АВТОР
системи інформаційної безпеки

УТВЕРЖДЕН
АЧСА.32248356.00182-01 96 01-ЛУ

Ключ электронный "Secure Token-337F"

Программное обеспечение.
Утилиты
"CryptoFlashManager"
и "CryptoFlash"

АЧСА.32248356.00182-01 96 01

Руководство пользователя

Листов 24

2014

Оглавление

1. Введение

Документ содержит описание управляющего программного обеспечения - утилит "CryptoFlashManager" и "CryptoFlash", для эксплуатации носителей криптографической информации - ключей электронных "Secure Token-337F" (далее - "Secure Token-337F").

1.1 Назначение

Утилиты "CryptoFlashManager" и "CryptoFlash" предназначены для управления доступом к данным, находящимся во FLASH-памяти "Secure Token-337F".

1.2 Область применения

Утилиты "CryptoFlashManager" и "CryptoFlash" работают на персональных компьютерах с операционной системой Windows XP[1]/7/8/8.1 и Windows Server 2000/2003/2008/2012.

1.3 Определения и сокращения

- НКИ – носитель ключевой информации;
- ПК – персональный компьютер;
- ЭЦП - электронная цифровая подпись;
- АЦСК – аккредитованный центр сертификации ключей;
- ОС - операционная система.

2. Описание "Secure Token-337F"

Электронный ключ "SecureToken-337F" — это два устройства в одном корпусе: электронный ключ "Secure Token-337" и FLASH-память с логическими дисками для хранения любых данных пользователя.

"SecureToken-337F", как носитель ключевой информации, полностью совместим с электронным ключом "SecureToken-337", применяется для защищенного хранения и использования ключей электронной цифровой подписи (ЭЦП) налоговой службы Украины, ключей аккредитованных центров сертификации ключей (АЦСК) государственных и других организаций, в банковских и корпоративных системах, интернет-банкинге и т.п. Выполняет функции формирования и проверки электронной цифровой подписи, шифрования, аутентификации, хранения секретной (ключевой) информации.

[1] Для работы программного обеспечения CryptoFlash под ОС Windows XP необходим .Net Framework 3.5. При отсутствии .Net Framework 3.5 программное обеспечение CryptoFlash выдает сообщение "Ошибка при инициализации приложения (0xc0000135)". Для установки .Net Framework 3.5 используйте ссылку : http://www.microsoft.com/ru-ru/download/details.aspx?id=21

"SecureToken-337F", как устройство со встроенной FLASH-памятью, может использоваться для хранения любых данных пользователя с защитой от несанкционированного доступа. Поддерживает два типа дисковых массивов– открытый и защищенный, общим объёмом до 32 Гбайт. Все данные на защищенном носителе хранятся в зашифрованном виде.

Для хранения ключей и выполнения криптографических операций в электронном ключе "SecureToken-337F" используется смарт-чип P5CC037 компании NXP Semiconductors . (Сертифицирован в ГСССЗИ Украины, экспертное заключение №05/02/02-810 от 11.03.2013 г.)

2.1 Технические характеристики "Secure Token-337"

- Генерация и хранение ключевой информации согласно ДСТУ 4145-2002 (длина ключа – 163-509 бит) и RSA (длина ключа – 512-2048 бит);
- Шифрование/расшифрование электронных документов согласно ДСТУ ГОСТ 28147-2009, DES, 3-DES, AES;
- Формирование и проверка ЭЦП согласно ДСТУ 4145-2002 (длина ключа – 163-509 бит) и RSA (длина ключа – 512-2048 бит);
- Вычисление хеш-функций согласно ГОСТ 34.311-95, MD5, SHA;
- Реализация схемы аутентификации согласно ISO 9798-3;
- Объем памяти 36 Кбайт.

2.2 Технические характеристики FLASH-памяти

- Объем памяти: 4, 8, 16 или 32 Гбайт;
- Скорость чтения/записи данных на открытом диске, не менее 5 Мбайт/с;
- Скорость чтения/записи данных на защищенном диске и алгоритмы шифрования:

Алгоритм шифрования данных FLASH-памяти	ДСТУ ГОСТ 28147-2009	AES	RC5
Длина ключа, бит	256	128	128
Скорость чтения/записи данных, не менее, Мбайт/с	0,4	0,8	1,7

2.3 Поддерживаемые интерфейсы и стандарты

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

"SecureToken-337F" поддерживает работу со следующими операционными системами (ОС): Windows XP/2003/2008/Vista/7/8, Linux, Mac OS.

Вся FLASH-память устройства "SecureToken-337F" делится на два логических диска - открытый диск и защищенный диск.

Открытый диск – это диск общего назначения предназначен для хранения данных в открытом виде с возможностью установки ограничения на запись.

Защищенный диск - это закрытый диск пользователя, данные на котором хранятся в зашифрованном виде, а доступ организовывается по паролю. В начальном состоянии защищенный диск не создан (состояние «извлечен») и, в зависимости от установок в ОС, может вообще не отображаться системой либо отображаться как пустой диск.

Созданный защищенный диск может находиться в одном из следующих состояний: "извлечен" (состояние по умолчанию, после подключения к ПК) или "подключен" (состояние после правильного ввода пароля). В состоянии "подключен" данные доступны для использования в обычном режиме, аналогично данным на других логических дисках.

В процессе инициализации защищенного диска активируются пароль и ключевое слово и, случайным образом, генерируется секретный ключ для шифрования. Секретный ключ, пароль и ключевое слово хранятся во внутренней памяти управляющего микроконтроллера, защищенной от считывания внешними средствами. Во избежание подбора кодов доступа, количество попыток ввода пароля ограничено 10-ю попытками, количество попыток ввода ключевого слова ограничено 5-ю попытками. После исчерпания всех попыток ключ, на котором шифруются данные во FLASH-памяти, удаляется, и доступ к диску блокируется. После этого, данные, находившиеся в защищенной области диска, восстановить невозможно.

Для изменения основных параметров FLASH-памяти устройства используется утилита "CryptoFlashManager".

Для создания и управления состояниями защищенного диска используется утилита "CryptoFlash".

3. Утилита "CryptoFlashManager"

Для изменения основных параметров FLASH-памяти устройства "Secure Token-337F" используется утилита "CryptoFlashManager".

С помощью утилиты возможно управление следующими параметрами:

- выбор языка интерфейса утилит;
- выбор алгоритма шифрования данных на защищенном диске;
- размеры логических дисков FLASH-накопителя;
- установка защиты от перезаписи открытого диска.

3.1 Запуск утилиты "CryptoFlashManager"

Для запуска утилиты "CryptoFlashManager" необходимо установить "Secure Token-337F" в свободный USB-порт. При этом, в разделе "Мой компьютер" или "Этот компьютер" должно быть обнаружено новое дисковое устройство - открытый диск "UTILS ST-337F" (рисунок 1).

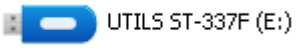


Рисунок 1

На открытом дисковом устройстве "UTILS ST-337F" находятся утилиты для работы с устройством. Для изменения параметров "Secure Token-337F" необходимо открыть дисковое устройство "UTILS ST-337F", выбрать папку "ST337F" и запустить программу "CryptoFlashManager.exe" (рисунок 2).

