ООО «ВАЛИДАТА»

УТВЕРЖДЕН
ВАМБ.00060-05 91 01–ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ «ВАЛИДАТА CSP» ВЕРСИЯ 5.0

РУКОВОДСТВО ПО УСТАНОВКЕ И НАСТРОЙКЕ

ВАМБ.00060-05 91 01

2016

Аннотация

Данный документ содержит описание процесса установки, удаления и настройки средства криптографической защиты информации (СКЗИ) «Валидата CSP».

Документ предназначен для системных администраторов и администраторов безопасности как руководство по по установке, удалению и настройке криптографического провайдера «Валидата CSP».

Содержание

1 НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ 4
1.1 Назначение . . . 4
1.2 Условия применения . . . 4

2 УСТАНОВКА И УДАЛЕНИЕ СКЗИ «Валидата CSP» 5
2.1 Установка СКЗИ «Валидата CSP» . . . 5
2.2 Удаление СКЗИ «Валидата CSP» . . . 9

3 НАСТРОЙКА СКЗИ «Валидата CSP» 11
3.1 Конфигурационная программа СКЗИ «Валидата CSP» . . . 11
3.1.1 Запуск конфигурационной программы . . . 11
3.1.2 Настройка программного модуля считывания ДСЧ . . . 12
3.1.3 Настройка программных модулей считывателей ключа . . . 14
3.1.4 Настройка параметров работы с ключами . . . 17
3.1.5 Настройка параметров совместимости . . . 18
3.1.6 Настройка параметров криптографических алгоритмов . . . 19
3.2 Протоколирование событий . . . 20
3.2.1 Настройка протоколирования . . . 20
3.2.2 Протоколирование в Конфигурационной программе . . . 21

ПЕРЕЧЕНЬ РИСУНКОВ 22

1 НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ

1.1 Назначение

Криптографический провайдер «Валидата CSP» предназначен для:

– вычисления и проверки электронной подписи (ЭП) в соответствии с ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012;

– выполнения зашифрования и расшифрования данных в соответствии с ГОСТ 28147-89;

– вычисления имитозащиты данных в соответствии с ГОСТ 28147-89 (при этом поддерживаются имитозащита длиной 4 байта и имитозащита длиной 8 байт);

– вычисления ключа парной связи Диффи-Хелмана с использованием пар закрытых и открытых ключей, созданных в соответствии с ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012;

– вычисления хэш-функции данных в соответствии с ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012;

– выработки случайного числа заданной длины;

– создания (генерации) закрытых ключей в соответствии с ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012;

– вычисления открытых ключей в соответствии с ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012.

1.2 Условия применения

Криптографический провайдер «Валидата CSP» работает под управлением следующих ОС:

– Microsoft Windows Vista с пакетом обновлений 1 и выше;

– Microsoft Windows Server 2008 с пакетом обновлений 1 и выше;

– Microsoft Windows 7;

– Microsoft Windows Server 2008 R2;

– Microsoft Windows 8/8.1;

– Microsoft Windows Server 2012/2012 R2.

При этом поддерживаются как 32-битные ОС Microsoft Windows (x86), так и 64-битные ОС Microsoft Windows (x64).

2 УСТАНОВКА И УДАЛЕНИЕ СКЗИ «Валидата CSP»

2.1 Установка СКЗИ «Валидата CSP»

Для установки СКЗИ «Валидата CSP» необходимо зарегистрироваться в ОС Microsoft Windows с правами администратора. После этого необходимо смонтировать дистрибутивный носитель программного обеспечения (ПО) и запустить процесс установки из Проводника двойным щелчком «мыши» по файлу дистрибутива ПО **acsptls_x86.msi** (для ОС Microsoft Windows x86) или **acsptls_AMD64.msi** (для ОС Microsoft Windows x64).

После запуска процесса установки будет отображен начальный диалог (Рисунок 1).

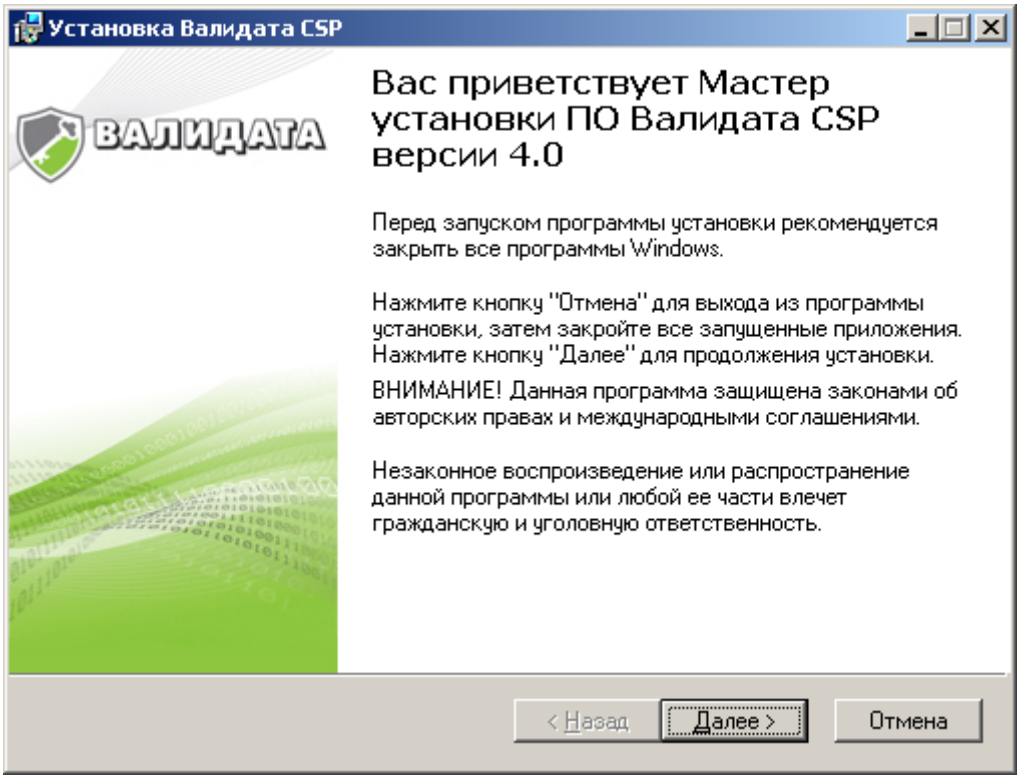

Рисунок 1 – Начальный диалог установки

Необходимо нажать на кнопку «Далее». Будет выведен диалог (Рисунок 2) с именем пользователя, названием организации и полем для ввода номера продукта (или ключа установки).

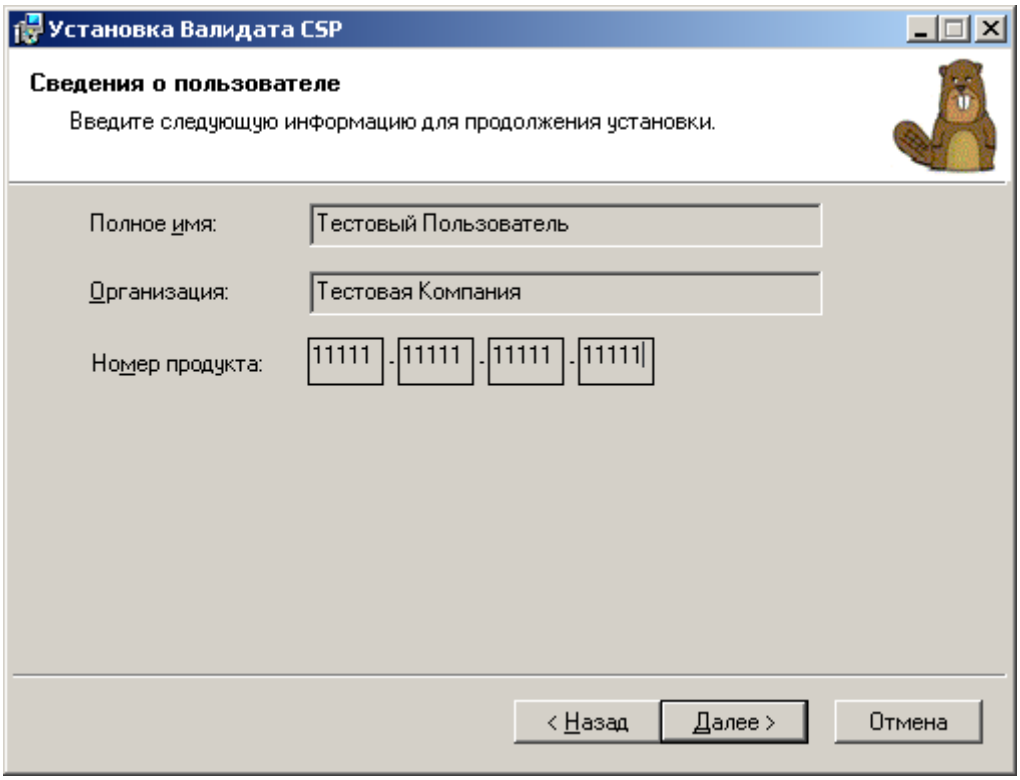

Рисунок 2 – Диалог ввода номера продукта

Необходимо ввести действительный номер продукта для продолжения установки и нажать на кнопку «Далее». В случае ввода недействительного номера (ключа установки) на экран будет выдано соответствующее сообщение (Рисунок 3).

