R301 Форос USB для СКЗИ VipNet CSP
Инструкция по установке и эксплуатации

ООО "СмартПарк",
Москва, 127220, ул. 2-я Квесисская д. 24, корп. 3, офис №10.
Тел./факс: (495) 927-0033
Web: www.smart-park.ru
Техническая поддержка: help@smart-park.ru

Оглавление

Используемые термины, определения и сокращения

Пароль - это секретное слово или набор символов, предназначенный для подтверждения личности или полномочий.

ПИН - (англ. Personal Identification Number — персональный идентификационный номер) аналог Пароля.

Криптопровайдер (Cryptography Service Provider, CSP) - это независимый программный модуль, позволяющий осуществлять криптографические операции в операционных системах Microsoft.

Ключ - секретная информация, используемая криптографическим алгоритмом при зашифровании/расшифровании сообщений, генерации и проверке цифровой подписи, вычислении имитовставки.

Ути́лита (англ. *utility*) - специальная компьютерная программа, расширяющая стандартные возможности оборудования, выполняющая узкий круг специфических задач по администрированию оборудования

Администратор - администратор безопасности, администратор защиты - должностное лицо, устанавливающее политику безопасности и идентифицирующее объекты и участников, к которым применяется эта политика. Это субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации.

Оператор – физическое лицо управляющее работой компьютера.

1 Применение и назначение

Носитель R301 Форос USB для СКЗИ VipNet CSP (далее - Носитель) применяется совместно с криптопровайдерами компании Инфотекс (VipNet CSP 4.4 и выше, VipNet CSP Linux 4.4 и выше) в качестве носителя ключевой и идентификационной информации.

R301 Форос USB для СКЗИ VipNet CSP Ологически и физически объединяют носитель ФОРОС-смарт-карту-VipNet и компактный смарт-карт ридер. Носители соответствуют стандарту CCID, реализуют в себе решение Plug-and-Play и не требуют установки драйверов. Носитель имеет высокопрочный алюминиевый корпус и допускает его графическую кастомизацию при заказе партиями.

Носитель может использоваться совместно с программными продуктами, использующими криптопровайдеры VipNet CSP в качестве средства криптографической защиты информации (СКЗИ) соответствующего классам.

Основным назначением Носителя является:

- Безопасное хранение контейнеров программных СКЗИ VipNet CSP, пользовательских данных, сертификатов, паролей и др.;
- обеспечение защиты критических данных (в т.ч. закрытых ключей ЭП) в случае утери или хищения Носителя;
- организация строгой аутентификации в информационных системах и сервисах;
- обеспечение юридической значимости документов и действий пользователей с помощью электронной подписи;
- обеспечение возможности выполнения административных функций в т.ч. связанных с разблокировкой Носителей, заблокированных по причине превышения допустимого числа попыток неудачного предъявления пароля пользователя (ПИН пользователя).

2 Технические характеристики и конфигурация

Для хранения данных (ключей, сертификатов, идентификационных, аутентификационых и т.д.) Носитель использует защищенный смарт-карт микроконтроллер с объемом защищенной энергонезависимой памяти 80 или 160 Кбайт (по выбору потребителя), в которой размещается необходимая для этого файловая структура.

Основные технические характеристики Носителя приведены ниже в

таблице:

