

ООО «ВАЛИДАТА»

УТВЕРЖДЕН  
ВАМБ.00060-06-ЛУ

**СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ  
«ВАЛИДАТА CSP» ВЕРСИЯ 6**

**ФУНКЦИОНАЛЬНЫЙ КЛЮЧЕВОЙ НОСИТЕЛЬ «ВАЛИДАТА VDTOKEN»  
ВЕРСИЯ 2.0**

Руководство пользователя

ВАМБ.000060-06 92 03

2020

## **Аннотация**

Настоящий документ содержит описание применения функционального ключевого носителя «Валидата vdToken» версия 2.0 (далее — ФКН «vdToken») в программном комплексе (ПК) ВАМБ.00060-06 «СКЗИ «Валидата CSP» версия 6» (далее - СКЗИ «Валидата CSP»), а также в программных комплексах, использующих СКЗИ «Валидата CSP».

Документ предназначен для администраторов и пользователей СКЗИ «Валидата CSP».

## Содержание

<b>1</b>	<b>ОБЩЕЕ ОПИСАНИЕ</b>	<b>4</b>
1.1	Назначение . . . . .	4
1.2	Режимы использования . . . . .	4
1.3	ПИН-код . . . . .	4
1.4	Сервисы и драйверы . . . . .	4
1.5	Условия применения . . . . .	5
1.6	Сроки действия ключей ЭП . . . . .	5
1.6.1	Удаление ключей с ключевого носителя . . . . .	5
1.6.2	Уничтожение ключевого носителя . . . . .	5
<b>2</b>	<b>ПОДГОТОВКА К ПРИМЕНЕНИЮ</b>	<b>6</b>
2.1	Форматирование . . . . .	6
2.1.1	Форматирование ключевого носителя в «неизвлекаемом» режиме . . . . .	7
2.1.2	Форматирование ключевого носителя в «извлекаемом» режиме	11
2.2	Смена ПИН-кода . . . . .	13
2.2.1	Ключевые носители с установленным ПИН-кодом . . . . .	13
2.2.2	Ключевые носители без ПИН-кода . . . . .	14
2.3	Отключение экономии энергии . . . . .	15
<b>3</b>	<b>РАБОТА С КЛЮЧАМИ</b>	<b>17</b>
3.1	Создание ключа на носителе . . . . .	17
3.1.1	Создание «извлекаемого» ключа . . . . .	17
3.1.2	Создание «неизвлекаемого» ключа . . . . .	18
3.2	Удаление ключа с носителя . . . . .	19
3.2.1	Удаление ключа с «неизвлекаемого» ключевого носителя . . .	20
3.2.2	Удаление ключа с «извлекаемого» ключевого носителя . . . .	21
3.3	Копирование ключей . . . . .	21
3.3.1	Копирование ключей с «неизвлекаемого» ключевого носителя	21
3.3.2	Копирование ключей с «извлекаемого» ключевого носителя .	21
	<b>ПЕРЕЧЕНЬ СОКРАЩЕНИЙ</b>	<b>23</b>
	<b>ПЕРЕЧЕНЬ РИСУНКОВ</b>	<b>25</b>

# 1 ОБЩЕЕ ОПИСАНИЕ

## 1.1 Назначение

Функциональный ключевой носитель «Валидата vdToken» версия 2.0 представляет собой «USB-токен», который предназначен для хранения и использования ключей электронной подписи (ЭП) пользователей СКЗИ «Валидата CSP». Дополнительно к ключу пользователя на ФКН «vdToken» можно записать его личный сертификат.

*Примечание — Отличия ФКН «Валидата vdToken» от ФКН «Валидата vdToken» версия 2.0 приведены в документе ВАМБ.00060-06 30 01 «СКЗИ «Валидата CSP» версия 6. Формуляр».*

## 1.2 Режимы использования

Ключи, находящиеся в ФКН «vdToken», можно использовать в «неизвлекаемом» режиме, при котором ключ пользователя никогда не попадает из ФКН «vdToken» в память компьютера, что обеспечивается за счет выполнения криптографических операций непосредственно в самом ФКН «vdToken».

В целях универсальности ФКН «vdToken» можно применять в обычном «извлекаемом» режиме, когда ключ хранится на носителе, а для использования загружается в память компьютера.

ФКН «vdToken» позволяет одновременно хранить разные ключи пользователя на одном носителе как в «неизвлекаемом», так и «извлекаемом» режимах.

*Примечание - В интерфейсе для указания на использование ФКН «vdToken» в «неизвлекаемом» режиме применяется обозначение «считыватель vdToken (ФКН)», на использование в «извлекаемом» режиме – «считыватель vdToken».*

## 1.3 ПИН-код

ФКН «vdToken» предусматривает установку ПИН-кода (пароля) при форматировании для доступа к использованию функций ФКН «vdToken». В ФКН «vdToken» обеспечивается процедура смены ПИН-кода.

ПИН-код должен состоять из не менее чем 8 символов при мощности алфавита не менее 36. Смена ПИН-кода должна выполняться с периодом не более 6 месяцев.

Использование ФКН «vdToken» возможно без ПИН-кода, но в этом случае только в «извлекаемом» режиме, так как для «неизвлекаемого» режима наличие ПИН-кода является обязательным условием.

## 1.4 Сервисы и драйверы

Для работы с ФКН «vdToken» не нужно устанавливать на компьютер никаких дополнительных программ, сервисов и драйверов, так как ФКН «vdToken» использует стандартные сервисы и драйверы, входящие в операционную систему (ОС) Windows для поддержки «смарт-карт».

## **1.5 Условия применения**

Учет ФКН «vdToken» ведется порядком, установленным в эксплуатирующей организации для внешних съемных носителей.

## **1.6 Сроки действия ключей ЭП**

Максимальные сроки действия ключей ЭП в зависимости от условий эксплуатации приведены в документе ВАМБ.00060-06 31 01 «СКЗИ «Валидата CSP» версия 6. Описание применения».

### **1.6.1 Удаление ключей с ключевого носителя**

По окончании срока действия ключей ЭП соответствующие ключи должны быть удалены с ключевого носителя (см. подраздел 3.2 настоящего документа).

После удаления ключей ФКН «vdToken» готов к дальнейшей работе — созданию и записи новой ключевой информации.

### **1.6.2 Уничтожение ключевого носителя**

В том случае, если ФКН «vdToken» не предполагается использовать, его необходимо уничтожить порядком, установленным эксплуатирующей организацией.

## 2 ПОДГОТОВКА К ПРИМЕНЕНИЮ

### 2.1 Форматирование

Прежде всего ФКН «vdToken» нужно отформатировать.

Для этого запустите программу конфигурации (Рисунок 1) СКЗИ «Валидата CSP».

*Примечание — В интерфейсе программы конфигурации СКЗИ «Валидата CSP» обозначается как «СКЗИ».*

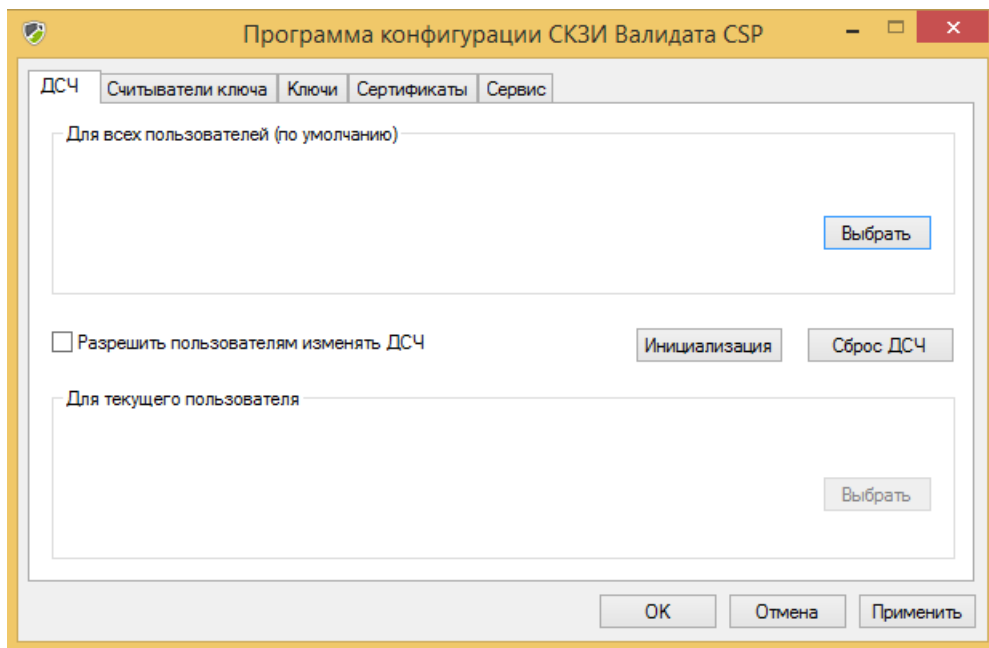


Рисунок 1 – Программа конфигурации

Выберите вкладку «Сервис» (Рисунок 2).