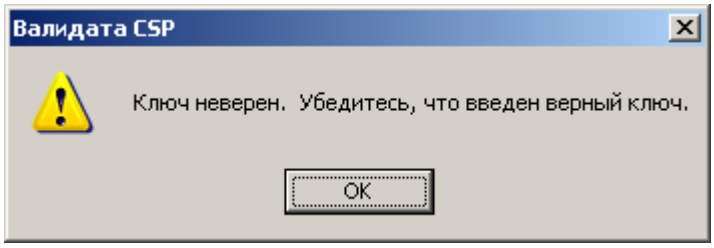

Рисунок 3 – Сообщение о неверном ключе установки

Иначе будет отображен диалог выбора типа установки (Рисунок 4).

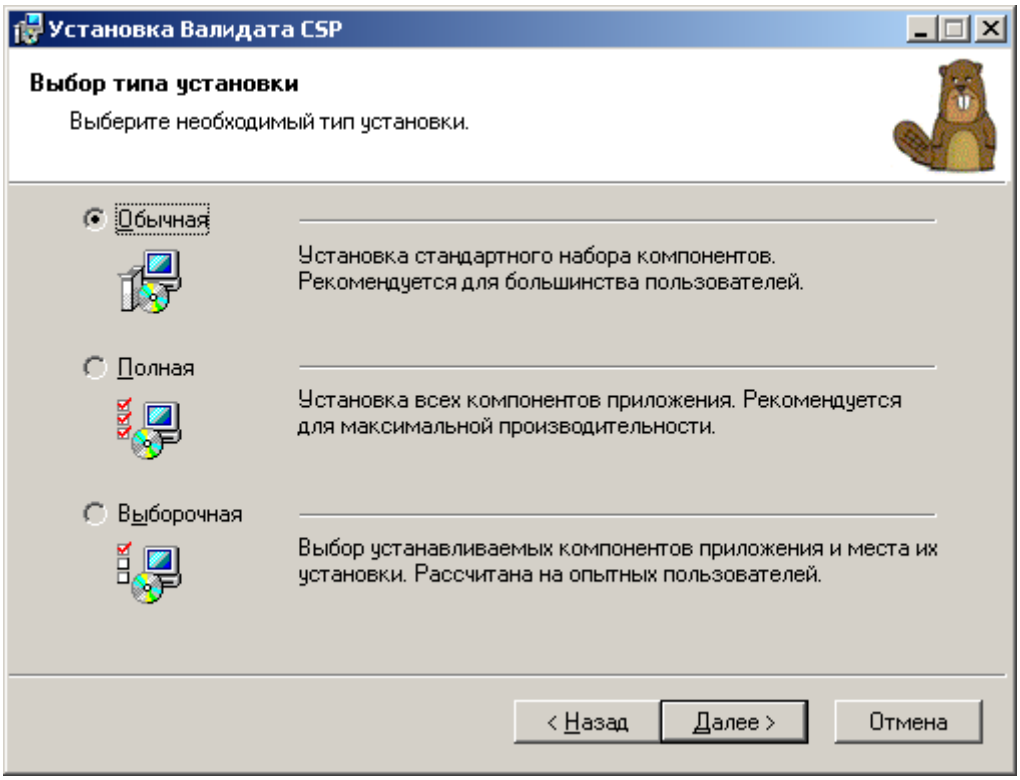

Рисунок 4 – Диалог выбора типа установки

Необходимо выбрать тип установки и нажать на кнопку «Далее». Тип установки влияет на количество устанавливаемых библиотек поддержки датчиков случайных чисел (ДСЧ) и считывателей ключей, а также библиотек совместимости, утилит и компонентов модуля поддержки TLS. При выборе Полной установки будут установлены все доступные библиотеки и утилиты. При выборе Обычной установки будут установлены Биологический ДСЧ, Считыватели Съемный Диск (сменные USB-носители типа Flash и гибкие магнитные диски), ruToken, eToken, vdToken (ФКН) и vdToken, Утилита копирования ключа СКЗИ СКАД «Сигнатура», а также Поддержка протокола TLS и Поддержка защищенной почты в Microsoft Office Outlook. Выборочный тип установки позволяет указать все необходимые для установки компоненты (Рисунок 5).

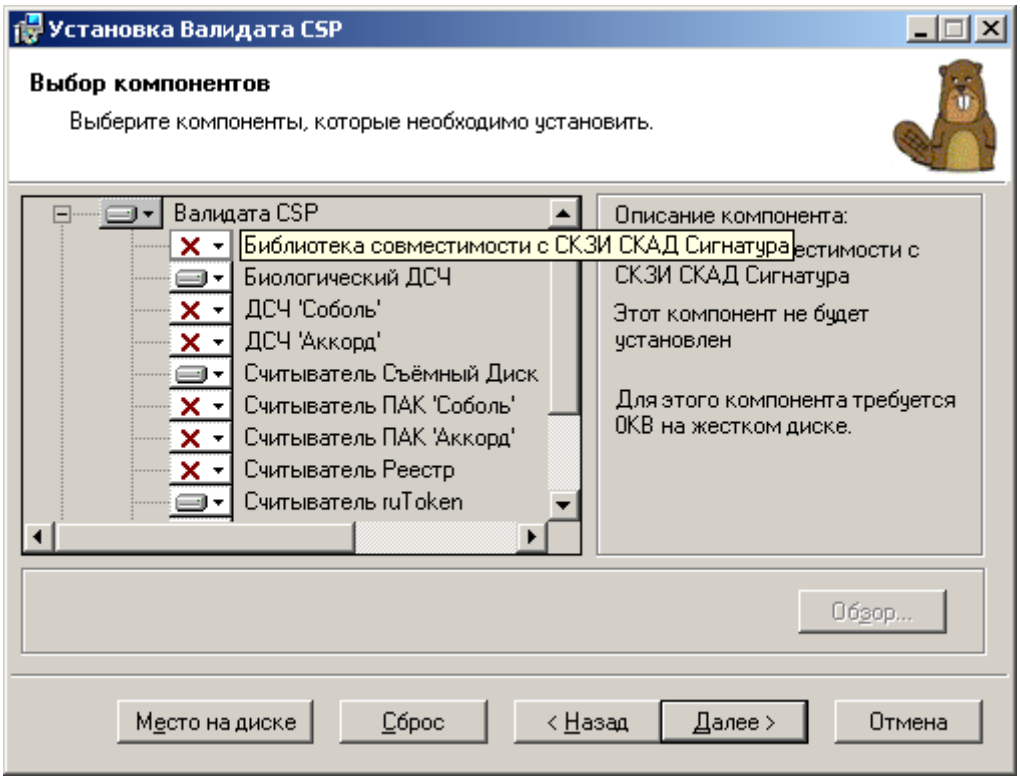

Рисунок 5 – Выборочный тип установки

Выбрав нужные для установки компоненты, необходимо нажать на кнопку «Далее». Появится диалог о готовности к установке (Рисунок 6).

