ООО «ВАЛИДАТА»

УТВЕРЖДЕН
ВАМБ.00060-06–ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ «ВАЛИДАТА CSP» ВЕРСИЯ 6

Руководство по установке и настройке

ВАМБ.00060-06 91 01

2020

Аннотация

Данный документ содержит описание процесса установки, удаления и настройки программного комплекса (ПК) ВАМБ.00060-06 «СКЗИ «Валидата CSP» версия 6» (далее по тексту — СКЗИ «Валидата CSP»).

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

Содержание

1 НАЗНАЧЕНИЕ

Выполняемые 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 УСТАНОВКА И УДАЛЕНИЕ СКЗИ «ВАЛИДАТА CSP»

Перед установкой СКЗИ «Валидата CSP» необходимо удалить предыдущие версии СКЗИ «Валидата CSP», если они были ранее установлены.

Перед установкой СКЗИ «Валидата CSP» (исполнение 3), в целях обеспечения защиты по классу КС3, необходимо установить средства создания замкнутой программной среды из перечня, приведенного в документе ВАМБ.00060-06 30 01 «СКЗИ «Валидата CSP» версия 6. Формуляр». При установке средств создания замкнутой программной среды необходимо руководствоваться соответствующей документацией.

Перед установкой СКЗИ «Валидата CSP» необходимо проверить целостность установочного комплекта с помощью программы контроля целостности **hashfile.exe**, находящейся на передаточном носителе.

Описание работы с программой контроля целостности, требования и порядок проведения процедуры контроля целостности описаны в документах ВАМБ.00060-06 93 02 «СКЗИ «Валидата CSP» версия 6. Контроль целостности. Руководство администратора информационной безопасности» и ВАМБ.00060-06 92 01 «СКЗИ «Валидата CSP» версия 6. Программа контроля целостности. Руководство пользователя».

2.1 Установка СКЗИ «Валидата CSP»

Для установки СКЗИ «Валидата CSP» необходимо запустить процесс установки следующим образом:

– извлечь во временный каталог файл дистрибутива ПО (**acsptls_x86.msi** для ОС Microsoft Windows x86 или **acsptls_AMD64.msi** для ОС Microsoft Windows x64) из поставляемого на дистрибутивном носителе архива;

– запустить командную строку посредством щелчка правой кнопки «мыши» по иконке «Командная строка», находящейся в программной группе «Стандартные», и выбора пункта контекстного меню «Запуск с правами администратора»;

– ввести в появившемся окне командной строки полный путь и имя файла дистрибутива ПО и нажать кнопку «Ввод».

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

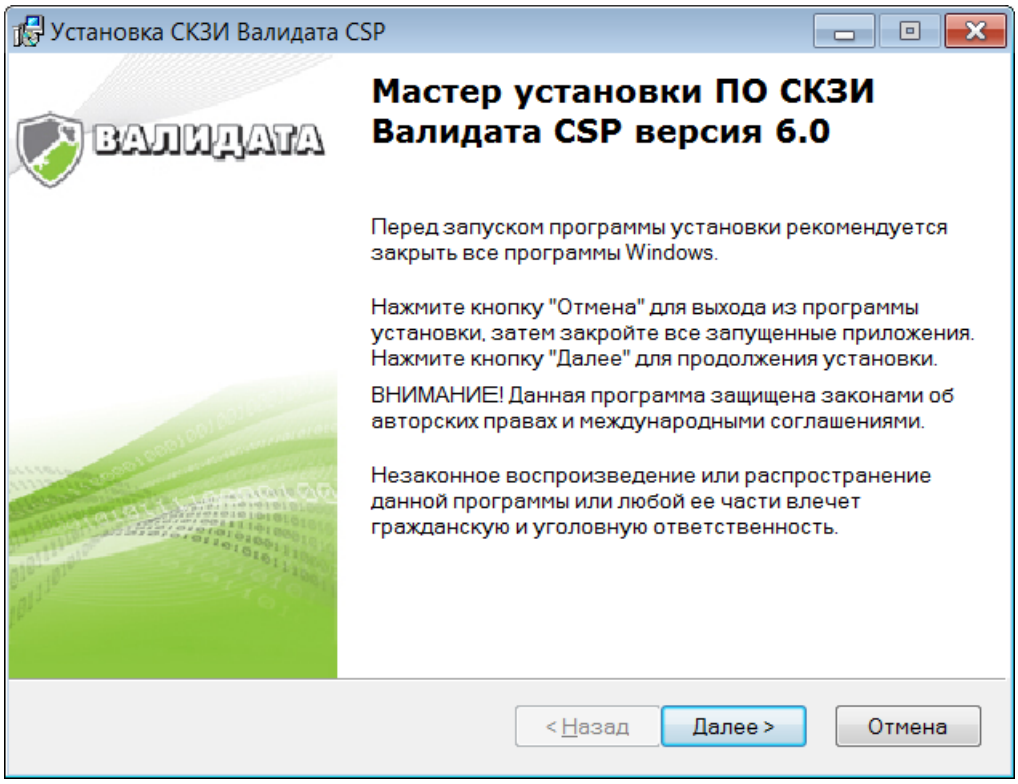

Рисунок 1 – Начальный диалог установки

Нажмите кнопку «Далее». В следующем диалоге укажите имя пользователя и наименование организации (Рисунок 2).

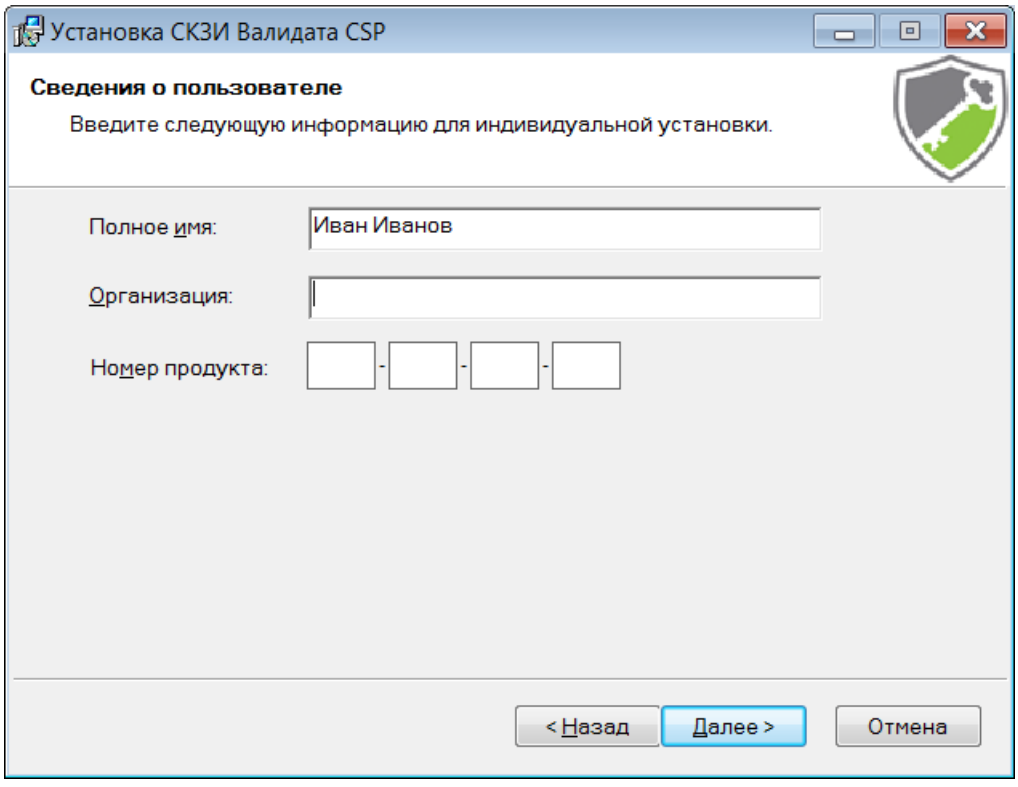

Рисунок 2 – Сведения о пользователе

Нажмите кнопку «Далее». Отображается диалог выбора типа установки (Рисунок 3).

