

ООО «ВАЛИДАТА»

УТВЕРЖДЕН
ВАМБ.00060-06-ЛУ

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

Руководство администратора

ВАМБ.00060-06 95 01

2020

Аннотация

Данный документ содержит описание процесса эксплуатации программного комплекса ВАМБ.00060-06 «Средство криптографической защиты информации «Валидата CSP» версия 6» (далее по тексту — СКЗИ «Валидата CSP»).

Документ предназначен для пользователей как руководство по эксплуатации СКЗИ «Валидата CSP».

Перед чтением настоящего документа рекомендуется ознакомиться с документом ВАМБ.00060-06 31 01 «СКЗИ «Валидата CSP» версия 6. Описание применения».

Содержание

1 НАЗНАЧЕНИЕ	5
2 СЧИТЫВАТЕЛИ КЛЮЧЕЙ	6
2.1 Настройка считывателей ключей	6
2.2 Графический интерфейс пользователя при работе с ключами	8
2.2.1 Интерактивный выбор ключа	8
2.2.2 Пароли для защиты ключа	10
2.2.3 Особенности работы с различными ключевыми носителями . .	12
3 ДАТЧИКИ СЛУЧАЙНЫХ ЧИСЕЛ	13
3.1 Настройка ДСЧ	13
3.2 Инициализация ДСЧ	14
3.2.1 Автоматическая инициализация	15
3.2.2 Принудительная инициализация	17
3.3 Инициализация ДСЧ ФКН	18
4 СЕРВИСНЫЕ ФУНКЦИИ ПРОГРАММЫ КОНФИГУРАЦИИ	20
4.1 Операции с ключами	20
4.1.1 Копирование ключа	20
4.1.2 Удаление ключей	21
4.1.3 Смена пароля ключа	22
4.1.4 Преобразование ключа	22
4.1.5 Обновление масок ключа	23
4.1.6 Просмотр информации о ключе	23
4.2 Операции с сертификатами	24
4.2.1 Установка сертификата в системное хранилище	25
4.2.2 Запись сертификата на смарт-карту	29
4.3 Дополнительные операции	30
4.3.1 Уничтожение содержимого файла	31
4.3.2 Проверка подписи программных модулей	31
4.3.3 Форматирование и смена ПИН-кода ключевого носителя	32
5 ГРАФИЧЕСКИЙ ИНТЕРФЕЙС ПОЛЬЗОВАТЕЛЯ СЕРВИСОВ	35
6 ПРОГРАММНЫЙ МОДУЛЬ ПОДДЕРЖКИ TLS	39
6.1 Использование Internet Information Server (IIS) с модулем поддержки TLS	39
6.2 Использование Microsoft Internet Explorer с модулем поддержки TLS	41
6.3 Использование Terminal Services с модулем поддержки TLS	42
6.4 Использование Terminal Services Gateway с модулем поддержки TLS	43
6.5 Использование Remote Desktop Client с модулем поддержки TLS	45
6.6 Использование протокола Kerberos PKInit с модулем поддержки TLS	47
6.7 TLS монитор	52
6.7.1 Запуск и включение TLS монитора	52

6.7.2	Конфигурация TLS монитора	54
	ПЕРЕЧЕНЬ СОКРАЩЕНИЙ	56
	ПЕРЕЧЕНЬ РИСУНКОВ	58

1 НАЗНАЧЕНИЕ

Выполняемые ПК ВАМБ.00060-06 «Средство криптографической защиты информации «Валидата CSP» версия 6» (далее — СКЗИ «Валидата CSP») функции, используемые операционные системы (ОС), в среде которых работает СКЗИ «Валидата CSP», и допустимые при работе с СКЗИ «Валидата CSP» типы ключевых носителей перечислены в документе ВАМБ.00060-06 30 01 «СКЗИ «Валидата CSP» версия 6. Формуляр».

2 СЧИТЫВАТЕЛИ КЛЮЧЕЙ

Для выполнения большинства криптографических операций требуются ключи. Ключ ЭП обычно хранится на отчуждаемых носителях (USB flash, «таблетках» — Touch Memory и т.д.). Для чтения и записи ключей на ключевые носители предназначены программные модули — считыватели ключей. СКЗИ «Валидата CSP» может работать с несколькими считывателями ключей, их использование регулируется **программой конфигурации** СКЗИ «Валидата CSP».

2.1 Настройка считывателей ключей

Для запуска **программы конфигурации** СКЗИ «Валидата CSP» необходимо вызвать пункт меню «Пуск»→«Программы»→«СКЗИ Валидата CSP»→«Конфигурационная программа СКЗИ». Для настройки считывателей ключей надо перейти на вкладку «Считыватели ключа» (Рисунок 1).

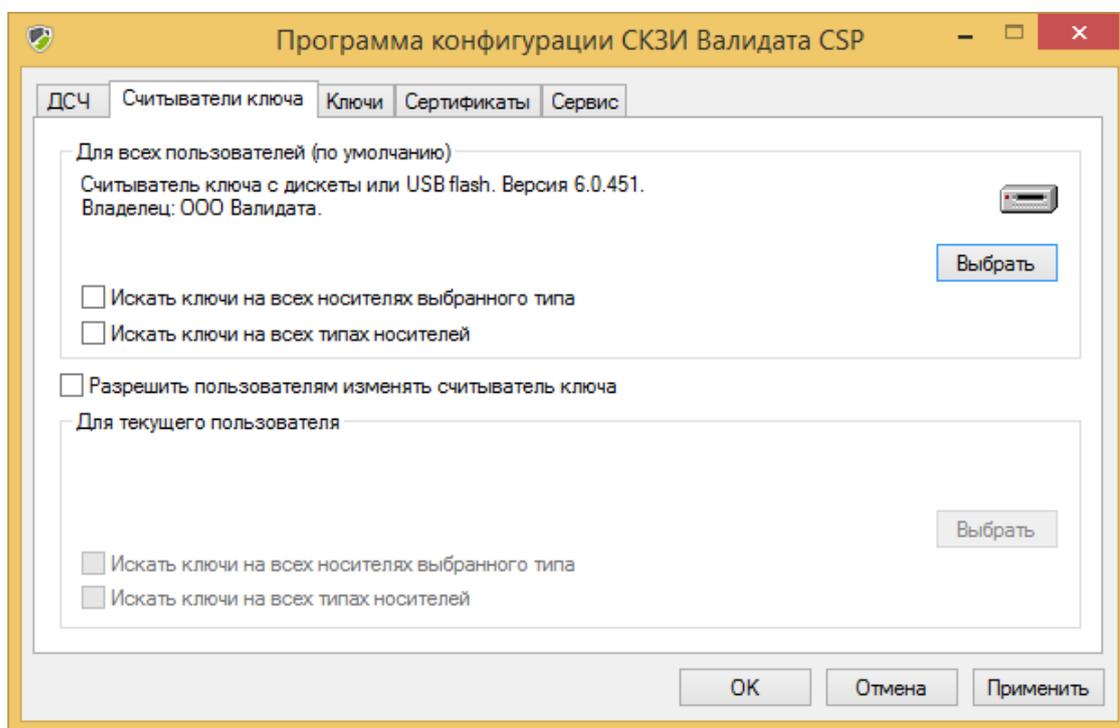


Рисунок 1 - Вкладка «Считыватели ключа»

Считыватель ключа по умолчанию может быть задан администратором (см. документ ВАМБ.00060-06 91 01 «СКЗИ «Валидата CSP» версия 6. Руководство по установке и настройке»). Если администратор задал считыватель ключа с USB flash (Рисунок 1), то все пользователи при попытке чтения ключа будут обращаться к флэш-памяти. Пользователь не может изменить эту установку, но если администратор разрешил пользователям изменять считыватель ключа, то пользователь получает возможность задать считыватель ключа только для себя, нажав кнопку «Выбрать» в нижней части вкладки.

На экране появится диалоговое окно выбора считывателей ключа (Рисунок 2).

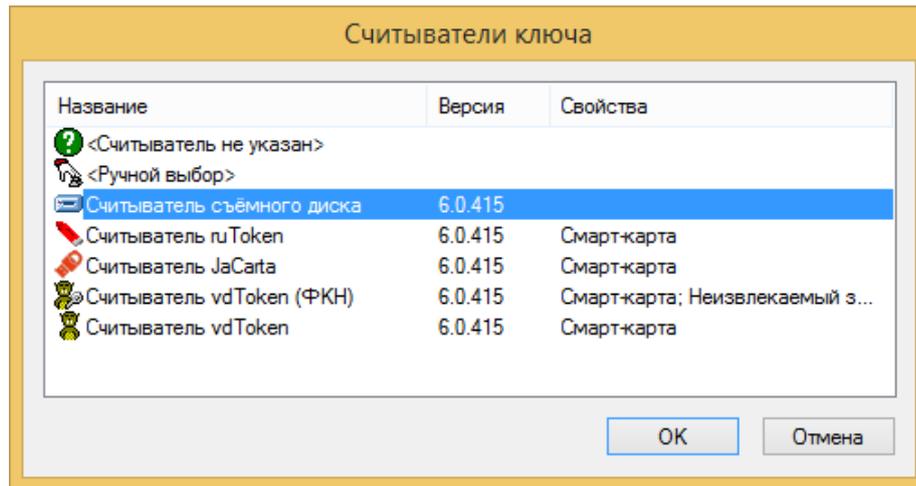


Рисунок 2 - Диалог выбора считывателя ключа

Выберите другой считыватель ключа и нажмите кнопку «ОК». Появится диалоговое окно (Рисунок 3).

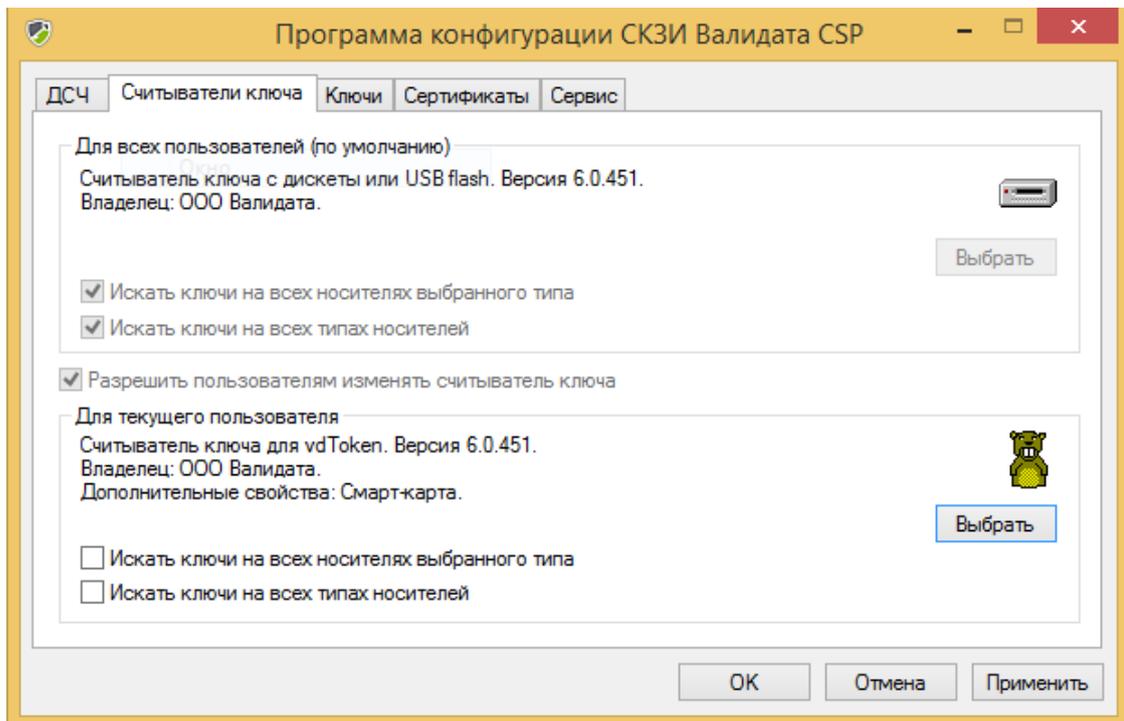


Рисунок 3 - Изменение считывателя ключа для текущего пользователя

Если в диалоге (Рисунок 2) выбрать пункт «**Считыватель не указан**», и при этом считыватель также не указан для всех пользователей (по умолчанию), то при обращении к ключам может выдаваться дополнительный диалог выбора считывателя ключа. Если в диалоге (Рисунок 2) выбрать пункт «**Ручной выбор**», то при обращении к ключам может выдаваться дополнительный диалог выбора считывателя ключа, даже если задан считыватель для всех пользователей (по умолчанию).

Если установить режим «**Искать ключи на всех носителях выбранного типа**», то при пролистывании и загрузке ключей не будет выдаваться диалог

выбора ключевого носителя, поиск ключей будет производиться на всех обнаруженных ключевых носителях заданного типа, загружаться будет первый найденный ключ с заданным именем.

Если дополнительно установить режим **«Искать ключи на всех типах носителей»**, то при пролистывании и загрузке ключей не будут выдаваться диалоги выбора считывателя и ключевого носителя, поиск ключей будет производиться на всех обнаруженных ключевых носителях всех типов, загружаться будет первый найденный ключ с заданным именем.

Для того чтобы изменения вступили в силу, нажмите кнопку **«Применить»**.

2.2 Графический интерфейс пользователя при работе с ключами

2.2.1 Интерактивный выбор ключа

В общем случае алгоритм выбора считывателя ключа таков: если пользователю разрешено изменять считыватель ключа, и он сделал это, используется считыватель ключа, указанный пользователем. Если нет – используется считыватель ключа, заданный администратором. Если и администратор не назначил считыватель ключа по умолчанию, на экран выдаётся диалоговое окно, предлагающее выбрать считыватель ключа (Рисунок 4).

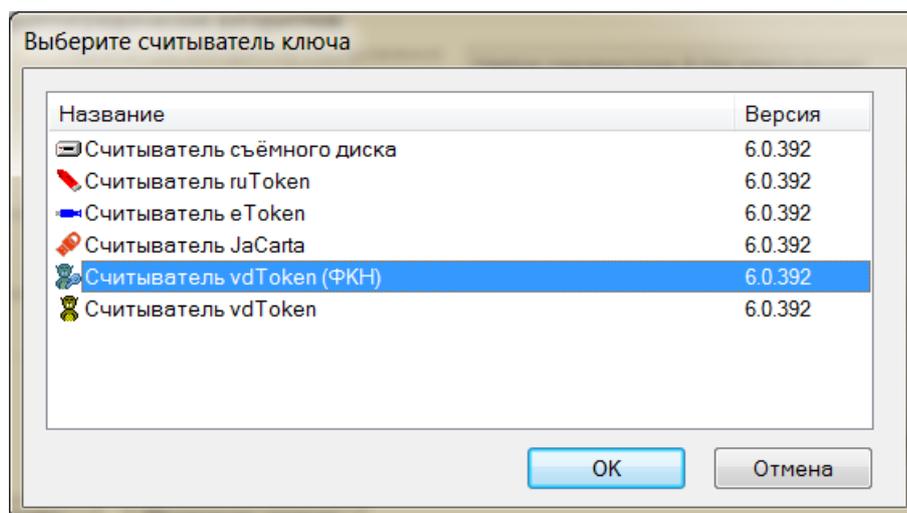


Рисунок 4 – Диалог выбора ключа

Это же окно выдаётся, если пользователь задал режим **«Ручной выбор»**, независимо от настроек администратора.

Если пользователем установлен режим **«Искать ключи на всех типах носителей»**, то при пролистывании и загрузке ключей не будет выдаваться диалог выбора считывателя, поиск ключей будет производиться на всех обнаруженных ключевых носителях всех типов, загружаться будет первый найденный ключ с заданным именем.

В некоторых случаях такой диалог будет возникать даже при назначенном считывателе ключа – например, в ситуации, когда надо скопировать ключ с одного типа устройства на другое.

После выбора считывателя при работе с ключами нужно выбрать ключевой носитель, для этого на экран выдаётся диалоговое окно, предлагающее выбрать ключевой носитель (например, USB-flash) (Рисунок 5).

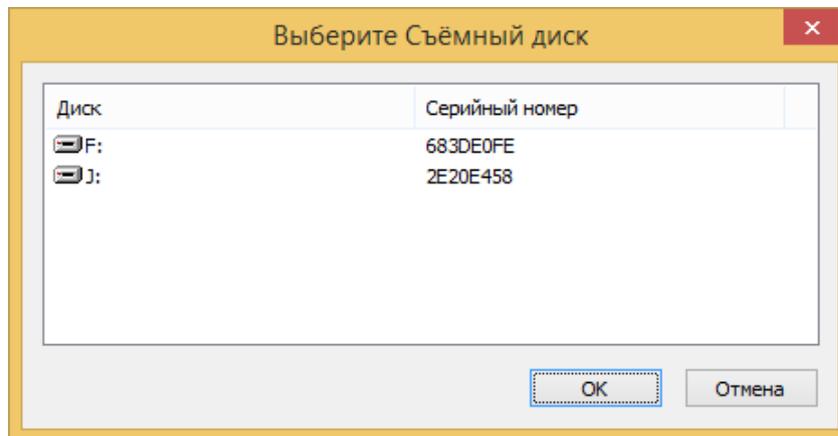


Рисунок 5 – Диалог выбора ключевого носителя

При пролистывании и загрузке ключей этот диалог не выдаётся, если система обнаруживает лишь один ключевой носитель выбранного типа или же пользователем установлен режим «**Искать ключи на всех носителях выбранного типа**».

Если считыватель ключа не обнаруживает ни одного диска, он выдаст сообщение (Рисунок 6).

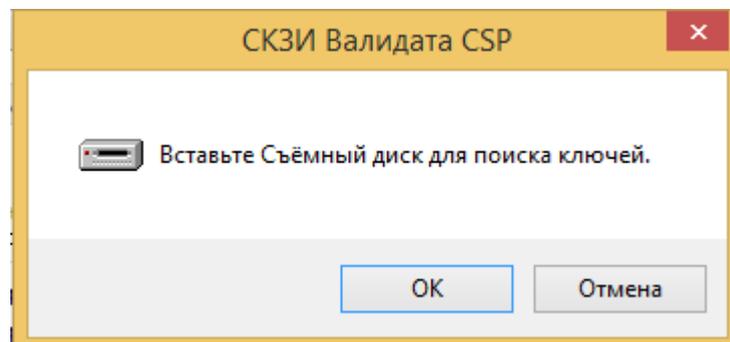


Рисунок 6 – Ключевой носитель не найден

После выбора ключевого носителя часто бывает необходимо выбрать один из нескольких, находящихся на нём ключей. Для этого служит диалог выбора ключа (Рисунок 7).

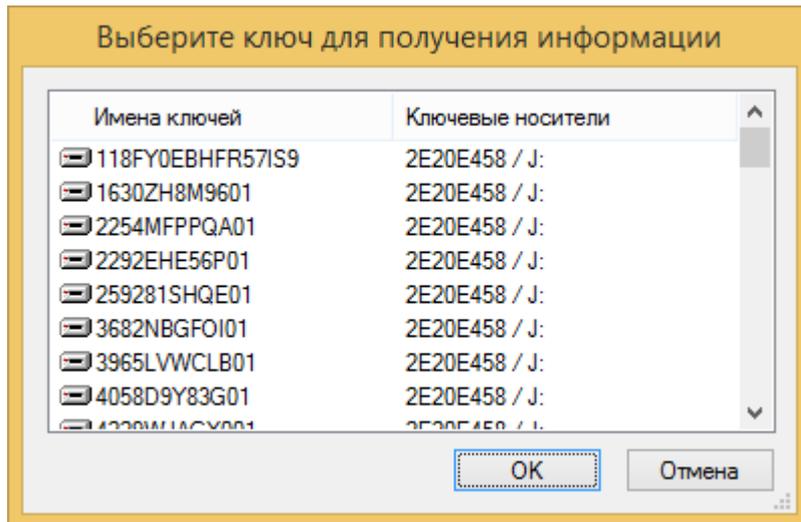


Рисунок 7 – Диалог выбора ключа

Выберите ключ для операции, название которой указано в заголовке окна, и нажмите кнопку «**ОК**».

2.2.2 Пароли для защиты ключа

При записи (генерации и т.д.) ключа пользователю предлагается ввести пароль для защиты ключа (Рисунок 8).