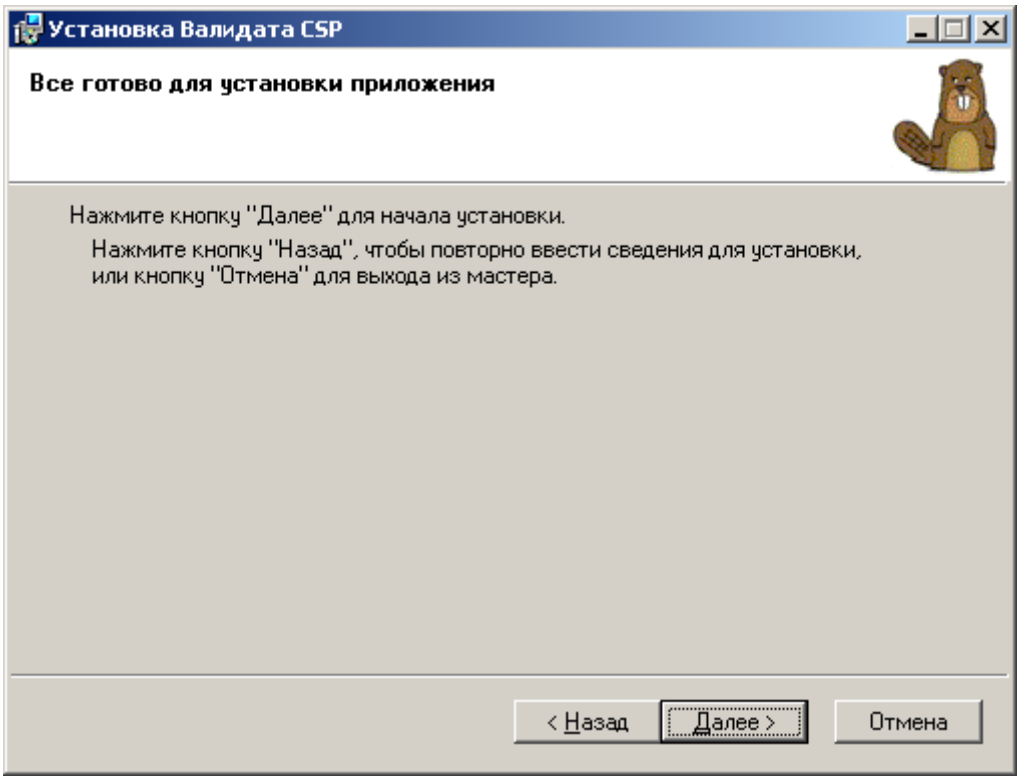

Рисунок 6 – Диалог готовности к установке

После отображения диалога о готовности к установке необходимо нажать на кнопку «Далее» для завершения процесса установки. По завершении процесса установки будет выдан диалог о завершении процесса установки (Рисунок 7).

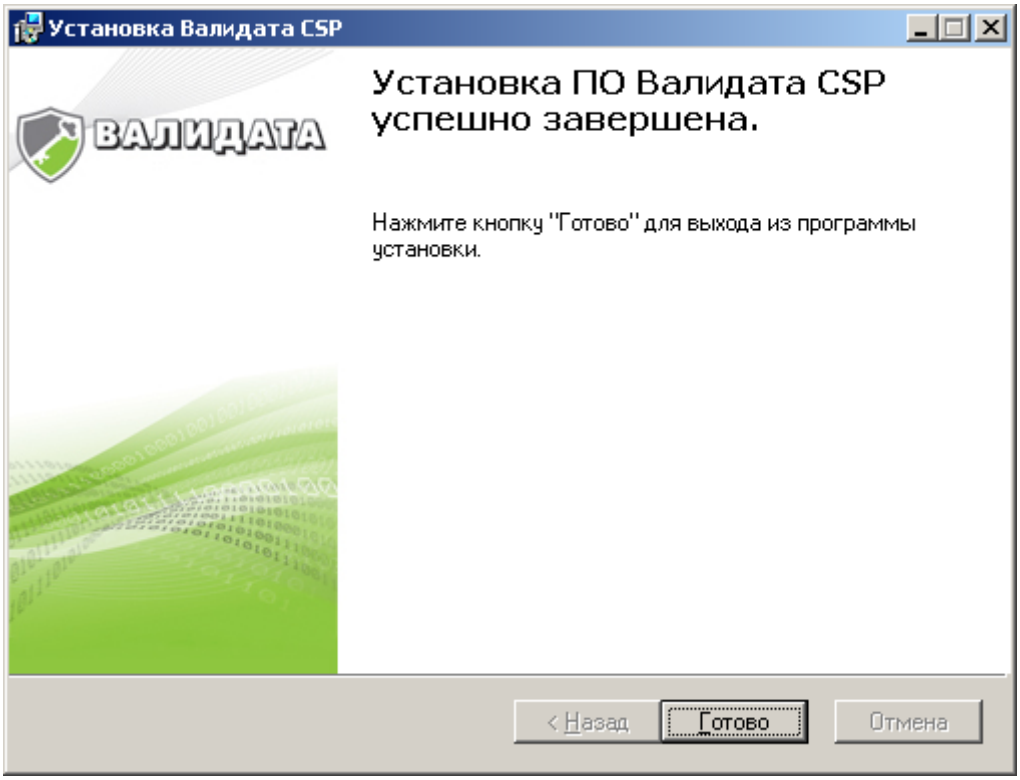

Рисунок 7 – Диалог завершения установки

Необходимо нажать на кнопку «Готово». После этого будет выдано диалоговое окно, запрашивающее выполнение перезагрузки ОС (Рисунок 8). Необходимо нажать на кнопку «Да».

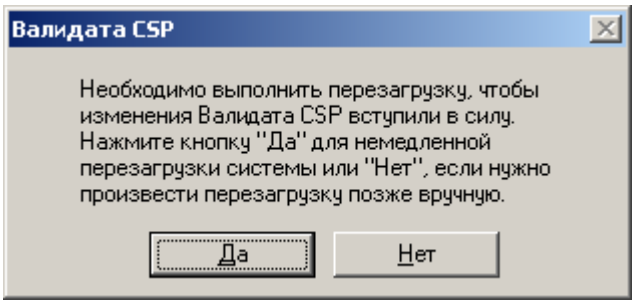

Рисунок 8 – Диалог перезагрузки ОС

2.2 Удаление СКЗИ «Валидата CSP»

Для удаления СКЗИ «Валидата CSP» необходимо зарегистрироваться в ОС Microsoft Windows с правами администратора. После этого необходимо запустить Панель управления и запустить оснастку Установка/Удаление Программ. Далее необходимо найти в списке установленных программ строку - СКЗИ «Валидата CSP»и, подсветив найденную строку, нажать кнопку «Удалить». На диалоговое сообщение, запрашивающее подтверждение удаления СКЗИ «Валидата CSP»(Рисунок 9), необходимо нажать кнопку «Да».

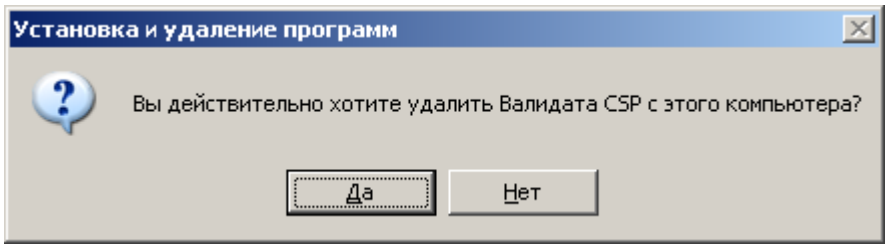

Рисунок 9 – Диалог подтверждения удаления

По окончании удаления ПО будет выдано диалоговое окно, запрашивающее выполнение перезагрузки ОС (Рисунок 10). Необходимо нажать на кнопку «Да».

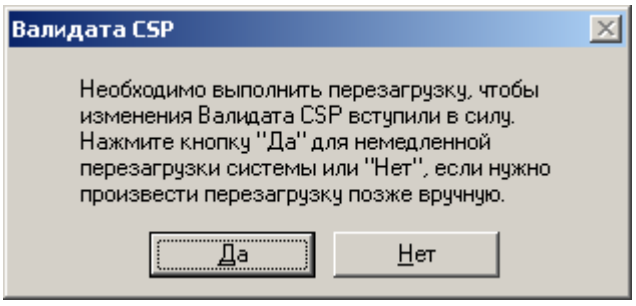

Рисунок 10 – Диалог перезагрузки ОС

3 НАСТРОЙКА СКЗИ «Валидата CSP»

3.1 Конфигурационная программа СКЗИ «Валидата CSP»

3.1.1 Запуск конфигурационной программы

Для запуска конфигурационной программы СКЗИ «Валидата CSP» необходимо вызвать пункт меню «Пуск»->«Программы»->СКЗИ «Валидата CSP»->«Конфигурационная программа СКЗИ». На экране появится главное окно программы (Рисунок 11).

