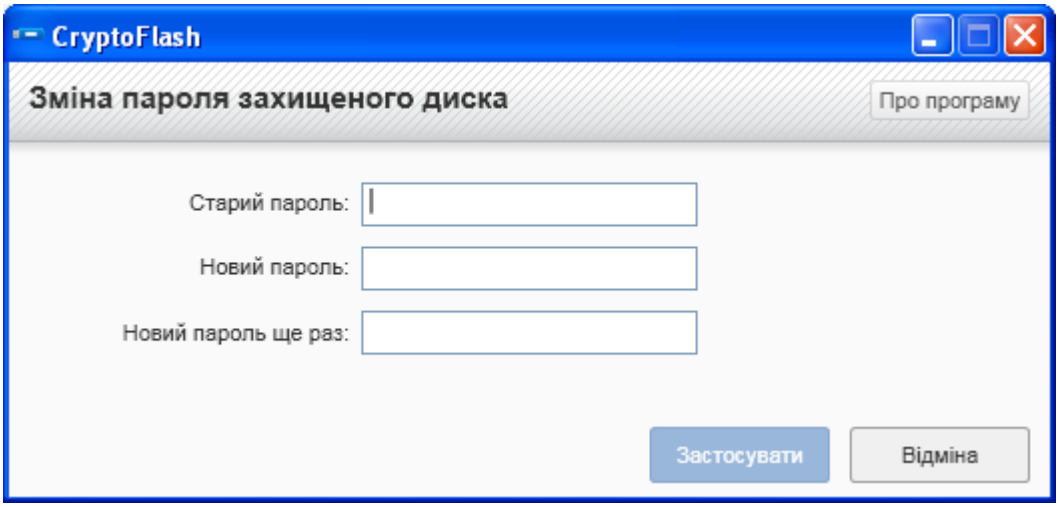


Рисунок 26

При невірному введенні старого пароля кількість спроб зменшиться (рисунок 27). Після досягнення ліміту спроб неправильного введення пароля, поведінка пристрою визначається пунктом 4.7.

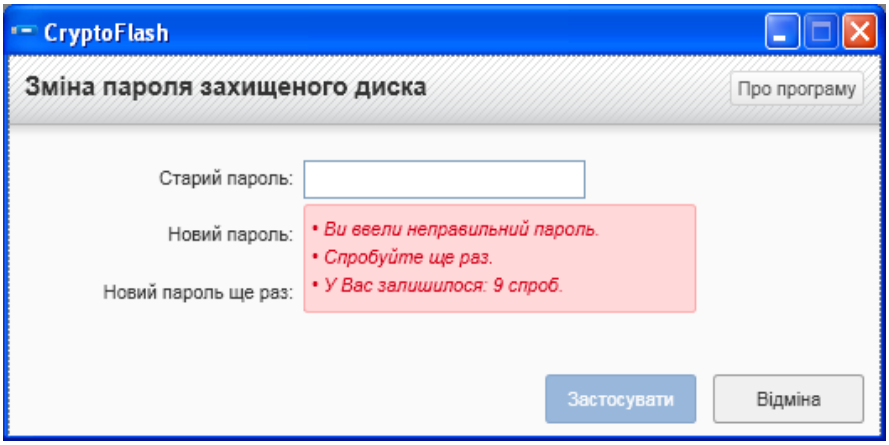


Рисунок 27

Після введення і підтвердження пароля необхідно натиснути кнопку "Застосувати", внаслідок чого з'явиться повідомлення про успішну зміну пароля (рисунок 30), або помилці, в разі неправильної довжини використовуваного пароля (рисунок 28) або помилки в його підтвердженні (рисунок 29).

