

ООО «ВАЛИДАТА»

УТВЕРЖДЕН
ВАМБ.00060-06-ЛУ

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

ПРОГРАММНО-АППАРАТНЫЙ МОДУЛЬ БЕЗОПАСНОСТИ «VDHSM»

Руководство пользователя

ВАМБ.00060-06 92 04

2022

Аннотация

Настоящий документ содержит описание применения ВАМБ.00138-01 программно-аппаратного модуля безопасности «vdHSM» (далее — ПАМБ «vdHSM») в программном комплексе (ПК) ВАМБ.00060-06 «Средство криптографической защиты информации «Валидата CSP» версия 6» (далее — СКЗИ «Валидата CSP»), а также в ПК, использующих СКЗИ «Валидата CSP».

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

Содержание

1	ОБЩЕЕ ОПИСАНИЕ	4
1.1	Назначение	4
1.2	Условия применения	4
1.3	Сроки действия ключей ЭП	4
2	ПОДГОТОВКА К ПРИМЕНЕНИЮ	5
2.1	Инициализация устройства ПАМБ «vdHSM»	5
2.2	Просмотр информации о ключах	8
3	РАБОТА С КЛЮЧАМИ	10
3.1	Создание ключа на носителе	10
3.2	Удаление ключа с носителя	10
3.3	Копирование ключей	12
	ПЕРЕЧЕНЬ СОКРАЩЕНИЙ	12
	ПЕРЕЧЕНЬ РИСУНКОВ	14

1 ОБЩЕЕ ОПИСАНИЕ

1.1 Назначение

ВАМБ.00138-01 «Программно-аппаратный модуль безопасности “vdHSM”» (далее — ПАМБ «vdHSM») представляет собой ключевой носитель, который предназначен для хранения и использования ключей электронной подписи (ЭП) пользователей программного комплекса (ПК) ВАМБ.00060-06 «Средство криптографической защиты информации «Валидата CSP» версия 6» (далее — СКЗИ «Валидата CSP»).

СКЗИ «Валидата CSP» не поддерживает зашифрование ключей пользователей, хранящихся на устройстве ПАМБ «vdHSM», с использованием симметричного ключа шифрования абонента.

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

ПАМБ «vdHSM» позволяет одновременно хранить разные ключи разных пользователей.

1.2 Условия применения

Эксплуатация устройства ПАМБ «vdHSM» должна выполняться согласно эксплуатационной документации данного устройства.

В настоящем документе приведены сведения об инициализации работы СКЗИ «Валидата CSP» с устройством ПАМБ «vdHSM», а также о порядке работы пользователя с его ключами, хранящимися в устройстве ПАМБ «vdHSM».

1.3 Сроки действия ключей ЭП

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

2 ПОДГОТОВКА К ПРИМЕНЕНИЮ

2.1 Инициализация устройства ПАМБ «vdHSM»

Подключение СКЗИ «Валидата CSP» к устройству ПАМБ «vdHSM» выполняется правомочной коалицией администраторов информационной безопасности ПАМБ «vdHSM» (далее — администратор информационной безопасности ПАМБ «vdHSM»).

Примечание — Подробная информация о роли администратора информационной безопасности ПАМБ «vdHSM» и определение понятия «правомочная коалиция» приведены в эксплуатационной документации устройства ПАМБ «vdHSM».

Прежде всего необходимо загрузить файл конфигурации ПАМБ «vdHSM».

Примечание — Файл конфигурации ПАМБ «vdHSM» создается на автоматизированном рабочем месте управления ПАМБ «vdHSM».

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

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

Для настройки использования устройства ПАМБ «vdHSM» для всех пользователей ЭВМ необходимо запустить программу конфигурации с правами администратора на локальном компьютере. В этом случае все действия администратора информационной безопасности ПАМБ «vdHSM» должны контролироваться системным администратором.

Для настройки использования устройства ПАМБ «vdHSM» для одного пользователя ЭВМ необходимо запустить пользовательскую программу конфигурации.