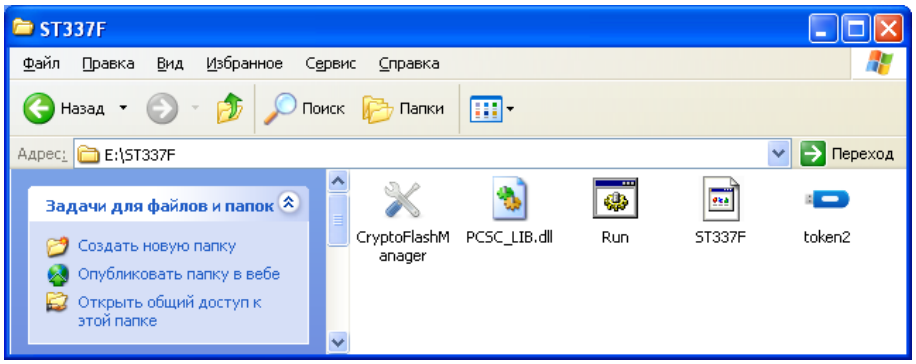


Рисунок 2

При запуске утилиты "CryptoFlashManager" производится поиск устройства "Secure Token-337F" и если, по какой-то причине, устройство не было обнаружено, выводиться сообщение (рисунок 3).

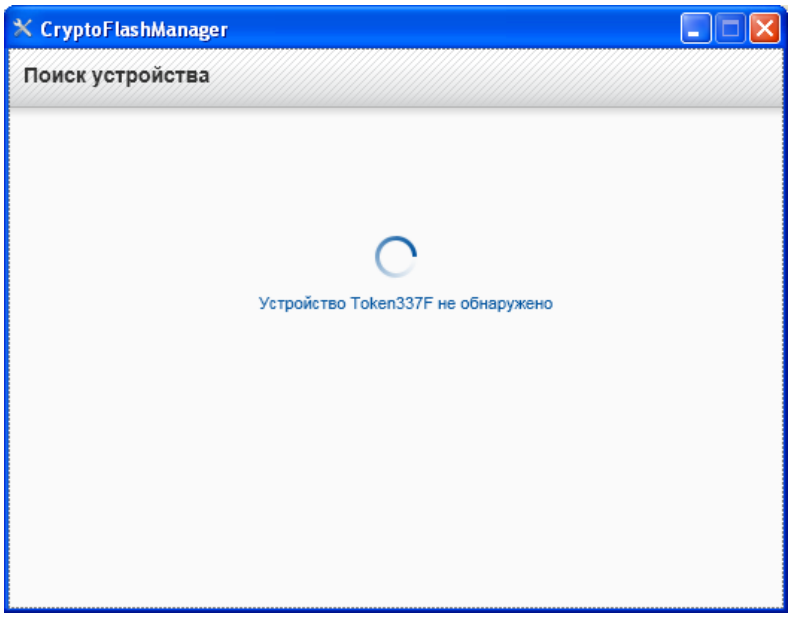


Рисунок 3

При успешном запуске утилиты "CryptoFlashManager" и обнаружении устройства "Secure Token-337F" получаем окно настройки дисков, рисунок 4.

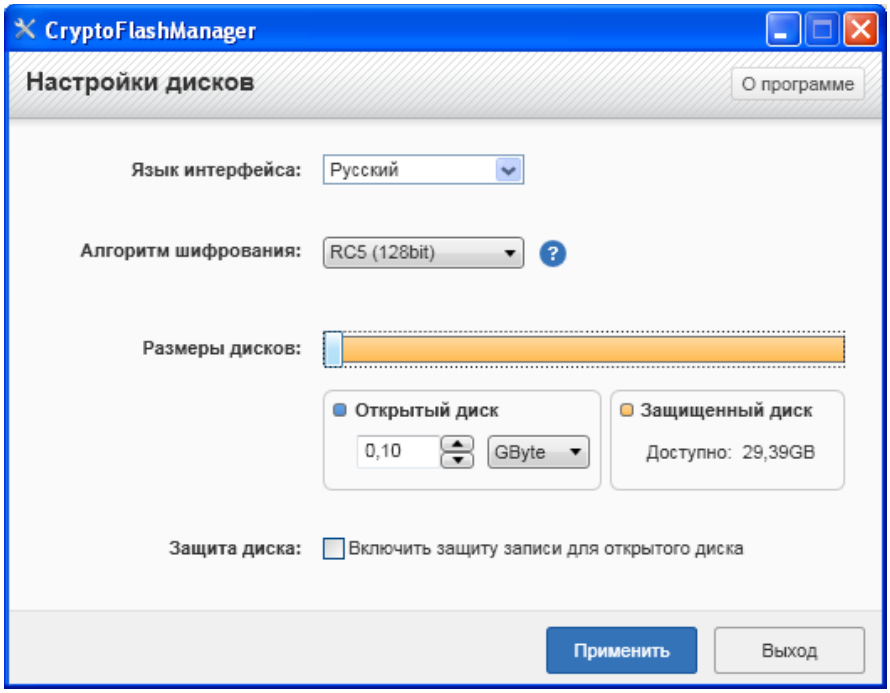
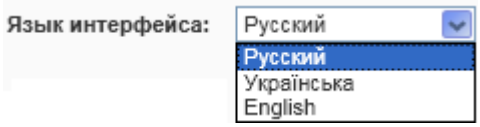


Рисунок 4

3.2 Работа с утилитой "CryptoFlashManager"

Из языков интерфейса доступны: Украинский, Русский, Английский.



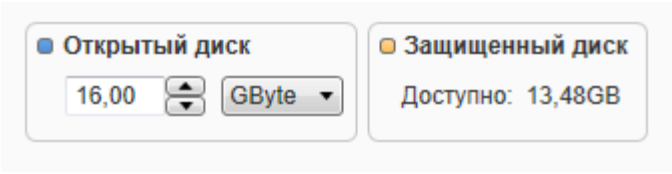
Для создания защищенного диска может быть использован один из трех алгоритмов шифрования данных: RC5, AES, GOST.

RC5 – самый быстрый из поддерживаемых алгоритмов шифрования, в тоже время достаточно криптостойкий алгоритм с длиной ключа 128 бит.

AES (Advanced Encryption Standard) — алгоритм шифрования принятый в качестве стандарта шифрования правительством США. В данном изделии AES используется с длиной ключа 128 бит.

GOST (ДСТУ ГОСТ 28147:2009) — алгоритм шифрования принятый в качестве стандарта шифрования в Украине с длиной ключа 256 бит.

Flash-память встроенная в устройство "Secure Token-337F" по умолчанию разбита на два логических диска "Открытый диск" и "Защищенный диск".



Пользователь имеет возможность изменять размеры "Открытого диска" и "Защищенного диска" при помощи ползунка "Размеры дисков". Минимальный размер "Открытого диска" или "Защищенного диска" не может быть меньше 5 Мбайт, рисунок 5.

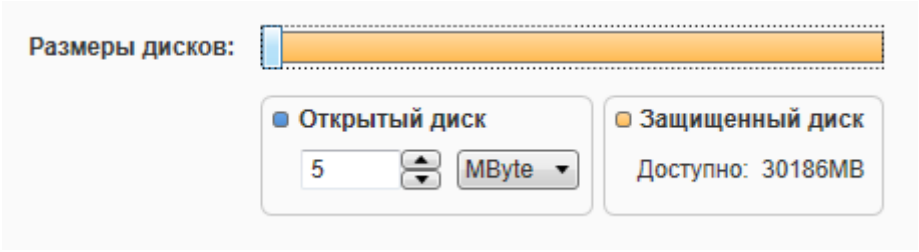


Рисунок 5

Для точного задания размеров дисков необходимо выбрать размерность открытого диска GByte (ГигаБайты) или MByte (МегаБайты), по умолчанию GByte, кликнуть курсором на поле ввода размера открытого диска, вручную ввести нужное значение и нажать клавишу «Enter», рисунок 6.

