R301 ФОРОС USB
для СКЗИ «КриптоПро CSP»
Инструкция по установке и эксплуатации

Версия 2.3.1.U.03

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

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 «КриптоПро CSP» (далее - Носитель) применяется совместно с криптопровайдерами компании КриптоПро (КриптоПро CSP 3.0 и выше) в любых системах в качестве носителя ключевой и идентификационной информации.

Носитель логически и физически объединяет два устройства:

- смарт-карт ридер, соответствующий спецификации CCID;
- смарт-карту с операционной системой Форос с установленным приложением ключевого носителя для криптопровайдера КриптоПро CSP.

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

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;
- обеспечение возможности выполнения административных функций связанных с разблокировкой Носителя, заблокированных по причине превышения допустимого числа попыток неудачного предъявления пароля пользователя (ПИН пользователя) или пароля администратора (опционально).

Сертификаты соответствия:

- сертификата ФСТЭК России №4490 от 14 декабря 2021 г. (ПАК ФОРОС 2 6958 6427.58.29.29.000.003);
- сертификат ООО «КРИПТО-ПРО» от 08.11.2019г.;
- сертификат ООО «Аванпост» от 10.11.2021 г.

2 Технические характеристики и конфигурация

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

Основные характеристики Носителя приведены в таблице:

Параметр	R301 Форос 80	R301 Форос 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 [Д х Ш х В]	48 х 16 х 8 мм	
Масса	6.3 г. +\-10%	
Потребляемая мощность	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		
Число контейнеров	6	14
Размер контейнера (допустимый размер сертификата)	9 Кбайт	9 Кбайт
Поддержка ключей 512 бит ГОСТ Р34.10-2012	Есть	
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	15	
Функция форматирования (очистки)	Есть	
Доступ к функции форматирования (очистки)	по паролю Администратора	

Возможно изменение логической конфигурации 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.

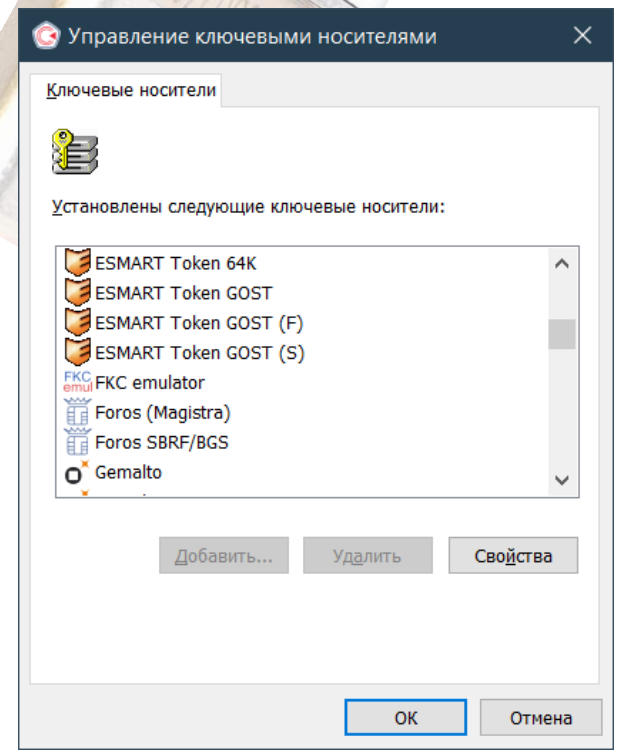
Детализация состояний индикаторов приведена в нижеследующей таблице:

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 Поддержка Носителя в КриптоПро CSP

Программный модуль поддержки Носителя встроен в дистрибутив КриптоПро CSP начиная с версии 3.0. Дополнительная инсталляция Носителя в криптопровайдере не требуется.

Носитель распознается встроенным в КриптоПро CSP модулем поддержки как носитель «Магистра».



5 Эксплуатация

5.1 Схема разграничения доступа к данным Носителя

Доступ к контейнерам КриптоПро CSP на Носителе защищается Паролем Пользователя (иначе - ПИН Пользователя). Сервисы КриптоПро CSP запрашивают ПИН 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 ***ПИН*** (Пароля) Пользователя. Если все попытки предъявления ПИН (Пароля) Пользователя будут неудачными, то механизм ввода ПИН Пользователя будет **заблокирован** автономным механизмом Носителя, и последующий доступ криптопровайдера 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 - ПИН Администратора). Способы доступа к механизмам администрирования описаны ниже.

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 предусмотрен свободный доступ к функции форматирования (очистки). Если доступ к функции форматирования ***(очистки)*** установлен «по Паролю Администратора» - восстановление работоспособности невозможно.

Примечание. 1. Функция форматирования (см. п. 5.6) удаляет из Носителя все данные. При ее выполнении требуется указывать новые значения паролей Пользователя и Администратора.

2. Режим доступа к функции форматирования определяется при заказе Носителей.

В случае утери рабочего значения Пароля Пользователя утилита разблокирования предусматривает операцию смены значения Пароля Пользователя на основании предъявленного Пароля Администратора.