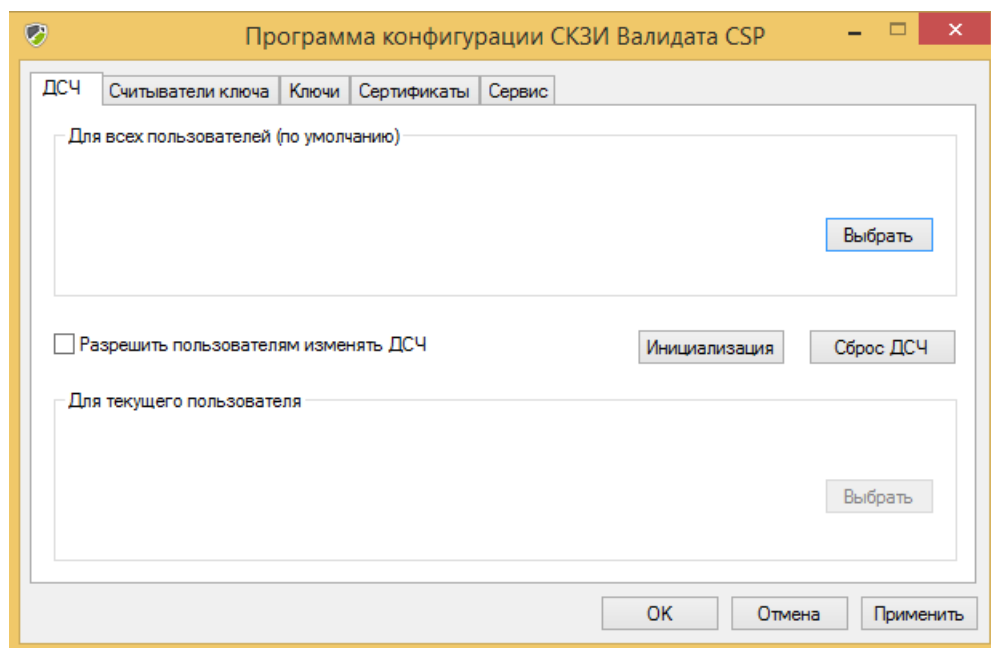


Рисунок 1 – Программа конфигурации

Выберите вкладку «Сервис» (Рисунок 2).

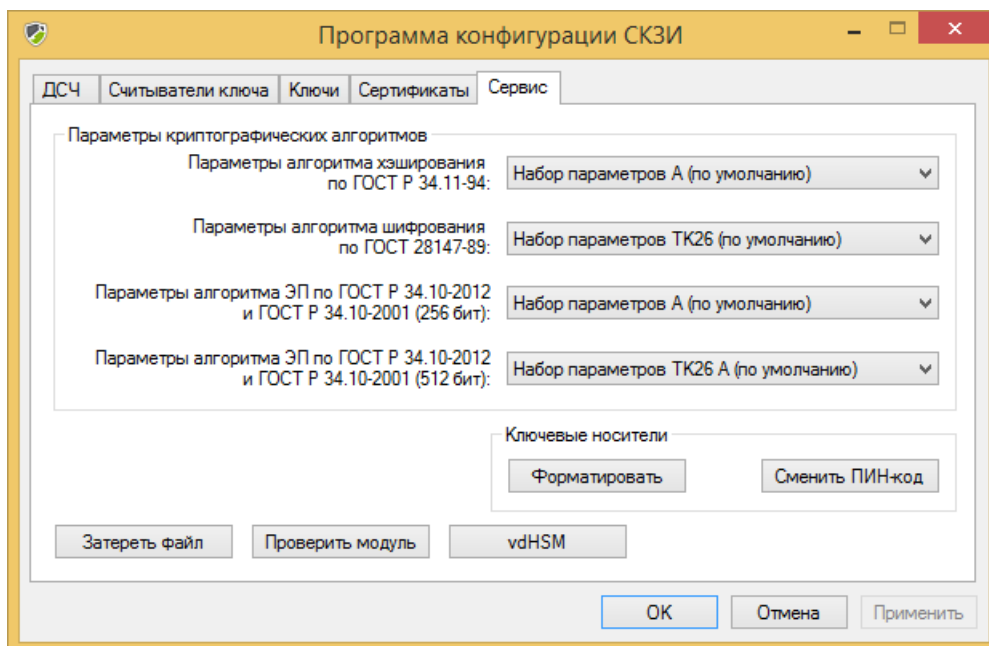


Рисунок 2 – Вкладка «Сервис»

