

## **ПАК R301 ФОРОС USB ФКН**

### **Инструкция по установке и эксплуатации**



© ООО "СмартПарк", 2022

Все права защищены.

"Форос" является зарегистрированным товарным знаком ООО "СмартПарк".

Разрешено цитирование материалов в ограниченном объеме, но с обязательным указанием ООО "СмартПарк" и ссылки на сайт.

ООО "СмартПарк",

Москва, 127220, ул. 2-я Квесиская д. 24, корп. 3, офис №10.

Тел./факс: (495) 927-0033

Web: [www.smart-park.ru](http://www.smart-park.ru)

Техническая поддержка: [help@smart-park.ru](mailto: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

<b>1</b>	<b>ПРИМЕНЕНИЕ И НАЗНАЧЕНИЕ</b> .....	<b>5</b>
<b>2</b>	<b>ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ И КОНФИГУРАЦИЯ</b> .....	<b>6</b>
<b>3</b>	<b>АППАРАТНЫЕ КРИПТОГРАФИЧЕСКИЕ ВОЗМОЖНОСТИ</b> .....	<b>7</b>
<b>4</b>	<b>СВЕТОВАЯ ИНДИКАЦИЯ РЕЖИМОВ РАБОТЫ</b> .....	<b>8</b>
<b>5</b>	<b>ПОДДЕРЖКА НОСИТЕЛЯ В КРИПТОПРО CSP</b> .....	<b>8</b>
<b>6</b>	<b>ЭКСПЛУАТАЦИЯ</b> .....	<b>9</b>
6.1	СХЕМА РАЗГРАНИЧЕНИЯ ДОСТУПА К ДАННЫМ ФКН-НОСИТЕЛЯ .....	9
6.2	ТРАНСПОРТНЫЕ ЗНАЧЕНИЯ ПАРОЛЯ ПОЛЬЗОВАТЕЛЯ И РУК-КОДА .....	10
6.3	МЕХАНИЗМЫ АДМИНИСТРИРОВАНИЯ ФКН-НОСИТЕЛЯ .....	10
6.4	СМЕНА ПИН (ПАРОЛЯ) ПОЛЬЗОВАТЕЛЯ.....	12
6.4.1	Установка рабочих значений паролей.....	13
6.4.2	Смена рабочих значений паролей.....	14
6.5	РАЗБЛОКИРОВКА ПИН (ПАРОЛЯ) ПОЛЬЗОВАТЕЛЯ.....	17
6.6	СПРАВОЧНЫЕ ФУНКЦИИ.....	18
<b>7</b>	<b>КОНТРОЛЬ НОСИТЕЛЯ</b> .....	<b>18</b>
<b>8</b>	<b>ТРЕБОВАНИЯ К УСЛОВИЯМ ПРИМЕНЕНИЯ</b> .....	<b>19</b>
8.1	УСЛОВИЯ ПРИМЕНЕНИЯ .....	19
8.2	УСЛОВИЯ ХРАНЕНИЯ.....	20
8.3	УСЛОВИЯ ТРАНСПОРТИРОВКИ .....	20

## Используемые термины, определения и сокращения

**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.

**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.

**Оператор** – физическое лицо управляющее работой компьютера.

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

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

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

**ФКН** - функциональный ключевой носитель - неизвлекаемые ключи с защитой канала связи с носителем.

## 1 Применение и назначение

Носитель ПАК R301 ФОРОС USB ФКН (далее - Носитель) применяется совместно с криптопровайдерами компании КриптоПро (КриптоПро CSP 5.0 R2 и выше) в любых системах в качестве носителя ключевой и идентификационной информации. При этом обеспечивается неизвлекаемость закрытых ключей электронной подписи и защита канала связи криптопровайдера с Носителем.

Носитель логически и физически объединяет два устройства:

- смарт-карт ридер соответствующий спецификации CCID;
- смарт-карту с программным обеспечением аппаратного модуля СКЗИ Форос 2 в конфигурации «ФКН» с установленным приложением «Ключевой контейнер КриптоПро CSP-ФКН».

Носитель применяется в прикладных системах использующих криптопровайдеры КриптоПро CSP в соответствии с правилами и регламентами этих систем, правилами и регламентами СКЗИ КриптоПро CSP, а также с учетом положений настоящей Инструкции.

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

Носитель поддерживает протокол CCID и не требует установки дополнительных драйверов.

Основным назначением Носителя является:

- обеспечение защищенного хранения ключей и сертификатов, применяемых в рамках информационной технологии криптопровайдеров КриптоПро CSP;
- обеспечение защиты критических данных в случае утери или хищения Носителя, а также от их перехвата в канале связи с криптопровайдером;
- обеспечение возможности выполнения административных функций связанных с разблокировкой Носителя, заблокированного по причине превышения допустимого числа попыток неудачного предъявления пароля пользователя (ПИН пользователя).

Носитель ПАК R301 ФОРОС USB ФКН, ПАК смарт-карта ФОРОС ФКН для СКЗИ «КриптоПро CSP» (сертификат ФСБ) представляют собой исполнение сертифицированного СКЗИ Форос 2.

Сертификаты соответствия:

- сертификаты ФСБ России СФ/114-3909, СФ/124-3910 от 22.09.2020, выписка из Заключения ЦЗИ и СС ФСБ России (предоставляется по отдельному запросу);
- сертификат ООО «КРИПТО-ПРО» от 24.01.2021г.;

На Носитель распространяется действие сертификата ФСТЭК России №4490 от 14 декабря 2021 г. (ПАК ФОРОС 2 6958 6427.58.29.29.000.003).

