ООО «ВАЛИДАТА»

УТВЕРЖДЕН
ВАМБ.00060-05-ЛУ

АППАРАТНО_ПРОГРАММНОН КОМПЛЕКС «СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ «ВАЛИДАТА CSP» ВЕРСИЯ 5.0»

ФУНКЦИОНАЛЬНЫЙ КЛЮЧЕВОЙ НОСИТЕЛЬ «ВАЛИДАТА VDTOKEN»

Руководство пользователя

ВАМБ.00060-05 92 04

2015

АННОТАЦИЯ

Настоящий документ содержит описание применения функционального ключевого носителя «Валидата vdToken» версия 1.0 (далее – ФКН «vdToken») при совместной работе со средством криптографической защиты информации «Провайдер криптографического сервиса «Валидата CSP» версия 5.0».

Документ предназначен для администраторов и пользователей СКЗИ «Валидата CSP» версия 5.0» (далее по тексту - СКЗИ «Валидата CSP»).

СОДЕРЖАНИЕ

1 ОБЩЕЕ ОПИСАНИЕ

1.1 Назначение

Функциональный ключевой носитель «Валидата vdToken» версия 1.0 (далее - ФКН «vdToken») представляет собой «USB-токен» (далее – «токен»), который предназначен для хранения и использования закрытых ключей шифрования и ключей ЭП пользователей СКЗИ «Валидата CSP» версия 5.0. Дополнительно к ключу пользователя на ФКН «vdToken» можно записать его личный сертификат.

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 «токене», а для использования загружается в память компьютера.

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

1.3 ПИН-код

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

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

ФКН «vdToken» работает под управлением операционных систем (ОС) Windows 7 /2008 /2008R2 /8 /8.1 /2012 /2012R2.

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

1.6 Сроки действия ключей ЭП

1.6.1 Сроки действия ключей в случае применения «извлекаемого» режима

Ключ ЭП – не более 15 месяцев.

1.6.2 Сроки действия ключей в случае применения «неизвлекаемого» режима

Ключи ЭП , записываемые на ФКН в режиме «неизвлекаемого» ключа, – не более 3 (трех) лет.

1.6.3 Удаление ключей с ключевого носителя

По окончании срока действия ключей ЭП соответствующие ключи должны быть удалены с ключевого носителя в соответствии с разделом 3.2 данного документа.

После удаления ключей изделие ФКН «vdToken» готово к дальнейшей работе – созданию и записи новой ключевой информации.

1.6.4 Уничтожение ключевого носителя

В том случае, если изделие ФКН «vdToken» не предполагается использовать, его необходимо уничтожить установленным порядком представителями территориального учреждения или иного структурного подразделения по месту эксплуатации изделия.

2 ПОДГОТОВКА К ПРИМЕНЕНИЮ

2.1 Форматирование

Прежде всего ФКН «vdToken» нужно отформатировать.

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

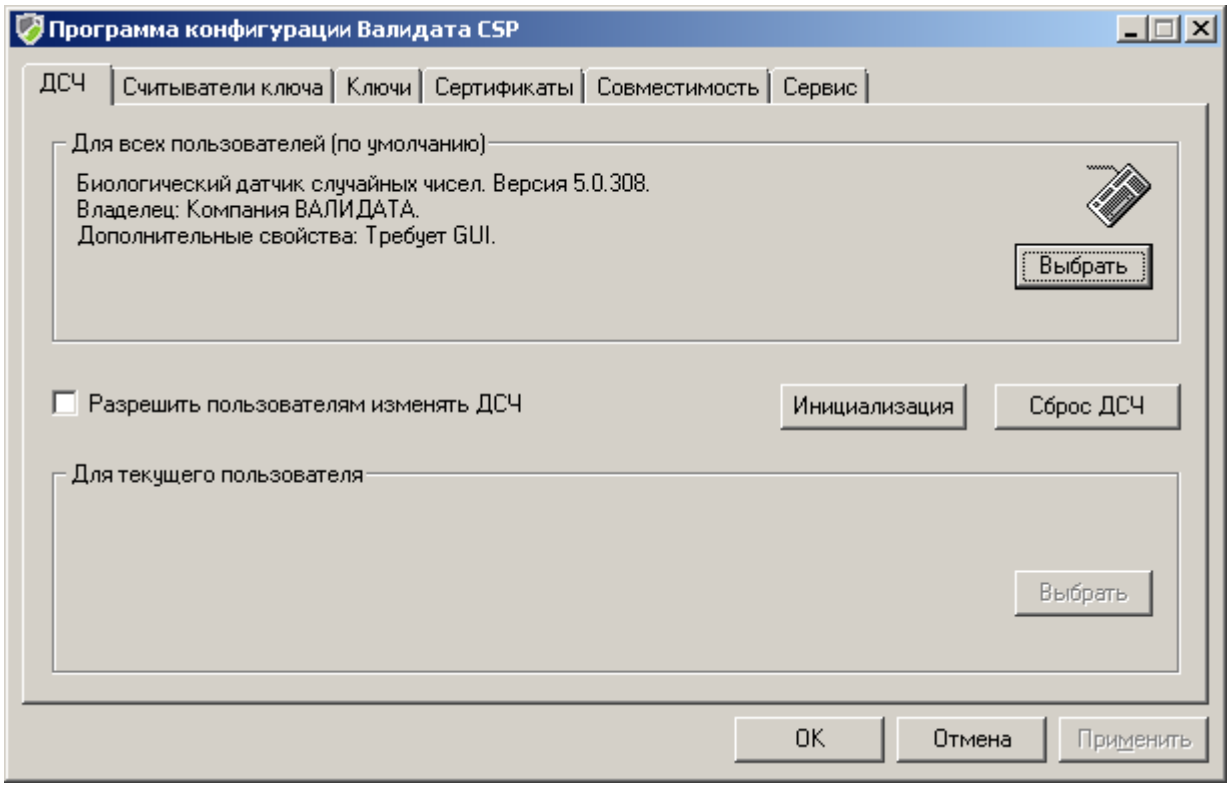

Рисунок 1 - Конфигурационная программа

Выберите закладку «Сервис» (Рисунок 2).

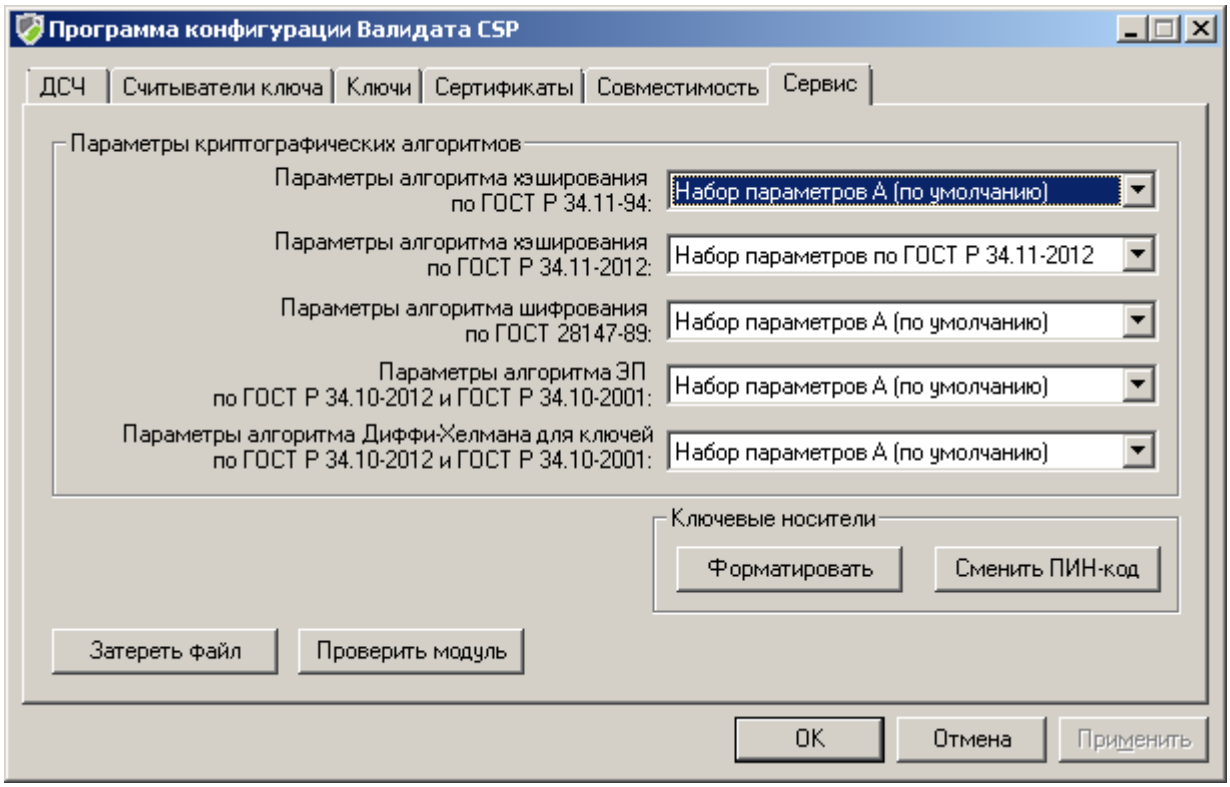

Рисунок 2 - Закладка «Сервис»

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 выберете «Считыватель vdToken (ФКН)» и нажмите кнопку «ОК» (Рисунок 3).

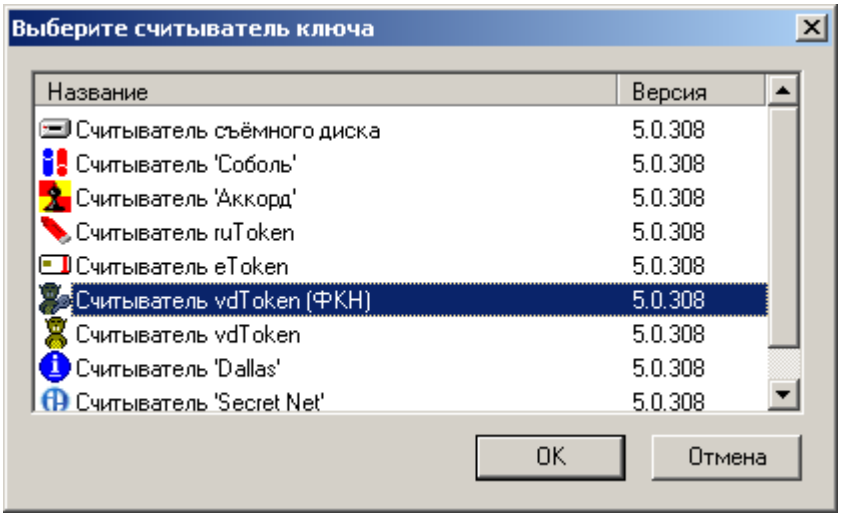

Рисунок 3 - Выбор считывателя

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

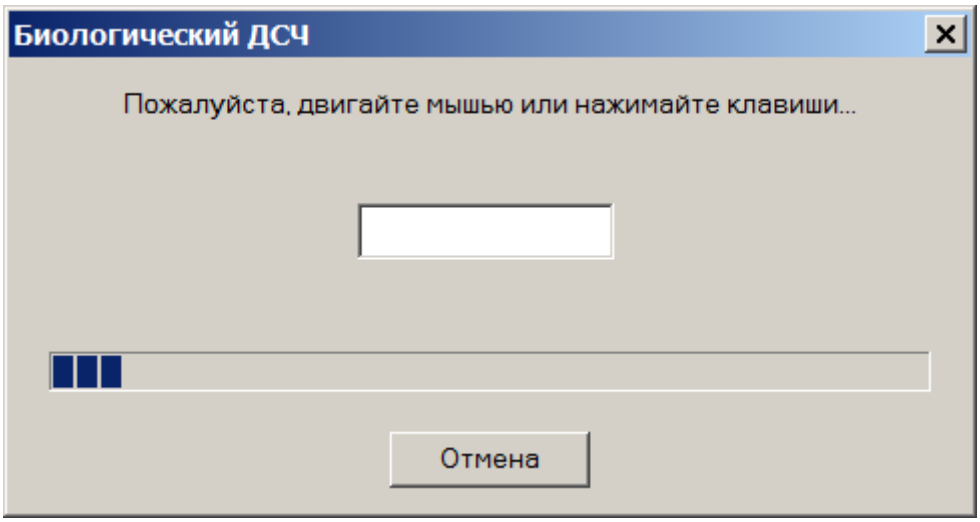

Рисунок 4 – Инициализация ДСЧ

Подвигайте «мышь» или понажимайте клавиши клавиатуры. После завершения инициализации ДСЧ данное окно (Рисунок 4) закроется самостоятельно.

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

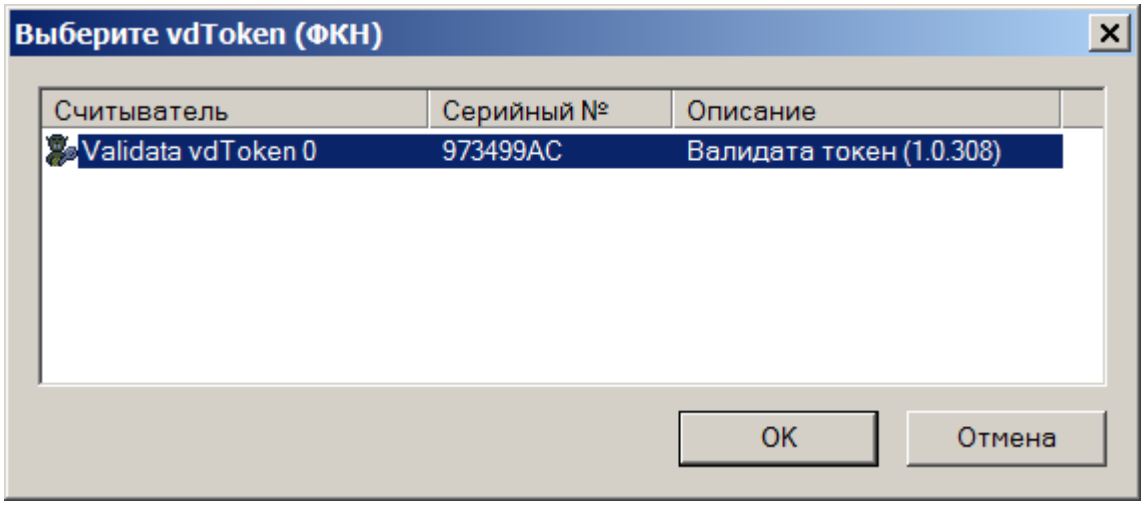

Рисунок 5 - Выбор ключевого носителя

Окно форматирования «токена» в «неизвлекаемом» режиме предлагает задать максимальный размер сертификата (в DER-кодировке), который можно будет записать на этот «токен» (Рисунок 6).

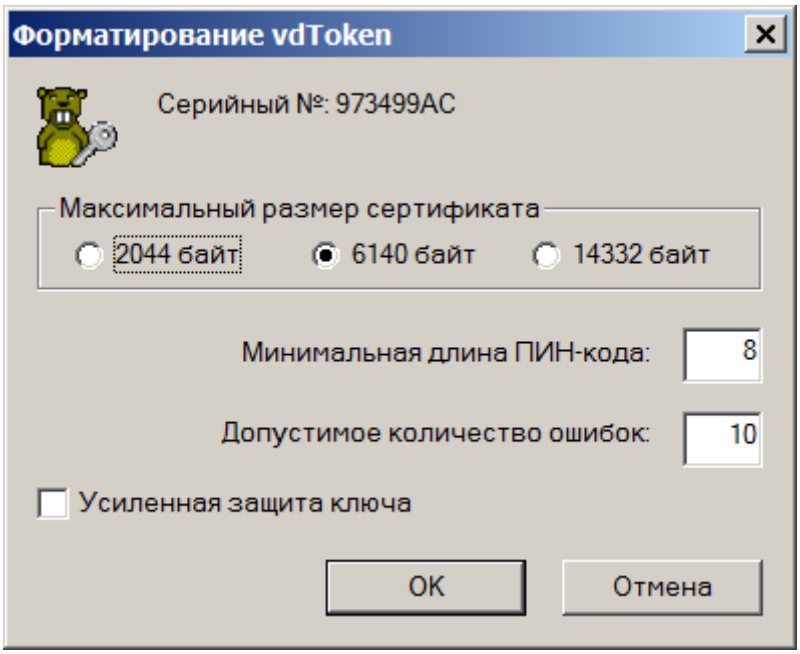

Рисунок 6 - Окно форматирования

Параметр «максимальный размер сертификата» влияет на максимальное количество ключей, поддерживаемых отформатированным 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 «токен» в USB-разъем. Данная защита нужна от возможного программного подбора ПИН-кода.

