Криптографический USB накопитель-считыватель FLASH карт

1. Назначение

Криптографический USB накопитель-считыватель FLASH карт предназначен для криптографической защиты информации, записываемой в FLASH карты памяти, с обеспечением защиты от попыток несанкционированного доступа.

Устройство позволяет обеспечить:

- защищенное хранение информации на FLASH картах;
- защищенный перенос информации между различными персональными компьютерами, оснащенными данным устройством, посредством сменных FLASH карт памяти.

Криптографический USB накопитель-считыватель реализован на микроконтроллере отечественного производства (ЗАО «ПКК Миландр»).

2. Основные выполняемые функции

2.1. Криптографическая защита, записываемой информации, осуществляется по алгоритму шифрования ГОСТ 28147-89, с длиной ключа до 55 бит.
2.2. Энергонезависимое хранение зашифрованной информации в FLASH карте памяти.
2.3. Поддержка операционных систем Windows 9x / 2000 / XP / Vista / 7.
2.4. Защиту от несанкционированного доступа к зашифрованной информации с помощью пароля доступа.
2.5. Наличие специального пароля автоматической смены ключевой информации для блокирования доступа к ранее записанной информации.
2.6. Возможность непосредственного ввода ключевой информации шифрации для доступа к зашифрованной информации.
2.7. Наличие «открытого накопителя» с неизменяемой информацией, содержащей программное обеспечение для идентификации пользователя (ввод, смена пароля и т.д.).
2.8. Наличие «закрытого накопителя» с содержимым карты памяти, недоступного пользователю и операционной системе до проведения корректной аутентификации пользователя.
2.9. Возможность смены накопителя, т.е. замены FLASH карт памяти.
2.10. Возможность работы с двумя наборами паролей доступа и ключевой информации для обеспечения доступа к различным картам памяти.

3. Технические характеристики

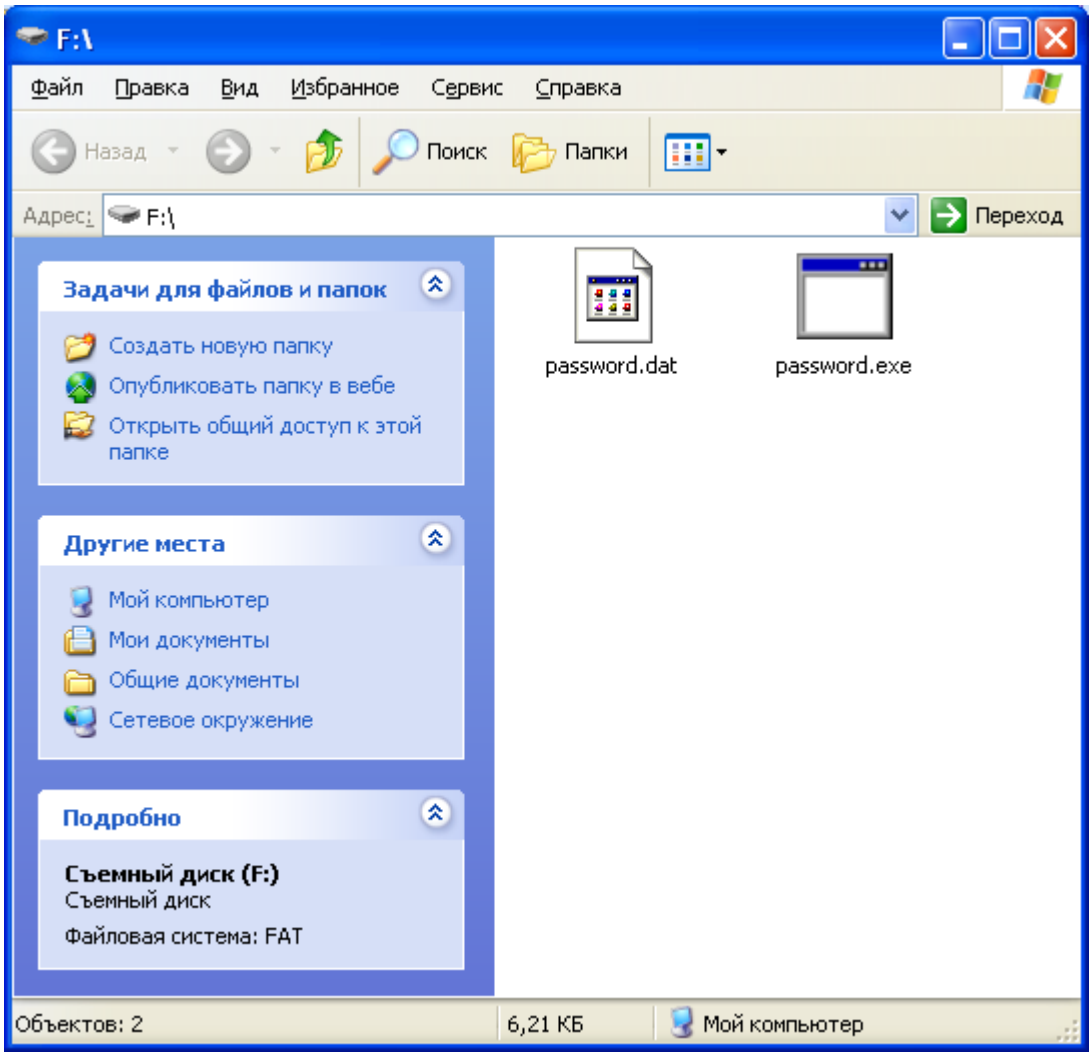
3.1. Устройство реализовано в малогабаритном корпусе. На корпусе установлены следующие разъемы:
3.1.1. USB разъем (тип A) для подключения устройства к персональному компьютеру,
3.1.2. разъем для подключения FLASH карт памяти типа microSD.
3.2. Для обеспечения обмена данными с персональным компьютером используется физический интерфейс USB 2.0 или USB 1.1, режим «Full Speed», со скоростью обмена 12 Мбит/с.