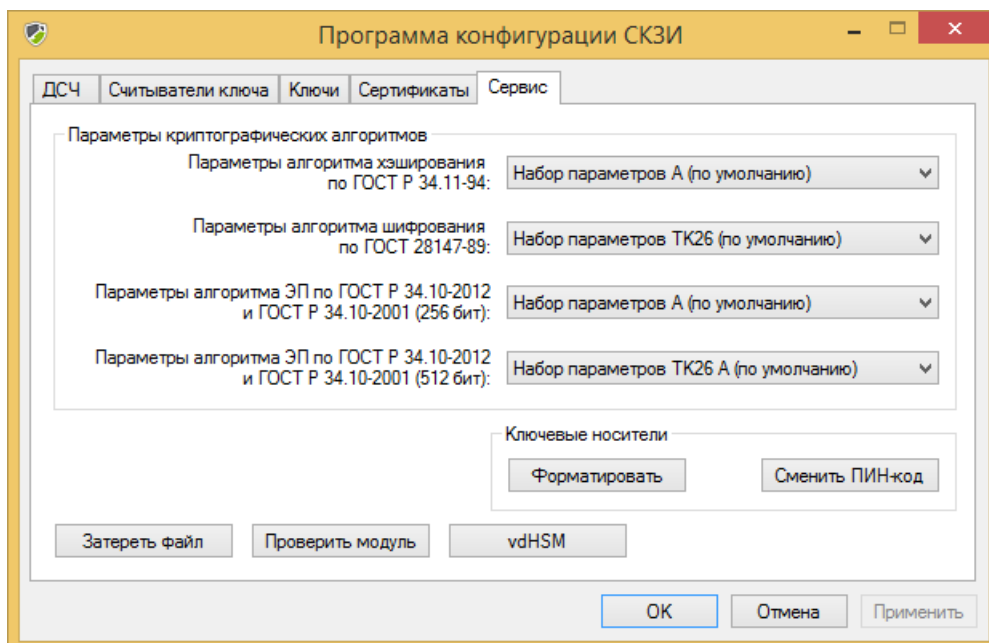


Рисунок 2 – Вкладка «Сервис»

Установите ФКН «vdToken» в USB-разъем.  
Нажмите кнопку «Форматировать».

### 2.1.1 Форматирование ключевого носителя в «неизвлекаемом» режиме

Для форматирования ключевого носителя в «неизвлекаемом» режиме выберите «Считыватель vdToken (ФКН)» и нажмите кнопку «ОК» (Рисунок 3).

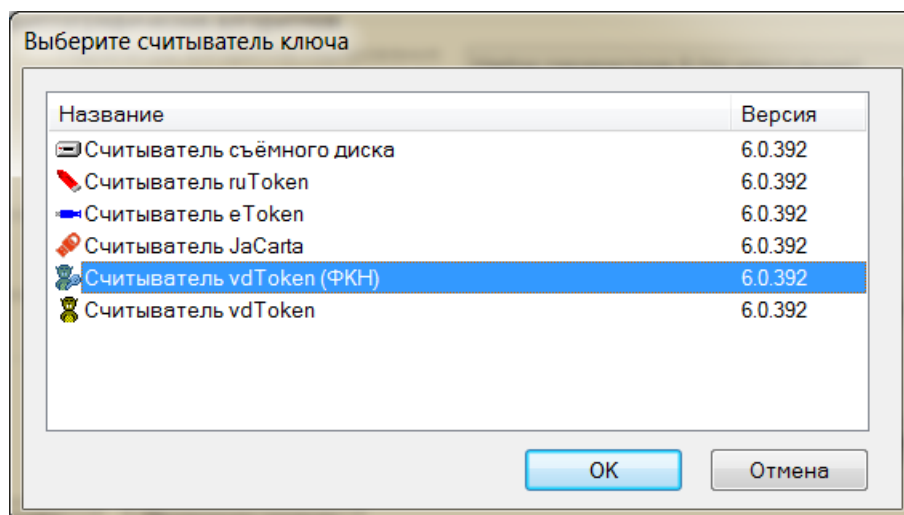


Рисунок 3 – Выбор считывателя

Если на компьютере еще не был проинициализирован датчик случайных чисел (ДСЧ), то на экран компьютера может быть выдано диалоговое окно для его инициализации. Например, в случае, если в качестве ДСЧ задан «Биологический ДСЧ», будет выдан следующий диалог (Рисунок 4).

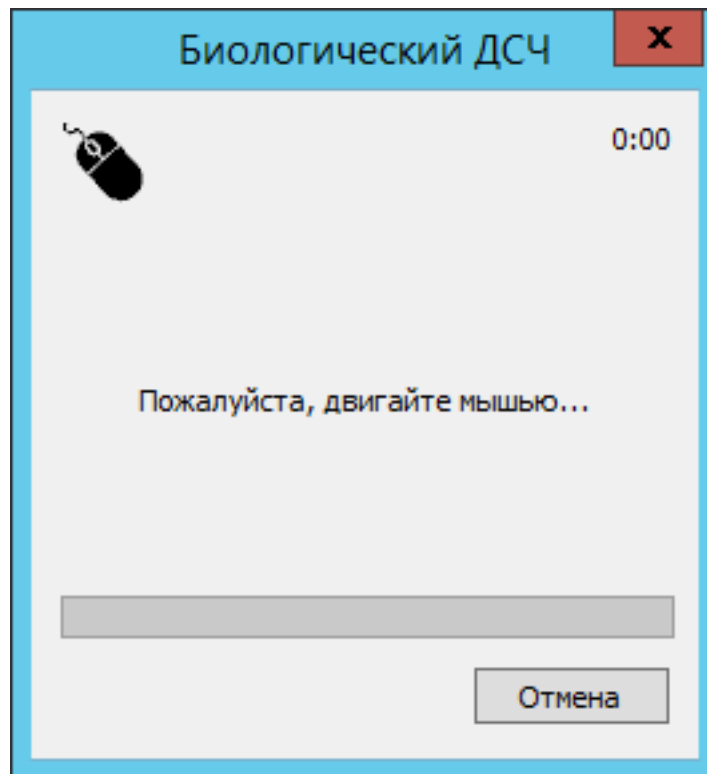


Рисунок 4 – Инициализация ДСЧ

Порядок действий, выполняемых для инициализации биологического ДСЧ, приведен в документе ВАМБ.00060-06 95 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора». После завершения инициализации ДСЧ данное окно (Рисунок 4) закроется самостоятельно.

Выберите установленный ключевой носитель и нажмите «ОК» (Рисунок 5).

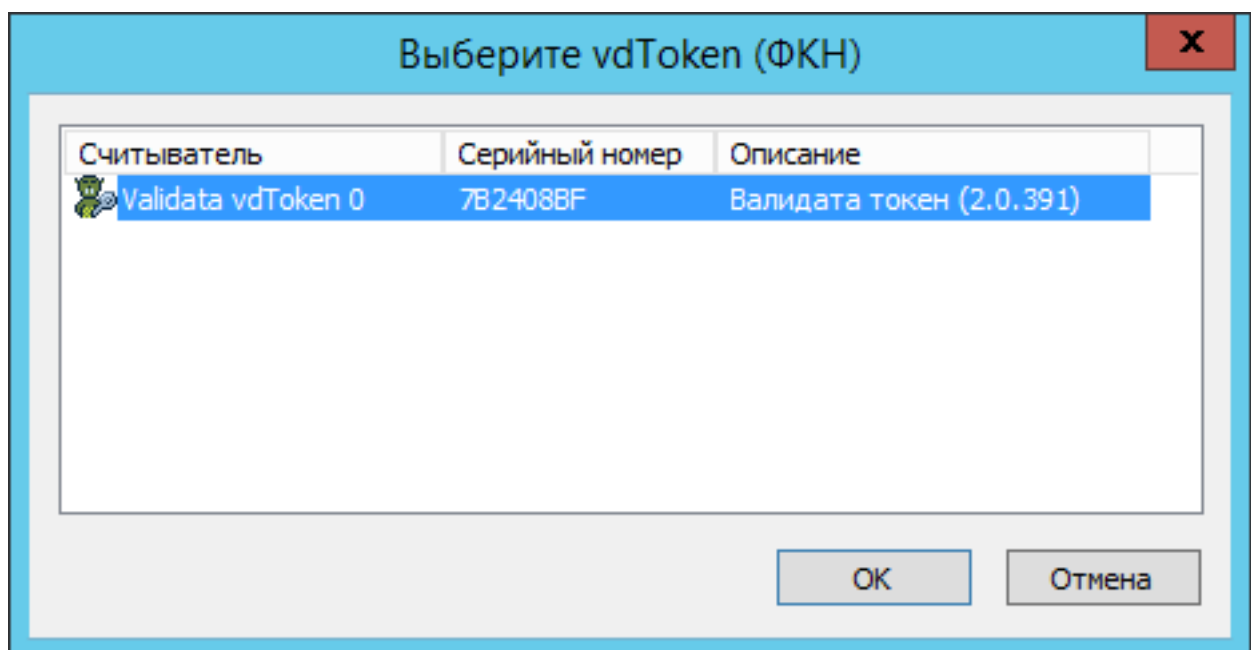


Рисунок 5 – Выбор ключевого носителя

Окно форматирования ФКН «vdToken» в «неизвлекаемом» режиме предлага-



ет задать максимальный размер сертификата (в DER-кодировке), который можно будет записать на этот ключевой носитель (Рисунок 6).