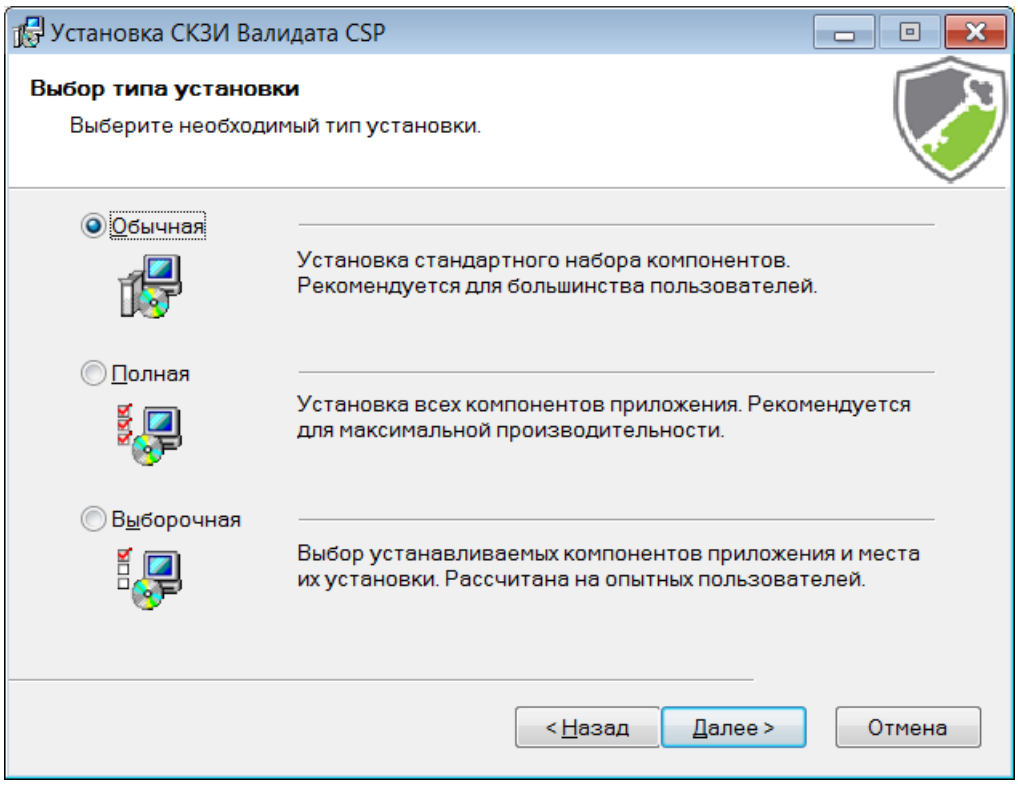

Рисунок 3 – Диалог выбора типа установки

Необходимо выбрать тип установки и нажать 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 Графический интерфейс пользователя сервисов, Биологический ДСЧ, Считыватели Съемный Диск (сменные USB-носители типа Flash), ruToken, eToken, vdToken (ФКН) и vdToken, Утилита копирования ключа СКЗИ «Валидата CSP», а также Поддержка протокола TLS и Поддержка защищенной почты в Microsoft Office Outlook. Выборочный тип установки позволяет пользователю самостоятельно указать все необходимые компоненты для установки (Рисунок 4).

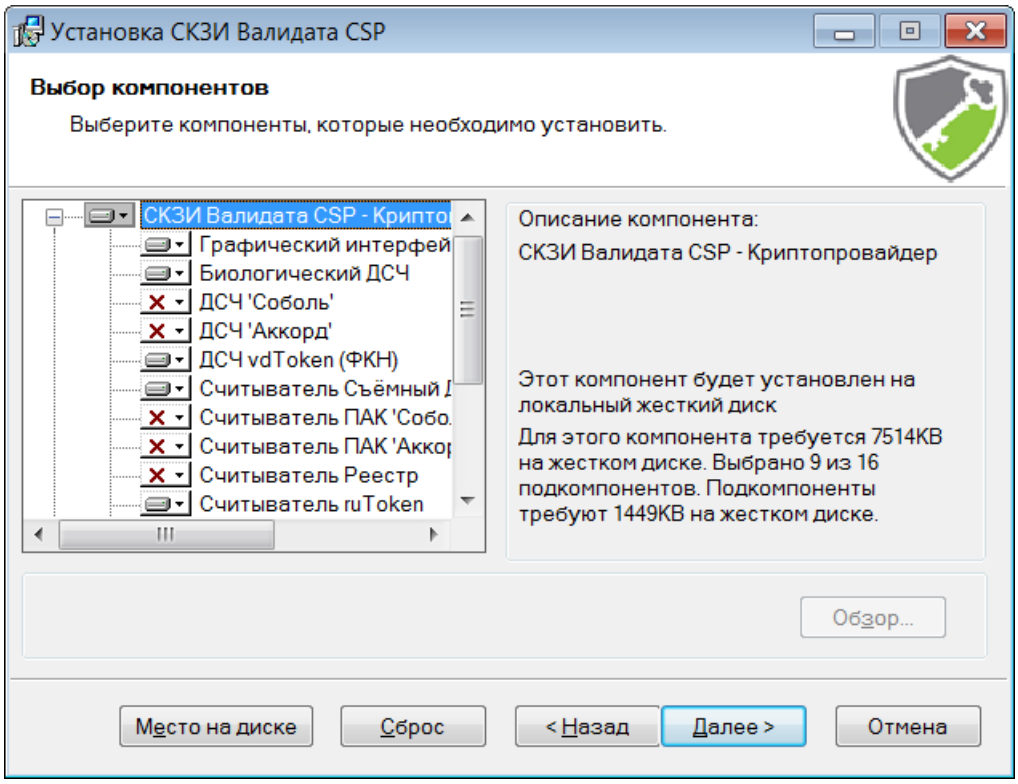

Рисунок 4 – Тип установки «Выборочная»

Выбрав нужные для установки компоненты, необходимо нажать кнопку «Далее». Появится диалог о готовности к установке (Рисунок 5).