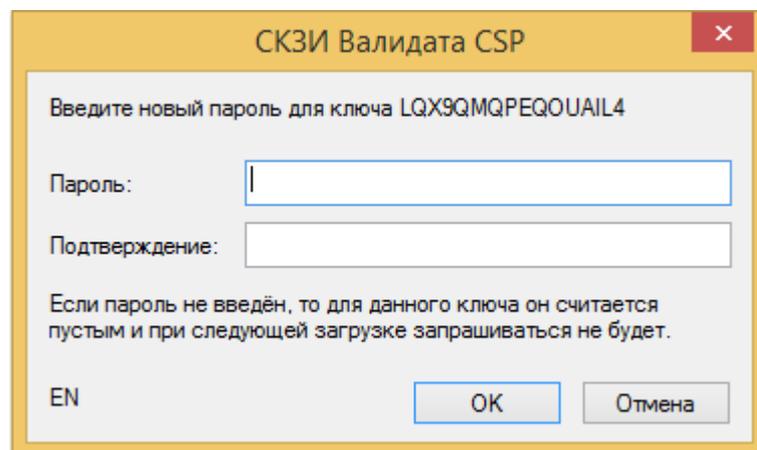


Рисунок 8 – Диалог задания пароля ключа

Введите пароль два раза и нажмите кнопку «**ОК**». Если введённые значения отличаются друг от друга, система предложит повторить попытку (Рисунок 9).

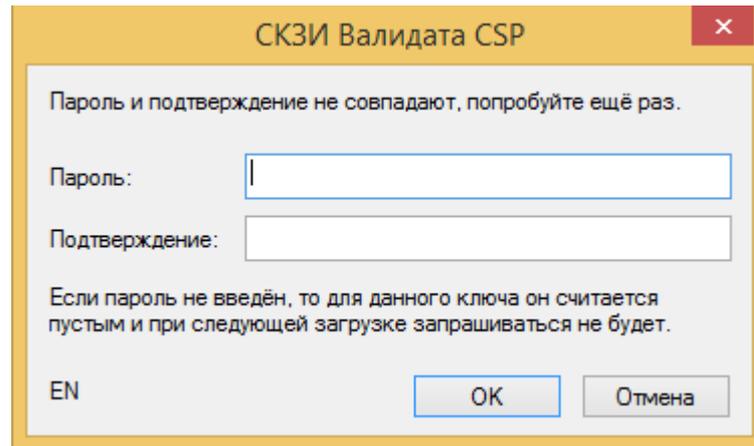


Рисунок 9 – Диалог повторного задания пароля ключа

Если пользователь не хочет защищать ключ паролем, он должен нажать кнопку «ОК», не вводя пароля. Нажатие кнопки «Отмена» отменяет не пароль, а всю операцию с ключом.

При чтении ключа, защищённого паролем, пользователю предлагается ввести пароль (Рисунок 10).

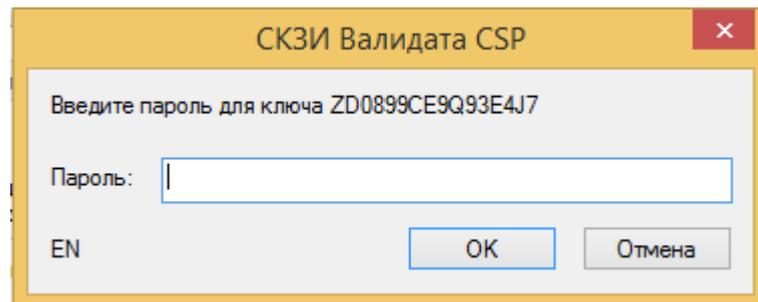


Рисунок 10 – Диалог проверки пароля ключа

При неправильном вводе пароля пользователю предлагается повторить ввод с указанием количества оставшихся попыток (Рисунок 11).

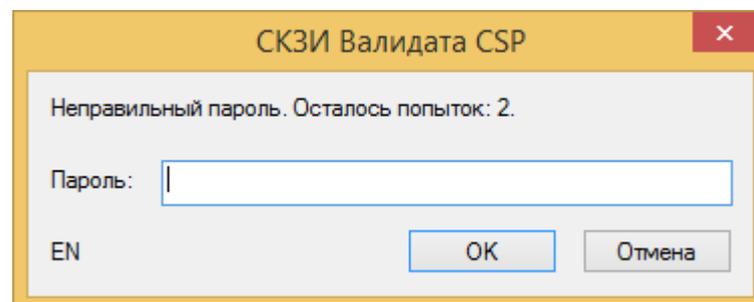


Рисунок 11 – Диалог повторной проверки пароля ключа

Если количество неуспешных попыток ввода пароля ключа электронной подписи (ЭП) становится равным максимально возможному (3 попытки), загрузка ключа ЭП не производится и соответствующий код ошибки возвращается прикладному программному обеспечению (ПО).

Если ключ ЭП не защищен паролем, то при его чтении диалоговое окно проверки пароля ключа не выдается.

2.2.3 Особенности работы с различными ключевыми носителями

В случае возникновения ошибки 0xE0BE50DE «Ошибка ф-ии RtlLoginToken» при использовании считывателя РуТокен, необходимо отключить кэширование PIN-кодов на вкладке Настройки Панели управления РуТокен, запустив ее из Панели управления ОС Windows (Рисунок 12).

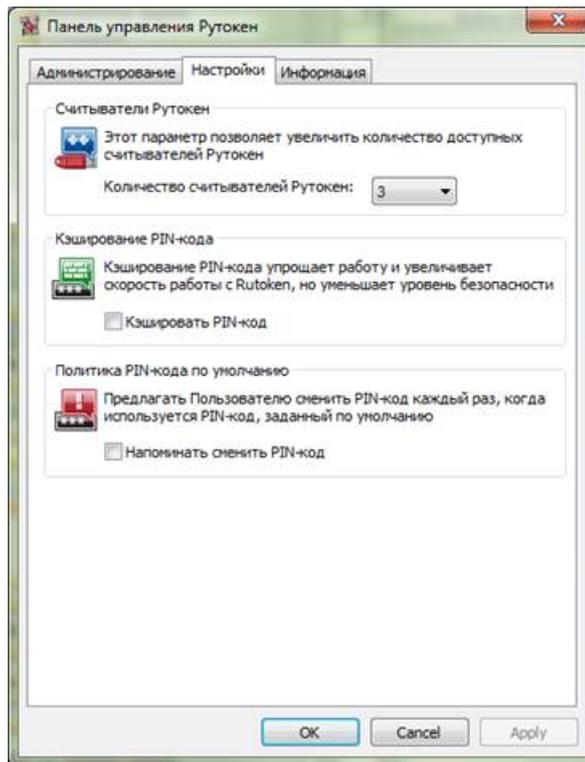


Рисунок 12 - Панель управления РуТокен

3 ДАТЧИКИ СЛУЧАЙНЫХ ЧИСЕЛ

Для работы СКЗИ «Валидата CSP» требуется датчик случайных чисел (ДСЧ). СКЗИ «Валидата CSP» может работать с различными типами ДСЧ, их использование регулируется программой конфигурации СКЗИ «Валидата CSP».

3.1 Настройка ДСЧ

Настройка ДСЧ производится на вкладке «ДСЧ» программы конфигурации СКЗИ «Валидата CSP» (Рисунок 13).

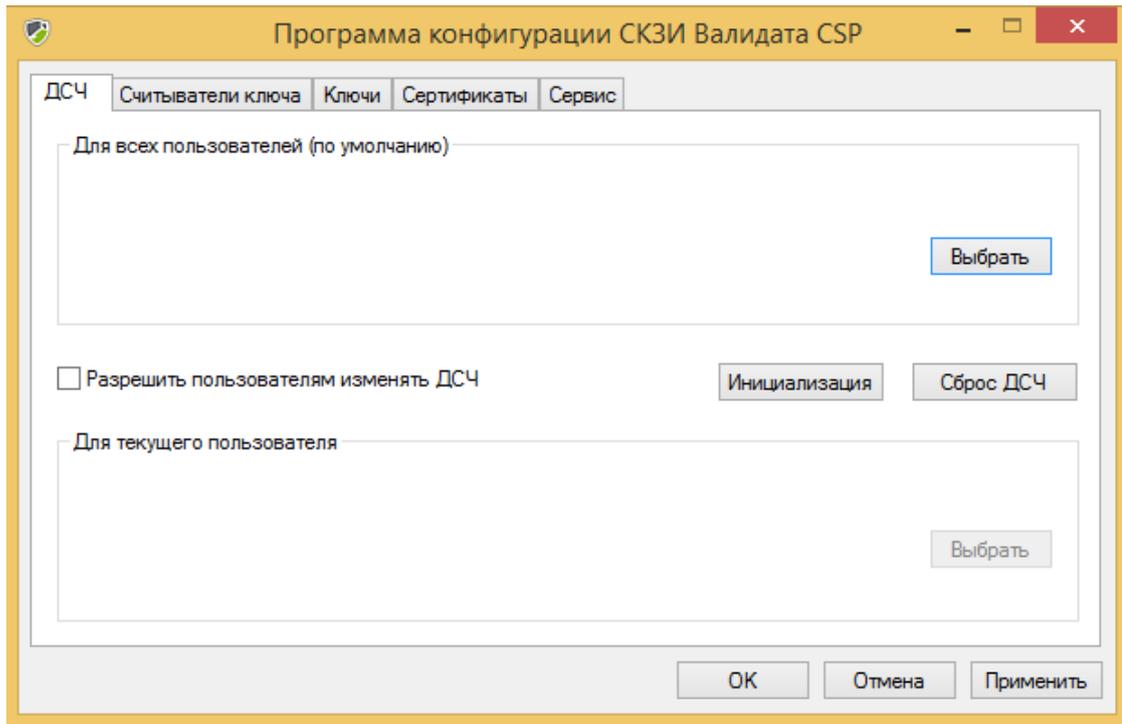


Рисунок 13 - Вкладка «ДСЧ»

Тип ДСЧ по умолчанию может быть задан администратором (см. ВАМБ.00060-06 91 01 «СКЗИ «Валидата CSP» версия 6. Руководство по установке и настройке»).

Если администратор задал биологический ДСЧ (Рисунок 13), то для всех пользователей будет вызываться этот датчик. Пользователь не может изменить эту установку, но если администратор разрешил пользователям задавать тип ДСЧ, то пользователь получает возможность изменить тип ДСЧ только для себя, нажав кнопку «Выбрать» в нижней части вкладки.

На экране появится диалоговое окно выбора типа ДСЧ (Рисунок 14).

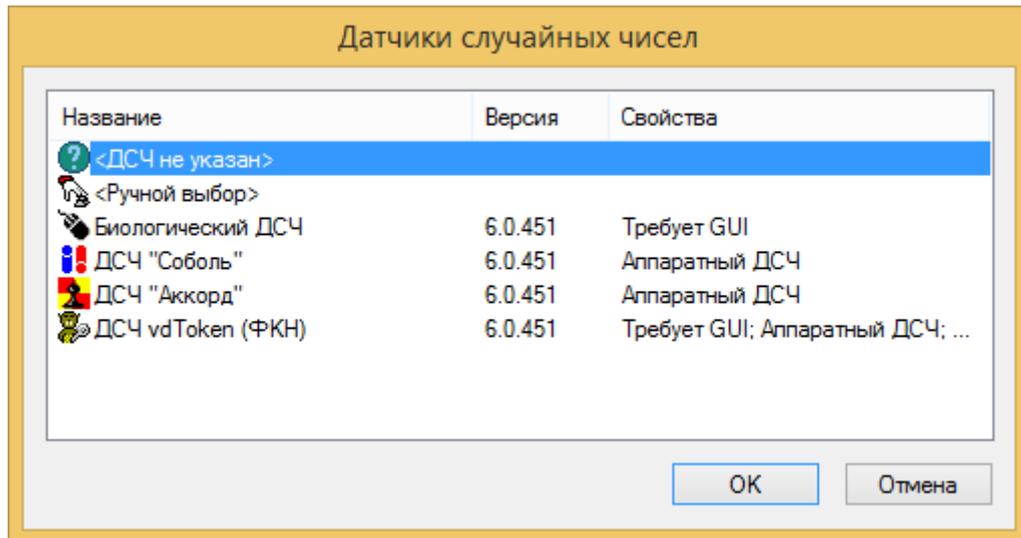


Рисунок 14 – Диалог выбора ДСЧ

Выберите тип ДСЧ и нажмите кнопку «ОК». На экране появится исходное окно с информацией о выбранном ДСЧ (Рисунок 15).

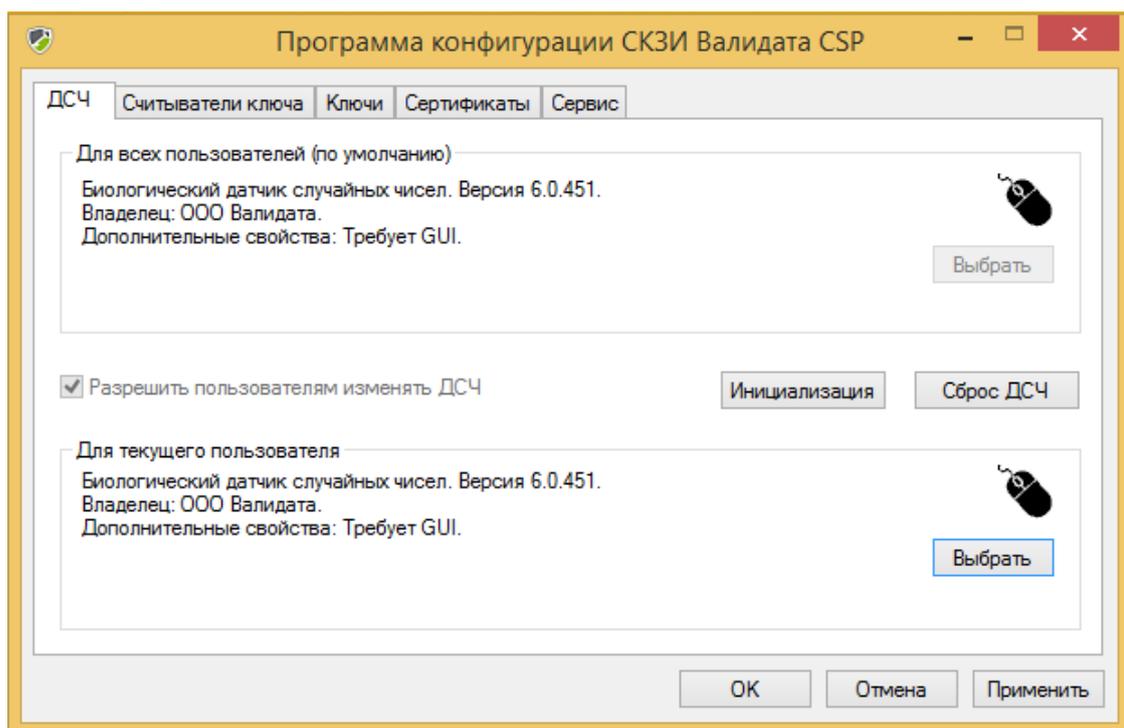


Рисунок 15 – ДСЧ для текущего пользователя изменён

Для того чтобы сделанные изменения вступили в силу, нажмите кнопку «Применить».

3.2 Инициализация ДСЧ

ДСЧ требует инициализации после каждой загрузки ОС «Windows».

Примечание — Для инициализации ДСЧ СКЗИ «Валидата CSP» ключ ЭП не требуется.

3.2.1 Автоматическая инициализация

Запуск процедуры инициализации ДСЧ выполняется в автоматическом режиме при выполнении первой криптографической операции после загрузки ОС Windows.

Инициализация ДСЧ не требует участия пользователя, за исключением случая набора первичных случайных данных при использовании биологического ДСЧ (Рисунок 16). Выполнение требований, изложенных ниже, гарантирует успешное завершение процедуры инициализации ДСЧ с использованием биологического ДСЧ.

Примечание — Набор первичных случайных данных при использовании биологического ДСЧ выполняется при инициализации ДСЧ в процессе установки СКЗИ «Валидата CSP» или перед выполнением первой криптографической операции (если ДСЧ не был инициализирован ранее), а также после принудительного сброса ДСЧ (см. п. 3.2.2 настоящего документа).

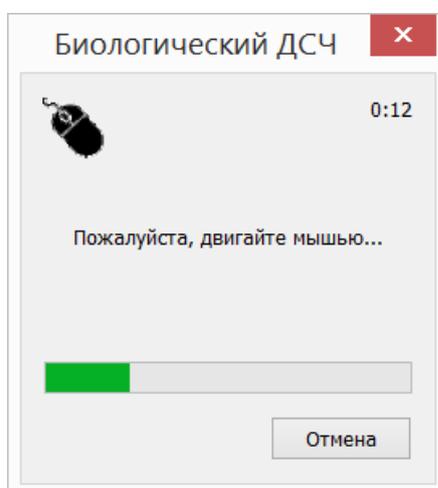


Рисунок 16 – Инициализация биологического ДСЧ

Если сгенерированные пользователем случайные данные не удовлетворяют требованиям, предъявляемым к инициализирующей последовательности ДСЧ, окно инициализации биологического ДСЧ (Рисунок 16) будет выведено на экран повторно.

Работа с биологическим ДСЧ

После запуска процедуры инициализации ДСЧ на экране появляется рабочее окно в виде квадрата.

С точки зрения пользователя процесс инициализации можно представлять, как «рисование» курсором в рабочем окне некоторой достаточно хаотичной траектории.

При этом пользователю следует соблюдать следующие общие требования:

- процедура инициализации ДСЧ осуществляется с использованием компьютерной «мыши». Необходимо настроить параметры «мыши» таким образом, чтобы «ползунок», задающий скорость движения указателя (курсора), на вкладке «Параметры указателя» был установлен ровно посередине шкалы (для светоди-

одной «мыши») или был сдвинут на два деления влево от середины шкалы (для лазерной «мыши») (Рисунок 17);

- использование беспроводной «мыши» не допускается;
- не следует заходить за границы рабочего окна (это замедляет процесс инициализации ДСЧ). Вместе с тем непреднамеренные выходы за границы окна допускаются;
- траектория движения «мыши» должна быть непрерывной;
- рисование траекторий должно осуществляться весьма энергично, т.е. таким образом, чтобы время, затрачиваемое на инициализацию ДСЧ, не превышало 60 секунд. Если рисование траектории выполняется недостаточно энергично, может потребоваться повторная инициализация ДСЧ. В этом случае на экране вновь появится рабочее окно в виде квадрата.

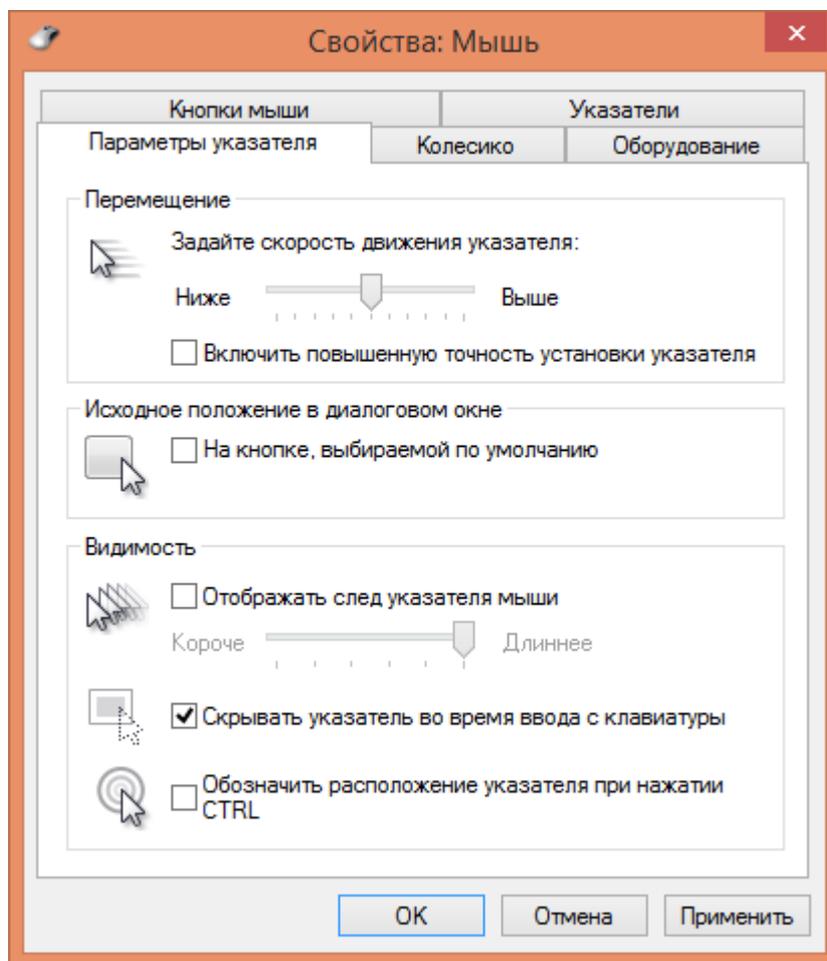


Рисунок 17 – Пример настройки «мыши»

Пользователю надлежит «зарисовывать» курсором всё внутреннее пространство (площадь) рабочего окна кругами диаметром порядка одной трети размера стороны окна.

Ниже (Рисунок 18) приведено изображение фрагмента типичной траектории движения «мыши».