Носитель работает в любых ОС с поддержкой спецификации PCSC. В частности:

- Microsoft Windows 7 и новее
- Microsoft Windows Server 2008 и новее
- 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 соответствующей версии СКЗИ «КриптоПро CSP».

## 2 Технические характеристики и конфигурация

Носитель содержит защищенный микроконтроллер с объемом энергонезависимой памяти 80 или 160 Кбайт, в которой размещается его файловая структура.

Основные характеристики Носителя приведены в таблице:

Параметр	ПАК R301 Форос USB ФКН	
<b>Технические характеристики</b>		
<b>Модель</b>	80	160
<b>Физический объем защищенной памяти</b>	80 Кбайт	160 Кбайт
<b>Тип USB-разъема</b>	Стандартный Тип А	
<b>Интерфейс подключения</b>	USB 2.0 ISO/IEC 7816-12, 12 Мбит/сек	
<b>Скорость обмена данными</b>	до 323 Кбит/сек, 4 МГц; 500кбит/сек, 6МГц	
<b>Поддерживаемые протоколы</b>	ISO 7816 T=0	
<b>Скорость чтения данных</b>	до 13000 байт/с	
<b>Поддержка CCID</b>	Есть	
<b>Габаритные размеры [Д x Ш x В]</b>	48 x 16 x 8 мм	
<b>Масса</b>	6.3 г. +/-10%	
<b>Потребляемая мощность</b>	около 130 мВт в активном состоянии	
<b>Диапазон рабочих температур</b>	от 0 до +70°С	
<b>Диапазон температур хранения</b>	от -40 до +85°С	
<b>Допустимая относительная влажность</b>	от 0 до 85% (без конденсата)	
<b>Время хранения данных (в нормальных условиях в соответствии с ГОСТ 15150-69)</b>	30 лет	
<b>Гарантированное количество циклов стирания\записи</b>	1 000 000	
<b>Типовые параметры логической конфигурации</b>		
<b>Число контейнеров</b>	2	8
<b>Размер контейнера (допустимый размер сертификата)</b>	7 Кбайт	7 Кбайт

Максимальное число последовательных неуспешных попыток ввода пароля пользователя	10
Допустимое общее число неудачных попыток предъявления паролей пользователя и администратора	96
Функция разблокирования/восстановления пароля пользователя по паролю администратора	Есть
Максимальное число последовательных неуспешных попыток ввода пароля администратора	10
Допустимые размеры паролей пользователя и администратора	От 6 до 160 символов
Функция форматирования (очистки)	Нет
Транспортное значение пароля Пользователя [символы ASCII – текста]	123456
Транспортное значение пароля Администратора [символы ASCII – текста]	123456

Возможно изменение параметров конфигурации Носителя и/или встраивание в Носитель дополнительных функциональных приложений, разработанных по запросам корпоративных Заказчиков.

### 3 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<sup>1,2</sup>): 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<sup>1,2</sup>): вычисление значения хеш-функции данных, в том числе с возможностью последующего формирования электронной подписи;
- ГОСТ 28147-89: генерация ключей шифрования, 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 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)<sup>1,2</sup>;
- 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)<sup>2,3</sup>;

- 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)<sup>2,3</sup>;

- Расшифрование по схеме EC El-Gamal<sup>2</sup>;

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

- ECDSA с кривыми secp256k1<sup>4</sup> и secp256r1<sup>2</sup>: генерация ключевых пар с настраиваемой проверкой качества, импорт ключевых пар, формирование электронной подписи;

- генерация последовательности случайных чисел требуемой длины

<sup>1</sup> – в СКЗИ «ФОР ОС 2» применяется совместно с использованием соответствующего криптопровайдера

<sup>2</sup> – доступно в СКЗИ «ФОР ОС 3»

<sup>3</sup> – доступно в СКЗИ «ФОР ОС 2»

<sup>4</sup> – применяется совместно с использованием соответствующего криптопровайдера

#### 4 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:

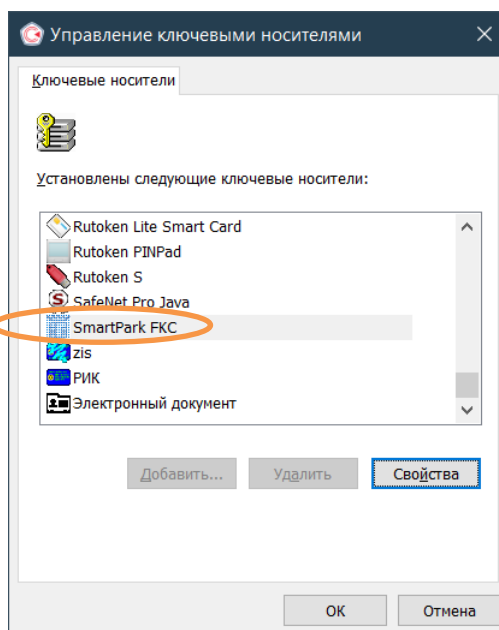
Назначение индикатора	Цвет	Состояние	Процесс
Индикатор USB	Красный	Мигает	Установка соединения по USB
		Непрерывно светит	Соединение по USB установлено (готовность к работе)
		Мигает нерегулярно	Обмен данными по USB (выполнение операций)
		Не светит	Нарушение системной области, неисправность
Индикатор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

#### 5 Поддержка Носителя в КриптоПро CSP

Программный модуль поддержки Носителя встроен в дистрибутив



КриптоПро CSP (начиная с версии 5.0 R2 и далее во всех последующих) Дополнительная инсталляция Носителя в криптопровайдере не требуется. Носитель распознается встроенным в КриптоПро CSP модулем поддержки как носитель «SmartPark ФКС».



