

127018, Москва, ул. Сущёвский вал, д. 16 строение 5

Телефон: +7 (495) 780 4820

Факс: +7 (495) 780 4820

<http://www.CryptoPro.ru>

E-mail: info@CryptoPro.ru



Средство Криптографической Защиты Информации	КриптоПро HSM Руководство пользователя
---	--

ЖТЯИ.00046-01 90 05

Листов 41

2009 г.

Содержание

1.	АННОТАЦИЯ	3
2.	СПИСОК СОКРАЩЕНИЙ.....	4
3.	НАЗНАЧЕНИЕ ПО «КЛИЕНТ HSM».....	5
4.	УСТАНОВКА ПРИЛОЖЕНИЯ ПО «КЛИЕНТ HSM».....	7
5.	УДАЛЕНИЕ ПРИЛОЖЕНИЯ ПО «КЛИЕНТ HSM».....	12
6.	НАСТРОЙКА ПРИЛОЖЕНИЯ «КЛИЕНТ HSM».....	13
6.1.	Выбор считывателя.....	16
6.2.	Установка ключа и сертификата доступа к ПАКМ в Реестр Windows.	17
6.3.	Действия с текущим ключом и сертификатом доступа к ПАКМ.	19
7.	УСТАНОВКА СВЯЗИ С ПАКМ.....	24
8.	Управление ключами ЭЦП и сертификатами ключей ЭЦП.	26
8.1.	Установка личного сертификата.....	26
8.2.	Изменение пароля на контейнере личного ключа.....	33
8.3.	Удаление контейнера личного ключа.....	35
9.	УСТАНАВЛИВАЕМЫЕ КРИПТОПРОВАЙДЕРЫ	38
10.	ЛИТЕРАТУРА.....	40

1. АННОТАЦИЯ

Данный документ содержит инструкцию по установке, настройке и использованию программного обеспечения «Клиент HSM» (версия для рабочих станций пользователей средства криптографической защиты информации (СКЗИ)) на платформе ОС Windows, являющегося составной частью подсистем криптографической защиты информации (ПКЗИ), работающей вкуче с программно-аппаратным криптографическим модулем (ПАКМ) «КриптоПро HSM».

Документ предназначен для конечных пользователей СКЗИ ПАКМ «КриптоПро HSM», использующих на своих местах приложения, требующие выполнения криптографических запросов, для администраторов информационной безопасности учреждений, осуществляющих установку, обслуживание контроль за соблюдением требований к эксплуатации средств СКЗИ, а также администраторам Серверов, сетевых ресурсов предприятия и других работников службы информационной безопасности, осуществляющим настройку рабочих мест для работы со средствами СКЗИ.

2. СПИСОК СОКРАЩЕНИЙ

CRL	Список отозванных сертификатов (Certificate Revocation List)
ITU-T	Международный комитет по телекоммуникациям (International Telecommunication Union)
IETF	Internet Engineering Task Force
АРМ	Автоматизированное рабочее место
ГМД	Гибкий магнитный диск
ДСЧ	Датчик случайных чисел
HDD	Жесткий магнитный диск
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПАКМ	Программно-аппаратный криптографический модуль
ПО	Программное обеспечение
Регистрация	Присвоение определенных атрибутов (адреса, номера ключа, прав использования и т.п.) абоненту
Регламент	Совокупность инструкций и другой регламентирующей документации, обеспечивающей функционирование автоматизированной системы во всех режимах.
Сертификат	Электронный документ, подтверждающий принадлежность открытого ключа и определенных атрибутов конкретному абоненту
Сертификация	Процесс изготовления сертификата открытого ключа абонента в центре сертификации
СКЗИ	Средство криптографической защиты информации
СОС	Список отозванных сертификатов (Certificate Revocation List)
СС	Справочник сертификатов открытых ключей. Сетевой справочник.
ЦС	Центр Сертификации (Удостоверяющий Центр)
ЦР	Центр Регистрации
ЭД	Электронный документ
ЭЦП	Электронная цифровая подпись

3. НАЗНАЧЕНИЕ ПО «КЛИЕНТ HSM»

ПАКМ – программно–аппаратный криптографический модуль, внешний программный интерфейс которого соответствует криптографическому интерфейсу «КриптоПро CSP» версии 3.6.

ПАКМ «КриптоПро HSM.» может использоваться в корпоративных локальных сетях, как разделяемое СКЗИ, обслуживающее криптографические запросы обычных пользователей сети. При этом секретные ключи пользователей формируются и хранятся в ПАКМ в зашифрованном виде, и ответственность за их сохранность и несанкционированное использование разделяется между владельцами-служащими и службой безопасности компании. Таким образом, снижается вероятность компрометации ключей пользователей за счет утери или хищения ключевого носителя, обеспечивается дополнительный контроль над использованием ключа, снижаются затраты компании на сопровождение средств криптографической защиты информации.

Взаимодействие любого приложения на рабочих станциях пользователей или серверах с СКЗИ ПАКМ «КриптоПро HSM» осуществляется через посредника – «Клиента HSM».

ПО «Клиент HSM» является неотъемлемой частью подсистемы криптографической защиты информации (ПКЗИ) и представляет собой набор программных модулей, устанавливаемых на рабочих станциях пользователей/серверах.

Данное ПО зависит от используемой платформы, и от назначения целевого компьютера. ПО «Клиент HSM» предназначен для:

- трансляции вызовов функций интерфейса «Crypto-Pro CSP» (MS CryptoAPI) от приложений к удаленному разделяемому СКЗИ ПАКМ «КриптоПро HSM»
- обеспечения процедур аутентификации пользователей СКЗИ перед ПАКМ и ПАКМ перед пользователями
- обеспечения защищенного (шифрованного) канала передачи информации между рабочими станциями/серверами и ПАКМ.

Для взаимодействия приложений пользователей с ПАКМ используется «канал K2». Для его реализации на сервер необходимо установить ПО «Клиент HSM».

Для доступа к ПАКМ пользователь должен иметь ключ и сертификат ключа доступа (аутентификации) к ПАКМ. Данный ключ и сертификат формируется обычно на смарт-карте Администратором ПАКМ и передается пользователю. Пользователь ПАКМ должен использовать данную смарт-карту при каждой попытке подключения к ПАКМ.

Существует вариант формирования ключа и сертификата доступа на дискете или специальных USB устройствах. В случае формирования ключей на дискете пользователь, получивший от Администратора ПАКМ дискету, может выполнить определенную процедуру по установке ключа с дискеты в защищенное хранилище Реестра Windows. В данном случае ключ защищается паролем, заданным пользователем. После переноса ключа в Реестр, он автоматически удаляется с дискеты. Необходимо только помнить, что данная процедура понижает общий уровень криптографической защиты информации (когда ключи пользователей хранятся на неотчуждаемых носителях).

В случае порчи или утери ключей, носителей, а также в случае подозрения в компрометации ключа доступа, пользователь должен немедленно сообщить об этом Администратору ПАКМ.

Администратор ПАКМ имеет возможность заблокировать работу пользователей, использующих данный ключ доступа, после чего сформировать новый ключ пользователю.

4. УСТАНОВКА ПРИЛОЖЕНИЯ ПО «КЛИЕНТ HSM»

Установка программного обеспечения «Клиент HSM» осуществляется пользователем, имеющим права администратора на локальном компьютере¹!