Параметр	R301 Форос USB 80	R301 Форос USB 160
Технические характеристики		
Физический объем защищенной памяти	80 Кбайт	160 Кбайт
Тип USB-разъема	Стандартный Тип А	
Интерфейс подключения	USB 2.0 Full Speed Device, 12 Мбит/сек	
Скорость обмена данными	до 323 Кбит/сек, 4 МГц; 500кбит/сек, 6МГц	
Поддерживаемые протоколы	ISO 7816 T=0	
Скорость чтения данных	до 13000 байт/с	
Поддержка CCID	Есть	
Габаритные размеры USB-носителя [Д х Ш х В]	48 х 16 х 8 мм	
Масса USB-носителя	6.3 г. +\-10%	
Потребляемая мощность USB-носителя	около 130 мВт в активном состоянии	
Диапазон рабочих температур	от 0 до +50˚С	
Диапазон температур хранения	от -20 до +50˚С	
Допустимая относительная влажность	от 0 до 85% (без конденсата)	
Время хранения данных	30 лет	
Гарантированное количество циклов стирания\записи	500 000	
Типовые параметры логической конфигурации контейнера PKCS#11 (для VipNet CSP 4.4…)*		
Допустимое кол-во ключевых пар ЭП, не менее	2	4
Допустимое кол-во открытых ключей ЭП, не менее	2	4
Размер области хранения открытых объектов [Кбайт]	14	31
Размер области хранения приватных объектов [Кбайт]	2	5
Максимальное число последовательных неуспешных попыток ввода пароля пользователя	5	
Функция разблокирования/восстановления пароля пользователя по паролю администратора	Есть	
Максимальное число последовательных неуспешных попыток ввода пароля администратора	5	
Функция форматирования (очистки)	Есть	
Доступ к функции форматирования (очистки)	по паролю Администратора	
Транспортное значение пароля Пользователя [символы ASCII – текста]	11111111	
Транспортное значение пароля Администратора [символы ASCII – текста]	87654321	

***) Указанные параметры могут уточняться производителем носителя**

При заказе партиями возможно изменение логической конфигурации Носителей под требования Заказчика, а также встраивание в Носитель дополнительных функциональных приложений, разработанных по ТЗ Заказчика.

3 Световая индикация режимов работы

Носитель имеет два встроенных светодиодных индикатора. Красный индикатор отображает состояние процессов информационного обмена смарт-

карт ридера с компьютером по USB, синий - отображает состояние процессов информационного обмена смарт-карт ридера с установленной в него смарт-картой.

Детализация состояний индикаторов приведена в нижеследующей таблице:

Назначение индикатора	Цвет	Состояние	Процесс
Индикатор USB	**Красный**	Мигает	Установка соединения по USB
		Непрерывно светит	Соединение по USB установлено
		Мигает нерегулярно	Обмен данными по USB
Индикатор смарт-карты	**Синий**	Выключен	Смарт-карты нет или она неисправна
		Непрерывно светит	Смарт-карта установлена
		Мигает	Обмен данными со смарт-картой

4 Установка Носителя в VipNet CSP

Программный модуль поддержки Носителя со стороны VipNet CSP устанавливается посредством установки библиотечного файла foros_pkcs11.dll в системный каталог \windows\system32 для версии x64 (и соответствующей версии в \windows\SysWOW64 для версии x86).

Также, для этого могут использоваться инсталляционные пакеты SetupForosPKCS11.msi (или SetupForosPKCS11x86.msi только для x86) соответственно.

После этого Носитель распознается встроенным в VipNet CSP модулем поддержки как носитель Magistra, Foros2.