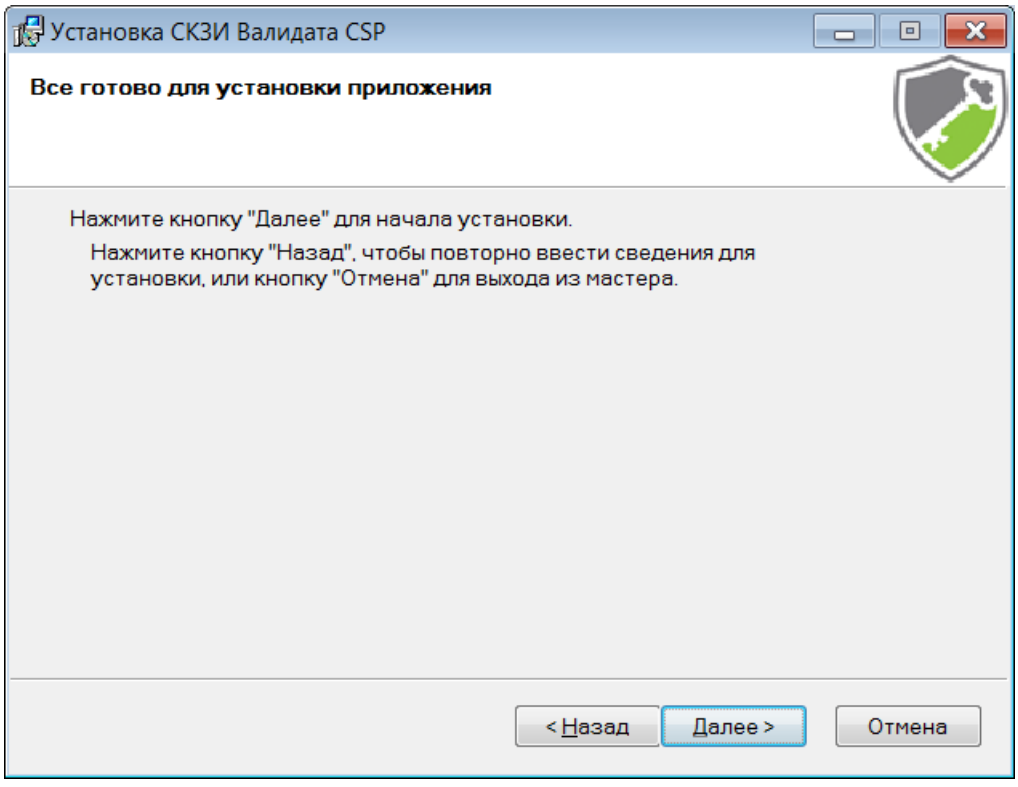

Рисунок 5 – Диалог готовности к установке

После отображения диалога о готовности к установке необходимо нажать кнопку «Далее» для проведения установки с указанными параметрами.

После установки СКЗИ «Валидата CSP» автоматически запускается процедура инициализации ДСЧ (Рисунок 6).

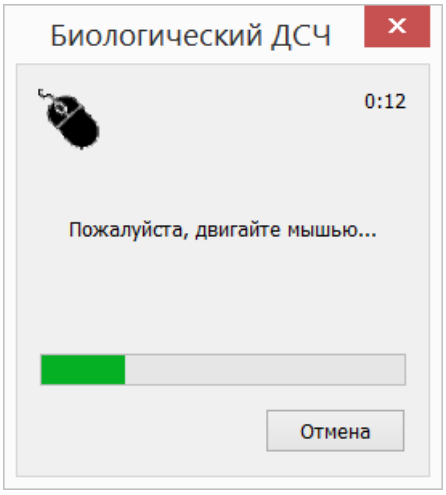

Рисунок 6 – Инициализация ДСЧ

Рекомендации по выполнению инициализации ДСЧ приведены в документе ВАМБ.00060-06 95 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора».

Примечание – Возникновение ошибки инициализации ДСЧ или отсутствие окна инициализации на завершающем этапе установки не является препятствием для успешного завершения установки. ДСЧ можно будет инициализировать после установки, например, запустив программу конфигурации СКЗИ.

По завершении процесса установки и инициализации ДСЧ будет выдан диалог о завершении процесса установки (Рисунок 7).

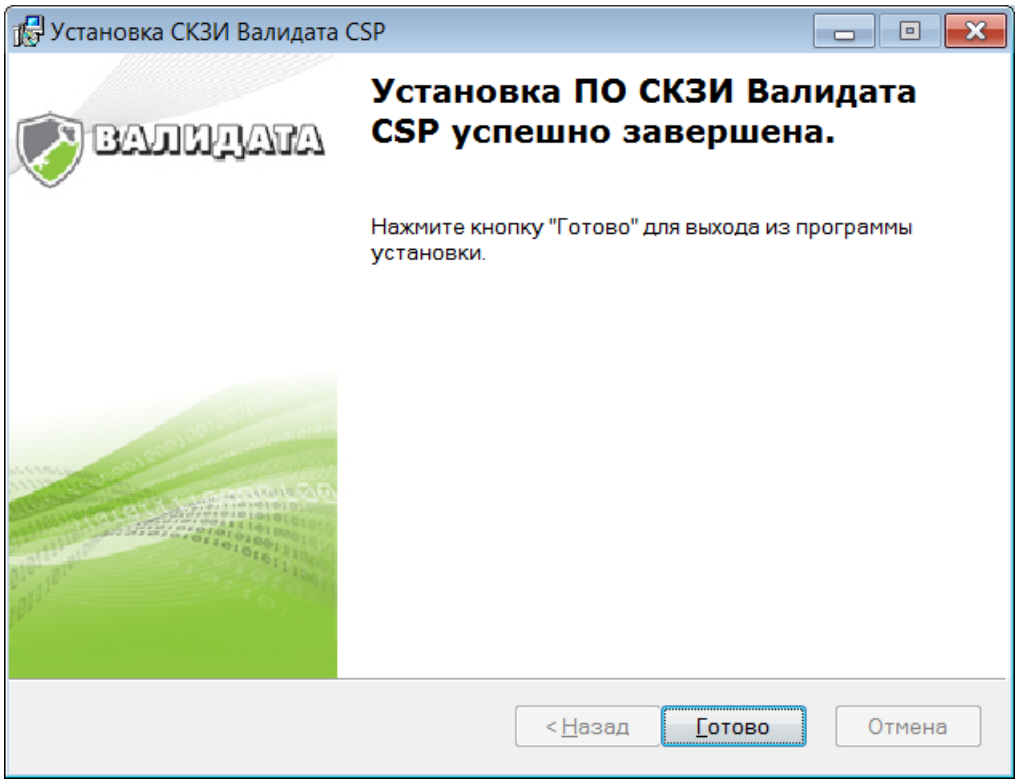

Рисунок 7 – Диалог завершения установки

Необходимо нажать кнопку «Готово».

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

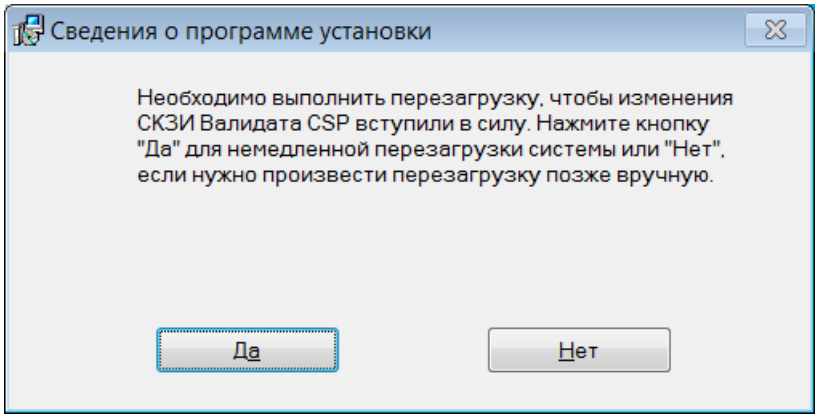

Рисунок 8 – Диалог перезагрузки ОС

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».