Оснастка КриптоПро CSP/Оборудование/Настроить типы носителей.

## 6 Эксплуатация

### 6.1 Схема разграничения доступа к данным ФКН-Носителя

Доступ к контейнерам КриптоПро CSP на Носителе защищается Паролем Пользователя (иначе - ПИН Пользователя или Пароль носителя). Сервисы КриптоПро CSP запрашивают ПИН Пользователя при выполнении операций, требующих доступа к закрытой информации, хранящейся на Носителе.

У Пользователя есть 10 (Десять) попыток (параметр устанавливается по умолчанию) для ввода (предъявления) правильного значения **ПИН** (Пароля) Пользователя.

Если все разрешенные попытки предъявления ПИН (Пароля) Пользователя будут неудачными, то механизм его ввода будет **заблокирован** внутренними средствами Носителя. Соответственно последующий доступ к закрытой информации Носителя будет невозможен даже в случае 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 (иначе – PUK-код).

Механизм ввода **PUK-кода** допускает строго ограниченное число последовательных попыток неудачного ввода. При достижении этого числа PUK-код безвозвратно блокируется и административные операции на таком носителе становятся невозможными.

При выполнении операции разблокирования Пароля Пользователя по PUK, предусматривается также возможность ввода нового значения Пароля Пользователя

## **6.2 Транспортные значения пароля Пользователя и PUK-кода**

ФКН-Носитель имеет механизм индикации наличия транспортных (первичных) значений паролей.

При поставке ФКН-Носителей, производитель устанавливает Пароль (ПИН) Пользователя и PUK (ПИН Администратора) в транспортные (первичные) значения, которые приведены в разделе 2 (Технические характеристики и конфигурация) данного документа.

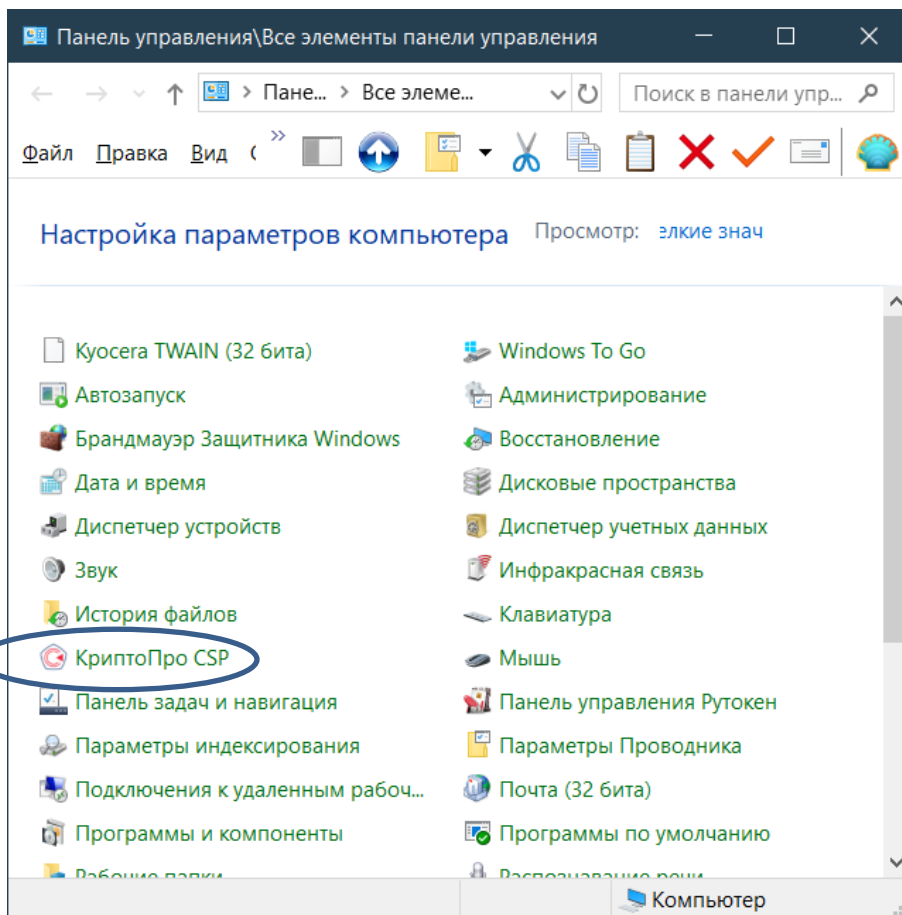
Криптопровайдер, при обнаружении Носителя с первичной установкой паролей, всегда выдает запрос на смену этих значений на рабочие перед выполнением любых операций, требующих предъявления паролей Носителя.