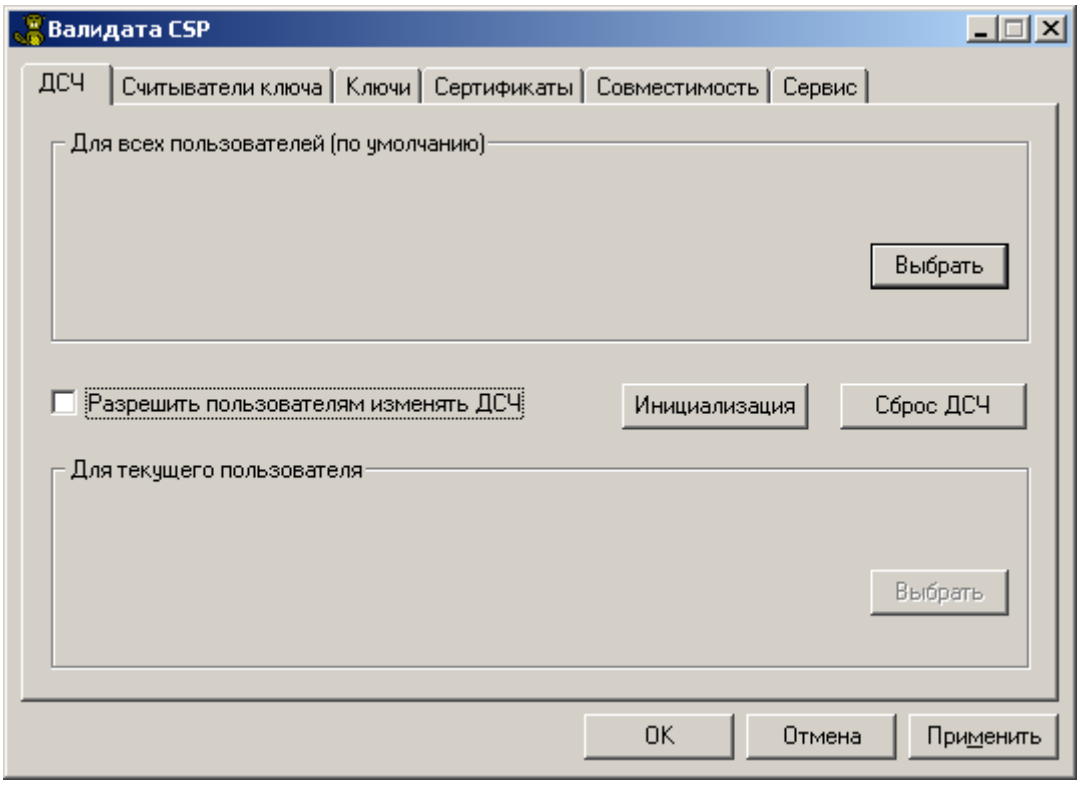

Рисунок 11 – Главное окно программы

Примечание - Для использования всех возможностей конфигурационной программы её необходимо запускать с правами администратора на локальном компьютере.

Вы можете просмотреть информацию о версии конфигурационной программы СКЗИ «Валидата CSP», выбрав в системном меню (в левом верхнем углу) пункт «О программе. . . », появится информация о программе (Рисунок 12).

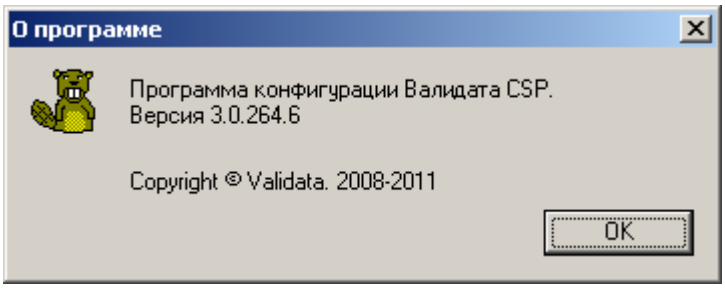

Рисунок 12 – Информация о программе

Нажатие кнопки «ОК», расположенной на главном окне конфигурационной программы, приводит к завершению работы последней с сохранением изменений в настройках ПО. Нажатие кнопки «Отмена» приводит к завершению работы конфигурационной программы без сохранения изменений в настройках ПО. Нажатие кнопки «Применить» приводит к сохранению изменений в настройках ПО, но конфигурационная программа не завершается.

3.1.2 Настройка программного модуля считывания ДСЧ

Для работы СКЗИ «Валидата CSP» требуется ДСЧ. Настройка программного модуля считывания ДСЧ производится на закладке «ДСЧ».

В поставку СКЗИ входит несколько программных модулей считывания ДСЧ, администратор может задать тип ДСЧ, вызываемый по умолчанию, для всех пользователей. Для этого нужно нажать кнопку «Выбрать» в верхней части диалога. На экране появится диалоговое окно выбора типа ДСЧ (Рисунок 13).

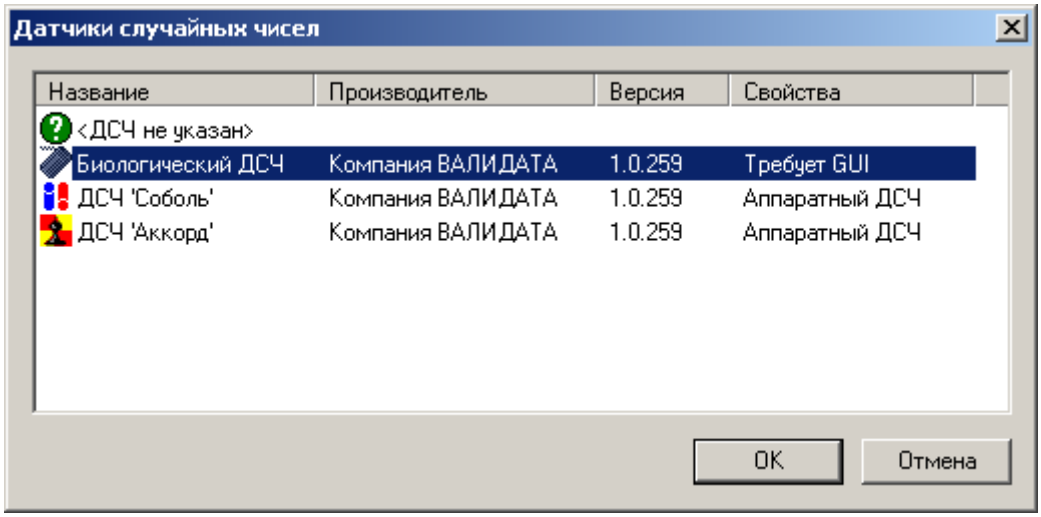

Рисунок 13 – Диалог выбора ДСЧ

Выберите ДСЧ и нажмите кнопку «ОК». На экране появится исходное окно с информацией о выбранном ДСЧ (Рисунок 14).

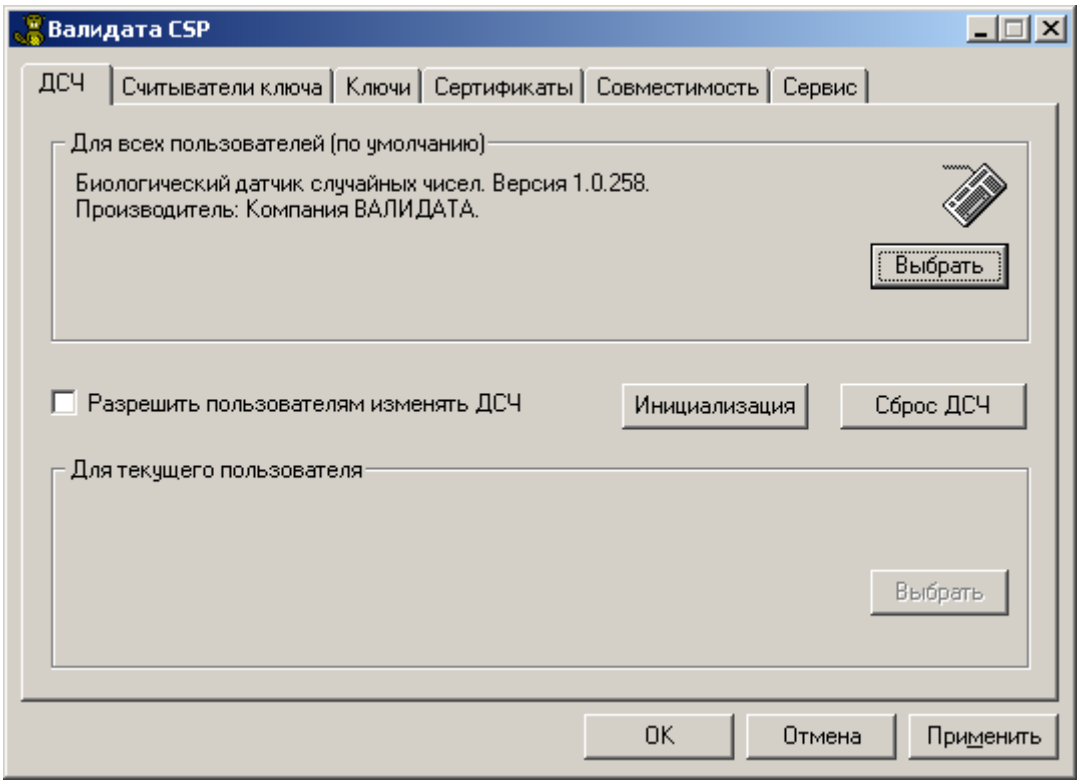

Рисунок 14 – ДСЧ для всех пользователей выбран

Примечание - Для большинства датчиков (кроме биологического ДСЧ) требуется установка на компьютере специальной аппаратуры (например, СЗИ «Аккорд-АМДЗ» или СЗИ «Соболь») и соответствующего программного обеспечения.