Установка опции «Усиленная защита ключа» позволяет использовать хэширование по ГОСТ Р 34.11-2012 для сжатия 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).

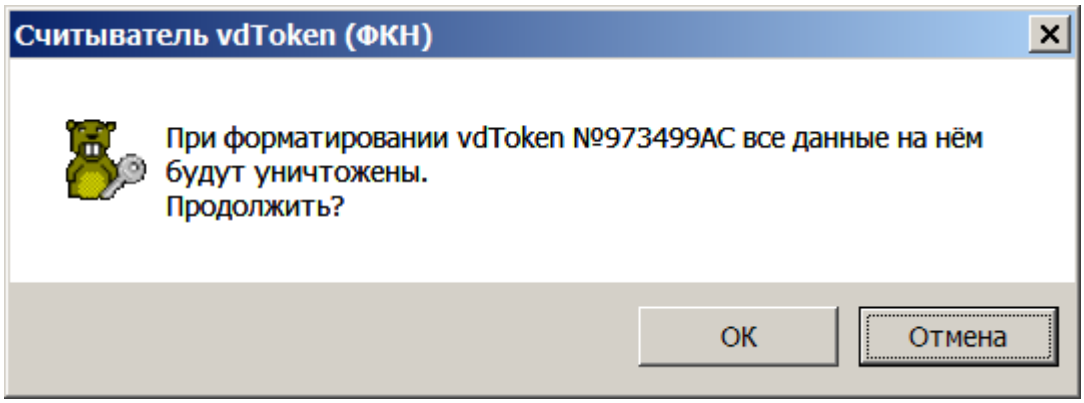

Рисунок 7 - Предупреждение перед форматированием

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

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

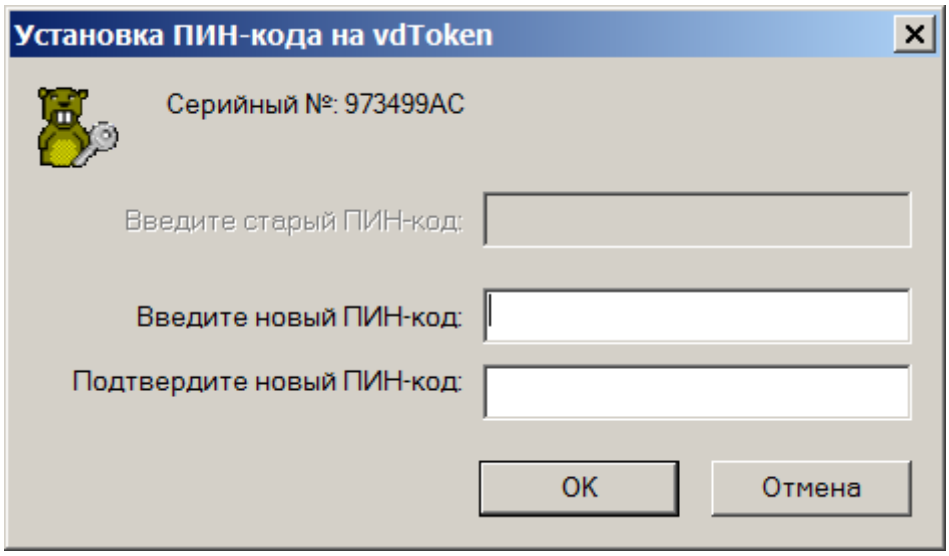

Рисунок 8 - Установка PIN-кода

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

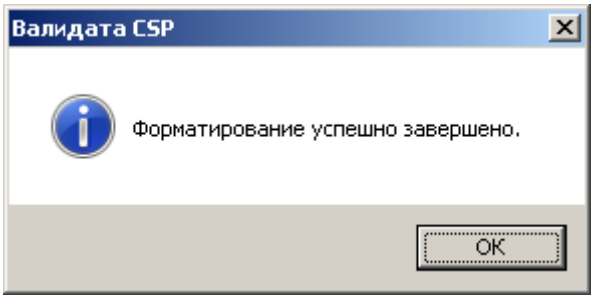

Рисунок 9 - Сообщение об успешном форматировании

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).

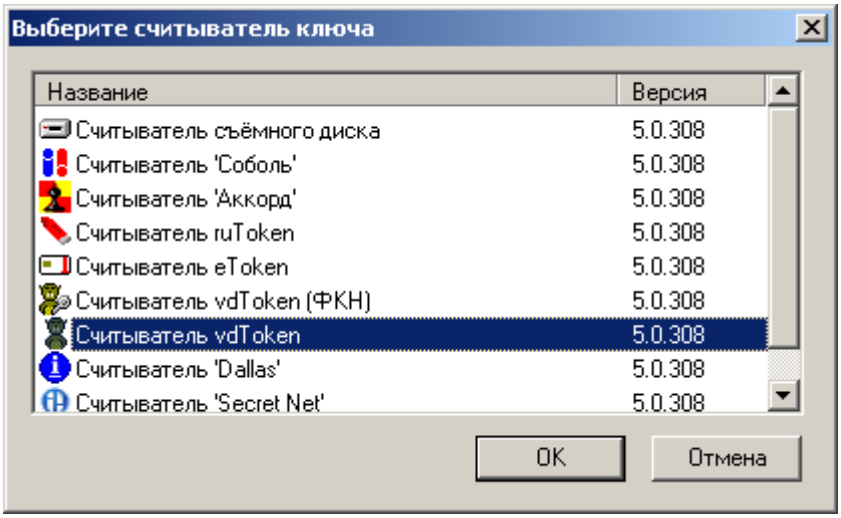

Рисунок 10 - Выбор считывателя

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

Подвигайте «мышь» или понажимайте клавиши клавиатуры. После завершения инициализации ДСЧ данное окно (Рисунок 4) закроется самостоятельно.

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

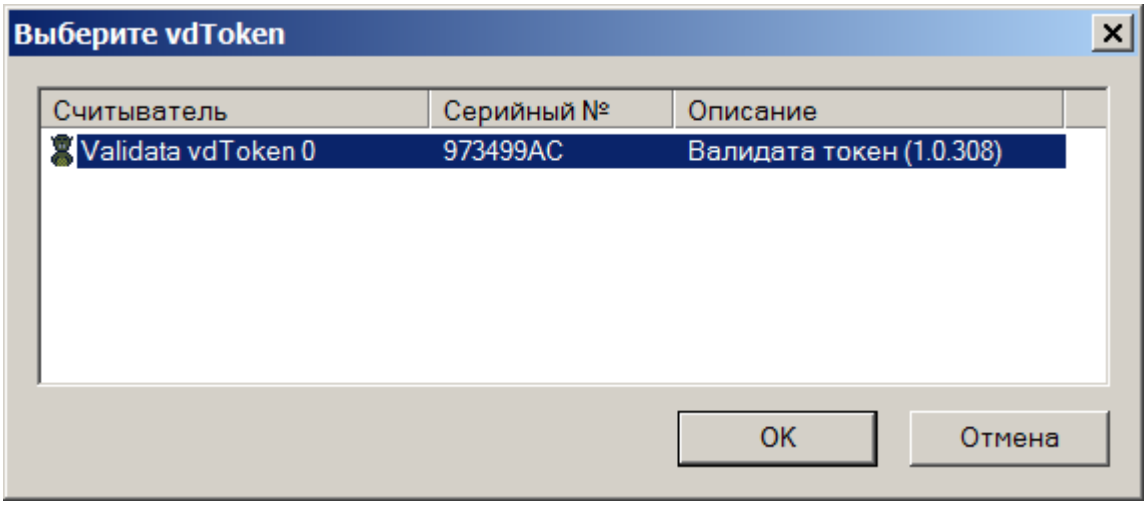

Рисунок 11 - Выбор ключевого носителя

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

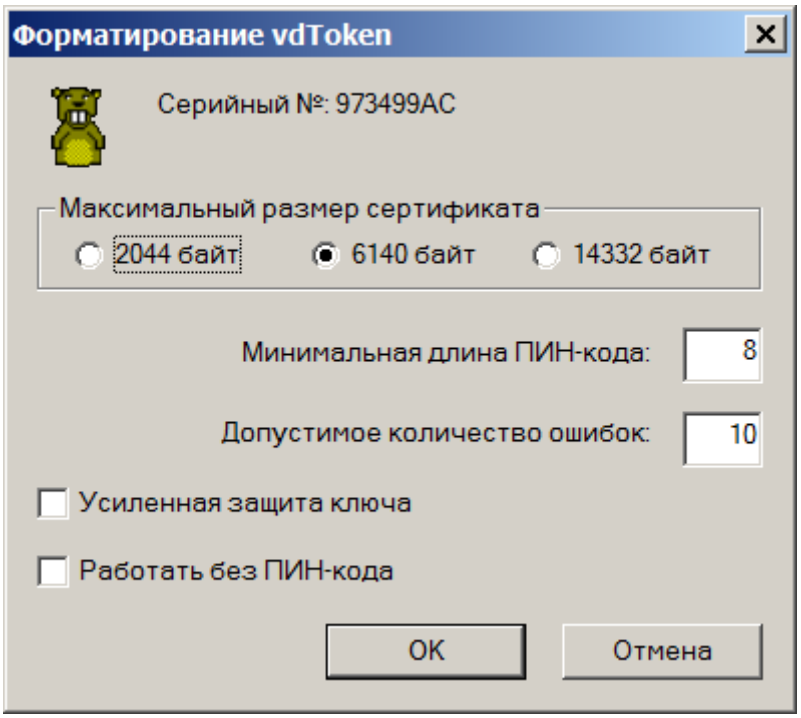

Рисунок 12 - Окно форматирования

Параметр «Максимальная длина ПИН-кода» влияет на максимальное количество ключей, поддерживаемых отформатированным 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 «токен» установить в USB-разъем. Данная защита нужна от возможного программного подбора ПИН-кода.

Установка опции «Усиленная защита ключа» позволяет использовать хэширование по ГОСТ Р 34.11-2012 для сжатия ПИН-кода.

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

Нажмите «ОК».

На экран выдается предупреждение, что при форматировании все ключевые данные (ключи и сертификаты), находящиеся на ФКН «vdToken», будут уничтожены (Рисунок 13).

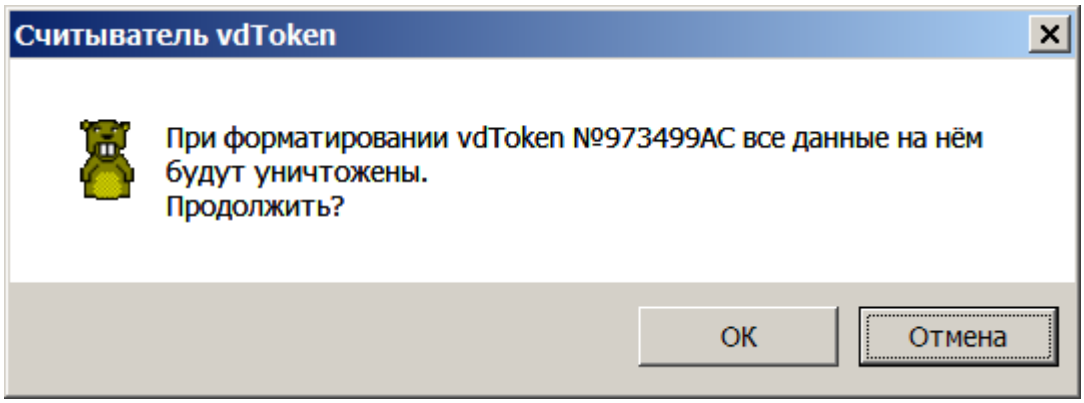

Рисунок 13 - Предупреждение перед форматированием

Если данные на «токене» уже не нужны или форматирование выполняется первый раз, то нажмите кнопку «ОК».

В появившемся окне (Рисунок 14) введите ПИН-код и его подтверждение. Нажмите «ОК».

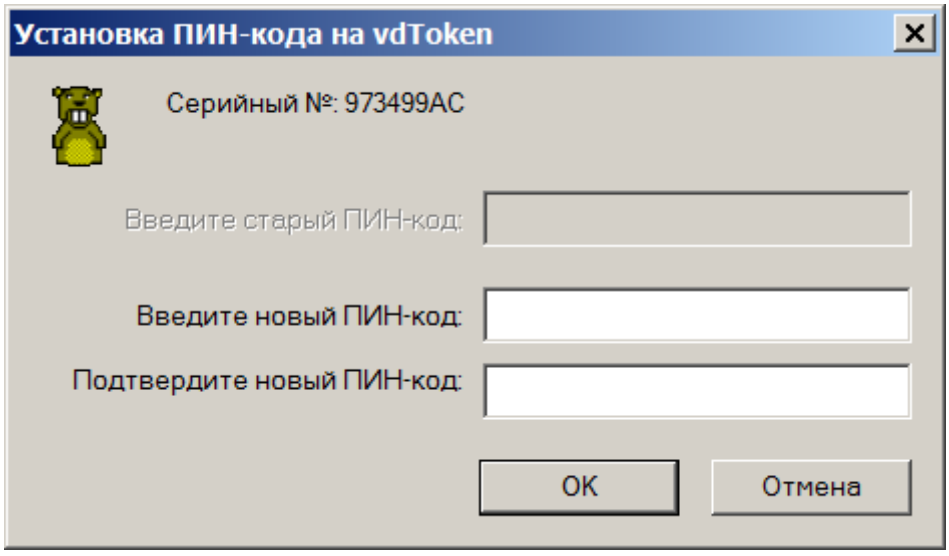

Рисунок 14 - Установка ПИН-кода

Форматирование выполнено успешно, нажмите «ОК» (Рисунок 15).

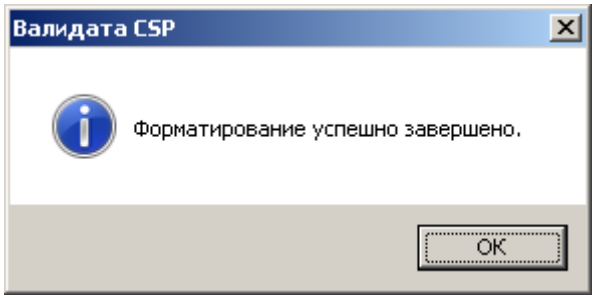

Рисунок 15 - Сообщение об успешном форматировании

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 «токену».

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

Смена ПИН-кода всегда доступна пользователю в программе конфигурации СКЗИ «Валидата CSP» версия 5.0. Для этого нужно выбрать закладку «Сервис» (Рисунок 16).