## **6.3 Механизмы администрирования ФКН- Носителя**

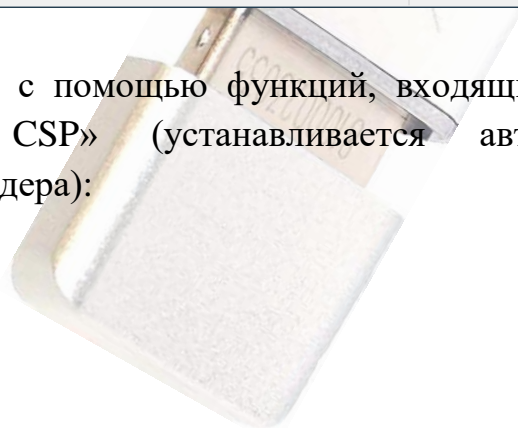
Набор административных функций Носителя включает:

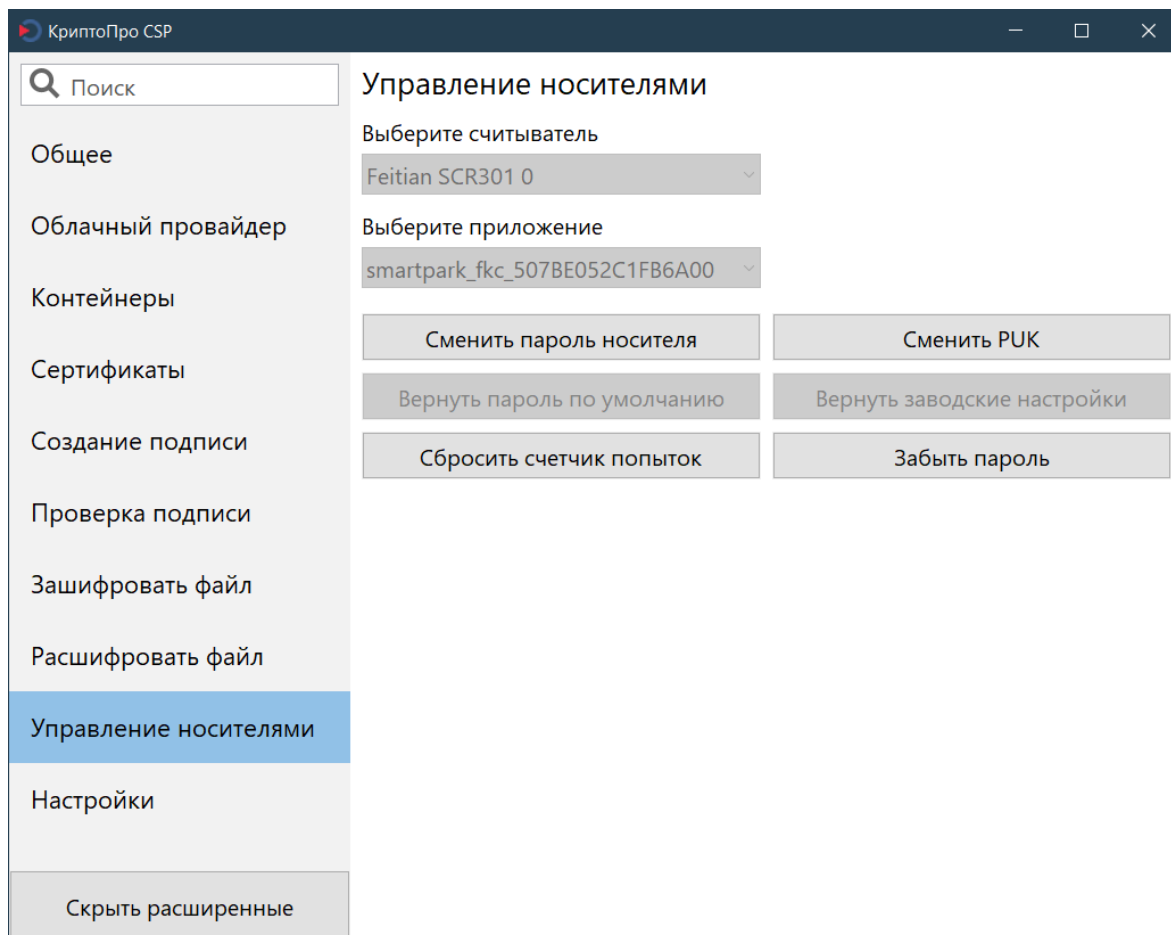
- функция изменения и разблокирования Пароля Пользователя;
- функции изменения значения Пароля Администратора (PUK-кода);
- контрольные функции (проверка СЗИ).

Функции администрирования ФКН-Носителем реализуются через функции панели управления КриптоПро CSP (устанавливается автоматически при установке криптопровайдера)



а также с помощью функций, входящих в состав ПО «Инструменты КриптоПро CSP» (устанавливается автоматически при установке криптопровайдера):





Также функции администрирования ФКН-Носителем реализуются с помощью программного обеспечения FOROS-Master предназначенного для административного управления приложениями носителей семейства R301 ФОРОС USB/смарт-карты ФОРОС (вкладка «КриптоПро CSP-ФКН»).

Программа управления носителями ФОРОС FOROS-Master может быть загружена с сайта ООО «СмартПарк» на странице:

[https://smart-park.ru/support/#div\\_block-29-30](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».

