ПАК R301 ФОРОС USB
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

Производитель оставляет за собой право вносить изменения в документацию изделий, без предварительного уведомления при выходе новой модификации изделия.

Актуальная документация предоставляется в комплекте при поставке изделий.

Оглавление

Используемые термины, определения и сокращения

Администратор - субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации, устанавливающий политику безопасности и идентифицирующий объекты и участников, к которым применяется эта политика.

Гость - Субъект доступа прикладной системы, обладающий уровнем доступа к функциям СКЗИ к которым не требуется предъявления какого-либо права.

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.

Носитель – носитель ПАК R301 ФОРОС USB и ПАК Смарт-карта ФОРОС.

ПАК - программно-аппаратный комплекс.

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

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

Пользователь - субъект доступа, участвующий в эксплуатации Носителя и использующий результаты его функционирования в пределах установленных для него прав и функций.

Прикладная система - автоматизированная информационная система или другое прикладное программное обеспечение, использующее Носители.

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

Оператор – физическое лицо управляющее работой компьютера.

ЭП - Электронная подпись в соответствии с ГОСТ Р 34.10-2001 и ГОСТ Р34.10-2012. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

1 Применение и назначение

Носитель ПАК R301 ФОРОС USB (далее - Носитель) интегрирует на единой платформе:

- функционал носителя ключевой и идентификационной информации для применения совместно с криптопровайдерами компании КриптоПро (КриптоПро CSP версии 3.0 и всеми последующими);

- функционал носителя ключевой и идентификационной информации для применения совместно с криптопровайдерами компании и Инфотекс (VipNet CSP версии 4.4 и всеми последующими, VipNet CSP Linux версии 4.4 и всеми последующими);

- функционал персонального электронного идентификатора в ОС Windows (2022/11/10/8.1/2019/2016/2012R2/8/2012/7/2008R2/Vista/2008/XP/2003,) в рамках информационной технологии компании Microsoft.

Каждый функциональный раздел Носителя реализован в форме изолированного и самодостаточного приложения с собственной файловой структурой охваченной собственной системой разграничения доступа. Носитель ФОРОС без дополнительной настройки готов к применению по любому из трех назначений или по всем одновременно.

Носитель является исполнением ФОРОС 2-КН R301 средства защиты информации (СЗИ) «Программно-аппаратный комплекс аутентификации, управления доступом и безопасного хранения информации и персональных данных пользователей, ключевой носитель ФОРОС 2» (сертификат ФСТЭК №4490 от 14 декабря 2021 г.).

ПАК R301 ФОРОС USB логически и физически объединяют носитель ФОРОС-смарт-карту и компактный смарт-карт ридер. Носители соответствуют стандарту CCID, Plug-and-Play и не требуют установки драйверов.

Носитель имеет высокопрочный корпус из алюминия и пластика и допускает его графическую кастомизацию при заказе партиями.

Носитель может использоваться совместно с программными продуктами, использующими криптопровайдеры КриптоПро CSP и VipNet CSP в качестве средств криптографической защиты информации (СКЗИ) соответствующих классам КС1, КС2 и КС3.

Основным назначением Носителя является:

- безопасное хранение контейнеров программных СКЗИ КриптоПро CSP и VipNet CSP, пользовательских данных, сертификатов, паролей и др.;
- обеспечение применения квалифицированной электронной подписи, сертификатов стандарта X509, обеспечение юридической

значимости документов и действий пользователей с помощью электронной подписи;

- 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 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 Прикладные возможности Носителя

Носитель ФОРОС совместим с СКЗИ "КриптоПро CSP" версий 3.6 и старше с дополнительной поддержкой функций администрирования.

Носитель совместим с СКЗИ "VipNet CSP" версий 4.4 с дополнительной поддержкой функций администрирования.

Через Минидрайвер (программный компонент между встроенным криптопровайдером Microsoft Smart Card Base Cryptographic Service Provider и носителем ФОРОС) Носитель может применяться как ключевой носитель для инструментов безопасности ОС Windows.

Для корпоративных Заказчиков в Носителях возможна реализация поддержки дополнительных приложений.

Поддерживаемые программные интерфейсы:

- Microsoft Crypto API
- PKCS#11
- Microsoft Smartcard API

Носитель работает в любых ОС с поддержкой спецификации PC/SC. В частности:

- Microsoft Windows XP и новее (в том числе Windows 8/8.1/10/11)
- Microsoft Windows Server 2003 и новее (в том числе 2012, 2012R2)
- GNU/Linux, в том числе отечественные
- Apple macOS 10.9 и новее
- Android 5 и новее
- iOS 11 и новее
- Аврора 4+

Поддерживаемые ОС в рамках работы носителя с СКЗИ «КриптоПро

CSP» смотрите в формуляре соответствующего СКЗИ «КриптоПро CSP».

Поддерживаемые ОС в рамках работы носителя с СКЗИ «VipNet CSP» смотрите в формуляре соответствующего СКЗИ «VipNet CSP».

3 Возможности использования Носителя для аутентификации пользователей

Носитель может применяться для реализации многофакторной аутентификации пользователей в качестве устройства аутентификации отделенного от информационной системы и предоставляет для этого следующие возможности:

- двухфакторная аутентификация по предъявлению самого Носителя, по предъявлению пароля (PIN-кода);
- поддержка 3-х категорий владельцев: Администратор, Пользователь, Гость;
- поддержка Глобальных паролей (PIN-кодов): Администратора и Пользователя;
- возможность поддержки комбинированной (многофакторной) аутентификации по произвольной схеме, в том числе по схеме «Администратор или Пользователь»;
- ограничение числа неудачных попыток ввода пароля (PIN-кода);
- настраиваемый минимальный размер пароля (PIN-кода) (для каждого пароля отдельно).
- разграничение доступа к файловым объектам в соответствии с уровнем доступа роли.

Опционально обеспечиваются следующие возможности:

- возможность поддержки паролей (PIN-кодов) для защиты конкретных прикладных объектов данных в памяти Носителя;
- создание паролей (PIN-кодов) и ключей аутентификации для защиты от НСД ключевой информации и/или прикладных данных, хранящихся в энергонезависимой памяти носителя; возможность одновременной работы с несколькими локальными/глобальными паролями (PIN-кодами) (до 127 шт.);
- аутентификация по Глобальным паролям (PIN-кодам) в сочетании с аутентификацией по Локальным паролям (PIN-кодам), аутентификация с применением криптоалгоритмов.

4 Специальные возможности Носителя

Носитель ФОРОС сертифицирован ФСТЭК России и может применяться для обработки информации ограниченного доступа, не составляющей государственную тайну:

- в значимых объектах критической информационной инфраструктуры до 1-ой категории,
- в государственных информационных системах до 1 класса защищенности,
- в автоматизированных системах управления производственными и технологическими процессами до 1 класса защищенности,
- в информационных системах персональных данных при необходимости обеспечения до 1 уровня защищенности персональных данных, в информационных системах общего пользования II класса.

Носитель обеспечивает:

- администрирование ключевой информацией с применением не удаляемых административных ключей;
- автономное журналирование ошибок операций безопасности;
- возможность доверенного считывания журнала ошибок операций безопасности;
- индикацию факта смены паролей (PIN-кодов) с транспортных значений на рабочие.

Носитель оснащен:

- автономным счетчиком смен паролей (PIN -кодов);
- встроенным счетчиком изменений файловой системы;
- встроенными средствами контроля в составе:
  - контроль целостности исполняемого программного кода носителя (микропрограммы);
  - контроль целостности системных областей памяти Носителя;
  - проверка целостности файлов (SF, BF, KF…) в памяти Носителя перед любым их использованием;
  - контроль конфигурации файловой структуры Носителя, защита от несанкционированного внесения изменений (контроль аутентичности) по криптографической контрольной сумме;
  - проверка правильности функционирования встроенных в Носитель криптографических алгоритмов.