Для установки приложения необходимо выбрать программу установки в зависимости от используемого языка операционной системы и типа процессора:

hsm-win32-eng.msi

hsm-win32-rus.msi

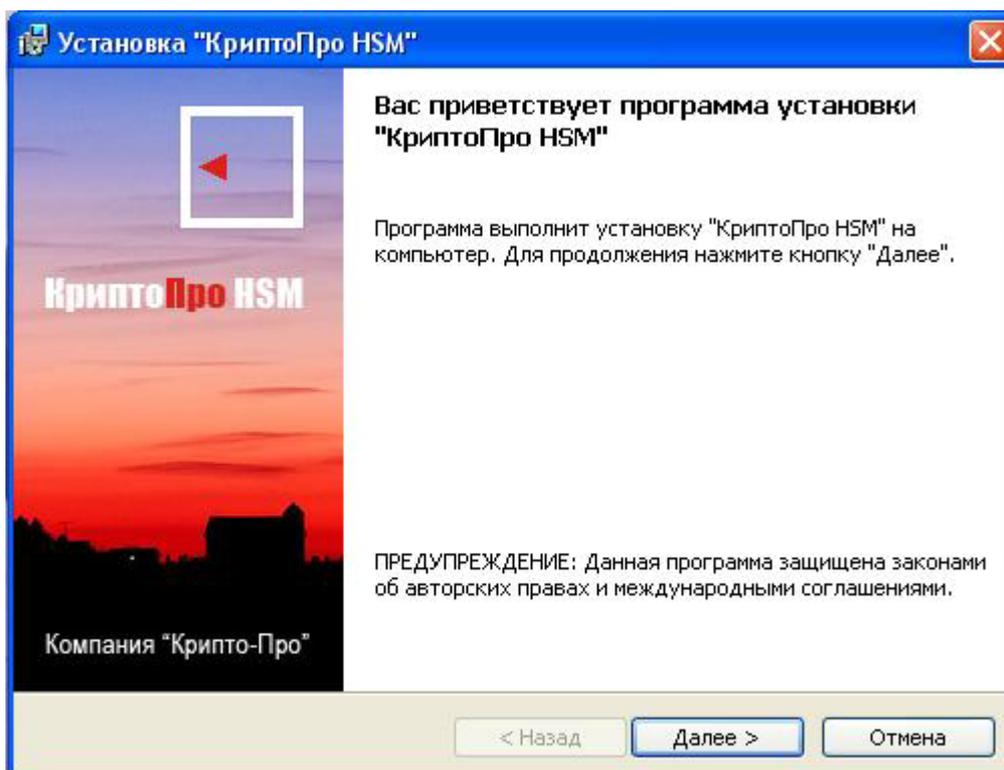
hsm-itanium-eng.msi

hsm-itanium-rus.msi

hsm-x64-eng.msi

hsm-x64rus.msi

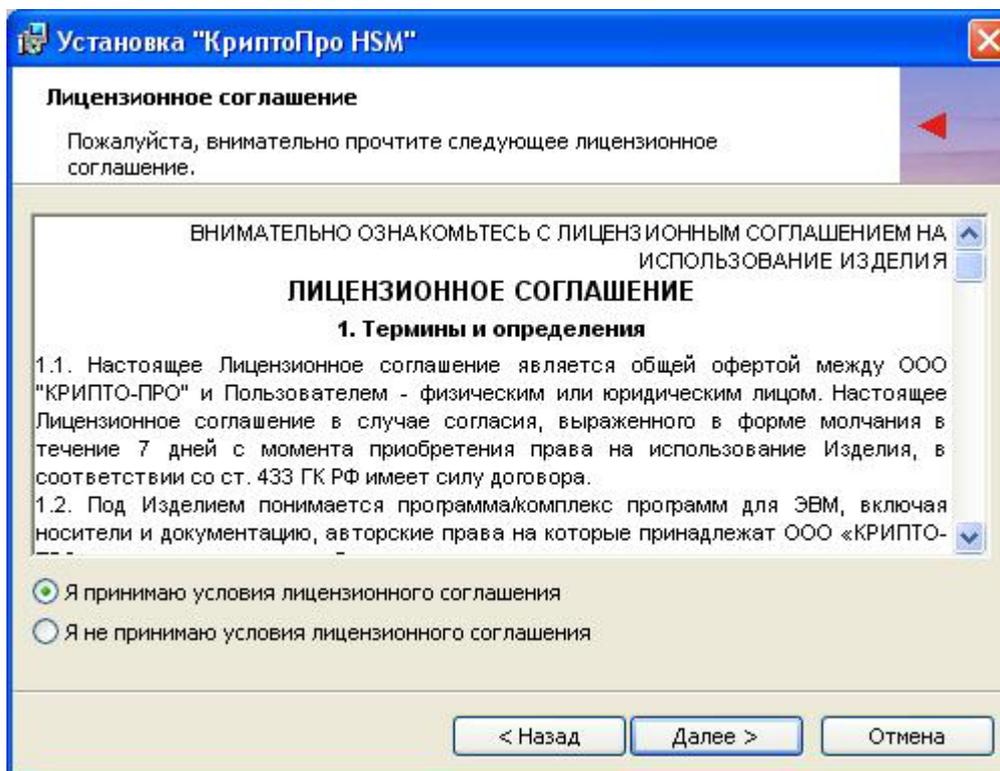
Необходимо запустить нужную программу и следовать инструкциям, которые предлагает Мастер установки.



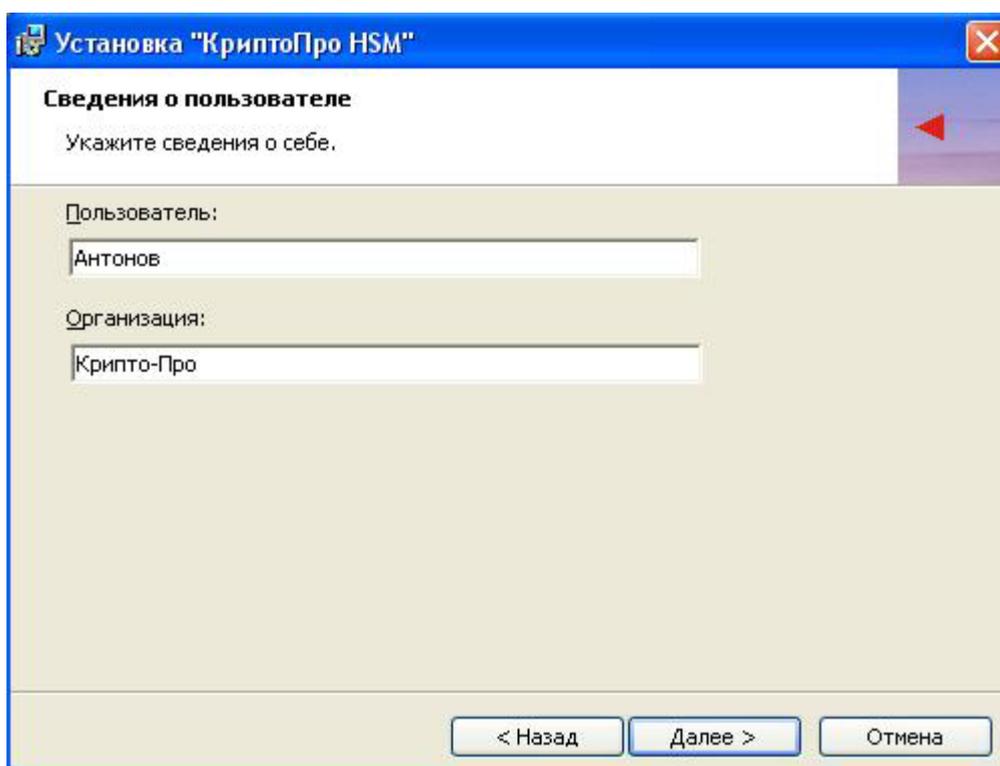
¹ В некоторых конфигурациях с жесткими ограничениями доменных политик требуется запуск инсталляционного задания в режиме «Запуск от имени администратора». Для этого необходимо создать «ярлык» с командой: `msiexec /i <имя дистрибутива.msi>` и используя правую кнопку мыши, кликая на созданном ярлыке, выбрать данный режим.