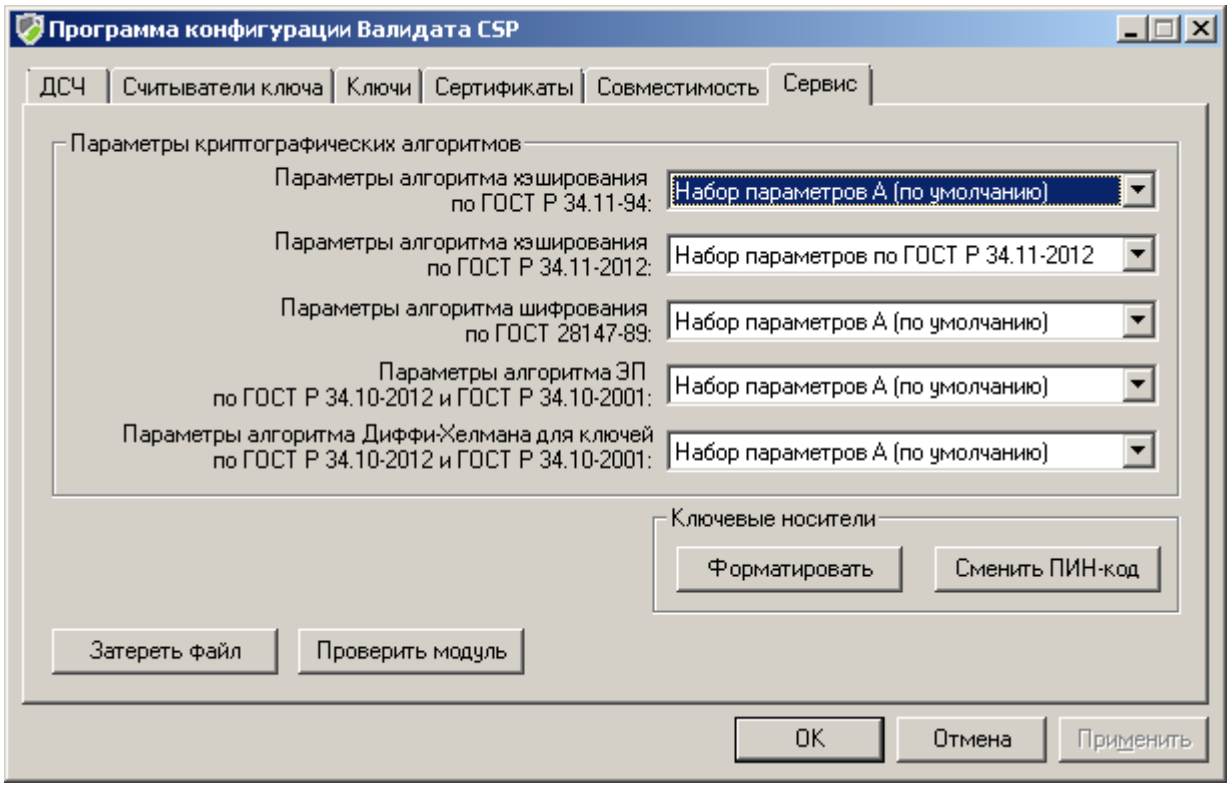

Рисунок 16 - Закладка «Сервис»

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 17).

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

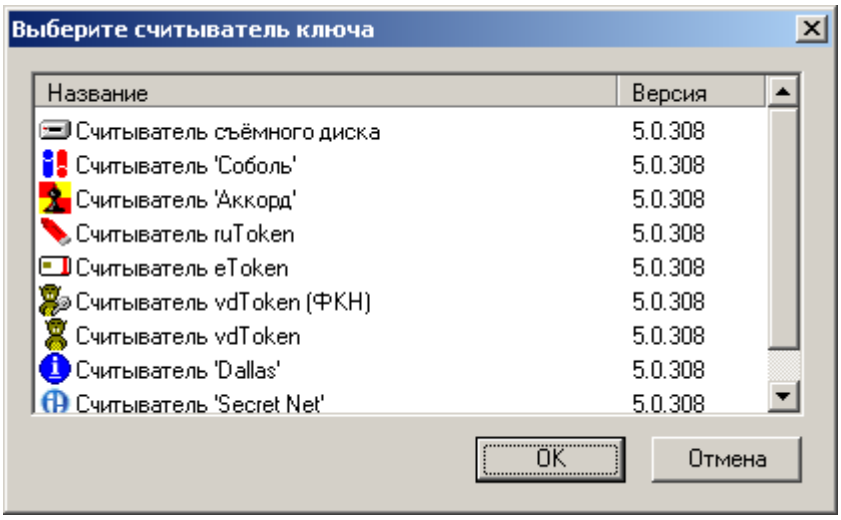

Рисунок 17 - Выбор считывателя

Установите ФКН «vdToken» в USB-разъем.

Например, выберите «неизвлекаемый» считыватель «Считыватель vdToken (ФКН)» и нажмите «ОК» (Рисунок 18).

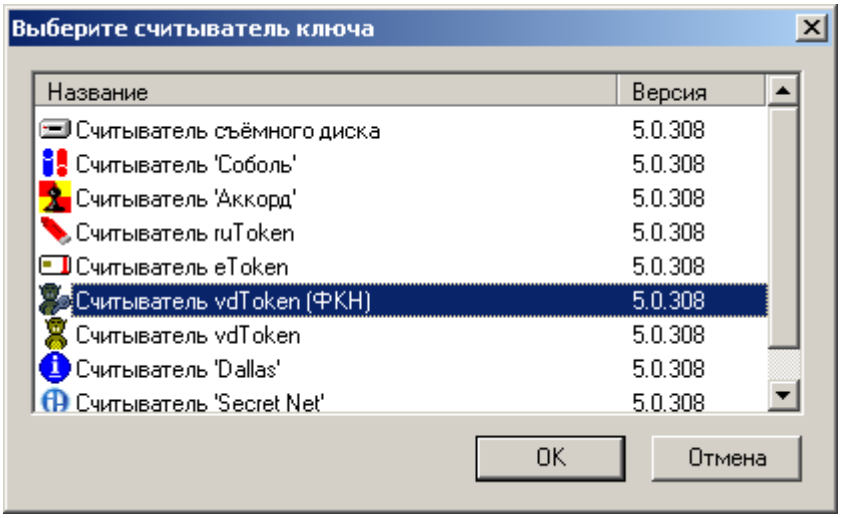

Рисунок 18 - Выбор «неизвлекаемого» считывателя

Выберите установленный «токен» и нажмите «ОК».

2.2.1 «Токены» с установленным ПИН-кодом

Если установленный «токен» был отформатирован с ПИН-кодом, то на экран будет выдано окно, приведенное ниже (Рисунок 19).

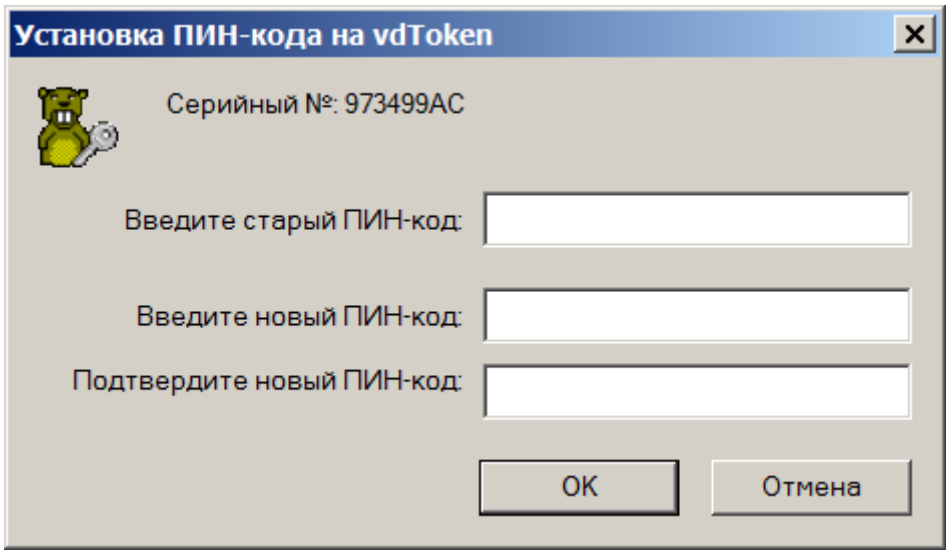

Рисунок 19 - Окно смены ПИН-кода

Для замены ПИН-кода введите в строке «Введите старый ПИН-код:» текущий ПИН-код «токена», 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 20).

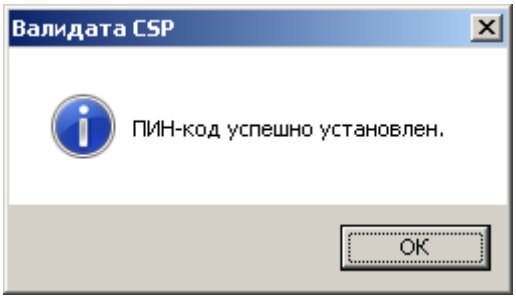

Рисунок 20 - Сообщение о замене ПИН-кода

Теперь при использовании данного «токена» нужно будет вводить новый ПИН-код. Нажмите кнопку «ОК».

2.2.2 «Токены» без ПИН-кода

Если установленный «токен» был отформатирован без установки ПИН-кода, то будет выдано на экран следующее окно (Рисунок 21).

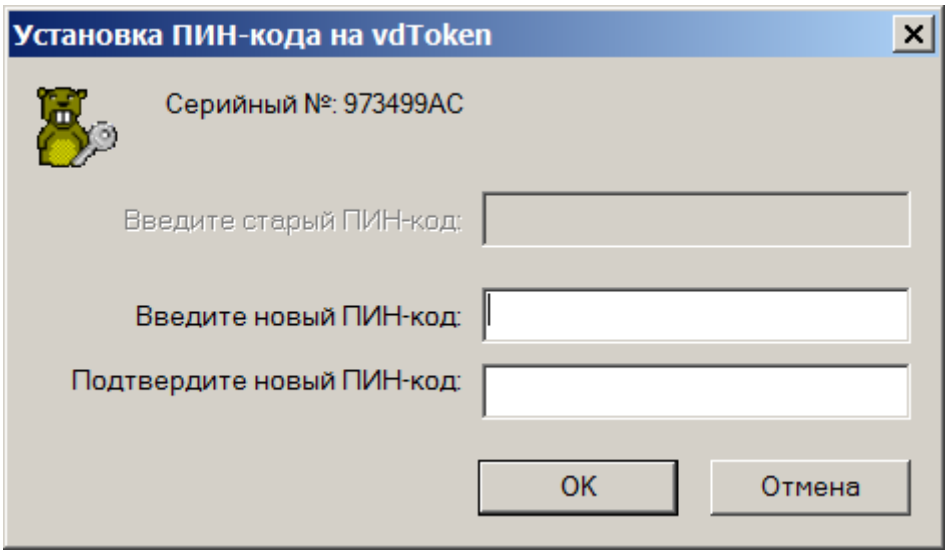

Рисунок 21 - Окно установки ПИН-кода

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

Примечание - На «токене» 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 «токен» 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 22).

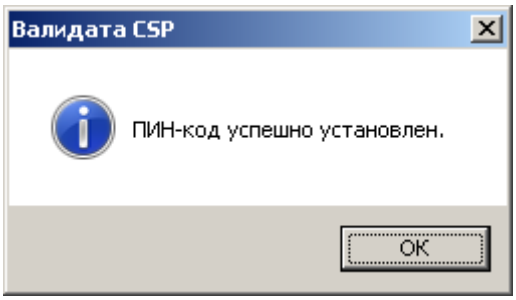

Рисунок 22 - Сообщение об установке PIN-кода

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

3 РАБОТА С КЛЮЧАМИ

3.1 Создание ключа на носителе

Ключи можно создавать только на отформатированном ФКН «vdToken».

Перед генерацией ключа на экран выдается предупреждение (Рисунок 23).

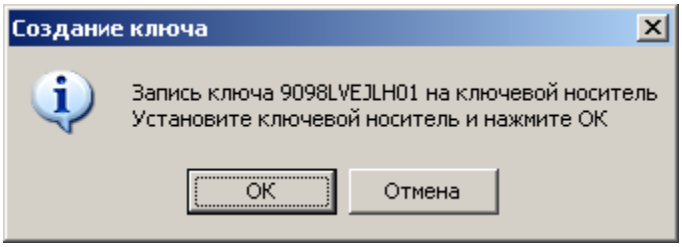

Рисунок 23 - Предупреждение при генерации ключа

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

Выберите ключевой считыватель (Рисунок 24).

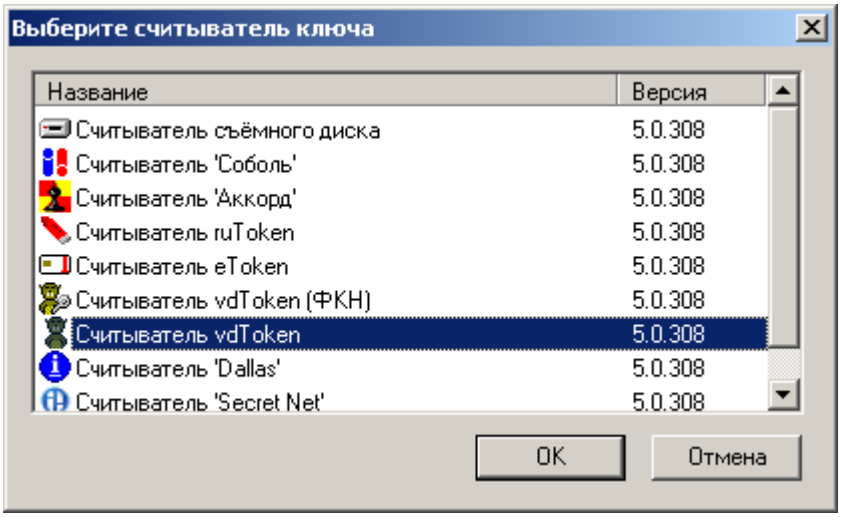

Рисунок 24 - Выбор ключевого считывателя

Если в конфигурации криптографического ядра - 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.

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 «СКАД Сигнатура» предусмотрена его защита паролем (Рисунок 25).

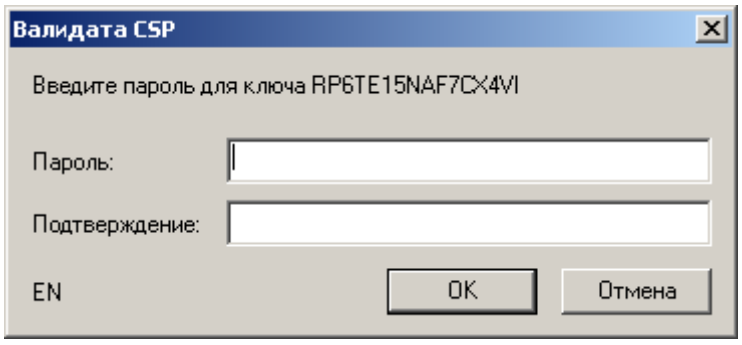

Рисунок 25 - Окно ввода ключевого пароля

Например, если пароль не ввести, а просто нажать «ОК», ключ не будет зашифрован паролем, и при работе с таким ключом запроса на ввод пароля предлагаться не будет.

Выберите «токен» и нажмите «ОК» (Рисунок 26).

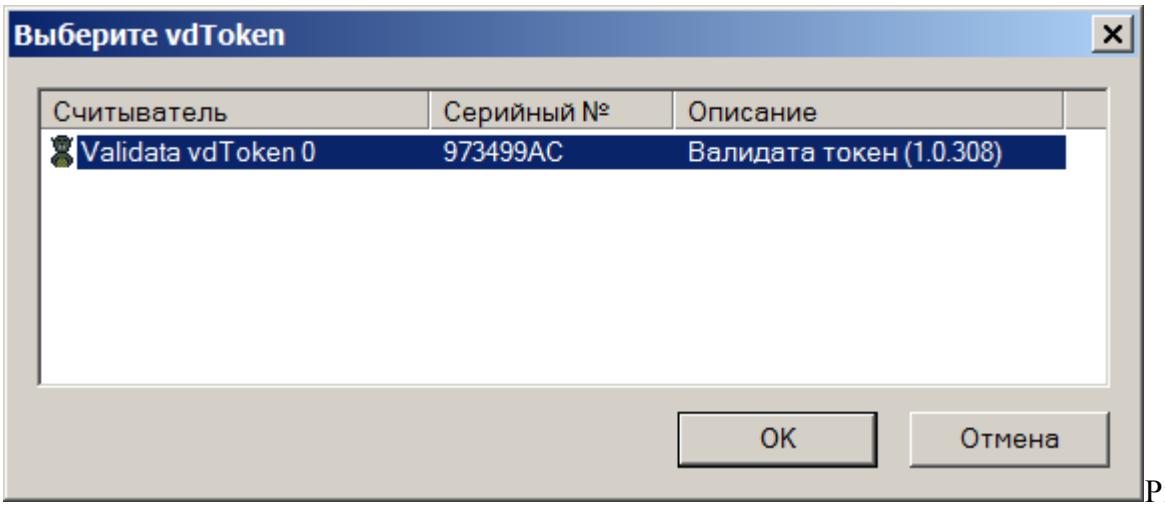

Рисунок 26 - Выбор ключевого носителя

Введите ПИН-код этого «токена» (Рисунок 27).