5 Технические характеристики и конфигурация приложений Носителя

Для хранения данных (ключей, сертификатов, идентификационных, аутентификационых данных и т.д.) Носитель использует ориентированный на применение в смарт-картах специализированный защищенный микроконтроллер. Объем защищенной энергонезависимой памяти составляет 80 или 160 Кбайт (в зависимости от модификации Носителя). В программной

памяти Носителя размещается встроенная операционная система соответствующая стандартам группы ГОСТ Р ИСО МЭК 7816, а в энергонезависимой памяти носителя размещается файловая структура приложений Носителя соответствующая положениям стандарта ГОСТ Р ИСО МЭК 7816-4.

Низкоуровневый интерфейс носителя соответствует положениям стандарта ГОСТ Р ИСО МЭК 7816-4, высокоуровневый интерфейс определяется применяемым операционным окружением и прикладным ПО.

Архитектура файловой системы построена на основе File Allocation Table (FAT). Количество папок в файловой системе и уровень их вложенности ограничен только объемом свободной памяти.

Ключевая информация на носителе хранится в специальных защищенных файлах (EF с атрибутами безопасности). Для хранения разных видов ключевой информации используются предопределенные папки с автоматическим выбором нужной папки при создании и использовании EF-файлов.

Ниже в таблице приведены технические характеристики и конфигурация приложений Носителя.

Таблица 1. Технические характеристики и конфигурация приложений Носителя

Параметр	**ПАК R301 ФОРОС USB**	
Технические характеристики		
Физический объем защищенной энергонезависимой перепрограммируемой памяти	80 Кбайт	160 Кбайт
Объем памяти доступной для размещения файловой структуры, ключевой информации	65 Кбайт	137 Кбайт
Тип USB-разъема	Стандартный Тип А	
Интерфейс подключения	USB 2.0 ISO/IEC 7816-12, 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 x Ш x В]	48 x 16 x 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 +70˚С	
Диапазон температур хранения	от -40 до +85˚С	
Допустимая относительная влажность	от 0 до 85% (без конденсата)	
Время хранения данных	30 лет	
Гарантированное количество циклов стирания\записи	1,000,000	
Типовые параметры логической конфигурации «контейнера» для КриптоПро CSP*		
Число контейнеров	4	8
Размер контейнера (допустимый размер сертификата)	7 Кбайт	9 Кбайт
Поддержка ключей 512 бит ГОСТ Р34.10-2012	Есть	
Политика смены пароля Пользователя: Пользователь или Администратор	Выбирается по умолчанию	
Политика смены пароля Пользователя: только	Устанавливается по отдельному запросу	

Пользователь	Заказчика	
Возможность изменения политики смены пароля Пользователя	При инициализации носителя	
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	
Функция форматирования (очистки) по паролю Администратора	Выбирается по умолчанию	
Функция форматирования (очистки) свободнодоступная	Устанавливается по отдельному запросу Заказчика	
Транспортное значение пароля Пользователя [символы ASCII – текста]	11111111	
Транспортное значение пароля Администратора [символы ASCII – текста]	87654321	
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]	12	31
Размер области хранения приватных объектов [Кбайт]	2	6
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	
Специальные параметры		
Подсчет числа смен паролей (ПИН)	Есть	
Индикация смены транспортных значений паролей (ПИН)	Есть	
Журнал событий с доверенным получением	Есть	
Поддержка ФОРОС Windows	Есть	

*) Указанные параметры могут уточняться производителем носителя

При заказе Носителей партиями, по запросу Заказчика возможно применение опциональных параметров, а также изменение логической конфигурации Носителей. Также возможно встраивание в Носитель дополнительных функциональных приложений, реализуемых по требованиям Заказчика.

6 Аппаратные криптографические возможности

- ГОСТ Р 34.10-2001 генерация ключевых пар с проверкой качества, формирование и проверка электронной подписи;

- ГОСТ Р 34.10-2012/ГОСТ 34.10-2018 (256 бит и 512 бит[1,2]): генерация ключевых пар с проверкой качества, формирование и проверка электронной

подписи;

- ГОСТ Р 34.11-94: вычисление значения хеш-функции данных, в том числе с возможностью последующего формирования электронной подписи;

- ГОСТ Р 34.11-2012/ГОСТ 34.11-2018 (256 бит и 512 бит[1,2]): вычисление значения хеш-функции данных, в том числе с возможностью последующего формирования электронной подписи;

- ГОСТ 28147-89: генерация ключей шифрования (запрет экспорта)[3], шифрование данных в режимах простой замены, гаммирования и гаммирования с обратной связью, вычисление и проверка криптографической контрольной суммы данных (имитовставки ГОСТ);

- ГОСТ Р 34.12-2015/ГОСТ 34.12-2018, ГОСТ Р 34.13-2015/ГОСТ 34.13-2018 алгоритм шифрования «Кузнечик»: генерация (запрет экспорта) и импорт ключей шифрования, шифрование данных в режимах простой замены, гаммирования и гаммирования с обратной связью, вычисление и проверка криптографической контрольной суммы данных (имитовставки ГОСТ)[2];

- ГОСТ Р 34.12-2015/ГОСТ 34.12-2018, ГОСТ Р 34.13-2015/ГОСТ 34.13-2018 алгоритм шифрования «Магма»: генерация и импорт ключей шифрования, шифрование данных в режимах простой замены, гаммирования и гаммирования с обратной связью, вычисление и проверка криптографической контрольной суммы данных (имитовставки ГОСТ)[2,3];

- выработка сессионных ключей (ключей парной связи):
  - по схеме VKO GOST R 34.10-2001 (RFC 4357);
  - по схеме VKO GOST R 34.10-2012 (RFC 7836)[2,3];

- Расшифрование по схеме EC El-Gamal[2];

- RSA: поддержка ключей размером 1024, 2048, 4096[4] бит, генерация ключевых пар с настраиваемой проверкой качества[4], импорт ключевых пар, формирование электронной подписи;

- ECDSA с кривыми secp256k1[4] и secp256r1[2]: генерация ключевых пар с настраиваемой проверкой качества, импорт ключевых пар, формирование электронной подписи;

- AES, DES, 3DES, SHA1, TDES MAC- 8, AES MAC-16 [2];

- генерация последовательности случайных чисел требуемой длины.

1 – применяется в ОС «Магистра 1.30» совместно с использованием соответствующего криптопровайдера

2 – доступно в СКЗИ ОС «ФОРОС 2.01» (ОС «Магистра 2.01»)

3 – доступно в рамках СКЗИ «ФОРОС 2», «ФОРОС 3»

4 – применяется совместно с использованием соответствующего криптопровайдера

7 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:

Таблица 2. Состояния индикаторов Носителя ПАК R301 ФОРОС USB

Назначение индикатора	Цвет	Состояние	Процесс
Индикатор USB	**Красный**	Мигает	Установка соединения по USB
		Непрерывно светит	Соединение по USB установлено (готовность к работе)
		Мигает нерегулярно	Обмен данными по USB (выполнение операций)
		Не светит	Нарушение системной области, неисправность
Индикатор смарт-карты	**Синий**	Выключен (не светит)	Смарт-карты нет или она неисправна, нарушение системной области
		Непрерывно светит	Смарт-карта установлена (готовность к работе)
		Мигает	Обмен данными со смарт-картой (выполнение операций)

8 Поддержка Носителя в КриптоПро CSP

Программный модуль поддержки Носителя со стороны КриптоПро CSP встроен в дистрибутив КриптоПро CSP начиная с версии 3.0.

Дополнительная инсталляция Носителя в криптопровайдере не требуется. Он распознается встроенным в КриптоПро CSP модулем поддержки как носитель «Foros (Magistra)».