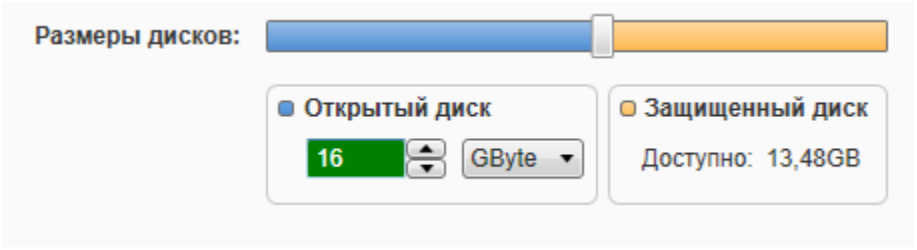


Рисунок 6

Если пользователю не нужен открытый диск, а необходим только защищенный диск на весь объем FLASH-памяти, то размер открытого диска задается как 0 Мбайт, ползунок "Размеры дисков" в крайнем левом положении (рисунок 7).

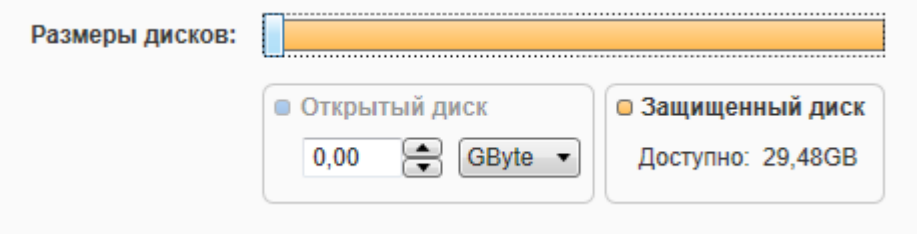


Рисунок 7

Если пользователям в работе не нужен защищенный диск, они могут создать только открытый диск на весь объем FLASH-памяти, для этого ползунок "Размеры дисков", необходимо перевести в крайнее правое положение (рисунок 8).

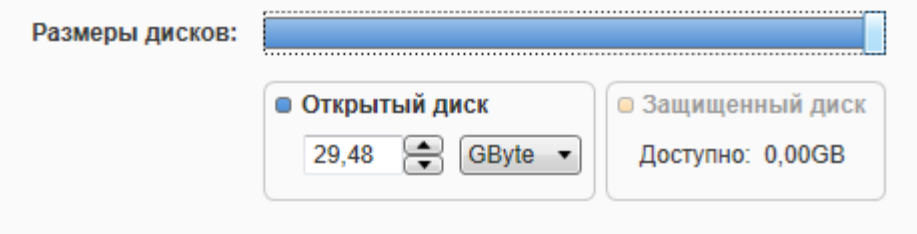


Рисунок 8

Если у пользователя есть необходимость в защите открытого диска от записи/изменения/удаления файлов, то пользователь должен установить флажок на разделе "Защита диска", рисунок 9. Это позволяет защитить данные от вредоносного действия вирусов, например в случаях, когда устройство используется на «чужом» компьютере.

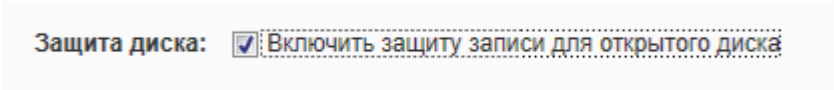


Рисунок 9

3.3 Применение параметров утилиты «CryptoFlashManager»

Для сохранения измененных параметров устройства "Secure Token-337F" необходимо нажать на кнопку "Применить". Устройство сохранит во внутренней памяти управляющего микроконтроллера измененные параметры и, если необходимо, будет предложено отключить устройство от USB (рисунок 10) для применения новых параметров.

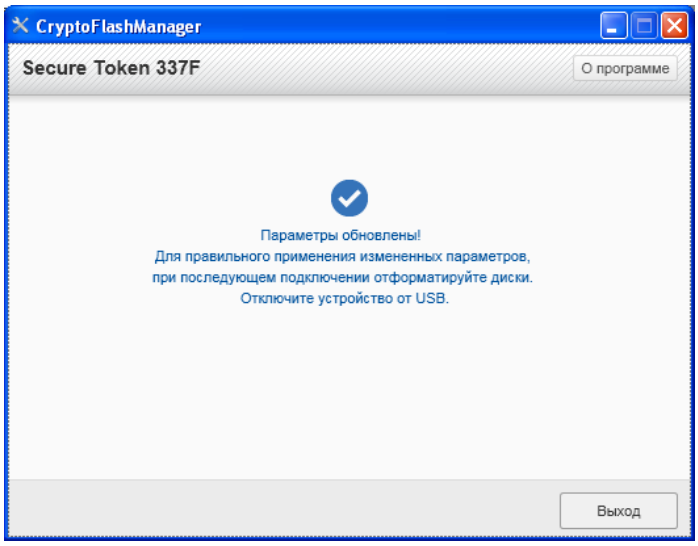


Рисунок 10

После повторного подключения устройства необходимо отформатировать открытый диск "UTILS ST-337F" предварительно сохранив с него всю информацию.

ВНИМАНИЕ! После изменения размеров открытого и защищенного диска устройства "Secure Token-337F" Windows будет неправильно определять размер открытого диска до его переформатирования. Windows ориентируется на размер диска по его предыдущему форматированию.

Форматировать открытый диск допустимо в любой файловой системе (FAT, FAT32, NTFS, extFAT), по умолчанию FAT32, рекомендуем указать метку тома и выбрать способ форматирования "Быстрое", рисунок 11.

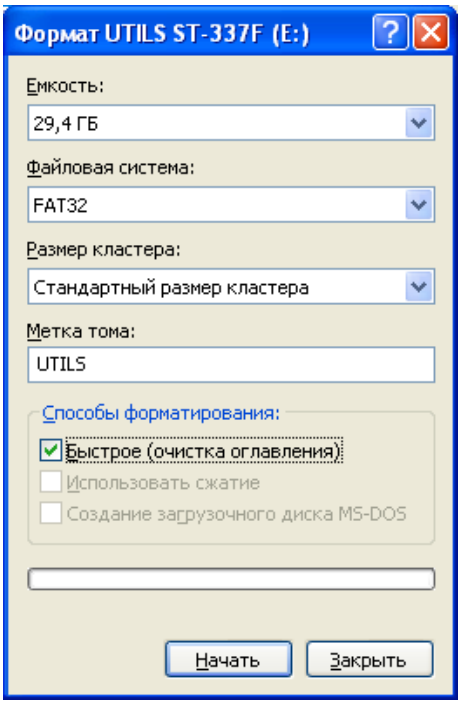


Рисунок 11

После форматирования, для удобства использования утилит, рекомендуем восстановить данные на открытом диске "UTILS ST-337F".

3.4 Информация об утилите

Чтобы получить сведения об утилите и версии прошивки "Secure Token-337F" (рисунок 12), необходимо нажать кнопку «О программе».