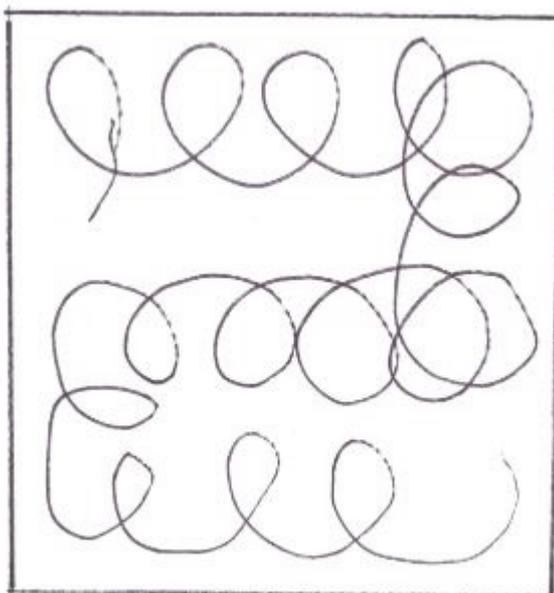


Рисунок 18 – Пример хаотичных кругообразных движений

На приведенном фрагменте (Рисунок 18) воображаемый центр окружностей совершает следующие движения:

- движение начинается в правом нижнем углу;
- из правого нижнего угла воображаемый центр переходит в левый нижний угол;
- поднимается вверх на воображаемую среднюю линию, делящую окно пополам;
- движется слева направо до правой границы окна;
- поднимается вверх в правый верхний угол;
- движется справа налево, попадая в верхний левый угол.

Затем движение аналогичным образом продолжается из верхнего левого угла в нижний правый угол и весь цикл повторяется до тех пор, пока не будет завершена процедура инициализации биологического ДСЧ.

3.2.2 Принудительная инициализация

В некоторых случаях, например, при работе с серверными приложениями, удобно выполнить инициализацию ДСЧ принудительно. Для этого надо нажать кнопку «Инициализация» на вкладке ДСЧ программы конфигурации СКЗИ «Валидата CSP». Программа выполнит инициализацию ДСЧ так же, как было описано в п. 3.2.1 и выдаст сообщение (Рисунок 19).

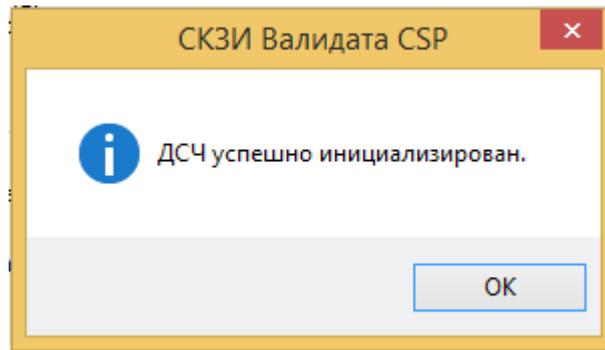


Рисунок 19 – Сообщение об удачной инициализации ДСЧ

При повторной попытке принудительной инициализации программа выдаст сообщение (Рисунок 20).

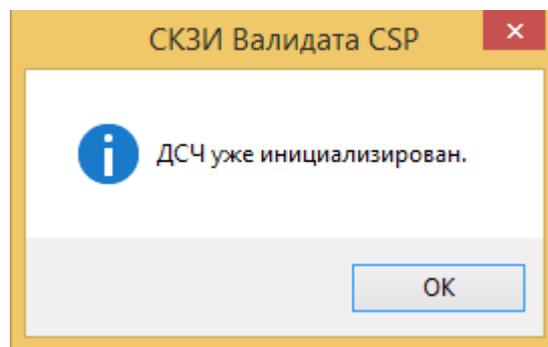


Рисунок 20 – Сообщение об инициализованном ДСЧ

Чтобы вернуть ДСЧ в начальное (неинициализированное) состояние, пользователь может нажать кнопку «Сброс ДСЧ» на вкладке ДСЧ.

3.3 Инициализация ДСЧ ФКН

В состав СКЗИ «Валидата CSP» входит утилита загрузки инициализационной последовательности ДСЧ функционального ключевого носителя (ФКН), которая позволяет инициализировать ДСЧ ФКН «Валидата vdToken» и «Валидата vdToken» версия 2.0.

Примечания

1 ФКН «Валидата vdToken» и ФКН «Валидата vdToken» версия 2.0 поставляются пользователям с уже инициализированным ДСЧ, в связи с чем использование данной утилиты для работы с ФКН не является обязательным.

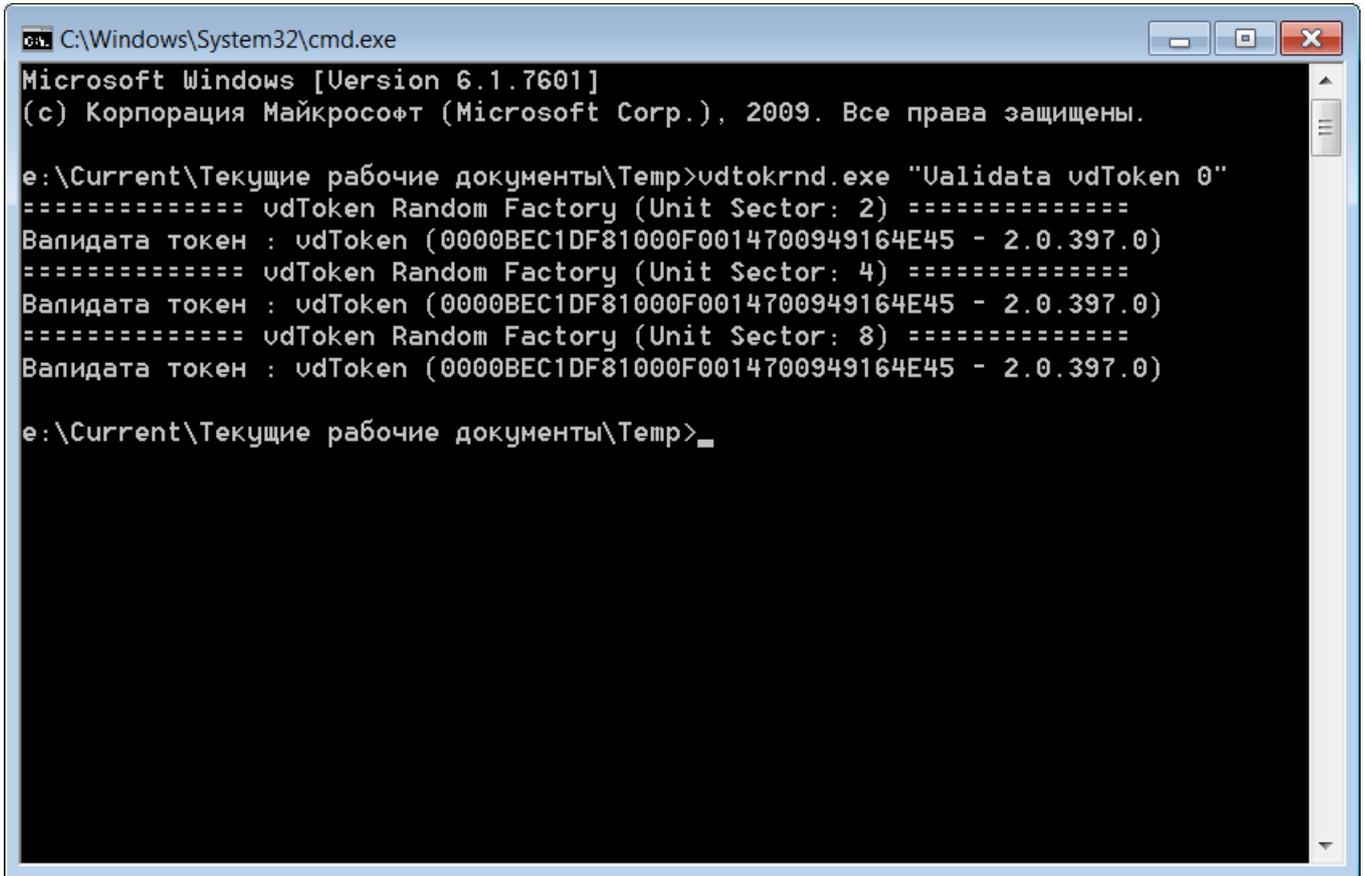
2 В результате работы данной утилиты с носителя будут безвозвратно удалены все данные.

Программа **vdtokrnd.exe** представляет собой консольное приложение. Для выполнения инициализации ДСЧ необходимо в командной строке вызвать утилиту **vdtokrnd.exe** со следующими параметрами:

vdtokrnd.exe "Validata vdToken <номер устройства>",

где <номер устройства> — порядковый номер ФКН (>=0), для которого выполняется инициализация ДСЧ, как устройства типа смарт-карта в ОС Windows.

В случае ошибки начальной инициализации ДСЧ ФКН будет выдано соответствующее сообщение об ошибке. Пример вызова программы **vdtokrnd.exe** и сообщения, выдаваемые в процессе ее работы при успешной начальной инициализации ДСЧ, приведены ниже на рисунке (Рисунок 21).



```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
(с) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.

e:\Current\Текущие рабочие документы\Temp>vdtokrnd.exe "Ualidata vdToken 0"
===== vdToken Random Factory (Unit Sector: 2) =====
Валидата токен : vdToken (0000BEC1DF81000F0014700949164E45 - 2.0.397.0)
===== vdToken Random Factory (Unit Sector: 4) =====
Валидата токен : vdToken (0000BEC1DF81000F0014700949164E45 - 2.0.397.0)
===== vdToken Random Factory (Unit Sector: 8) =====
Валидата токен : vdToken (0000BEC1DF81000F0014700949164E45 - 2.0.397.0)

e:\Current\Текущие рабочие документы\Temp>_
```

Рисунок 21 - Пример работы программы в случае успешной инициализации ДСЧ ФКН

4 СЕРВИСНЫЕ ФУНКЦИИ ПРОГРАММЫ КОНФИГУРАЦИИ

4.1 Операции с ключами

На вкладке «Ключи» расположены кнопки, позволяющие копировать, удалять, менять пароли, преобразовывать ключи и обновлять маски ключей (Рисунок 22).

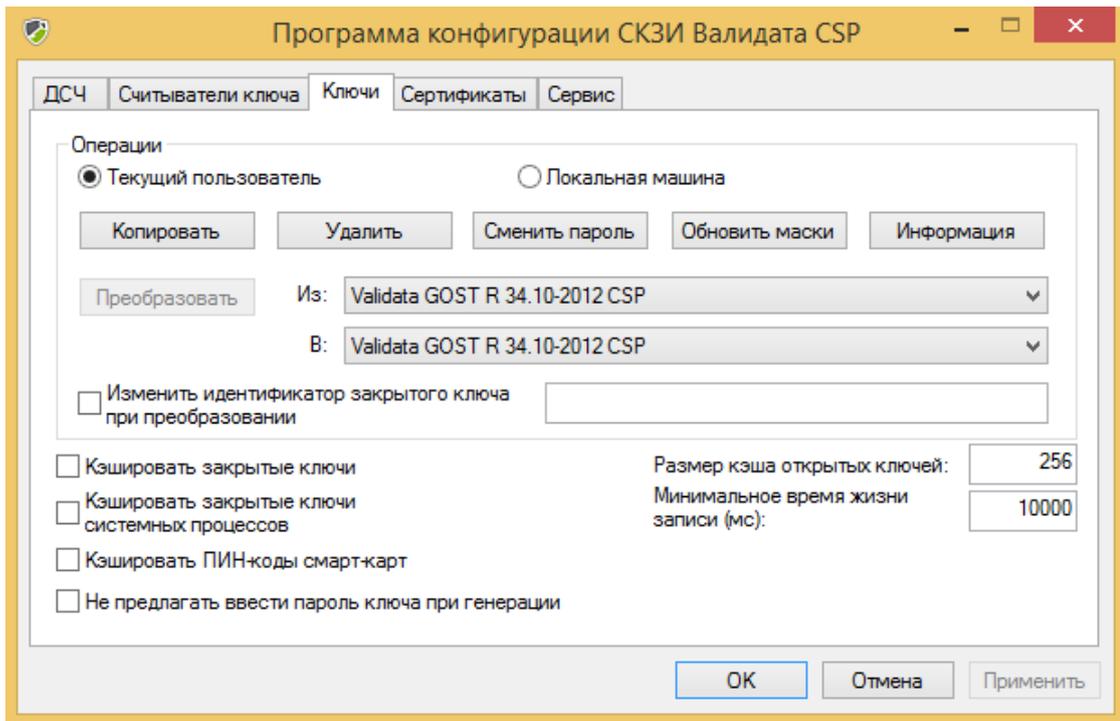


Рисунок 22 – Вкладка «Ключи»

4.1.1 Копирование ключа

Для копирования ключа с одного носителя на другой нажмите кнопку «Копировать». Если инициализация ДСЧ ещё не была выполнена, на экране появятся диалоги инициализации ДСЧ (см. п. 3.2.1). Затем, даже если в конфигурации задан считыватель ключа по умолчанию, на экране появится диалог выбора считывателя ключа. Это делается для того, чтобы пользователь мог копировать ключи с разных ключевых носителей. После того, как пользователь выберет ключ для копирования, на экране появится сообщение (Рисунок 23).

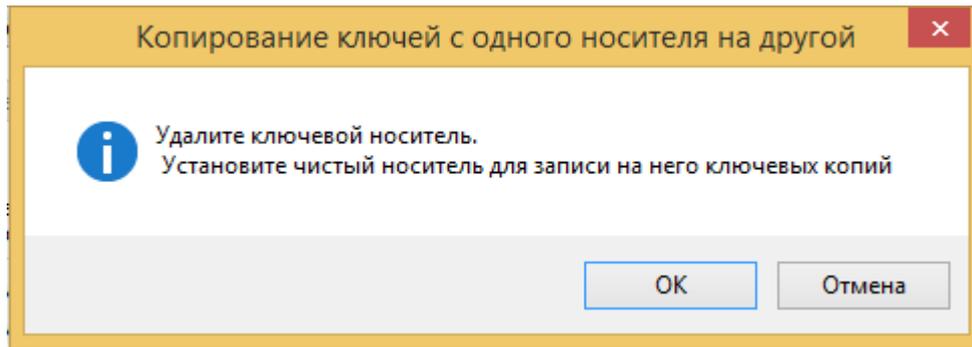


Рисунок 23 – Сообщение о замене ключевого носителя

Если для установки ключевого носителя, на который пользователь хочет скопировать ключ, необходимо удалить текущий ключевой носитель, это надо сделать после появления такого сообщения. В противном случае данное сообщение можно оставить без внимания. После нажатия кнопки «ОК» необходимо выбрать считыватель ключа, на который будет производиться копирование ключа, и дождаться завершения операции. На экране появится сообщение об успешном завершении или сообщение об ошибке, например (Рисунок 24).

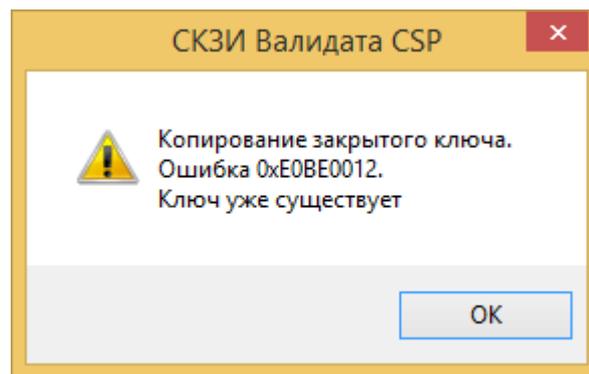


Рисунок 24 – Сообщение об ошибке при копировании ключа

Следует отметить, что доли секрета ключей, сформированных в формате «3 из 6» или «2 из 3», копируются по отдельности.

Примечания

1 Процесс копирования ключа сопровождается запросом пароля ключа (при его наличии).

2 Процесс копирования ключа с vdToken с ПИН-кодом или vdToken (ФКН) сопровождается запросом ПИН-кода. Количество допустимых неуспешных попыток ввода ПИН-кода определяется установленным при форматировании носителя значением (Рисунок 42). При превышении допустимого количества ошибок возникает сообщение о блокировке ПИН-кода. При переустановке носителя блокировка ПИН-кода снимается.

4.1.2 Удаление ключей

Для удаления ключей нажмите кнопку «Удалить». Если инициализация ДСЧ ещё не была выполнена, на экране появятся диалоги инициализации ДСЧ (см.

п. 3.2.1). Затем на экране появится диалог выбора ключей (Рисунок 25). В отличие от остальных операций, при удалении пользователь может выбрать сразу несколько ключей, пользуясь клавишами «Shift» и «Ctrl».

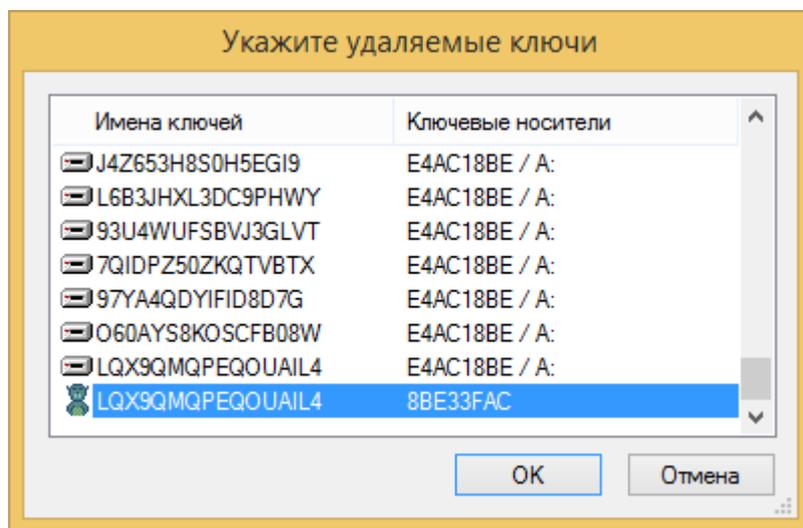


Рисунок 25 – Диалог выбора ключей для удаления

По окончании операции на экране появится сообщение об успешном завершении или сообщение об ошибке. При удалении ключа происходит трёхкратное затирание той части физической памяти носителя, где находился ключ, поэтому операция удаления может продолжаться дольше, чем просто запись ключа.

4.1.3 Смена пароля ключа

Для смены пароля ключа нажмите кнопку «Сменить пароль». Если инициализация ДСЧ ещё не была выполнена, на экране появятся диалоги инициализации ДСЧ (см. п. 3.2.1). Затем на экране появится диалог выбора ключа. Если пользователь выбрал ключ, на который уже был установлен пароль, пользователь должен ввести его, а затем задать новый пароль с подтверждением (см. п. 2.2.2).

Примечание – Смена пароля ключа на носителях с ПИН-кодом сопровождается запросом ПИН-кода.

4.1.4 Преобразование ключа

Функцию преобразования ключа ЭП следует использовать при необходимости копирования этого ключа из одного криптографического провайдера в другой.

Выполнение преобразования возможно только для ключей ЭП, разрешенных для экспорта в зашифрованном виде.

Для преобразования ключа необходимо выбрать из соответствующих списков криптографические провайдеры - источник и приемник. Если включить опцию «Изменить идентификатор закрытого ключа при преобразовании», будет сгенерировано новое имя для преобразованного ключа. Далее следует нажать кнопку «Преобразовать» (кнопка «Преобразовать» становится доступной при выборе допустимого набора параметров).

На экран будет выдан список имен доступных для преобразования ключей. Выберите ключ из списка и нажмите кнопку «ОК». При необходимости введите

пароль для ключа и укажите ключевой носитель для записи преобразованного ключа. Если была установлена опция «Изменить идентификатор закрытого ключа при преобразовании», после выполнения преобразования эта опция и новое имя ключа будут очищены.

4.1.5 Обновление масок ключа

Функцию обновления масок (перегенерации) ключа ЭП следует использовать исключительно для регенерации ключей ЭП квалифицированных сертификатов, сформированных в формате «3 из 6» или «2 из 3». Данную процедуру необходимо применять для возможности использования таких ключей ЭП в течение увеличенного интервала времени (не превышающего максимальный срок действия ключа ЭП, приведенный в документе ВАМБ.00060-06 31 01 «СКЗИ «Валидата CSP» версия 6. Описание применения»).

Для обновления масок ключа ЭП нажмите кнопку «Обновить маски». Если инициализация ДСЧ ещё не была выполнена, на экране появятся диалоги инициализации ДСЧ (см. п. 3.2.1). Затем на экране появится диалог выбора ключа, сформированного в формате «3 из 6» или «2 из 3». Следует загрузить требуемое количество ключей-долей секрета (3 - для ключей, сформированных в формате «3 из 6»; 2 - для ключей, сформированных в формате «2 из 3»), после чего произвести запись обновленных ключей-долей секрета (6 - для ключей, сформированных в формате «3 из 6»; 3 - для ключей, сформированных в формате «2 из 3») на чистые ключевые носители.

4.1.6 Просмотр информации о ключе

Для просмотра информации о ключе нажмите кнопку «Информация». Выберите нужный ключ из списка ключей, находящихся на носителе (Рисунок 26), и нажмите кнопку «ОК».