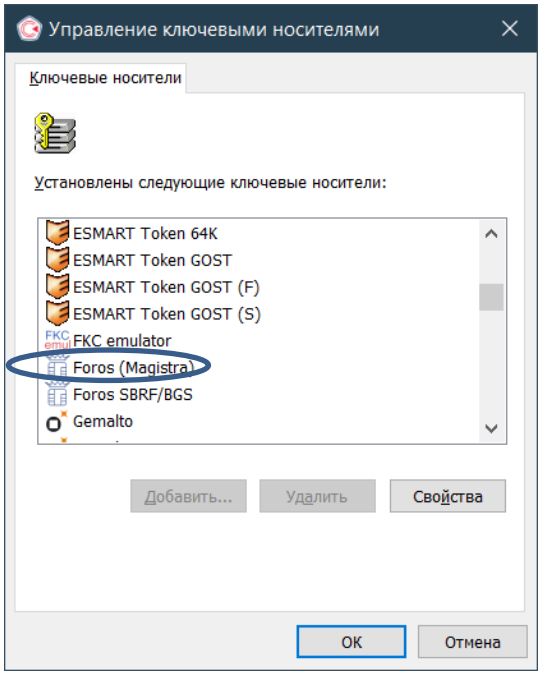


Рисунок 1

9 Поддержка Носителя в VipNet CSP

Программный модуль поддержки Носителя со стороны VipNet CSP устанавливается посредством установки модуля поддержки foros_pkcs11.dll соответствующей версии в системный каталог \windows\system32 для версии x64 или в \windows\SysWOW64 для версии x86.

Инсталляционный пакет в форме архива «ForosPKCS11.zip» доступен по ссылке:

http://smart-park.ru/util/ForosPKCS11.zip

Для установки модуля поддержки следует использовать имеющиеся в архиве пакеты x64 или x86 в зависимости от модели компьютера.

После успешной установки Носитель распознается встроенным в VipNet CSP модулем поддержки подключаемых устройств как носитель «R301 Foros» (в некоторых версиях VipNet CSP - «Magistra»).

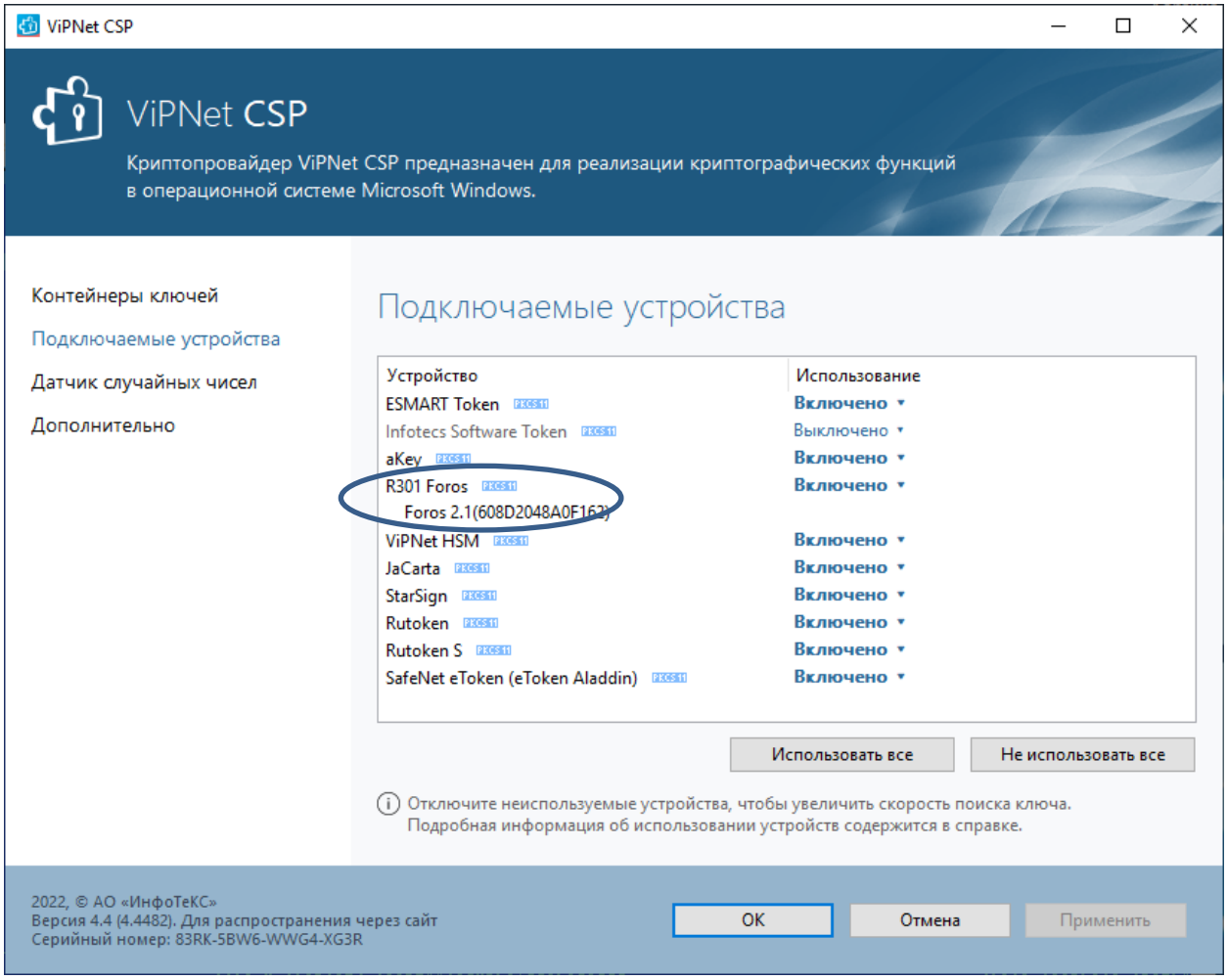


Рисунок 2

10 Эксплуатация Носителя в КриптоПро CSP

10.1 Схема разграничения доступа к данным Носителя

Доступ к размещенному в Носителе контейнеру КриптоПро CSP защищается встроенным в носитель механизмом аутентификации Пользователя по паролю (по ПИН-коду) (ПИН Пользователя). Сервисы КриптоПро CSP запрашивают этот ПИН у Пользователя и направляют его Носителю для аутентификации Пользователя при выполнении операций, требующих доступа к закрытой информации, хранящейся на Носителе.

У Пользователя есть 5 (Пять) попыток для ввода (предъявления) правильного значения *ПИН* (Пароля) Пользователя. Если все попытки предъявления ПИН (Пароля) Пользователя будут неудачными, то механизм аутентификации Пользователя будет **заблокирован** Носителем. После этого последующий доступ криптопровайдера к закрытой информации Носителя будет невозможен даже в случае ввода верного значения Пароля Пользователя.

Разблокирование Пароля Пользователя, а также некоторые другие административные функции, можно выполнить лишь при условии предъявления оператором права Администратора путем успешного ввода Пароля Администратора (иначе - ПИН Администратора).

Механизм ввода ***ПИН*** (Пароля) Администратора допускает строго ограниченное число последовательных попыток неудачного ввода. При достижении этого числа Пароль Администратора блокируется. После этого восстановление работоспособности Носителя для сервисов криптопровайдера становится возможным, только если в Носителе предусмотрен опциональный свободный доступ к функции форматирования (очистки). Если доступ к функции форматирования ***(очистки)*** установлен «по Паролю Администратора» (устанавливается «по умолчанию»), то восстановление доступа к механизмам администрирования невозможно.

Примечание. Функция форматирования (см. п. 10.7) удаляет из Носителя все данные контейнера КриптоПро. При ее выполнении требуется указывать новые значения паролей Пользователя и Администратора.

При производстве Носителей устанавливается безопасный режим доступа к функции форматирования «по паролю Администратора». При заказе партий Заказчик имеет возможность указать на необходимость установки опционального режима свободного доступа к функции форматирования.

Примечание. Заказчику следует учитывать, что производитель Носителей считает этот режим небезопасным, поскольку существенно упрощает реализацию атаки типа «отказ в обслуживании».

На случай утери рабочего значения пароля Пользователя, в Носителе предусмотрена возможность выполнения его смены также и на основании предъявленного пароля Администратора.

При заказе партиями Заказчик имеет возможность указать на необходимость установки опционального режима «смена пароля пользователя по паролю пользователя». Также Заказчик может запросить установку собственных ограничений по числу допустимых последовательных попыток неудачного предъявления паролей Пользователя и Администратора в диапазоне от 2 до 15.