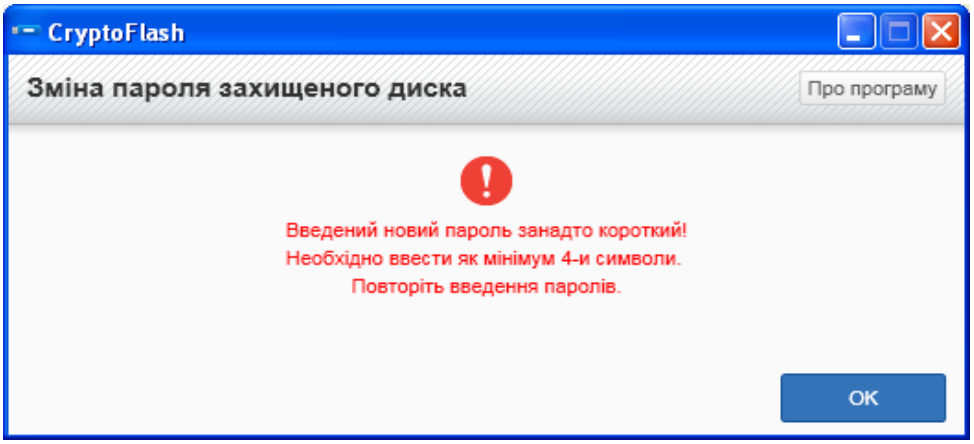


Рисунок 28

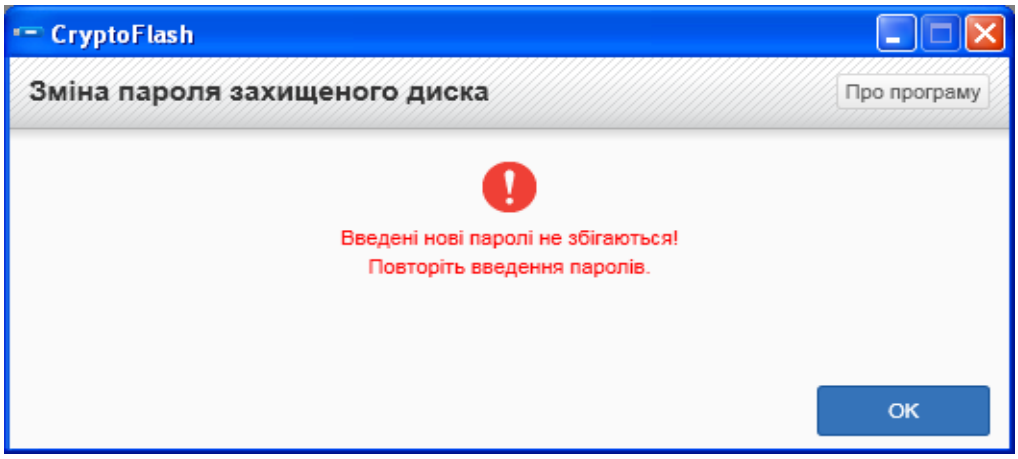


Рисунок 29

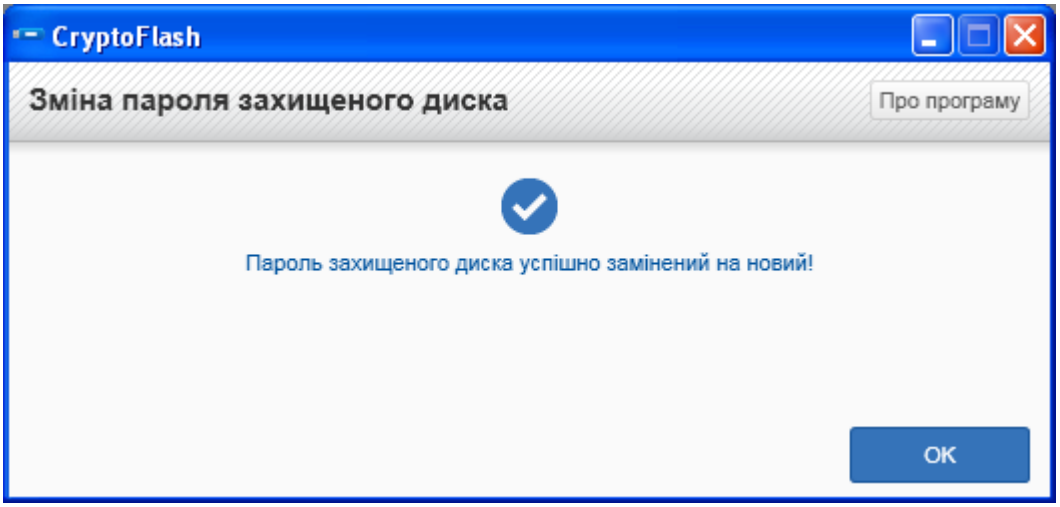


Рисунок 30

4.6 Видалення диска

Для видалення захищеного диска і повернення до незахищеного диска необхідно натиснути кнопку "Видалити диск" (рисунок 24) і перейти в меню "Видалення захищеного диска"(рисунок 31). Для підтвердження видалення захищеного диска необхідно ввести пароль доступу до