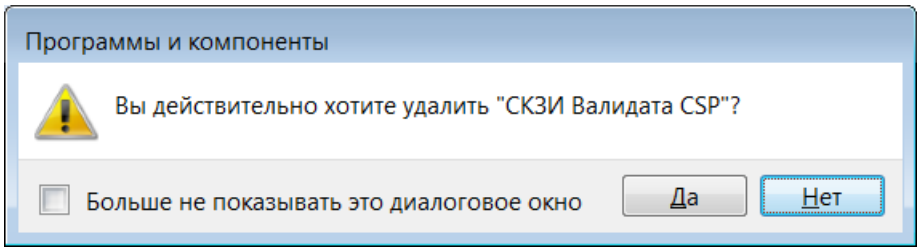

Рисунок 9 – Диалог подтверждения удаления

По окончании удаления ПО будет выдано диалоговое окно, запрашивающее выполнение перезагрузки ОС (Рисунок 8). Необходимо нажать кнопку «Да».

3 УСТАНОВКА И УДАЛЕНИЕ СКЗИ «ВАЛИДАТА CSP» БЕЗ ВЫВОДА ПОЛЬЗОВАТЕЛЬСКОГО ИНТЕРФЕЙСА (В «ТИХОМ» РЕЖИМЕ)

Установка и удаление программного обеспечения (ПО) выполняется утилитой ***msiexec.exe***, входящей в состав ОС Windows. Имя установочного файла (пакета ***MSI***) передается утилите ***msiexec.exe*** в командной строке сразу после ключа ***/i***. Имя удаляемого файла (пакета ***MSI***) передается утилите ***msiexec.exe*** в командной строке сразу после ключа ***/x***.

Для установки и удаления ПО без вывода пользовательского интерфейса утилите ***msiexec.exe*** необходимо в командной строке передать ключ ***/qn***.

Для указания устанавливаемых функциональных возможностей ПО необходимо перечислить их идентификаторы через запятую после параметра ***ADDLOCAL=*** командной строки (без пробелов).

Ниже (Таблица 1) приведен перечень функциональных возможностей СКЗИ «Валидата CSP» и соответствующих им идентификаторов установки.

Таблица 1 – Идентификаторы установки

Идентификатор	**Функциональная возможность СКЗИ «Валидата CSP»**
	Библиотеки ДСЧ
feGIPS	Графический интерфейс пользователя сервисов
feBioRnd	Биологический ДСЧ (устанавливается во всех случаях)
feSobolRnd	ДСЧ Соболь
feAccrdRnd	ДСЧ Аккорд
fevdTokenFCRnd	ДСЧ vdToken (ФКН)
	Библиотеки считывателей
feFlashRdr	Считыватель Съёмный Диск (устанавливается во всех случаях)
feSobolRdr	Считыватель ПАК «Соболь»
feAccrdRdr	Считыватель ПАК «Аккорд»
feruTokenRdr	Считыватель ruToken
feeTokenRdr	Считыватель eToken
feJaCartaRdr	Считыватель JaCarta
fevdTokenFCRdr	Считыватель vdToken (ФКН)
fevdTokenRdr	Считыватель vdToken
feDallasRdr	Считыватель Dallas
feSecretNetRdr	Считыватель ПАК Secret Net
	Модуль поддержки TLS
feTLSSupport	Поддержка протокола TLS
feOutlookSupport	Поддержка защищенной почты в Microsoft Office Outlook
feWinlogonSupport	Поддержка входа в Microsoft Active Directory по протоколу Kerberos

Пример установки СКЗИ «Валидата CSP» со считывателями vdToken (ФКН) и vdToken и модулем поддержки TLS:

```
msiexec.exe /qn /i acsptls_AMD64.msi ADDLOCAL=fevdTokenFCRdr,fevdTokenRdr,
feTLSSupport
```

Пример удаления СКЗИ «Валидата CSP»:

```
msiexec.exe /qn /x acsptls_AMD64.msi
```

4 НАСТРОЙКА СКЗИ «ВАЛИДАТА CSP»

4.1 Программа конфигурации СКЗИ «Валидата CSP»

4.1.1 Запуск программы конфигурации

Для запуска программы конфигурации СКЗИ «Валидата CSP» необходимо вызвать пункт меню «Пуск»->«Программы»->«СКЗИ Валидата CSP»->«Программа конфигурации СКЗИ». На экране появится главное окно программы (Рисунок 10).