10.2 Специальные механизмы Носителя

10.2.1 Механизм регистрации событий

В носитель встроен механизм регистрации ошибок (механизм журналирования).

Журнал формируется встроенным в Носитель программным обеспечением в энергонезависимой памяти микроконтроллера Носителя. Журнал представляет собой циклический файл записей, он не доступен для записи извне, но может быть свободно прочитан. При заполнении журнала новая запись затирает самую старую. Размер журнала устанавливается при производстве носителя.

Запись в журнале формируется самим Носителем при возникновении ошибок исполнения низкоуровневых команд. Каждая запись содержит сквозной номер и информацию о низкоуровневой команде, выполненной с ошибкой (код команды, параметры команды, код ошибки).

Журнал может быть свободно прочитан из памяти Носителя средствами административной утилиты.

Содержание журнала предназначается для служб технической поддержки.

10.2.2 Механизм доверенной выгрузки журнала [*)]

Каждый экземпляр носителя содержит административную ключевую пару, записываемую в память Носителя в процессе его производства. Соответственно выгружаемое из Носителя содержимое журнала сопровождается электронной подписью формируемой Носителем на этом (административном) ключе.

Административная утилита предоставляет возможность прочитать (функция «Прочитать журнал») журнал с электронной подписью, а также проверить целостность и аутентичность полученных данных путем проверки подписи журнала (функция «Проверить журнал»).

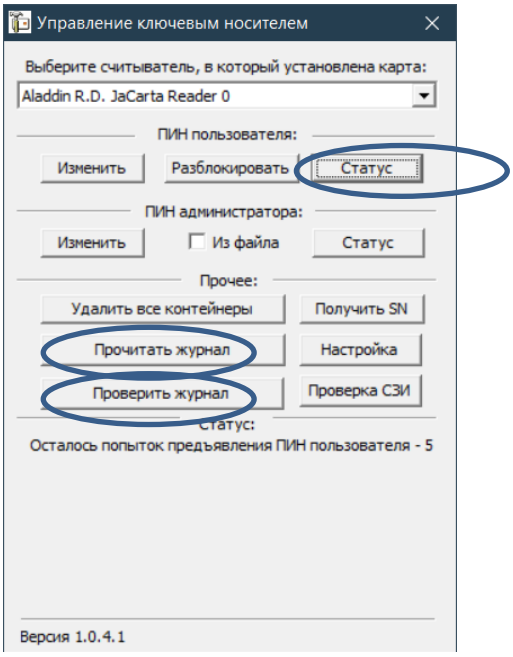


Рисунок 3

В результате успешного выполнения функции «Прочитать журнал» на экран выводится окно «Управление журналом», содержащее считанную из журнала информацию, которая представлена в виде текста.

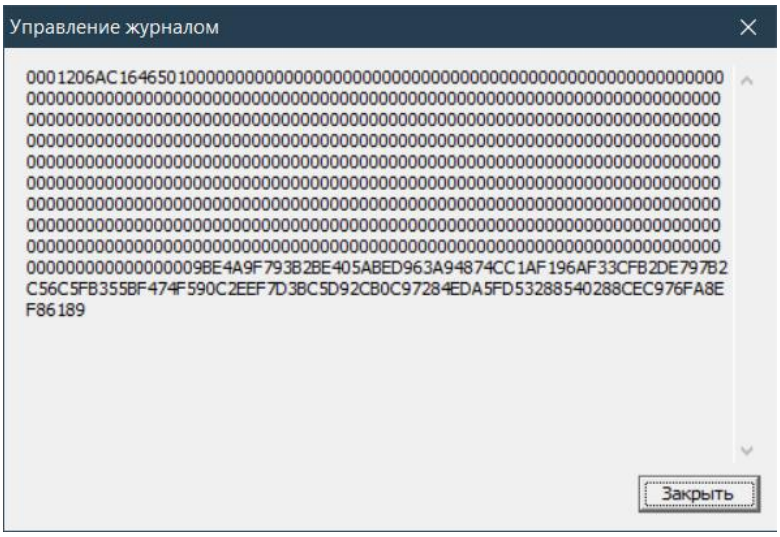


Рисунок 4

Информация из журнала может быть «передана» на проверку целостности и аутентичности. Для этого следует «выделить» стандартным образом (движением «мышки» при нажатой левой кнопке) все содержимое прочитанного журнала и скопировать его в обменный буфер:

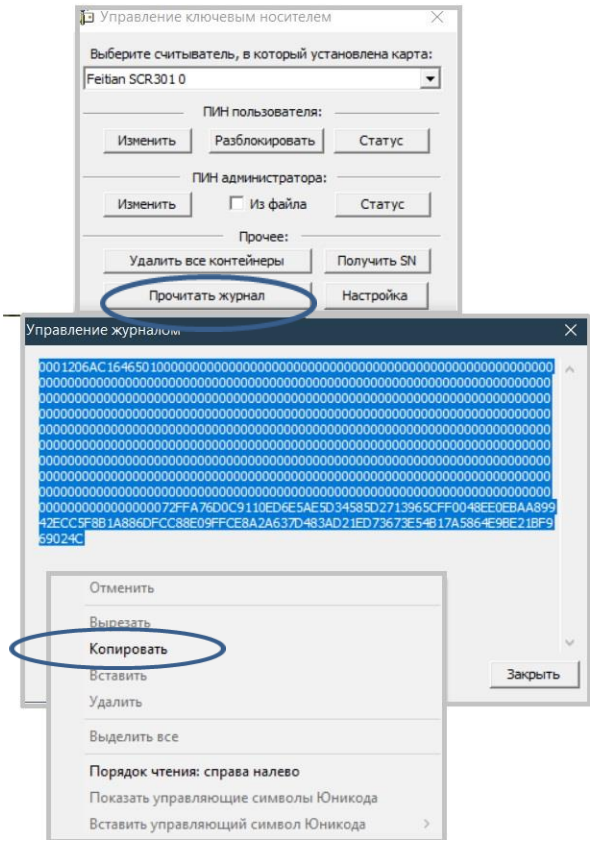


Рисунок 5

Содержимое Журнала может быть проверено «на месте». Для этого следует активировать выполнение функции «Проверить журнал», «вставить» проверяемую информацию из буфера и активировать функцию «Проверить журнал» в окне «Управление журналом».

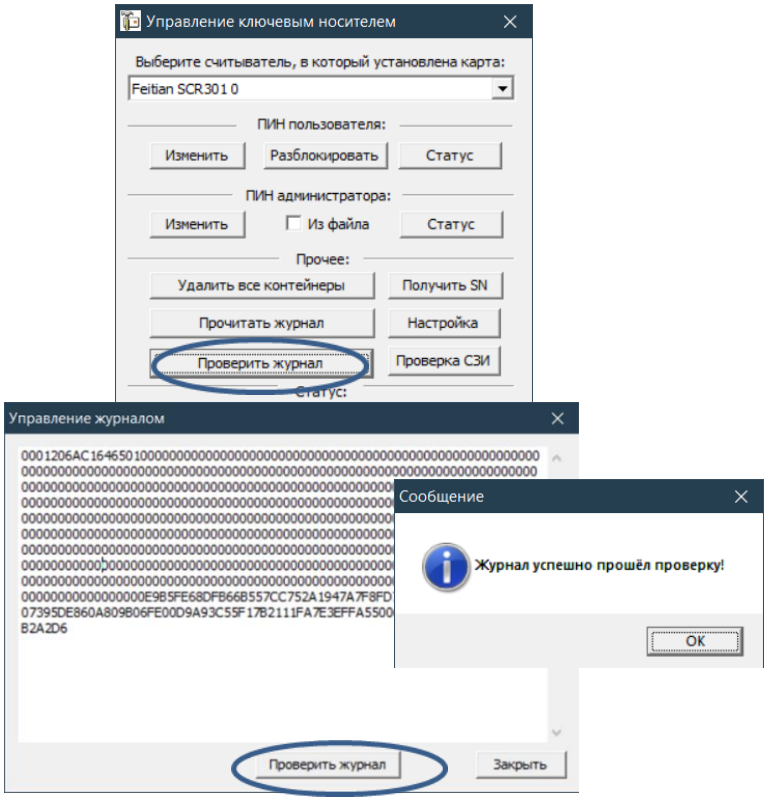


Рисунок 6

Если проверяемое содержимое журнала искажено, то будет выдано сообщение об ошибке.