диска. На рисунку 33 показаний результат успішного виконання процедури видалення захищеного диска.

Увага! При успішному видаленні захищеного диска всі дані, які на ньому знаходилися, будуть безповоротно втрачені!

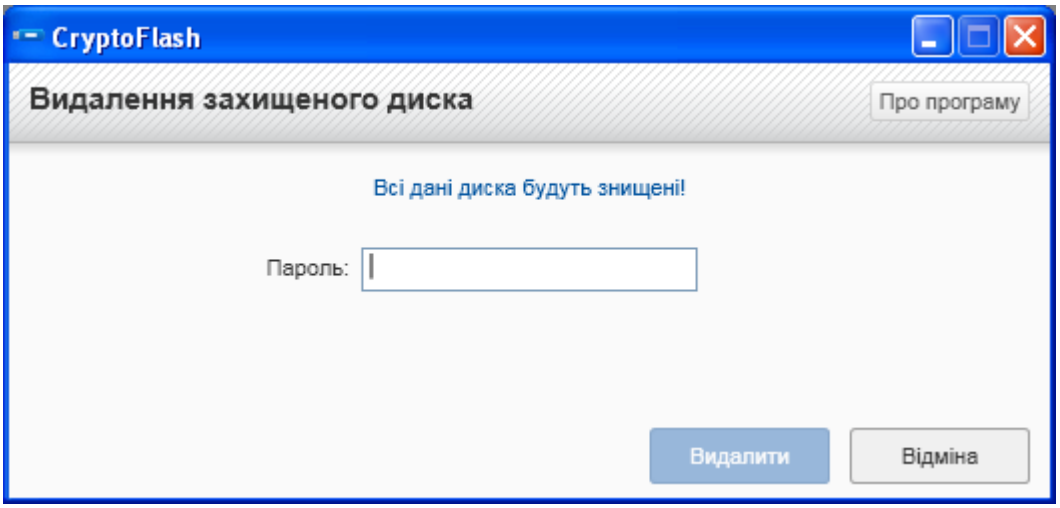


Рисунок 31

При невірному введенні пароля кількість спроб зменшиться (рисунок 32). Після досягнення ліміту спроб неправильного введення пароля, поведінка пристрою визначається пунктом 4.7