Администратор может разрешить пользователям изменять выбор ДСЧ, для этого необходимо выбрать опцию «Разрешить пользователям менять ДСЧ», после чего станет доступной кнопка «Выбрать» в нижней части диалога (Рисунок 15).

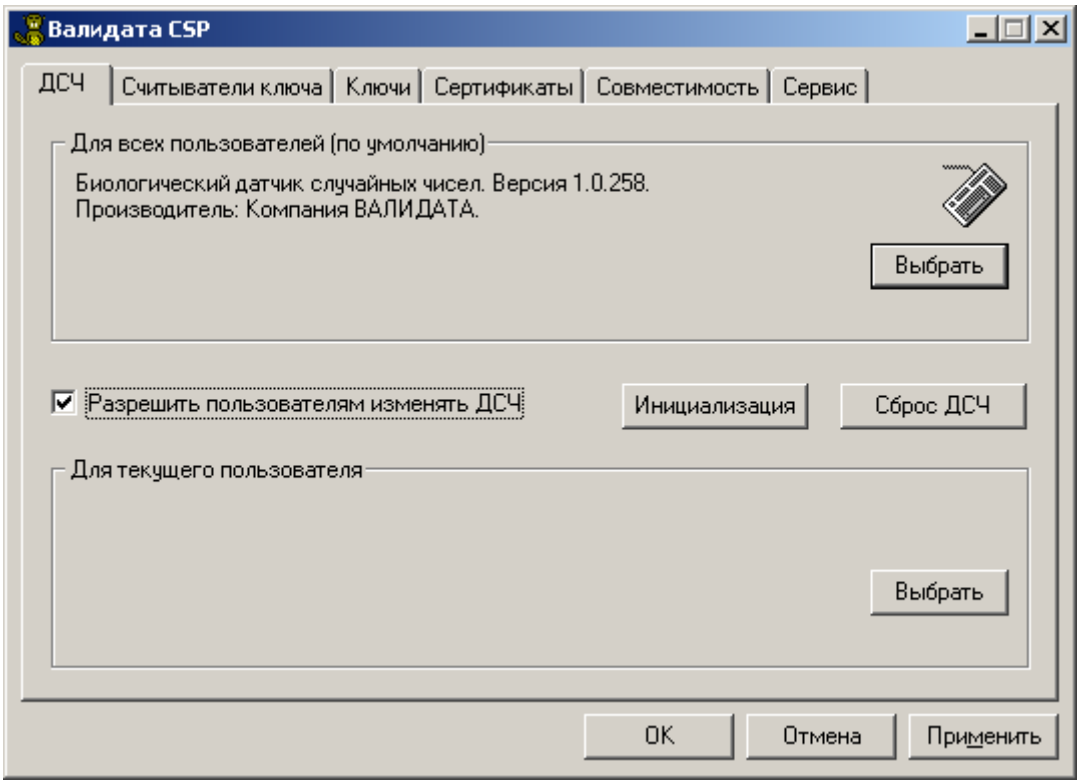

Рисунок 15 – Включена опция выбора типа ДСЧ пользователями

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

3.1.3 Настройка программных модулей считывателей ключа

Настройка программных модулей считывателей ключа (далее - считывателей ключа) производится на закладке «Считыватели ключа» (Рисунок 16).

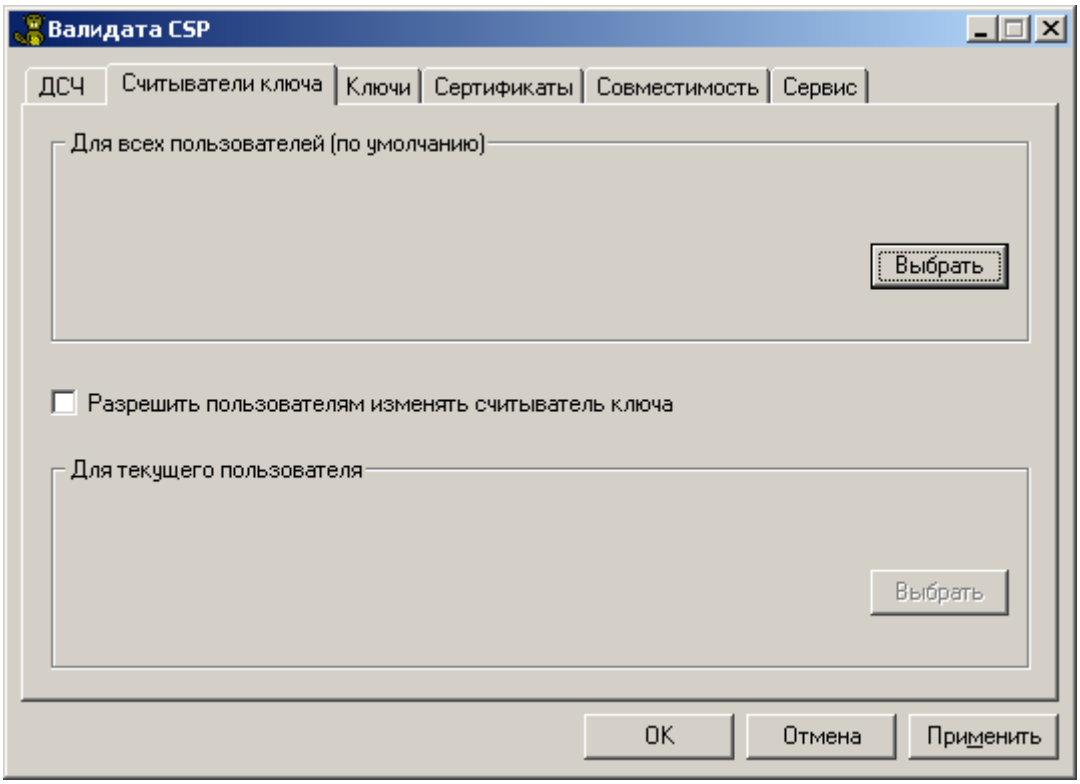

Рисунок 16 – Закладка «Считыватели ключа»

СКЗИ «Валидата CSP» может работать с различными типами считывателей ключей, администратор может задать считыватель ключа, вызываемый по умолчанию, для всех пользователей. Для этого нужно нажать кнопку «Выбрать» в верхней части диалога. На экране появится диалоговое окно выбора считывателей ключа (Рисунок 17).

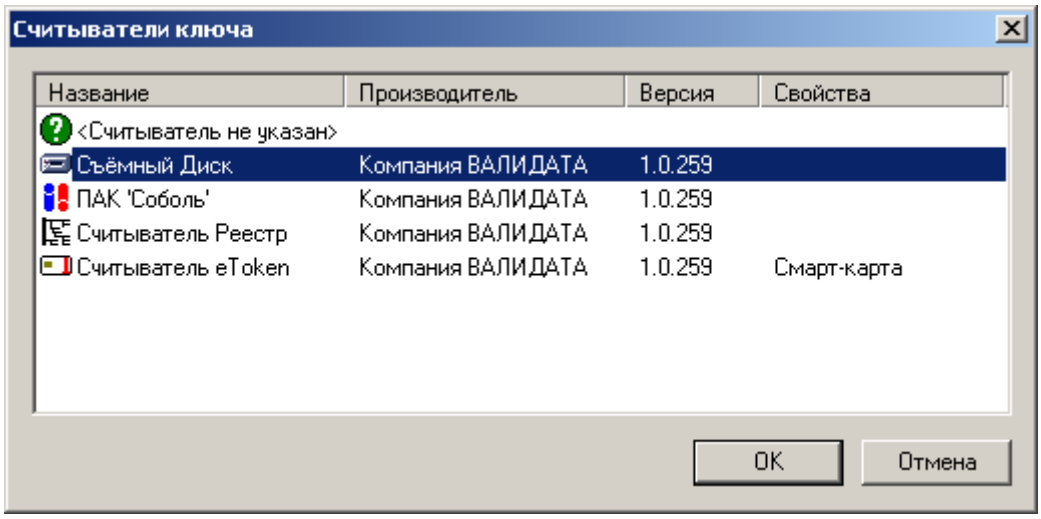

Рисунок 17 – Диалог выбора считывателя ключа

Выберите считыватель и нажмите кнопку «OK». На экране появится исходное окно с информацией о выбранном считывателе ключа (Рисунок 18).