Нажмите кнопку «vdHSM». На экран будет выдано окно, позволяющее загрузить системную или пользовательскую конфигурацию ПАМБ «vdHSM» (Рисунок 3).

В случае если были заданы и системная, и пользовательская конфигурации, СКЗИ «Валидата CSP» будет использовать пользовательскую конфигурацию для подключения к ПАМБ «vdHSM».

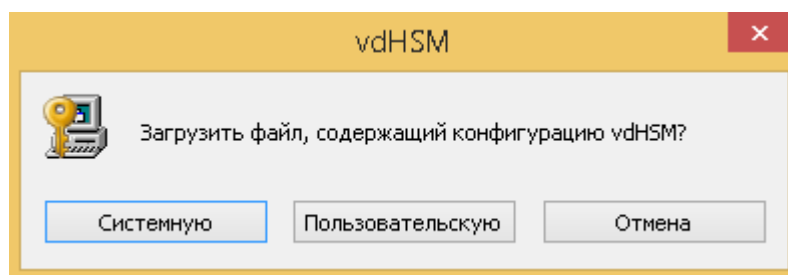


Рисунок 3 – Окно выбора типа конфигурации

Далее необходимо выбрать файл конфигурации и нажать кнопку «Загрузить» (Рисунок 4). Нажатие кнопки «Отмена» приведет к отмене загрузки конфигурации ПАМБ «vdHSM».