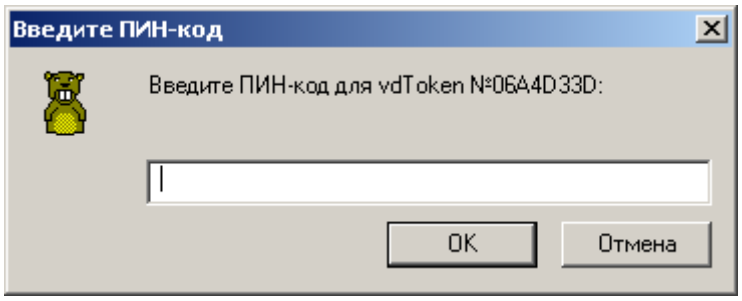

Рисунок 27 - Окно ввода ПИН-кода

Примечание - Если «токен» 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 «токен» в «извлекаемом» режиме.

3.1.2 Создание «неизвлекаемого» ключа

Выберите «неизвлекаемый» считыватель «Считыватель vdToken (ФКН)» и нажмите кнопку «ОК» (Рисунок 28).

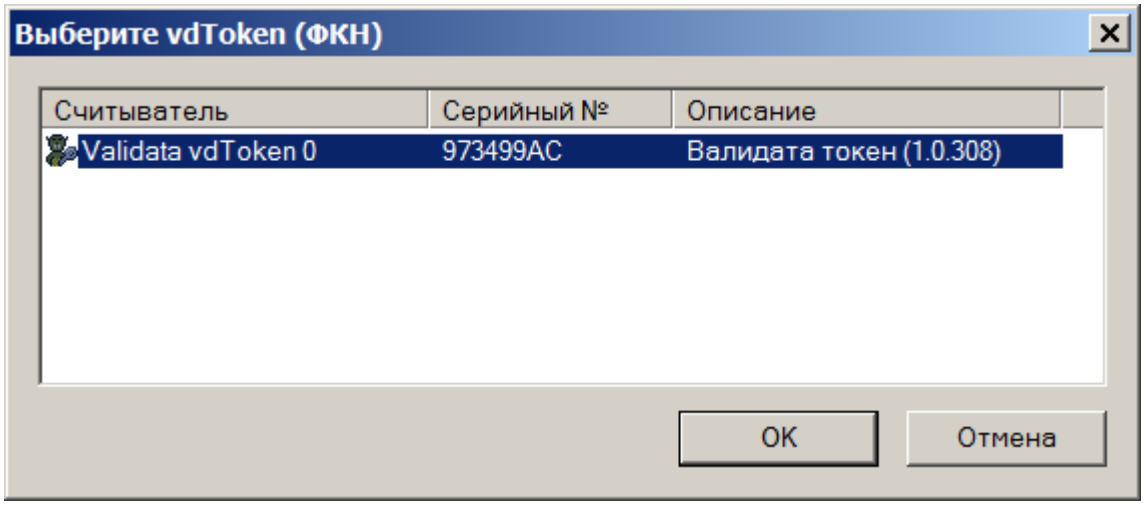

Рисунок 28 - Окно выбора носителя

Введите PIN-код этого «токена» (Рисунок 29).

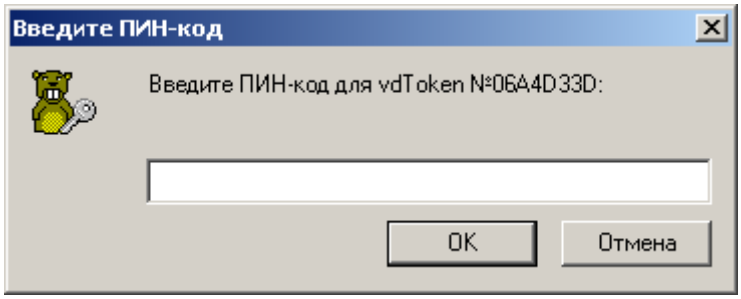

Рисунок 29 - Окно ввода PIN-кода

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

Для предоставления пользователю возможности создания резервной копии этого ключа в момент его генерации выдается диалоговое окно (Рисунок 30).

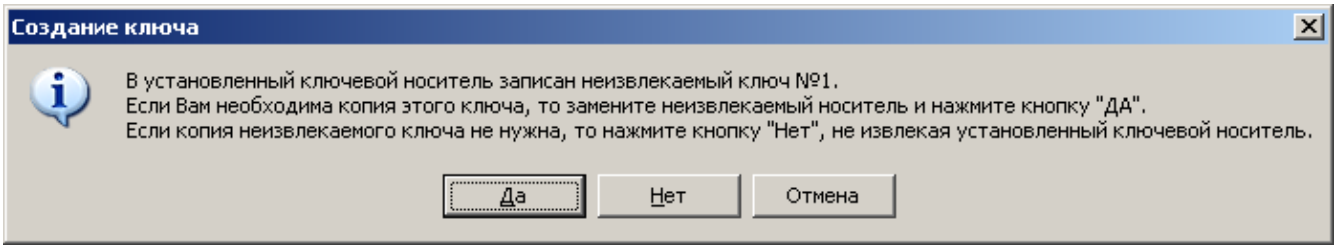

Рисунок 30 - Диалог создания резервной копии ключа

Так как ключ создан на «токене» 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 носители 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 «токен», предназначенный для резервной копии и нажмите кнопку «ОК» (Рисунок 31).

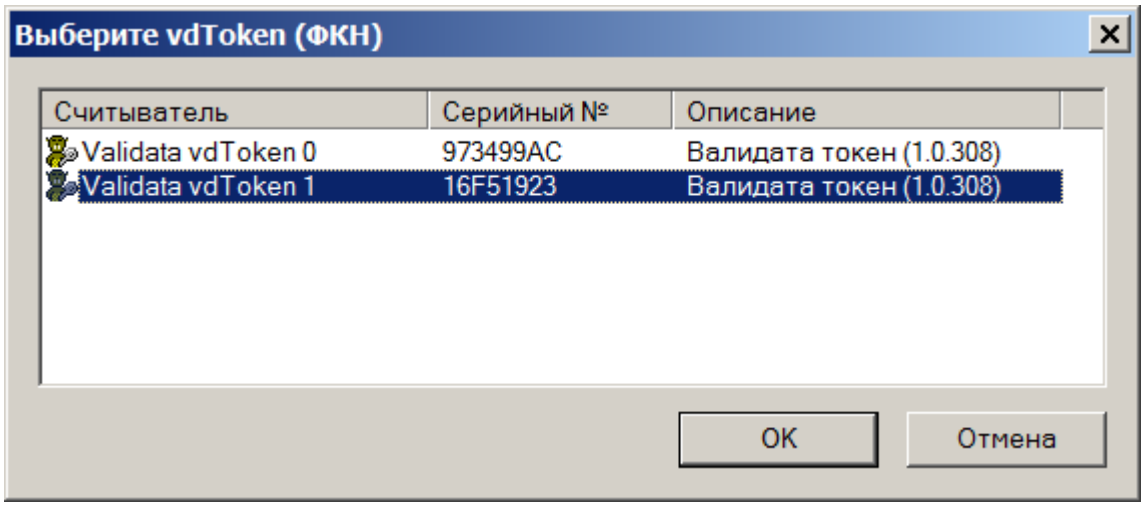

Рисунок 31 - Окно выбора резервного носителя

Введите ПИН-код этого резервного «токена» (Рисунок 32).

Если ПИН-код введен правильный, то будет выполнено создание резервной копии ключа на другом «токене» в «неизвлекаемом» режиме.

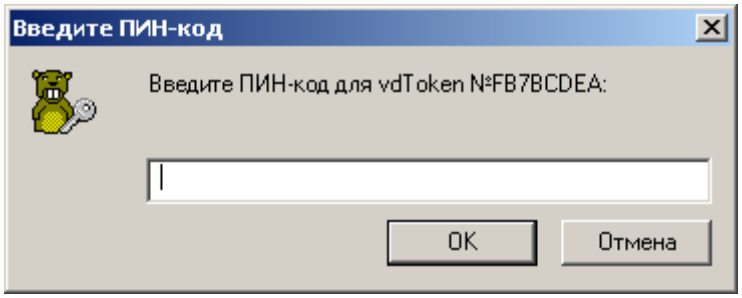

Рисунок 32 - Окно ввода ПИН-кода

Следующий диалог предлагает повторить процедуру создания резервных копий ключа на любом количестве ФКН «vdToken» (Рисунок 33).

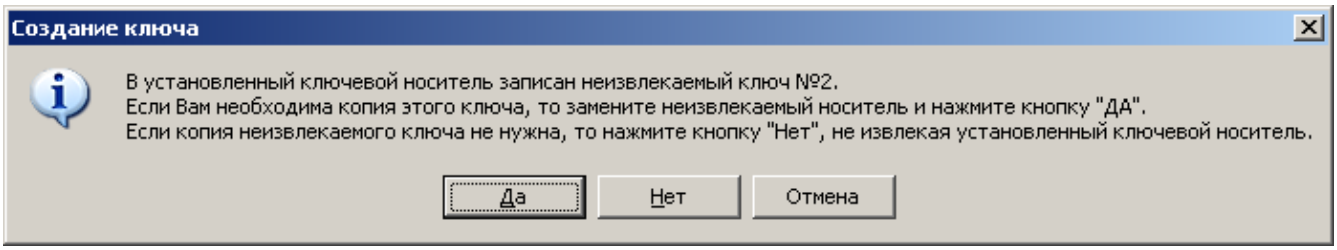

Рисунок 33 - Диалог создания резервной копии ключа

Нажмите кнопку «Нет» или «Да».

Введите ПИН-код последнего созданного «токена» (Рисунок 34).

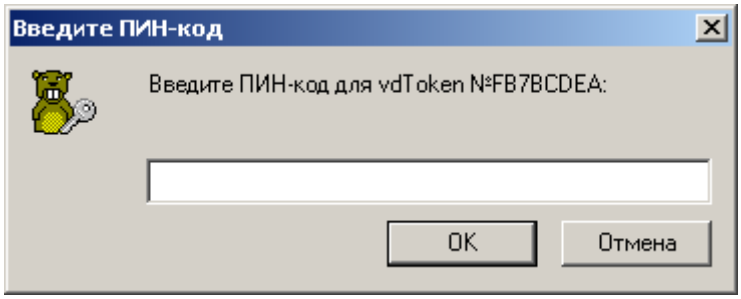

Рисунок 34 - Окно ввода ПИН-кода

Процедура генерации ключа с созданием одной резервной копии завершена.

3.2 Удаление ключа с носителя

Удаление ключа с носителя ФКН «vdToken» всегда доступно пользователю в программе конфигурации СКЗИ «Валидата CSP». Для этого выберите закладку «Ключи» (Рисунок 35).

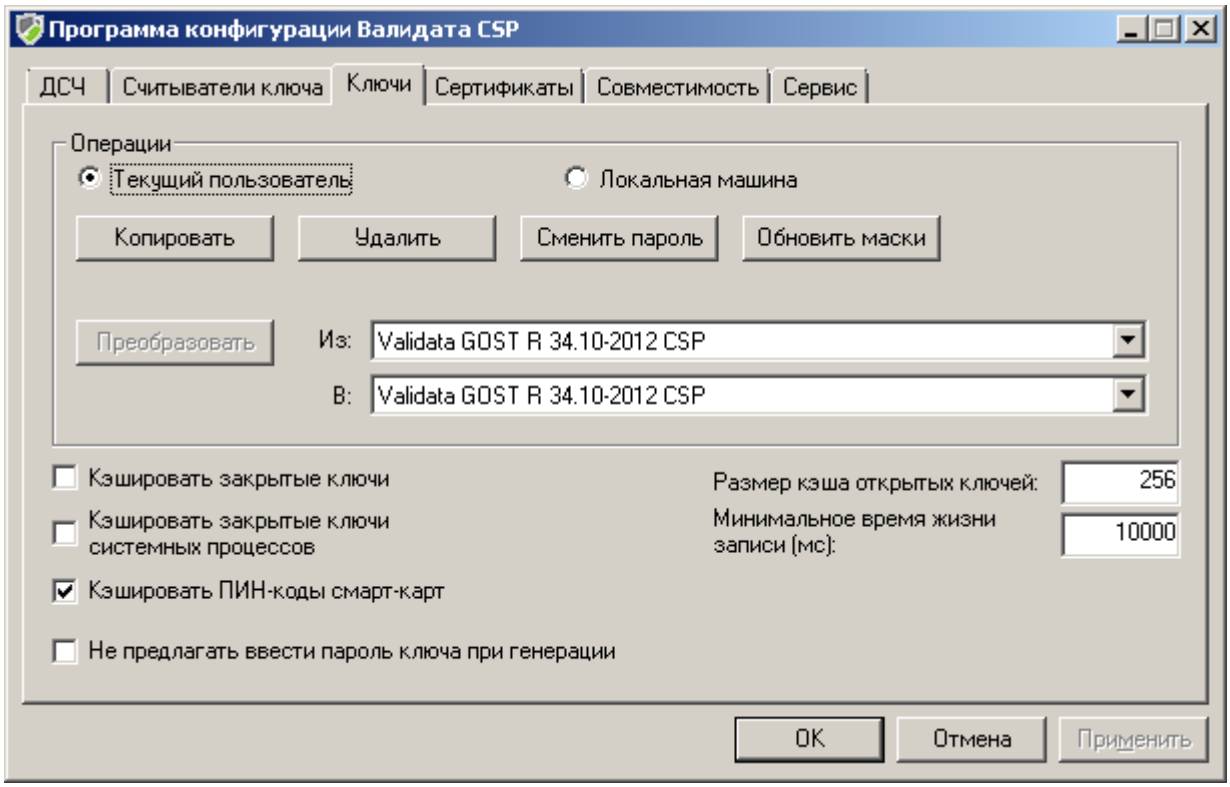

Рисунок 35 - Закладка «Ключи»

Установите ФКН «vdToken» в USB-разъем.

Нажмите кнопку «Удалить».

3.2.1 Удаление ключа с «неизвлекаемого» ключевого носителя

Выберите считыватель для «неизвлекаемых» ключей «Считыватель vdToken (ФКН)». Нажмите «ОК».

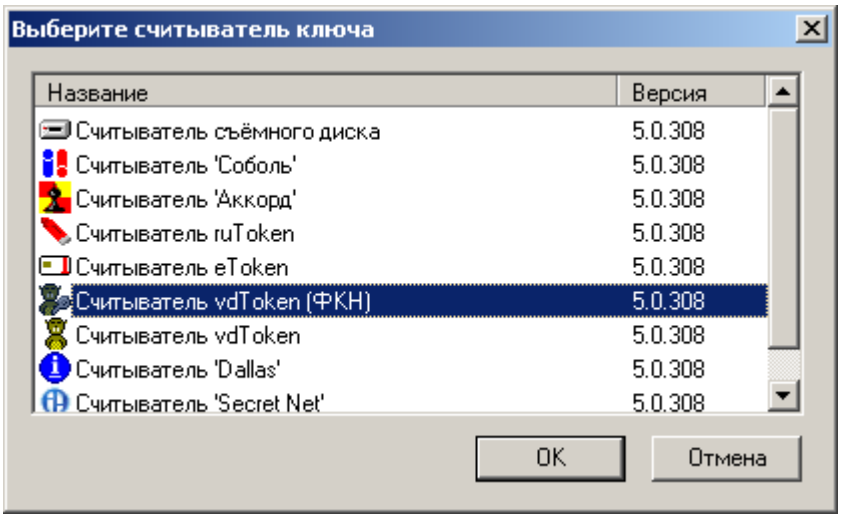

Рисунок 36 - Выбор ключевого считывателя

Выберите «токен», с которого необходимо удалить ключ и нажмите «ОК» (Рисунок 37).