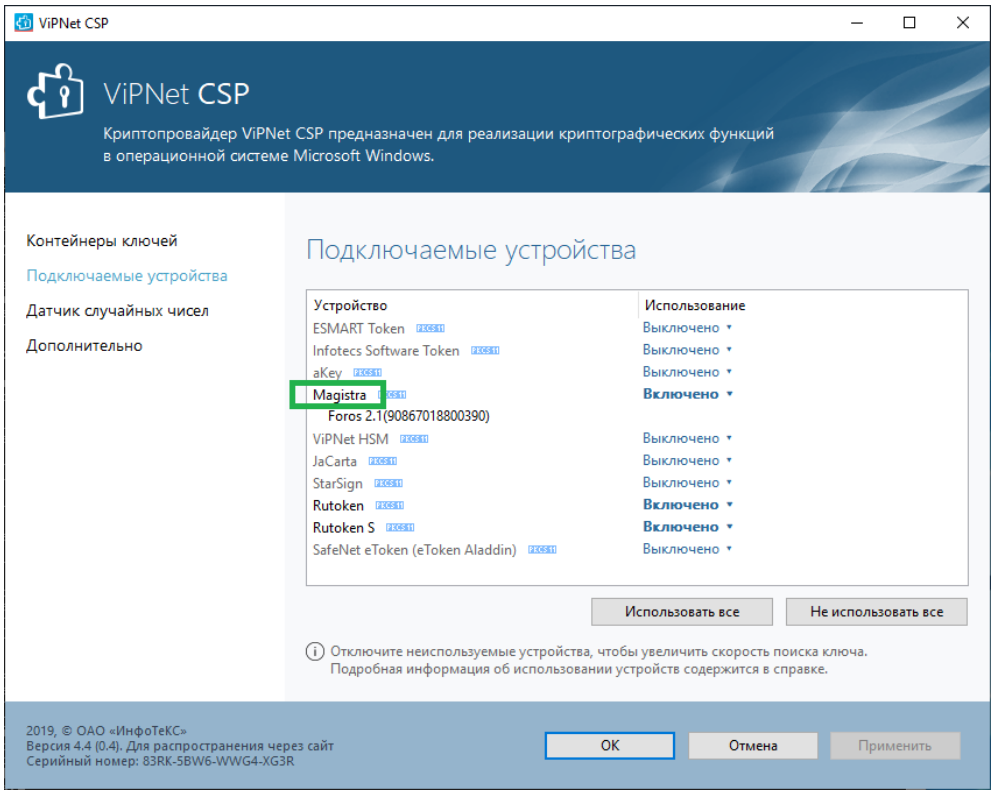

Рисунок 1

5 Эксплуатация Носителя в VipNet CSP

5.1 Схема разграничения доступа к данным

Доступ к приватным объектам данных PKCS#11 на Носителе защищается Паролем Пользователя (USER PIN).

Сервисы VipNet CSP запрашивают Пароль Пользователя при выполнении операций, требующих доступа к закрытой информации, хранящейся на Носителе.

У Пользователя есть 5 (Пять) попыток (параметр устанавливается по умолчанию) для ввода (предъявления) правильного значения Пароля Пользователя. Если все попытки предъявления Пароля Пользователя будут неудачными, то механизм его предъявления будет **заблокирован** автономным механизмом Носителя, и последующий доступ криптопровайдера к приватным объектам данных будет невозможен даже в после ввода верного значения Пароля Пользователя.

Разблокирование механизма ввода Пароля Пользователя и некоторые другие административные функции можно выполнить лишь при условии подтверждения оператором права Администратора путем успешного ввода Пароля Администратора (SO PIN). Способы доступа к механизмам администрирования описаны ниже.

Механизм ввода Пароля Администратора допускает строго ограниченное число последовательных попыток неудачного ввода. При достижении этого числа Пароль Администратора блокируется.

5.2 Механизмы администрирования Носителя

Носитель ФОРОС PKCS#11 предоставляет возможность разблокирования пароля пользователя (USER PIN), а также его смены (переустановки), смены пароля администратора и очистку данных пользователя. Для этого в Носителе предусмотрен соответствующий механизм разблокирования, основанный на использовании пароля администратора.

Для доступа оператора и/или администратора безопасности к механизму разблокирования носителей предоставляется утилита UnblockPKCS11.exe. Для ее эксплуатации также необходима библиотека PKCS#11 ***foros_pkcs11.dll***, которая должна быть доступна в путях поиска исполняемых модулей.

Утилита UnblockPKCS11.exe предназначена для использования администраторами безопасности систем. Режим использования утилиты, способы распространения, хранения и применения значений

административных паролей определяется регламентом безопасности системы.

Доступ к механизму разблокирования/смены паролей в носителях становиться возможным после успешного выполнения процедуры предъявления права администратора.

Данное право подтверждается путем предъявления соответствующего секретного элемента в форме пароля администратора (SO PIN).

Предъявление пароля администратора осуществляется в рамках взаимодействия оператора с утилитой разблокирования (UnblockPKCS11.exe).