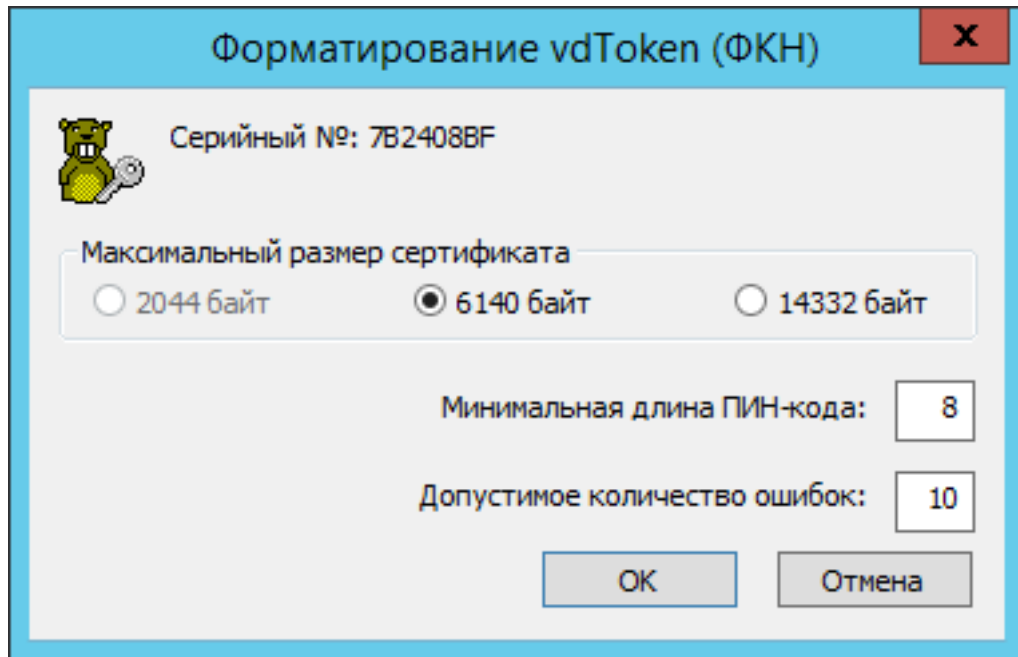


Рисунок 6 – Окно форматирования

Параметр «максимальный размер сертификата» влияет на максимальное количество ключей, поддерживаемых отформатированным ключевым носителем:

- «2044 байт» — 63 ключа;
- «6140 байт» — 31 ключ;
- «14332 байт» — 15 ключей.

Минимальная длина ПИН-кода может быть установлена в диапазоне от 8 до 32 символов.

Допустимое количество ошибок можно задать от 3 до 10. Если при вводе ПИН-кода допустить ошибок более, чем указано в этом параметре, то для продолжения работы потребуется вынуть ФКН «vdToken» из USB-разъема и повторно установить ключевой носитель в USB-разъем. Данная защита нужна от возможного программного подбора ПИН-кода.

Нажмите «ОК».

Перед форматированием на экран выдается предупреждение, что при форматировании все ключевые данные (ключи и сертификаты), находящиеся на ФКН «vdToken», будут уничтожены (Рисунок 7).

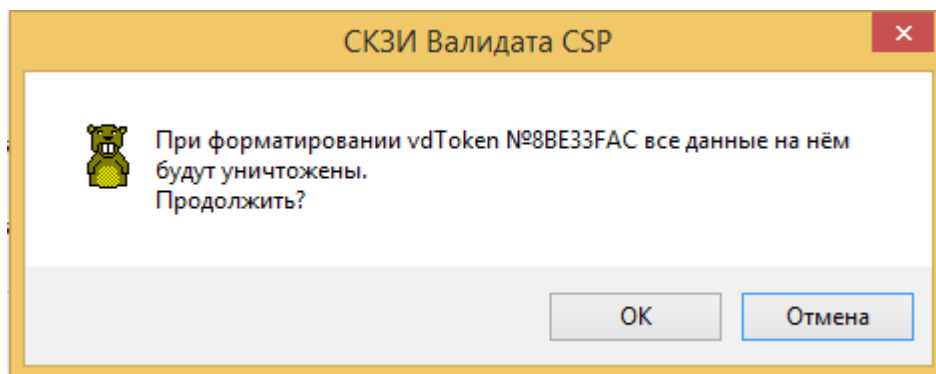


Рисунок 7 – Предупреждение перед форматированием

Если данные (ключи и сертификаты) на ключевом носителе уже не нужны или форматирование выполняется первый раз, то нажмите кнопку «ОК».

Введите ПИН-код и его подтверждение. Нажмите «ОК» (Рисунок 8).

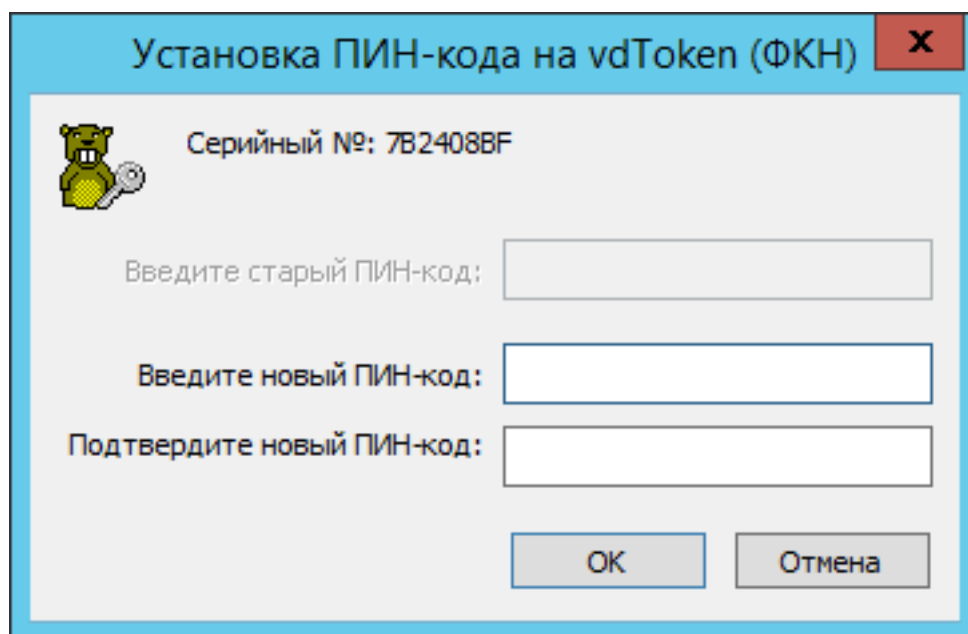


Рисунок 8 – Установка PIN-кода

Форматирование выполнено успешно, нажмите «ОК» (Рисунок 9).

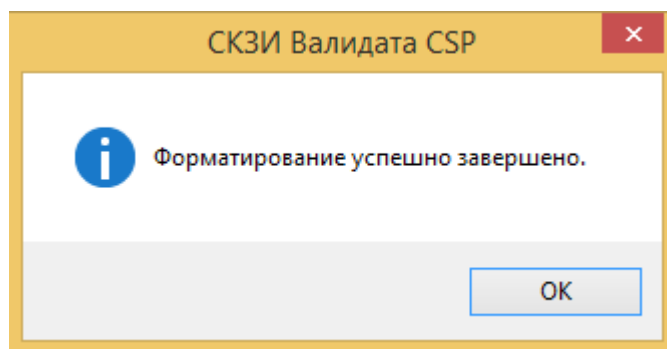


Рисунок 9 – Сообщение об успешном форматировании

На ФКН «vdToken», отформатированном в «неизвлекаемом» режиме, можно одновременно записывать ключи как в «неизвлекаемом» режиме, так и в «извлекаемом» режиме.

### 2.1.2 Форматирование ключевого носителя в «извлекаемом» режиме

Для форматирования ключевого носителя в «извлекаемом» режиме выберите «Считыватель vdToken» и нажмите кнопку «ОК» (Рисунок 10).