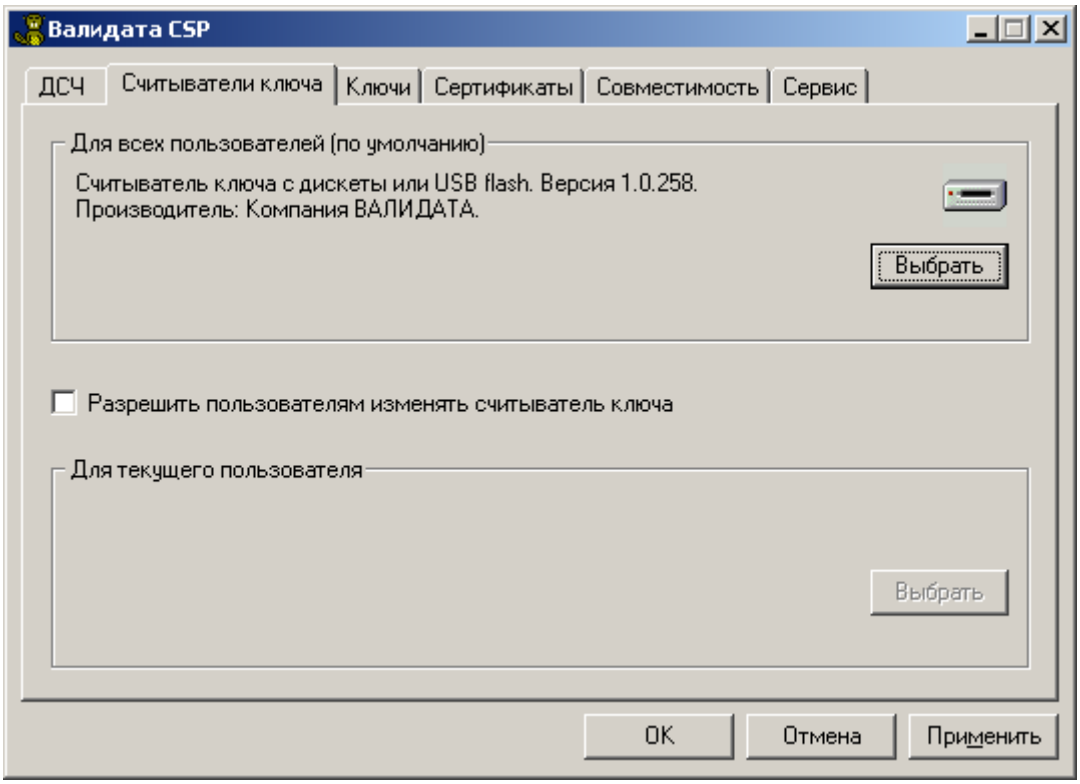

Рисунок 18 – Считыватель для всех пользователей выбран

Администратор может разрешить пользователям изменять выбор считывателя, для этого необходимо выбрать соответствующую опцию, после чего станет доступной кнопка «Выбрать» в нижней части диалога (Рисунок 19).

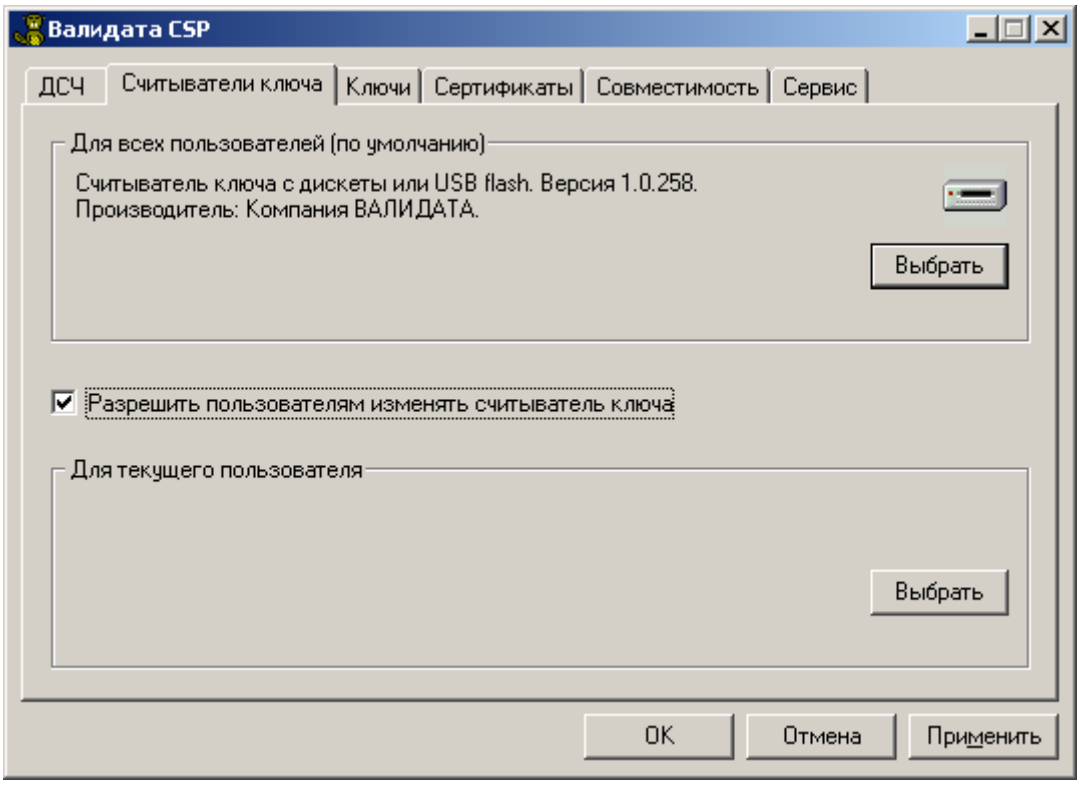

Рисунок 19 – Включена опция выбора считывателя ключа пользователями

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

3.1.4 Настройка параметров работы с ключами

Администратор может настраивать параметры работы с ключами, перейдя на закладку «Ключи» (Рисунок 20).

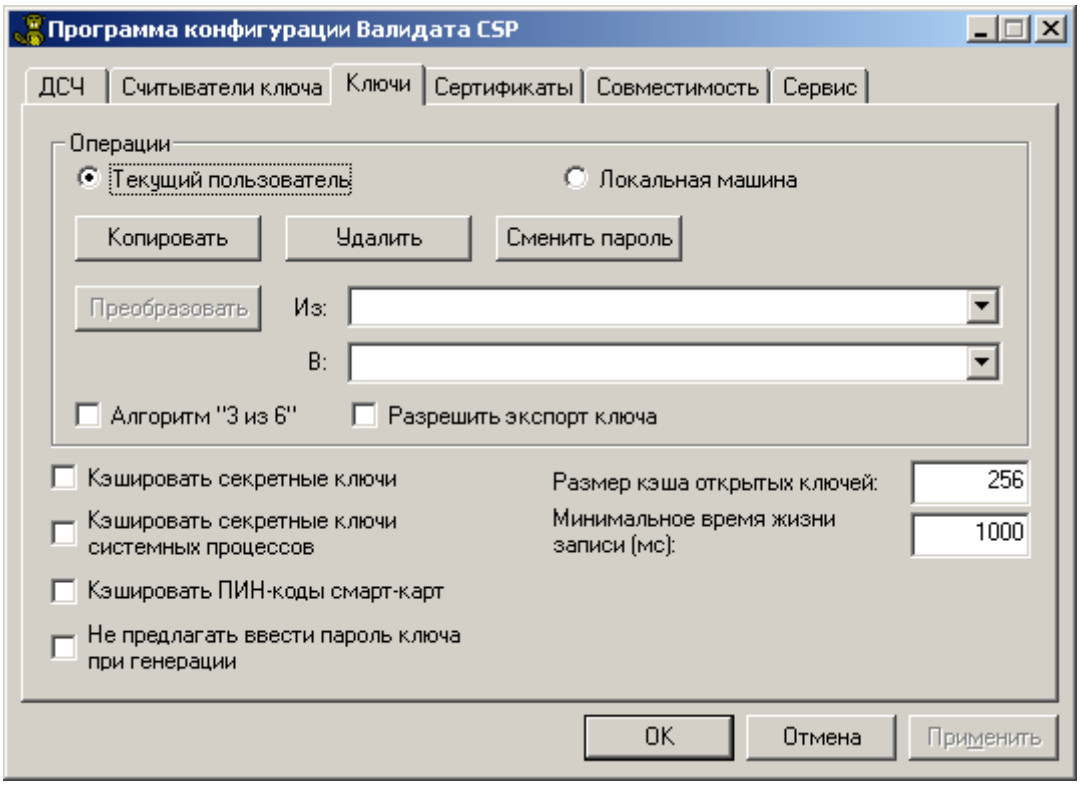

Рисунок 20 – Закладка «Ключи»

Настройка параметров кэширования ключей

Для ускорения работы СКЗИ «Валидата CSP» может кэшировать (сохранять в виртуальной памяти процесса) ключи ЭП и ключи проверки ЭП.