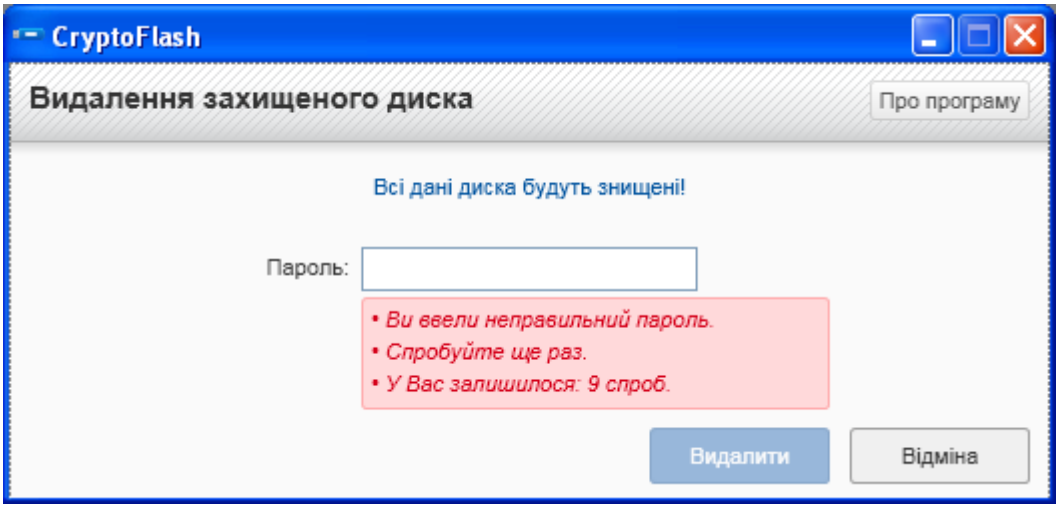


Рисунок 32

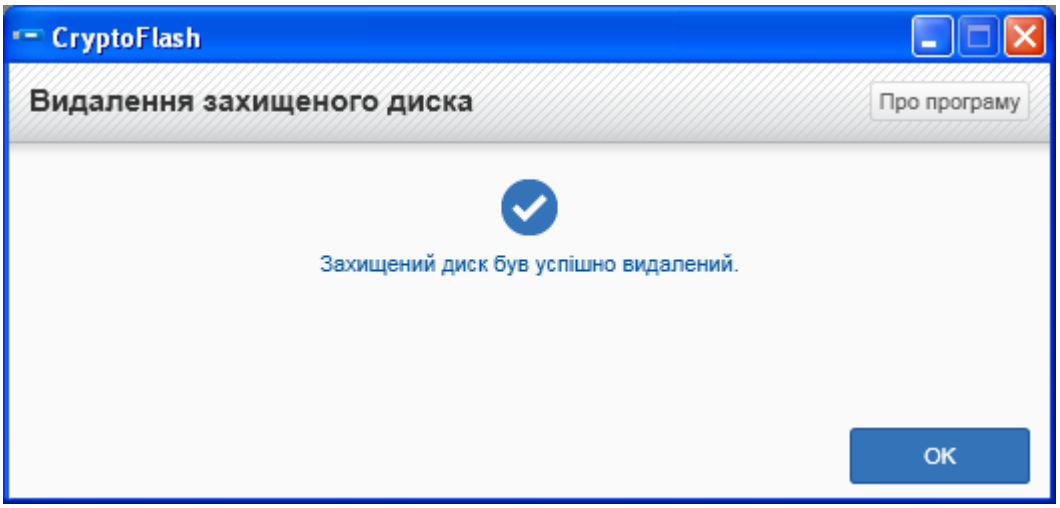


Рисунок 33

4.7 Блокування захищеного диска і кодове слово

Після вичерпання числа спроб введення пароля захищений диск заблокується до введення кодового слова (рисунок 34), якщо кодове слово задавалося на етапі створення захищеного диска (п.4.2). Якщо ж кодове слово не вводилося, диск перейде у вихідний стан, втративши при цьому всю інформацію із захищеного диска (рисунок 35).