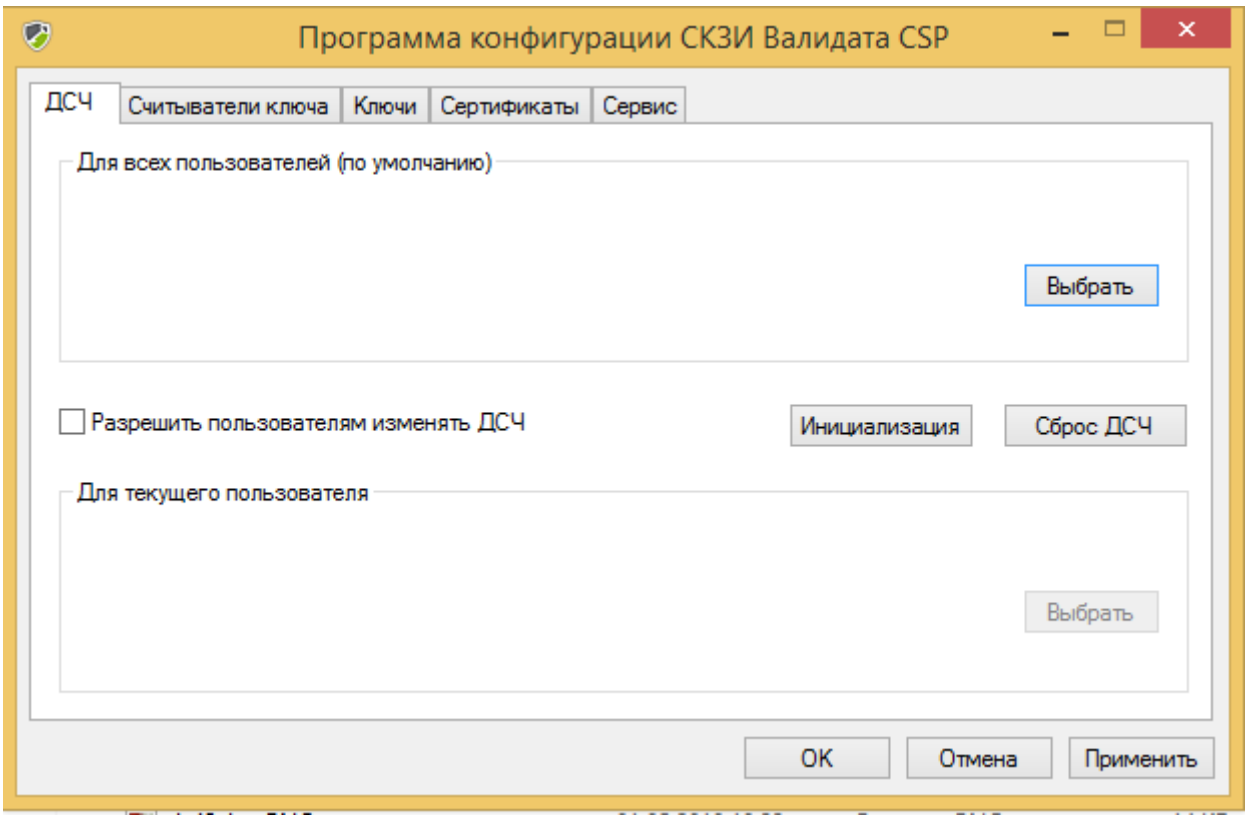

Рисунок 10 – Главное окно программы

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

Вы можете просмотреть информацию о версии программы конфигурации СКЗИ «Валидата CSP», выбрав в системном меню (в левом верхнем углу) пункт «О программе. . . », появится информация о программе (Рисунок 11).

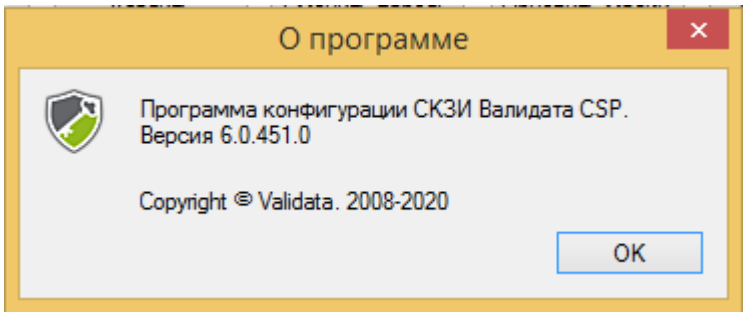

Рисунок 11 – Информация о программе

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

4.1.2 Настройка программного модуля считывания ДСЧ

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

В поставку СКЗИ «Валидата CSP» входит несколько программных модулей считывания ДСЧ, системный 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 12).

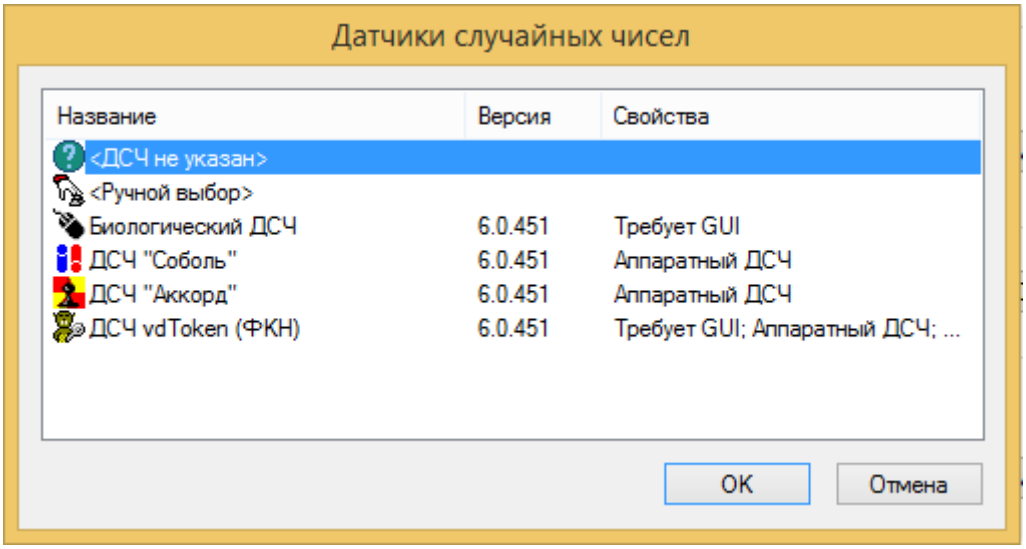

Рисунок 12 – Диалог выбора ДСЧ

Выберите ДСЧ и нажмите кнопку «ОК». На экране появится исходное окно с информацией о выбранном ДСЧ (Рисунок 13).

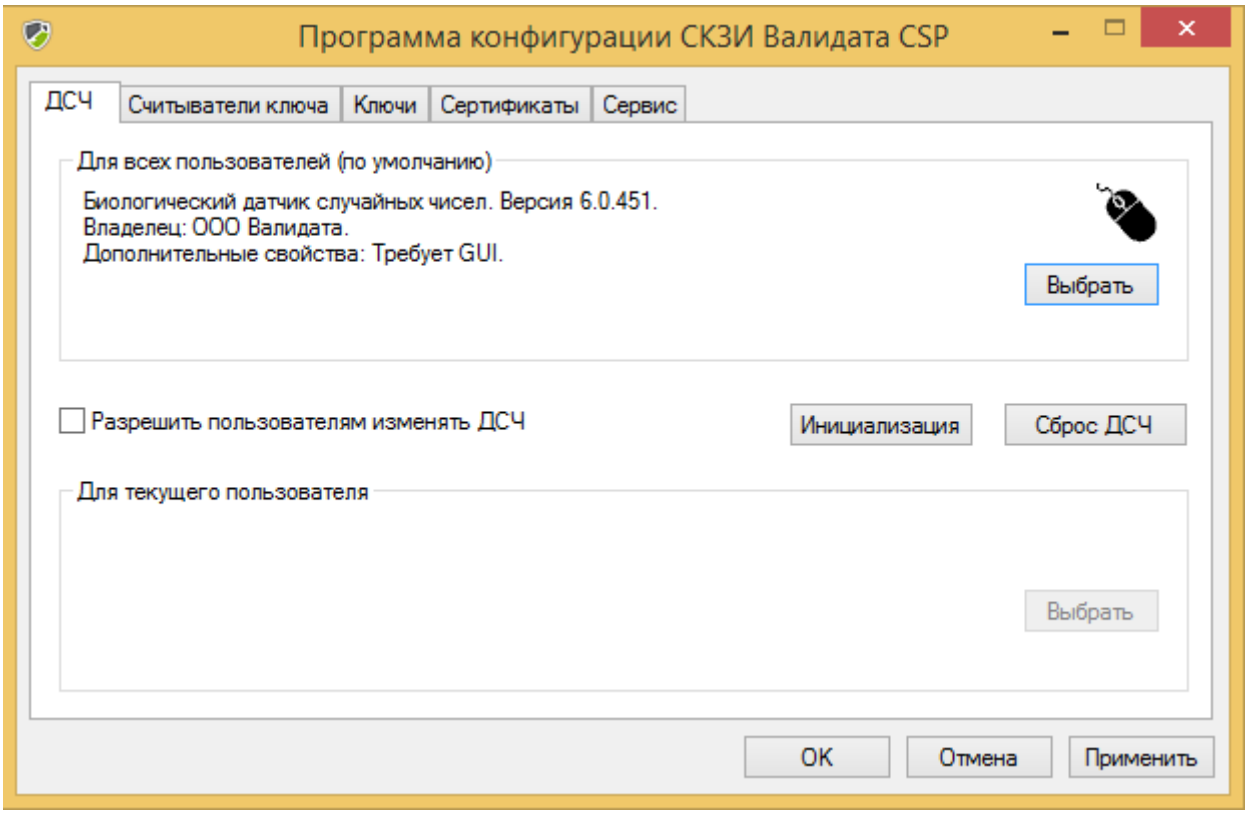

Рисунок 13 – ДСЧ для всех пользователей выбран

Системный 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 14).