5.2 Механизмы администрирования Носителя

Набор административных функций Носителя состоит из:

– функции разблокирования Пароля Пользователя;
– функции изменения значения Пароля Администратора;
– функции форматирования (очистки) Носителя (удаление информации из контейнеров);
– справочные функции.

Предъявление Пароля Администратора и выполнение разблокирования, смены значений Паролей и проч. возможно путем применения утилиты разблокирования, либо с помощью web-приложения реализуемого в системе Заказчика на основе применения продукта «ForosWKT».

Утилита разблокирования представляет собой исполняемый программный модуль и может быть загружена с сайта компании ООО «СмартПарк»: http://www.smart-park.ru/index.php/support/driver.html

Web-приложение может быть реализовано в системе Заказчика на основе программного продукта «ForosWKT», который предоставляет интерфейс функций администрирования Носителя.

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

Программное обеспечение «ForosWKT» может быть загружено с сайта компании ООО «СмартПарк»:

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

Продукт «ForosWKT» применяется путем встраивания в пользовательские Web-страницы обращений к интерфейсу администрирования ключевым контейнером КриптоПро CSP, размещенным на носителе "Форос".

Продукт предназначен для применения в WEB-браузерах

- Microsoft Internet Explorer (версии 10, 11)
- Google Chrome (версия 52 и выше)

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).

Тестовая страница (образец применения) размещена на сайте ООО "СмартПарк" по адресу:

http://smart-park.ru/foroswkt/testpage.html

5.3 Смена ПИН (пароля) Пользователя

Внимание!

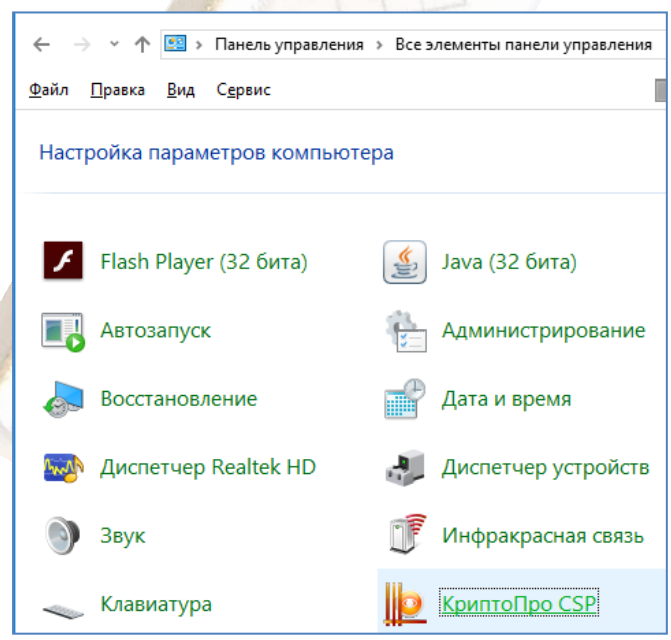
При вводе Носителя в эксплуатацию, Пользователь должен сменить установленное производителем транспортное значение Пароля Пользователя, на собственное.

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.

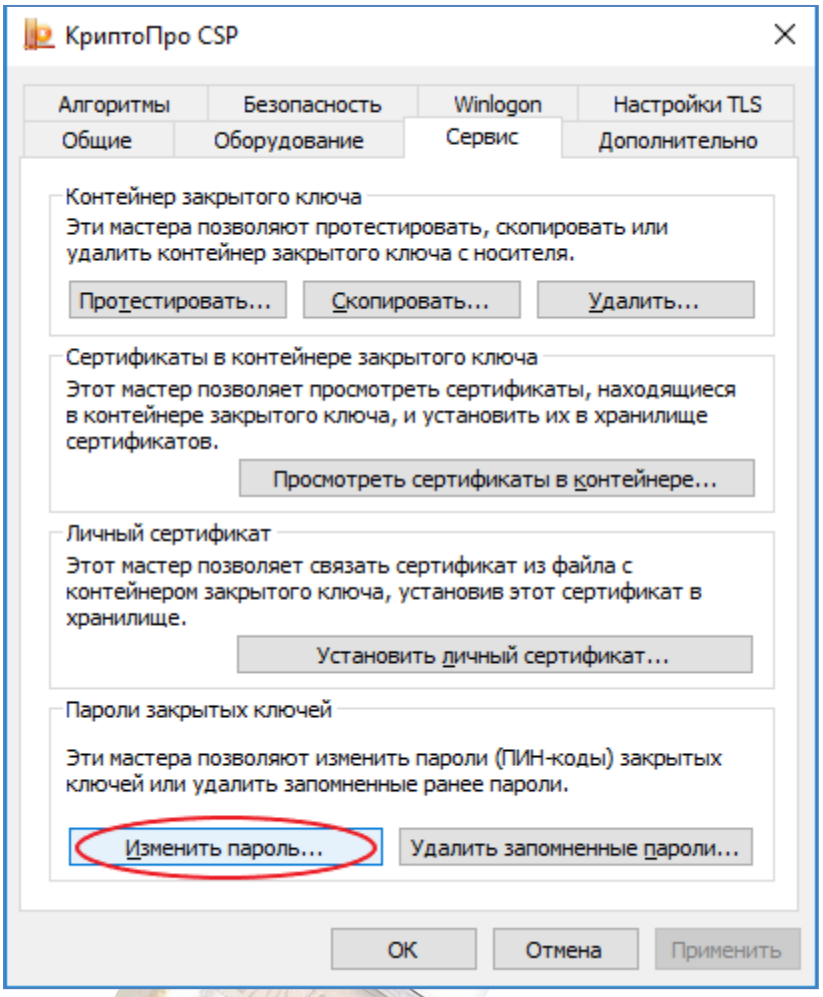
Смена Пароля Пользователя в штатном режиме производится средствами криптопровайдера КриптоПро CSP в «Панели управления».