3.3. Устройство является стандартным съемным дисковым накопителем (поддерживает систему команд USB Mass Storage Devices).
3.4. Встроенное программное обеспечение для идентификации пользователя поддерживает работу с операционными системами Windows 9x / 2000 / XP / Vista / 7.
3.5. Поддерживаются файловые структуры операционных систем Windows 9x / 2000 / XP / Vista / 7.
3.6. Поддерживаемый тип FLASH карт – microSD, microSDHC.
3.7. Объем используемых FLASH карт - до 32 Гбайт.
3.8. Скорость шифрования/расшифровывания записываемых/считываемых данных до 300 кбайт/с.

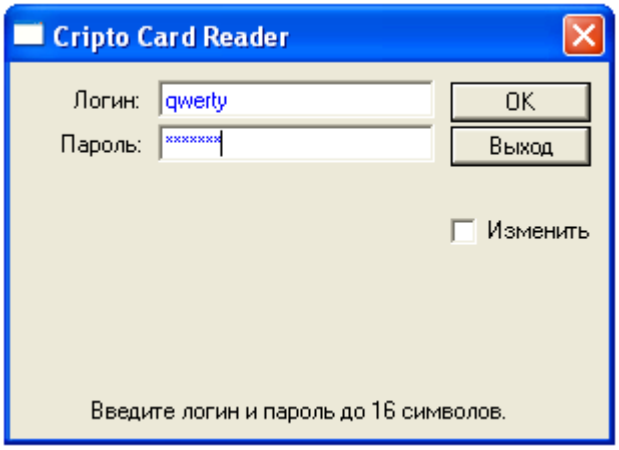
4. Работа с криптографическим накопителем-считывателем

4.1. Проведение аутентификации пользователя.

Подключите криптографический накопитель-считыватель (далее КНС) к компьютеру. Если на Вашем компьютере задан автозапуск просмотра файлов, то откроется накопитель с программой аутентификации («открытый накопитель»). Если автозапуск не задан - произведите открытие накопителя.

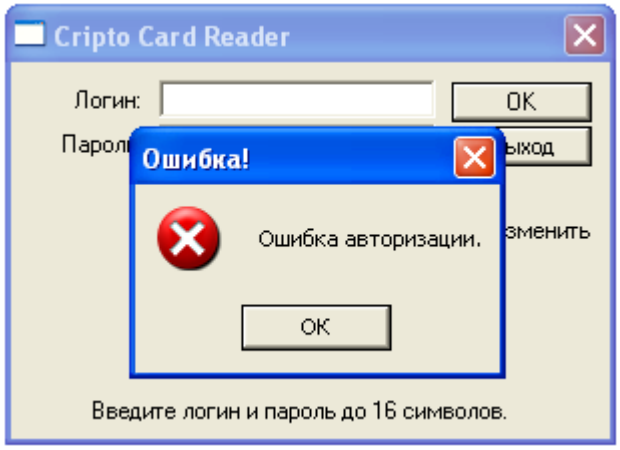


Запустите файл password.exe. В соответствующие поля программы введите имя и пароль. Вводимое имя отображается на экране, а вводимый пароль отображается символами «*». После ввода имени и пароля нажмите «OK».