По умолчанию кэширование ключей ЭП выключено. Администратор может включить его, отметив опцию **«Кэшировать закрытые ключи»**. Если необходимо включить кэширование ключей ЭП для процессов, выполняющихся под учетной записью локальной системы или локального или сетевого сервиса (системных процессов), следует отметить опцию **«Кэшировать закрытые ключи системных процессов»**. Включение опции **«Кэшировать закрытые ключи»** автоматически приводит к включению опции **«Кэшировать закрытые ключи системных процессов»**, поскольку в этом случае ключи ЭП системных процессов также будут кэшироваться. Следует обратить внимание на то, что выключение опции **«Кэшировать закрытые ключи»** не приводит к автоматическому выключению опции **«Кэшировать закрытые ключи системных процессов»**, оставляя эту настройку на усмотрение администратора. Размер кэша практически не ограничен.

Кэширование ключей проверки ЭП по умолчанию включено, и размер кэша составляет 16 записей. Администратор может установить другое значение **«Размер кэша открытых ключей»** (не более 65535 записей) или полностью выключить кэширование, установив этот параметр в 0. Кроме того, администратор может изменить время, в течение которого открытый ключ гарантированно не удаляется из кэша, даже если кэш заполнен. По умолчанию это время

равно 1 секунде, в целях оптимизации производительности оно может быть изменено в поле **«Минимальное время жизни записи»** (указывается в миллисекундах). Следует отметить, что каждая запись кэша ключей проверки ЭП занимает примерно 16 Кб оперативной памяти.

Для того чтобы сделанные изменения вступили в силу, нажмите кнопку «Применить». При этом внесенные изменения будут отражены в работающих процессах только после их перезапуска.

Настройка прочих параметров

Для включения кэширования ПИН-кодов смарт-карт, которое может быть необходимо при работе с приложениями, не имеющими возможности выдавать множественные запросы на ввод ПИН-кода, нужно отметить опцию **«Кэшировать ПИН-коды смарт-карт»**. По умолчанию кэширование ПИН-кодов выключено.

Для возможности отключения диалоговых окон, предлагающих установить защиту создаваемого ключа паролем (т.е. запрос пароля при загрузке ключа) следует включить опцию **«Не предлагать ввести пароль ключа при генерации»**.

Для того, чтобы сделанные изменения вступили в силу, нажмите кнопку «Применить». При этом внесенные изменения будут отражены в работающих процессах только после их перезапуска.

3.1.5 Настройка параметров совместимости

Администратор может настраивать параметры совместимости с другими провайдерами, перейдя на закладку «Совместимость» (Рисунок 21).

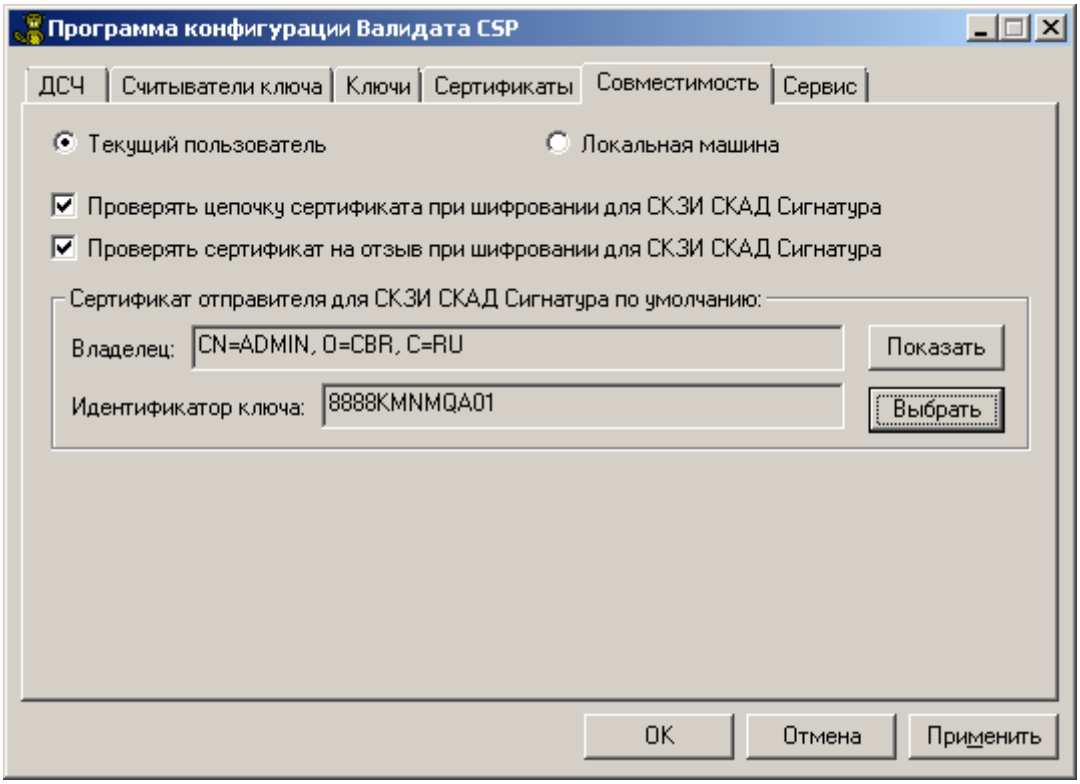

Рисунок 21 – Закладка «Совместимость»

При выполнении операций зашифрования и расшифрования в простом формате (формате зашифрованных и/или подписанных данных СКЗИ СКАД Сигнатура версии 3.6) требуется

сертификат получателя/отправителя зашифрованного сообщения. Для указания этого сертификата нажмите кнопку «Выбрать» (Рисунок 22).

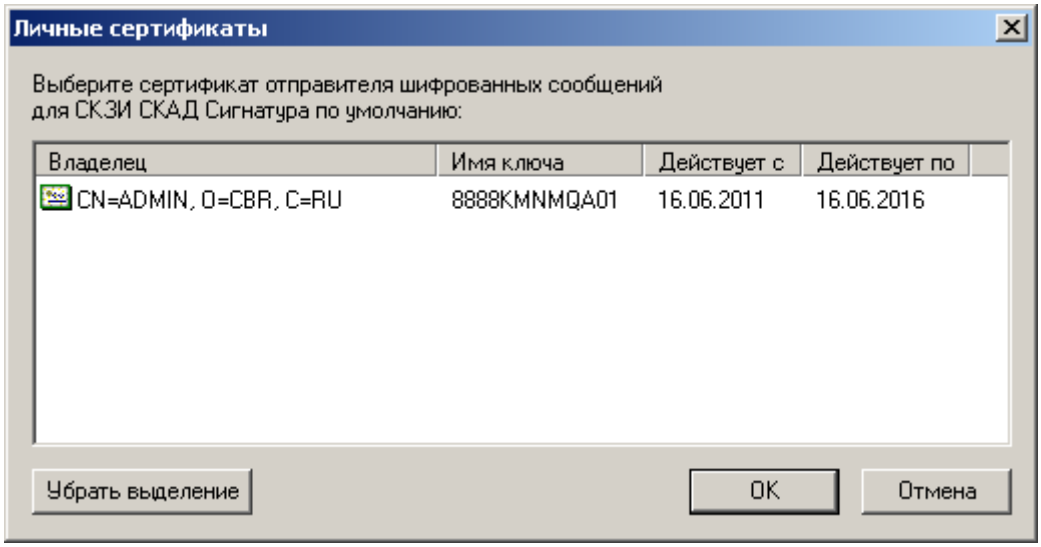

Рисунок 22 – Диалог выбора сертификата отправителя

Выберите сертификат отправителя из списка и нажмите кнопку «OK».