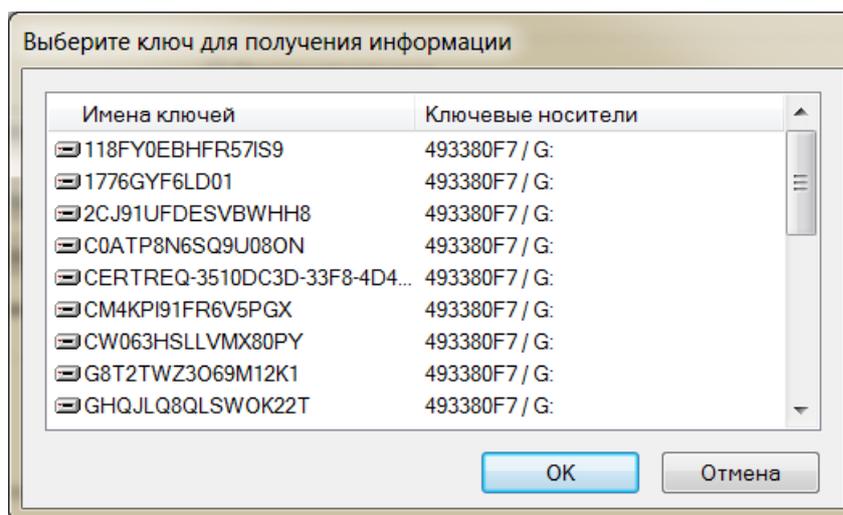


Рисунок 26 – Список ключей

В появившемся окне отображается информация о выбранном ключе (Рисунок 27).

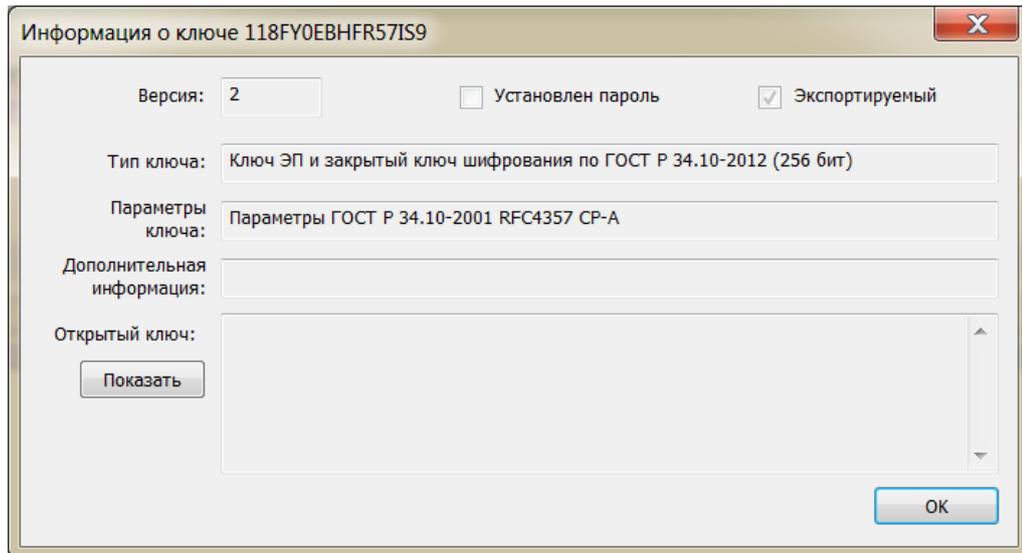


Рисунок 27 – Информация о ключе

Дополнительно можно посмотреть ключ проверки ЭП, соответствующий выбранному ключу ЭП, для чего нужно воспользоваться кнопкой «Показать» (Рисунок 28).

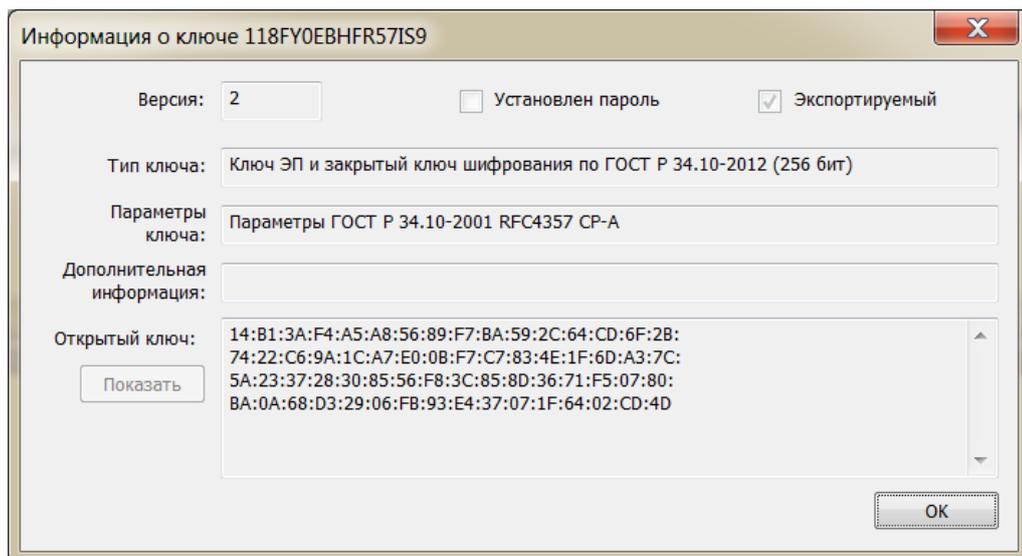


Рисунок 28 – Информация о ключе с отображением ключа проверки ЭП

4.2 Операции с сертификатами

Перейдя на вкладку «Сертификаты», пользователь может выполнять операции по установке сертификатов в различные хранилища (Рисунок 29).

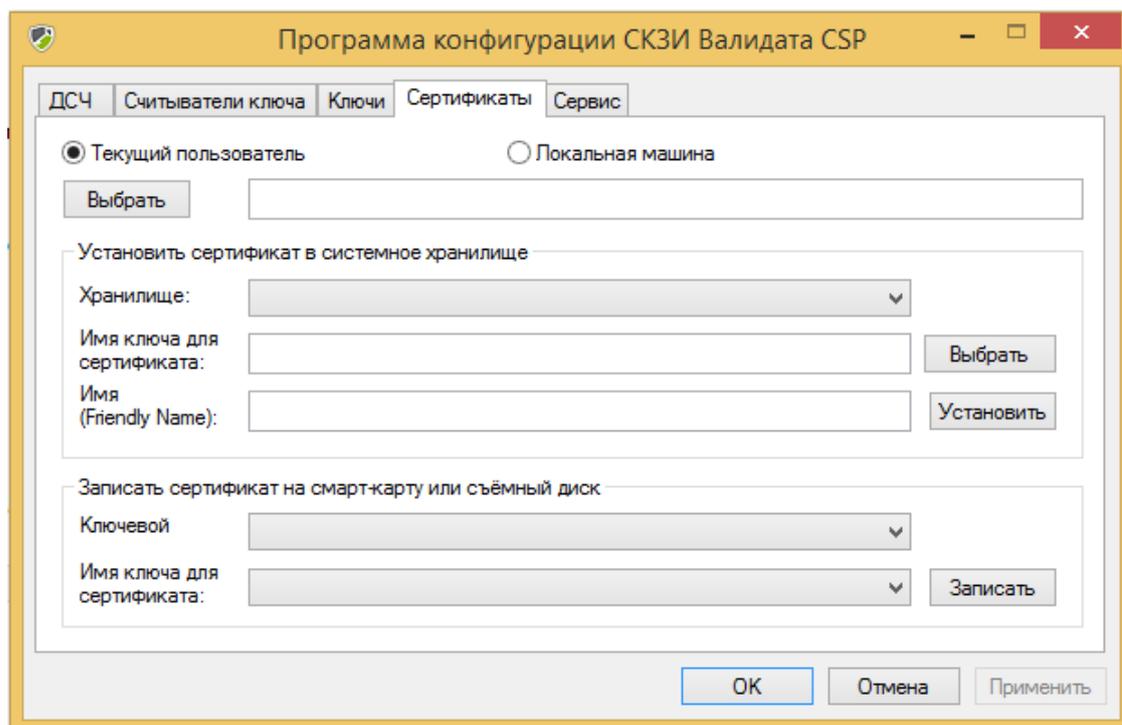


Рисунок 29 – Вкладка «Сертификаты»

4.2.1 Установка сертификата в системное хранилище

Программа конфигурации СКЗИ «Валидата CSP» позволяет помещать сертификат в системное хранилище ОС Windows. Сначала пользователь должен выбрать сертификат, для этого надо нажать кнопку «Выбрать» и в стандартном диалоговом окне выбрать файл сертификата. После этого на экране появится диалог, отображающий выбранный сертификат (Рисунок 30).

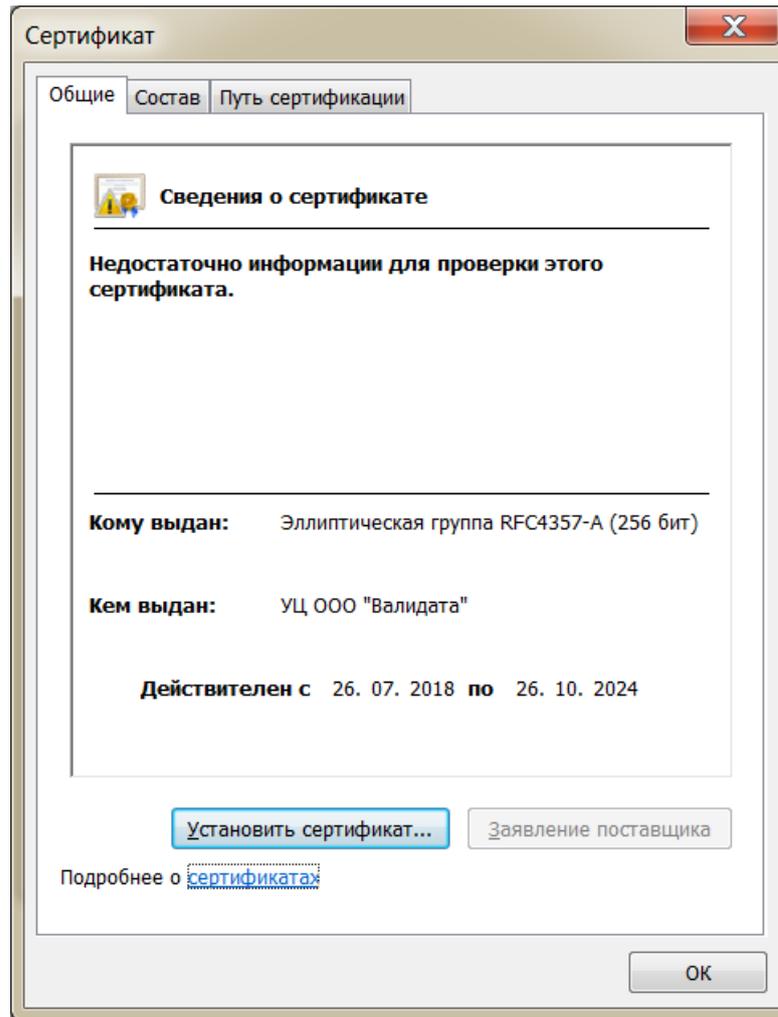


Рисунок 30 - Отображение выбранного сертификата

Программа конфигурации анализирует выбранный сертификат и предлагает системное хранилище, в которое его следует установить. Далее программа пытается извлечь из сертификата имя (идентификатор) соответствующего ключа ЭП. Программа записывает его (если обнаружит) в поле «Имя ключа для сертификата», а извлечённое из сертификата имя владельца - в поле «Имя (Friendly Name)» (Рисунок 31).

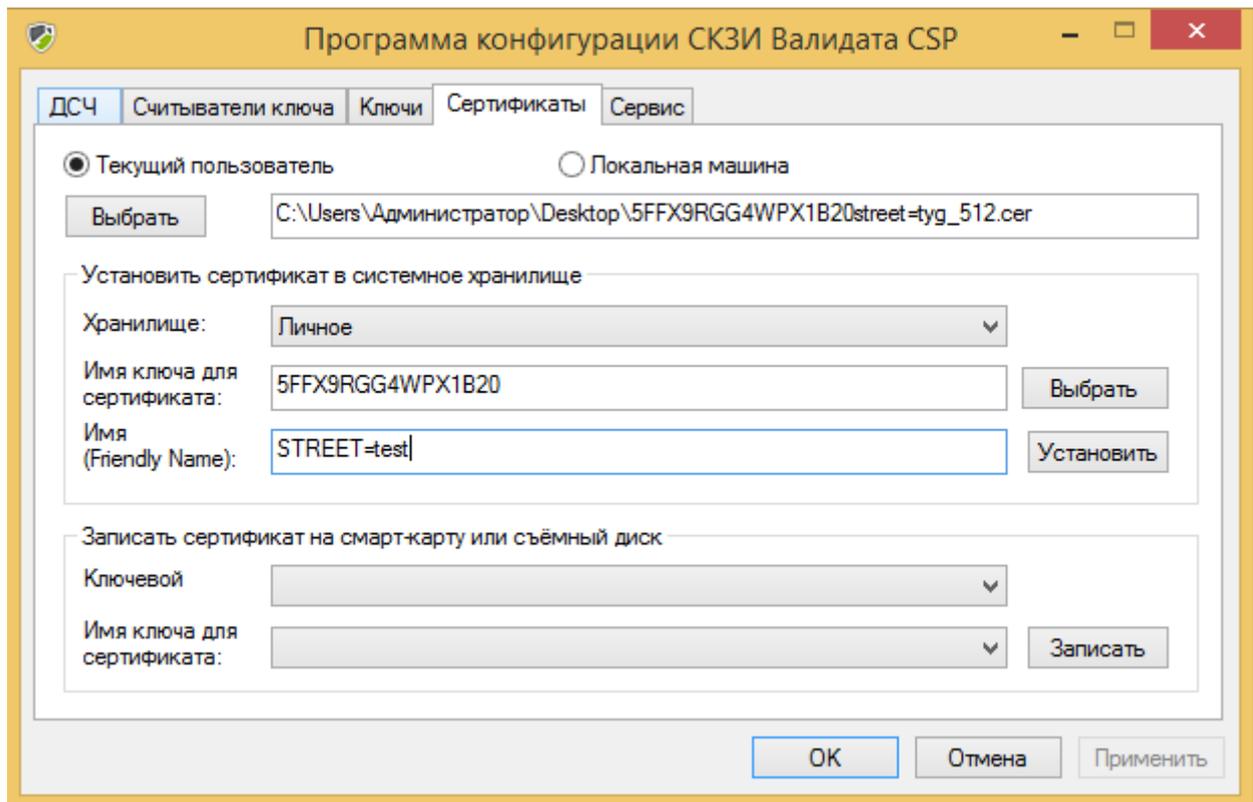


Рисунок 31 – Сертификат выбран

Пользователь может изменить хранилище, в которое следует поместить выбранный сертификат (Рисунок 32).

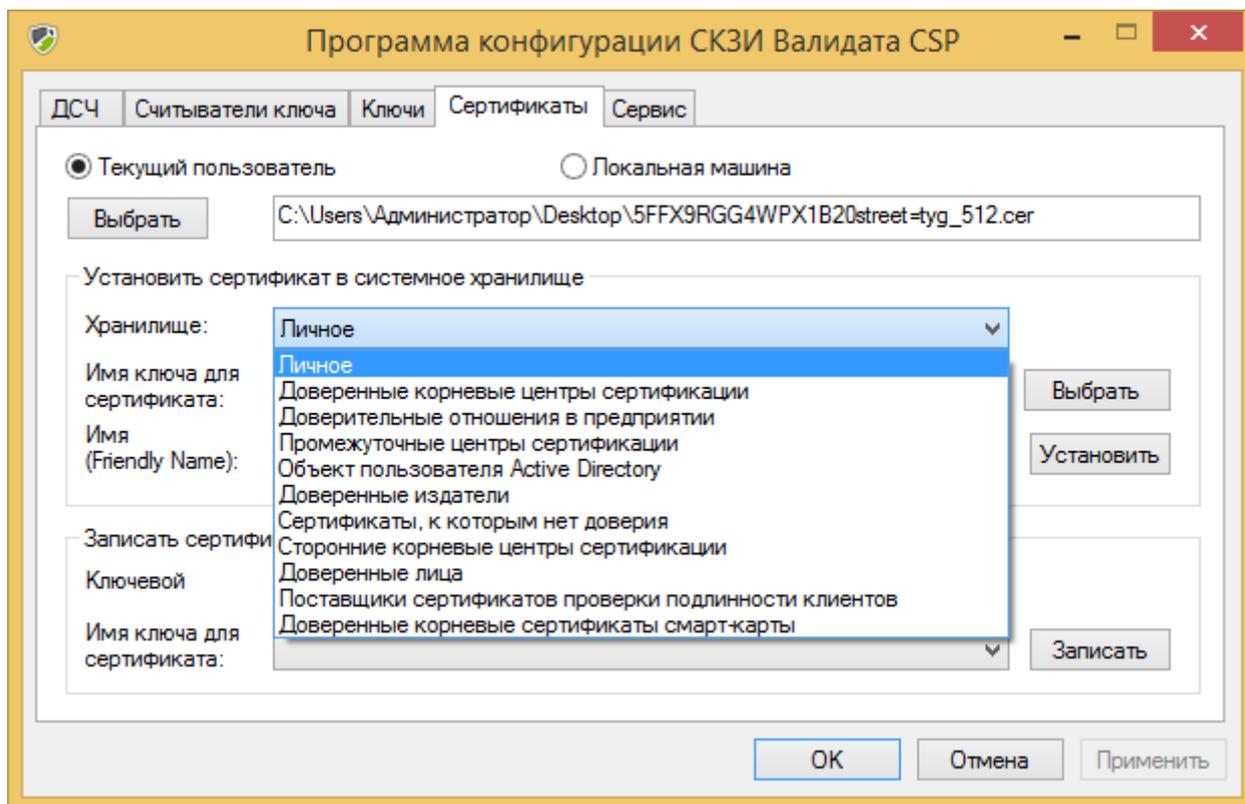


Рисунок 32 – Выбор хранилища для сертификата

Пользователь также может изменить имя (идентификатор) ключа ЭП, который будет привязан к сертификату через свойства (Property) системного хранилища. Для этого следует либо ввести имя вручную, либо выбрать из открывающегося списка. Если привязка ключа ЭП не требуется, пользователь может очистить это поле. Содержимое поля «Имя (Friendly Name)», которое помещается в соответствующее свойство системного хранилища, также может быть отредактировано вручную. Обычный пользователь может помещать сертификаты в системное хранилище только в раздел «Текущий пользователь». Если у пользователя есть соответствующие права, он может помещать сертификаты в раздел «Локальный компьютер». Для этого необходимо перевести переключатель в верхней части вкладки в положение «Локальная машина».

После того, как все параметры заданы, пользователь должен нажать кнопку «Установить». Программа определяет, в какое хранилище должен быть установлен сертификат, запрашивает соответствующий сертификату ключ и помещает сертификат в хранилище. В случае успеха выдаётся сообщение (Рисунок 33).

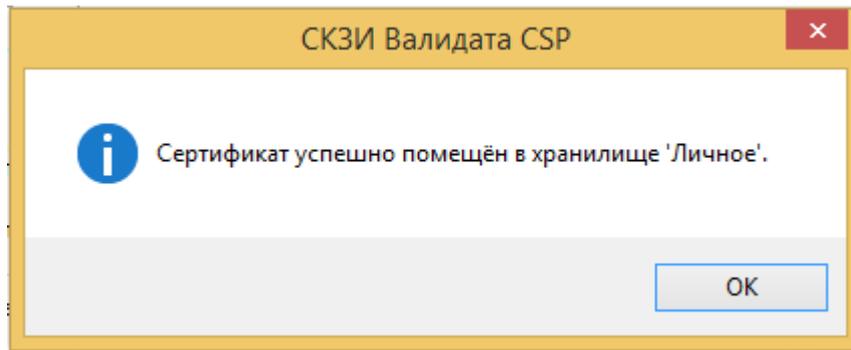


Рисунок 33 – Сообщение об успешном размещении сертификата

4.2.2 Запись сертификата на смарт-карту

Программа конфигурации СКЗИ «Валидата CSP» позволяет записывать сертификат на смарт-карту, на которой находится соответствующий сертификату ключ ЭП. Сначала пользователь должен выбрать сертификат, для этого надо нажать кнопку «Выбрать» и в стандартном диалоговом окне выбрать файл сертификата. После этого на экране появится диалог, отображающий выбранный сертификат. Затем необходимо выбрать смарт-карту из открывающегося списка подключённых к компьютеру смарт-карт (Рисунок 34).