Нажмите кнопку "Далее".

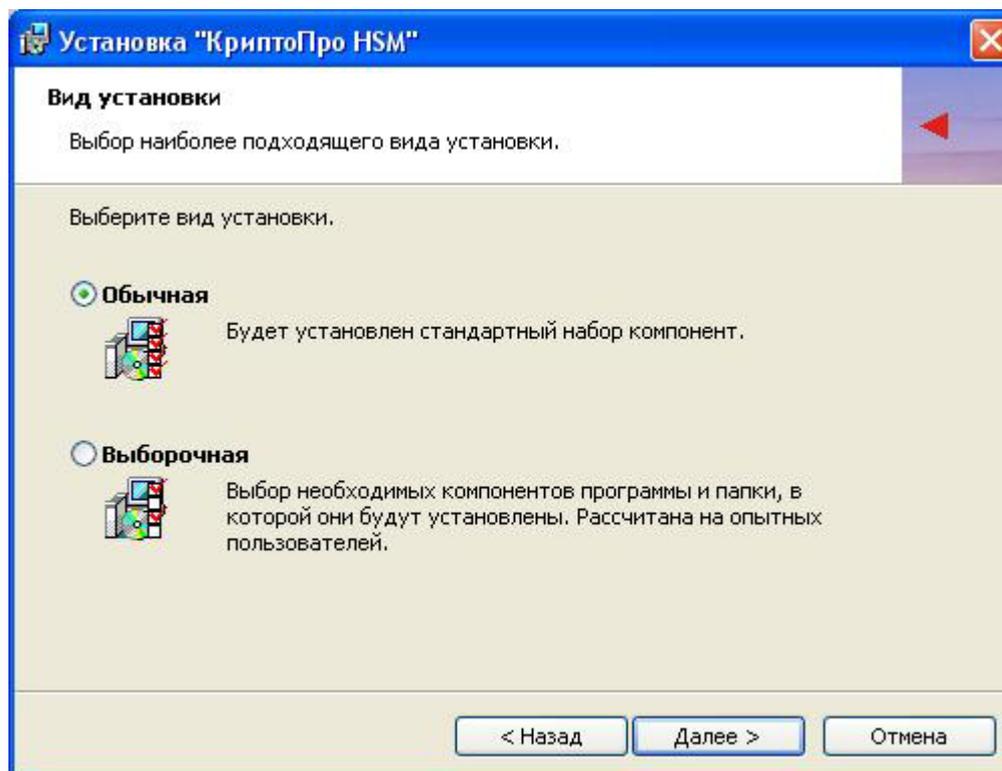
В следующем окне прочитайте лицензионное соглашение и, в случае согласия с ним, отметьте поле «Я принимаю лицензионное соглашение», и нажмите «Далее»:



Введите имя пользователя и название организации:

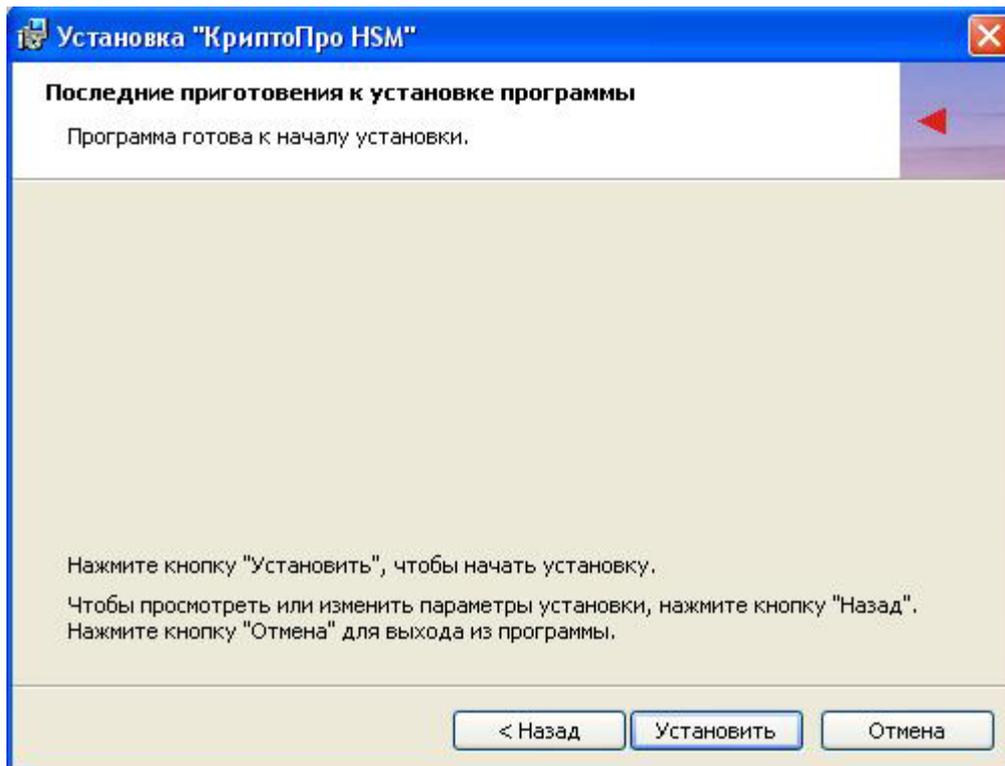


Выберите вид установки:

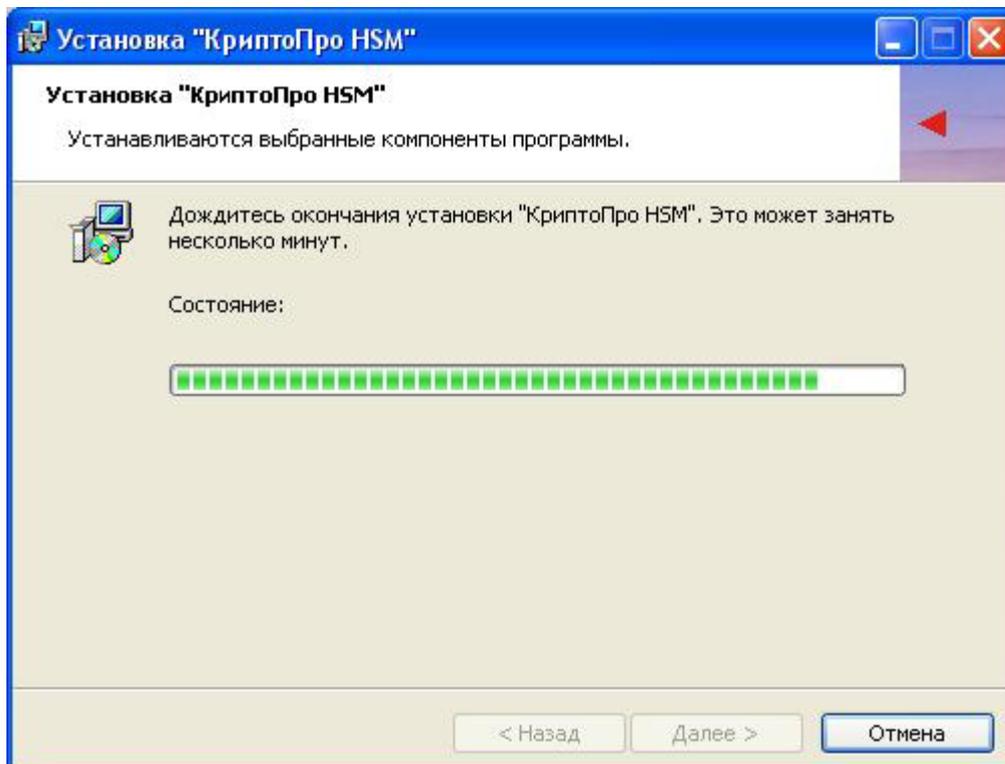


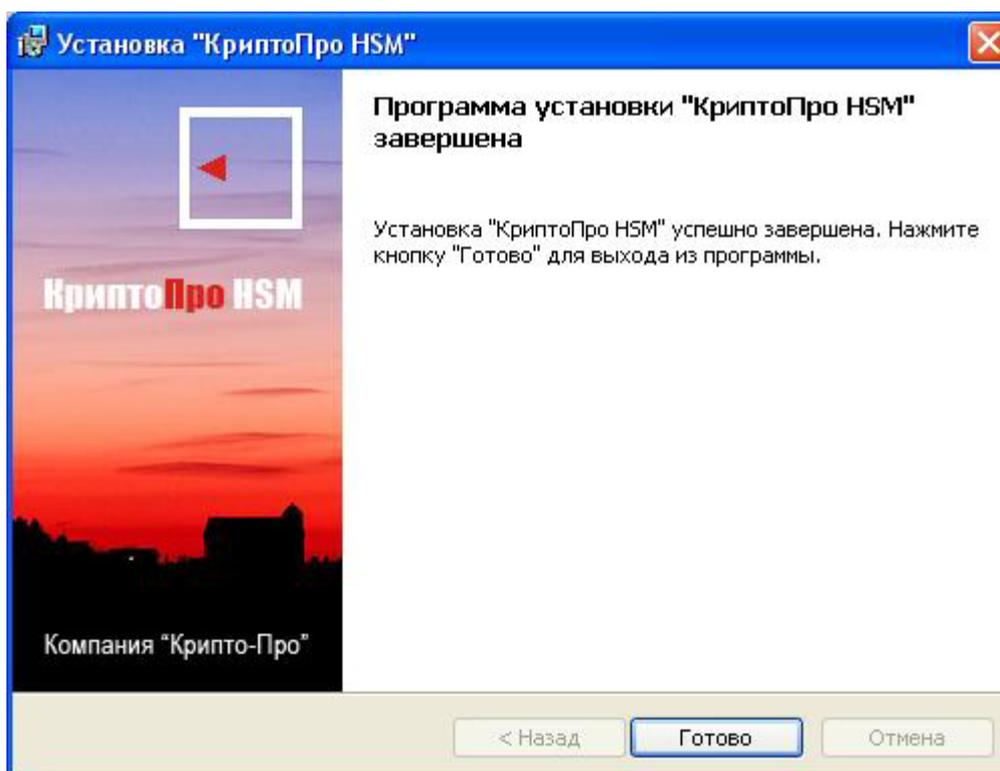
В «выборочном» варианте установки имеется возможность установить дополнительно компонент «КриптоПро Revocation Provider». Подробно о данном компоненте можно прочитать на сайте компании КриптоПро по ссылке <http://www.cryptopro.ru/cryptopro/products/rp/default.htm>.

Нажмите кнопку «Установить»:

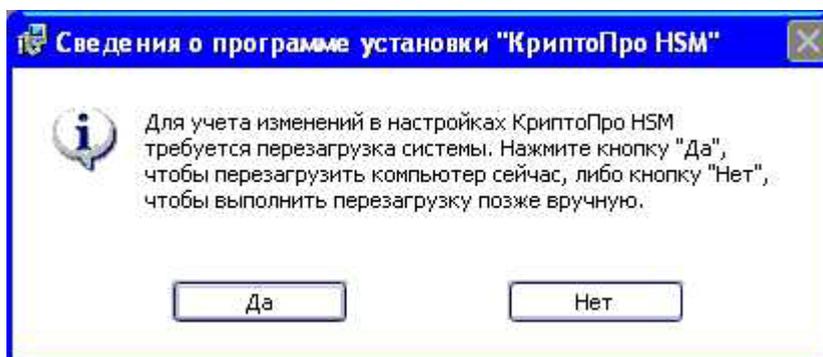


Дождитесь окончания установки:





После успешного завершения работы Мастера установки появится окно с предложением перезагрузить операционную систему.



После перезагрузки на панели задач появится новый значок:



5. УДАЛЕНИЕ ПРИЛОЖЕНИЯ ПО «КЛИЕНТ HSM»

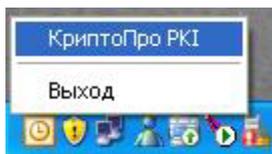
Для удаления приложения необходимо открыть окно «Панель управления» Windows, выбрать пункт «Установка и удаление программ», в списке установленных программ выделить «КриптоПро HSM» и нажать кнопку «Удалить».

Удалить приложение «Клиент КриптоПро HSM» может только пользователь, имеющий права администратора на локальном компьютере.

6. НАСТРОЙКА ПРИЛОЖЕНИЯ «КЛИЕНТ HSM».