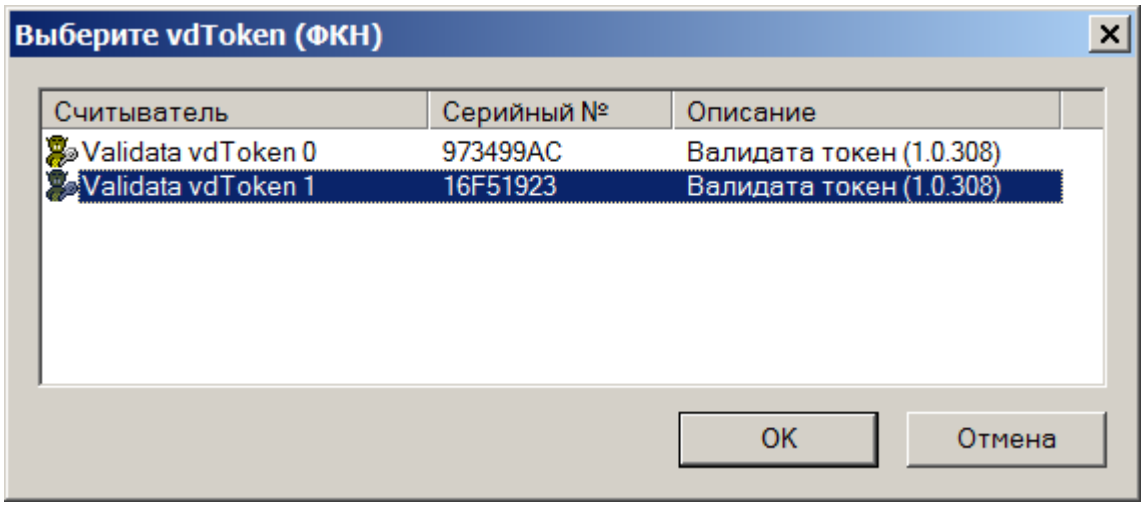

Рисунок 37 - Окно выбора носителя

На экран выдается окно со списком номеров ключей, которые находятся на выбранном носителе (Рисунок 38).

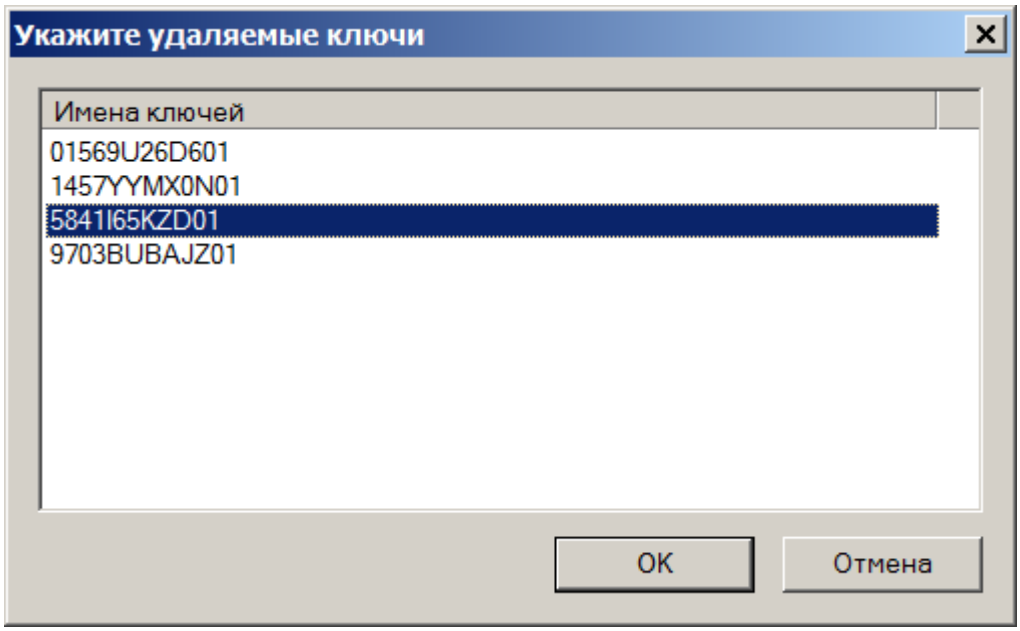

Рисунок 38 - Окно выбора ключей для удаления

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 кнопки «Ctrl» или «Shift».

Выберем один номер ключа и нажмем «ОК».

Сообщение с предупреждением потребует выполнить дополнительное нажатие кнопки «ОК» (Рисунок 39).

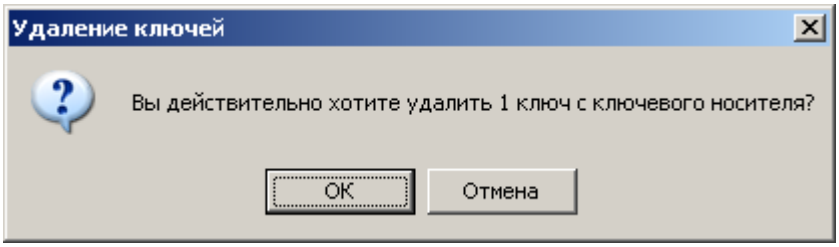

Рисунок 39 - Предупреждение об удалении ключей

Введите ПИН-код для доступа к функции удаления на «токене» (Рисунок 40).

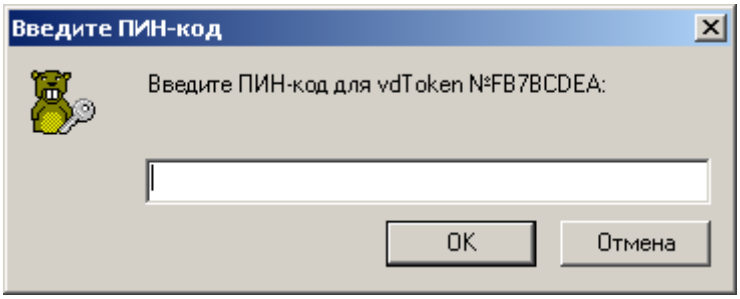

Рисунок 40 - Окно ввода ПИН-кода

Ключ удален из «токена». Нажмите «ОК» (Рисунок 41).

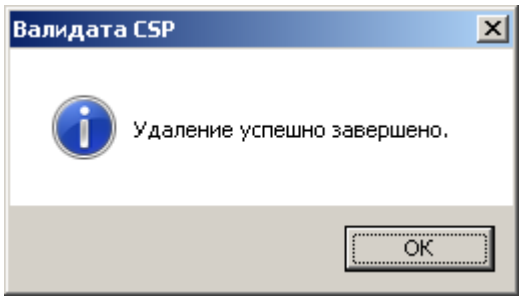

Рисунок 41 – Сообщение об удалении ключа

3.2.2 Удаление ключа с «извлекаемого» ключевого носителя

Выберите считыватель для «извлекаемых» ключей «Считыватель vdToken». Нажмите «ОК» (Рисунок 42).

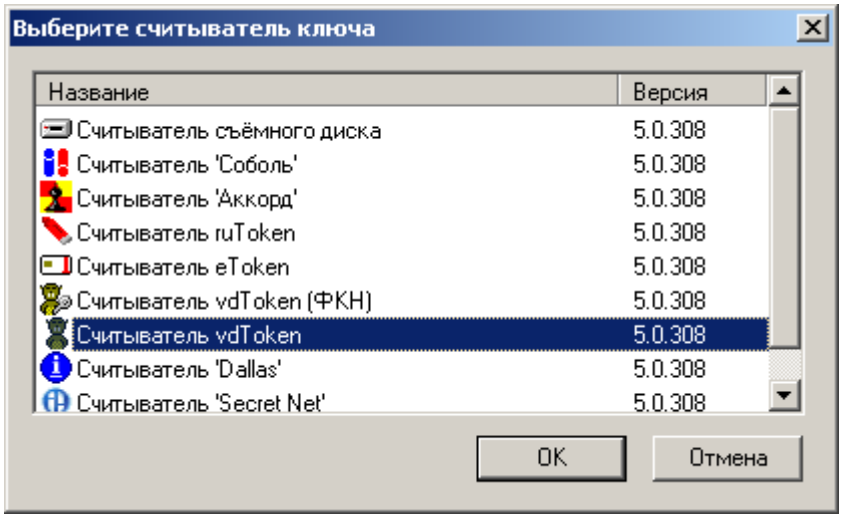

Рисунок 42 - Выбор ключевого считывателя

Выберите «токен», с которого необходимо удалить ключ, и нажмите «ОК».

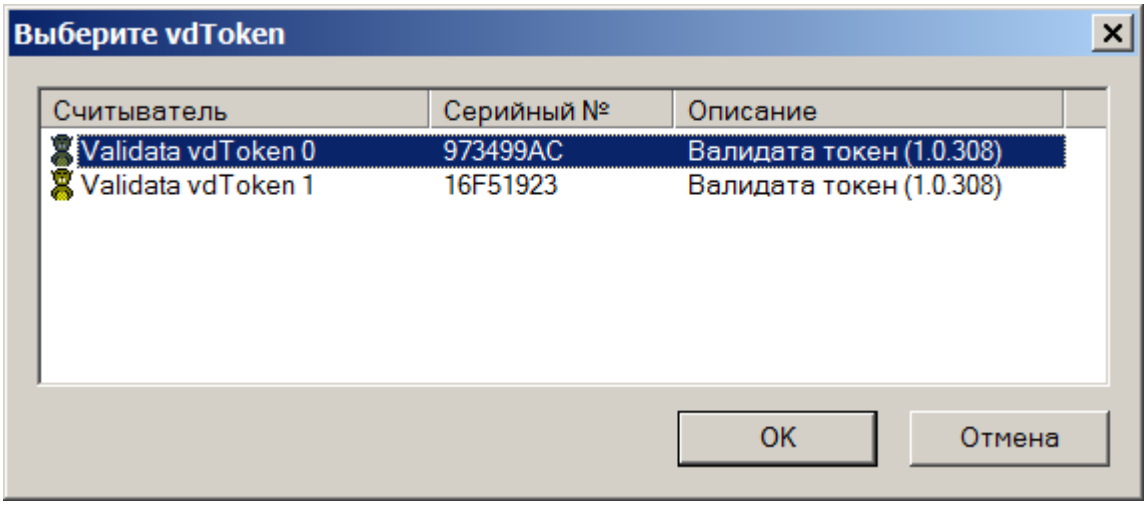

Рисунок 43 - Окно выбора носителя

На экран выдается окно со списком номеров ключей, которые находятся на выбранном носителе (Рисунок 44).

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 кнопки «Ctrl» или «Shift».

Выберите один номер ключа и нажмите «ОК».

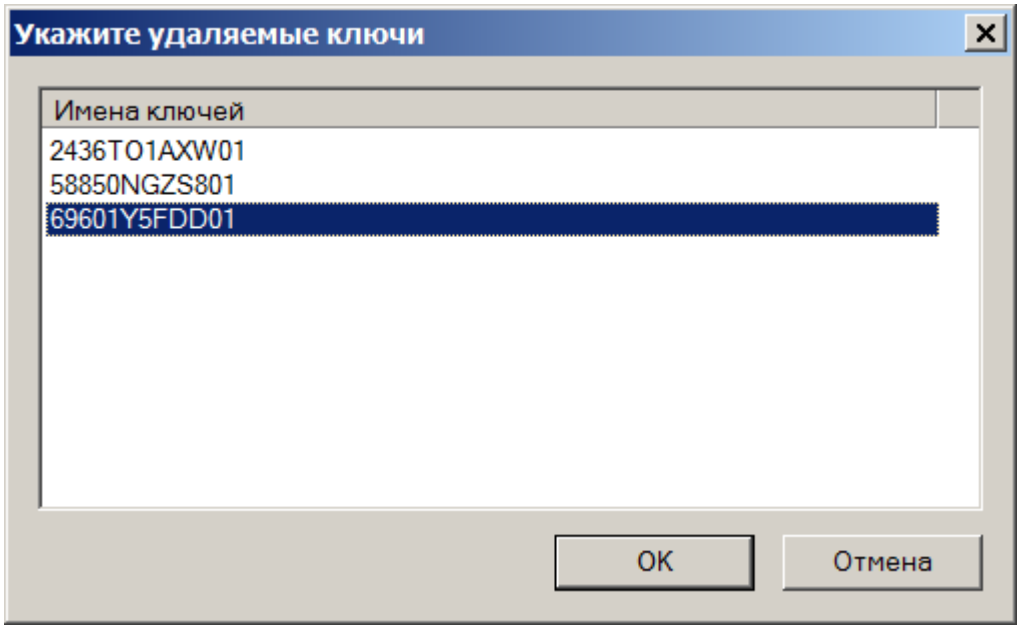

Рисунок 44 - Окно выбора ключей для удаления

Сообщение с предупреждением потребует выполнить дополнительное нажатие кнопки «ОК» (Рисунок 45).

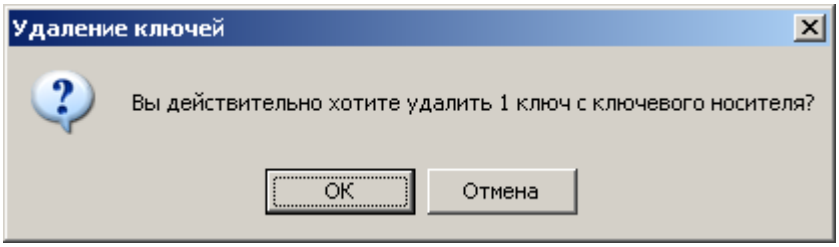

Рисунок 45 - Предупреждение об удалении ключей

Введите ПИН-код для доступа к функции удаления на «токене» (Рисунок 46).

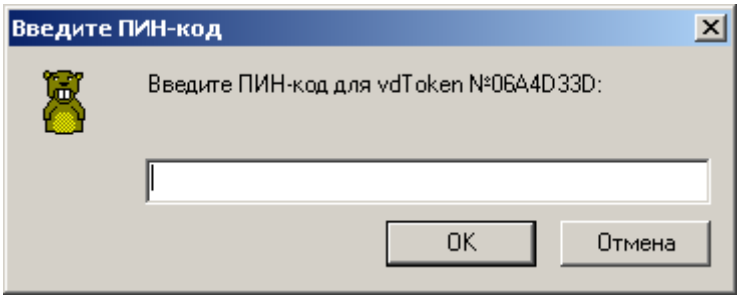

Рисунок 46 - Окно ввода ПИН-кода

Примечание - Если «токен» был отформатирован без ПИН-кода, то окно ввода ПИН-кода на экран выдаваться не будет.

Ключ удален из «токена». Нажмите «ОК» (Рисунок 47).

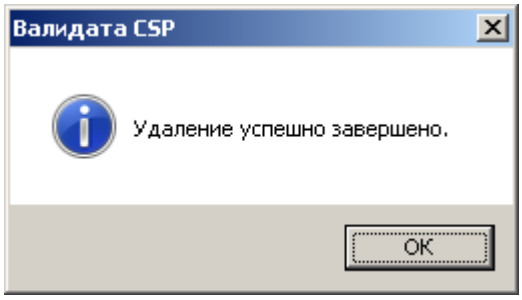

Рисунок 47 - Сообщение об удалении ключа

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 48).