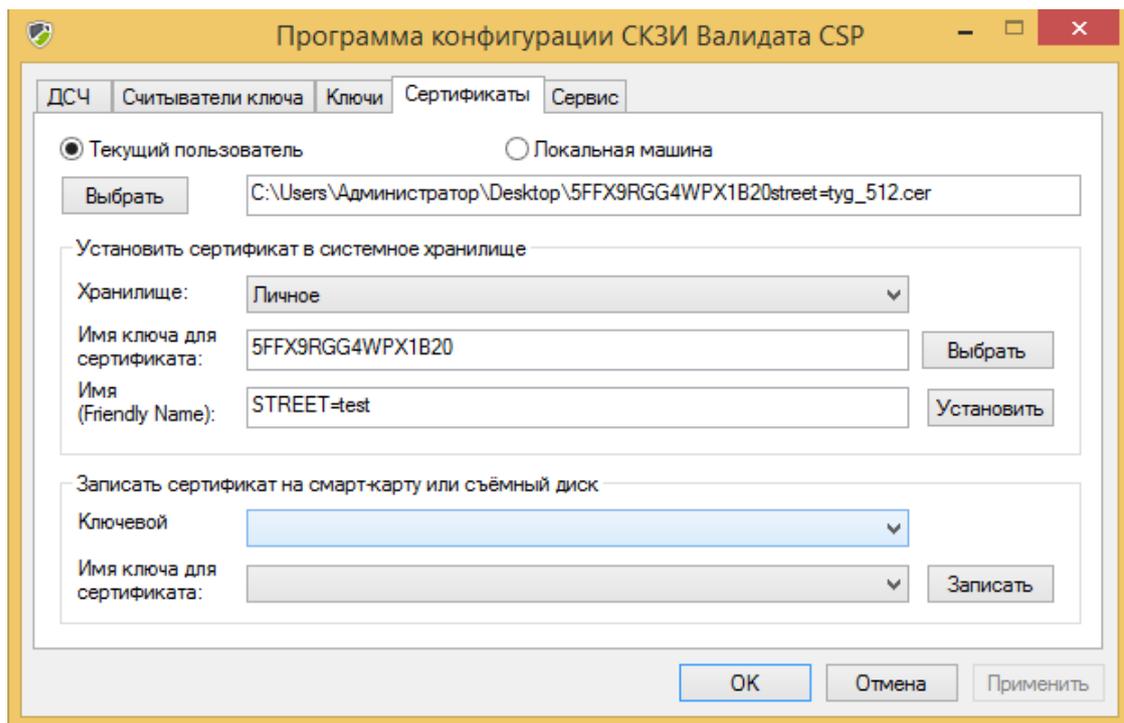


Рисунок 34 – Выбор смарт-карты

Если для выбранного типа смарт-карты не установлен считыватель ключа ЭП, будет выдана ошибка (Рисунок 35).

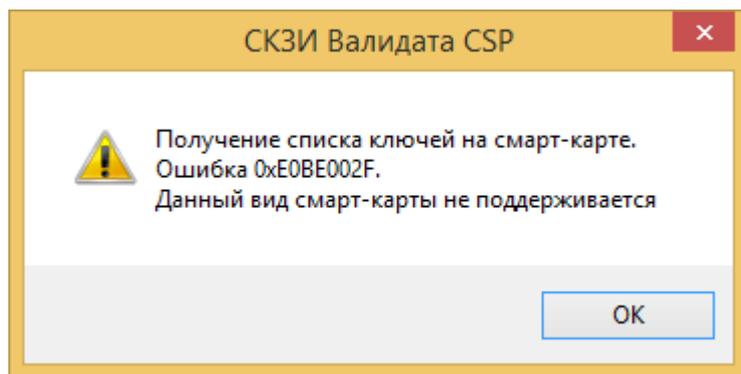


Рисунок 35 – Сообщение о неподдерживаемом типе смарт-карты

Затем следует выбрать из списка ключей ЭП, обнаруженных на смарт-карте, тот ключ, который соответствует записываемому сертификату, и нажать кнопку «Записать». В случае успеха выдаётся сообщение (Рисунок 36).

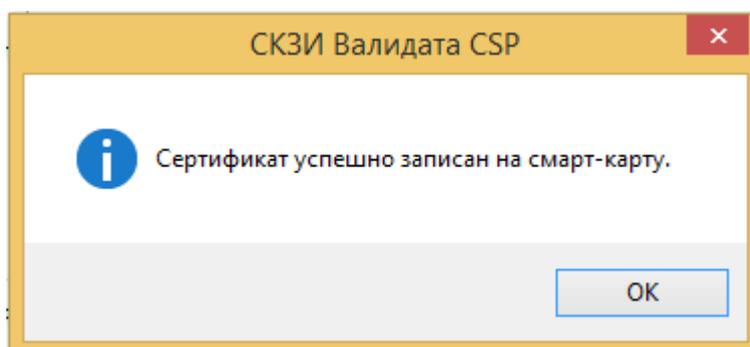


Рисунок 36 – Сообщение об успешной записи сертификата

При использовании смарт-карт с записанными на них сертификатами рекомендуется отключить их автоматическое распространение (т.е. помещение этих сертификатов в системные хранилища ОС Windows). Для этого следует настроить параметры службы «Распространение сертификата» (CertPropSvc) ОС Windows посредством редактирования групповой политики локального компьютера, установив значение параметра «Включить распространение сертификатов со смарт-карты» (находящегося в папке «Конфигурация компьютера»->«Административные шаблоны»->«Компоненты Windows»->«Смарт-карта») в «Отключить».

4.3 Дополнительные операции

Сервисные функции, не имеющие отношения к ключам и сертификатам, реализованы на вкладке «Сервис» программы конфигурации СКЗИ «Валидата CSP» (Рисунок 37).

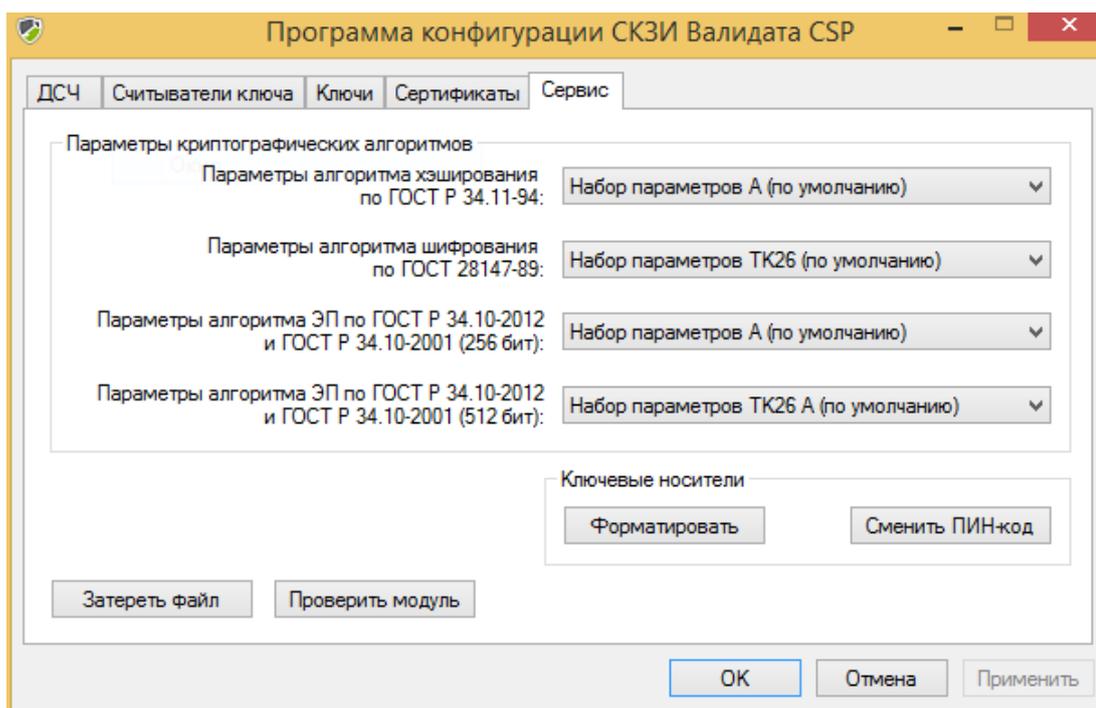


Рисунок 37 – Вкладка «Сервис»

4.3.1 Уничтожение содержимого файла

Для надёжного уничтожения содержимого файла пользователь должен нажать кнопку «Затереть файл» и указать затираемый файл в стандартном диалоге выбора файла. Программа попросит подтверждение (Рисунок 38).

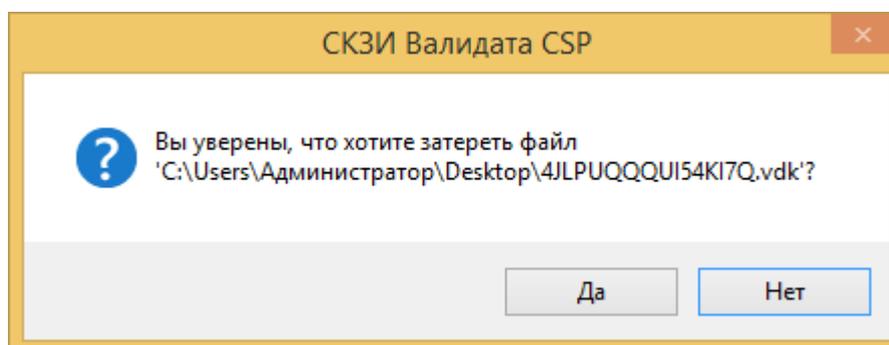


Рисунок 38 – Подтверждение затирания файла

Если пользователь нажмёт кнопку «Да», содержимое файла будет трижды перезаписано, после чего файл будет удалён из файловой системы.

4.3.2 Проверка подписи программных модулей

Во избежание умышленной или случайной подмены все исполняемые модули, входящие в СКЗИ «Валидата CSP», подписаны. Нижеследующие модули, ответственные за выполнение криптографических операций и работу с ключами ЭП, подписаны по ГОСТ Р 34.10-2012 с использованием ключа ЭП разработчика ПО:

- модули криптографических библиотек;

- модуль библиотеки работы с подключаемыми модулями;
- подключаемые модули ДСЧ и считывателей;
- модуль конфигурационной программы.

Остальные модули подписаны с использованием сертификата разработчика, полученного в компании VeriSign, с помощью утилиты Sign Tool (signtool.exe) из состава Microsoft Windows WDK. Проверка ЭП модулей, ответственных за выполнение криптографических операций и работу с ключами ЭП, выполняется автоматически перед их загрузкой, т.е. исполняемый модуль не будет загружен при возникновении ошибки при проверке его ЭП.

При необходимости пользователь может проверить подпись любого модуля ПО, нажав кнопку «Проверить модуль» и выбрав модуль в стандартном диалоге выбора файла. В случае успеха на экран будет выдано сообщение (Рисунок 39). Следует иметь в виду, что при проверке модулей на ОС Windows 7/Server 2008R2, подписанных с использованием алгоритмов RSA и SHA-2, может выдаваться ошибка проверки подписи из-за того, что в указанных устаревших ОС поддержка указанных алгоритмов неполна.

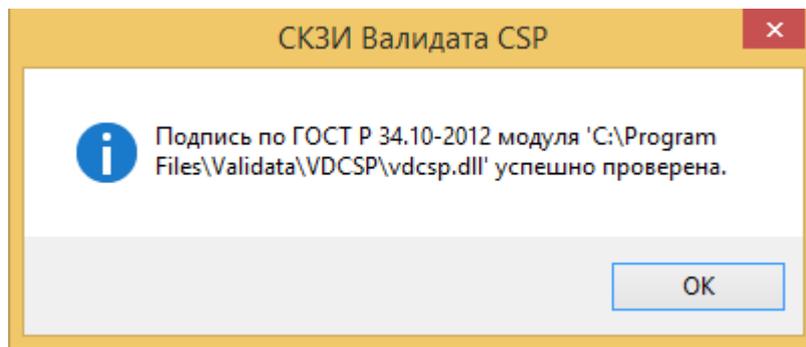


Рисунок 39 – Сообщение об успешной проверке подписи

В противном случае будет выдано сообщение об ошибке, например (Рисунок 40).

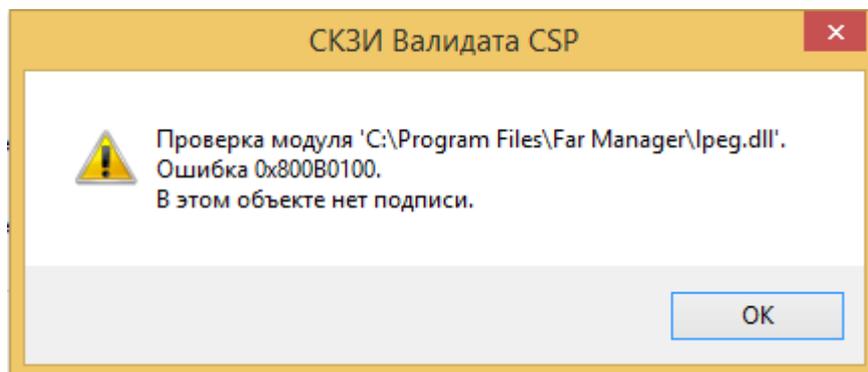


Рисунок 40 – Сообщение об отсутствии подписи в модуле

4.3.3 Форматирование и смена ПИН-кода ключевого носителя

Для подготовки ключевого носителя к работе можно использовать функцию форматирования ключевого носителя. Для этого пользователь должен нажать

кнопку «Форматировать» и указать требуемый считыватель в диалоговом окне выбора считывателей ключа (Рисунок 4).

Далее следует выбрать ключевой носитель для форматирования (Рисунок 41).

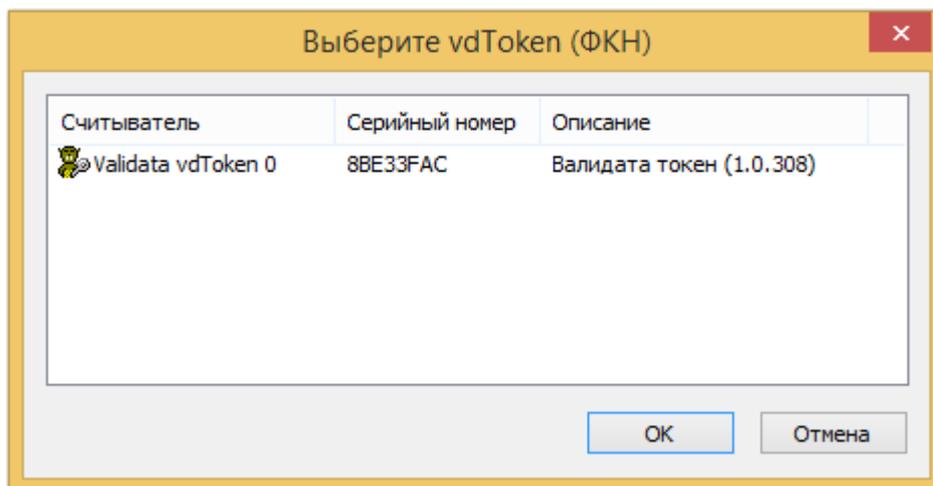


Рисунок 41 – Выбор ключевого носителя

Примечание – В колонке «Считыватель» цифры, указанные после наименования считывателя, являются нумерацией одновременно установленных в компьютер носителей (нумерация начинается с «0»). Нумерация необходима, чтобы носители ключей одинакового типа можно было отличить друг от друга при выполнении операций с ними.

В диалоговом окне ввода параметров форматирования ключевого носителя (Рисунок 42) следует указать требуемые параметры форматирования и нажать кнопку «ОК»:

– параметр «Максимальный размер сертификата» указывает максимальный размер сертификата в DER-кодировке, который можно будет записать на ключевой носитель;

– при включении опции «Работать без ПИН-кода» использование носителя в качестве функционального ключевого носителя (ФКН) будет невозможным.

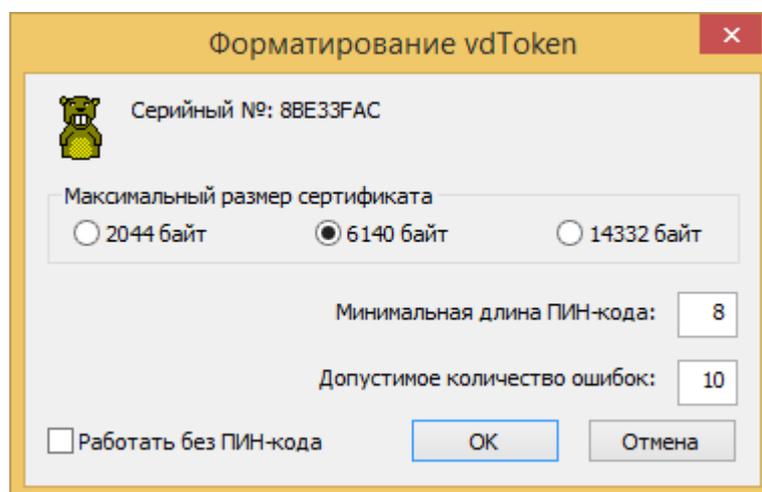


Рисунок 42 – Параметры форматирования

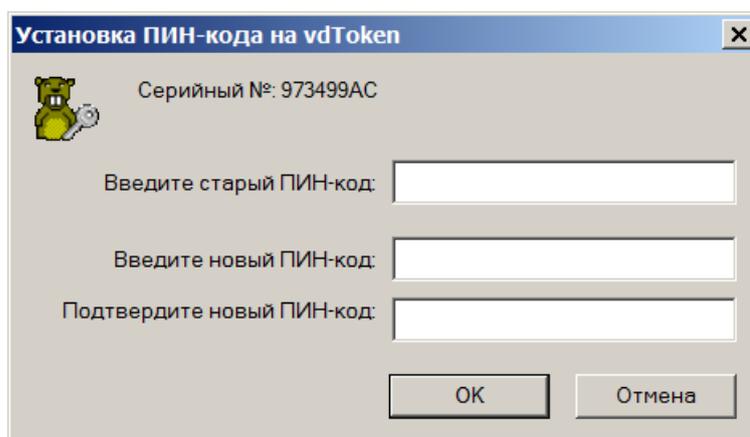
Перед началом процедуры форматирования будет выдано предупреждение о необратимом удалении данных на форматируемом носителе.

В настоящее время функция смены ПИН-кода поддерживается для считывателей vdToken (ФКН) и vdToken.

Для смены ПИН-кода ключевого носителя пользователь должен нажать кнопку «Сменить ПИН-код» и указать требуемый считыватель в диалоговом окне выбора считывателей ключа (Рисунок 4).

Далее следует выбрать ключевой носитель для смены ПИН-кода (Рисунок 41).

В диалоговом окне смены ПИН-кода ключевого носителя (Рисунок 43) следует ввести старый ПИН-код (если он был установлен ранее), ввести два раза новый ПИН-код и нажать кнопку «ОК».



Установка ПИН-кода на vdToken

Серийный №: 973499AC

Введите старый ПИН-код:

Введите новый ПИН-код:

Подтвердите новый ПИН-код:

ОК Отмена

Рисунок 43 – Смена ПИН-кода

5 ГРАФИЧЕСКИЙ ИНТЕРФЕЙС ПОЛЬЗОВАТЕЛЯ СЕРВИСОВ

Программный модуль «Графический Интерфейс Пользователя Сервисов» (далее — ПМ ГИПС), входящий в состав СКЗИ «Валидата CSP», предназначен для вывода на экран некоторых диалоговых окон СКЗИ «Валидата CSP» от процессов, запущенных как сервис (служба) с правами системной учётной записи. В ОС Windows 10 вывод диалоговых окон сервисов (служб) напрямую невозможен.

ПМ ГИПС является сервером именованного канала (Named Pipe), запускается автоматически после аутентификации пользователя; его можно запустить вручную по имени исполняемого файла: `gips.exe`. Два экземпляра ПМ ГИПС не могут быть запущены одновременно, кроме того, ПМ ГИПС запускается только локально (в «физической» консоли). После запуска иконка ГИПС должна появиться в области уведомлений (Рисунок 44).



Рисунок 44 – Область уведомлений с иконкой ПМ ГИПС

Если иконка не видна, её можно настроить с помощью пункта «Настройка значков уведомлений» контекстного меню области уведомлений, как показано ниже (Рисунок 45).