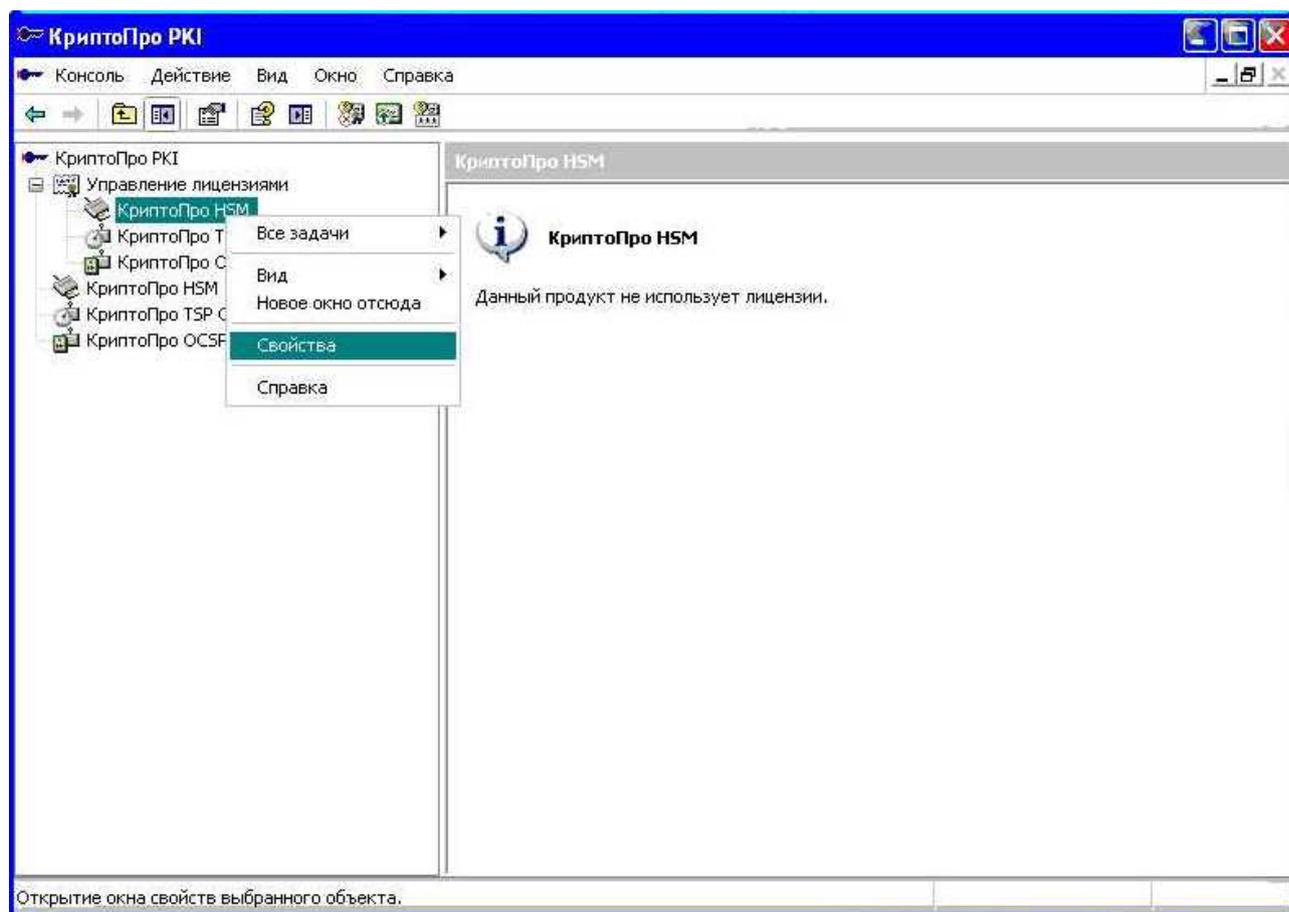
Управление продуктами, произведенными компанией КРИПТО-ПРО, осуществляется с единой консоли управления «КриптоПро PKI».

Для настройки ПО «Клиент HSM» щелкните правой кнопкой мыши на значке «Клиент КриптоПро HSM» на панели задач, и в выпадающем меню выберите пункт «КриптоПро PKI»:

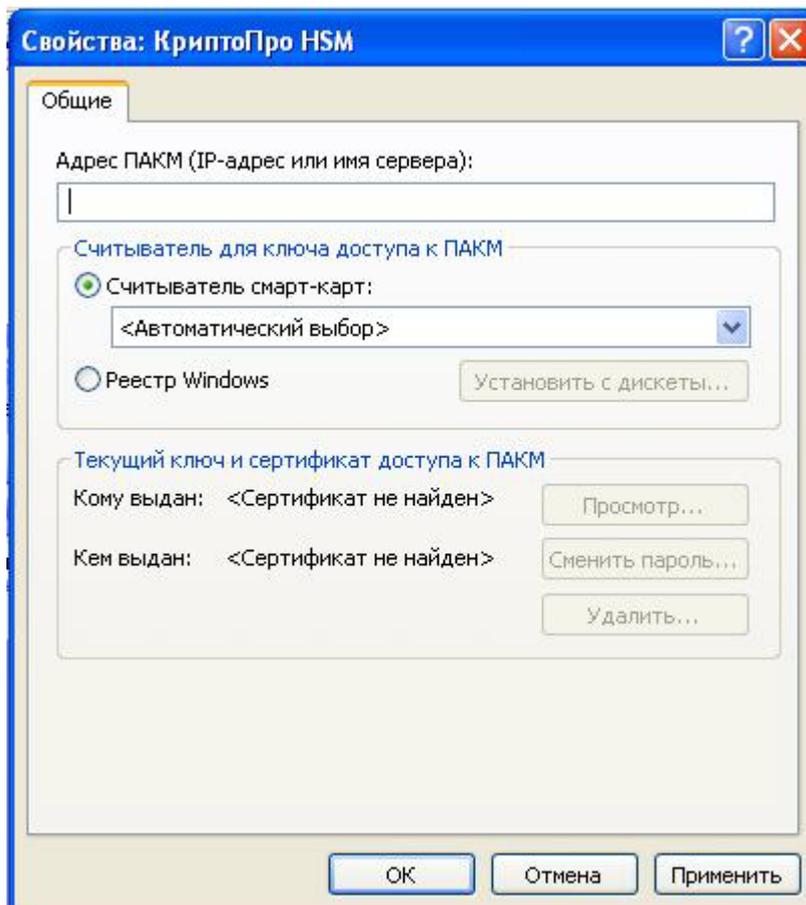


После этого появится окно «КриптоПро PKI».

Щелкните правой кнопкой мыши на пункте «КриптоПро HSM» в левой части окна и в выпадающем меню выберите пункт «Свойства»:



После этого появится окно «Свойства: КриптоПро HSM».

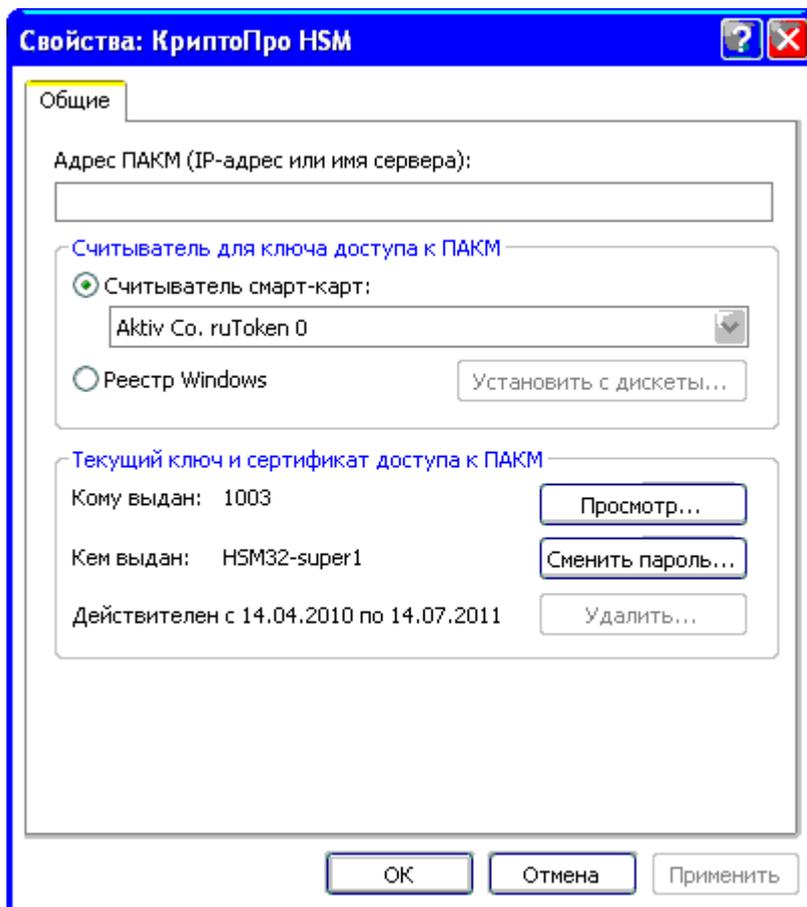


Если до вызова этого окна была произведена настройка считывателя ключа доступа к ПАКМ на считыватель смарт-карт (см. пункт 6.1), и в считыватель не вставлена карта, предварительно появится окно с предложением вставить носитель:



Это окно вызывается для получения информации о ключе и сертификате доступа к ПАКМ и отображения этой информации в окне «Свойства». Можно закрыть его кнопкой «Отмена», и тогда информация о ключе доступа к ПАКМ в окне свойств отображена не будет. Если вставить карту в

считыватель, это окно исчезнет, и в окне свойств будет отображена информация, прочитанная из ключевого контейнера на карте.



Внимание! Если в системе не зарегистрировано ни одного считывателя смарт-карт (или USB токенов, зарегистрированных в Windows как устройства чтения смарт-карт), то перед отображением окна свойств будет выдано сообщение об ошибке, а выпадающий список «Считыватель смарт-карт» будет пустым.

Основными настройками ПО «Клиент HSM» являются сетевой (IP) адрес ПАКМ, куда будут транслироваться вызовы криптографических функций, и тип считывателя, который будет использоваться для доступа к ключу аутентификации пользователя.

Тип считывателя «Реестр» рекомендуется использовать только на компьютерах, не оснащенных считывателями смарт-карт. В данном случае ключ и сертификат доступа, сформированный Администратором ПАКМ пользователю, хранится не на отчуждаемом носителе, а в защищенном хранилище реестра ОС Windows. Ключ не может быть впоследствии использован для доступа с других рабочих станций.

Если рабочая станция оснащена несколькими считывателями смарт-карт, то рекомендуется выбрать конкретный, который будет использоваться для карточки с ключами доступа к ПАКМ.

В окне свойств необходимо ввести IP-адрес HSM в поле «Адрес ПАКМ», и выбрать считыватель для ключа доступа к ПАКМ.

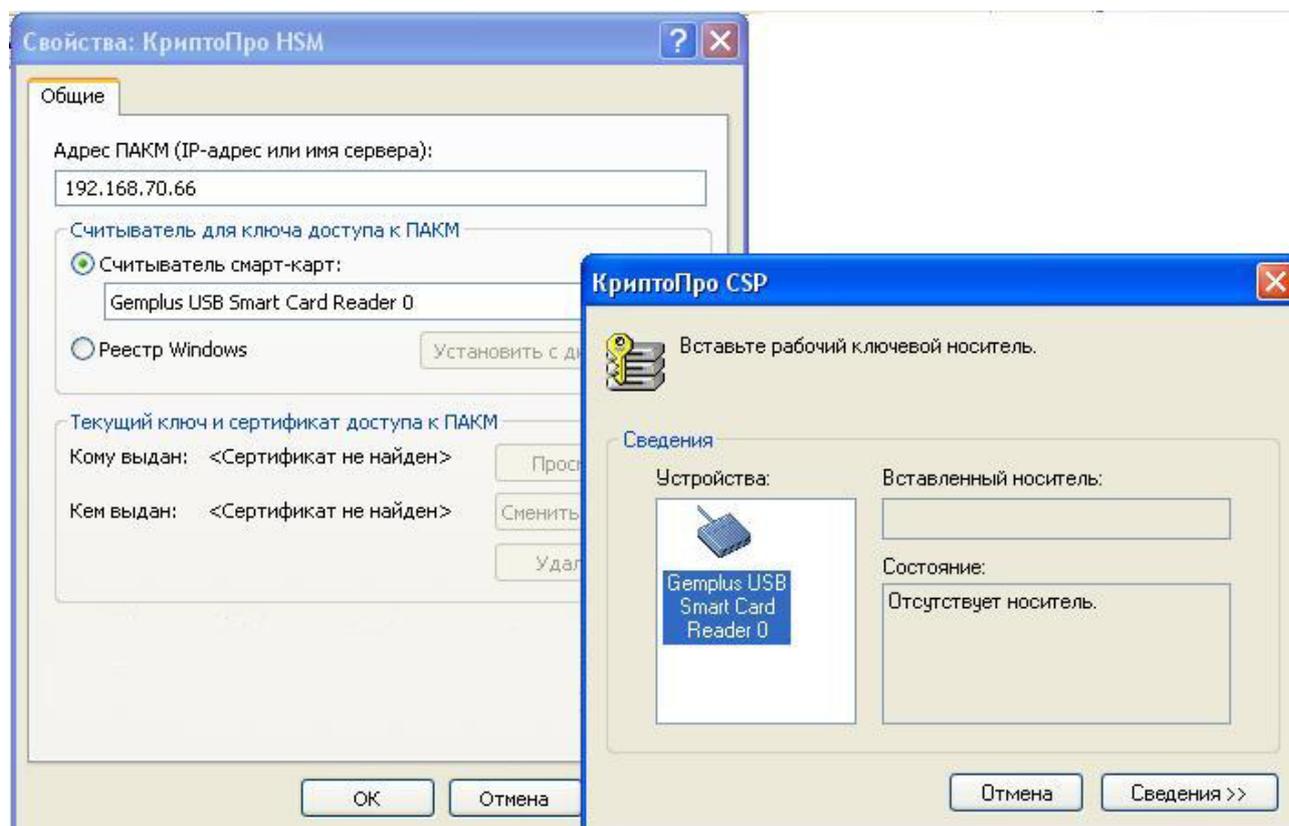
Кнопки «ОК» и «Применить» сохраняют введенный тип считывателя и адрес ПАКМ. Кнопка «Отмена» закрывает окно без сохранения настроек.

Устанавливать тип считывателя и адрес ПАКМ может только пользователь, имеющий права администратора на локальном компьютере. Эти настройки являются общими для всех пользователей на компьютере.

Впоследствии, после изменения IP-адреса ПАКМ, типа считывателя или при переустановке ключа в реестре для дальнейшей работы необходима перезагрузка компьютера.

6.1. Выбор считывателя.