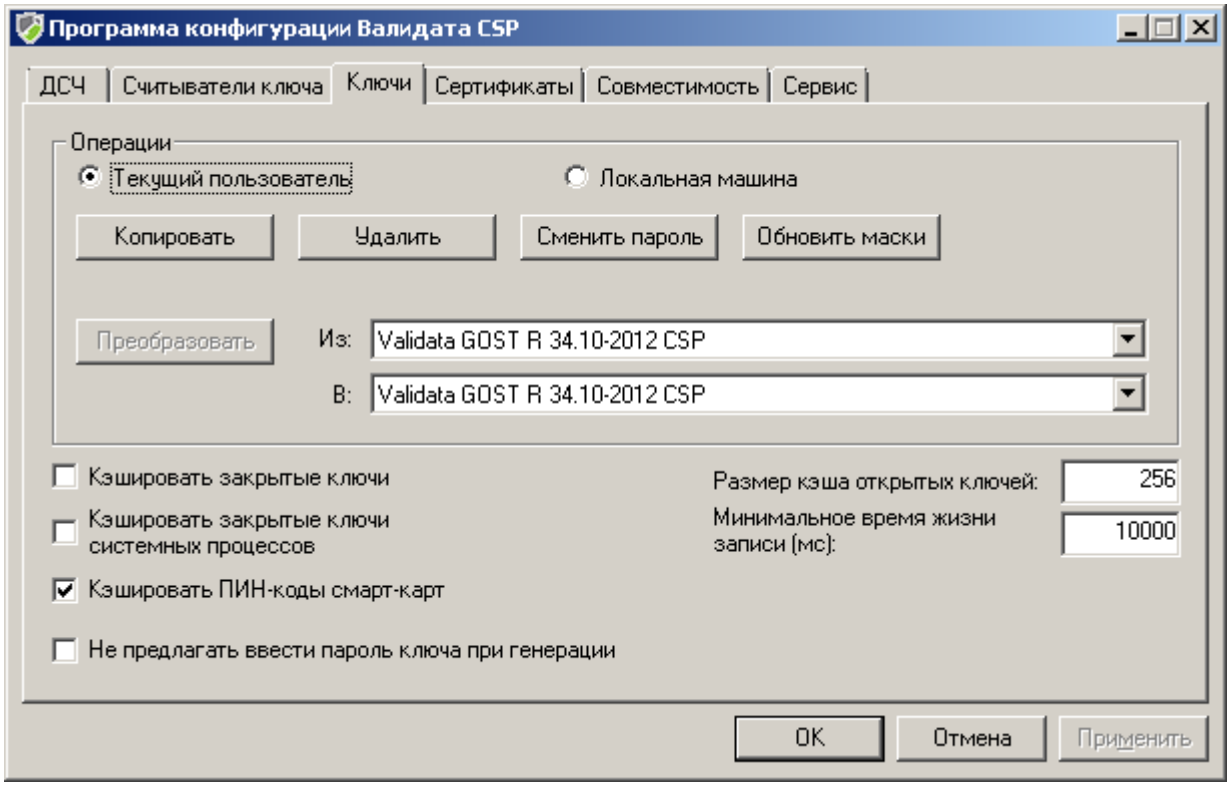

Рисунок 48 - Закладка «Ключи»

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.

Попробуем это проверить.

Установите ФКН «vdToken», на котором есть «неизвлекаемые» ключи, в USB-разъем.

Нажмите кнопку «Копировать» (Рисунок 48).

Выберите считыватель для «неизвлекаемых» ключей - «Считыватель vdToken (ФКН)». Нажмите «ОК» (Рисунок 49).

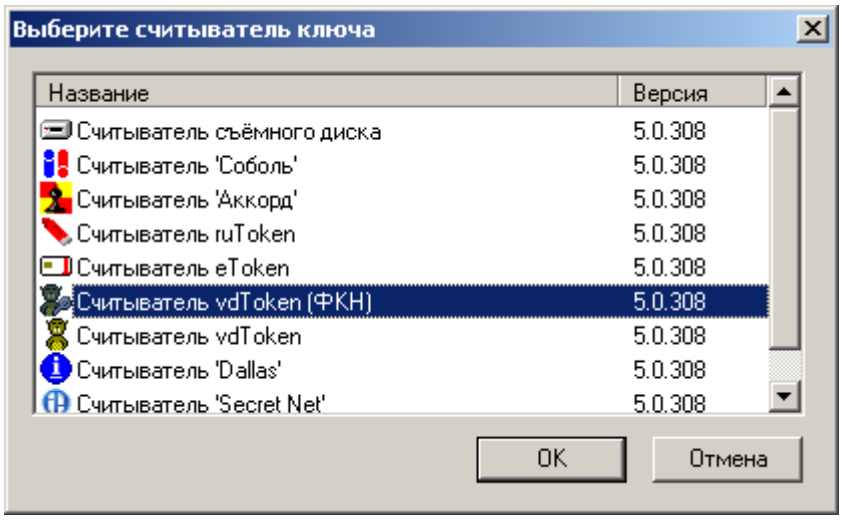

Рисунок 49 - Выбор ключевого считывателя

Приведенное ниже сообщение предупреждает, что копировать ключ с «неизвлекаемого» носителя невозможно (Рисунок 50).

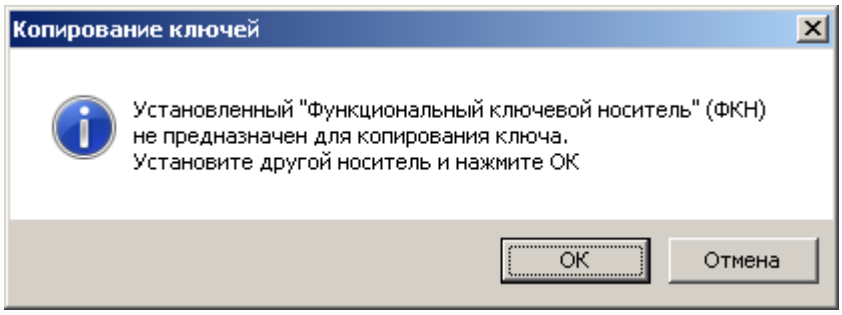

Рисунок 50 - Сообщение о невозможности копировании ключа

Если попробовать скопировать ключ, например, с дискеты на «неизвлекаемый» носитель, то на экран будет выдано предупреждение о том, что это недопустимая операция ФКН «vdToken» (Рисунок 51).

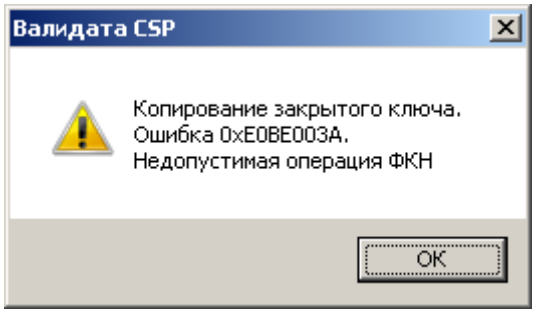

Рисунок 51 - Предупреждение при попытке копирования ключа

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 «дискеты» на «извлекаемый» носитель ФКН «vdToken».

Установите «дискету» с ключом в дисковод компьютера и нажмите кнопку «Копировать» (Рисунок 48).

Выберите считыватель съемного диска, как это показано на рисунке (Рисунок 52). Нажмите кнопку «ОК».

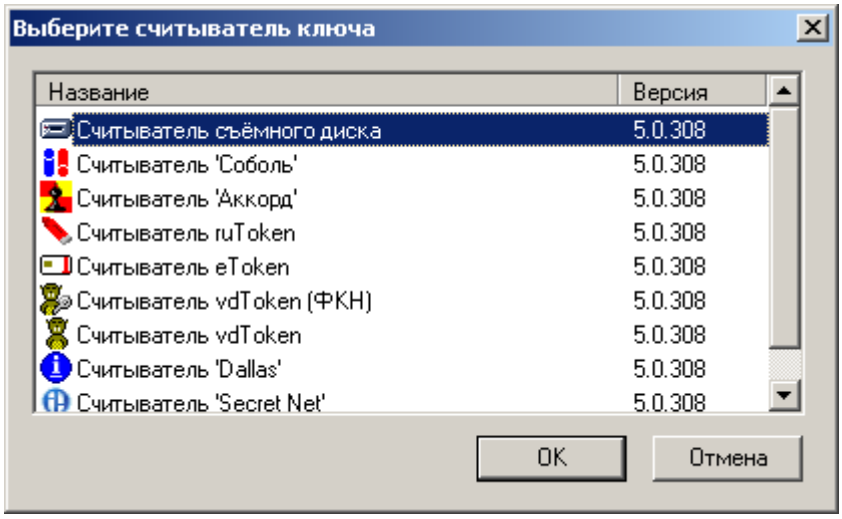

Рисунок 52 - Выбор ключевого считывателя

Укажите дисковод «A:» и нажмите «ОК» (Рисунок 53).

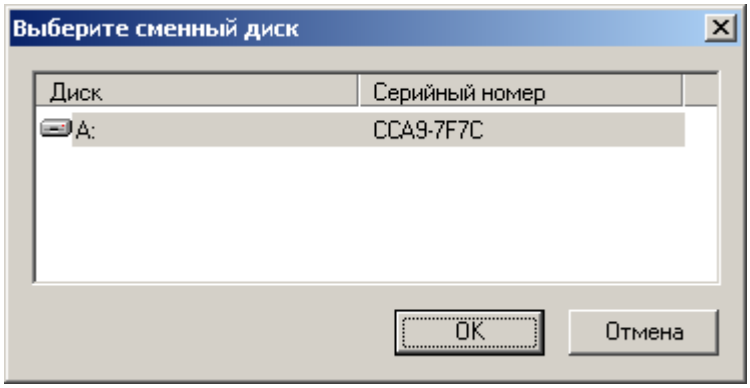

Рисунок 53 - Выбор сменного диска

Выберите из списка номер ключа, который нужно скопировать, и нажмите «ОК» (Рисунок 54).

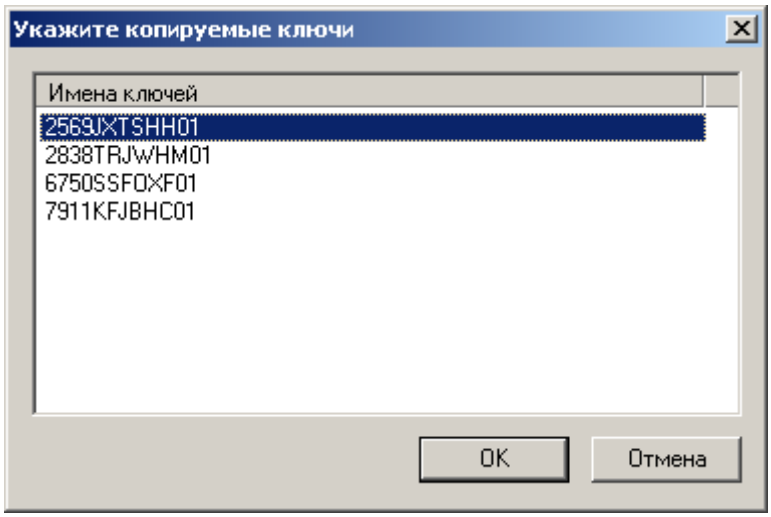

Рисунок 54 - Выбор ключа

Удалите ключевую дискету и установите ФКН «vdToken» в USB разъем. Нажмите кнопку «ОК» (Рисунок 55).

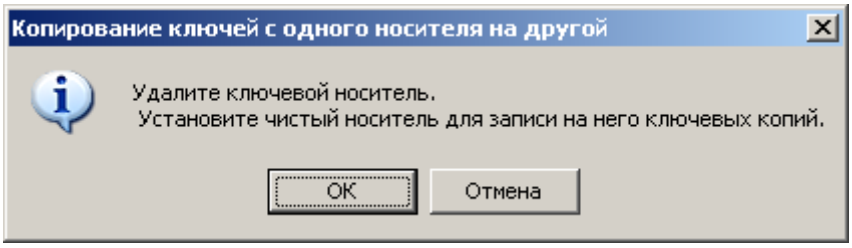

Рисунок 55 - Предупреждение процедуры копирования ключа

Выберите считыватель для «извлекаемых» ключей «Считыватель vdToken». Нажмите «ОК» (Рисунок 56).

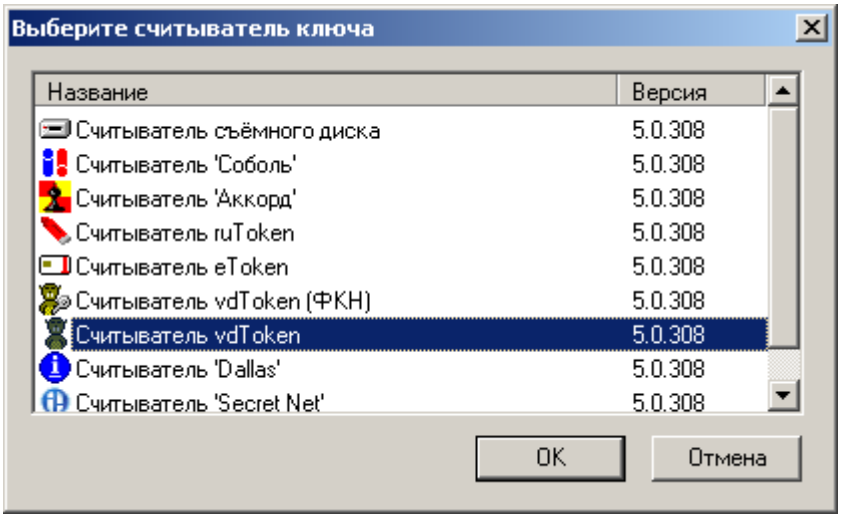

Рисунок 56 - Выбор ключевого считывателя

Выберите «токен», с которого нужно скопировать ключ, и нажмите «ОК» (Рисунок 57).

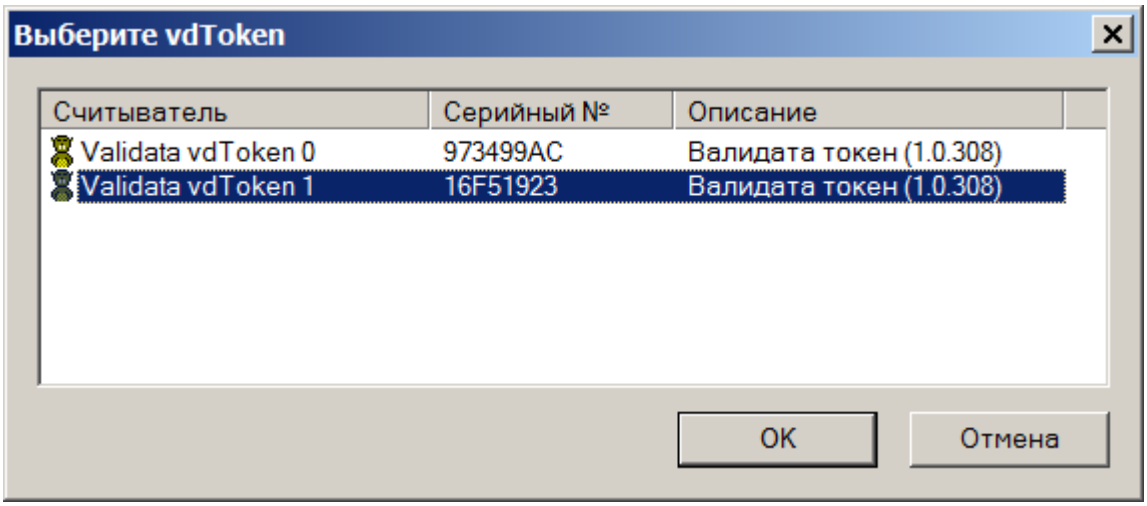

Рисунок 57 - Окно выбора носителя

Введите ПИН-код для доступа к установленному «токену» (Рисунок 58).

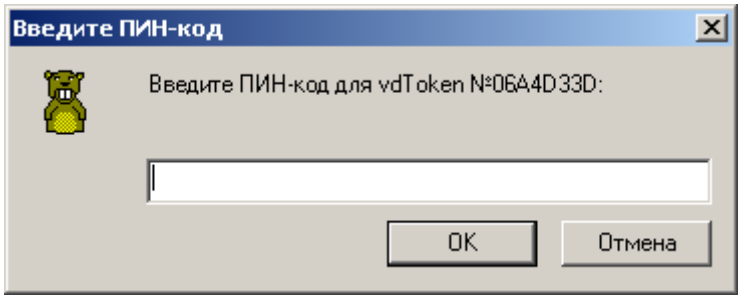

Рисунок 58 - Окно ввода РПИН-кода

Примечание - Если «токен» был отформатирован без ПИН-кода, то окно ввода ПИН-кода на экран выдаваться не будет.

Процедура копирования ключа на «извлекаемый» носитель завершена (Рисунок 59).

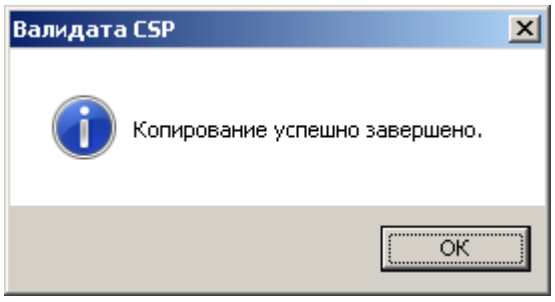

Рисунок 59 - Сообщение об успешном завершении копирования

4 ИСПОЛЬЗОВАНИЕ «ТОКЕНА»

Продемонстрируем работу с ключами на ФКН «vdToken» на примере системы Специализированный архиватор электронных сообщений (САЭС).