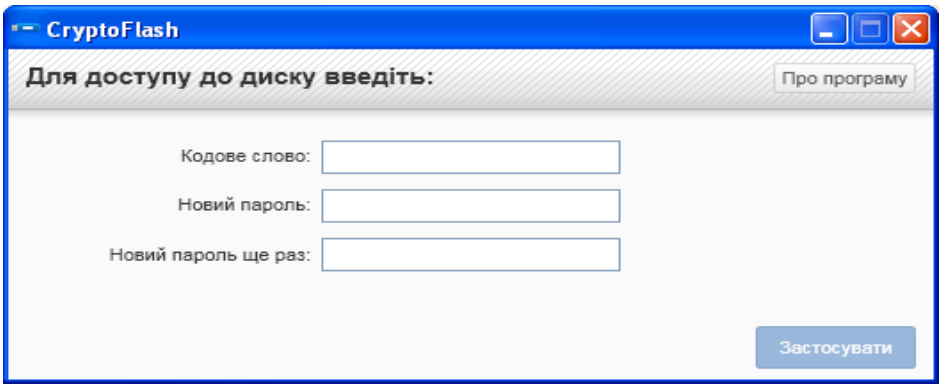


Рисунок 34

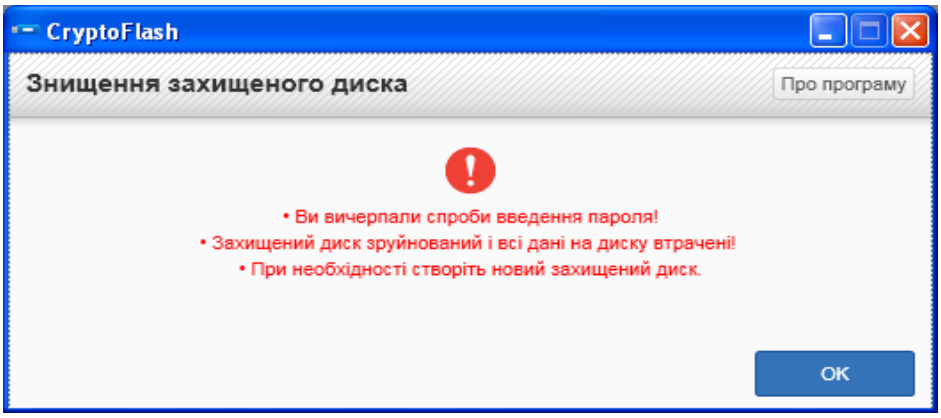


Рисунок 35

Для розблокування захищеного диска, необхідно ввести кодове слово і задати новий пароль з підтвердженням (рисунок 34). Після введення кодового слова, нового пароля і підтвердження, необхідно натиснути кнопку «Застосувати», внаслідок чого захищений диск знову стане доступним.

В разі неправильного введення кодового слова, кількість спроб зменшиться (рисунок 36), при цьому, аби дістати можливість повторного введення кодового слова, необхідно витягнути пристрій з ПК і знову вставити в порт USB.

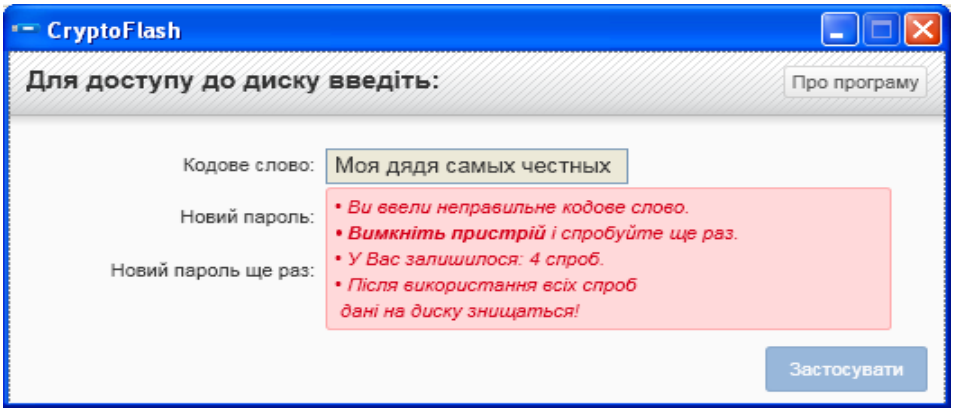


Рисунок 36

При вичерпанні кількості спроб введення кодового слова, захищений диск перейде в стан "витягнутий", втративши при цьому всю інформацію закритого диска (рисунок 37).

