# Инструкция
# по установке и эксплуатации
# ключевого носителя Форос-USB для КриптоПро CSP

# Используемые термины, определения и сокращения

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

**ПИН** - аналог Пароль.

**Криптопровайдер** - (Cryptography Service Provider, CSP) - это независимый программный модуль, позволяющий осуществлять криптографические операции в операционных системах Microsoft, управление которым происходит с помощью функций Crypto API.

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

**Ути́лита** (англ. *utility*) - компьютерная программа, расширяющая стандартные возможности оборудования и операционных систем, выполняющая узкий круг специфических задач.

**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 Основное назначение

Ключевой носитель ФОРОС-USB логически и физически объединяет два устройства: CCID-смарт-карт ридер и смарт-карту.

По функциональным возможностям ключевой носитель ФОРОС-USB идентичен ключевому носителю КриптоПро на смарт-карте установленной в стандартный CCID-смарт-карт ридер.

Ключевой носитель ФОРОС-USB предназначен для использования в офисных и домашних системах совместно с криптопровайдерами компании КриптоПро (CryptoPro CSP 3.6 и старше) в качестве носителя ключевой и идентификационной информации.

Ключевой носитель ФОРОС-USB (далее - Носитель) без ограничений может использоваться по назначению совместно с программными продуктами, использующими криптопровайдеры компании КриптоПро в качестве средства криптографической защиты информации (СКЗИ) соответствующего классам КС2 и КС3.

Основным назначением Носителя является:

- обеспечение защищенного хранения ключей и сертификатов применяемых в рамках информационной технологии криптопровайдера КриптоПро CSP;
- обеспечение защиты критических данных в случае утери или хищения идентификатора;
- обеспечение возможности выполнения административных функций связанных с безопасной разблокировкой носителей, заблокированных по причине превышения числа попыток неудачного предъявления пароля пользователя.

# 2 Конфигурация поставки

Носитель имеет несколько функционально идентичных исполнений, различающихся между собой объемом энергонезависимой памяти. Предусмотрены исполнения носителя с энергонезависимой памятью физическим объемом 80 или 160 Кбайт.

Для Носителя с защищенной энергонезависимой памятью 80 Кбайт:

Кол-во контейнеров - 6 шт. (по умолчанию).

Размер контейнера - 9 Кб. (по умолчанию).

Поддержка ключей 512 бит ГОСТ Р34.10-2012 - есть

Максимальное число последовательных неуспешных вводов пароля пользователя, - 5 (по умолчанию).

Функция разблокирования/восстановления пароля пользователя по паролю администратора - Есть.

Максимальное число последовательных неуспешных вводов пароля Администратора - 15 (по умолчанию).

Функция форматирования - Есть

Доступ к функции форматирования - по паролю администратора (по умолчанию).

Для Носителя с защищенной энергонезависимой памятью 160 Кбайт:

Кол-во контейнеров – 12 шт. (по умолчанию).

Размер контейнера – 9 Кб. (по умолчанию).

Поддержка ключей 512 бит ГОСТ Р34.10-2012 - Есть

Максимальное число последовательных неуспешных вводов пароля пользователя, – 5 (по умолчанию).

Функция разблокирования/восстановления пароля пользователя по паролю администратора – Есть.

Максимальное число последовательных неуспешных вводов пароля Администратора - 15 (по умолчанию).

Функция форматирования - Есть

Доступ к функции форматирования - по паролю администратора (по умолчанию).

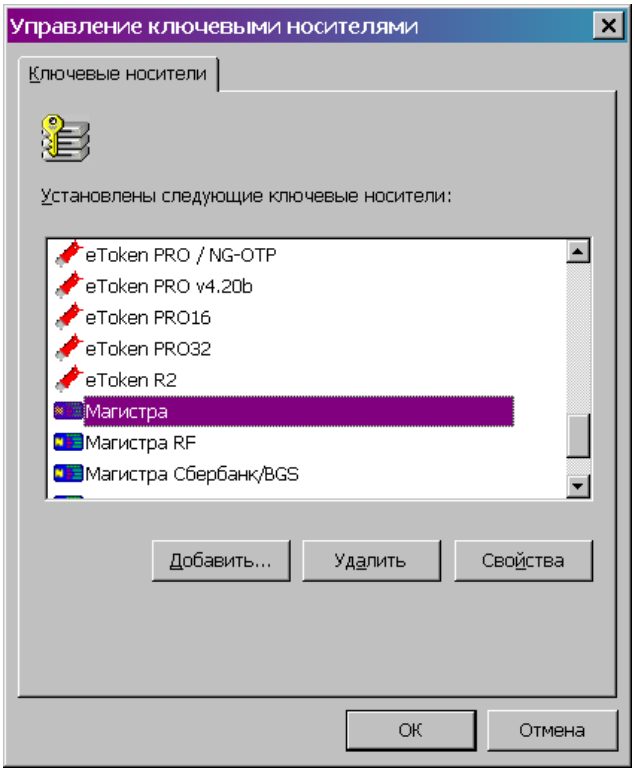
Для корпоративных пользователей:

1. Допускается адаптация логической конфигурации носителя с учетом функциональных особенностей систем Заказчика.
2. Возможно встраивание дополнительных приложений, реализуемых по спецификации Заказчика.