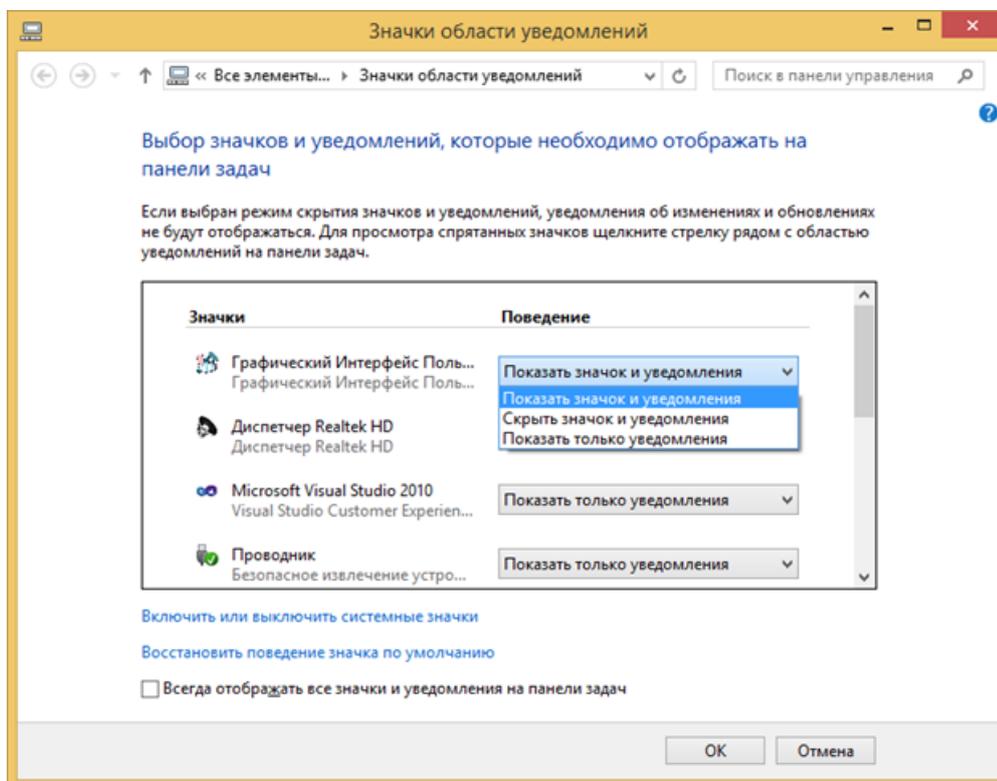


Рисунок 45 – Настройка отображения иконки ПМ ГИПС

Щелчком правой кнопки «мыши» по иконке ПМ ГИПС вызывается контекстное меню (Рисунок 46).

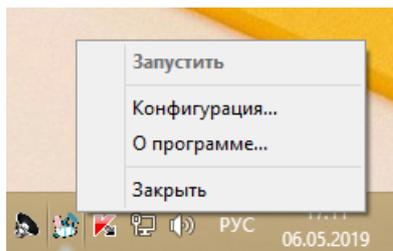


Рисунок 46 – Контекстное меню ПМ ГИПС

Чтобы закрыть ПМ ГИПС, выберите пункт меню «Закреть».

Пункт меню «Запустить» становится активным только при остановке ПМ ГИПС в результате ошибки и используется для возобновления работы ПМ ГИПС.

При выборе пункта «О программе» контекстного меню на экране появляется диалоговое окно с информацией о текущей версии ПМ ГИПС (Рисунок 47).

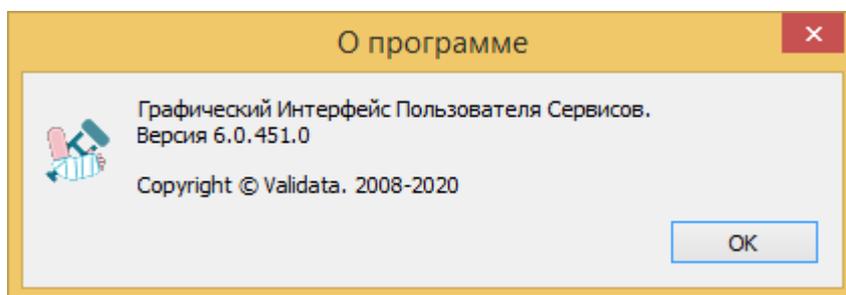


Рисунок 47 – Диалоговое окно «О программе»

Чтобы посмотреть и/или изменить конфигурационные настройки выберите пункт меню «Конфигурация». В диалоговом окне конфигурации (Рисунок 48):

- параметр «Таймаут клиента» (значение по умолчанию – 1000 миллисекунд) – устанавливает время, которое даётся клиентам ПМ ГИПС на установление соединения по именованному каналу;

- параметр «Таймаут сервера» (значение по умолчанию – 1000 миллисекунд) – устанавливает время, которое даётся серверу ПМ ГИПС на выполнение асинхронной операции с именованным каналом;

- опции «Протоколировать ошибки», «Протоколировать предупреждения» и «Протоколировать события» определяют уровни информационных сообщений, протоколируемых в журнале приложений Windows. В качестве источника события указывается «GIPS».

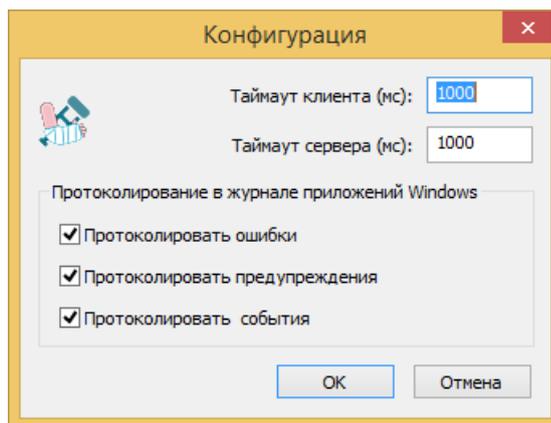


Рисунок 48 – Диалоговое окно «Конфигурация»

Пример записи ошибки ПМ ГИПС приведён ниже (Рисунок 49).

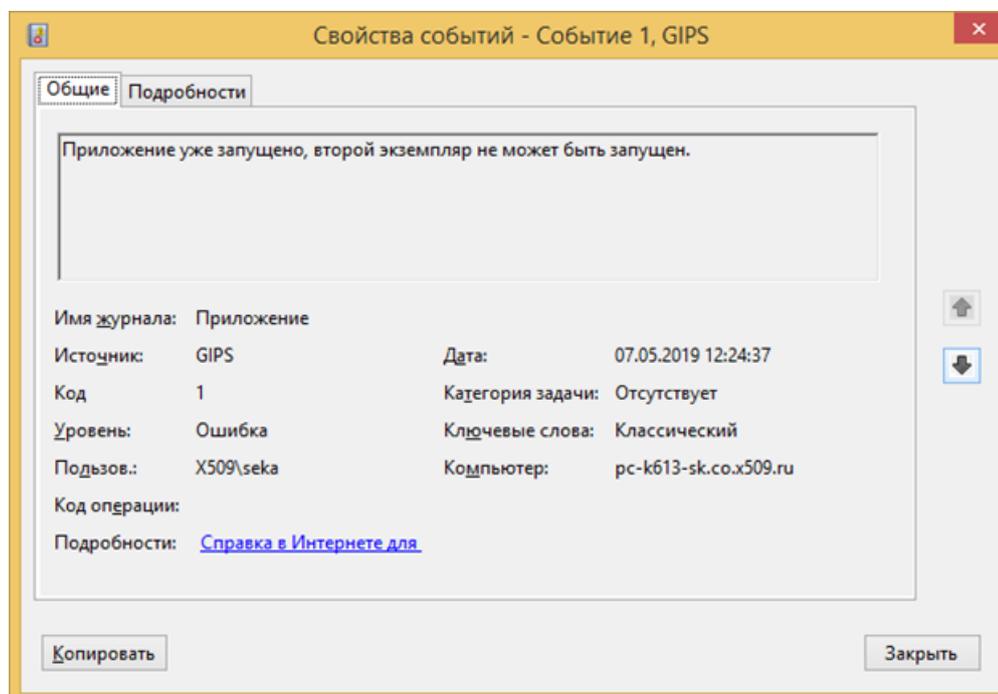


Рисунок 49 – Пример записи ошибки в журнале приложений Windows

Когда из системного сервиса происходит попытка вызова диалогов доступа к ключевым носителям, СКЗИ «Валидата CSP» проверяет значение параметра **UseGIPS** ключа реестра **HKEY_LOCAL_MACHINE\SOFTWARE\Validata\VDCSP**. Если параметр отсутствует или значение параметра нулевое, происходит попытка отобразить диалог стандартным образом, что может привести к «зависанию» сервиса (в зависимости от версии и настроек Windows). Если значение параметра ненулевое, СКЗИ «Валидата CSP» обращается к ПМ ГИПС через именованный канал. Право доступа к этому каналу есть только у сервисов, запущенных от имени LocalSystem, LocalService и NetworkService. В случае успешного соединения СКЗИ «Валидата CSP» передаёт в ПМ ГИПС параметры требуемого диалогового окна, а ПМ ГИПС отображает его на экране (Рисунок 50).

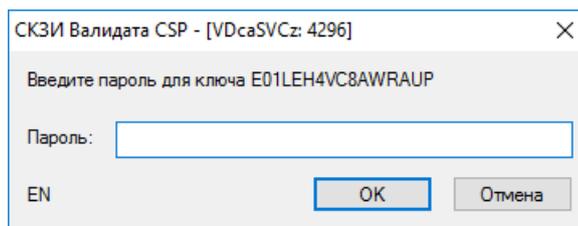


Рисунок 50 - Пример отображения диалогового окна

В заголовке в квадратных скобках указывается имя сервиса и идентификатор процесса, из которого вызван диалог.

Если пользователь не закрыл диалог в течение 600 секунд, он будет закрыт принудительно, вызвавший его сервис получит ошибку. Время ожидания можно изменить, создав в ключе реестра **HKEY_LOCAL_MACHINE\SOFTWARE\Validata\VDCSP** параметр **GipsClientTimeout** типа REG_DWORD и задав в нём количество миллисекунд. Пока на экране отображается диалог, выданный ПМ ГИПС, попытка отобразить через ПМ ГИПС другой диалог вернёт ошибку вызывающему сервису.

6 ПРОГРАММНЫЙ МОДУЛЬ ПОДДЕРЖКИ TLS

Назначение программного модуля поддержки TLS и особенности использования файлового кэша для повторной загрузки объектов приведены в документе ВАМБ.00060-06 31 01 «СКЗИ «Валидата CSP» версия 6. Описание применения».

6.1 Использование Internet Information Server (IIS) с модулем поддержки TLS

Перед началом использования Microsoft Internet Information Server (IIS) совместно с программным модулем поддержки TLS криптопровайдера СКЗИ «Валидата CSP» необходимо поместить все требуемые сертификаты и списки аннулированных сертификатов (САС) в системное хранилище сертификатов локального компьютера. Для этого необходимо выполнить следующие шаги:

- загрузить корневой(ые) сертификат(ы) Центра сертификации (ЦС) и соответствующие ему (им) САС(ы) в системное хранилище корневых сертификатов ЦС локального компьютера посредством использования оснастки Сертификаты консоли управления Microsoft (Microsoft Management Console, MMC);

- загрузить промежуточный(ые) сертификат(ы) ЦС и соответствующие ему (им) САС(ы) в системное хранилище промежуточных сертификатов ЦС локального компьютера посредством использования оснастки Сертификаты консоли управления Microsoft (Microsoft Management Console, MMC);

- загрузить сертификат Web-сервера IIS с одновременной привязкой его к контейнеру с соответствующим ключом ЭП в системное хранилище личных сертификатов локального компьютера посредством использования конфигурационной программы СКЗИ «Валидата CSP». При выдаче сертификата Web-сервера IIS необходимо учесть, что в нем должен присутствовать OID Проверки подлинности сервера (1.3.6.1.5.5.7.3.1) и должно быть указано разрешённое использование ключа ЭП (Key Usage) для выполнения ЭП и шифрования. Дополнительно, DNS-имя Web-сервера должно быть прописано в атрибуте CN X.500-имени владельца (Subject Name) и в альтернативном имени владельца (Subject Alternative Name) сертификата Web-сервера.

Далее необходимо настроить Web-сервер IIS на использование установленного сертификата. Для этого необходимо вызвать пункт меню «Пуск»→«Программы»→«Администрирование»→«Диспетчер служб IIS» и, подсветив нужный Web-сайт правой кнопкой «мыши», выбрать пункт меню «Свойства». После этого необходимо выбрать вкладку «Безопасность каталога» и нажать на кнопку «Сертификат» группы «Безопасные подключения» (Рисунок 51).

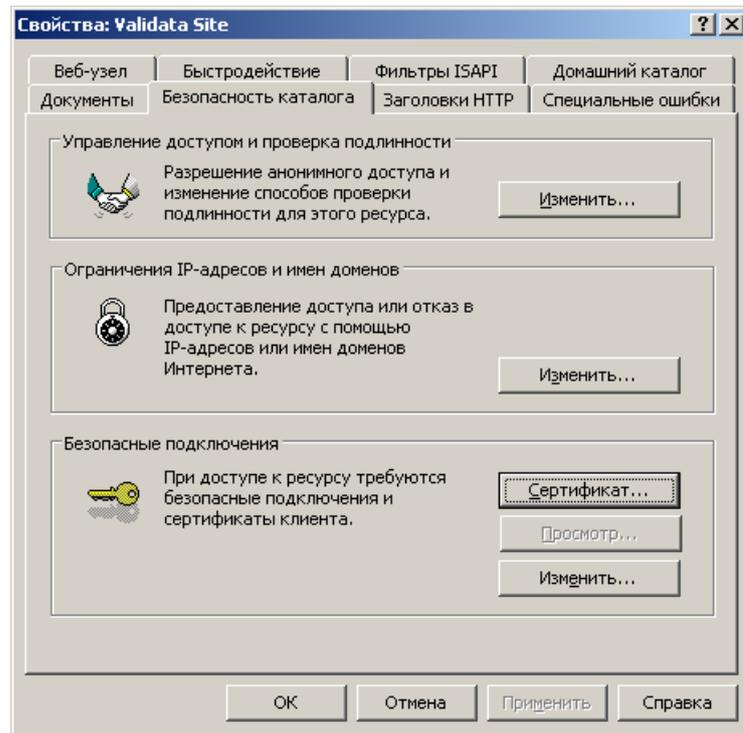


Рисунок 51 – Диалог безопасности каталога

В появившемся диалоге необходимо выбрать пункт «Назначение существующего сертификата» и нажать кнопку «Далее». На экран будет выдан диалог выбора сертификата для Web-сервера IIS (Рисунок 52).

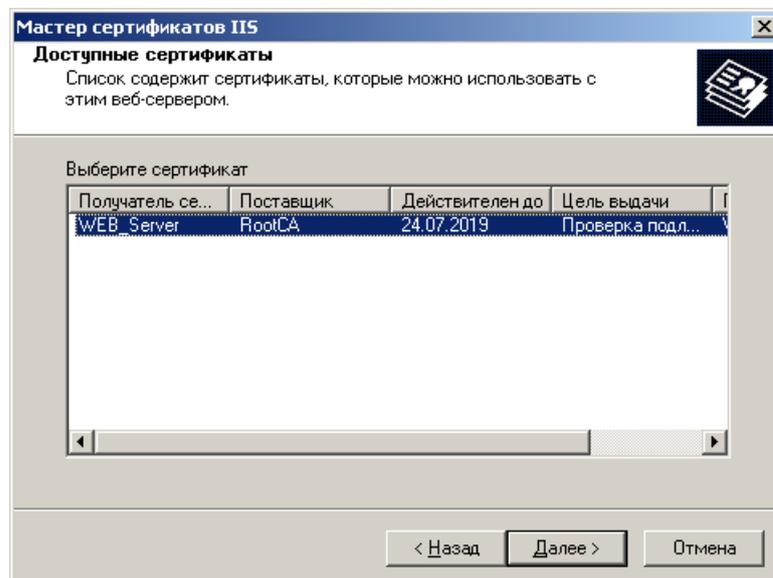


Рисунок 52 – Диалог выбора сертификата

Выбрав нужный сертификат, необходимо нажать кнопку «Далее» на этом и следующем диалогах, а в конце нажать на кнопку «Готово».

По умолчанию Web-сервер IIS не требует наличия сертификатов у клиентов и, соответственно, не проводит проверку подлинности клиентов на основании их сертификатов. Для включения проверки подлинности клиентов необходимо

в диалоге безопасности каталога нажать на кнопку «Изменить» группы «Безопасные подключения» (Рисунок 53).

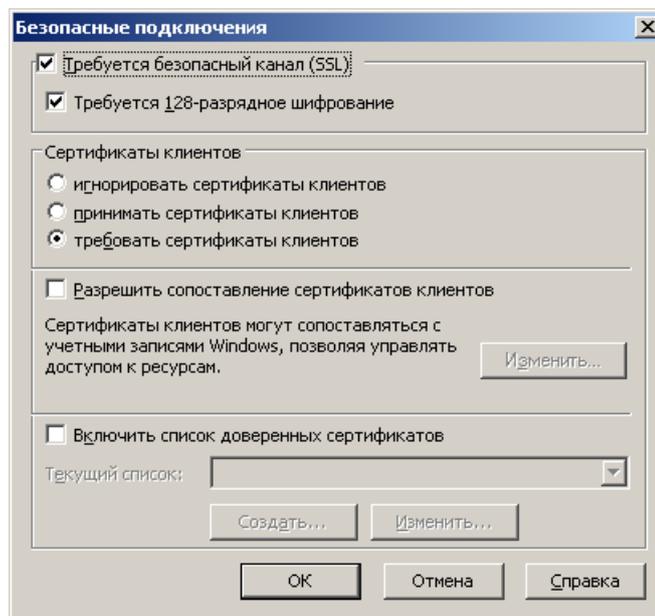


Рисунок 53 - Диалог подключений

Далее в диалоге подключений необходимо включить свойство «Требуется безопасный канал (SSL)», установить переключатель «Сертификаты клиентов» в положение «требовать сертификаты клиентов» и нажать на кнопку «ОК».

Для правильной работы Web-сервера IIS совместно с модулем поддержки TLS необходимо выполнение следующих требований:

- у ключа ЭП Web-сервера IIS должен отсутствовать пароль и/или ПИН-код;
- при использовании биологического ДСЧ (или любого другого ДСЧ, требующего отображения графического интерфейса при инициализации) последний должен быть проинициализирован перед использованием Web-сервера IIS;
- носитель с ключом ЭП Web-сервера IIS должен быть смонтирован перед использованием Web-сервера IIS.

6.2 Использование Microsoft Internet Explorer с модулем поддержки TLS

Перед началом использования Microsoft Internet Explorer (IE) совместно с программным модулем поддержки TLS криптопровайдера СКЗИ «Валидата CSP» необходимо поместить все требуемые сертификаты и САС в системное хранилище сертификатов пользователя. Для этого необходимо выполнить следующие шаги:

- загрузить корневой(ые) сертификат(ы) ЦС и соответствующие ему (им) САС(ы) в системное хранилище корневых сертификатов ЦС пользователя посредством использования оснастки Сертификаты консоли управления Microsoft (Microsoft Management Console, MMC);

– загрузить промежуточный(ые) сертификат(ы) ЦС и соответствующие ему (им) САС(ы) в системное хранилище промежуточных сертификатов ЦС пользователя посредством использования оснастки Сертификаты консоли управления Microsoft (Microsoft Management Console, MMC);

– загрузить сертификат клиента с одновременной привязкой его к контейнеру с соответствующим ключом ЭП в системное хранилище личных сертификатов пользователя посредством использования программы конфигурации СКЗИ «Валидата CSP». При выдаче сертификата клиента необходимо учесть, что в нем должен присутствовать OID Проверки подлинности клиента (1.3.6.1.5.5.7.3.2).

Запускать программу TLS монитора специально не требуется, так как модуль поддержки TLS будет автоматически определять алгоритм ключа проверки ЭП сертификата Web-сайта и, в зависимости от этого алгоритма, вырабатывать ключи шифрования для защиты канала.

6.3 Использование Terminal Services с модулем поддержки TLS

Для настройки службы терминалов в ОС Windows Server (начиная с 2012 R2) следует пользоваться специальным командным файлом, настраивающим службу терминалов через инструментарий управления Windows (Windows Management Instrumentation, WMI).

Для начала следует определить так называемый отпечаток (Thumbprint) сертификата терминального сервера, который состоит из двадцати байт. Для этого следует, используя MMC, просмотреть свойства сертификата терминального сервера и скопировать его отпечаток (в виде строки, состоящей из пар шестнадцатиричных цифр, разделенных пробелами) в текстовый редактор (например, Notepad). Далее в копии строки с отпечатком следует удалить пробелы и скопировать получившуюся строку в приведенный ниже шаблон командного файла, заменив ей строку xxx:

```
@echo off

set WMIC=%WINDIR%\system32\Wbem\wmic.exe

echo.

%WMIC% /NAMESPACE:\\root\CIMV2\TerminalServices PATH
Win32_TSGeneralSetting SET MinEncryptionLevel="3"
%WMIC% /NAMESPACE:\\root\CIMV2\TerminalServices PATH
Win32_TSGeneralSetting SET SecurityLayer="2"
%WMIC% /NAMESPACE:\\root\CIMV2\TerminalServices PATH
Win32_TSGeneralSetting SET SSLCertificateSHA1Hash="
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"

echo.

%WMIC% /NAMESPACE:\\root\CIMV2\TerminalServices PATH
Win32_TSGeneralSetting GET MinEncryptionLevel
```

```
%WMIC% /NAMESPACE:\\root\CIMV2\TerminalServices PATH  
Win32_TSGeneralSetting GET SecurityLayer  
%WMIC% /NAMESPACE:\\root\CIMV2\TerminalServices PATH  
Win32_TSGeneralSetting GET SSLCertificateSHA1Hash
```

Для завершения процедуры настройки следует выполнить получившийся командный файл и перезагрузить терминальный сервер.