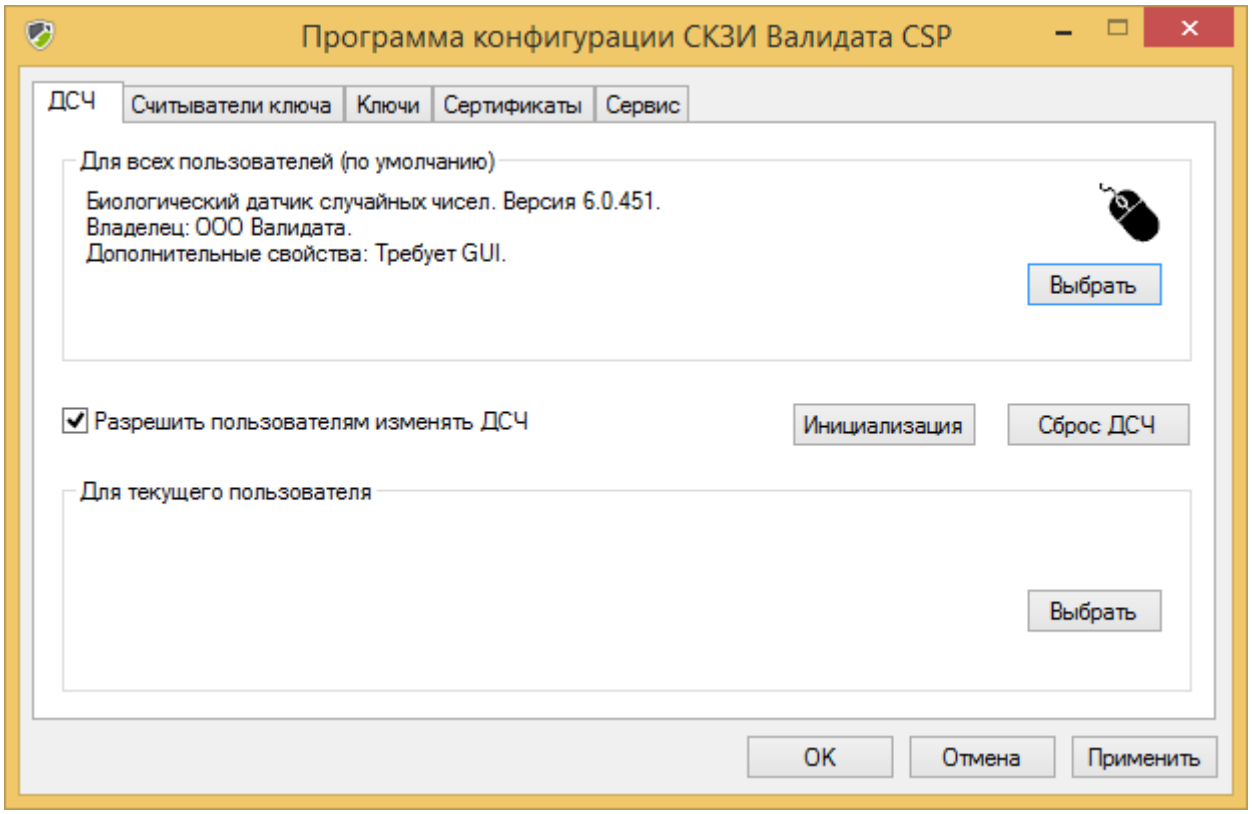

Рисунок 14 – Включена опция выбора типа ДСЧ пользователями

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

4.1.3 Настройка программных модулей считывателей ключа

Настройка программных модулей считывателей ключа (далее - считывателей ключа) производится на вкладке «Считыватели ключа» (Рисунок 15).

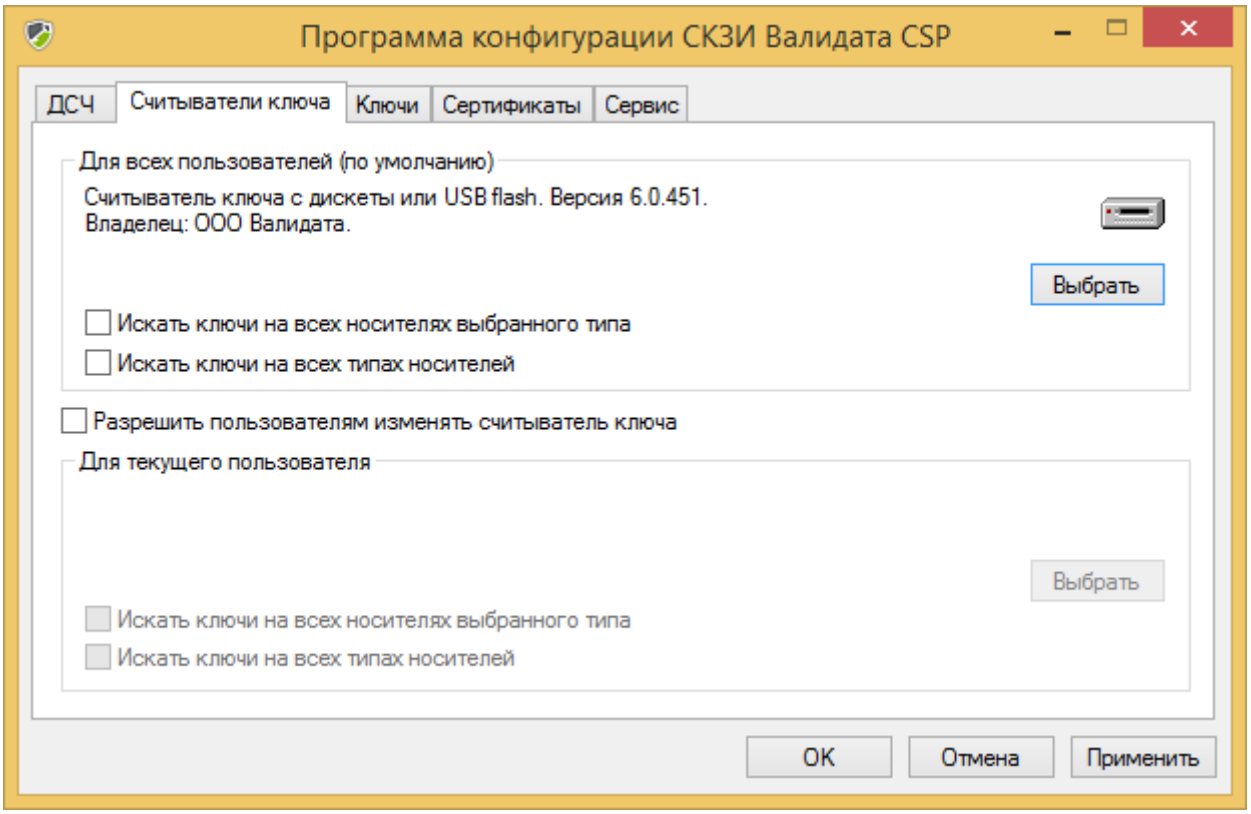

Рисунок 15 – Вкладка «Считыватели ключа»

СКЗИ «Валидата CSP» может работать с различными типами считывателей ключей, системный 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 16).