Чтобы цепочка этого сертификата проверялась при выполнении операций шифрования, включите опцию **«Проверять цепочку сертификата при шифровании для СКЗИ СКАД Сигнатура»**. При этом станет доступной опция **«Проверять сертификат на отзыв при шифровании для СКЗИ СКАД Сигнатура»**. Включите эту опцию для проверки цепочки сертификатов отправителя зашифрованного сообщения на отзыв.

Сертификат отправителя должен быть в хранилищах L«MY», L«TrustedPeople», L«AddressBook». Отключить цепочку может потребоваться, например, при расшифровании файла в случае отзыва сертификата отправителя.

3.1.6 Настройка параметров криптографических алгоритмов

СКЗИ «Валидата CSP» предоставляет возможность администратору указать используемые по умолчанию при выполнении криптографических преобразований параметры криптографических алгоритмов:

– параметры алгоритма хэширования по ГОСТ Р 34.11-94 - набор параметров, описывающий используемый узел замены при выполнении операции хэширования;

– параметры алгоритма хэширования по ГОСТ Р 34.11-2012 - набор параметров, приведенный в ГОСТ Р 34.11-2012 и используемый при выполнении операции хэширования;

– параметры алгоритма шифрования по ГОСТ 28147-89 - набор параметров, описывающий используемый узел замены при выполнении операций шифрования и вычисления имитовставки;

– параметры алгоритма электронной подписи (ЭП) по ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 - используемый набор параметров эллиптической кривой при генерации ключей ЭП;

– параметры алгоритма Диффи-Хелмана для ключей по ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 - используемый набор параметров эллиптической кривой при генерации ключей ЭП и закрытых ключей шифрования, а также эфемерных закрытых ключей шифрования.

Для этого необходимо перейти на закладку «Сервис» и выбрать требуемые значения параметров из списков (Рисунок 23).

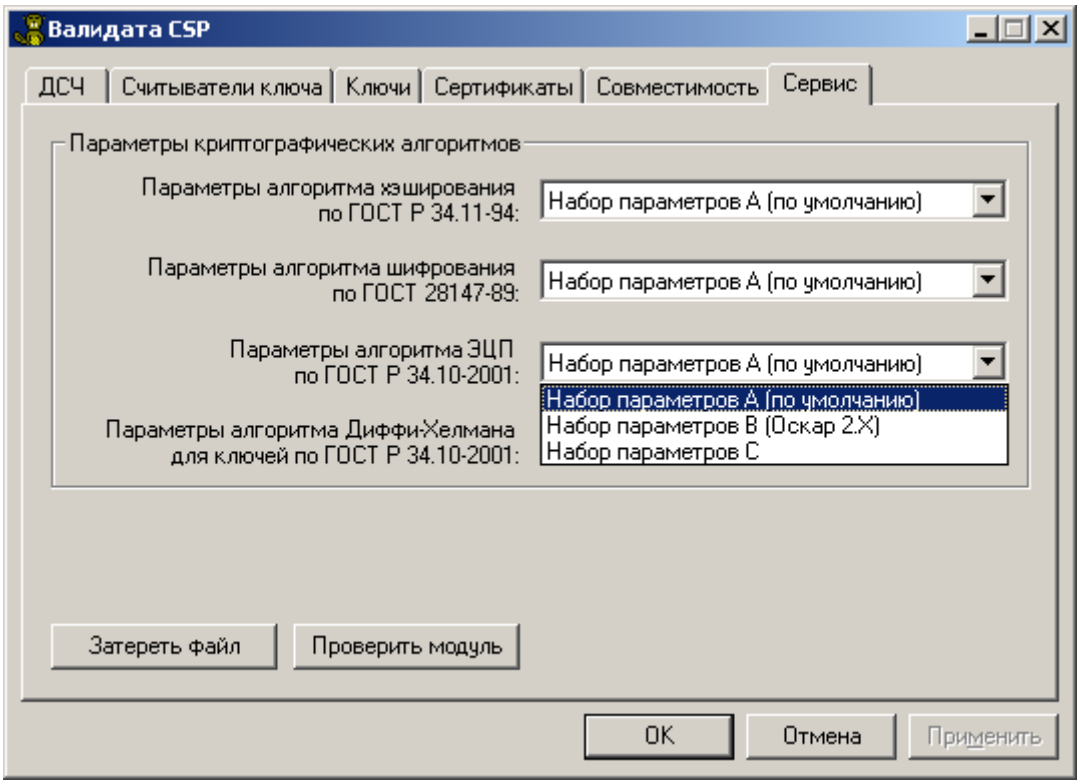

Рисунок 23 – Изменение параметров криптоалгоритмов

Для того чтобы сделанные изменения вступили в силу, нажмите кнопку «Применить». Следует иметь в виду, что настройка параметров криптографических алгоритмов имеет значение только для работы с ключами в формате СКЗИ СКАД «Сигнатура» версии 5 и квалифицированными сертификатами. При использовании ключей ЭП (закрытых ключей шифрования) и сертификатов, совместимых с СКЗИ СКАД «Сигнатура» всегда используется набор параметров криптографических алгоритмов A.

3.2 Протоколирование событий

3.2.1 Настройка протоколирования

СКЗИ «Валидата CSP»поддерживает пять типов протоколируемых событий:

– критические ошибки;

– ошибки;

– предупреждения;

– информационные сообщения;

– отладочные сообщения.

Протоколируемые события записываются в системный журнал «Приложения» от следующих источников:

– VDCSP - события криптографического провайдера интерфейса CSP;

– VDCNG - события криптографического провайдера интерфейса CNG;

– VDSSP - события Программного модуля поддержки TLS.

По умолчанию включено протоколирование критических ошибок, но, при необходимости, может быть включено протоколирование и остальных типов событий. Для источников событий

VDCSP и VDCNG может быть включено протоколирование только критических ошибок. Типы протоколируемых событий указываются соответственно источникам в значениях переменных VD_LOGMASK_CSP, VD_LOGMASK_CNG и VD_LOGMASK_SSP (типа DWORD) ключа реестра **«HKLM\System\CurrentControlSet\Control\Session Manager\Debug Print Filter»**. Каждому типу события соответствует своя маска - если она включена в значение данной переменной, то протоколирование данного типа событий от соответствующего источника будет выполняться:

- критические ошибки - 16;
- ошибки - 32;
- предупреждения - 64;
- информационные сообщения - 128;
- отладочные сообщения - 256.

Например, для протоколирования критических ошибок, ошибок и отладочных сообщений от источника VDCSP значение переменной VD_LOGMASK_CSP должно быть равно 16 + 32 + 256 = 304. Для протоколирования всех типов событий установите значение этой переменной равным 16 + 32 + 64 + 128 + 256 = 496, а для восстановления режима протоколирования по умолчанию установите ее значение равным 16.

3.2.2 Протоколирование в Конфигурационной программе

Дополнительно, Конфигурационная программа вне зависимости от настроек в реестре протоколирует следующие события (от имени источника VDCSP):

- начало и завершение сеанса работы Конфигурационной программы;
- возникновение ошибок при работе Конфигурационной программы;
- преобразование, копирование и удаление ключей;
- изменение параметров криптографических алгоритмов;
- изменение параметров кэширования ключей;
- уничтожение файлов.

ПЕРЕЧЕНЬ РИСУНКОВ

1 Начальный диалог установки . . . 5
2 Диалог ввода номера продукта . . . 6
3 Сообщение о неверном ключе установки . . . 6
4 Диалог выбора типа установки . . . 7
5 Выборочный тип установки . . . 8
6 Диалог готовности к установке . . . 8
7 Диалог завершения установки . . . 9
8 Диалог перезагрузки ОС . . . 9
9 Диалог подтверждения удаления . . . 10
10 Диалог перезагрузки ОС . . . 10
11 Главное окно программы . . . 11
12 Информация о программе . . . 11
13 Диалог выбора ДСЧ . . . 12
14 ДСЧ для всех пользователей выбран . . . 13
15 Включена опция выбора типа ДСЧ пользователями . . . 14
16 Закладка «Считыватели ключа» . . . 15
17 Диалог выбора считывателя ключа . . . 15
18 Считыватель для всех пользователей выбран . . . 16
19 Включена опция выбора считывателя ключа пользователями . . . 16
20 Закладка «Ключи» . . . 17
21 Закладка «Совместимость» . . . 18
22 Диалог выбора сертификата отправителя . . . 19
23 Изменение параметров криптоалгоритмов . . . 20

Лист регистрации изменений

Номера листов (страниц)					Всего листов (страниц) в докум	№ документа	Входящий № сопроводительного докум и дата	Подп	Дата
Изм	изменённых	заменённых	новых	аннулированных					