При первичной конфигурации носителей их производителем, в каждый носитель загружается соответствующий ПИН администратора со значением «по-умолчанию». При вводе Носителя в эксплуатацию это значение необходимо заменить на другое.

Режим дальнейшего использования функции разблокирования в системе должен определяется действующими в конкретных системах правилами и регламентами безопасности.

5.3 Управление паролем (ПИН) пользователя

5.3.1 Режим смены пароля (ПИН) пользователя

5.3.1.1 Необходимое условие успешного выполнения

- Оператор знает пароль пользователя для контейнера PKCS#11, с которым производится процедура смены.
- В распоряжении оператора имеется утилита разблокирования.

5.3.1.2 Порядок действий

1. Оператор подключает Носитель к компьютеру.
2. Оператор запускает утилиту разблокирования (UnblockPKCS11.exe).
3. Оператор выбирает считыватель, в котором находится необходимый Носитель (например, «Feitian SCR301 0»)
4. Оператор «нажимает кнопку» «Изменить», расположенную в разделе «ПИН пользователя» окна программы.

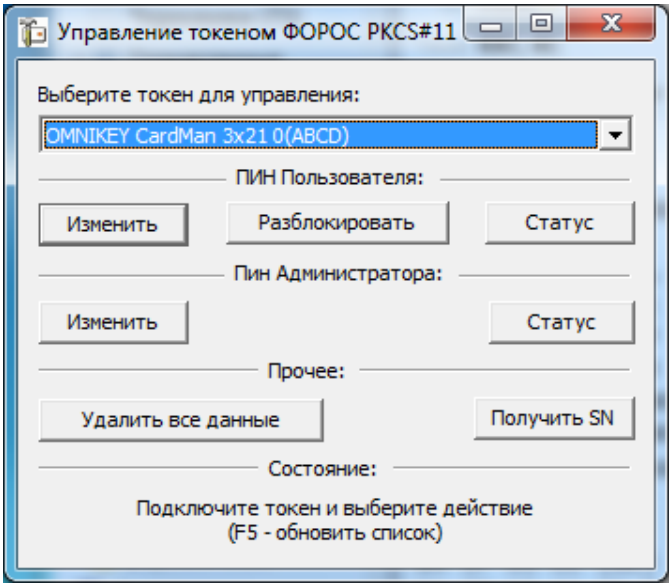

Рисунок 2

5. Оператор вводит прежнее значение ПИН пользователя в поле «Текущий ПИН пользователя».
6. Оператор вводит новое значение ПИН пользователя в полях «Новый ПИН» и «Повторите новый ПИН».
7. Оператор «нажимает» кнопку «Изменить».

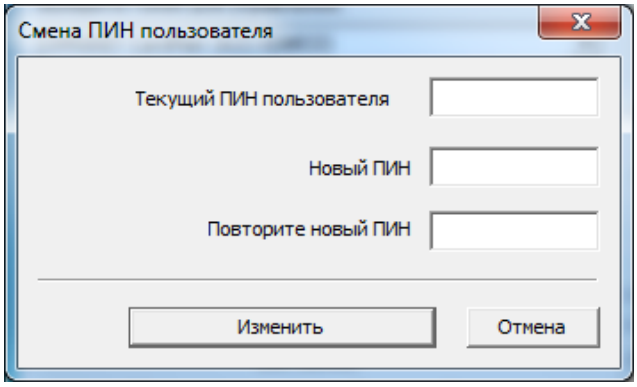

Рисунок 3

Если все данные введены правильно, то будет выполнена операция смены ПИН пользователя.

5.3.2 Режим разблокирования/установки ПИН пользователя

5.3.2.1 Необходимое условие успешного выполнения

- Оператору известен ПИН администратора для носителя, с которым производится процедура разблокирования ПИН пользователя.
- В распоряжении оператора имеется утилита разблокирования.

5.3.2.2 Порядок действий

1. Оператор подключает носитель с заблокированным ПИН пользователя к компьютеру.