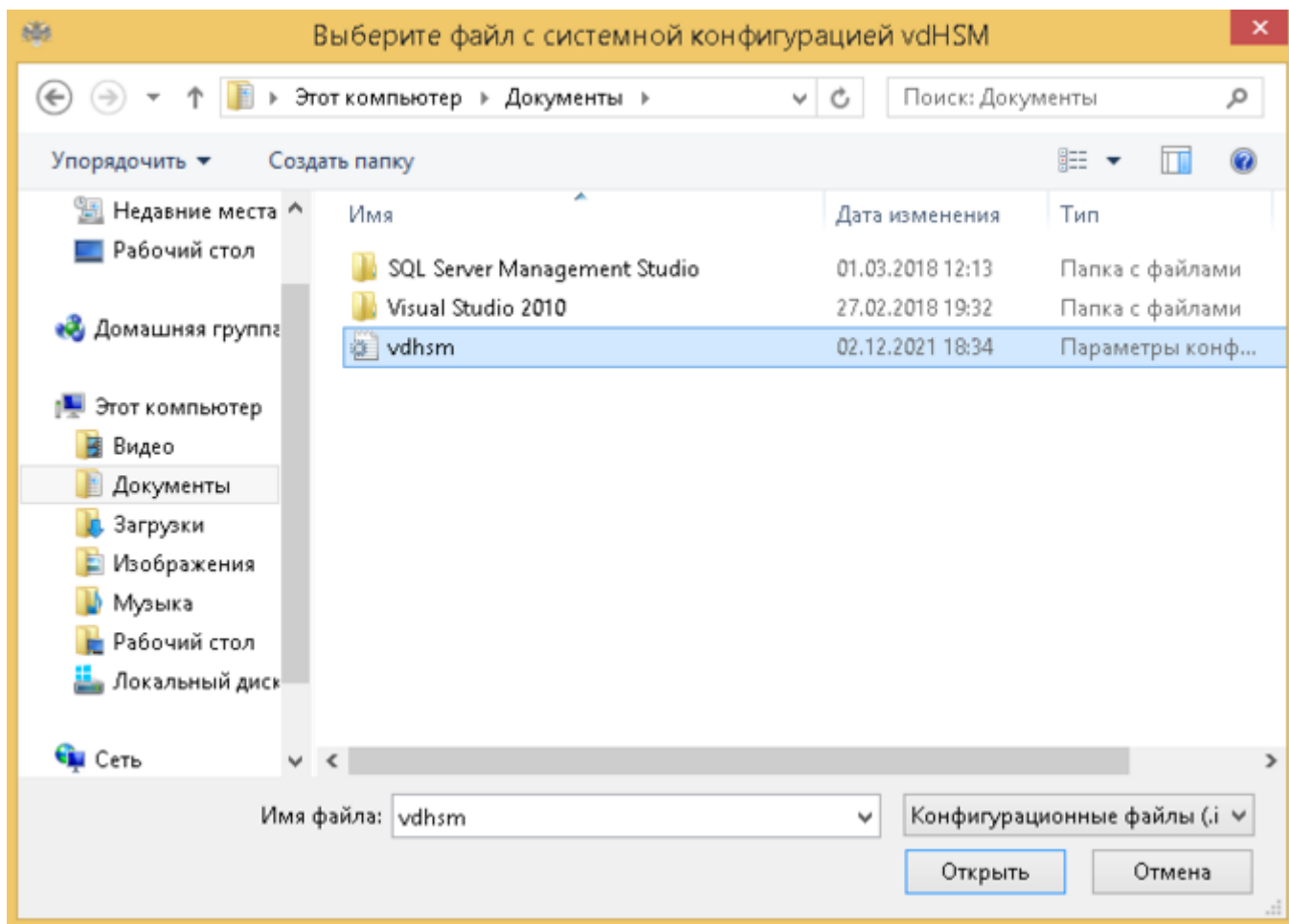


Рисунок 4 – Окно выбора файла конфигурации

При обращении к устройству ПАМБ «vdHSM» будет выполнена попытка загрузки ключа администратора информационной безопасности ПАМБ «vdHSM» (Рисунок 5). Повторная загрузка ключа администратора информационной безопасности ПАМБ «vdHSM» потребуется при смене процесса, обращающегося к устройству ПАМБ «vdHSM», например, при перезагрузке ЭВМ.

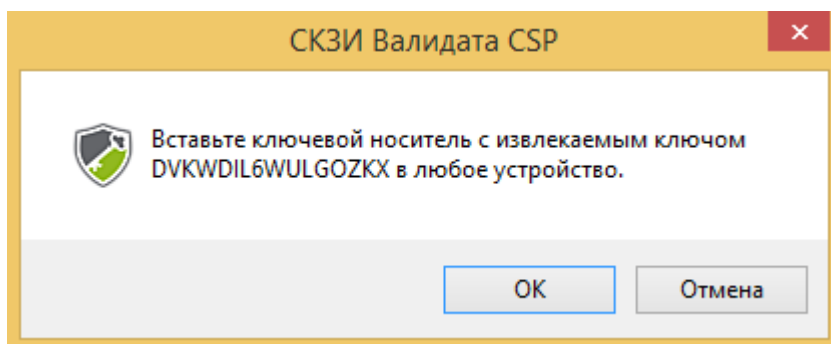


Рисунок 5 – Окно загрузки ключа

Если в устройство ПАМБ «vdHSM» не был загружен ключ администратора ключей (см. эксплуатационную документацию ПАМБ «vdHSM»), после загрузки ключа администратора информационной безопасности ПАМБ «vdHSM» будет выполнена попытка загрузки ключа администратора ключей.

Примечание — Подробная информация о роли администратора ключей ПАМБ «vdHSM» приведена в эксплуатационной документации устройства ПАМБ «vdHSM».

В целях загрузки ключа администратора информационной безопасности ПАМБ «vdHSM» или проверки доступности устройства ПАМБ «vdHSM» может использоваться операция получения информации о ключах.

2.2 Просмотр информации о ключах

Для просмотра информации о ключе нажмите кнопку «Информация» на вкладке «Ключи» (Рисунок 6).