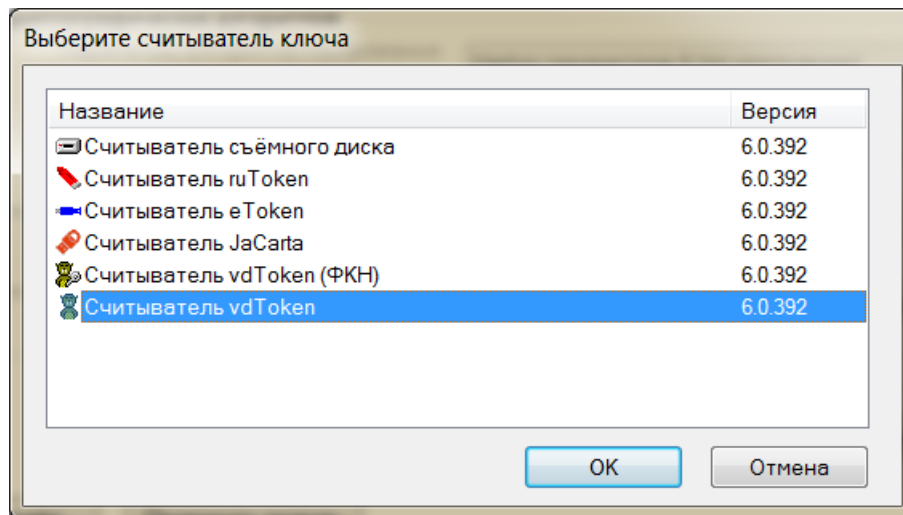


Рисунок 10 – Выбор считывателя

Если на компьютере еще не был проинициализирован ДСЧ, то на экран компьютера будет выдано диалоговое окно для его инициализации (Рисунок 4).

Порядок действий, выполняемых для инициализации биологического ДСЧ, приведен в документе ВАМБ.00060-06 95 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора». После завершения инициализации ДСЧ данное окно (Рисунок 4) закроется самостоятельно.

Выберите установленный ключевой носитель и нажмите «ОК» (Рисунок 11).

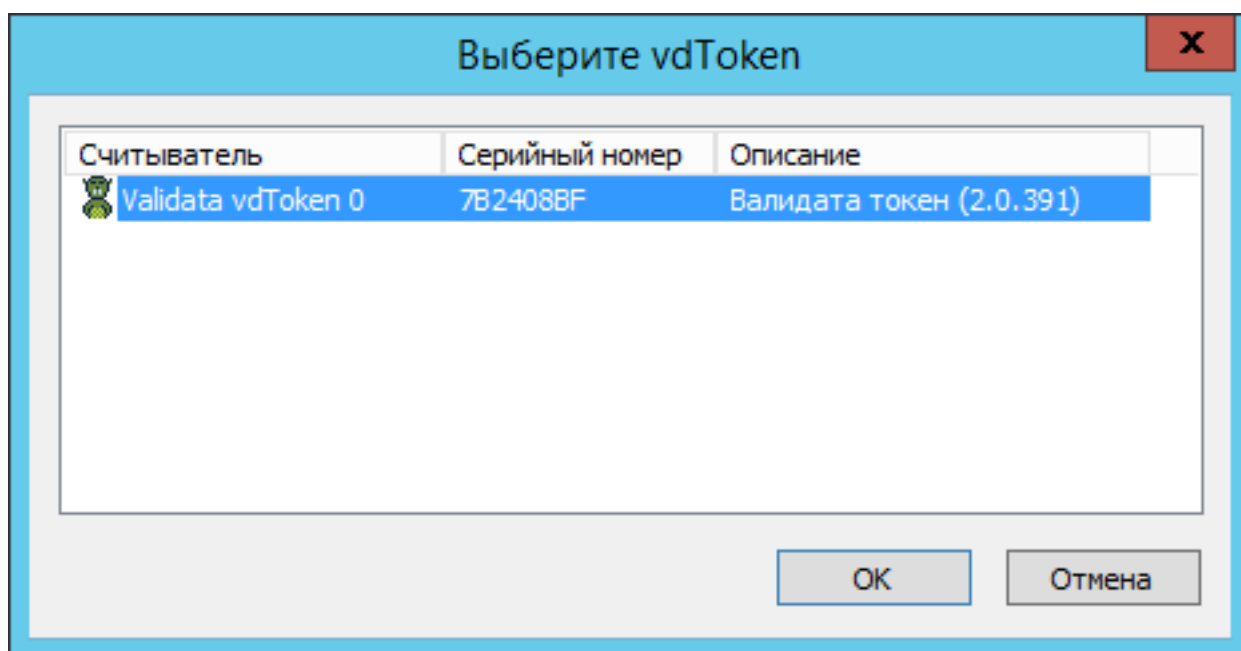


Рисунок 11 – Выбор ключевого носителя

Окно форматирования ключевого носителя в «извлекаемом» режиме предлагает задать максимальный размер сертификата (в DER-кодировке), который можно будет записать на этот ключевой носитель (Рисунок 12).

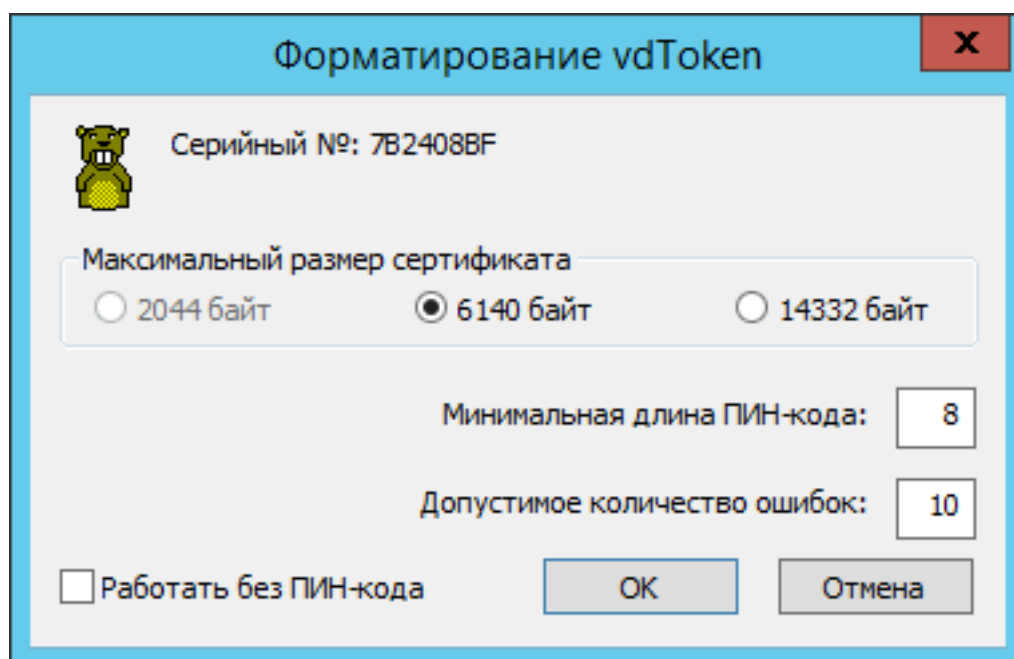


Рисунок 12 – Окно форматирования

Параметр «максимальный размер сертификата» влияет на максимальное количество ключей, поддерживаемых отформатированным ключевым носителем:

- «2044 байт» – 63 ключа;
- «6140 байт» – 31 ключ;

– «14332 байт» — 15 ключей.

Минимальная длина ПИН-кода возможна в диапазоне от 8 до 32 символов.

Допустимое количество ошибок можно задать от 3 до 10. Если при вводе ПИН-кода допустить ошибок более, чем указано в этом параметре, то для продолжения работы потребуется вынуть ФКН «vdToken» из USB-разъема и повторно установить ключевой носитель в USB-разъем. Данная защита нужна от возможного программного подбора ПИН-кода.

Параметр «Работать без ПИН-кода» позволяет отказаться от установки ПИН-кода. В этом случае работать с ключевым носителем можно без пароля, но хранить и использовать «неизвлекаемые» ключи на таком носителе нельзя.

Нажмите «ОК».

Перед форматированием на экран выдается предупреждение, что при форматировании все ключевые данные (ключи и сертификаты), находящиеся на ФКН «vdToken», будут уничтожены (Рисунок 7).

Если данные (ключи и сертификаты) на ключевом носителе уже не нужны, или форматирование выполняется первый раз, то нажмите кнопку «ОК».

Введите ПИН-код и его подтверждение. Нажмите «ОК» (Рисунок 8).

Форматирование выполнено успешно, нажмите «ОК» (Рисунок 9).

На ФКН «vdToken», отформатированный в «извлекаемом» режиме с установкой ПИН-кода, можно одновременно записывать ключи как в «извлекаемом» режиме, так и в «неизвлекаемом» режиме.

## 2.2 Смена ПИН-кода

ПИН-код – это единый пароль для доступа к ключам и функциям ФКН «vdToken», он не зависит от количества ключей и режима их использования («неизвлекаемый» или «извлекаемый»), то есть ПИН-код имеет отношение только к ключевому носителю.

Процедура форматирования ключевого носителя заставляет пользователя установить ПИН-код или отказаться от его использования, но в этом случае на ключевой носитель можно будет записать только «извлекаемый» ключ.