2. Оператор запускает утилиту разблокирования (UnblockPKCS11.exe).

3. Оператор выбирает считыватель, в котором находится необходимый Носитель (например, «Feitian SCR301 0»).

4. Оператор «нажимает» кнопку «Разблокировать», расположенную в разделе «ПИН пользователя» окна программы.

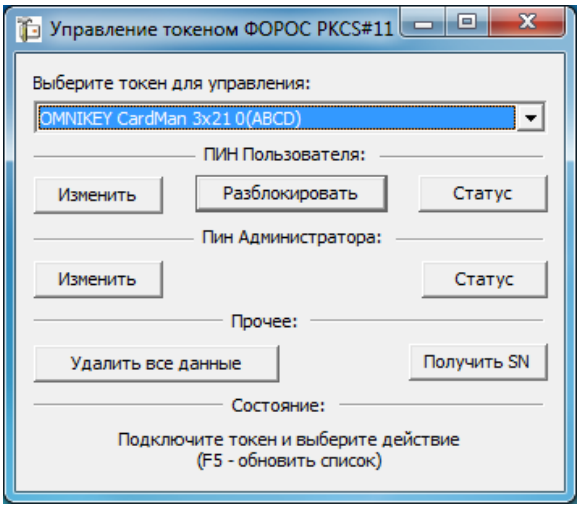

Рисунок 4

5. Оператор вводит значение ПИН администратора в поле «Текущий ПИН администратора».

6. Если необходимо также установить новое значение ПИН пользователя, то необходимо установить отметку по поле «Установить». В противном случае переход к п.8

7. Оператор вводит новое значение ПИН пользователя в полях «Новый ПИН» и «Повторите новый ПИН».

8. Оператор «нажимает» кнопку «Разблокировать».

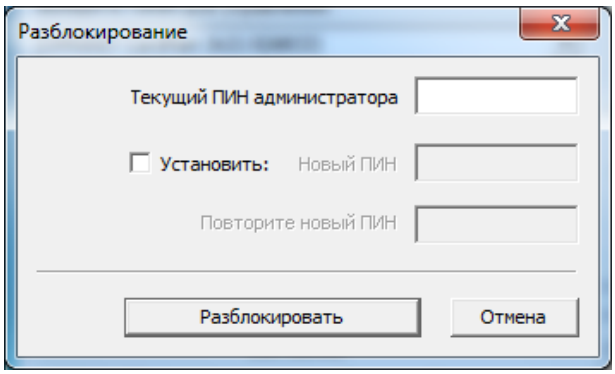

Рисунок 5

Если все данные введены правильно, то будет выполнена операция разблокирования (опционально: и установки) ПИН пользователя.

5.3.3 Режим проверки статуса ПИН пользователя

5.3.3.1 Необходимое условие успешного выполнения

- В распоряжении оператора имеется утилита разблокирования;

5.3.3.2 Порядок действий

1. Оператор подключает носитель к компьютеру.
2. Оператор запускает утилиту разблокирования (UnblockPKCS11.exe).
3. Оператор выбирает считыватель в котором находится необходимый Носитель (например, «Feitian SCR301 0»)
4. Оператор «нажимает» кнопку «Статус», расположенную в разделе «ПИН пользователя» окна программы.