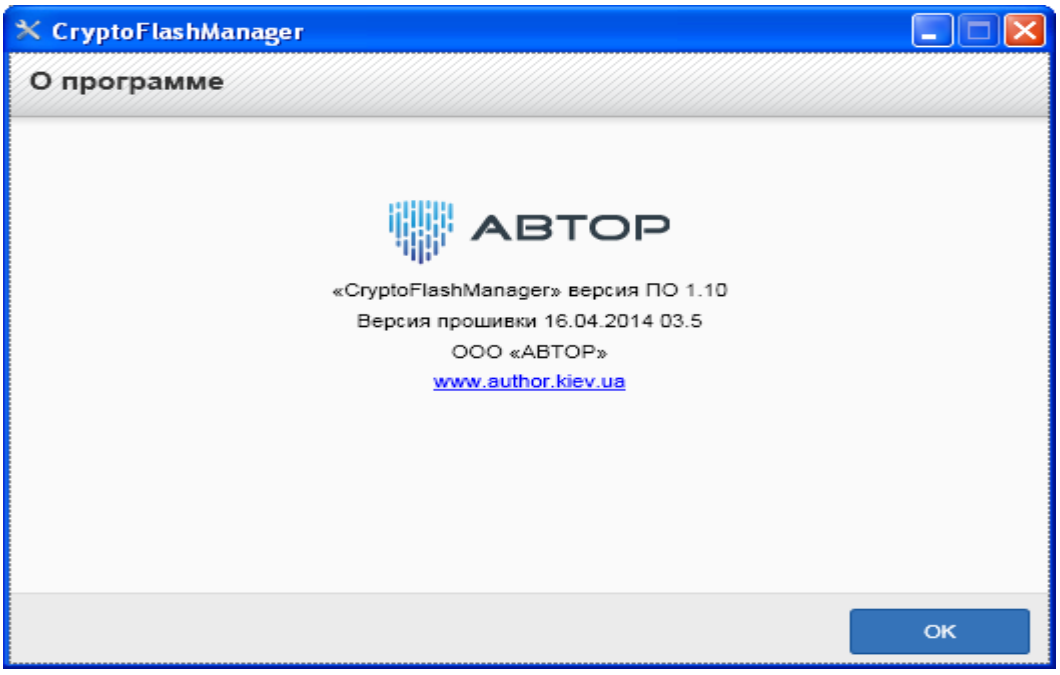


Рисунок 12

4. Утилита "CryptoFlash"

Для управления состояниями "Secure Token-337F" используется утилита "CryptoFlash". Если у пользователя нет необходимости в создании защищенного диска, то использовать утилиту "CryptoFlash" не нужно. В таком случае "Secure Token-337F" будет работать как обычный USB-флеш-накопитель, совмещенный с НКИ. Пользователю будет доступен только открытый диск устройства.

При использовании защищенного диска следует обратить внимание на то, что при потере пароля и ключевого слова к защищенному диску **данные, находившиеся на этом диске, восстановить невозможно**.

4.1 Запуск утилиты "CryptoFlash"

Для запуска утилиты "CryptoFlash" необходимо установить "Secure Token-337F" в свободный USB-порт. При этом, в разделе "Мой компьютер" или "Этот компьютер" должно быть обнаружено новое дисковое устройство - открытый диск "UTILS ST-337F" (рисунок 1).

Для создания защищенного диска необходимо открыть дисковое устройство "UTILS Token337F" и запустить программу "CryptoFlash.exe" (рисунок 13).

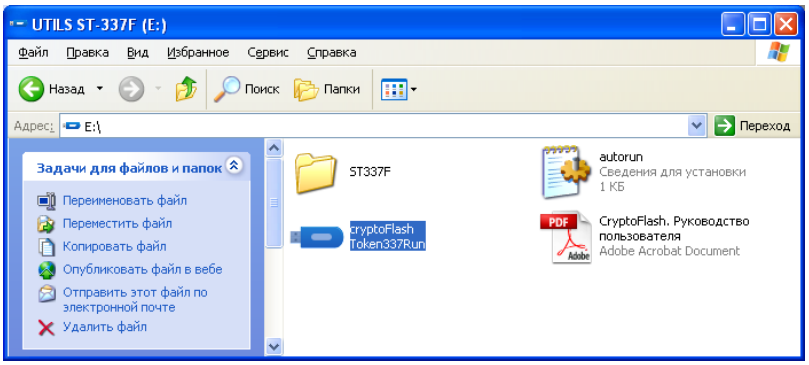


Рисунок 13

При запуске утилиты "CryptoFlash" производиться поиск "Secure Token-337F" и если, по какой-то причине, устройство не было обнаружено, выводиться сообщение (рисунок 14).

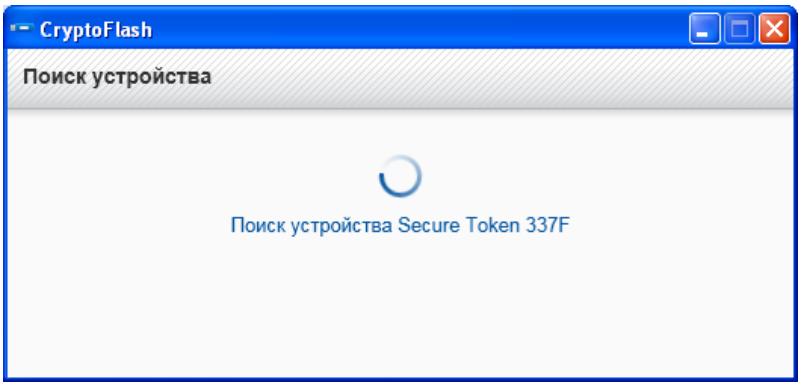


Рисунок 14

При обнаружении "Secure Token-337F" на экран выводиться диалоговое меню для создания защищенного (закрытого) диска, см. рисунок 15.

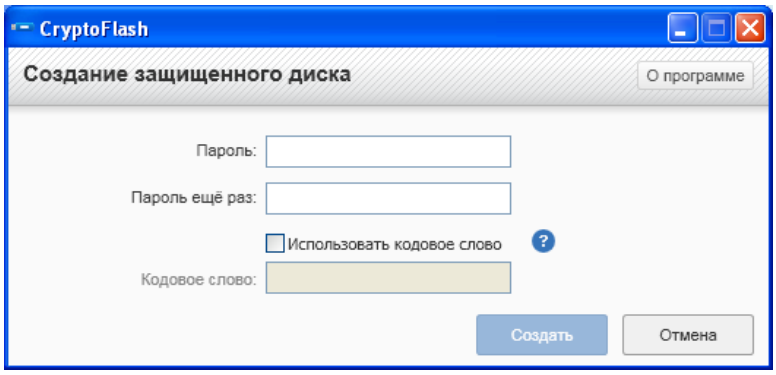


Рисунок 15

4.2 Создание защищенного диска

Для создания защищенного (закрытого) диска необходимо задать пароль длиной 4-16 символов в поле "Пароль". Этот пароль будет необходим для доступа к данным на закрытом диске после его создания. Пароль может состоять из цифр, символов и букв любого алфавита доступного на данном ПК. После ввода пароля его необходимо подтвердить, для этого надо ввести его еще раз в поле "Пароль еще раз".

Для возможности восстановления пароля, в случае его утери, рекомендуется воспользоваться дополнительной опцией "Кодовое слово"(рисунок 16). По кодовому слову или фразе, при блокировании диска из-за исчерпания попыток ввода пароля, появляется возможность создать новый пароль и возобновить доступ к данным на защищенном диске. Если кодовое слово не вводилось и число попыток ввода пароля исчерпалось, то данные на защищенном диске будут безвозвратно утеряны.