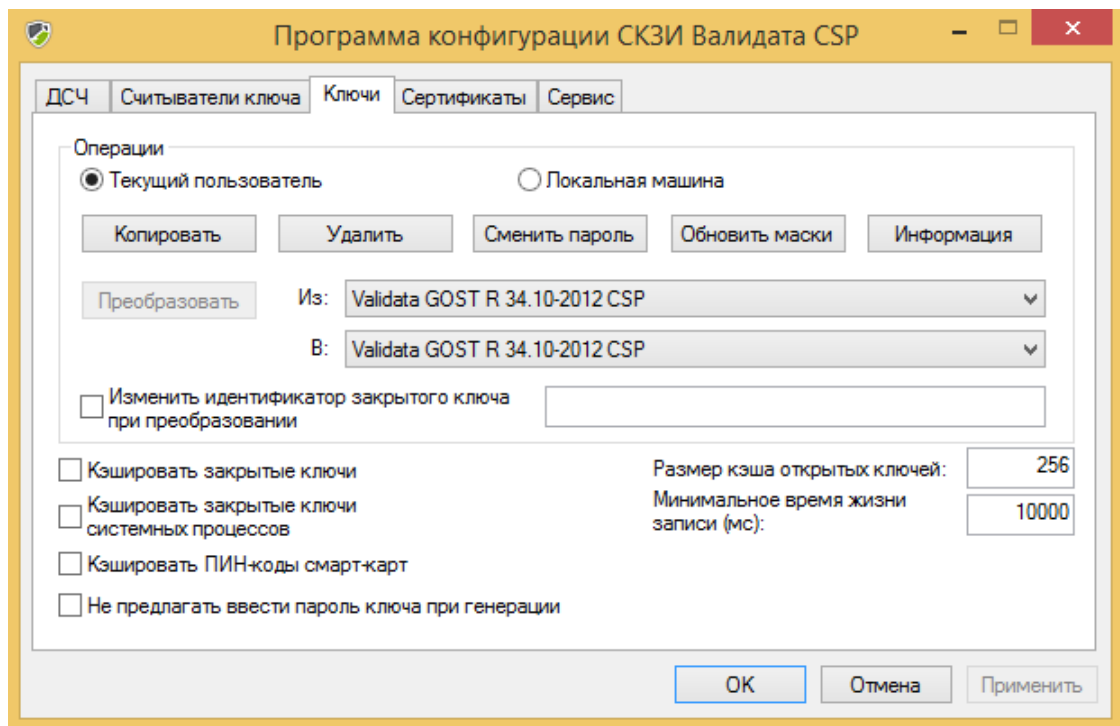



Рисунок 6 – Вкладка «Ключи»

На экран будет выведен список доступных ключей (Рисунок 7).

Ключи, находящиеся на устройстве ПАМБ «vdHSM», в интерфейсе СКЗИ «Валидата CSP» обозначены иконкой .

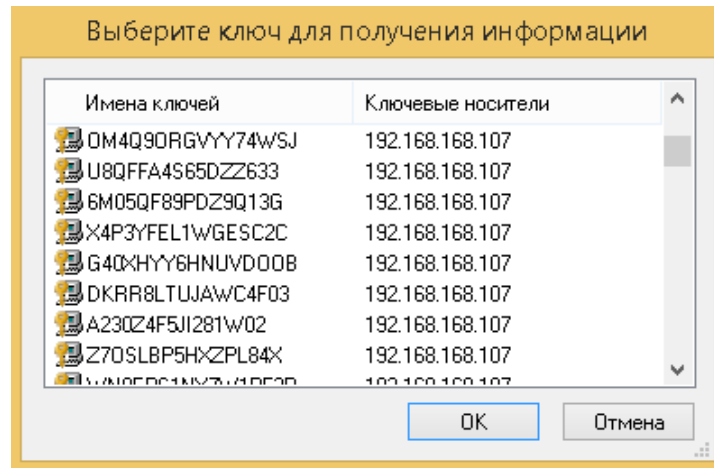


Рисунок 7 – Окно выбора ключа для получения информации

3 РАБОТА С КЛЮЧАМИ

3.1 Создание ключа на носителе

Перед созданием ключа на экран выдается предупреждение (Рисунок 8).