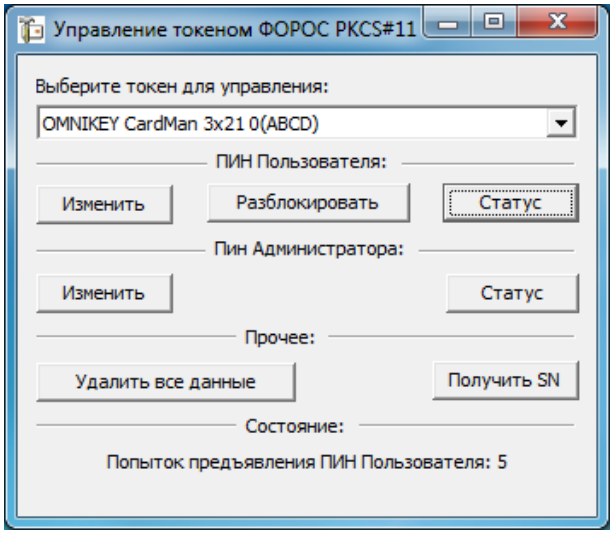

Рисунок 6

В случае успешного выполнения, в строке состояния будет выведена строка, описывающая количество оставшихся попыток предъявления ПИН пользователя, либо указывающая, что ПИН заблокирован.

5.4 Управление паролем (ПИН) администратора

5.4.1 Режим смены ПИН администратора

5.4.1.1 Необходимое условие успешного выполнения

- Оператору известен ПИН администратора для носителя, с которым производится процедура смены ПИН.
- В распоряжении оператора имеется утилита разблокирования.

5.4.1.2 Порядок действий

1. Оператор подключает носитель к компьютеру.
2. Оператор запускает утилиту разблокирования (UnblockPKCS11.exe).

3. Оператор выбирает считыватель в котором находится необходимый Носитель (например, «Feitian SCR301 0»)

4. Оператор «нажимает» кнопку «Изменить», расположенную в разделе «ПИН администратора» окна программы.

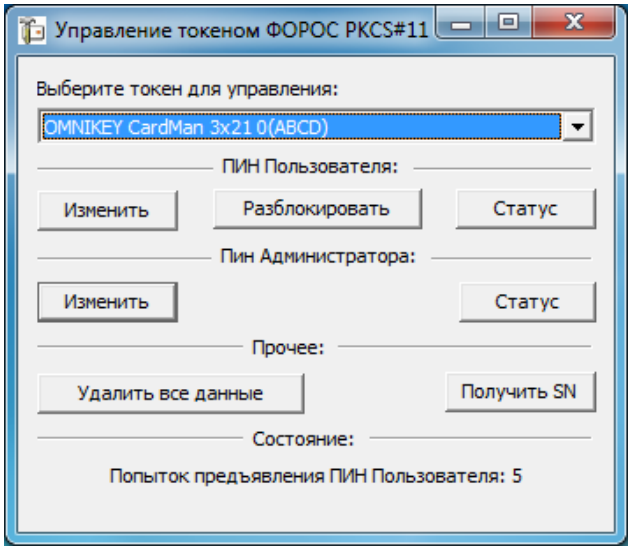

Рисунок 7

5. Оператор вводит значение ПИН администратора в поле «Текущий ПИН администратора».

6. Оператор вводит новое значение ПИН администратора в полях «Новый ПИН» и «Повторите новый ПИН».

7. Оператор «нажимает» кнопку «Изменить».

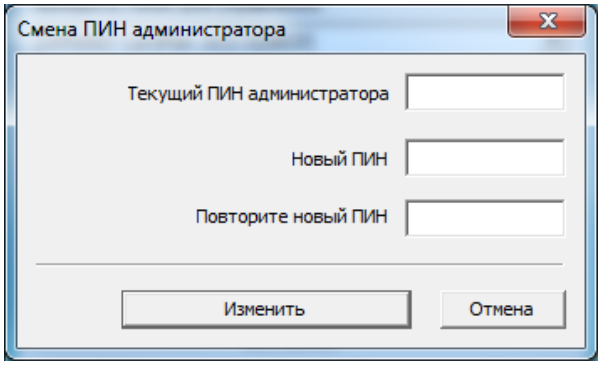

Рисунок 8

Если все данные введены правильно, то будет выполнена операция смены ПИН администратора.

5.4.2 Режим проверки статуса ПИН администратора

5.4.2.1 Необходимое условие успешного выполнения

- В распоряжении оператора имеется утилита разблокирования.