Смена ПИН-кода всегда доступна пользователю в программе конфигурации СКЗИ «Валидата CSP». Для этого нужно выбрать вкладку «Сервис» (Рисунок 2).

Нажмите кнопку «Сменить ПИН-код».

Смену ПИН-кода можно произвести как через «неизвлекаемый» считыватель «Считыватель vdToken (ФКН)», так и через «извлекаемый» считыватель «Считыватель vdToken» (Рисунок 3, Рисунок 10).

У ключевого носителя будет новый ПИН-код для доступа ко всем ключам, которые на нем находятся, вне зависимости от режима их использования («неизвлекаемый» или «извлекаемый»).

Установите ФКН «vdToken» в USB-разъем.

Выберите, например, «неизвлекаемый» считыватель «Считыватель vdToken (ФКН)» (Рисунок 3) и нажмите «ОК».

Выберите установленный ключевой носитель (Рисунок 5) и нажмите «ОК».

### 2.2.1 Ключевые носители с установленным ПИН-кодом

Если установленный ключевой носитель был отформатирован с ПИН-кодом, то на экран будет выдано окно, приведенное ниже (Рисунок 13).

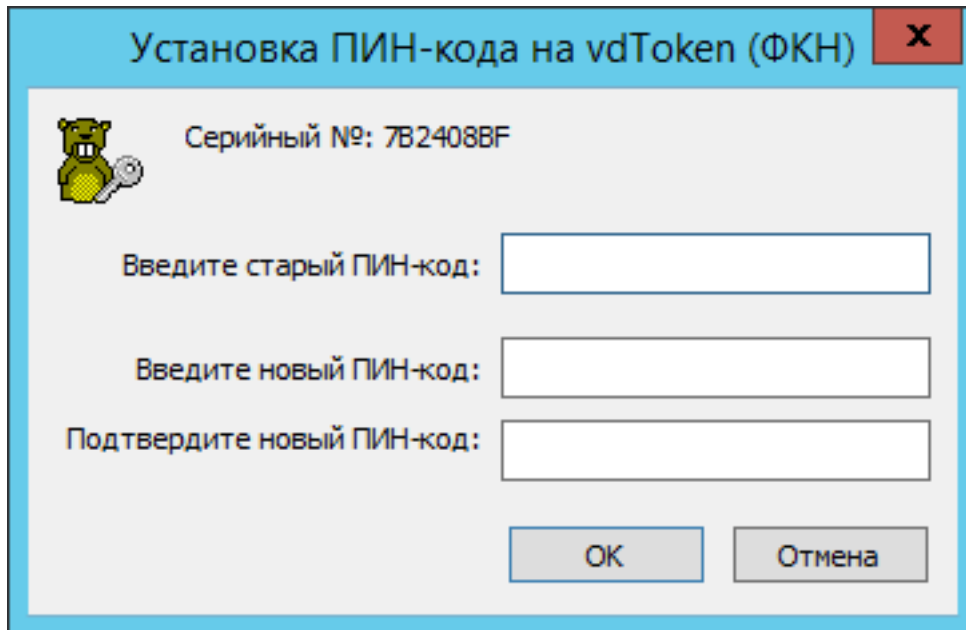


Рисунок 13 – Окно смены ПИН-кода

Для замены ПИН-кода введите в строке «Введите старый ПИН-код:» текущий ПИН-код ключевого носителя, в следующих строках новый ПИН-код, на который нужно перейти, два раза для контроля случайных ошибок.

Нажмите «ОК».

На экране появится сообщение об успешной замене ПИН-кода (Рисунок 14).

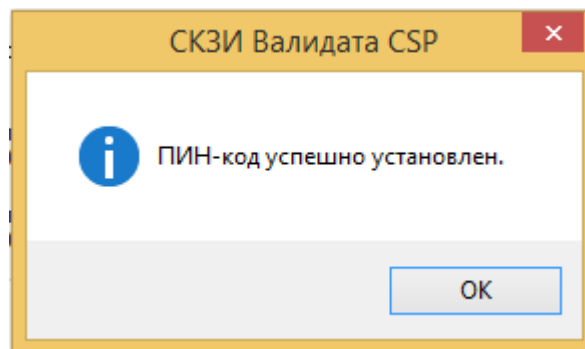


Рисунок 14 – Сообщение о замене ПИН-кода

Теперь при использовании данного ключевого носителя нужно будет вводить новый ПИН-код.

Нажмите кнопку «ОК».

### 2.2.2 Ключевые носители без ПИН-кода

Если установленный ключевой носитель был отформатирован без установки ПИН-кода, то будет выдано на экран окно установки ПИН-кода (Рисунок 8).

Для установки ПИН-кода введите его два раза для контроля случайных ошибок. Нажмите «ОК».

*Примечание - На ключевом носителе без ПИН-кода уже могут находиться «извлекаемые» ключи, так что после установки ПИН-кода эти ключи будут*

доступны, но для работы с ними нужно будет вводить ПИН-код. Вернуть ключевой носитель обратно в состояние без ПИН-кода можно будет только при форматировании с потерей всех ключей, так как процедуры удаления ПИН-кода не предусмотрено.

На экране появится сообщение об успешной установке ПИН-кода (Рисунок 14).

Нажмите кнопку «ОК». Теперь на этот ключевой носитель можно записывать как «извлекаемые» ключи, так и «неизвлекаемые» ключи.

## 2.3 Отключение экономии энергии

Для корректной работы ФКН «vdToken» необходимо отключить режим экономии энергии для USB-устройства. Это особенно важно для работы ФКН «vdToken» с сервером. Для этого перейдите в «Панель управления», «Оборудование», «Диспетчер устройств» или введите «devmgmt.msc» в командной строке. Для выполнения операции требуются права администратора. В случае их отсутствия нужно обратиться к системному администратору.

Откройте список «Контроллеры USB» (Рисунок 15).

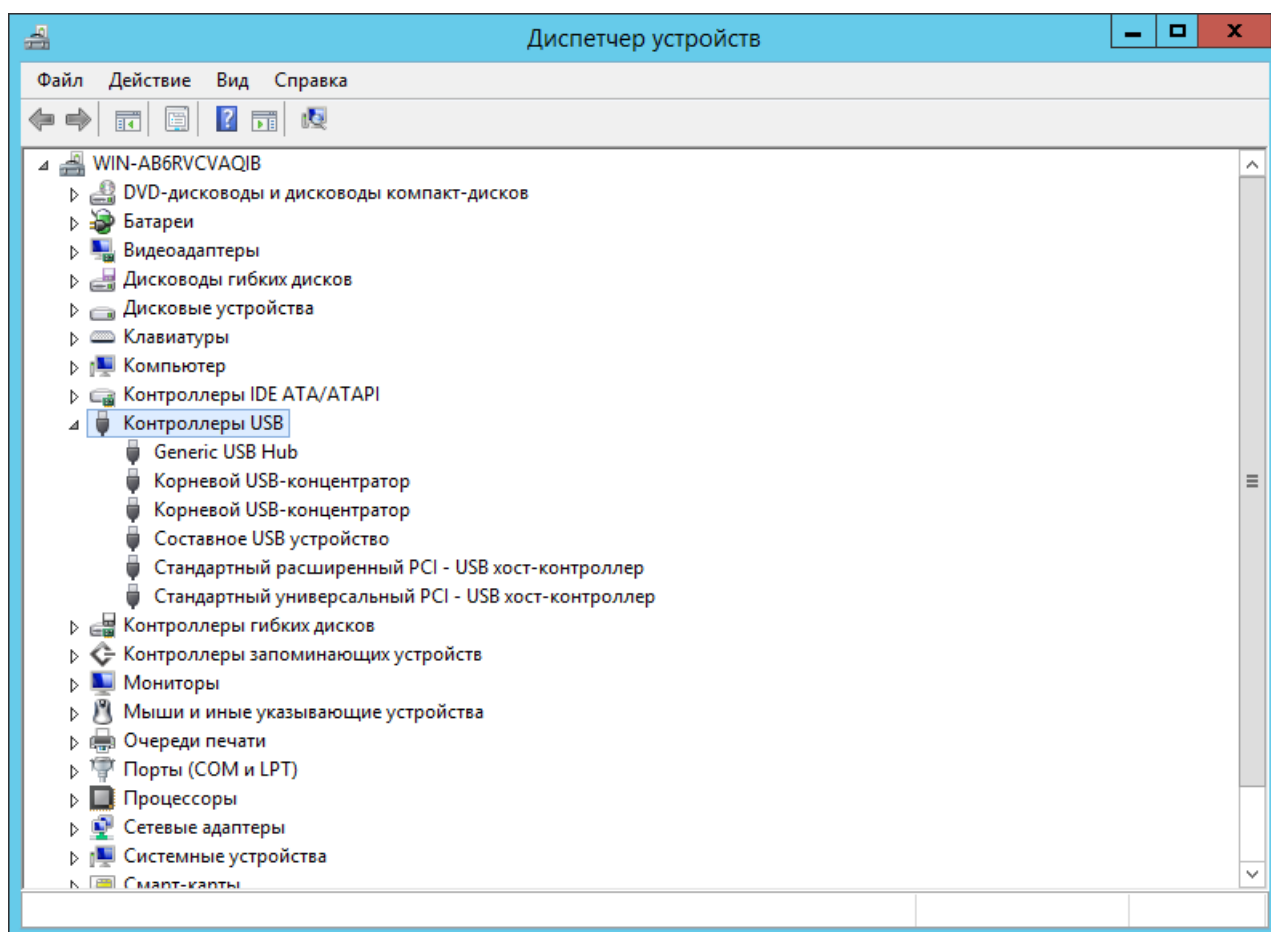


Рисунок 15 – Диспетчер устройств

Дважды нажмите на USB-концентратор, который использует ФКН «vdToken». Откройте вкладку «Управление электропитанием». Отключите пункт настроек «Разрешить отключение этого устройства для экономии энергии» (Рисунок 16).