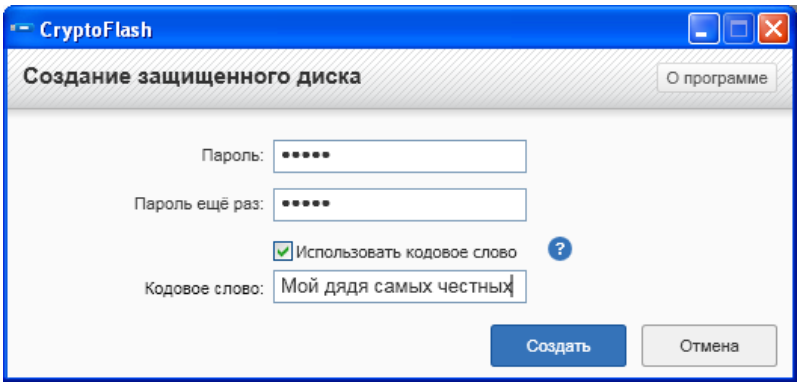


Рисунок 16

После нажатия кнопки "Создать" появится сообщение об успешном создании защищенного диска (рисунок 17), или ошибке, в случае неправильной длины используемого пароля (рисунок 18), или ошибки в его подтверждении (рисунок 19).

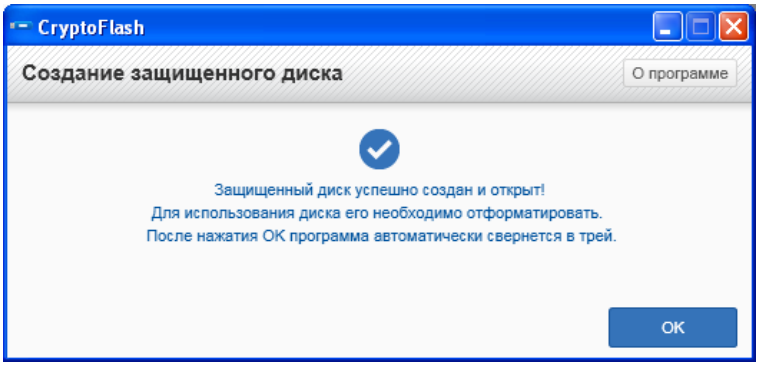


Рисунок 17

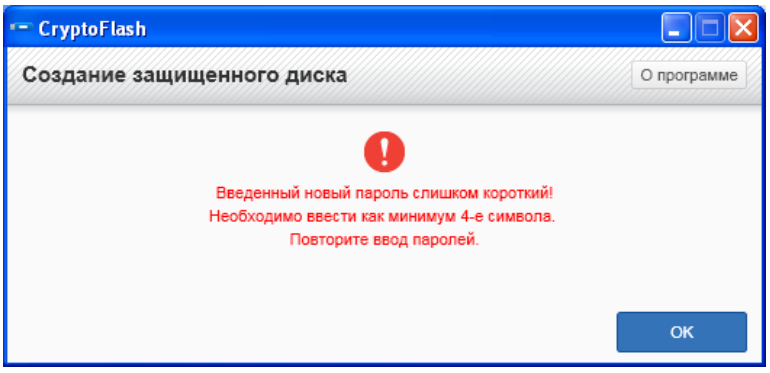


Рисунок 18

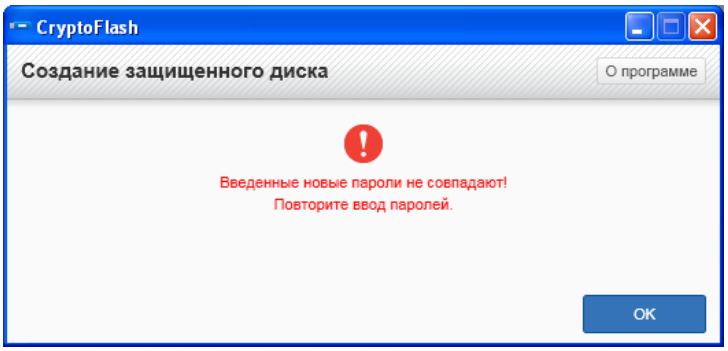


Рисунок 19

При создании защищенного диска, генерируется уникальный ключ для шифрования данных на диске. После успешного создания защищенного диска операционная система предложит провести его форматирование (рисунок 20).

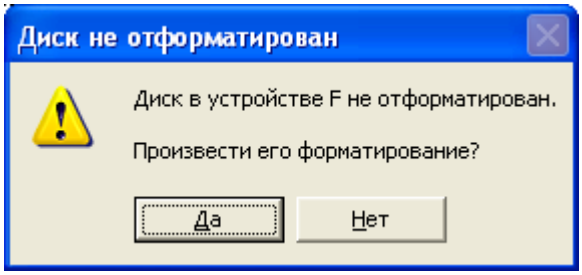


Рисунок 20

Защищенный диск необходимо отформатировать в нужной пользователю файловой системе FAT, FAT32, NTFS, exFAT. По умолчанию используется FAT32. Рекомендуется прописать метку тома и выбрать способ форматирования "Быстрое" (рисунок 21).

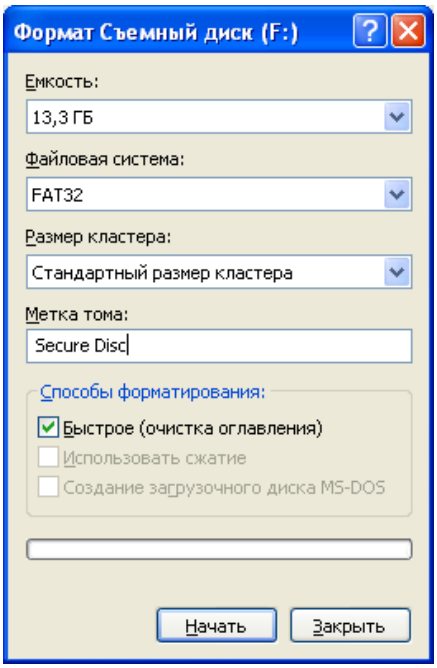


Рисунок 21

После форматирования в системе появится пустой защищенный диск.

4.3 Получение доступа к защищенному диску

При подключении к ПК устройства "Secure Token-337F" с созданным защищенным диском необходимо ввести пароль для получения доступа к защищенному диску (Рисунок 22).

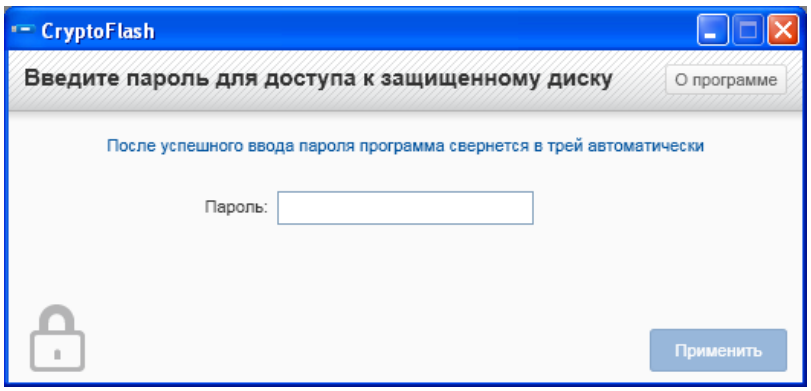


Рисунок 22

При неверном вводе пароля количество попыток уменьшится (рисунок 23). При достижении лимита попыток неправильного ввода пароля, поведение устройства определяется пунктом 4.7.