Содержимое журнала защищено от несанкционированного изменения. Как текстовое сообщение оно может быть отправлено по обычным каналам связи в техподдержку для технического анализа нештатных ситуаций.

*) Не в полном объеме поддерживается для младшей версии Носителя (с памятью 80 Кбайт).

10.2.3 Механизм подсчета числа смен паролей

Носитель имеет встроенный механизм подсчета числа смен значений паролей (ПИН-кодов).

Каждый пароль имеет индивидуальный сквозной не реверсивный двух байтовый счётчик, увеличивающийся на 1 при выполнении каждой операции смены (перезаписи) значения пароля. При достижении счётчиком максимального значения 0xFFFFh дальнейшая смена пароля запрещается. Предполагается, что в условиях нормальной эксплуатации максимальное значение счетчика смен недостижимо.

Текущее состояние счетчика смен паролей пользователя и администратора доступно для чтения средствами административной утилиты. Это обеспечивает справочная функция «Статус» (см. Рисунок 7) - запрос статуса Пароля (ПИН).

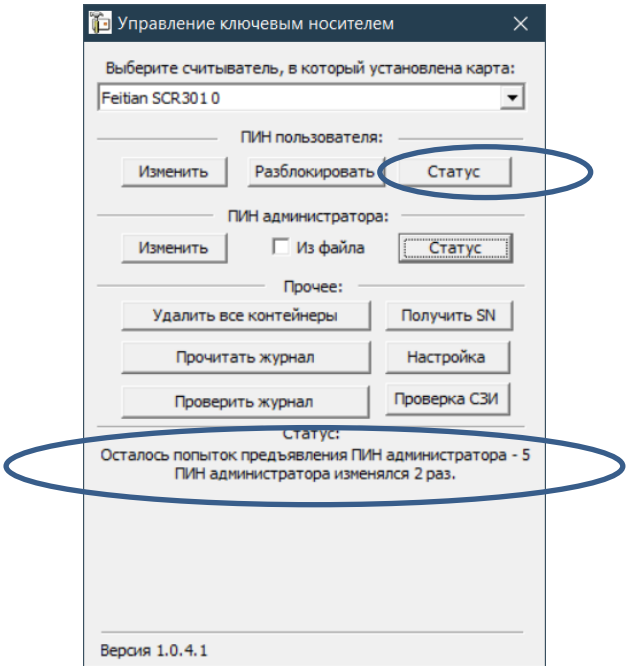


Рисунок 7

10.2.4 4-х байтовый серийный номер

Носитель может идентифицироваться по 4-х байтовому серийному номеру либо по 7-ми байтовому заводскому номеру микроконтроллера.

4-х байтовый серийный номер совпадает с номером носителя, выводимым панелью управления криптопровайдера КриптоПро CSP.

Административная утилита предоставляет возможность прочитать серийные номера Носителя. Для этого служит функция «Получить SN» (см. Рисунок 8).

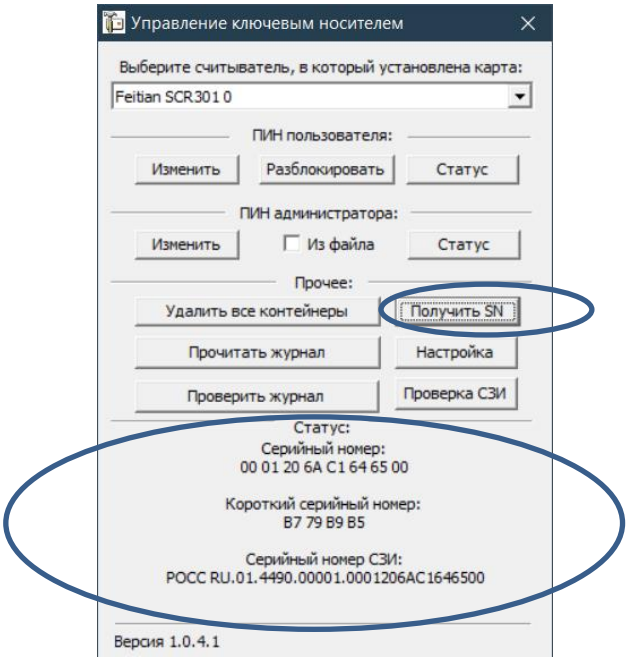


Рисунок 8

10.2.5 Механизм активации и деактивации минидрайвера

Носитель предоставляет возможность активировать и деактивировать функционал минидрайвера.

Примечание. Деактивация минидрайвера необходима для устранения конфликтной ситуации в случае применения функции КриптоПро Winlogon.

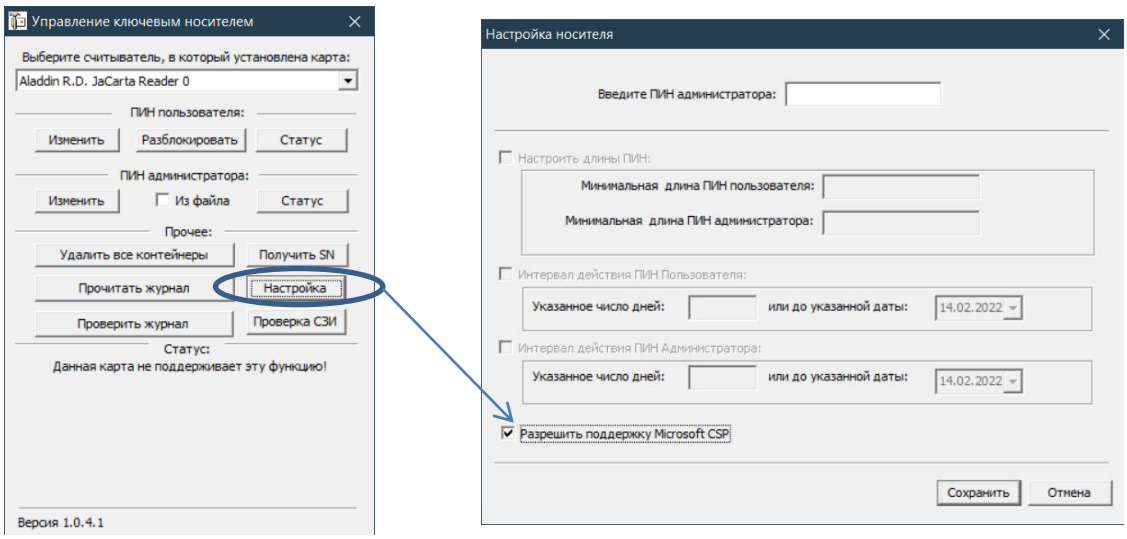


Рисунок 9

Минидрайвер деактивируется путем установки запрета поддержки Носителем Microsoft CSP (см. Рисунок 9).

По умолчанию Минидрайвер на Носителе деактивирован.

10.3 Механизмы администрирования Носителя

Набор административных функций Носителя включает:

- функции разблокирования Пароля Пользователя;
- функции смены значений Пароля Администратора и пароля Пользователя;
- функции форматирования (очистки) Носителя;
- функции считывания и проверки журнала ошибок;
- функции активации/деактивации минидрайвера;
- справочные функции (получение серийных номеров, параметров состояния паролей);
- контрольные функции (проверка СЗИ, контроль целостности микропрограммы);
- функции работы с журналом;
- настройка параметров административной утилиты.

Предъявление Пароля Администратора, выполнение разблокирования, смены значений Паролей и проч. возможно с помощью утилиты разблокирования UnblockUserPin или новой административной программы ForosMaster.