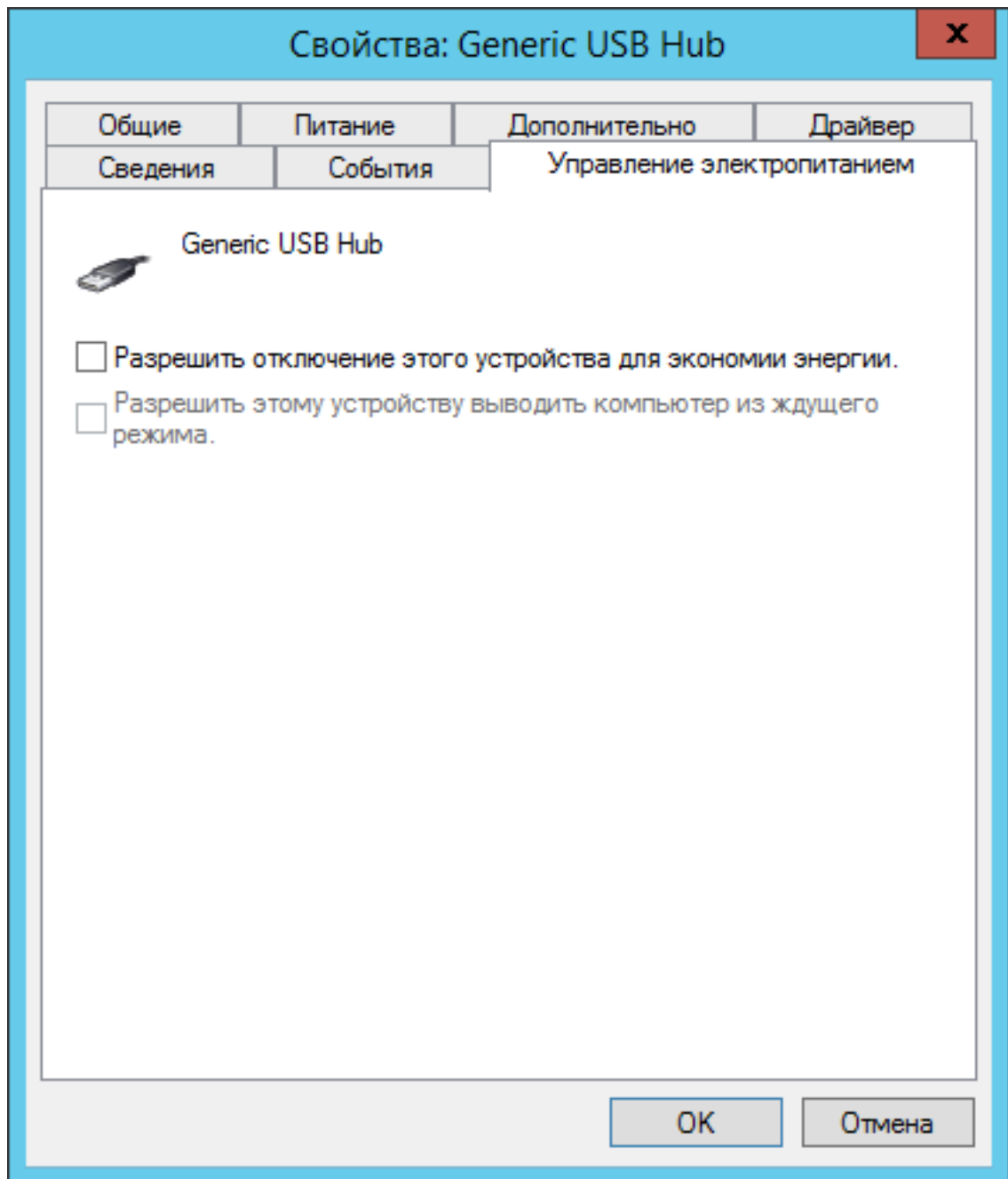


Рисунок 16 – Свойства USB-концентратора

Нажмите «ОК».



## 3 РАБОТА С КЛЮЧАМИ

### 3.1 Создание ключа на носителе

Ключи можно создавать только на отформатированном ФКН «vdToken». Перед созданием ключа на экран выдается предупреждение (Рисунок 17).

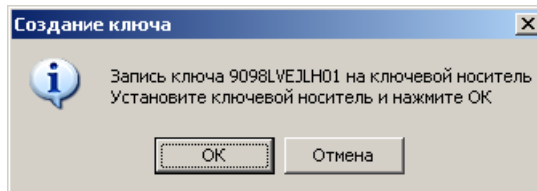


Рисунок 17 – Предупреждение при генерации ключа

Установите ФКН «vdToken» в USB-разъем. Нажмите «ОК».

Выберите считыватель ключа (Рисунок 3).

Если в программе конфигурации СКЗИ «Валидата CSP» установлен считыватель по умолчанию, то это окно («Выбор ключевого считывателя») выдаваться не будет, а программа будет переходить к следующему диалогу выбора ключевого носителя, выдавая сразу их список в рамках считывателя, установленного по умолчанию.

*Примечание — ФКН «vdToken 2.0», реализованный на базе микроконтроллера МК20DX256 (на аппаратной базе ФКН «vdToken»), не поддерживает генерацию ключей ЭП длиной 512 бит с использованием эллиптической кривой С (Эдвардса).*

#### 3.1.1 Создание «извлекаемого» ключа

Выберите «извлекаемый» считыватель «Считыватель vdToken» и нажмите кнопку «ОК».

Так как ключ на носитель записывается в обычном «извлекаемом» виде, то для защиты ключа в СКЗИ «Валидата CSP» предусмотрена его защита паролем (Рисунок 18).

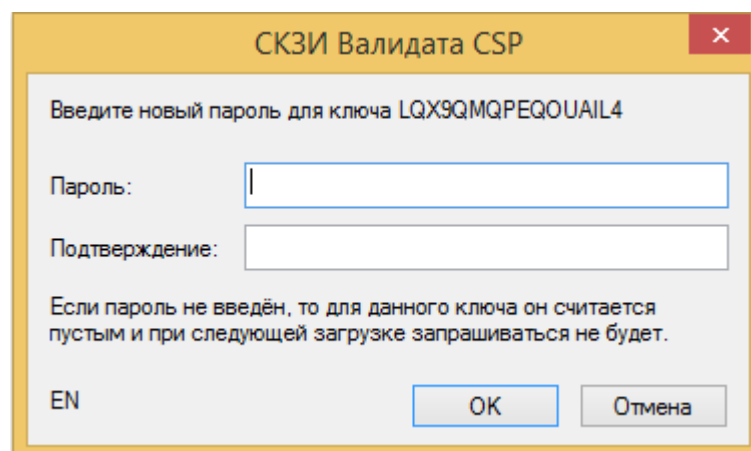


Рисунок 18 – Окно ввода ключевого пароля

Например, если пароль не ввести, а просто нажать «ОК», ключ не будет зашифрован паролем, и при работе с таким ключом пароль запрашиваться не будет.

Выберите ключевой носитель и нажмите «ОК» (Рисунок 5).

Введите ПИН-код этого ключевого носителя (Рисунок 19).

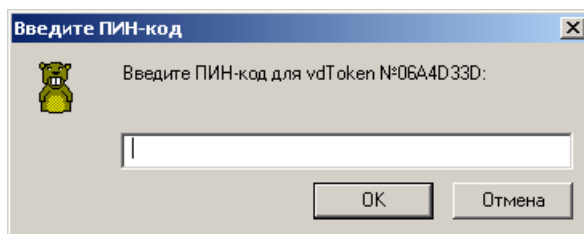


Рисунок 19 – Окно ввода ПИН-кода

*Примечание - Если ключевой носитель был отформатирован без ПИН-кода, то окно ввода ПИН-кода на экран выдаваться не будет.*

Если ПИН-код введен правильный, то будет выполнена генерация ключа и запись его на ключевой носитель в «извлекаемом» режиме.