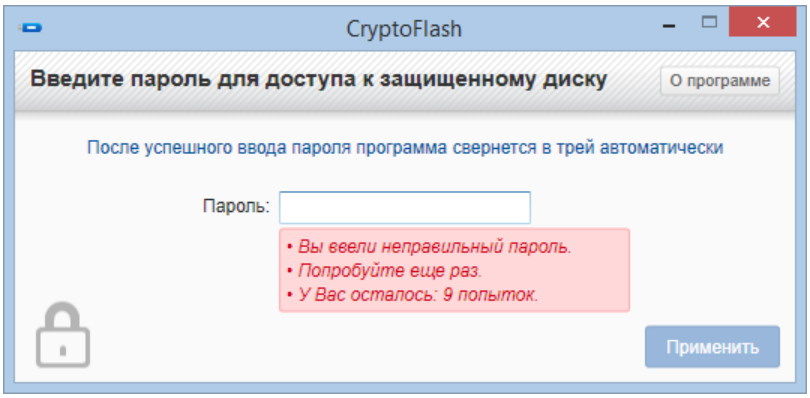


Рисунок 23

После успешного ввода пароля и открытия защищенного диска появляется меню «Работа с защищенным диском» (рисунок 24). Это меню позволяет выполнять операции закрытия диска, смены пароля доступа к защищенному диску, удаления защищенного диска.

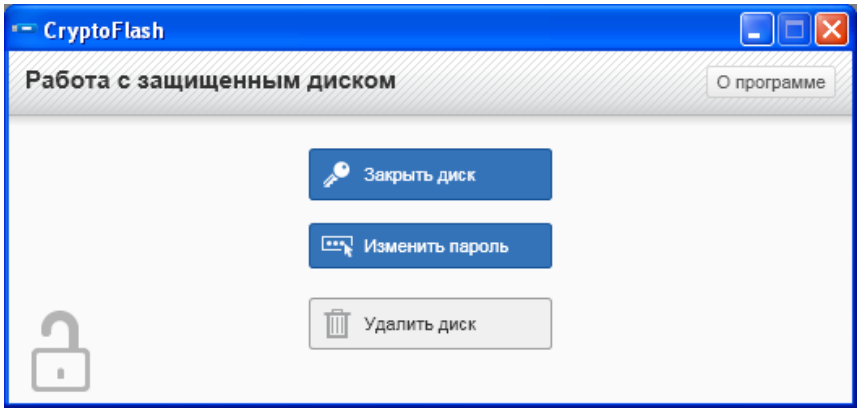


Рисунок 24

4.4 Закрытие доступа к защищенному диску

После завершения работы с защищенным диском, его можно закрыть для доступа (рисунок 24, кнопка "Закрыть диск"). Появится сообщение о закрытии диска (рисунок 25). При этом диск либо исчезнет из системы, либо будет отображаться как "пустой" (состояние "Извлечен"). В таком режиме доступ к данным на диске невозможен. Для получения доступа к диску необходимо повторно ввести пароль (рисунок 22) и нажать на кнопку "Применить".

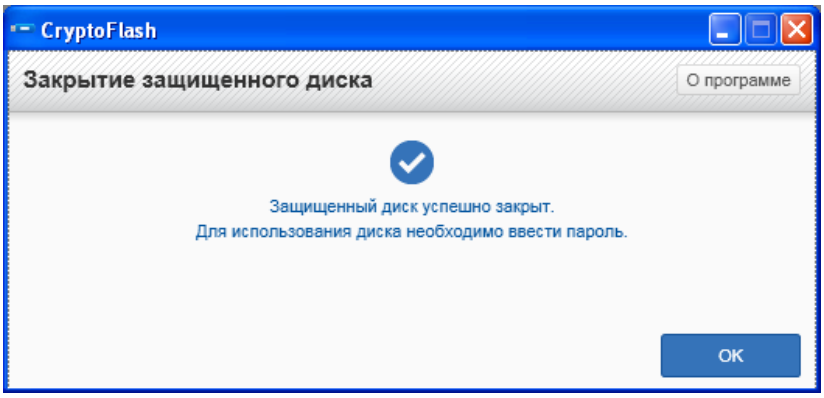


Рисунок 25

Примечание. Извлечение устройства "Secure Token-337F" из USB-порта ПК, не выполнив предварительно процедуру закрытия защищенного диска, приведет к его автоматическому закрытию.

4.5 Изменение пароля доступа к защищенному диску

Существует возможность изменения пароля доступа к защищенному диску (рисунок 24, кнопка "Изменить пароль"). Для этого нужно ввести старый пароль и новый с подтверждением (рисунок 26).

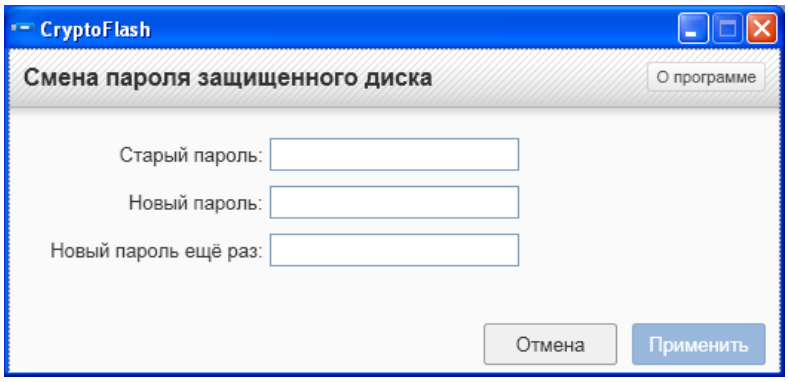


Рисунок 26

При неверном вводе старого пароля количество попыток уменьшится (рисунок 27). При достижении лимита попыток неправильного ввода пароля, поведение устройства определяется пунктом 4.7.

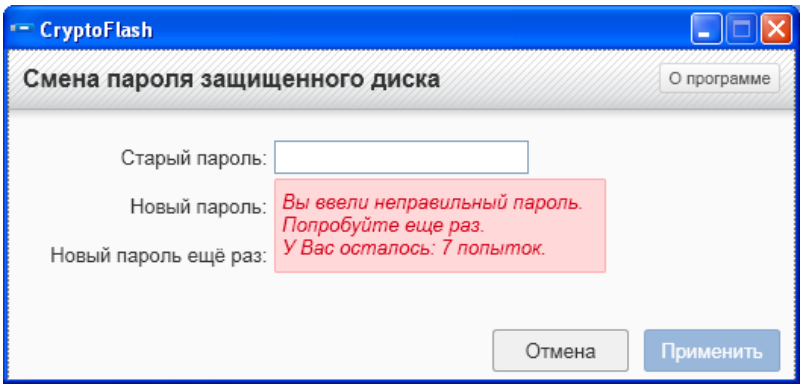


Рисунок 27

После ввода и подтверждения пароля необходимо нажать кнопку "Применить", в результате чего появится сообщение об успешном изменении пароля (рисунок 30), или ошибке, в случае неправильной длины используемого пароля (рисунок 28) или ошибки в его подтверждении (рисунок 29).