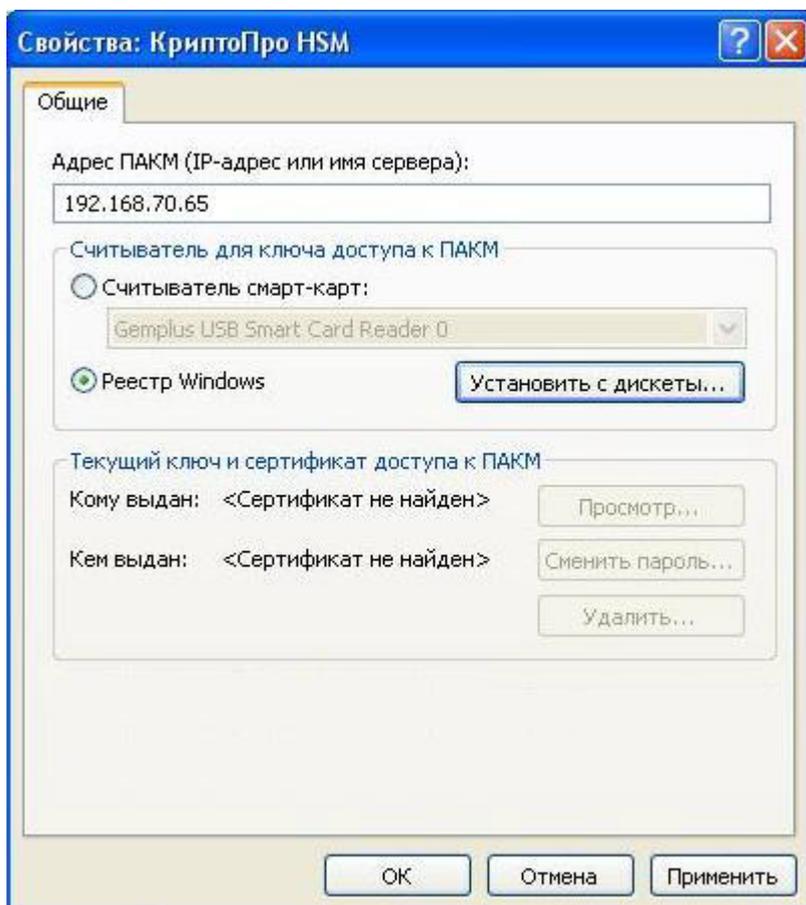
Для считывания ключа доступа со смарт-карт необходимо выбрать пункт «Считыватель смарт-карт» и выбрать в выпадающем списке тип считывателя. После этого, если в считыватель не вставлена карта, появится окно с предложением вставить ключевой носитель, как описано выше.



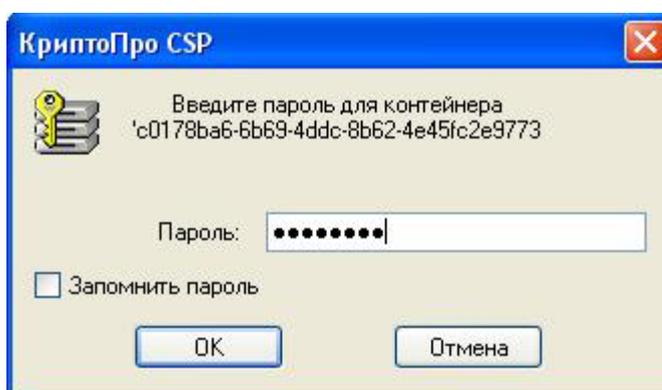
Для считывания ключа доступа из реестра необходимо выбрать пункт «Реестр Windows». Если ключ в реестре отсутствует, его необходимо установить.

6.2. Установка ключа и сертификата доступа к ПАКМ в Реестр Windows.

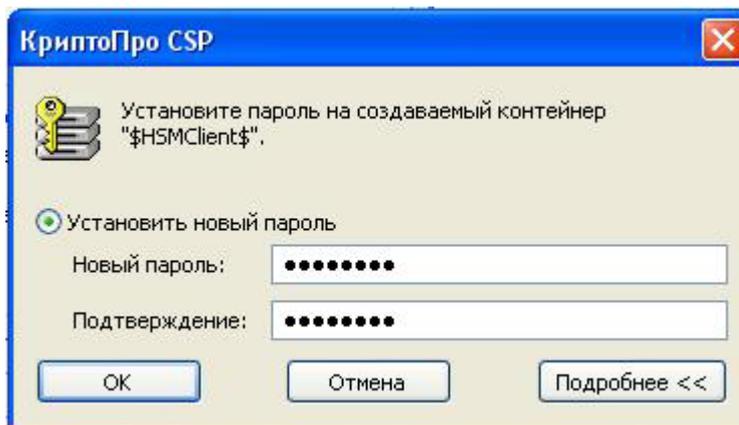
Для установки ключа доступа в реестре необходимо выбрать пункт «Реестр Windows», вставить дискету с ключом и сертификатом доступа, сформированными Администратором ПАКМ, в дисковод и нажать кнопку «Установить с дискеты».



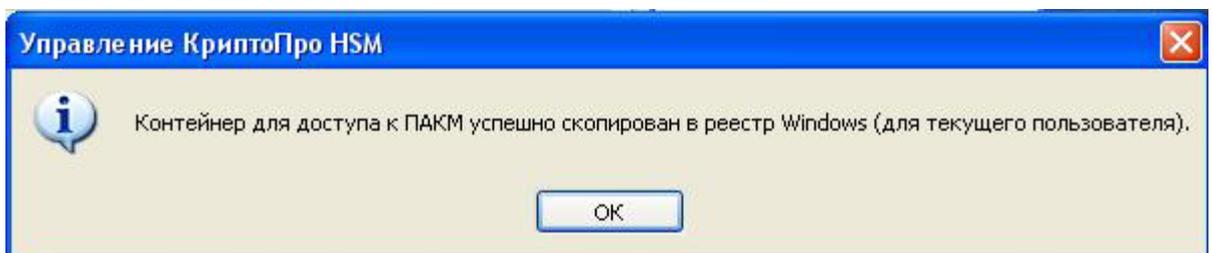
В появившемся окне необходимо ввести пароль для контейнера с закрытым ключом на дискете:



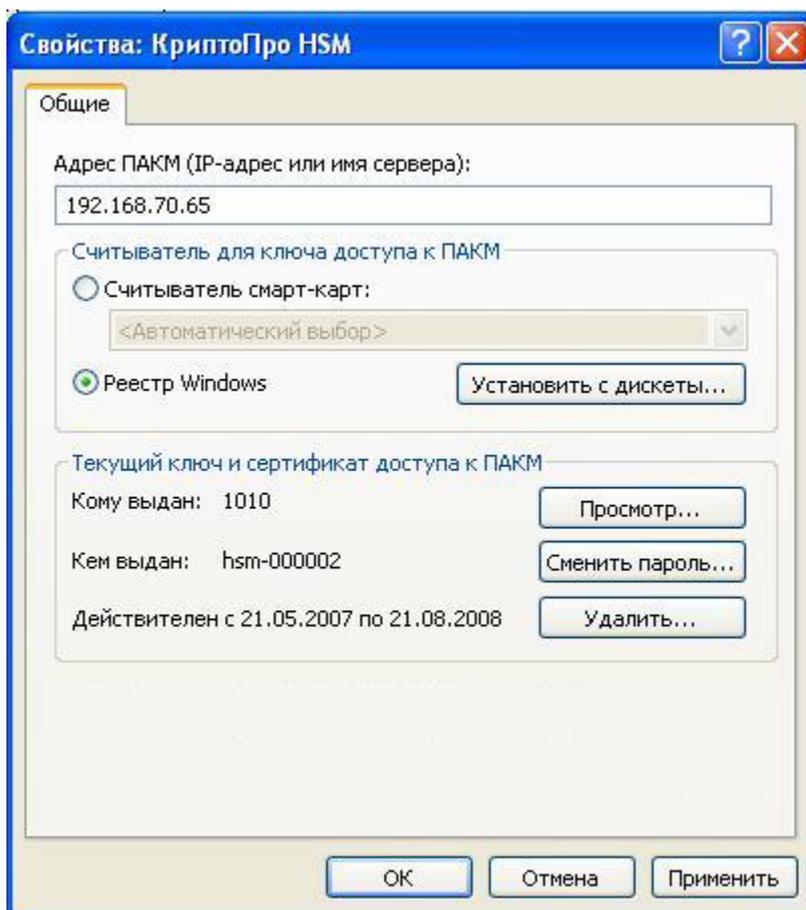
И затем необходимо ввести новый пароль для контейнера в реестре:



После этого появится сообщение об установке контейнера в реестр.



