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.

Pin-код, 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.

(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-КриптоПро-USB логически и физически объединяет два устройства: SSID-смарт-карт ридер и смарт-карту с приложением "Контейнер для криптопровайдера КриптоПро".

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

Носитель обеспечивает:

- защищенное хранение и использование ключей и сертификатов в рамках информационной технологии криптопровайдера КриптоПро CSP;
- защиту ключей и сертификатов от несанкционированного доступа в случае утери или хищения Носителя;
- возможность разблокирования Носителей, заблокированных по причине превышения числа попыток неудачного предъявления пароля пользователя.

2 Конфигурация Носителя

Носитель имеет ряд исполнений, различающихся между собой объемом энергонезависимой памяти.

Предусмотрены исполнения с памятью 18 Кбайт, 48 Кбайт, 80 Кбайт и 160 Кбайт. Потребитель может выбрать конкретное исполнение в зависимости от своих потребностей.

Предусмотрены следующие варианты логической конфигурации Носителя "по умолчанию":

Для Носителя с защищенной энергонезависимой памятью 18 Кбайт:

Кол-во контейнеров – 2шт. (по умолчанию).

Размер контейнера – 7 Кб. (по умолчанию).

Количество попыток неудачного предъявления пароля пользователя – 5

попыток (по умолчанию).

Функция разблокирования/восстановления пароля – ДА (по умолчанию). Количество попыток ввода пароля администратора – 15 попыток (по умолчанию).

Для Носителя с защищенной энергонезависимой памятью 48 Кбайт:

Кол-во контейнеров – 4шт.

Размер контейнера – 10 Кб. (по умолчанию).

Количество попыток неудачного предъявления пароля пользователя – 5 попыток (по умолчанию).

Функция разблокирования/восстановления пароля – ДА (по умолчанию). Количество попыток ввода пароля администратора - 15 попыток (по умолчанию).

Для Носителя с защищенной энергонезависимой памятью 80 Кбайт:

Кол-во контейнеров – 7 шт. (по умолчанию).

Размер контейнера – 10 Кб. (по умолчанию).

Количество попыток неудачного предъявления пароля пользователя – 5 попыток (по умолчанию).

Функция разблокирования/восстановления пароля – ДА (по умолчанию). Количество попыток ввода пароля администратора - 15 попыток (по умолчанию).

Для Носителя с защищенной энергонезависимой памятью 160 Кбайт:

Кол-во контейнеров – 15 шт. (по умолчанию).

Размер контейнера – 10 Кб. (по умолчанию).

Количество попыток неудачного предъявления пароля пользователя – 5 попыток (по умолчанию).

Функция разблокирования/восстановления пароля – ДА (по умолчанию). Количество попыток ввода пароля администратора - 15 попыток (по умолчанию).

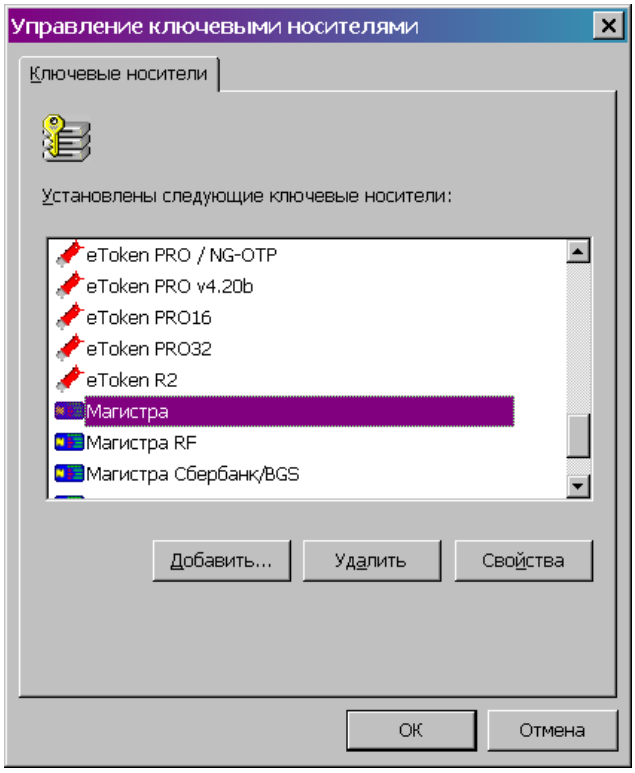
Для корпоративных пользователей:

1. Потребитель (Заказчик) может согласовать собственную конфигурацию приложения Носителя в зависимости от своих потребностей.
2. Возможно встраивание в Носитель дополнительных приложений, реализуемых по спецификации Заказчика.

3 Интеграция Носителя и Криптопровайдера

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

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

У Пользователя есть 5 попыток (параметр устанавливается По-умолчанию) для ввода правильного значения Pin-кода. Если все попытки ввода Pin-кода будут неудачными, то механизм ввода Pin-кода будет заблокирован автономным механизмом Носителя и дальнейший доступ к нему со стороны Криптопровайдера будет невозможен, даже в случае ввода

верного значения Pin-кода.

Разблокирование Носителя возможно путем применения утилиты разблокирования (http://smart-park.ru/util/Unblock_soft.rar) при условии, что оператор утилиты подтверждает свое право Администратора путем ввода известного ему пароля Администратора.

Механизм ввода пароля Администратора допускает 15 (параметр устанавливается По-умолчанию) последовательных попыток неудачного ввода, после чего безвозвратно блокируется и восстановление работоспособности Носителя для сервисов Криптопровайдера становится невозможным. Носитель с заблокированным паролем Администратора следует утилизировать или заменить в нем смарт-карту на новую.