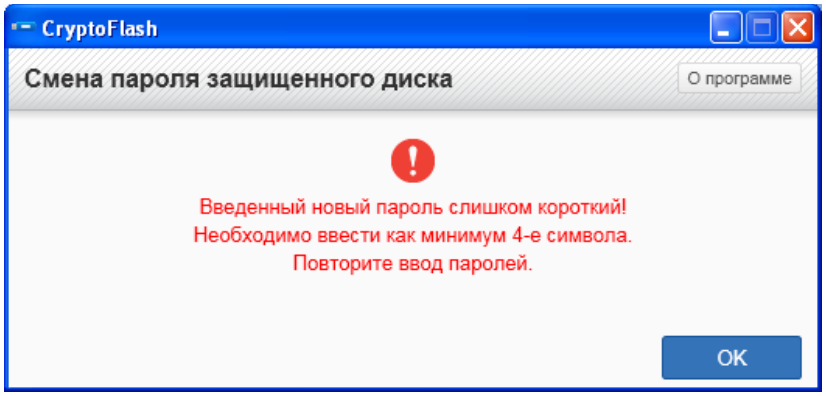


Рисунок 28

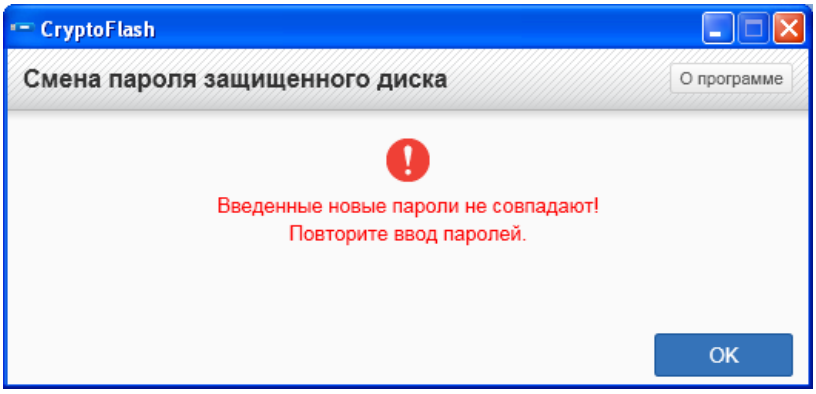


Рисунок 29

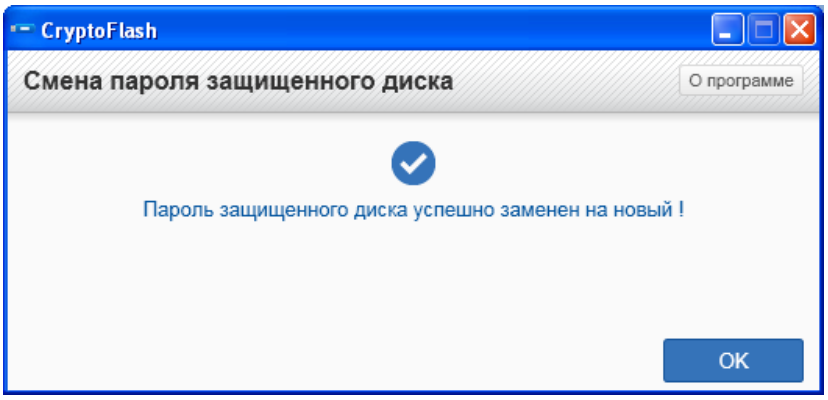


Рисунок 30

4.6 Удаление диска

Для удаления защищенного диска и возврата к незащищенному диску необходимо нажать кнопку "Удалить диск" (рисунок 24) и перейти в меню "Удаление защищенного диска"(рисунок 31). Для подтверждения удаления защищенного диска необходимо ввести пароль доступа к диску. На рисунке 33 показан результат успешного выполнения процедуры удаления защищенного диска.

Внимание! При успешном удалении защищенного диска все данные, которые на нем находились, будут безвозвратно утеряны!

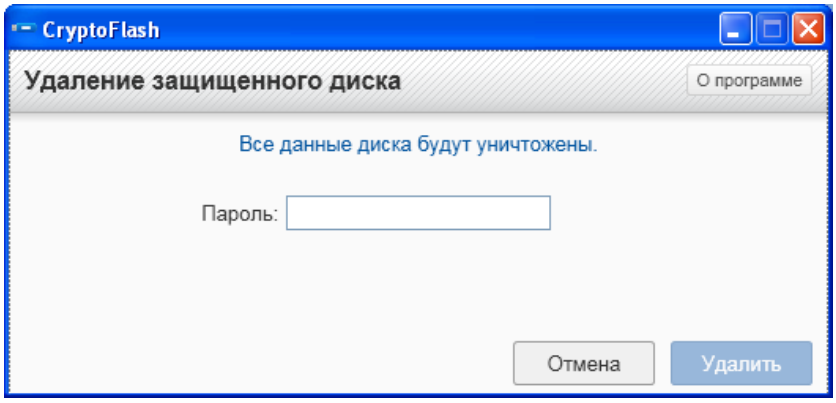


Рисунок 31

При неверном вводе пароля количество попыток уменьшится (рисунок 32). При достижении лимита попыток неправильного ввода пароля, поведение устройства определяется пунктом 4.7.

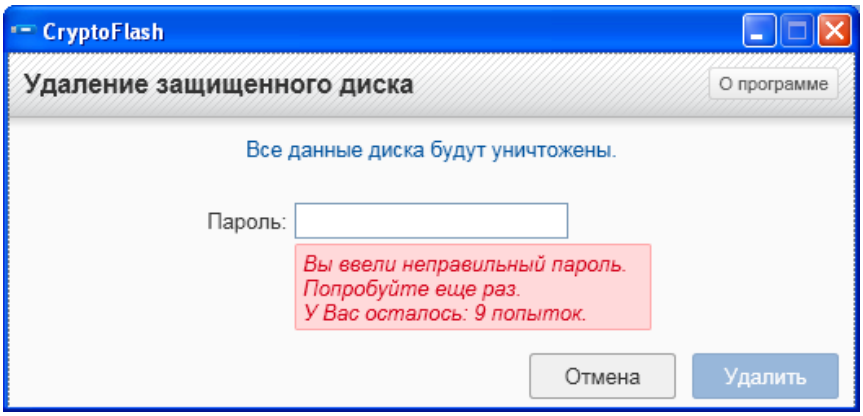


Рисунок 32

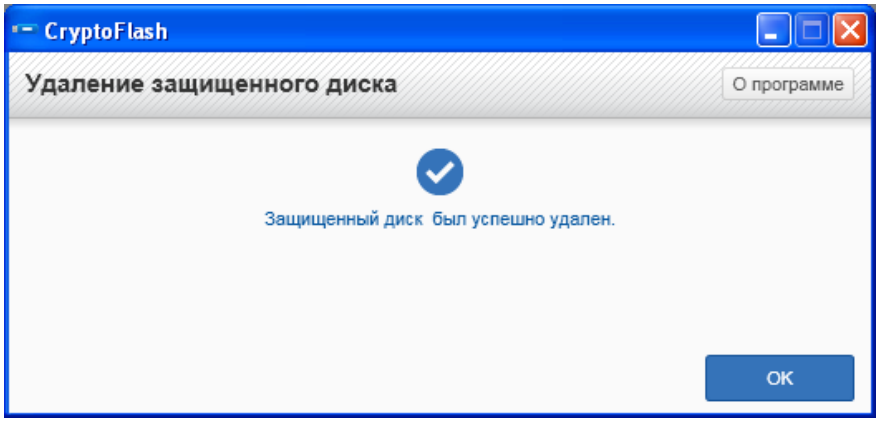


Рисунок 33

4.7 Блокировка защищенного диска и кодовое слово

После исчерпания числа попыток ввода пароля защищенный диск заблокируется до ввода кодового слова (рисунок 34), если кодовое слово задавалось на этапе создания защищенного диска (п.4.2). Если же кодовое слово не вводилось, диск перейдет в исходное состояние, потеряв при этом всю информацию с защищенного диска (рисунок 35).