В случае ввода верного значения имени и пароля, накопитель, содержащий программу аутентификации, отключается. К компьютеру подключится FLASH карта памяти («закрытый накопитель»). Программа аутентификации закроется.

В случае ввода ошибочного значения имени или пароля, накопитель, содержащий программу аутентификации, отключается от компьютера и за тем подключается повторно. Программа аутентификации выдает соответствующее сообщение об ошибке. Для повторного ввода имени и пароля необходимо закрыть сообщение об ошибке и повторить указанные выше действия.

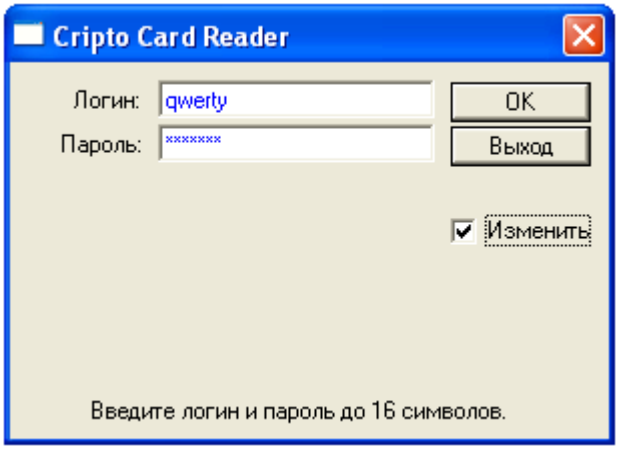


В случае ввода верного значения имени и «специального» пароля аутентификация будет считаться успешной, но при этом будет осуществлена автогенерация нового значения ключевой информации для шифрации. ВНИМАНИЕ: информация, ранее записанная на FLASH карты с использованием старого значения ключевой информации, будет УТРАЧЕНА.

Переход между полями «Логин/Пароль/OK» может производиться «мышью» или клавишей «TAB». Нажатие «OK» - «мышью» или, при выделенном данном поле, нажатием «Enter». Нажатие «Выход» закроет программу без осуществления аутентификации.

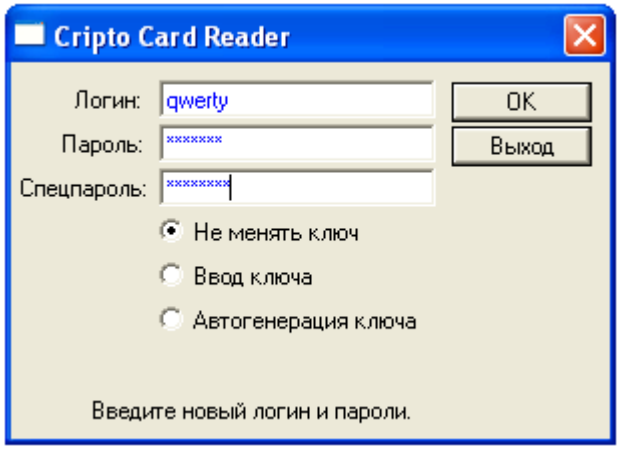
4.2. Изменение информации о пользователе.

Для изменения информации о пользователе произведите аутентификацию пользователя, как указано выше. Отличие заключается в необходимости установки «галочки» в поле «Изменить».



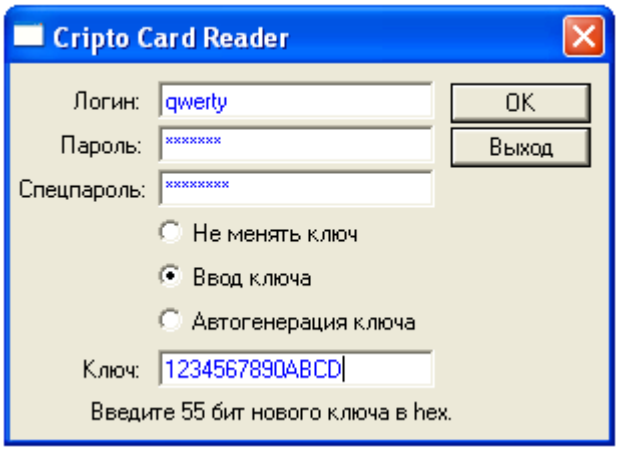
В случае верного ввода имени и пароля программа перейдет к вводу новых значений имени, пароля, «специального» пароля и ключевой информации.