#### **6.4 Смена ПИН (пароля) Пользователя**

##### **Внимание!**

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

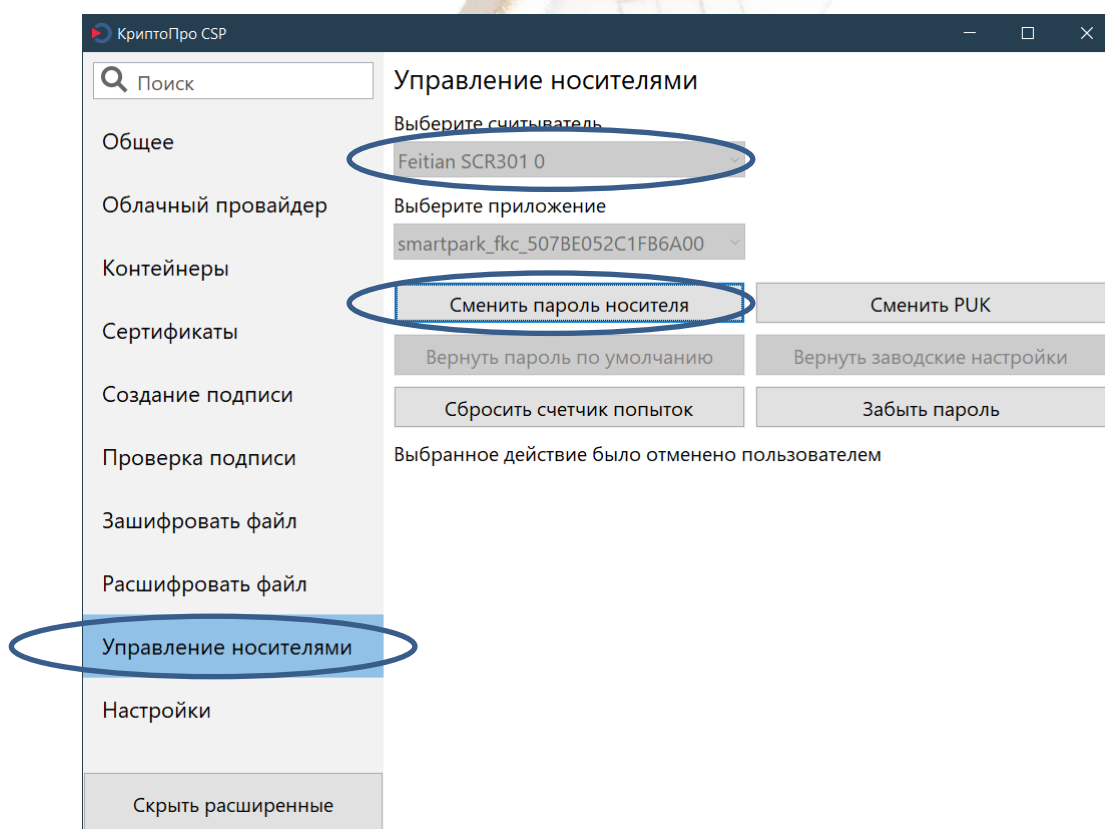
на собственное.

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

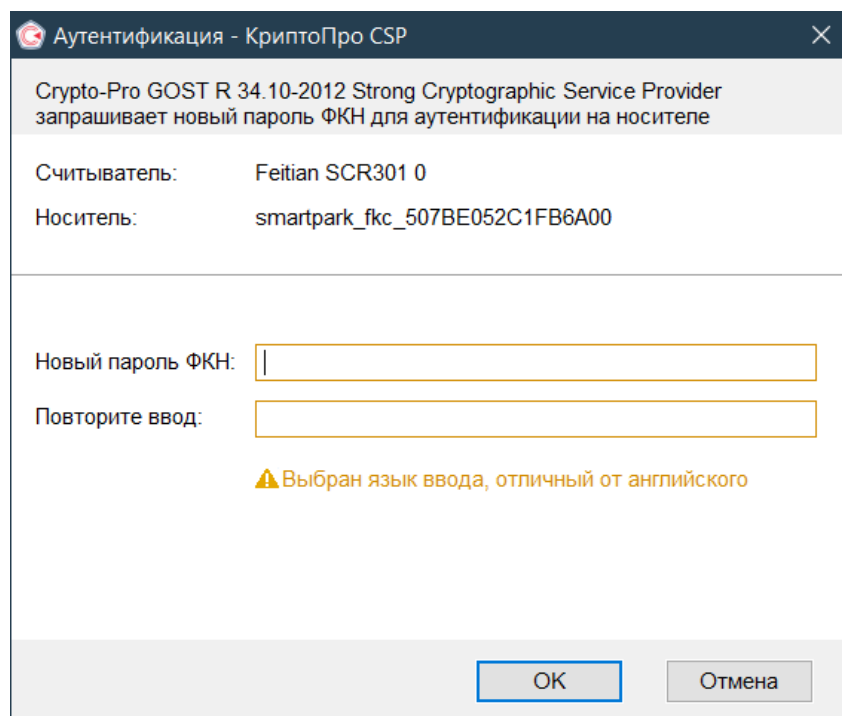
Производитель настоятельно рекомендует не использовать простых комбинаций символов для Пароля Пользователя.

#### 6.4.1 Установка рабочих значений паролей

Запустите программу, далее выберите вкладку /«Управление носителями». После этого выберите Носитель (вкладка «Выберите считыватель» Feitian SCR301, если используете Носитель ПАК R301 ФОРОС USB ФКН) и затем активируйте функцию «Сменить пароль носителя».



В открывшемся окне «Аутентификация-КриптоПро CSP» введите рабочее значение Пароля Пользователя в строку «Новый пароль ФКН»



Аналогичные действия следует выполнить для PUK-кода. Для этого активируйте функцию «Сменить PUK».

Смена транспортных паролей также можно произвести во время записи ключа/сертификата на носитель. Если на данном носителе установлены транспортные пароли, то в таком случае интерфейс КриптоПро CSP сам предложит сменить пароли.

Смена транспортных значений паролей также может быть выполнена с помощью ПО «FOROS-Master» (вкладка «КриптоПро CSP-ФКН», действие «Разблокировать и сменить») включая поточную смену на нескольких носителях с использованием пакетного режима.