Утилита UnblockUserPin может быть загружена с сайта ООО «СмартПарк» на странице:

https://smart-park.ru/support/#div_block-29-30

или по прямой ссылке:
https://smart-park.ru/wp-content/uploads/utils/UnblockUserPin.zip

Программа управления носителями ФОРОС FOROS-Master может быть загружена с сайта ООО «СмартПарк» на странице:
https://smart-park.ru/support/#div_block-29-30

или по прямой ссылке:
https://smart-park.ru/wp-content/uploads/utils/FMaster.zip

Соответствующие описание и инструкции приведены в документах «ФОРОС-Мастер_Руководство Администратора» и «ФОРОС-Мастер_Руководство Пользователя».

Также доступна возможность реализации административного управления носителями ФОРОС с помощью web-приложения реализуемого Заказчиком самостоятельно на основе применения продукта «ForosWKT».

Пакет «ForosWKT» доступен для применения с Web-браузерами Microsoft Internet Explorer (версии 10, 11) и Google Chrome (версия 52 и выше).

Продукт применяется путем встраивания обращений к интерфейсу администрирования ключевым контейнером КриптоПро CSP, размещенным на носителе "ФОРОС", в пользовательские WEB-страницы.

Разработка пользовательских WEB-страниц может выполняться с применением программного пакета ForosWKT SDK (см. ForosWKT SDK. Общее описание. 6958 6427. 58.29.29.000.001-2. 31.01.1).

Программно-доступный, интерфейс ForosWKT описан в документе ForosWKT. Руководство программиста (6958 6427. 58.29.29.000.001. 33.01.1).

Указанная документация, а также пакет ForosWKT SDK предоставляются по отдельному запросу.

Тестовая страница (образец применения) размещена на сайте ООО "СмартПарк" по адресу:
http://smart-park.ru/foroswkt/testpage.html

Программное обеспечение «ForosWKT» может быть загружено с сайта ООО «СмартПарк» по ссылке:
https://smart-park.ru/wp-content/uploads/utils/ForosWKT.rar

В рамках настоящего документа применение ForosWKT далее не рассматривается.

10.4 Смена ПИН (пароля) Пользователя

Внимание!

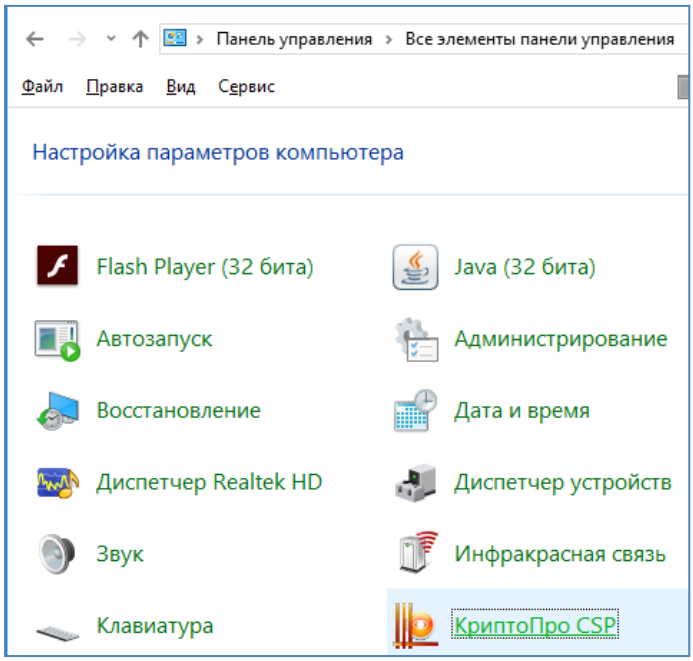
При вводе Носителя в эксплуатацию, Пользователь должен сменить установленное производителем транспортное значение Пароля Пользователя, на собственное.

Сохранение в тайне рабочего значения Пароля Пользователя и его своевременная смена, являются необходимыми условиями безопасной эксплуатации Носителя в рамках сервисов криптопровайдера.

Производитель настоятельно рекомендует не использовать простых комбинаций символов для паролей Носителя.

Смена Пароля Пользователя в штатном режиме производится средствами криптопровайдера КриптоПро CSP в «Панели управления».

Откройте оснастку управления КриптоПро CSP в «Панели управления»



(Пуск/Настройка/Панель управления/КриптоПро CSP)

Рисунок 10

Далее выберите вкладку «Сервис» и нажмите кнопку «Изменить пароль»:

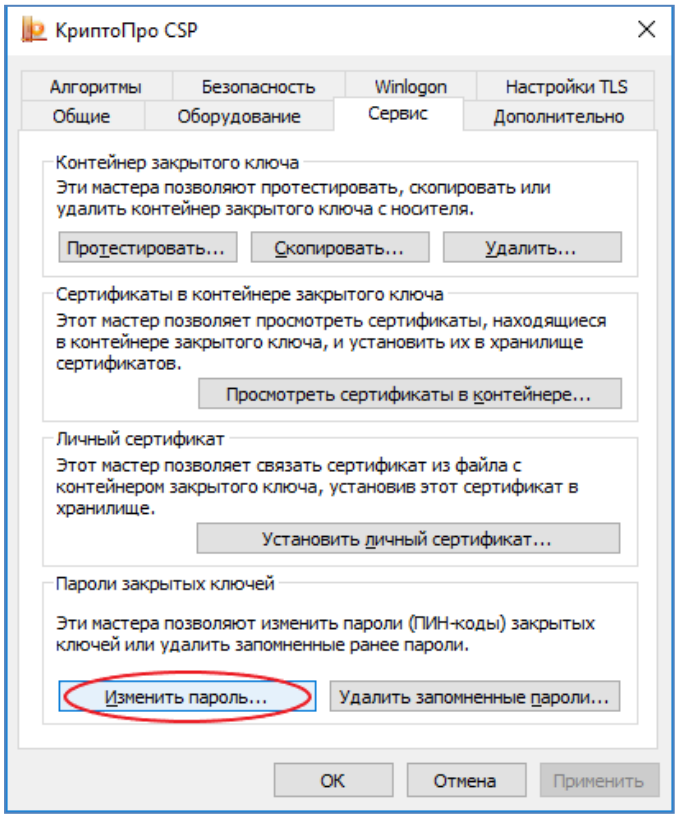


Рисунок 11

Далее следуйте указаниям мастера изменения пароля.

Эта процедура происходит в соответствии с регламентом КриптоПро CSP и описана в документации на криптопровайдер.

Примечание. Обратите внимание, что если при изменении значения Пароля Пользователя на «**пустое**», сервис КриптоПро CSP может выдать сообщение «Внутренняя ошибка», но, тем не менее, **может** произойти изменение ПИН на «пустое» значение.

10.5 Разблокировка ПИН (пароля) Пользователя

Разблокирование Пароля Пользователя производится средствами утилиты «UnblockUserPIN.exe», также это доступно средствами ПО «FOROS-Master».

Разблокирование средствами утилиты «UnblockUserPin» производится следующим образом:

1. Оператор подключает Носитель с заблокированным Паролем Пользователя к компьютеру.
2. Оператор запускает утилиту разблокирования «UnblockUserPIN.exe».
3. Оператор выбирает необходимый Носитель из списка
4. Оператор нажимает кнопку «Разблокировать», расположенную в разделе «Пароль Пользователя» окна программы.

5. Оператор вводит значение Пароля Администратора в поле «Текущий Пароль Администратора».
6. При необходимости оператор вводит новое значение Пароля Пользователя в полях «Новый Пароль Пользователя» и «Повторите новый Пароль Пользователя».
7. Оператор нажимает кнопку «Разблокировать».

Если все данные введены правильно, то будет выполнена операция разблокирования Пароля Пользователя, а также смена его старого значения на новое.

Средствами ПО «FOROS-Master» получение справочной информации доступно в разделе «КриптоПро».

10.6 Смена ПИН Администратора

Внимание!

При вводе Носителя в эксплуатацию, Администратор системы или Пользователь (в зависимости от действующего в системе регламента безопасности) должен сменить устанавливаемое по умолчанию транспортное значение Пароля Администратора на собственное.