# 3 Интеграция носителя и Криптопровайдера

Программный модуль поддержки Носителя встроен в дистрибутив Криптопровайдера начиная с Cryptopro CSP версии 3.6. Дополнительная инсталляция Носителя в Криптопровайдере не требуется.

Носитель распознается встроенным в Криптопровайдер модулем поддержки как носитель "Магистра".




# 4 Эксплуатация Носителя

## 4.1 Схема разграничения доступа к данным носителя

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

**У Пользователя есть 5 (Пять) попыток (параметр устанавливается По-умолчанию) для ввода правильного значения ПИН (Пароля). Если все попытки ввода ПИН Пользователя будут неудачными, то механизм ввода ПИН будет заблокирован автономным механизмом Носителя и дальнейший доступ Криптопровайдера к Носителю будет невозможен, даже в случае ввода верного значения ПИН.**

Разблокирование ПИН Пользователя и некоторые другие административные функции можно выполнить лишь при условии подтверждения оператором права Администратора путем успешного ввода ПИН (пароля) Администратора.

**Механизм ввода 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 либо невозможным, либо доступным с помощью встроенной в носитель функции форматирования**

**носителя при условии, что для нее заранее был задан режим свободного доступа.**

***Примечание***. 1. Функция форматирования 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 у производителя.

### 4.2 Средства администрирования

Набор административных функций носителя состоит из:

- функции разблокирования пароля Пользователя;
- функции изменения значения пароля Администратора;
- функции очистки носителя (удаления информации из контейнеров);
- справочных функций.

***Примечание***. Пароли Пользователя и Администратора автоматически блокируются носителем после достижения заданного порога на число последовательных неудачных попыток предъявления.

Счетчик неудачных предъявлений носителя сбрасывается после предъявления корректного значения пароля при условии, что заданный ограничительный порог не достигнут.

Средством администрирования является утилита UnblockUserPin которая может быть загружена с сайта компании СмартПарк:

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

Административные функции реализуются в рамках схемы разграничения доступа к данным носителя. Разблокирование Пароля Пользователя и некоторые другие административные функции можно выполнить лишь при условии подтверждения оператором права Администратора путем успешного ввода ПИН (пароля) Администратора.

#### *4.2.1 Смена Пароля Пользователя*

***Внимание!!!***

При вводе Носителя в эксплуатацию, Пользователь должен сменить устанавливаемое Производителем Носителя "по умолчанию" значение ПИН (Пароля) Пользователя, на собственное.

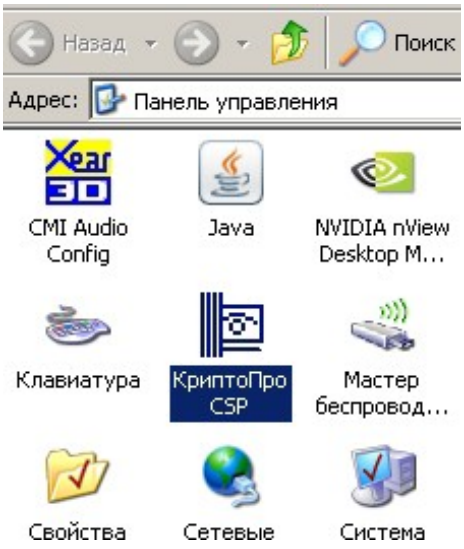
***Сохранение в тайне рабочего значения ПИН (Пароля) Пользователя и***

***его своевременная смена, являются необходимыми условиями безопасной эксплуатации Носителя в рамках сервисов Криптопровайдера.***

Производитель настоятельно рекомендует не использовать "простых" комбинаций символов для ПИН (Пароля) Пользователя.