Откройте оснастку управления КриптоПро CSP в «Панели управления»



(Пуск/Настройка/Панель управления/КриптоПро CSP)

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. 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.

5.4 Разблокировка ПИН (пароля) Пользователя

Разблокирование Пароля Пользователя производится с помощью утилиты «UnblockUserPIN.exe», либо с помощью Web-приложения реализованного на основе применения продукта «ForosWKT».

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 нажимает кнопку «Разблокировать», расположенную в разделе «Пароль Пользователя» окна программы.
4. Оператор вводит значение Пароля Администратора в поле «Текущий Пароль Администратора».
5. При необходимости оператор вводит новое значение Пароля Пользователя в полях «Новый Пароль Пользователя» и «Повторите новый Пароль Пользователя».
6. Оператор нажимает кнопку «Разблокировать».

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

В случае применения Web-приложения, оператор должен ввести Пароль Администратора и инициировать выполнение операции:

1. Оператор подключает Носитель с заблокированным Паролем Пользователя к компьютеру.
2. Оператор открывает Web-страницу для доступа к функциям администрирования.
3. Оператор вводит значение Пароля Администратора в соответствующее поле параметров операции разблокировки.
4. Оператор инициирует операцию выбором (нажатием) соответствующего элемента Web-страницы.

5.5 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) с помощью Web-приложения реализованного на основе применения продукта «ForosWKT».

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 в разделе «Пароль Администратора» нажимает кнопку «Изменить».
4. Оператор в поле «Текущий Пароль Администратора» вводит значение Пароля Администратора.
5. Оператор в поле «Новый Пароль Администратора» вводит новое значение Пароля Администратора и дублирует его в поле повтора.
6. Оператор нажимает кнопку «Изменить».

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

В случае применения Web-приложения, оператор должен ввести прежнее значение Пароля Администратора, ввести новое значение и инициировать выполнение операции смена Пароля Администратора:

1. Оператор подключает Носитель к компьютеру.
2. Оператор открывает Web-страницу для доступа к функциям администрирования.
3. Оператор вводит текущее и новое значения Пароля Администратора в соответствующие поля параметров операции смены Пароля Администратора.
4. Оператор инициирует операцию смены Пароля Администратора выбором соответствующего элемента Web-страницы.

5.6 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 активизирует функцию «Удалить все контейнеры».
3. Оператор вводит текущее и новое (с дублированием) значения Пароля Администратора, а также новое значение Пароля Пользователя (с дублированием).
4. Оператор инициирует операцию форматирования нажатием на соответствующий элемент управления.

В случае применения Web-приложения:

1. Оператор подключает Носитель к компьютеру.
2. Оператор открывает Web-страницу для доступа к функциям администрирования.
3. Оператор вводит текущее и новое значения Пароля Администратора, а также новое значение Пароля Пользователя в соответствующие поля параметров операции форматирования.
4. Оператор инициирует операцию выбором соответствующего элемента Web-страницы.

5.6.1 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.

5.7 Справочные функции

5.7.1 Получение количества оставшихся попыток предъявления Пароля Администратора/Пользователя

Получение количества оставшихся попыток производится с помощью утилиты «UnblockUserPIN.exe», либо с помощью Web-приложения на основе применения продукта «ForosWKT».

Средствами утилиты разблокирование производится следующим образом:

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

В случае применения Web-приложения оператор должен инициировать выполнение соответствующей операции:

1. Оператор подключает Носитель к компьютеру.
2. Оператор открывает Web-страницу для доступа к функциям администрирования.

3. Оператор инициирует операцию выбором соответствующего элемента Web-страницы.

5.7.2 Получение серийного номера микроконтроллера Носителя

Получение серийного номера производится с помощью утилиты «UnblockUserPIN.exe», либо с помощью Web-приложения на основе применения продукта «ForosWKT».

Средствами утилиты это выполняется следующим образом:

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

В случае применения Web-приложения оператор должен инициировать выполнение соответствующей операции:

1. Оператор подключает Носитель к компьютеру.
2. Оператор открывает Web-страницу для доступа к функциям администрирования.
3. Оператор инициирует операцию выбором соответствующего элемента Web-страницы.

6 Пароли Носителя, устанавливаемые по умолчанию

Роль	Значение Пароля по умолчанию
Пользователь	11111111
Администратор	87654321

7 Требования к условиям применения

7.1 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.

7.2 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.

7.3 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.