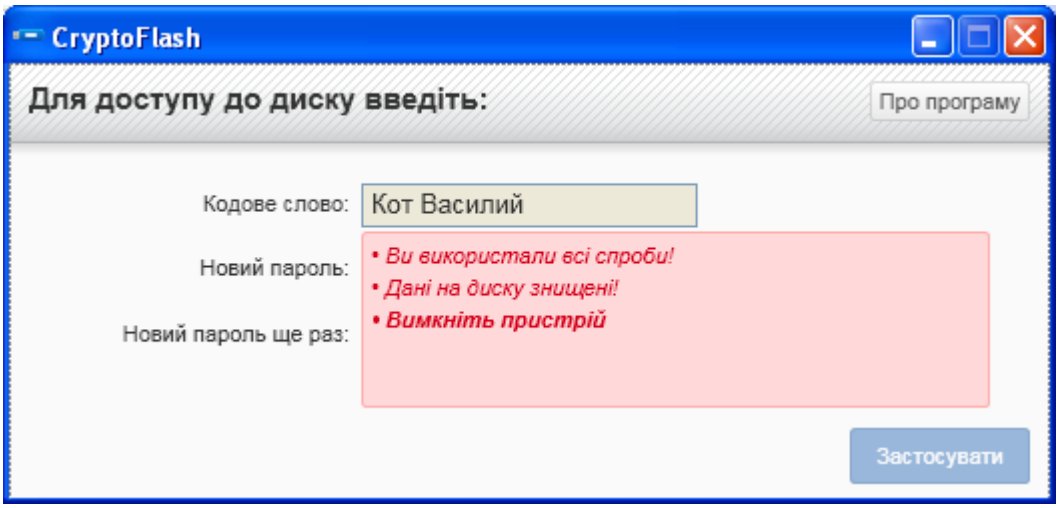


Рисунок 37

4.8 Інформація про утиліту

Аби отримати відомості про утиліту і версію прошивки "Secure Token-337F" (рисунок 38), необхідно натиснути кнопку «Про програму».

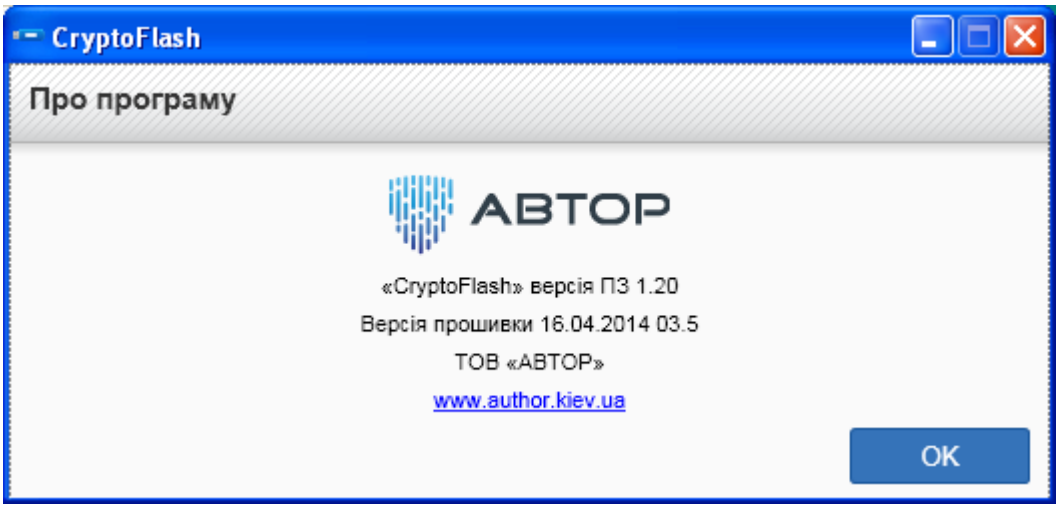


Рисунок 38

5. Про виробника

Ключ електронний "Secure Token-337F", утиліти "CryptoFlashManager" і "CryptoFlash" розроблені ТОВ «АВТОР»..

Поштова адреса: 03005, Київ, вул. Смоленська, 31-33
Телефон: (380 44) 538-00-89
Факс: (380 44) 538-00-89

WEB: http://author.kiev.ua, http://platimo.ua, http://pay.platimo.ua

E-mail: author@author.kiev.ua