Сохранение в тайне рабочего значения Пароля Администратора и его своевременная смена являются необходимым условием безопасной эксплуатации Носителя.

Производитель настоятельно рекомендует не использовать тривиальные комбинации символов для Пароля Администратора.

Смена Пароля Администратора может производиться двумя способами:

1) с помощью утилиты «UnblockUserPIN.exe»,
2) также это доступно средствами ПО «FOROS-Master» в разделе «КриптоПро».

С помощью утилиты «UnblockUserPIN.exe» смена Пароля Администратора производится следующим образом:

1. Оператор подключает Носитель к компьютеру.
2. Оператор запускает утилиту разблокирования «UnblockUserPIN.exe».
3. Оператор выбирает необходимый Носитель из списка
4. Оператор в разделе «Пароль Администратора» нажимает кнопку «Изменить».
5. Оператор в поле «Текущий Пароль Администратора» вводит значение Пароля Администратора.
6. Оператор в поле «Новый Пароль Администратора» вводит новое

значение Пароля Администратора и дублирует его в поле повтора.

7. Оператор нажимает кнопку «Изменить».

Если все данные введены правильно, то будет выполнена смена значения Пароля Администратора.

10.7 Форматирование (очистка) Носителя

Операция форматирования (очистки) Носителя заключается в удалении значений ранее созданных ключей и сертификатов и задании новых значений Паролей Пользователя и Администратора.

С помощью утилиты «UnblockUserPIN.exe» операция форматирования доступна после успешного предъявления действующего значения Пароля Администратора:

1. Оператор подключает Носитель к компьютеру.
2. Оператор выбирает необходимый Носитель из списка
3. Оператор активизирует функцию «Удалить все контейнеры».
4. Оператор вводит текущее и новое (с дублированием) значения Пароля Администратора, а также новое значение Пароля Пользователя (с дублированием).
5. Оператор инициирует операцию форматирования нажатием на соответствующий элемент управления.

Средствами ПО «FOROS-Master» данная возможность доступна в разделе «КриптоПро».

10.7.1 Варианты конфигурации правил доступа к функции форматирования

Носитель допускает два варианта конфигурации правила доступа к функции форматирования:

- Вариант, устанавливаемый по умолчанию: получение доступа к функции форматирования только после успешного предъявления Пароля Администратора.
- Опциональный вариант: разрешение свободного доступа к функции форматирования.

При необходимости Заказчик может выбрать опциональный вариант при заказе Носителей.

10.8 Справочные функции

10.8.1 Получение количества оставшихся попыток предъявления Пароля Администратора/Пользователя

Получение количества оставшихся попыток производится с помощью

утилиты «UnblockUserPIN.exe» следующим образом:

1. Оператор подключает Носитель к компьютеру.
2. Оператор запускает утилиту разблокирования «UnblockUserPIN.exe».
3. Оператор выбирает необходимый Носитель из списка
4. Оператор в разделе Пароль Пользователя нажимает кнопку «Статус», либо в разделе «Пароль Администратора».

10.8.2 Получение серийного номера микроконтроллера Носителя

Получение серийного номера производится с помощью утилиты «UnblockUserPIN.exe».

Средствами утилиты это выполняется следующим образом:

1. Оператор подключает Носитель к компьютеру.
2. Оператор запускает утилиту разблокирования «UnblockUserPIN.exe».
3. Оператор выбирает необходимый Носитель из списка
4. Оператор в разделе «Прочее» нажимает кнопку «Получить SN».

Средствами ПО «FOROS-Master» получение справочной информации доступно в разделе «Общие».

11 Эксплуатация Носителя в VipNet CSP

11.1 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.

11.2 Механизмы администрирования Носителя

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

Для доступа оператора и/или администратора безопасности к механизму разблокирования пароля Пользователя предоставляется утилита UnblockPKCS11.exe. Для загрузки утилиты необходимо «пройти» по ссылке:

https://smart-park.ru/support/#div_block-29-30

и загрузить:

UnblockUserpkcs - административная утилита для ключевого контейнера PKCS

Также операция разблокирования пароля Пользователя доступна в составе средств ПО «FOROS-Master» в разделе «PKCS#11».

Для эксплуатации утилиты и ПО «FOROS-Master» необходима библиотека PKCS#11 ***foros_pkcs11.dll***, которая должна быть доступна в путях поиска исполняемых модулей. Для загрузки установщика библиотеки необходимо «пройти» по ссылке:

https://smart-park.ru/support/#div_block-29-30

и загрузить:

FOROS PKCS11 (Windows)- **утилита установки dll, требующихся для работы с PKCS**

Утилита UnblockPKCS11.exe и ПО «FOROS-Master» могут применяться администраторами безопасности либо Пользователями. Режим их использования, способы распространения, хранения и применения значений административных паролей определяются регламентами безопасности конкретных систем.

Доступ к механизму разблокирования/смены паролей в носителях становится возможным после успешного выполнения процедуры предъявления права администратора путем предъявления соответствующего пароля администратора (SO PIN).

При первичной конфигурации носителей их производителем, в каждом Носителе ПИН администратора инициализируется транспортным значением (значением «по-умолчанию»). При вводе Носителя в эксплуатацию это значение необходимо заменить на другое, известное только субъекту - владельцу Пароля (Пользователю либо Администратору).

11.3 Управление паролем (ПИН) Пользователя

11.3.1 Режим смены пароля (ПИН) Пользователя

11.3.1.1 Необходимое условие успешного выполнения

- Оператор знает пароль Пользователя для контейнера PKCS#11, с которым производится процедура смены.

- В распоряжении оператора имеется утилита разблокирования либо ПО «FOROS-Master».

11.3.1.2 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.

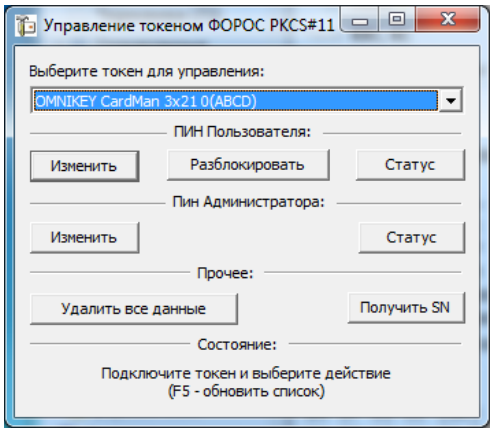


Рисунок 12

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».

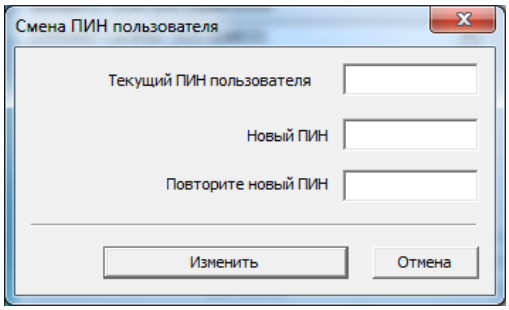


Рисунок 13

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

11.3.2 Режим разблокирования/установки ПИН пользователя

11.3.2.1 Необходимое условие успешного выполнения

- Оператору известен ПИН администратора для носителя, с которым производится процедура разблокирования ПИН пользователя.

- В распоряжении оператора имеется утилита разблокирования или ПО «FOROS-Master».

11.3.2.2 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.

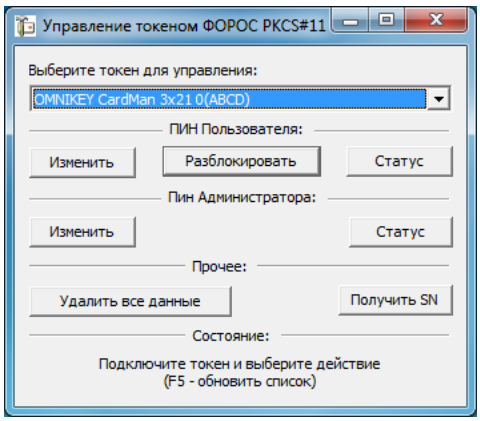


Рисунок 14

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».