6.4 Использование Terminal Services Gateway с модулем поддержки TLS

Перед началом использования Terminal Services Gateway (TS Gateway, шлюза служб терминалов) совместно с программным модулем поддержки TLS криптопровайдера СКЗИ «Валидата CSP» необходимо поместить все требуемые сертификаты и САС в системное хранилище сертификатов локального компьютера - также, как это описано для Internet Information Server (IIS) в подразделе 6.1.

Далее необходимо настроить шлюз служб терминалов на использование установленного сертификата. Для этого необходимо вызвать пункт меню «Пуск» → «Администрирование» → «Службы удаленных рабочих столов» → «Диспетчер шлюза удаленных рабочих столов», найти требуемый шлюз и, щелкнув по нему левой кнопкой «мыши», выбрать пункт меню «Свойства». Далее следует выбрать вкладку «Сертификат SSL» (Рисунок 54).

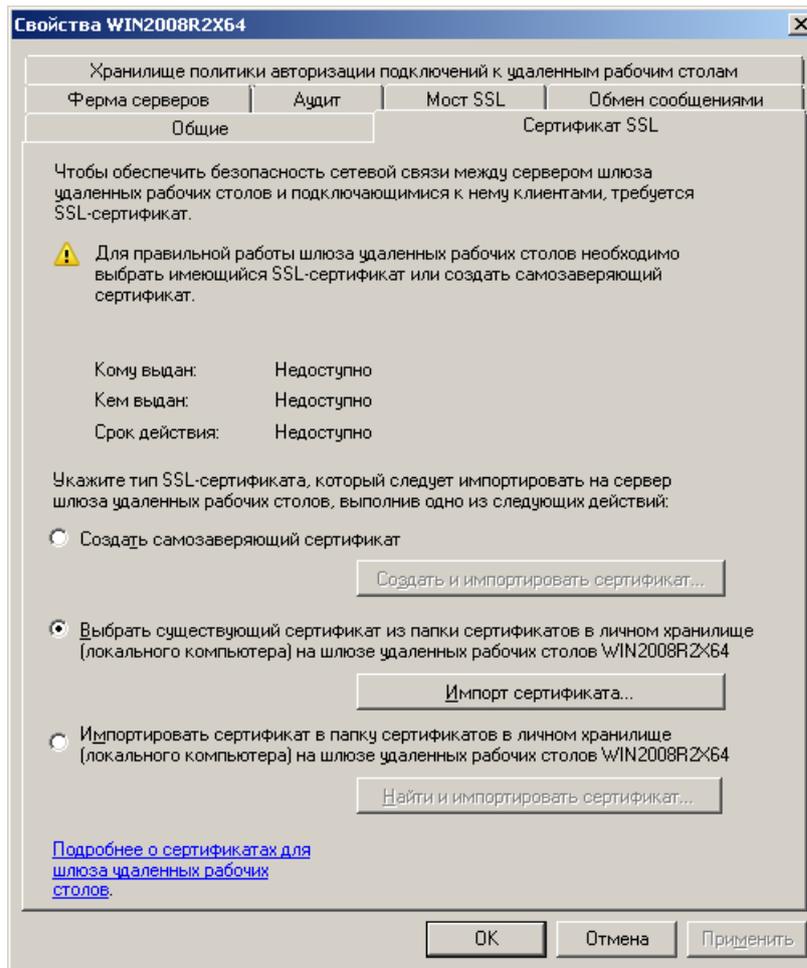


Рисунок 54 – Диалог свойств шлюза

После этого необходимо выбрать сертификат шлюза служб терминалов, нажав кнопку «Импорт сертификата» (Рисунок 55).

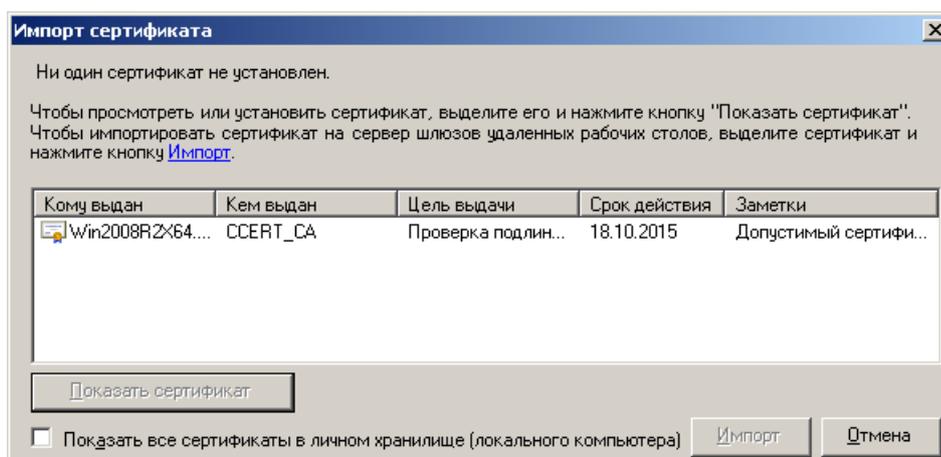


Рисунок 55 – Диалог выбора сертификата

Выбрав нужный сертификат, необходимо нажать кнопку «Импорт» и кнопку «ОК» на родительском диалоге.

Каждый шлюз служб терминалов позволяет различным пользователям подключаться к различным защищаемым данным шлюзом ресурсам (серверам терминалов). Нижеследующие политики безопасности шлюза служб терминалов позволяют гибко регламентировать подключения пользователей к защищаемым ресурсам (серверам терминалов):

– Политики авторизации подключений - данные политики позволяют указать разрешённые методы проверки подлинности Windows (пароль и/или смарт-карта) для каждого конкретного пользователя или группы пользователей;

– Политики авторизации ресурсов - данные политики позволяют указать конкретных пользователей или группы пользователей, которым разрешено подключаться к каждому конкретному защищаемому ресурсу (серверу терминалов).

Детальное руководство по настройке шлюза служб терминалов приведено (на русском языке) по ссылке [http://technet.microsoft.com/ru-ru/library/cc771530\(WS.10\).aspx](http://technet.microsoft.com/ru-ru/library/cc771530(WS.10).aspx).

Для правильной работы шлюза служб терминалов совместно с модулем поддержки TLS необходимо выполнение тех же требований к ключу ЭП шлюза служб терминалов и к состоянию инициализации ДСЧ, что приведены для Internet Information Server (IIS) в подразделе 6.1.

6.5 Использование Remote Desktop Client с модулем поддержки TLS

Перед началом использования Remote Desktop Client (RDC) совместно с программным модулем поддержки TLS криптопровайдера СКЗИ «Валидата CSP» необходимо поместить все требуемые сертификаты и САС в системное хранилище сертификатов пользователя - так же, как это описано для Microsoft Internet Explorer (IE) в подразделе 6.2.

После запуска RDC (программы MSTsc.exe) на экран будет выдано главное диалоговое окно программы (Рисунок 56) . Для возможности выполнения расширенной настройки нажмите кнопку «Параметры».

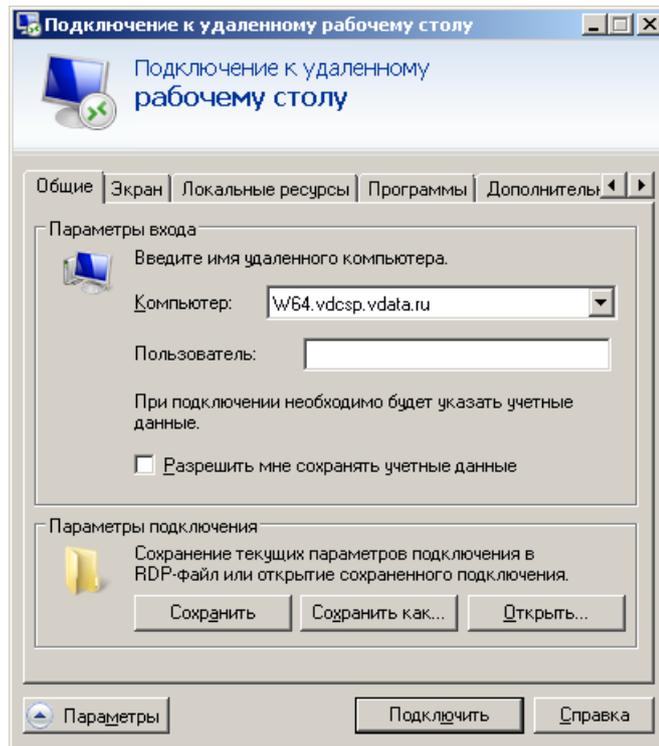


Рисунок 56 – Главное окно программы

Для ввода имени удаленного сервера терминалов используйте поле ввода «Компьютер». При необходимости, укажите имя шлюза служб терминалов, выбрав вкладку «Подключение» и нажав кнопку «Параметры...». В появившемся окне установите переключатель в положение «Использовать следующие параметры сервера шлюза удаленных рабочих столов» и введите имя шлюза служб терминалов в поле «Имя сервера» (Рисунок 57).

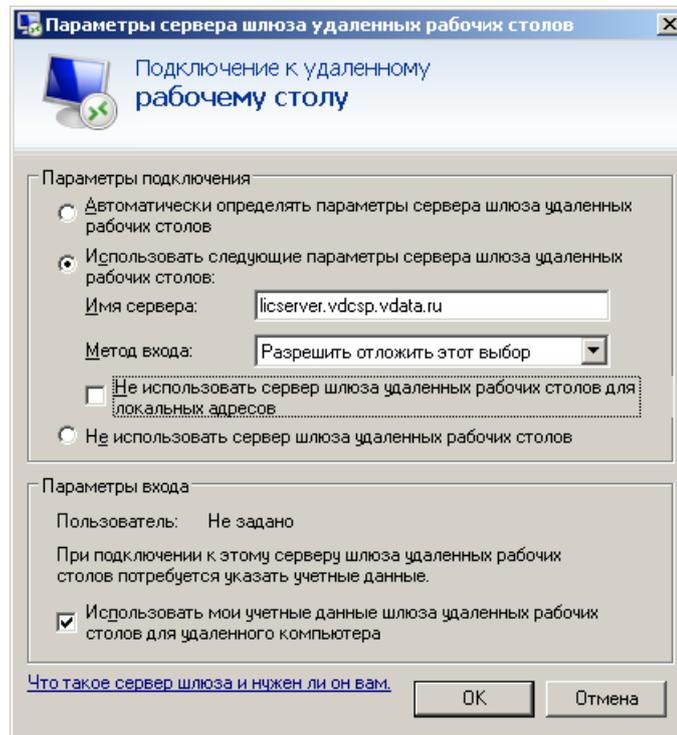


Рисунок 57 – Диалог ввода имени шлюза служб терминалов

После выполнения настройки необходимо нажать на кнопку «Подключить» для подключения к серверу терминалов.

Если свойство «Использовать мои учетные данные шлюза удаленных рабочих столов для удаленного компьютера» включено и подключение выполняется через шлюз служб терминалов, то учетные данные пользователя (имя пользователя и его пароль или ПИН-код смарт-карты) будут запрашиваться только один раз. Если же это свойство выключено и подключение выполняется через шлюз служб терминалов, то учетные данные пользователя будут запрашиваться дважды - первый раз для шлюза служб терминалов, а второй - для терминального сервера.

6.6 Использование протокола Kerberos PKInit с модулем поддержки TLS

Программный модуль поддержки TLS криптопровайдера СКЗИ «Валидата CSP» поддерживает аутентификацию пользователей по протоколу Kerberos PKInit в двух режимах: локальном и удаленном. В первом случае выполняется аутентификация непосредственно во время входа пользователя на рабочую станцию или сервер через Windows Login Screen. Во втором случае выполняется аутентификация пользователя в терминальной сессии при подключении через Remote Desktop Client по протоколу RDP.

Аутентификация пользователя выполняется одним из контроллеров домена на основании ключа ЭП пользователя и соответствующего ему сертификата. Ключ ЭП пользователя и его сертификат должны находиться на ключевом носителе типа смарт-карта (например, eToken или ruToken), поэтому такой процесс аутентификации пользователя называют «Входом со смарт-картой». Дополнительно, копия сертификата пользователя должна находиться в системном хра-

нилище личных сертификатов пользователя и быть привязана к ключу ЭП последнего.

Каждый контроллер домена, в котором пользователи используют протокол Kerberos PKInit для аутентификации, также должен иметь сертификат с соответствующим ему и привязанным к нему ключом ЭП, расположенный в системном хранилище личных сертификатов локального компьютера. При этом к контроллеру домена предъявляются следующие требования:

- у ключа ЭП сертификата контроллера домена должен отсутствовать пароль и/или ПИН-код;

- при использовании биологического ДСЧ (или любого другого ДСЧ, требующего отображения графического интерфейса при инициализации) последний должен быть проинициализирован перед тем, как пользователи начнут попытки входа со смарт-картой;

- носитель с ключом ЭП контроллера домена должен быть смонтирован перед тем, как пользователи начнут попытки входа со смарт-картой.

На рабочих станциях пользователей, на терминальных серверах и на шлюзах терминальных серверов, а также на контроллерах домена, в котором пользователи используют протокол Kerberos PKInit для аутентификации, должно быть установлено ПО поддержки (драйверы устройств и библиотеки) используемых ключевых носителей типа смарт-карта, а также библиотеки поддержки соответствующих ключевых носителей из состава СКЗИ «Валидата CSP».

В начале выполнения процесса аутентификации пользователя пакет безопасности Kerberos посылает в службу распространения ключей (Key Distribution Center, KDC), находящуюся на контроллере домена, первоначальный запрос на аутентификацию KRB_AS_REQ. Данный запрос содержит Имя участника-пользователя (User Principal Name, UPN), метку времени и их ЭП, вычисленную на ключе ЭП пользователя, а также сертификат пользователя. При получении запроса контроллер домена (KDC) проверяет ЭП запроса и подлинность сертификата пользователя. После успешного проведения проверок KDC подготавливает ответ KRB_AS_REP, содержащий зашифрованный сессионный ключ пользователя для обмена данными с KDC, и билет (Ticket Granting Ticket, TGT). Поскольку сессионный ключ зашифрован на ключе проверки ЭП из сертификата пользователя, только пользователь может его расшифровать с помощью своего ключа ЭП.

Для возможности выполнения начальной аутентификации по протоколу Kerberos PKInit сертификат пользователя должен удовлетворять следующим условиям:

- в сертификате пользователя должна быть указана функционирующая точка распространения САС (CRL Distribution Point);

- в сертификате пользователя должно быть указано разрешённое использование ключа ЭП (Key Usage) для выполнения ЭП и шифрования;

- в сертификате пользователя базовые ограничения (Basic Constraints) не должны содержать признак сертификата ЦС, и ограничение на длину пути должно отсутствовать;

- в сертификате пользователя расширенное использование ключа (Extended

Key Usage) должно содержать OID Проверки подлинности пользователя (1.3.6.1.5.5.7.3.2) и OID Входа со смарт-картой (1.3.6.1.4.1.311.20.2.2);

- в сертификате пользователя в альтернативном имени субъекта (Subject Alternative Name) должно присутствовать Имя участника-пользователя (например UPN=user1@contoso.com). Имя участника-пользователя имеет формат адреса электронной почты (RFC 822) и состоит из имени пользователя и полного имени домена Microsoft Active Directory;

- в сертификате пользователя имя субъекта (Subject Name) должно соответствовать имени контейнера пользователя в Microsoft Active Directory (например, CN=User1, CN=Users, DC=Contoso, DC=COM);

- сертификат ЦС, на котором был выпущен сертификат пользователя, должен присутствовать в Microsoft Active Directory в хранилище NTAuth, откуда он автоматически будет перенесен в локальные копии данного хранилища членов домена. Добавить сертификат в хранилище NTAuth можно, выполнив команду **certutil -dspublish -f <Файл сертификата ЦС> NTAuthCA** на одном из контроллеров домена (с правами администратора домена);

- все сертификаты ЦС и САС, необходимые для построения полной цепочки сертификатов пользователей и контроллеров домена, должны находиться в соответствующих системных хранилищах сертификатов ЦС (в хранилище корневых сертификатов ЦС - для корневого сертификата и САС цепочки, в хранилище промежуточных сертификатов - для промежуточных сертификатов ЦС и САС цепочки) локального компьютера (см. подраздел 6.1).

Для возможности выполнения начальной аутентификации по протоколу Kerberos PKInit сертификат контроллера домена должен удовлетворять следующим условиям:

- в сертификате контроллера домена должна быть указана функционирующая точка распространения САС (CRL Distribution Point);

- в сертификате контроллера домена должно быть указано разрешённое использование ключа ЭП (Key Usage) для выполнения ЭП и шифрования;

- в сертификате контроллера домена базовые ограничения (Basic Constraints) не должны содержать признак сертификата ЦС, и ограничение на длину пути должно отсутствовать;

- в сертификате контроллера домена расширенное использование ключа (Extended Key Usage) должно содержать OID Проверки подлинности сервера (1.3.6.1.5.5.7.3.1), OID Проверки подлинности пользователя (1.3.6.1.5.5.7.3.2), OID Входа со смарт-картой (1.3.6.1.4.1.311.20.2.2) и OID Аутентификации центра распределения ключей (1.3.6.1.5.2.3.5);

- в сертификате контроллера домена в альтернативном имени субъекта (Subject Alternative Name) должно присутствовать DNS-имя домена (например DNS=contoso.com);

- в сертификате контроллера домена имя субъекта (Subject Name) должно соответствовать DNS-имени сервера (например, CN=dc1.contoso.com);

- сертификат корневого ЦС, являющийся корневым элементом цепочки сертификата контроллера домена, должен присутствовать в Microsoft Active Directory в хранилище Root предприятия, откуда он автоматически будет пе-

ренесен в локальные копии данного хранилища членов домена. Добавить сертификат в хранилище Root предприятия можно, выполнив команду **certutil -dspublish -f <Файл сертификата корневого ЦС> RootCA** на одном из контроллеров домена (с правами администратора домена);

– все сертификаты ЦС и САС, необходимые для построения полной цепочки сертификатов пользователей и контроллеров домена, должны находиться в соответствующих системных хранилищах сертификатов ЦС (в хранилище корневых сертификатов ЦС - для корневого сертификата и САС цепочки, в хранилище промежуточных сертификатов - для промежуточных сертификатов ЦС и САС цепочки) локального компьютера (см. подраздел 6.1).

При использовании точки распространения САС, доступной по протоколу LDAP и расположенной в хранилище Microsoft Active Directory, к ней должен быть разрешен анонимный доступ посредством выполнения следующих действий:

– необходимо установить значение атрибута dsHeuristics, расположенного в контейнере CN=Directory Services,CN=Windows NT,CN=Services,CN=Configuration, в 0000002001001. Для изменения значения атрибута можно воспользоваться диалоговой программой adsiedit.msc;

– необходимо разрешить анонимный доступ к контейнеру точки распространения, в котором расположен САС. Это также можно сделать с помощью диалоговой программы adsiedit.msc, разрешив доступ на чтение к указанному выше контейнеру пользователю NT AUTHORITY\АНОНИМНЫЙ ВХОД.

Для выполнения локального входа со смарт-картой пользователю необходимо вставить смарт-карту в соответствующий считыватель и нажать Ctrl-Alt-Del (когда отображается Windows Login Screen). При этом ОС автоматически распознает вставленную смарт-карту, считает все находящиеся на ней сертификаты и предложит их список для выбора пользователя (Рисунок 58).

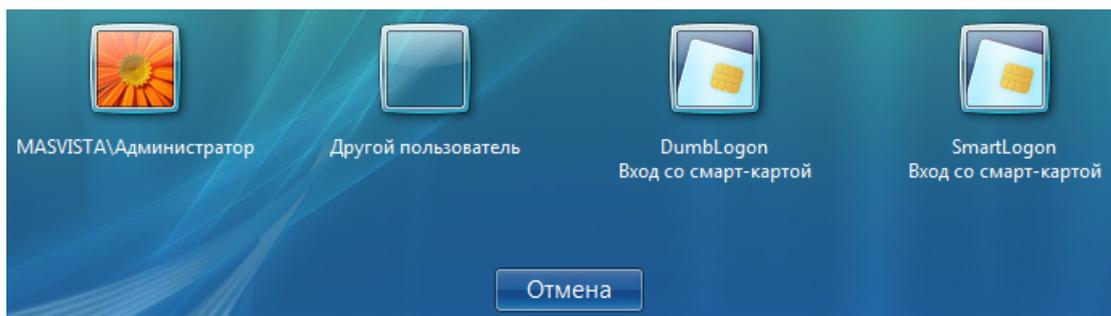


Рисунок 58 – Выбор сертификата

Далее, после выбора требуемого для входа сертификата пользователя, выдаётся диалог ввода ПИН-кода, необходимого для чтения ключа ЭП пользователя (Рисунок 59).