Например, выполним архивацию файлов на «неизвлекаемом» ключе, а разархивируем эти фалы на «извлекаемом» ключе.

4.1 Архивация на «неизвлекаемом» ключе

Откройте «Проводник».

Установите ФКН «vdToken» с «неизвлекаемым» ключом в USB-разъем.

Выделите 9 файлов (Рисунок 60).

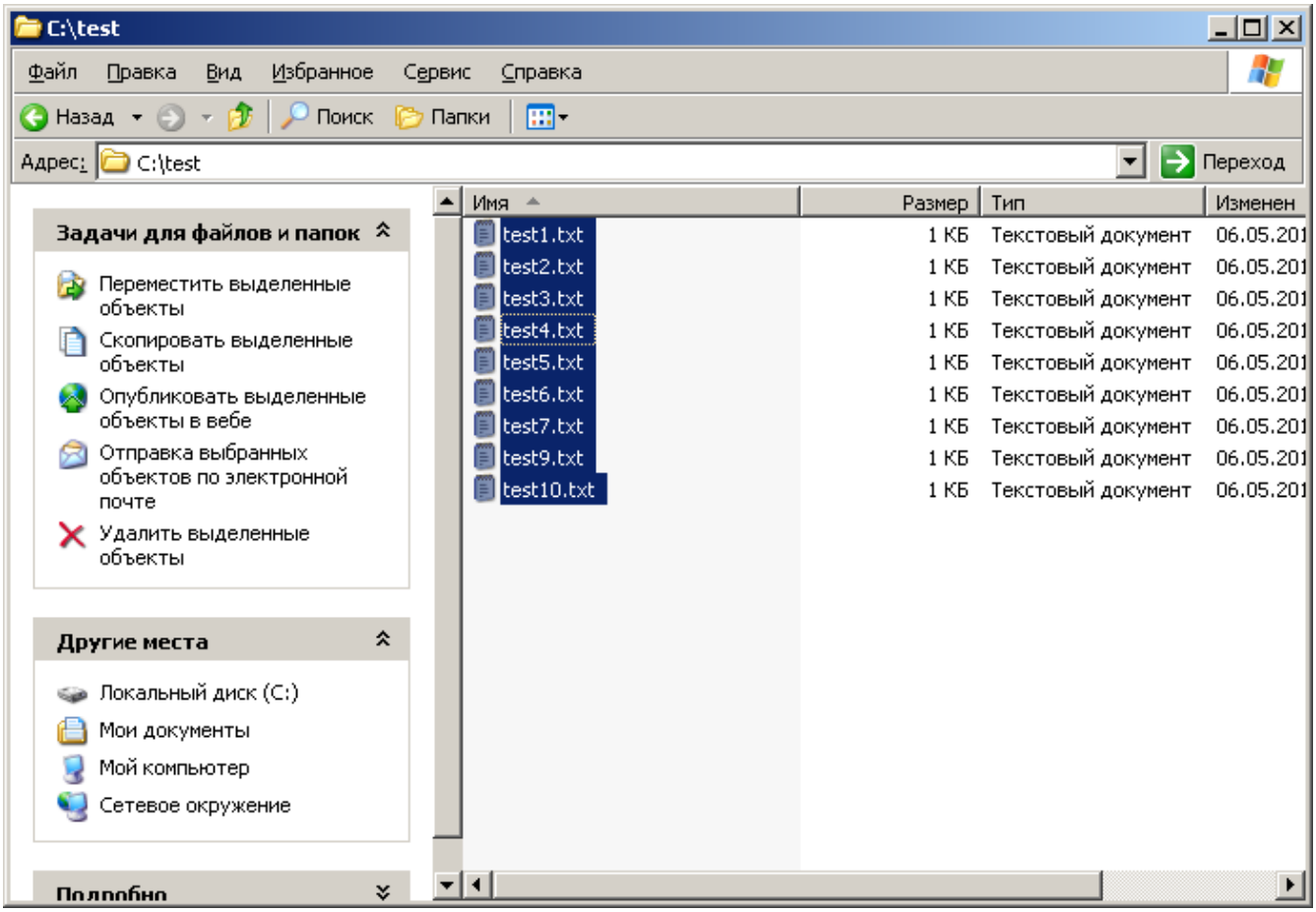

Рисунок 60 - Окно «Проводника»

Нажмите правой кнопкой «мыши» на выделенных файлах, и выполните пункт меню: «САЭС» -> «Архивировать».

На экран будет выдано предупреждение. Нажмите кнопку «Да» (Рисунок 61).

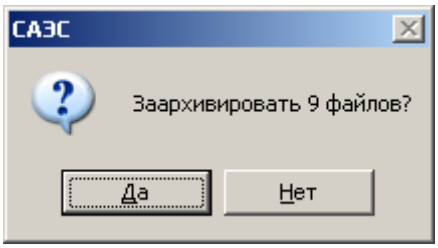

Рисунок 61 - Окно предупреждения

Выберите профиль пользователя, который использует «неизвлекаемый» ключ на носителе ФКН «vdToken». Нажмите «ОК» (Рисунок 62).

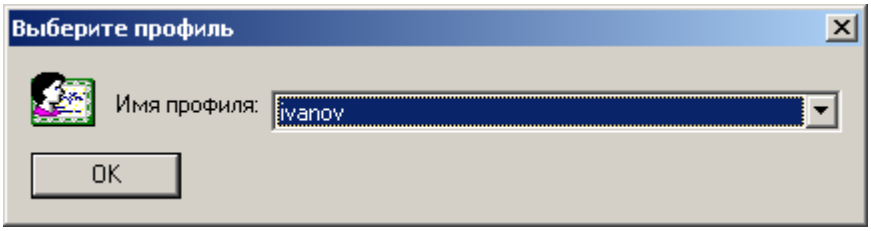

Рисунок 62 - Выбор профиля

Выберите «неизвлекаемый» считыватель «Считыватель vdToken (ФКН)». Нажмите «ОК» (Рисунок 63).

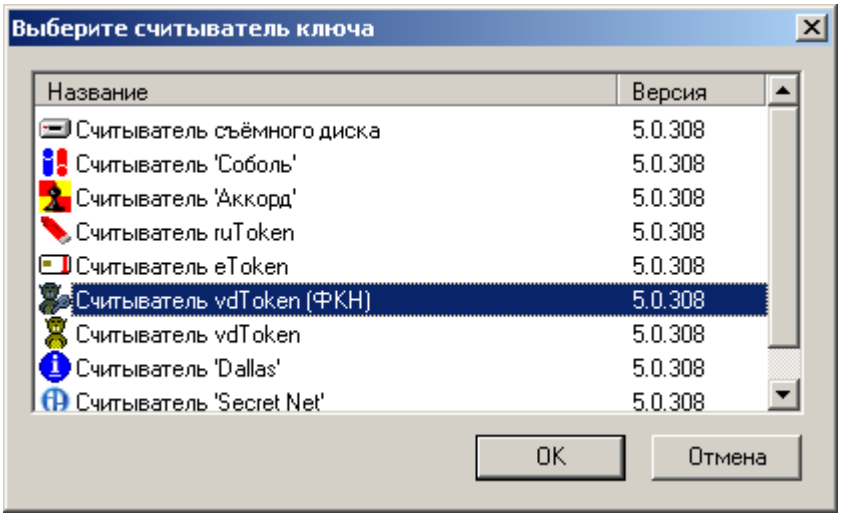

Рисунок 63 - Выбор ключевого считывателя

Введите правильный ПИН-код установленного «токена». Нажмите «ОК» (Рисунок 64).

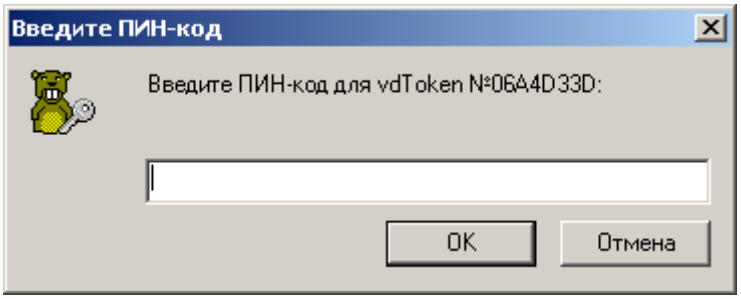

Рисунок 64 - Окно ввода ПИН-кода

Укажите двух получателей. Нажмите кнопку «Архивировать» (Рисунок 65).

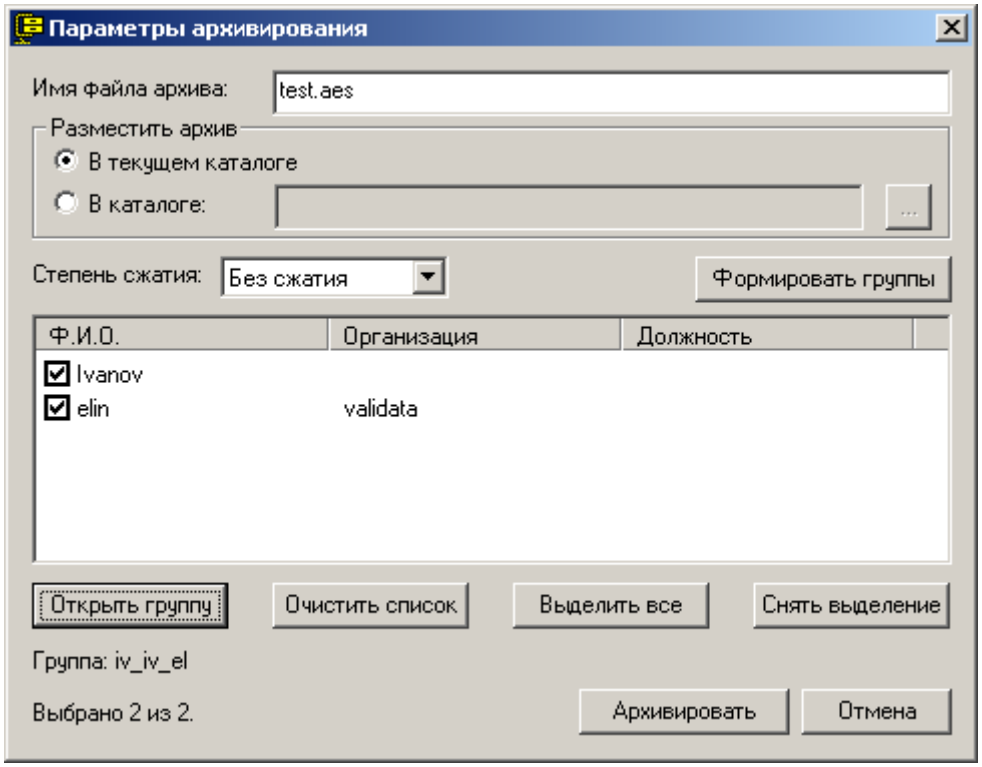

Рисунок 65 - Диалог архивации

Архивация на «неизвлекаемом» ключе выполнена успешно (Рисунок 66).

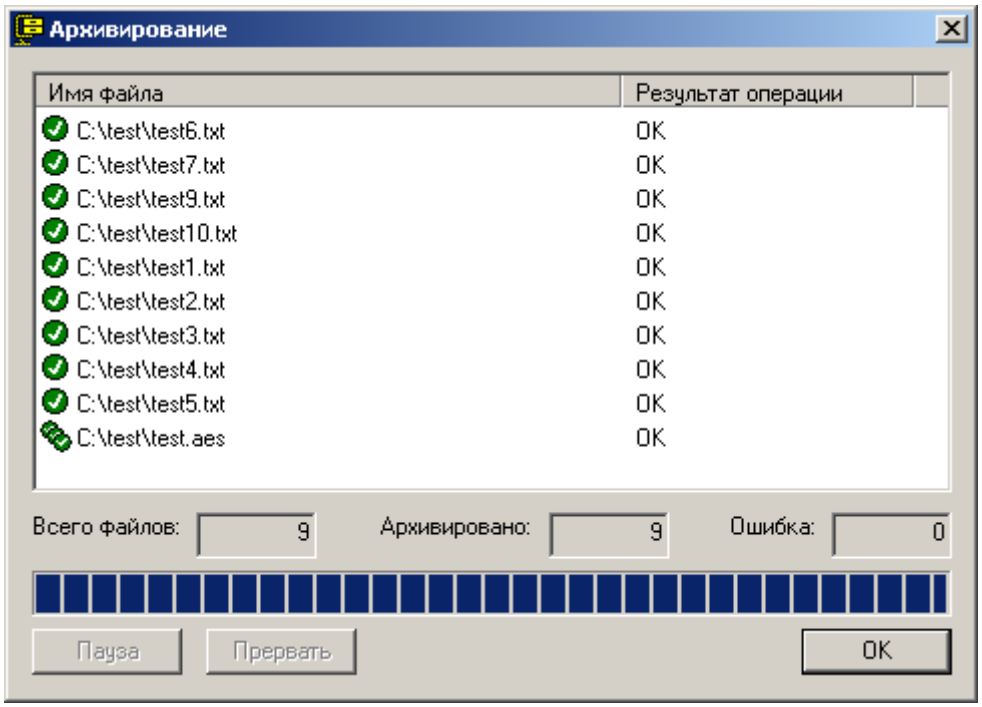

Рисунок 66 - Результат архивирования

4.2 Разархивация на «извлекаемом» ключе

Откройте «Проводник».

Установите ФКН «vdToken» с «извлекаемым» ключом в USB-разъем.

Выберите файл с архивом (Рисунок 67).

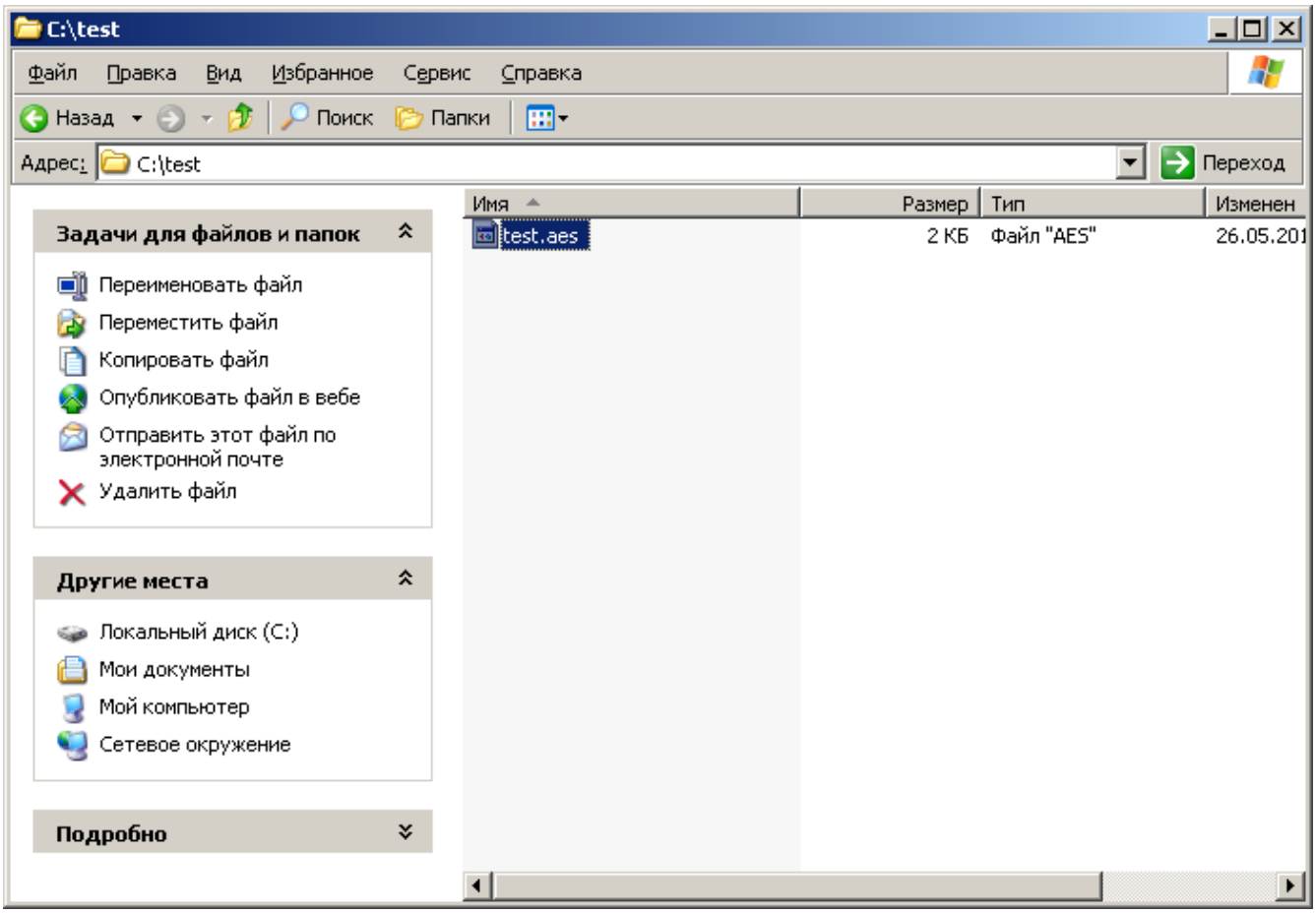

Рисунок 67 - Окно «проводника»

Нажмите правой кнопкой «мыши» на выделенном файле и выполните пункт меню: «САЭС» - >«Разархивировать».