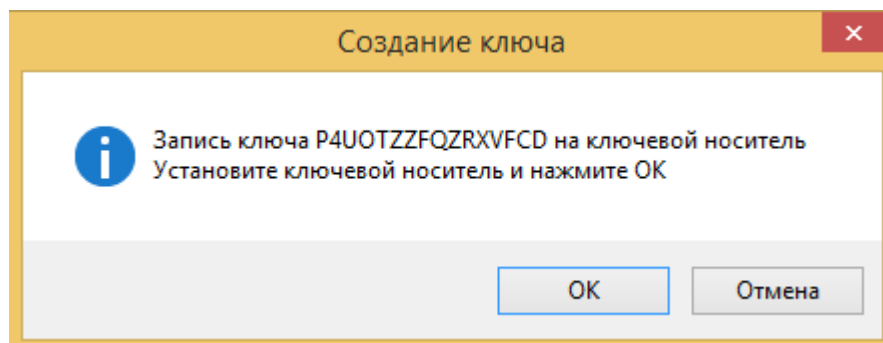


Рисунок 8 – Предупреждение при генерации ключа

Выберите считыватель ключа (Рисунок 9).

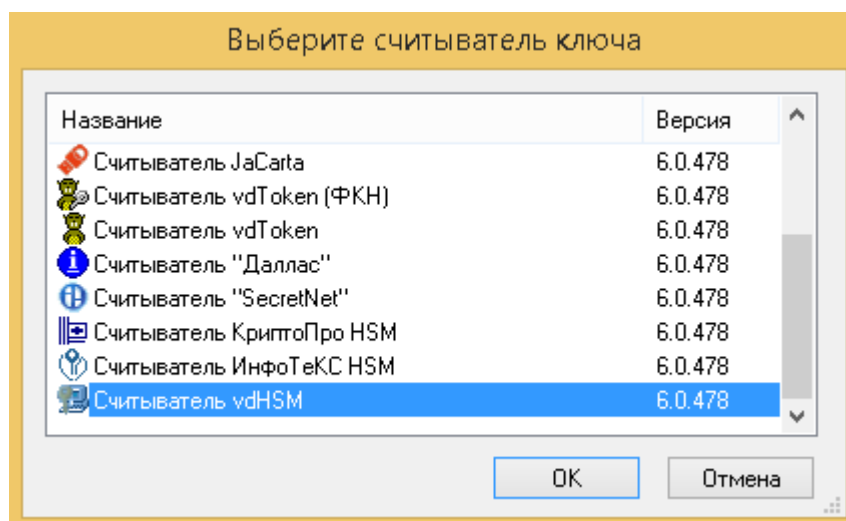


Рисунок 9 – Окно выбора считывателя ключа

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

3.2 Удаление ключа с носителя

Удаление своего ключа с ПАМБ «vdHSM» всегда доступно пользователю в программе конфигурации СКЗИ «Валидата CSP». Для этого выберите закладку «Ключи» (Рисунок 6).

Нажмите кнопку «Удалить». На экран выдается окно со списком номеров ключей и ключевых носителей, на которых они находятся (Рисунок 10).