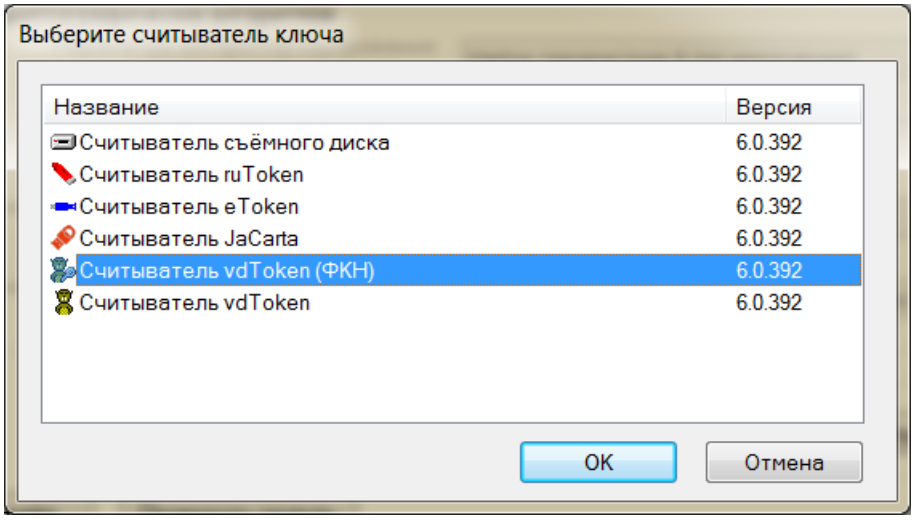

Рисунок 16 – Диалог выбора считывателя ключа

Выберите считыватель и нажмите кнопку «OK». На экране появится исходное окно с информацией о выбранном считывателе ключа (Рисунок 17).

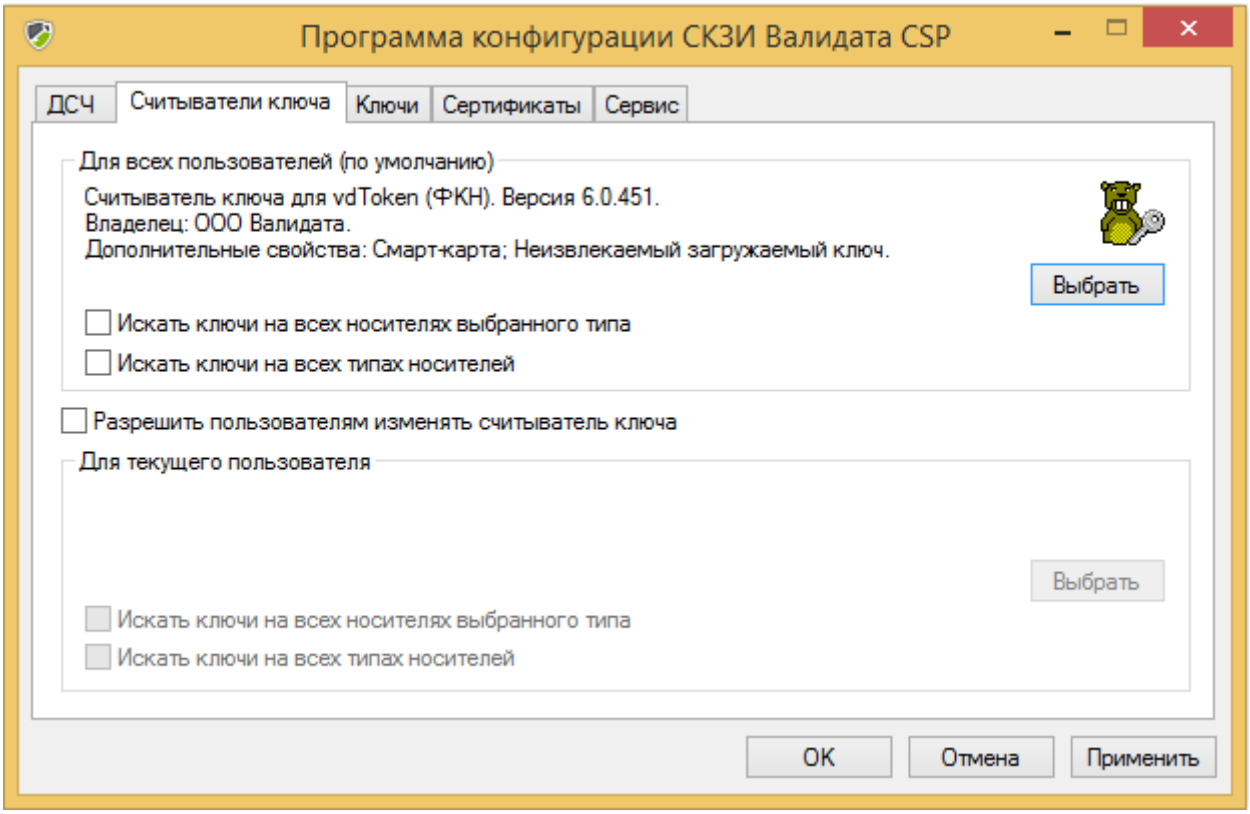

Рисунок 17 – Считыватель для всех пользователей выбран

Если в диалоге (Рисунок 16) выбрать пункт «**Считыватель не указан**», то при обращении к ключам может выдаваться дополнительный диалог выбора считывателя ключа.

Администратор может установить режим «**Искать ключи на всех носителях выбранного типа**». В этом случае 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.

Дополнительно может быть установлен режим «**Искать ключи на всех типах носителей**». В этом случае 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.

Системный администратор может разрешить пользователям изменять выбор считывателя, для этого необходимо выбрать соответствующую опцию, после чего станет доступной кнопка «**Выбрать**» в нижней части диалога.

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

4.1.4 Настройка параметров работы с ключами

Системный администратор может настраивать параметры работы с ключами, перейдя на вкладку «Ключи» (Рисунок 18).