### 3.1.2 Создание «неизвлекаемого» ключа

Выберите «неизвлекаемый» считыватель «Считыватель vdToken (ФКН)» и нажмите кнопку «ОК» (Рисунок 3).

Введите ПИН-код этого ключевого носителя. Если ПИН-код введен правильный, то будет выполнена генерация ключа и запись его на ключевой носитель в «неизвлекаемом» режиме.

Для предоставления пользователю возможности создания резервной копии этого ключа в момент его генерации выдается диалоговое окно (Рисунок 20).

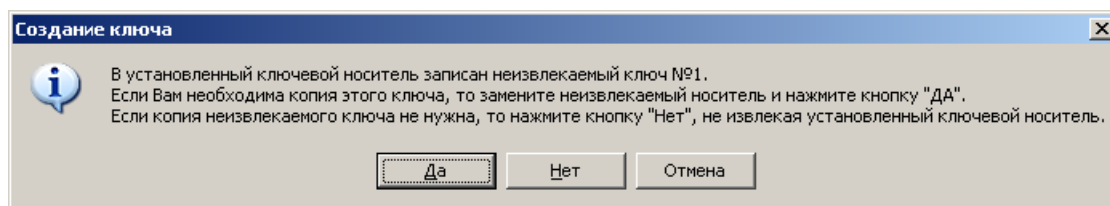


Рисунок 20 – Диалог создания резервной копии ключа

Так как ключ создан на ключевом носителе в «неизвлекаемом» режиме, то в дальнейшем сделать его копию будет невозможно. Единственный вариант, предоставляемый ФКН «vdToken»: создание дубликата ключа возможно только при его генерации и только на носителе ФКН «vdToken» в «неизвлекаемом» режиме. Это означает, что копии ключа нельзя создавать на «дискеты», «флешки» и другие носители.

Если резервная копия ключа не нужна, необходимо нажать кнопку «Нет».

Для создания резервной копии ключа установите другой ФКН «vdToken», который был заблаговременно отформатирован с установкой ПИН-кода. При наличии одного USB-разъема можно извлечь первый носитель и установить следующий резервный носитель в этот же USB-разъем.

Нажмите кнопку «Да».

Выберите ключевой носитель, предназначенный для резервной копии и нажмите кнопку «ОК» (Рисунок 5).

Введите ПИН-код этого резервного ключевого носителя. Если ПИН-код введен правильный, то будет выполнено создание резервной копии ключа на другом ключевом носителе в «неизвлекаемом» режиме.

Следующий диалог предлагает повторить процедуру создания резервных копий ключа на любом количестве ФКН «vdToken» (Рисунок 21).

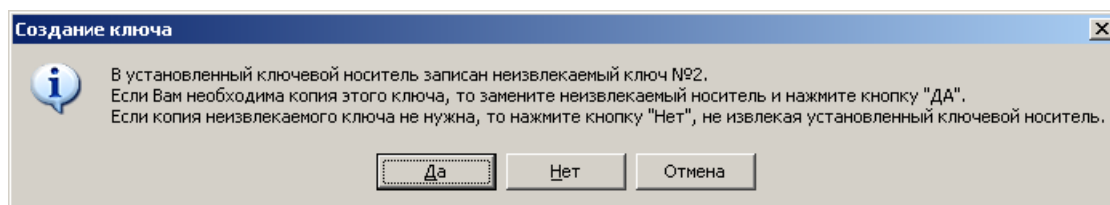


Рисунок 21 – Диалог создания резервной копии ключа

Нажмите кнопку «Нет» или «Да».

Введите ПИН-код последнего созданного ключевого носителя (Рисунок 19).

Процедура генерации ключа с созданием резервной копии завершена.

### 3.2 Удаление ключа с носителя

Удаление ключа с ФКН «vdToken» всегда доступно пользователю в программе конфигурации СКЗИ «Валидата CSP». Для этого выберите закладку «Ключи» (Рисунок 22).

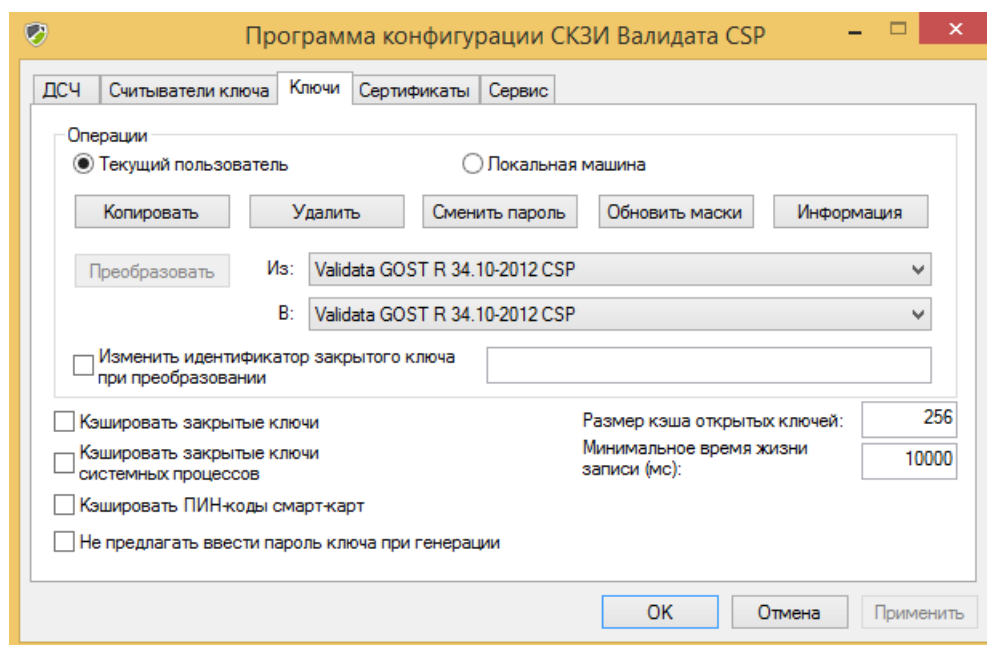


Рисунок 22 – Вкладка «Ключи»

Установите ФКН «vdToken» в USB-разъем.

Нажмите кнопку «Удалить».

### 3.2.1 Удаление ключа с «неизвлекаемого» ключевого носителя

На экран выдается окно со списком номеров ключей и ключевых носителей, на которых они находятся (Рисунок 23).

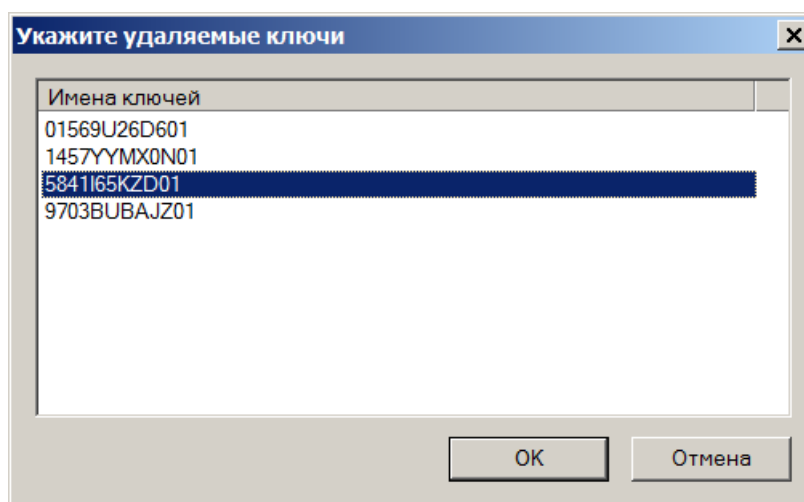


Рисунок 23 – Окно выбора ключей для удаления

В окне выбора ключей для удаления можно указать один или несколько ключей для удаления. Если нужно удалить несколько ключей, то выделять ключи нужно «мышью» с одновременным нажатием клавиши «Ctrl» или «Shift».

Выберите номер ключа (или номера ключей) и нажмите «OK».

Далее нужно подтвердить выполнение действия в окне предупреждения (Рисунок 24).

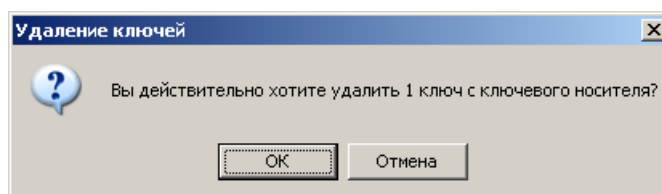


Рисунок 24 – Предупреждение об удалении ключей

Введите ПИН-код для доступа к функции удаления на ключевом носителе. Ключ удален с ключевого носителя. Нажмите «OK» (Рисунок 25).