5.4.2.2 Порядок действий

1. Оператор подключает носитель к компьютеру.
2. Оператор запускает утилиту разблокирования (UnblockPKCS11.exe).
3. Оператор выбирает считыватель в котором находится необходимый Носитель (например, «Feitian SCR301 0»)
4. Оператор «нажимает» кнопку «Статус», расположенную в разделе «ПИН администратора» окна программы.

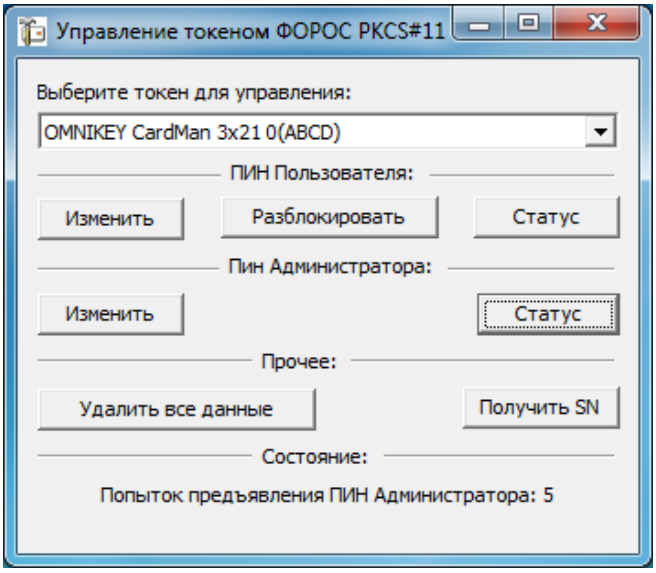

Рисунок 9

В случае успешного выполнения, в строке состояния будет выведена строка, либо описывающая количество оставшихся попыток предъявления ПИН администратора, либо указывающая, что ПИН заблокирован.

5.4.3 Режим удаления данных пользователя

5.4.3.1 Необходимое условие успешного выполнения

- Оператору известен ПИН администратора для носителя, с которым производится процедура смены ПИН.
- В распоряжении оператора имеется утилита разблокирования.

5.4.3.2 Порядок действий

1. Оператор подключает носитель к компьютеру.
2. Оператор запускает утилиту разблокирования (UnblockPKCS11.exe).
3. Оператор выбирает считыватель в котором находится необходимый Носитель (например, «Feitian SCR301 0»)
4. Оператор «нажимает» кнопку «Удалить все данные».

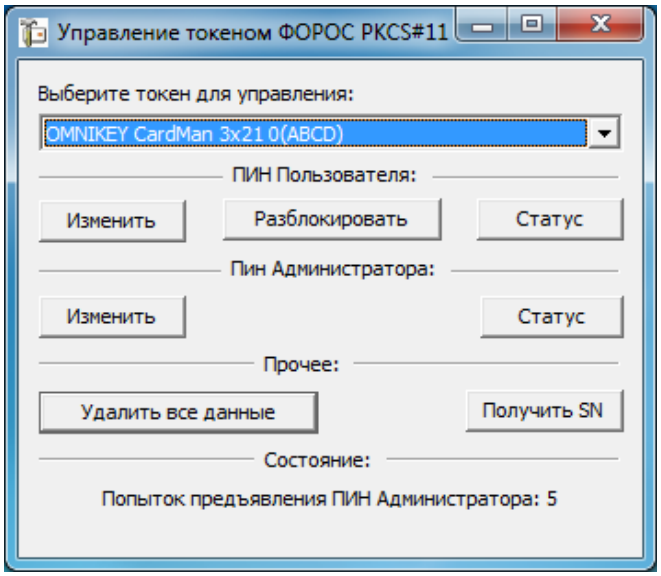

Рисунок 10

5. Оператор вводит новую метку, назначаемую Носителю и «нажимает» кнопку «Ввод».