На экран будет выдано предупреждение. Нажмите кнопку «Да» (Рисунок 68).

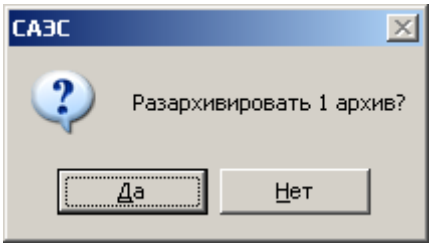

Рисунок 68 - Окно предупреждения

Выберите профиль пользователя, который использует «извлекаемый» ключ на носителе ФКН «vdToken». Нажмите «ОК» (Рисунок 69).

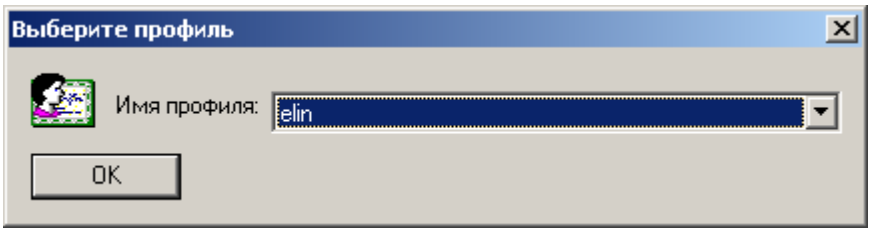

Рисунок 69 - Выбор профиля

Выберите «извлекаемый» считыватель «Считыватель vdToken». Нажмите «ОК» (Рисунок 70).

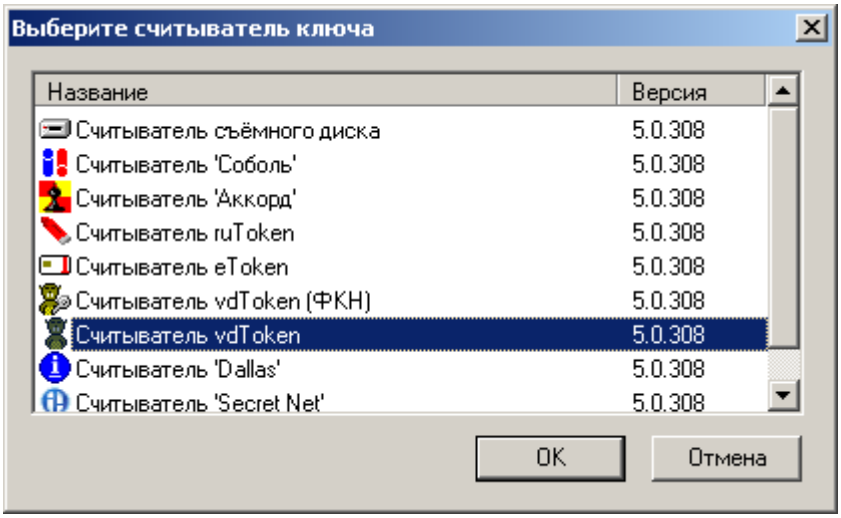

Рисунок 70 - Выбор ключевого считывателя

Введите правильный ПИН-код установленного «токена». Нажмите «ОК» (Рисунок 71).

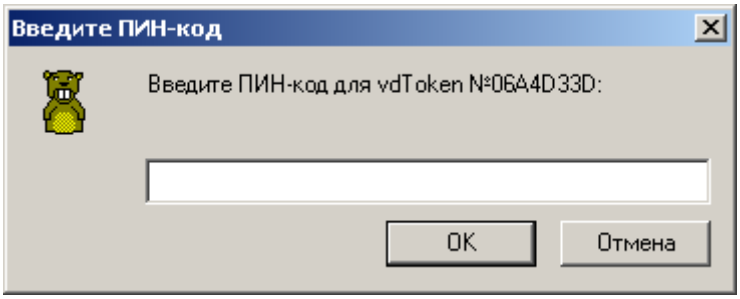

Рисунок 71 - Окно ввода ПИН-кода

Примечание -Если «токен» был отформатирован без ПИН-кода, то окно ввода ПИН-кода на экран выдаваться не будет.

Нажмем кнопку «Разархивировать» (Рисунок 72).

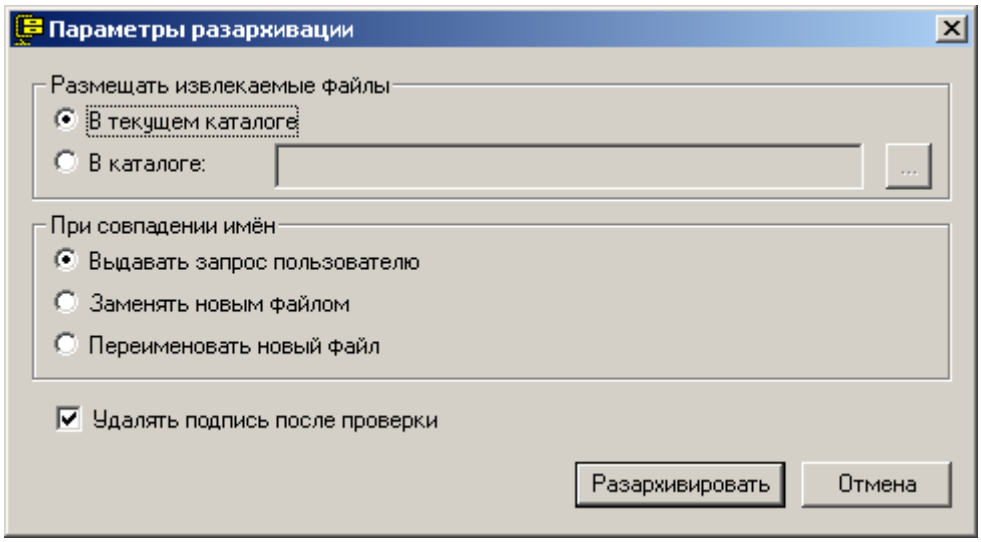

Рисунок 72 - Диалог разархивации

Разархивация на «извлекаемом» ключе выполнена успешно (Рисунок 73).

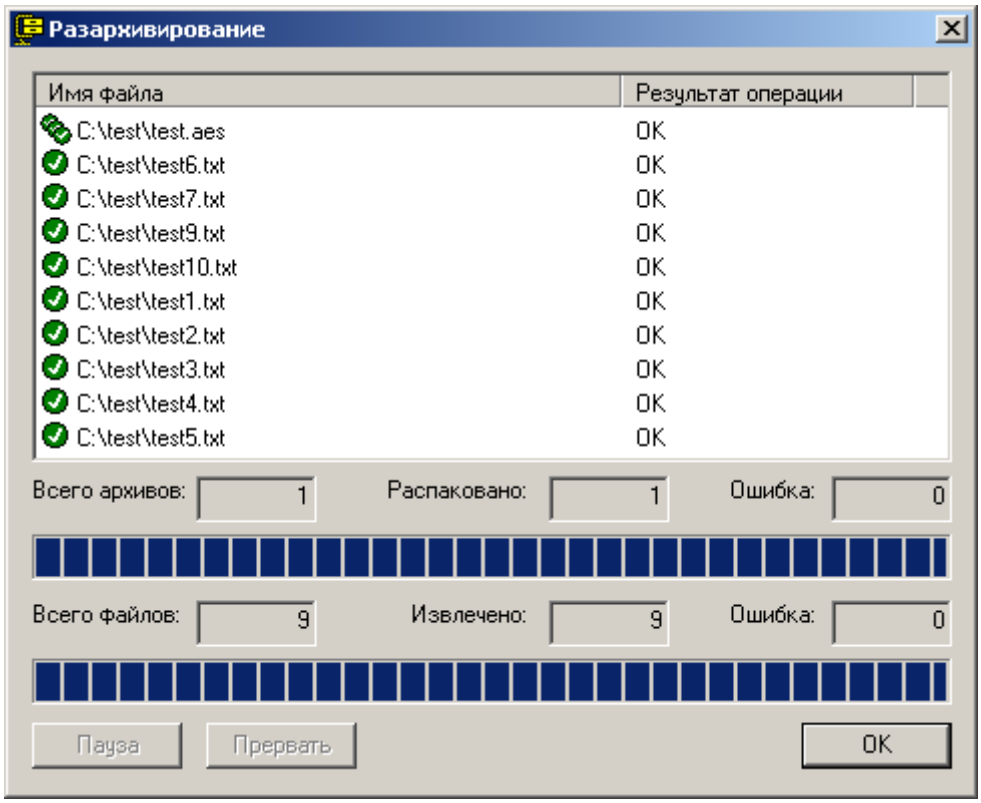

Рисунок 73 - Результат разархивирования

5 ПАМЯТКА ПО ОБРАЩЕНИЮ С ИЗДЕЛИЕМ

5.1 Гарантии изготовителя (исполнителя)

ИЗГОТОВИТЕЛЬ гарантирует качественную работу поставляемой Продукции на соответствие установленных техническими условиями ПЮЯИ.467649.001 ТУ требованиям и соответствие заявленным в технической документации функциональным возможностям.

Гарантийный срок хранения устройств в транспортной таре предприятия-изготовителя составляет 12 месяцев с даты изготовления на предприятии –изготовителе.

Гарантийный срок на поставляемую Продукцию составляет 12 (Двенадцать) месяцев со дня подписания ЗАКАЗЧИКОМ (территориальным учреждением или иным структурным подразделением ЗАКАЗЧИКА) Акта сдачи-приемки Продукции, но не более 18 (Восемнадцати) месяцев с даты изготовления.

ИСПОЛНИТЕЛЬ обеспечивает гарантийное сопровождение поставленной Продукции в процессе ее эксплуатации в течение гарантийного срока при условии соблюдения ЗАКАЗЧИКОМ технических условий эксплуатации Продукции согласно прилагаемой к ней документации.

5.2 Ограничения по транспортированию

Транспортирование устройств до потребителя должно производиться в потребительской упаковке завода-изготовителя в транспортной таре на любое расстояние закрытым автомобильном и железнодорожным транспортом, авиационным транспортом в герметизированных отсеках самолета.

Транспортирование должно осуществляться в соответствии с правилами перевозок, действующими на каждом виде транспорта.

5.3 Заметки по эксплуатации и хранению

Устройства должны храниться в складских помещениях, защищающих устройства от воздействий атмосферных осадков, на стеллажах в упаковке при отсутствии в воздухе паров кислот, щелочей и других агрессивных примесей.

В помещениях, где хранятся упакованные в соответствии с требованиями КД устройства, должна обеспечиваться температура окружающего воздуха от плюс 5 до 40 градусов Цельсия и относительной влажности не более 80% при температуре плюс 25 градусов Цельсия.

Эксплуатация устройств должна осуществляться в соответствии с данным Руководством пользователя ВАМБ.00060-05 92 03.

5.4 Гарантийное сопровождение

5.4.1 Гарантийное сопровождение включает в себя:

- консультирование по вопросам применения и эксплуатации Продукции в режиме «горячей линии» по телефону:

- +7 (495) 232 06 87 с 10 до 19 часов по московскому времени;

- - электронной почте : support_at_x509.ru - круглосуточно;

- приоритетное обслуживание запросов по горячей линии. Гарантированное время реагирования на поступивший запрос не более 8 часов (в рабочие дни);

- замену неисправных единиц Продукции в случае обнаружения конструктивного или производственного дефекта;

- устранение ошибок программных продуктов;

- адрес Исполнителя: 127015, г. Москва, Б. Новодмитровская ул., дом 14, корп. 2, офис 612.

5.4.2 В случае возникновения неисправности Продукции в процессе ее эксплуатации ЗАКАЗЧИК уведомляет об этом ИСПОЛНИТЕЛЯ путем обращения в службу технической поддержки. ИСПОЛНИТЕЛЬ вправе предпринять меры удаленной диагностики (телефону, электронной почте), направленные на установление факта возможной неисправности, ее причин и способов устранения. В случае, если указанные меры не привели к устранению неисправности, ЗАКАЗЧИК обязан письменно уведомить ИСПОЛНИТЕЛЯ по адресу, указанному в пункте 6.4.1.

5.4.3 В уведомлении ЗАКАЗЧИК указывает наименование Продукции, его уникальный номер, основные дефекты, признаки неисправности, обнаруженные в Продукции, условия эксплуатации, а также номер заявки в службу технической поддержки. В случае необходимости ИСПОЛНИТЕЛЬ принимает решение о выезде его представителя в территориальное учреждение или иное структурное подразделение ЗАКАЗЧИКА, откуда поступило уведомление. В этом случае Представитель ИСПОЛНИТЕЛЯ обязан явиться не позднее чем через четверо суток после получения уведомления (не считая времени, необходимого для проезда). О своем решении ИСПОЛНИТЕЛЬ уведомляет ЗАКАЗЧИКА.

5.4.4 ЗАКАЗЧИК, в случае необходимости, должен обеспечить хранение неисправных единиц Продукции. Хранение неисправных единиц продукции должно осуществляться администратором ключевой системы территориального учреждения и иного структурного подразделения ЗАКАЗЧИКА в опечатанном контейнере, но не более 1 (Одного) месяца с момента обнаружения неисправности. ИСПОЛНИТЕЛЬ проводит работы по определению

неисправности Продукции в присутствии администратора ключевой системы территориального учреждения и иного структурного подразделения ЗАКАЗЧИКА.

5.4.5 В случае приезда представителя ИСПОЛНИТЕЛЯ в территориальное учреждение или иное структурное подразделение ЗАКАЗЧИКА и обнаружении конструктивного или производственного дефекта представителями ИСПОЛНИТЕЛЯ и ЗАКАЗЧИКА составляется Рекламационный акт.

5.4.6 Уничтожение неисправной Продукции осуществляется установленным порядком представителями территориального учреждения и иного структурного подразделения ЗАКАЗЧИКА по месту эксплуатации Продукции.

5.4.7 Продукция с конструктивным или производственным дефектом должна быть бесплатно заменена путем отправки ЗАКАЗЧИКУ исправной Продукции в течение 30 (тридцати) календарных дней с момента получения уведомления.

5.4.8 Срок гарантии увеличивается на время простоя Продукции по причине наступления гарантийного случая.

5.4.9 ИСПОЛНИТЕЛЬ обязан подтвердить по телефону или электронной почте получение обращения ЗАКАЗЧИКА в службу технической поддержки.

5.5 Свидетельство о регистрации

Свидетельство о государственной регистрации - №2015613470 от 17 марта 2015г.

Регистрационный номер, выданный некоммерческой организацией USB Implementers Forum, Inc. – 0x2BB1 от 20 мая 2015г.

ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

ОС	Операционная система
СКЗИ	Средство криптографической защиты информации
ФКН	Функциональный ключевой носитель

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (стр.) в документе	№ документа	Входящий № сопроводительного документа	Подпись	Дата
	измененных	замененных	новых	аннулированных					