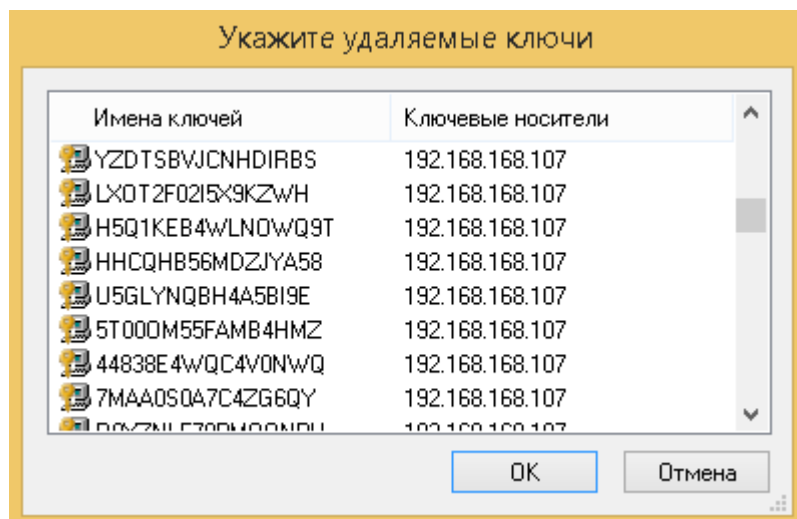


Рисунок 10 – Окно выбора ключей для удаления

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

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

Далее нужно подтвердить выполнение действия в окне предупреждения (Рисунок 11).

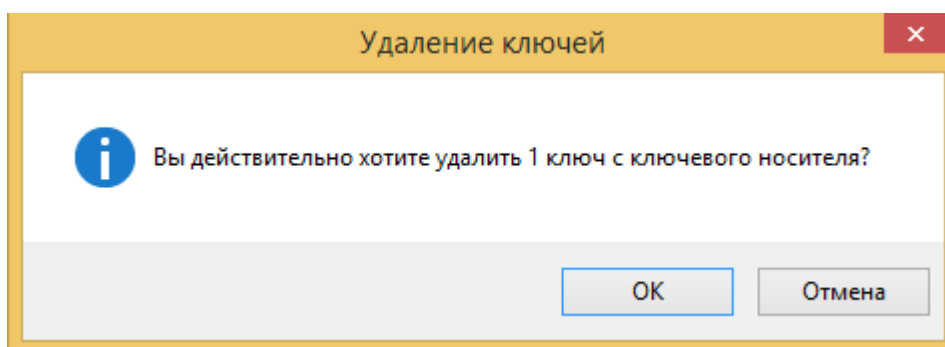


Рисунок 11 – Предупреждение об удалении ключей

Ключ удален с ключевого носителя. Нажмите «ОК» (Рисунок 12).

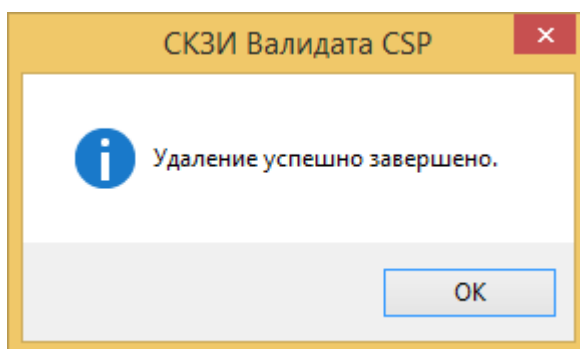


Рисунок 12 – Сообщение об удалении ключа

3.3 Копирование ключей

Копирование ключей с одного носителя на другой доступно только администратору ключей ПАМБ «vdHSM» и должно выполняться в соответствии с эксплуатационной документацией ПАМБ «vdHSM». Допускается копировать только ключи пользователей, не зашифрованные на симметричном ключе пользователя, и только в другое устройство ПАМБ «vdHSM».

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

HSM	Hardware Security Module
ПАМБ	Программно-аппаратный модуль безопасности
ПК	Программный комплекс
Средство КЗИ	Средство криптографической защиты информации

ПЕРЕЧЕНЬ РИСУНКОВ

1	Программа конфигурации	5
2	Вкладка «Сервис»	6
3	Окно выбора типа конфигурации	6
4	Окно выбора файла конфигурации	7
5	Окно загрузки ключа	7
6	Вкладка «Ключи»	8
7	Окно выбора ключа для получения информации	9
8	Предупреждение при генерации ключа	10
9	Окно выбора считывателя ключа	10
10	Окно выбора ключей для удаления	11
11	Предупреждение об удалении ключей	11
12	Сообщение об удалении ключа	11

[illegible][illegible]