Рисунок 59 – Ввод ПИН-кода

После ввода ПИН-кода выполняется аутентификация пользователя в Microsoft Active Directory.

Для выполнения удаленного входа со смарт-картой необходимо использовать Remote Desktop Client (RDC) версии 6.0 или выше. Нужно, чтобы тип используемой смарт-карты соответствовал настроенному считывателю ключа ЭП в конфигурации пользователя.

Пользователю следует вставить смарт-карту в соответствующий считыватель и запустить RDC (программу MSTsc.exe), как это описано в подразделе 6.5. После ввода имени удаленного сервера терминалов (и имени шлюза служб терминалов, если это необходимо) и нажатия кнопки «Подключить» на экран будет выдано диалоговое окно с доступными на смарт-карте сертификатами (Рисунок 60).

После выбора требуемого сертификата необходимо ввести ПИН-код для возможности доступа к ключу ЭП пользователя.

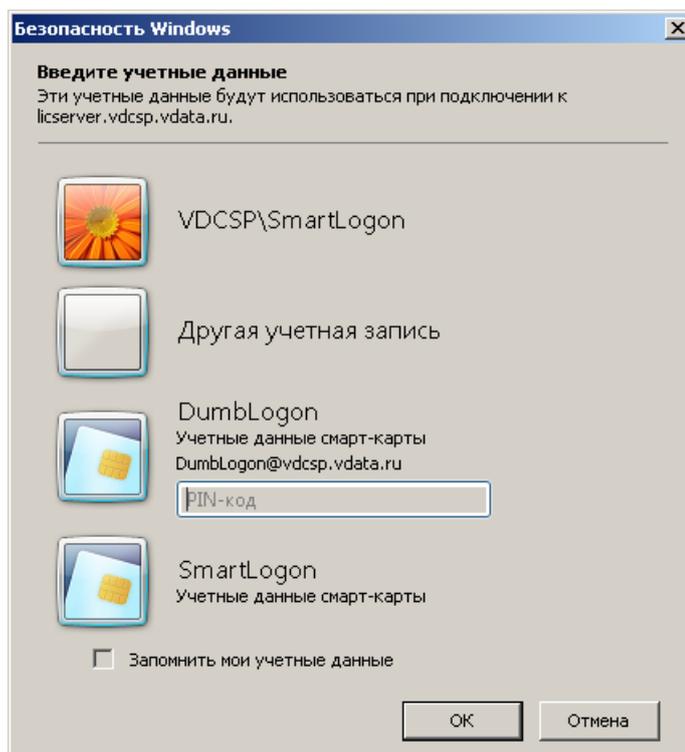


Рисунок 60 – Выбор сертификата и ввод ПИН-кода на ОС Windows Vista

После ввода ПИН-кода и нажатия кнопки «ОК» выполняется подключение к удалённому рабочему столу и аутентификация пользователя в Microsoft Active Directory.

6.7 TLS монитор

TLS монитор предназначен для ведения списка клиентских программ, использующих исключительно сертифицированную реализацию протокола TLS криптопровайдера СКЗИ «Валидата CSP», для включения и выключения использования данного списка, а также для выполнения других настроек модуля поддержки TLS.

Список программ, использующих исключительно сертифицированную реализацию протокола TLS, настраивается каждым пользователем индивидуально. По умолчанию он содержит программы клиента Internet Explorer (IExplore.exe) и Remote Desktop Client (MSTsc.exe) и для подавляющего большинства пользователей не потребует никакой дополнительной настройки.

6.7.1 Запуск и включение TLS монитора

После запуска TLS монитора (программы vdtls_mon.exe) на панели задач появится новый значок (Рисунок 61).



Рисунок 61 – Значок TLS монитора на панели задач

TLS монитор после запуска всегда оказывается в выключенном состоянии,

что обозначается красным цветом значка. Если подвести к нему курсор «мыши», появится всплывающая подсказка (Рисунок 62).

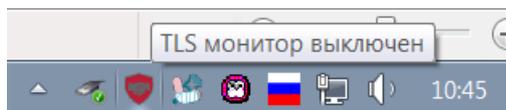


Рисунок 62 – Всплывающая подсказка TLS монитора

Если нажать на значок TLS монитора правой кнопкой «мыши», то появится контекстное меню (Рисунок 63).

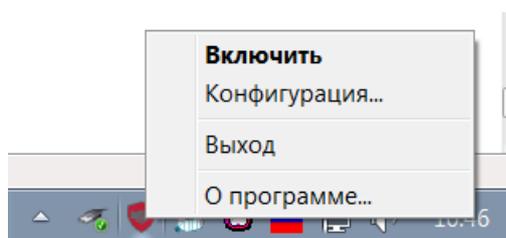


Рисунок 63 – Контекстное меню TLS монитора

Чтобы включить TLS выберите пункт меню «Включить» (или просто дважды щёлкните «мышью» на значке TLS монитора). Цвет значка монитора изменится на зелёный (Рисунок 64).

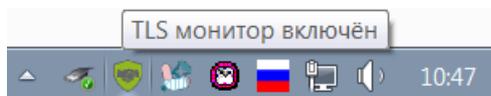


Рисунок 64 – TLS монитор включён

Чтобы выключить TLS монитор выберите в контекстном меню пункт «Выключить» или дважды щёлкните «мышью» на значке включённого TLS монитора.

Чтобы посмотреть информацию о версии TLS монитора (Рисунок 65), выберите в контекстном меню пункт «О программе ...».

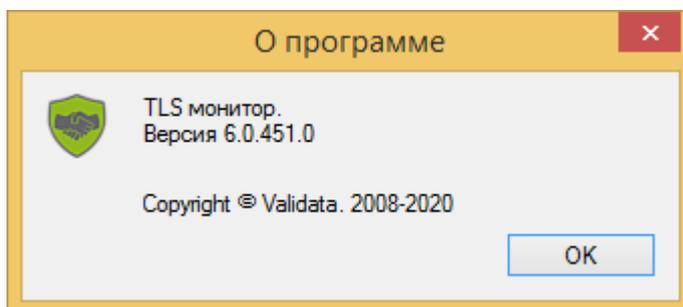


Рисунок 65 – Информация о версии TLS монитора

Для завершения работы TLS монитора выберите в контекстном меню пункт «Выход».

6.7.2 Конфигурация TLS монитора

Для того, чтобы запустить конфигурацию TLS монитора, выберите в контекстном меню пункт «Конфигурация ...» (Рисунок 66).

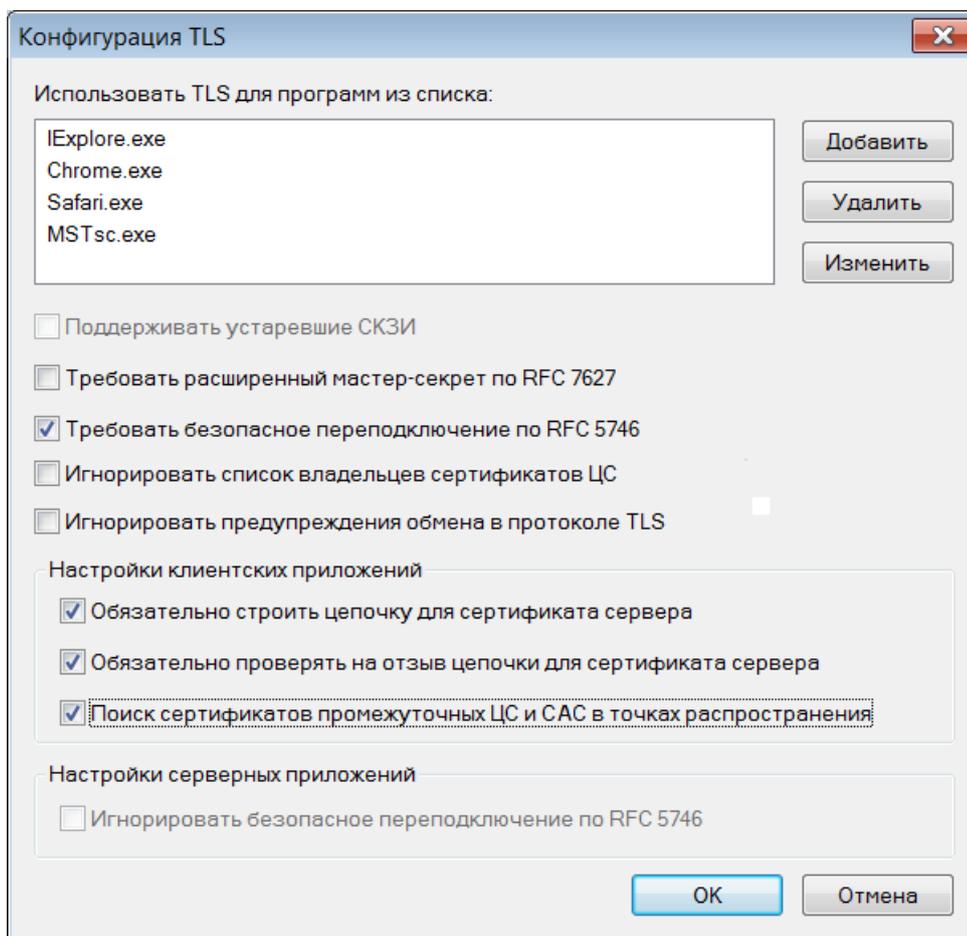


Рисунок 66 – Диалог конфигурации TLS

Чтобы добавить новый исполняемый модуль клиентской программы, который использует сертифицированную реализацию протокола TLS, нажмите кнопку «Добавить» и в стандартном диалоге открытия файла выберите требуемый модуль.

Чтобы удалить элемент списка, выделите его, нажмите кнопку «Удалить» и подтвердите своё решение (Рисунок 67).

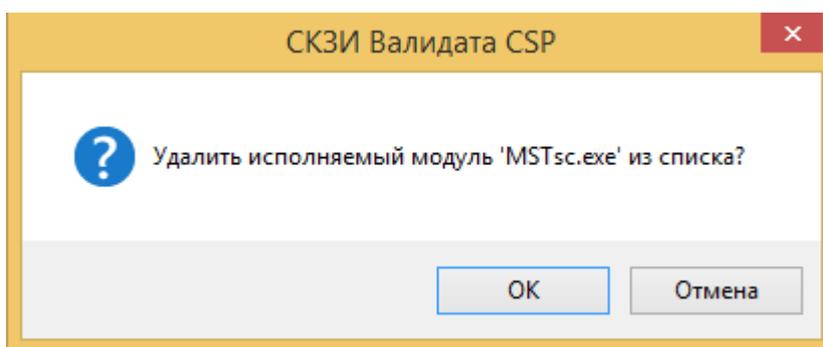


Рисунок 67 – Подтверждение удаления элемента списка

Чтобы заменить один модуль другим, выберите модуль в списке, нажмите кнопку «Изменить» и в стандартном диалоге открытия файла выберите новый исполняемый модуль.

Вы можете также отредактировать имя исполняемого модуля вручную - для этого выберите модуль в списке и ещё раз нажмите на него «мышью» (Рисунок 68).

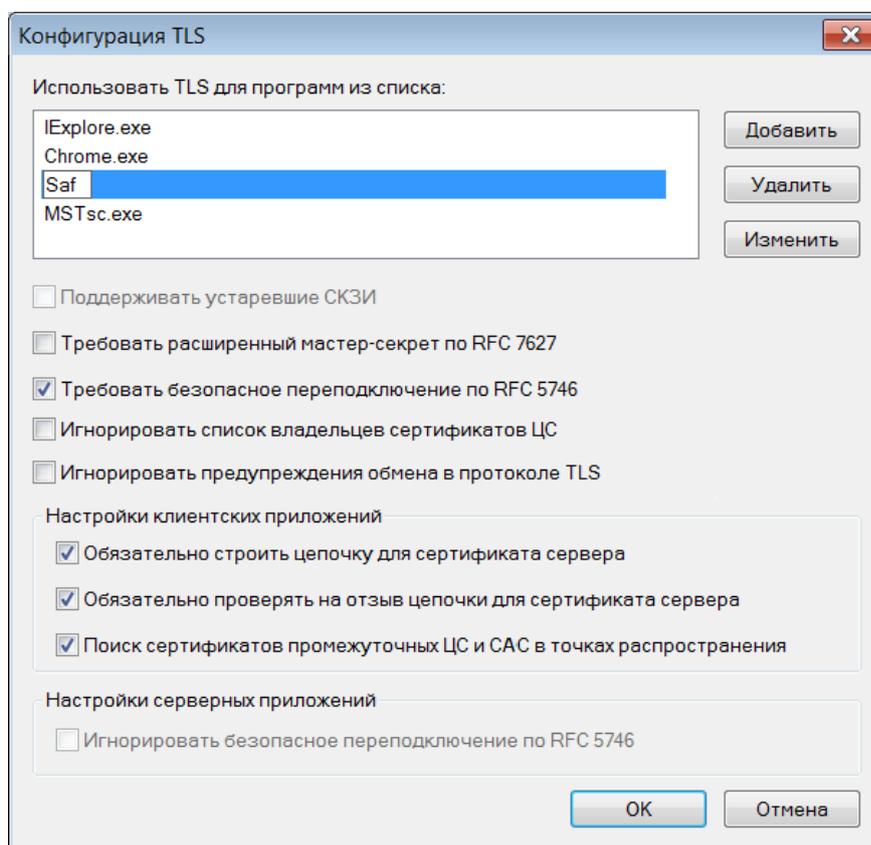


Рисунок 68 - Ручное редактирование элемента списка

Закончив редактирование, нажмите клавишу «Enter».

Кроме редактирования списка исполняемых модулей, TLS монитор позволяет выполнить следующие настройки модуля поддержки TLS (для их выполнения требуются права локального администратора, для вступления их в силу требуется перезагрузка):

– требовать расширенный мастер-секрет по RFC 7627 - данная опция может быть настроена как для серверной стороны, так и для клиентской. Если данная опция включена, то вычисленный мастер-секрет при создании новой TLS сессии будет усложняться с учетом уже отправленных и полученных данных переговоров в соответствии с RFC 7627. Включение данной опции возможно только при использовании новой реализации протокола TLS в соответствии с рекомендациями ТК №26;

– требовать безопасное переподключение по RFC 5746 - данная опция может быть настроена как для серверной стороны, так и для клиентской. Если данная опция включена, то все переподключения по созданию новой TLS сессии, выполняющиеся в контексте уже существующей TLS сессии, будут включать в себя

криптографически связывающие TLS расширения. При этом, если по какой-то причине криптографически связывающие TLS расширения отсутствуют, то переподключение будет невозможно;

– игнорировать список владельцев сертификатов ЦС - данная опция может быть настроена как для серверной стороны, так и для клиентской. При аутентификации клиента на основании его сертификата сервер посылает список имен владельцев сертификатов ЦС (список имен издателей), которые разрешены в качестве издателей сертификатов клиентов. Клиент же, со своей стороны, проверяет наличие имени издателя сертификата сервера в этом списке. Если данная опция включена, то отрицательный результат поиска имени издателя сертификата в списке имен издателей будет проигнорирован. По умолчанию отрицательный результат поиска имени издателя сертификата в списке имен издателей приводит к ошибочному завершению процедуры аутентификации;

– игнорировать предупреждения обмена в протоколе TLS - данная опция может быть настроена как для серверной стороны, так и для клиентской. Если данная опция включена, то все предупреждения обмена в протоколе TLS (TLS Alerts) будут проигнорированы. По умолчанию получение предупреждения обмена в протоколе TLS приводит к ошибочному завершению этого обмена;

– обязательно строить цепочку для сертификата сервера - данная опция может быть настроена только для клиентской стороны. Если данная опция включена, то построение и проверка цепочки сертификата сервера будет выполняться безусловно, независимо от поведения клиентского приложения. В этом случае, при ошибке построения или проверки цепочки сертификата сервера, защищенный канал связи между клиентом и сервером установлен не будет;

– обязательно проверять на отзыв цепочки сертификата сервера - данная опция может быть настроена только для клиентской стороны. Если данная опция включена, то проверка построенной цепочки сертификата сервера на аннулирование/прекращение действия будет выполняться безусловно, независимо от поведения клиентского приложения. В этом случае, при ошибке проверки цепочки сертификата сервера на аннулирование/прекращение действия, защищенный канал связи между клиентом и сервером установлен не будет;

– поиск сертификатов промежуточных ЦС и САС в точках распространения - данная опция может быть настроена только для клиентской стороны. Если данная опция включена, то при построении цепочки сертификата сервера будет разрешена загрузка необходимых сертификатов промежуточных ЦС и САС по сети из их точек распространения, независимо от поведения клиентского приложения.

– игнорировать безопасное переподключение по RFC 5746 - данная опция может быть настроена только для серверной стороны. Если данная опция включена, то сервер будет игнорировать все криптографически связывающие TLS расширения, посылаемые клиентом. Таким образом, включение данной опции блокирует возможность безопасного переподключения.

Примечание - Для изменения опций требуется наличие прав локального администратора. Изменения вступают в силу после перезагрузки компьютера.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ДСЧ	Датчик случайных чисел
КЗИ	Криптографическая защита информации
ОС	Операционная система (Operating System)
ПК	Программный комплекс
ПО	Программное обеспечение
САС	Список аннулированных сертификатов (Certificate Revocation List)
СКЗИ	Средство криптографической защиты информации
ЦС	Центр сертификации (Certification Authority)
ФКН	Функциональный ключевой носитель
ЭП	Электронная подпись (Digital Signature)

ПЕРЕЧЕНЬ РИСУНКОВ

1	Вкладка «Считыватели ключа»	6
2	Диалог выбора считывателя ключа	7
3	Изменение считывателя ключа для текущего пользователя	7
4	Диалог выбора ключа	8
5	Диалог выбора ключевого носителя	9
6	Ключевой носитель не найден	9
7	Диалог выбора ключа	10
8	Диалог задания пароля ключа	10
9	Диалог повторного задания пароля ключа	11
10	Диалог проверки пароля ключа	11
11	Диалог повторной проверки пароля ключа	11
12	Панель управления РуТокен	12
13	Вкладка «ДСЧ»	13
14	Диалог выбора ДСЧ	14
15	ДСЧ для текущего пользователя изменён	14
16	Инициализация биологического ДСЧ	15
17	Пример настройки «мыши»	16
18	Пример хаотичных кругообразных движений	17
19	Сообщение об удачной инициализации ДСЧ	18
20	Сообщение об инициализованном ДСЧ	18
21	Пример работы программы в случае успешной инициализации ДСЧ ФКН	19
22	Вкладка «Ключи»	20
23	Сообщение о замене ключевого носителя	21
24	Сообщение об ошибке при копировании ключа	21
25	Диалог выбора ключей для удаления	22
26	Список ключей	23
27	Информация о ключе	24
28	Информация о ключе с отображением ключа проверки ЭП	24
29	Вкладка «Сертификаты»	25
30	Отображение выбранного сертификата	26
31	Сертификат выбран	27
32	Выбор хранилища для сертификата	28
33	Сообщение об успешном размещении сертификата	29
34	Выбор смарт-карты	29
35	Сообщение о неподдерживаемом типе смарт-карты	30
36	Сообщение об успешной записи сертификата	30
37	Вкладка «Сервис»	31
38	Подтверждение затирания файла	31
39	Сообщение об успешной проверке подписи	32
40	Сообщение об отсутствии подписи в модуле	32
41	Выбор ключевого носителя	33
42	Параметры форматирования	33
43	Смена ПИН-кода	34
44	Область уведомлений с иконкой ПМ ГИПС	35
45	Настройка отображения иконки ПМ ГИПС	35

46	Контекстное меню ПМ ГИПС	36
47	Диалоговое окно «О программе»	36
48	Диалоговое окно «Конфигурация»	37
49	Пример записи ошибки в журнале приложений Windows	37
50	Пример отображения диалогового окна	38
51	Диалог безопасности каталога	40
52	Диалог выбора сертификата	40
53	Диалог подключений	41
54	Диалог свойств шлюза	44
55	Диалог выбора сертификата	44
56	Главное окно программы	46
57	Диалог ввода имени шлюза служб терминалов	47
58	Выбор сертификата	50
59	Ввод ПИН-кода	51
60	Выбор сертификата и ввод ПИН-кода на ОС Windows Vista	52
61	Значок TLS монитора на панели задач	52
62	Всплывающая подсказка TLS монитора	53
63	Контекстное меню TLS монитора	53
64	TLS монитор включён	53
65	Информация о версии TLS монитора	53
66	Диалог конфигурации TLS	54
67	Подтверждение удаления элемента списка	54
68	Ручное редактирование элемента списка	55