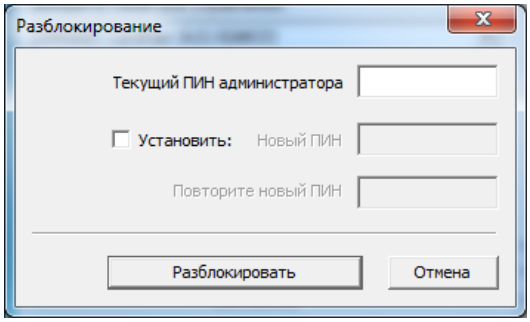


Рисунок 15

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

11.3.3 Режим проверки статуса ПИН пользователя

11.3.3.1 Необходимое условие успешного выполнения

- В распоряжении оператора имеется утилита разблокирования;

11.3.3.2 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.

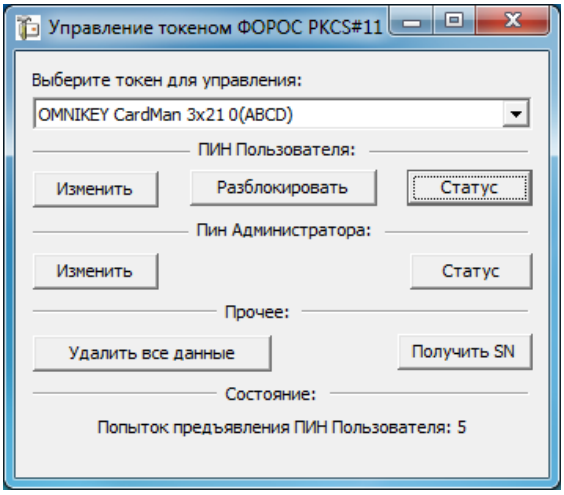


Рисунок 16

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

11.4 Управление паролем (ПИН) администратора

11.4.1 Режим смены ПИН администратора

11.4.1.1 Необходимое условие успешного выполнения

- Оператору известен ПИН администратора для носителя, с которым производится процедура смены ПИН.

- В распоряжении оператора имеется утилита разблокирования или ПО «FOROS-Master».

11.4.1.2 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.

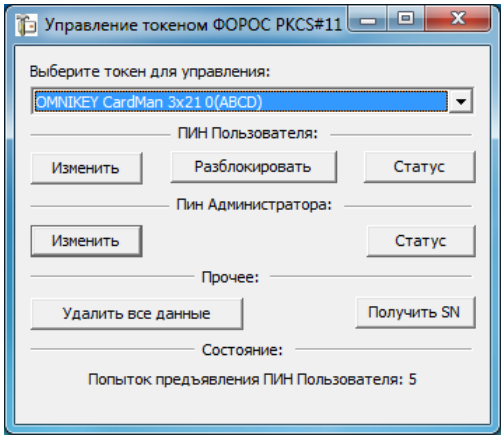


Рисунок 17

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».

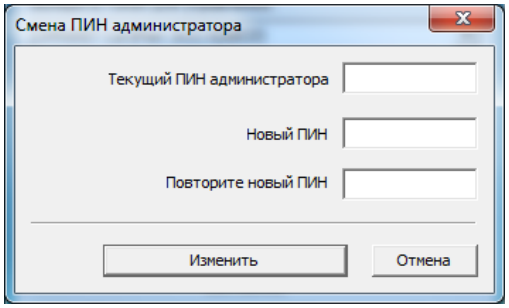


Рисунок 18

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

В ПО «FOROS-Master» аналогичные операции доступны в разделе «PKCS#11».

11.4.2 Режим проверки статуса ПИН администратора

11.4.2.1 Необходимое условие успешного выполнения

- В распоряжении оператора имеется утилита разблокирования.

11.4.2.2 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.

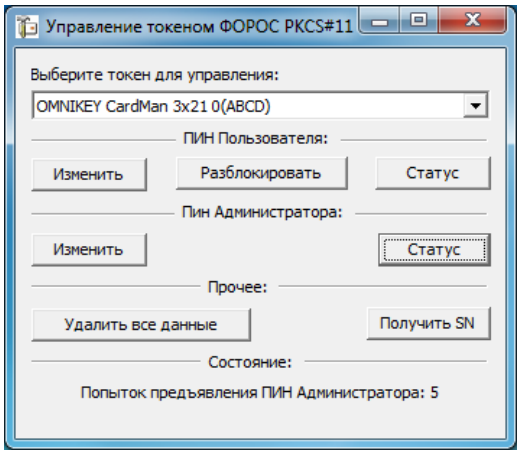


Рисунок 19

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

В ПО «FOROS-Master» данная информация доступна в разделе «PKCS#11».

11.4.3 Режим удаления данных пользователя

11.4.3.1 Необходимое условие успешного выполнения

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

11.4.3.2 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».

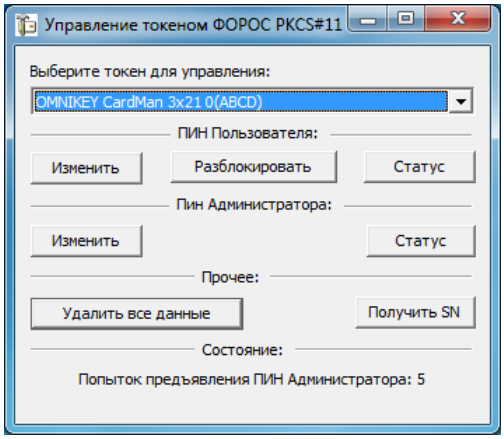


Рисунок 20

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

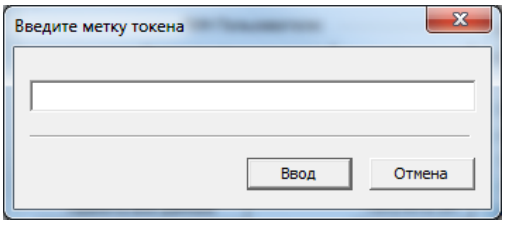


Рисунок 21

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»

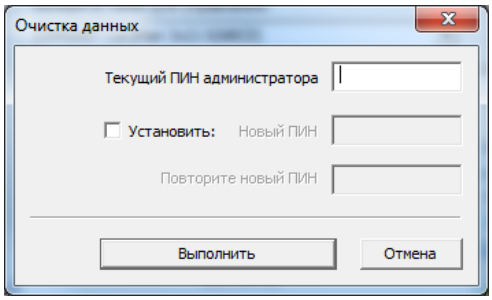


Рисунок 22

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

В ПО «FOROS-Master» данная операция доступна в разделе «PKCS#11».

12 Требования к условиям применения носителей ФОРОС

12.1 Условия применения

1. Носители предназначаются для использования в закрытых помещениях, в условиях влажности воздуха без конденсации влаги, при температуре окружающей среды от 0º С до плюс 70º С (предельное значение).

2. Носители не должны подвергаться механическим воздействиям, приводящим к деформации, нарушению целостности корпуса, USB-разъема, внутренней платы.

3. Носители можно подключать только к USB-разъемам исправного компьютера. Параметры USB-порта должны соответствовать спецификации для USB.

4. Для подключения Носителей не рекомендуется использовать USB-удлинители, а также USB-хабы без дополнительного питания.

5. Запрещается извлекать Носитель из порта компьютера, если на Носителе происходит работа с данными и мигает светодиодный индикатор.

6. Не рекомендуется оставлять Носитель подключенным к компьютеру во время перезагрузки, ухода в режим sleep.

7. Не рекомендуется оставлять Носитель подключенным к компьютеру, когда он не используется.

8. На время работы с Носителем рекомендуется отключать не используемые в настоящий момент USB-устройства и носители других типов.

9. Носители нельзя подвергать воздействию влаги, воздействию паров кислот, щелочей и других агрессивных примесей. Для очистки корпуса и разъема USB-носителя используйте сухую ткань. Использование органических растворителей недопустимо.

10. Запрещается разбирать Носители.

12.2 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 40°С до

плюс 85°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.

12.3 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.