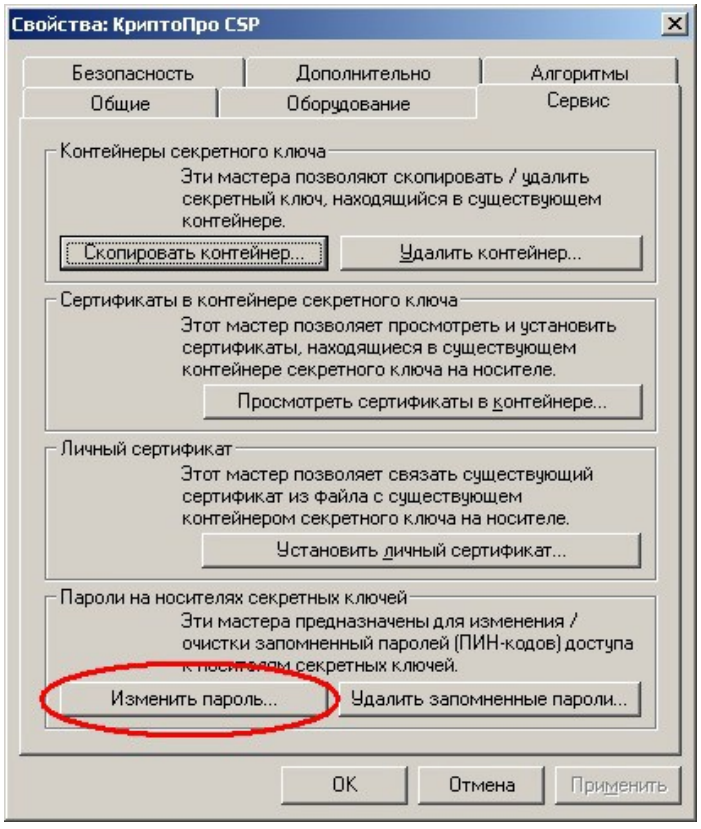
Смена ПИН (Пароля) Пользователя в штатном режиме производится средствами Криптопровайдера из оснастки КриптоПро CSP в Панели Управления.

Откройте оснастку управления КриптоПро 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 ПИН Пользователя на «**пустое**», оснастка КриптоПро CSP выдаст сообщение «Внутренняя ошибка», но, тем не менее, *может* произойти изменение ПИН на «пустое» значение.

### *4.2.2 Разблокировка ПИН (Пароля) Пользователя*

Разблокирование Средствами Утилиты производится следующим образом:

1. Оператор подключает Носитель с заблокированным ПИН Пользователя к компьютеру.
2. Оператор запускает утилиту разблокирования (UnblockUserPIN.exe).
3. Оператор «нажимает кнопку» «Разблокировать», расположенную в разделе «ПИН пользователя» окна программы.
4. Оператор вводит значение ПИН администратора в поле «Текущий ПИН администратора».
5. При необходимости оператор вводит новое значение ПИН пользователя в полях «Новый ПИН пользователя» и «Повторите новый ПИН пользователя».
6. Оператор «нажимает кнопку» «Разблокировать».

Если все данные введены правильно, то будет выполнена операция разблокирования ПИН (пароля) пользователя, а также смена его старого значения на указанное.

### *4.2.3 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 ПИН (Пароля) Администратора на собственное.**

***Сохранение в тайне рабочего значения ПИН Администратора и его своевременная смена являются необходимым условием безопасной эксплуатации Смарт-карты в рамках сервисов Криптопровайдера и в рамках системы в целом.***

Производитель настоятельно рекомендует не использовать "простых"

комбинаций символов для ПИН Администратора.

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

1. Оператор подключает Носитель к компьютеру.
2. Оператор запускает утилиту разблокирования (UnblockUserPIN.exe).
3. Оператор «нажимает кнопку» «Изменить», расположенную в разделе «ПИН администратора» окна программы.
4. Оператор вводит значение ПИН (пароля) администратора в поле «Текущий ПИН администратора».
5. Оператор вводит новое значение ПИН администратора в поле «Новый ПИН администратора» и дублирует его в поле повтора.
6. Оператор «нажимает кнопку» «Изменить».

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

### *4.2.4 Форматирование (очистка) Носителя*

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

Операция форматирования доступна после успешного предъявления действующего значения ПИН Администратора:

1. Оператор подключает Носитель к компьютеру.
2. Оператор активизирует функцию "Удалить все контейнеры".
3. Оператор вводит текущее и новое (с дублированием) значения ПИН администратора, а также новое значение ПИН Пользователя (с дублированием).
4. Оператор инициирует операцию форматирования нажатием на соответствующий элемент управления ("кнопку").

***Примечание***. 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.

Вариант "Опциональный" - установка свободного доступа к функции форматирования.

Корпоративный Заказчик может выбрать опциональный вариант при заказе носителей.

### *4.2.5 Получение количества оставшихся попыток предъявления ПИН (Пароля) Администратора/Пользователя*

Средствами Утилиты разблокирование производится следующим образом

1. Оператор подключает Носитель к компьютеру.
2. Оператор запускает утилиту разблокирования (UnblockUserPIN.exe).
3. Оператор «нажимает кнопку» «Статус», расположенную в разделе «ПИН пользователя» либо расположенную в разделе «ПИН администратора».

### *4.2.6 Получение серийного номера микроконтроллера ключевого Носителя*

Получение серийного номера микроконтроллера ключевого Носителя производится с помощью утилиты «UnblockUserPIN.exe» следующим образом

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

## 5 ПИН (Пароль) Носителя, устанавливаемый "по-умолчанию"

| **Владелец значения** | **Значение ПИН (Пароля) по умолчанию** (строка символов) |
|---|---|
| Пользователь | 11111111 |
| Администратор | 87654321<br>Для корпоративных Заказчиков может устанавливаться особо при наличии соответствующего запроса. |