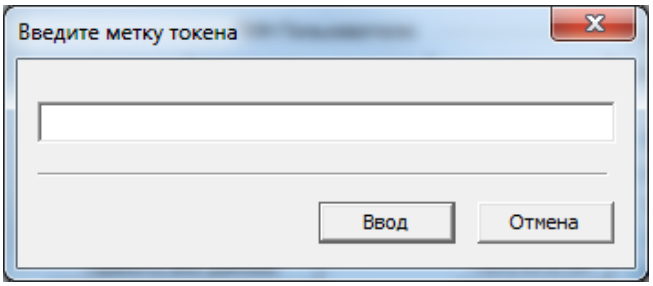

Рисунок 11

6. Оператор вводит значение ПИН администратора в поле «Текущий ПИН администратора».

7. Если необходимо также установить новое значение ПИН администратора, то необходимо установить отметку по поле «Установить». В противном случае переход к п.9

8. Оператор вводит новое значение ПИН администратора в полях «Новый ПИН» и «Повторите новый ПИН».

9. Оператор «нажимает» кнопку «Выполнить»

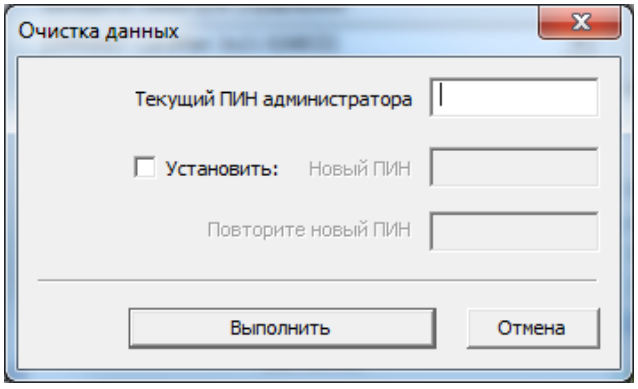

Рисунок 12

Если все данные введены правильно, то будет выполнена операция удаления данных пользователя. При этом ПИН пользователя будет установлен в значение «по-умолчанию».

6 Требования к условиям применения

6.1 Условия применения

Носитель предназначается для использования в закрытых помещениях в условиях влажности воздуха без конденсации влаги при температуре окружающей среды от 0º С до плюс 50º С.

Носители не должны подвергаться механическим воздействиям, приводящим к деформации корпуса, USB-разъема и нарушению их целостности.

Носители можно подключать только к USB-разъемам исправного компьютера.

Носители нельзя подвергать воздействию влаги, воздействию паров кислот, щелочей и других агрессивных примесей.

Категорически запрещается разбирать Носители.

6.2 Условия хранения

При складском хранении должны обеспечиваться следующие условия:

- хранение в складских помещениях, защищающих Носители от воздействия атмосферных осадков, в упаковке при отсутствии в воздухе паров кислот, щелочей и других агрессивных примесей;
- при длительном хранении Носителей, в складских помещениях должна обеспечиваться температура от плюс 5 до плюс 30°С и относительная влажность воздуха не более 85%;
- предельная температура хранения составляет от минус 20°С до плюс 50°С.

При хранении не допускаются резкие изменения температуры окружающего воздуха (более 20°С в час);

Распаковку Носителей в зимнее время после воздействия отрицательных температур следует производить в отапливаемом помещении, предварительно выдержав его в этом помещении не распакованным не менее двух часов.

6.3 Условия транспортировки

Транспортирование Носителей может производиться авиационным, автомобильным, железнодорожным или иным транспортом в условиях, исключающих механические повреждения, прямое попадание на

транспортную упаковку влаги, пыли и грязи, превышение предельных значений температуры окружающей среды.

При транспортировке должны соблюдаться следующие условия:

- температура окружающего воздуха от –20°С до +50°С;
- относительная влажность воздуха до 95% (без конденсации);
- исключение прямого воздействия солнечных лучей, атмосферных осадков и агрессивных примесей (паров кислот, щелочей);
- отсутствие повреждений упаковки.

После транспортировки Носителей при пониженной температуре, при последующем повышении температуры до нормальной, возможна конденсация влаги, в этом случае Носители необходимо выдержать при комнатной температуре до полного испарения конденсата.