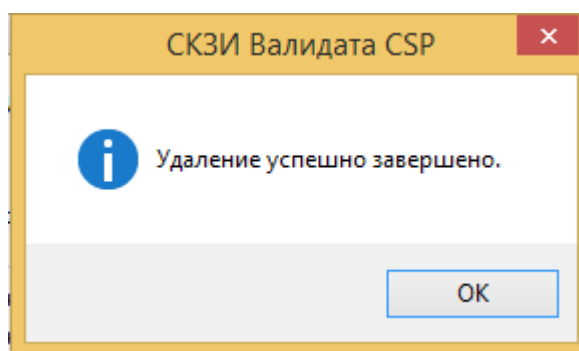


Рисунок 25 – Сообщение об удалении ключа

### **3.2.2 Удаление ключа с «извлекаемого» ключевого носителя**

На экран выдается окно со списком номеров ключей и ключевых носителей, на которых они находятся (Рисунок 23).

В окне выбора ключей для удаления можно указать один или несколько ключей для удаления. Если нужно удалить несколько ключей, то выделять ключи нужно «мышью» с одновременным нажатием клавиши «Ctrl» или «Shift».

Выберите номер ключа (или номера ключей) и нажмите «ОК».

Далее нужно подтвердить выполнение действия в окне предупреждения (Рисунок 24).

Введите ПИН-код для доступа к функции удаления на ключевом носителе (Рисунок 19).

*Примечание - Если ключевой носитель был отформатирован без ПИН-кода, то окно ввода ПИН-кода на экран выдаваться не будет.*

Ключ удален с ключевого носителя. Нажмите «ОК» (Рисунок 25).

## **3.3 Копирование ключей**

Копирование ключей с одного носителя на другой доступно пользователю в программе конфигурации СКЗИ «Валидата CSP». Для этого выберите закладку «Ключи» (Рисунок 22).

### **3.3.1 Копирование ключей с «неизвлекаемого» ключевого носителя**

Копирование ключей с «неизвлекаемого» носителя запрещено, так как «неизвлекаемый» носитель не поддерживает функции чтения ключа с носителя.

### **3.3.2 Копирование ключей с «извлекаемого» ключевого носителя**

Копирование ключей как с «извлекаемого» носителя, так и на «извлекаемый» носитель выполняется обычным образом, как это предусмотрено в СКЗИ «Валидата CSP».

Например, рассмотрим процедуру копирования ключа с флеш-накопителя на «извлекаемый» носитель ФКН «vdToken».

Установите флеш-накопитель с ключом в соответствующий разъем компьютера и нажмите кнопку «Копировать» (Рисунок 22).

Выберите считыватель съемного диска (Рисунок 26). Нажмите кнопку «ОК».

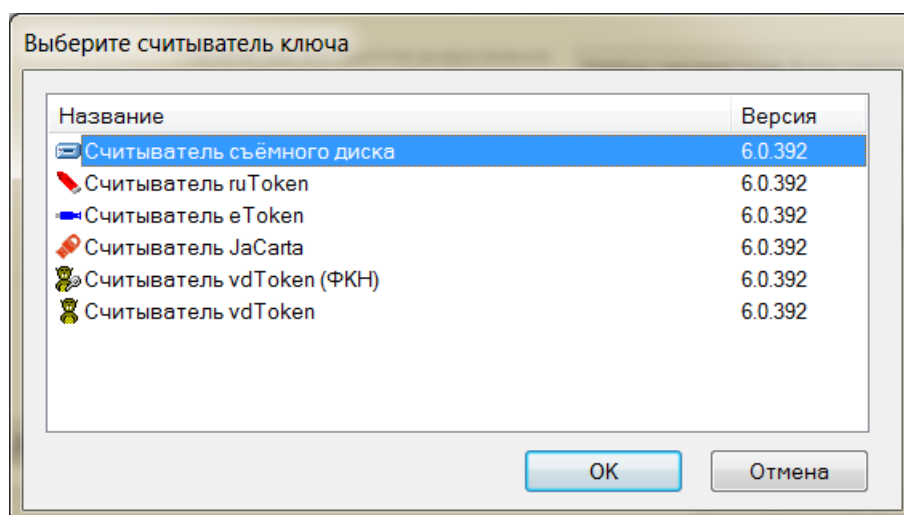


Рисунок 26 – Выбор считывателя ключа

Выберите из списка ключ, который нужно скопировать, и нажмите «ОК» (Рисунок 27).

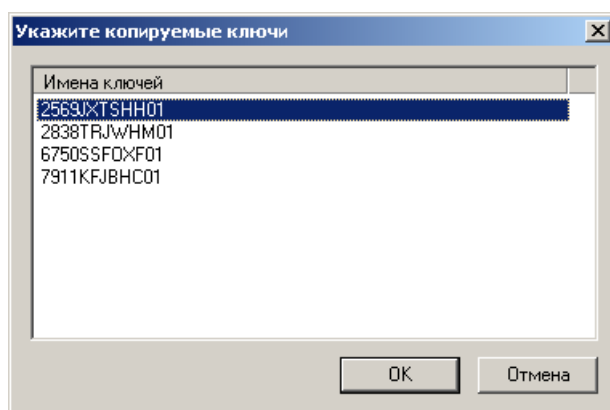


Рисунок 27 – Выбор ключа

Удалите флеш-накопитель с копируемым ключом и установите ФКН «vdToken» в USB-разъём. Нажмите кнопку «ОК» (Рисунок 28).

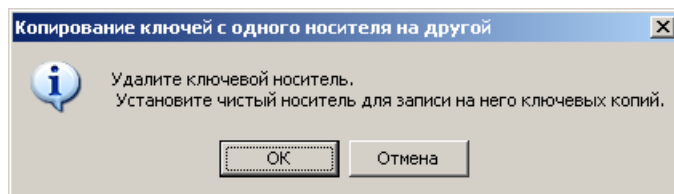


Рисунок 28 – Предупреждение процедуры копирования ключа

Выберите считыватель для «извлекаемых» ключей «Считыватель vdToken». Нажмите «ОК» (Рисунок 10).

Выберите ключевой носитель для копирования ключа и нажмите «ОК» (Рисунок 11).

Введите ПИН-код для доступа к установленному ключевому носителю (Рисунок 19).

*Примечание - Если ключевой носитель был отформатирован без ПИН-кода, то окно ввода ПИН-кода на экран выдаваться не будет.*

Процедура копирования ключа на «извлекаемый» носитель завершена (Рисунок 29).

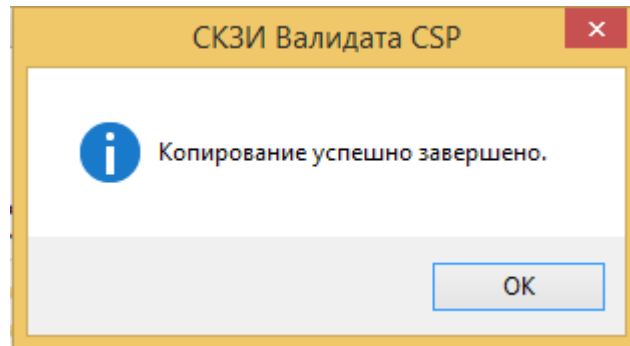


Рисунок 29 – Сообщение об успешном завершении копирования

## **ПЕРЕЧЕНЬ СОКРАЩЕНИЙ**

ДСЧ	Датчик случайных чисел
КЗИ	Криптографическая защита информации
ОС	Операционная система (Operating System)
ПК	Программный комплекс
СКЗИ	Средство криптографической защиты информации
ФКН	Функциональный ключевой носитель
ЭП	Электронная подпись



## ПЕРЕЧЕНЬ РИСУНКОВ

1	Программа конфигурации . . . . .	6
2	Вкладка «Сервис» . . . . .	7
3	Выбор считывателя . . . . .	7
4	Инициализация ДСЧ . . . . .	8
5	Выбор ключевого носителя . . . . .	8
6	Окно форматирования . . . . .	9
7	Предупреждение перед форматированием . . . . .	10
8	Установка PIN-кода . . . . .	10
9	Сообщение об успешном форматировании . . . . .	10
10	Выбор считывателя . . . . .	11
11	Выбор ключевого носителя . . . . .	12
12	Окно форматирования . . . . .	12
13	Окно смены ПИН-кода . . . . .	14
14	Сообщение о замене ПИН-кода . . . . .	14
15	Диспетчер устройств . . . . .	15
16	Свойства USB-концентратора . . . . .	16
17	Предупреждение при генерации ключа . . . . .	17
18	Окно ввода ключевого пароля . . . . .	17
19	Окно ввода ПИН-кода . . . . .	18
20	Диалог создания резервной копии ключа . . . . .	18
21	Диалог создания резервной копии ключа . . . . .	19
22	Вкладка «Ключи» . . . . .	19
23	Окно выбора ключей для удаления . . . . .	20
24	Предупреждение об удалении ключей . . . . .	20
25	Сообщение об удалении ключа . . . . .	20
26	Выбор считывателя ключа . . . . .	22
27	Выбор ключа . . . . .	22
28	Предупреждение процедуры копирования ключа . . . . .	22
29	Сообщение об успешном завершении копирования . . . . .	23

[illegible]