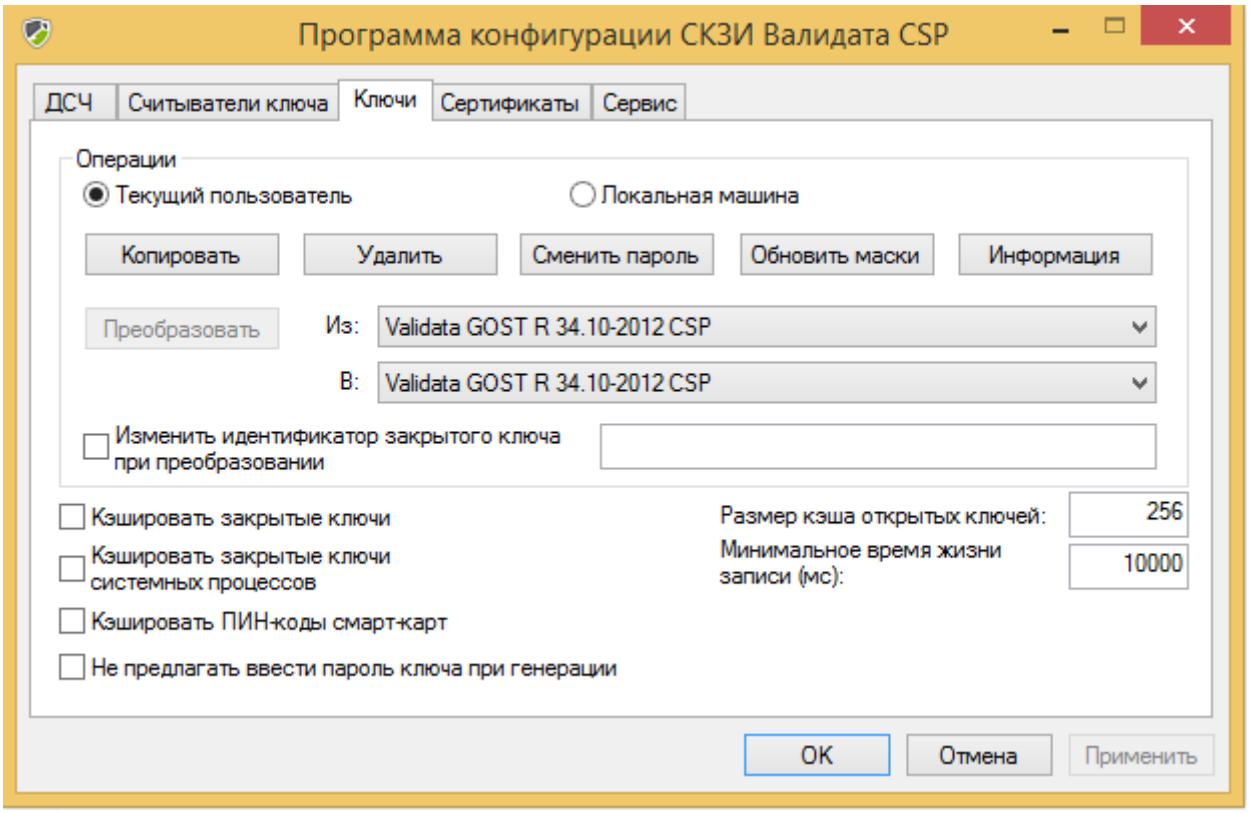

Рисунок 18 – Вкладка «Ключи»

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. Системный 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 системного администратора. Размер кэша практически не ограничен.

Кэширование ключей проверки ЭП по умолчанию включено, и размер кэша составляет 16 записей. Системный администратор может установить другое значение **«Размер кэша открытых ключей»** (не более 65535 записей) или полностью выключить кэширование, установив этот параметр в 0. Кроме того, системный 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.

4.1.5 Настройка криптографических алгоритмов

Администратор может настроить криптографические алгоритмы, используемые по умолчанию для выполнения криптографических преобразований. Для этого используется вкладка «Сервис» (Рисунок 19).

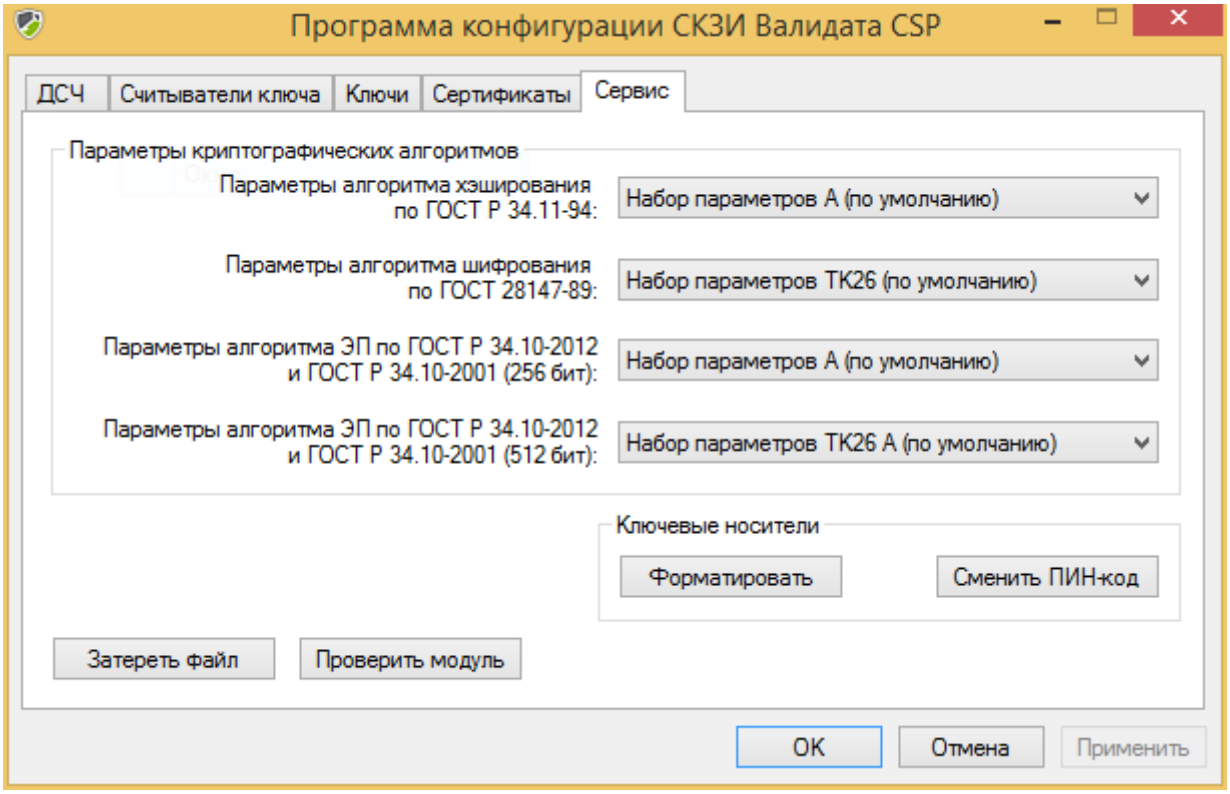

Рисунок 19 – Настройка криптографических алгоритмов

Нажмите кнопку «Применить» для сохранения и применения изменений.

4.2 Протоколирование событий

4.2.1 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.

4.2.2 Протоколирование в программе конфигурации

Программа конфигурации вне зависимости от настроек в реестре протоколирует следующие события (от имени источника VDCSP):

– начало и завершение сеанса работы программы конфигурации;

– возникновение ошибок при работе программы конфигурации;
– преобразование, копирование и удаление ключей;
– изменение параметров криптографических алгоритмов;
– изменение параметров кэширования ключей;
– уничтожение файлов.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

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

ПЕРЕЧЕНЬ РИСУНКОВ

Лист регистрации изменений

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