В случае утери рабочего значения Pin-кода Пользователя, его разблокировка не приводит к положительному эффекту, так как доступ к данным остается закрытым. Для выхода из этой ситуации утилита разблокирования предусматривает операцию смены значения Pin-кода Пользователя на основании предъявленного права Администратора.

4.2 Смена Pin-кода Пользователя

Внимание!!!

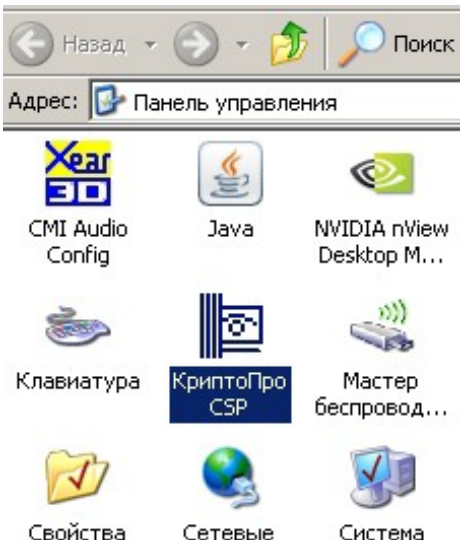
При вводе Носителя в эксплуатацию, Пользователь должен сменить транспортное значение Pin-кода Пользователя, на собственное.

Сохранение в тайне рабочего значения Pin-кода Пользователя и его своевременная смена, являются необходимым условием безопасной эксплуатации Носителя.

Настоятельно не рекомендуется использование "простых" комбинаций символов для Pin-кода Пользователя.

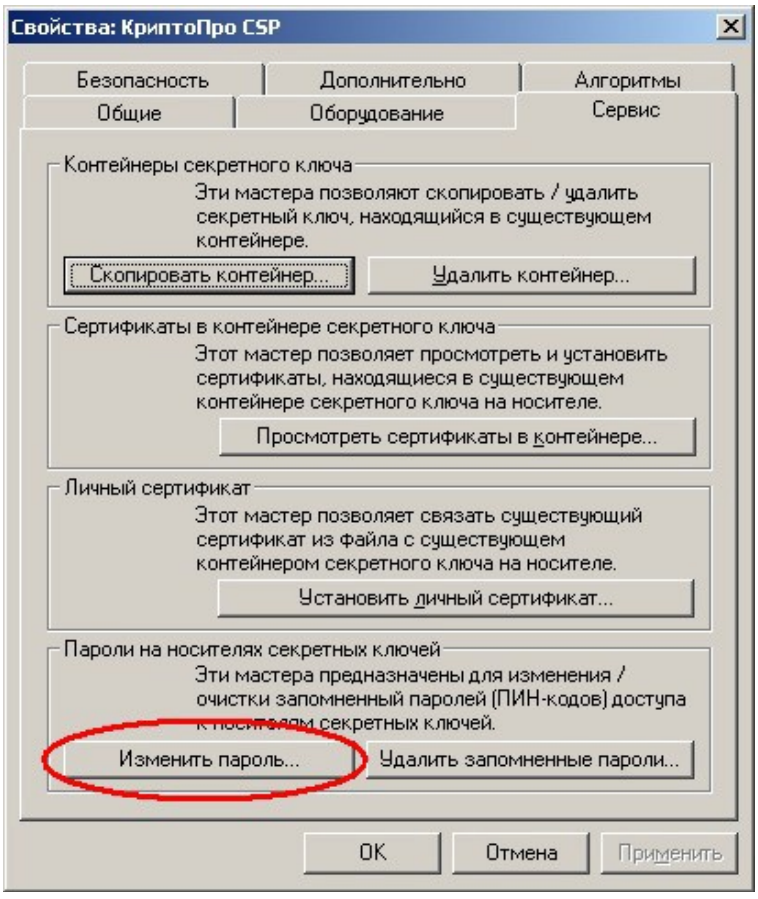
Смена Pin-кода Пользователя в штатном режиме производится средствами "оснастки" КриптоПро CSP в Панели Управления Криптопровайдером.

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 оригинальной документации.

Примечание. Обратите внимание, что при изменении значения Pin-кода Пользователя на **пустое**, оснастка КриптоПро CSP выдает сообщение «Внутренняя ошибка», но, тем не менее, происходит изменение Pin-кода на пустое значение.

4.3 Разблокировка Pin-кода Пользователя

Разблокирование Pin-кода Пользователя производится с помощью утилиты «UnblockUserPIN.exe». Данная утилита может быть загружена с сайта компании СмартПарк в составе пакета Unblock_soft.rar (http://smart-park.ru/util/Unblock_soft.rar).

Разблокирование Pin-кода Пользователя производится следующим образом

1. Оператор подключает Носитель с заблокированным Pin-кодом 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 пользователя, а также смена старого значения на указанное.

4.4 Смена Pin-кода 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 Pin-кода Администратора на собственное.

Сохранение в тайне рабочего значения Pin-кода Администратора и его своевременная смена являются необходимым условием безопасной

эксплуатации Носителя в рамках сервисов Криптопровайдера и в рамках системы в целом.

Производитель настоятельно рекомендует не использовать "простых" комбинаций символов для Pin-кода Администратора.

Смена Pin-кода Администратора производится с помощью утилиты «UnblockUserPIN.exe».

Разблокирование 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 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.

5 Pin-коды Носителя, устанавливаемый "по умолчанию"

Владелец значения Pin-кода	**Значение PIN-код по умолчанию** (строка символов)
Пользователь	11111111
Администратор	- 87654321 или - другое значение, передаваемое потребителю отдельно