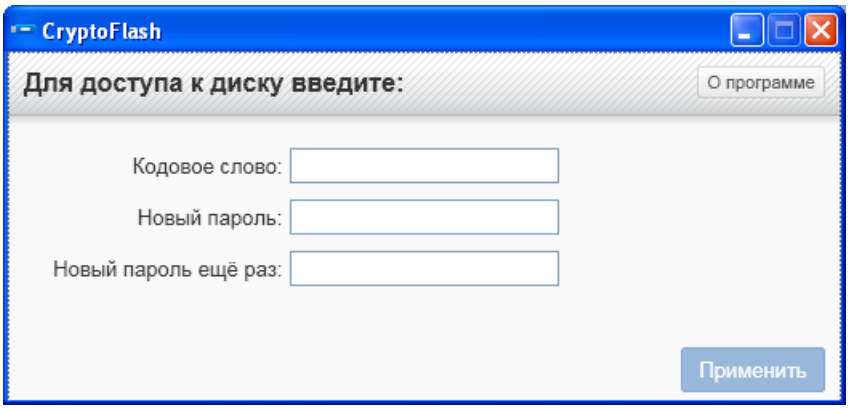


Рисунок 34

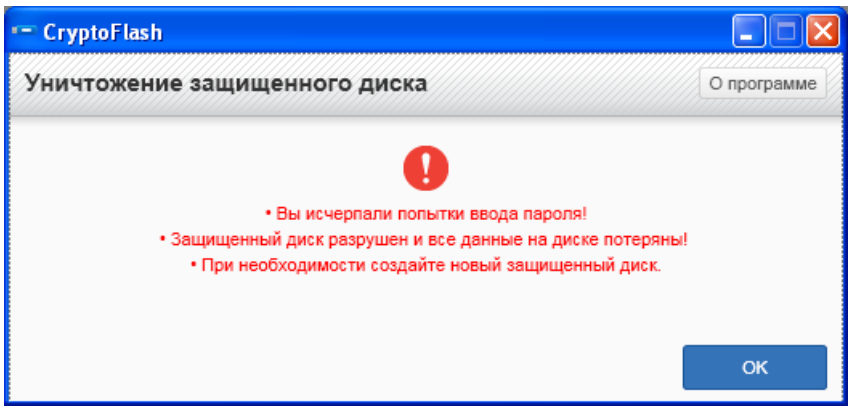


Рисунок 35

Для разблокировки защищенного диска, необходимо ввести кодовое слово и задать новый пароль с подтверждением (Рисунок 34). После ввода кодового слова, нового пароля и подтверждения, необходимо нажать кнопку «Применить», в результате чего защищенный диск снова станет доступным.

В случае неправильного ввода кодового слова, количество попыток уменьшится (рисунок 36), при этом, чтобы получить возможность повторного ввода кодового слова, необходимо извлечь устройство из ПК и снова вставить в порт USB.

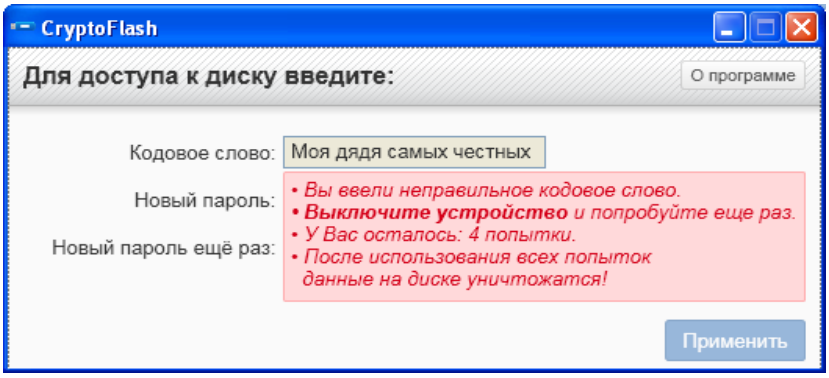


Рисунок 36

При исчерпании количества попыток ввода кодового слова, защищенный диск перейдет в состоянии "извлечен", потеряв при этом всю информацию закрытого диска (рисунок 37).

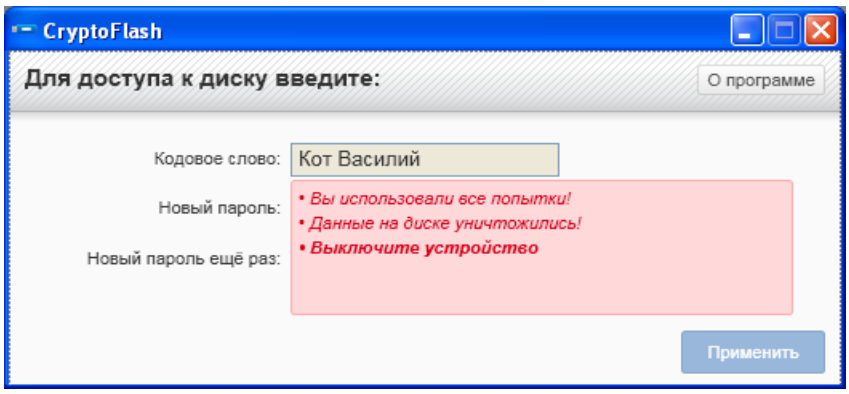


Рисунок 37

4.8 Информация об утилите

Чтобы получить сведения об утилите и версии прошивки "Secure Token-337F" (рисунок 38), необходимо нажать кнопку «О программе».

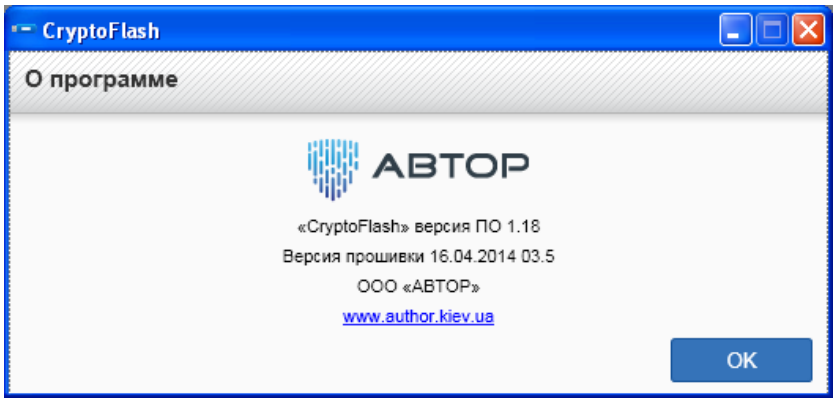


Рисунок 38

5. О производителе

Ключ электронный "Secure Token-337F", утилиты "CryptoFlashManager" и "CryptoFlash" разработаны ООО «АВТОР».

Почтовый адрес: 03005, Киев, ул. Смоленская, 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