#### **6.4.2 Смена рабочих значений паролей**

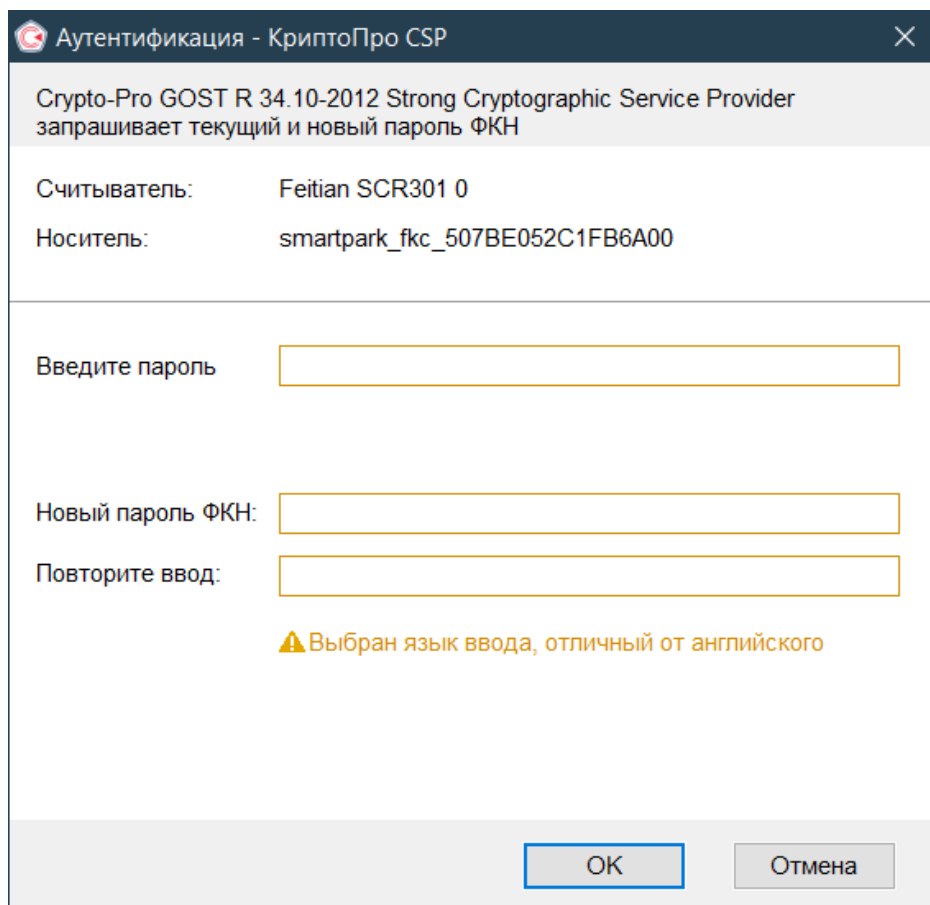
Смену рабочих паролей можно выполнить средствами ПО «Инструменты КриптоПро CSP», а также через Панель управления КриптоПро CSP и ПО «Форос-Мастер» (вкладка «КриптоПро CSP-ФКН», действие «Разблокировать и сменить», «Сменить»).

##### **6.4.2.1 Смена рабочих значений паролей средствами ПО «Инструменты КриптоПро CSP»**

Запустите программу, далее выберите вкладку /«Управление носителями». После этого выберите Носитель (вкладка «Выберите считыватель» Feitian SCR301, если используете Носитель ПАК R301 ФОРΟΣ USB ФКН) и затем активируйте функцию «Сменить пароль носителя».

В открывшемся окне «Аутентификация-КриптоПро CSP» введите  
*ООО «СмартПарк»*

рабочее значение Пароля Пользователя в строку «Введите пароль», а затем введите устанавливаемое значение в поле «Новый пароль ФКН»



Аутентификация - КриптоПро CSP

Crypto-Pro GOST R 34.10-2012 Strong Cryptographic Service Provider  
запрашивает текущий и новый пароль ФКН

Считыватель: Feitian SCR301 0  
Носитель: smartpark\_fkc\_507BE052C1FB6A00

Введите пароль

Новый пароль ФКН:

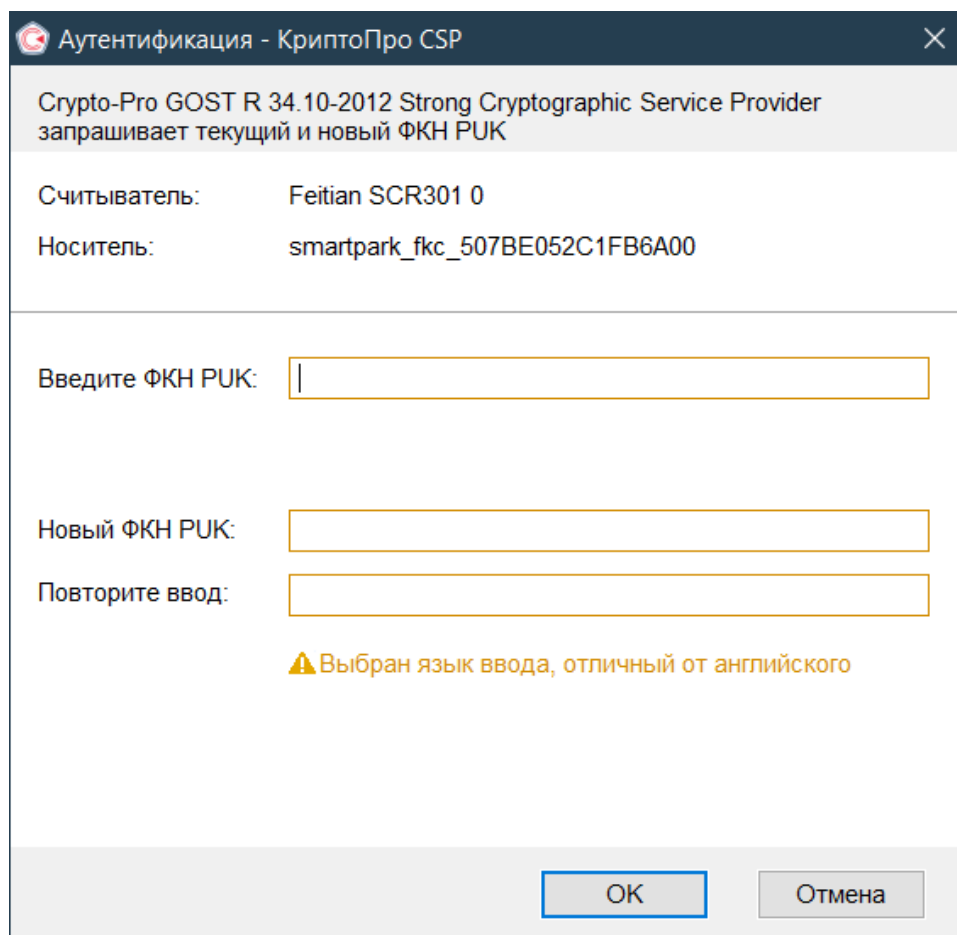
Повторите ввод:

⚠ Выбран язык ввода, отличный от английского

ОК Отмена

Если исходное рабочее значение Пароля Пользователя было указано верно, а также совпадают новое значение пароля и его дубль, то в носителе будет установлено новое рабочее значение Пароля Пользователя.

Аналогичные действия следует выполнить для смены рабочего значения PUK-кода на новое. Для этого активируйте функцию «Сменить PUK» и заполните соответствующую экранную форму.



Аутентификация - КриптоПро CSP

Crypto-Pro GOST R 34.10-2012 Strong Cryptographic Service Provider запрашивает текущий и новый ФКН PUK

Считыватель: Feitian SCR301 0  
Носитель: smartpark\_fkc\_507BE052C1FB6A00

Введите ФКН PUK:

Новый ФКН PUK:

Повторите ввод:

⚠ Выбран язык ввода, отличный от английского

ОК Отмена

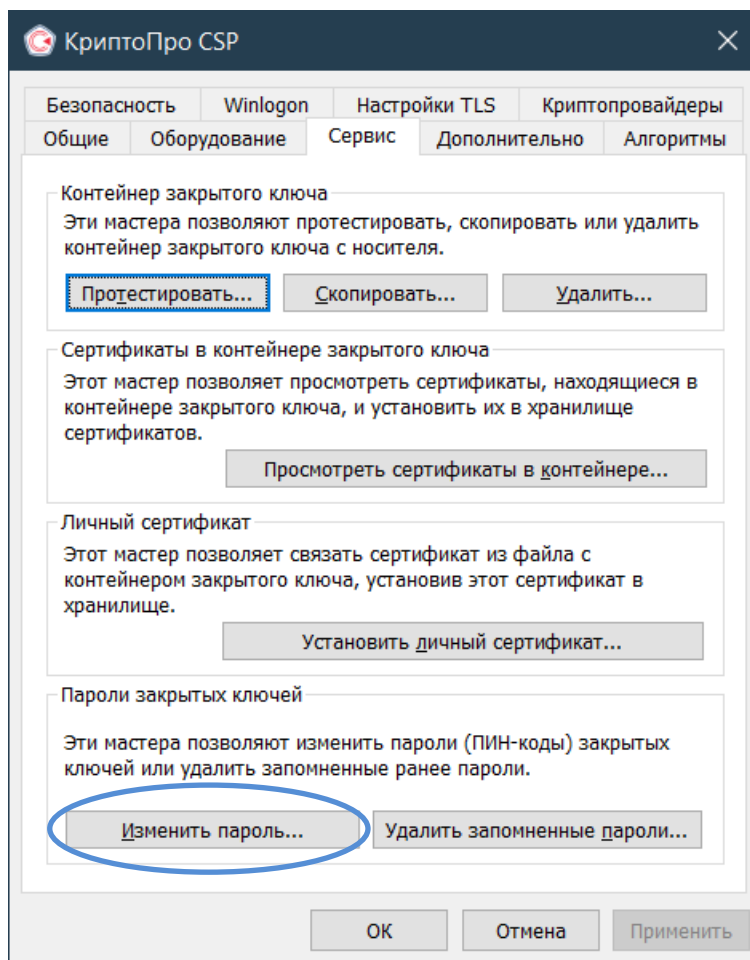
#### 6.4.2.2 Смена Пароля Пользователя через Панель управления КриптоПро CSP

Смена Пароля Пользователя ФКН-Носителя возможна также через «Панель управления» криптопровайдера КриптоПро CSP.

Откройте оснастку управления КриптоПро CSP в «Панели управления» (Пуск/Настройка/Панель управления/КриптоПро CSP)

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





Далее следуйте указаниям мастера изменения пароля.