При вводе новых значений имени, вводимые символы отображаются на экране, а при вводе пароля и «специального» пароля, вводимые символы заменяются «*». Необходимо обратить внимание, что строчные и заглавные буквы считаются разными. Также при совпадении значения пароля и «специального» пароля, «специальный» пароль игнорируется.

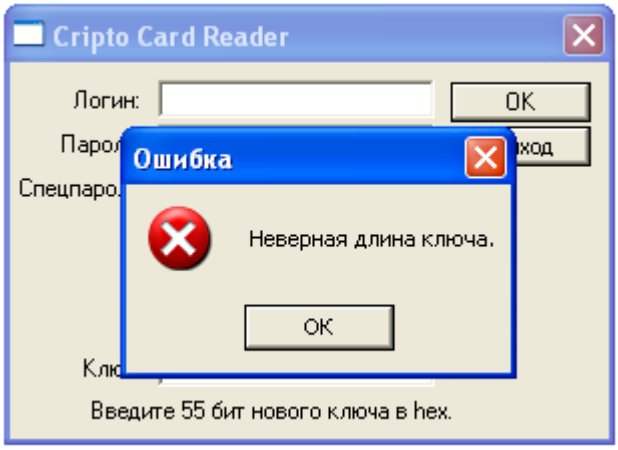


При изменении информации о пользователе можно оставить прежнее значение ключевой информации (отметить «Не менять ключ»). В этом случае информация, ранее записанная на FLASH карты, останется доступной.

Можно непосредственно ввести новое значение ключевой информации (отметить «Ввод ключа»). В этом случае информация, ранее записанная на FLASH карты, будет УТРАЧЕНА. Новое значение ключа вводится в шестнадцатеричном коде (14 символов, первый – символы 0…7, далее – символы 0…9, A, B, C, D, E, F).



В случае ошибки ввода ключа выдается сообщение:

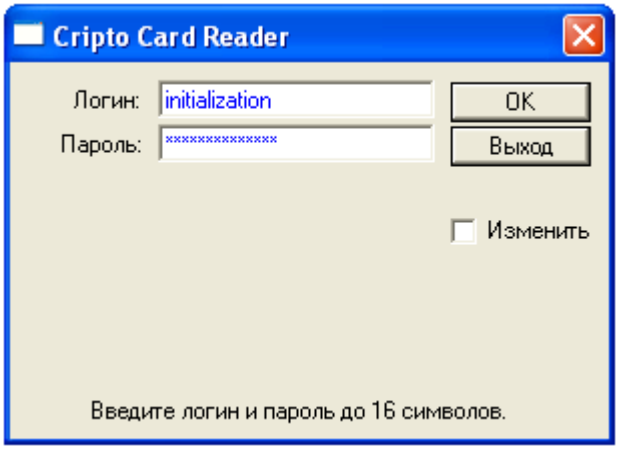


Также можно произвести автогенерацию нового значения ключевой информации с помощью встроенного генератора случайных чисел (отметить «Автогенерация ключа»). В этом случае информация, ранее записанная на FLASH карты, будет УТРАЧЕНА.

Для ввода в КНС нового значения информации о пользователя нажмите «OK». При этом накопитель, содержащий программу аутентификации, отключается. К компьютеру подключится FLASH карта памяти. Программа аутентификации закроется.

4.3. Удаление информации о пользователях.

КНС хранит информацию о двух пользователях. В случае необходимости удаления информации о пользователях необходимо произвести инициализацию. Для этого в качестве имени и пароля необходимо ввести «initialization». При этом все имена пользователей и пароли заменяются на «пустое» значение, производится автогенерация новых значений ключевой информации. Информация, ранее записанная на FLASH карты, будет УТРАЧЕНА.



В дальнейшем для задания новых имен и паролей, проведите аутентификацию пользователя с «пустыми» значениями имени и пароля.

4.4. Работа с FLASH картой памяти.

После проведения успешной аутентификации FLASH карта подключается к компьютеру. При первом применении и после смены ключевой информации шифрования, необходимо произвести форматирование FLASH карты. Для этого могут быть использованы штатные средства операционной системы. Для FLASH карт объемом до 4 ГБайт рекомендуется производить форматирование с типом файловой системы FAT16 (FAT).

Далее работа с FLASH картой памяти не отличается от работы со стандартным съемным USB FLASH накопителем. Необходимо только учесть, что при выключении компьютера, даже в случае наличия напряжения питания на разъеме USB, перезагрузке компьютера, отключении от компьютера, КНС отключит FLASH карту и для повторного ее подключения необходимо произвести повторную аутентификацию.

Для смены FLASH карты необходимо отключить КНС от компьютера.