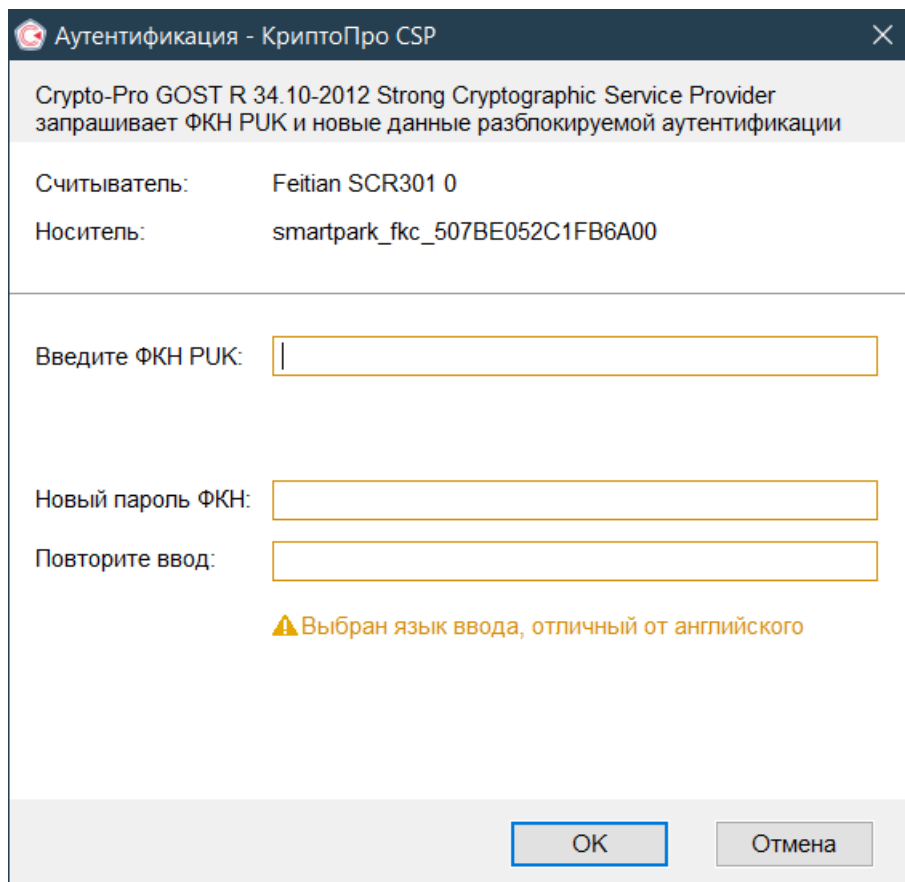
Эта процедура происходит в соответствии с регламентом КриптоПро CSP и описана в документации на криптопровайдер.

**Примечание.** Если носитель еще не содержит ключей и сертификатов, то тогда смену паролей можно выполнить средствами ПО «Инструменты КриптоПро CSP» или ПО «Форос-Мастер».

### 6.5 Разблокировка ПИН (пароля) Пользователя

Разблокирование Пароля Пользователя может быть выполнено как через Панель управления, так через ПО «Инструменты КриптоПро CSP» и ПО «Форос-Мастер» (вкладка «КриптоПро CSP-ФКН», действие «Разблокировать и сменить»).

Экранная форма функции разблокирования предлагается оператору автоматически, если вы пытаетесь использовать носитель с заблокированным паролем Пользователя:



Аутентификация - КриптоПро CSP

Crypto-Pro GOST R 34.10-2012 Strong Cryptographic Service Provider запрашивает ФКН PUK и новые данные разблокируемой аутентификации

Считыватель: Feitian SCR301 0  
Носитель: smartpark\_fkc\_507BE052C1FB6A00

Введите ФКН PUK:

Новый пароль ФКН:

Повторите ввод:

⚠ Выбран язык ввода, отличный от английского

OK Отмена

## 6.6 Справочные функции

### 6.6.1 Получение количества оставшихся попыток предъявления Пароля Администратора/Пользователя

Число оставшихся попыток предъявления Пароля Пользователя и PUK выводятся на экран в составе информации, выводимой при их неуспешном предъявлении.

Также справочная информация доступна с помощью и ПО «Форос-Мастер» (вкладка «Общее»).

## 7 Контроль носителя

Контроль подлинности/целостности Носителя в соответствии с требованиями ФСБ, производится по ключевой контрольной сумме. Операции контроля выполняются в соответствии с п. 5 Формуляра 6958 6427.58.29.29.000.002.30.01.1. Формуляр и/или программное средство контроля предоставляется Заказчику отдельному запросу.

Контроль подлинности/целостности изделия по требованиям ФСТЭК производится по ключевой контрольной сумме, контроль целостности - по контрольной сумме CRC32. Операции контроля выполняются в соответствии

с п. 6.1 Формуляра 6958 6427.58.29.29.000.003.30.01.1. Операция контроля по CRC32 выполняется средствами административной утилиты. Программное средство контроля может быть получено с сайта компании ООО «СмартПарк» со страницы:

<http://www.smart-park.ru/index.php/support/driver.html>

или непосредственно по ссылке:

<http://smart-park.ru/util/checkSZI.zip>

Также операции контроля доступны с помощью ПО «FOROS-Master» (вкладка «Общее», действия «Проверка целостности», «Проверка целостности и подлинности»).

## **8 Требования к условиям применения**

### **8.1 Условия применения**

1. Носители предназначены для использования в закрытых помещениях, в условиях влажности воздуха без конденсации влаги, при температуре окружающей среды от 0° С до плюс 70° 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.

## 8.2 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°C и относительная влажность воздуха не более 85%;
- предельная температура хранения составляет от минус 40°C до плюс 85°C.

При хранении не допускаются резкие изменения температуры окружающего воздуха (более 20°C 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.

## 8.3 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°C до +50°C;
- 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.