В окне «Свойства: КриптоПро HSM» появится информация о ключе и сертификате доступа к ПАКМ.



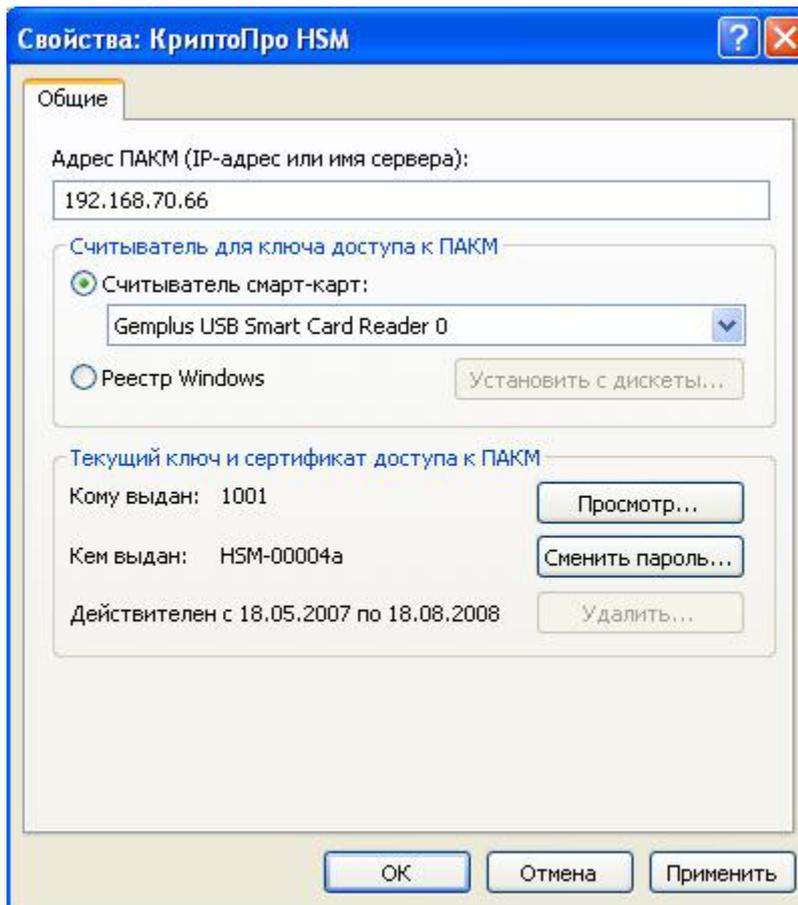
В результате успешного выполнения данной процедуры ключ с дискеты будет удален.

Перед установкой в реестр нового ключа доступа прежний ключ необходимо предварительно удалить. Для этого необходимо нажать кнопку «Удалить...» и в появившемся окне подтвердить удаление.

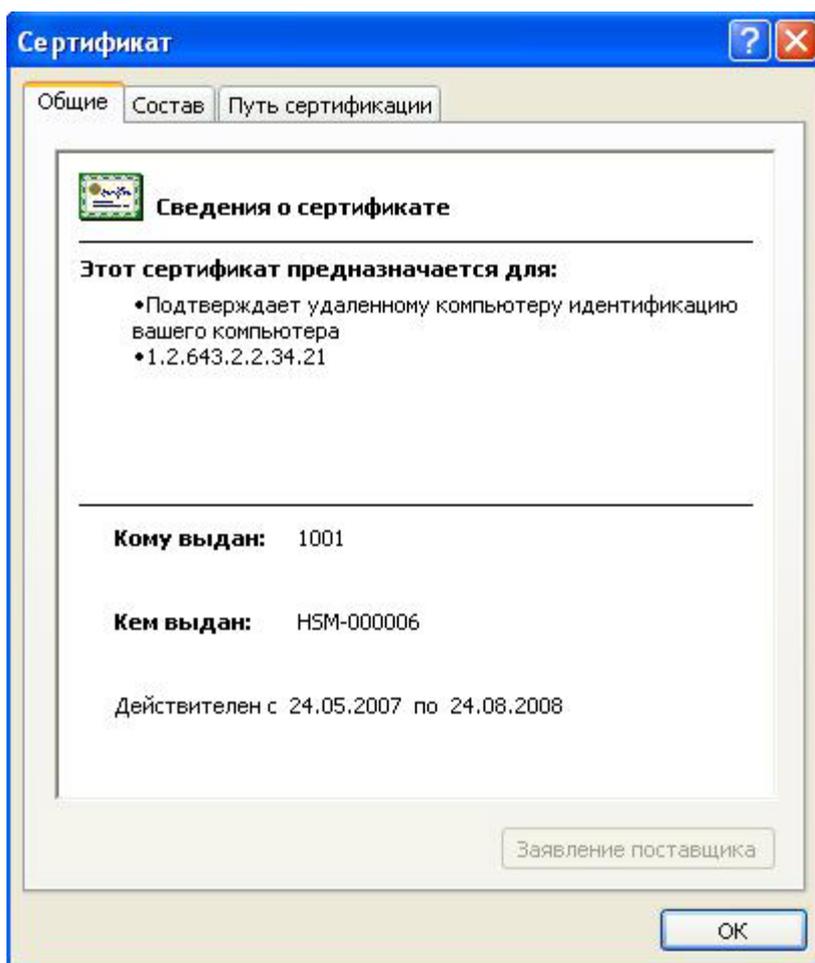
Ключевой контейнер и сертификат доступа к ПАКМ устанавливаются в реестр и удаляются оттуда индивидуально для каждого пользователя. Операцию может и должен выполнять пользователь – владелец ключа и сертификата доступа к ПАКМ.

6.3. Действия с текущим ключом и сертификатом доступа к ПАКМ.

Если произведена настройка на считывание ключа со смарт-карт, то для работы с ключом перед вызовом окна свойств необходимо вставить карту в считыватель.

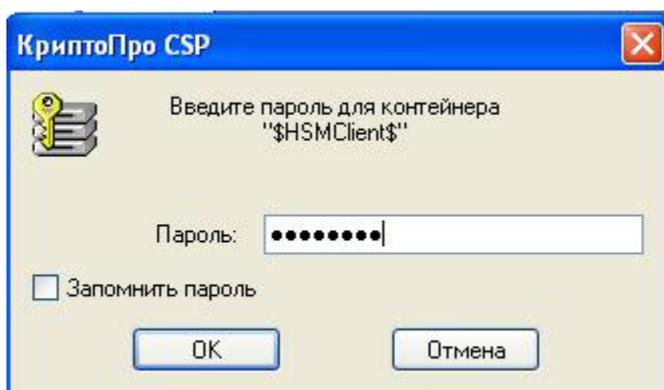


Для просмотра сертификата необходимо нажать «Просмотр...», после чего появится стандартное окно просмотра сертификата.

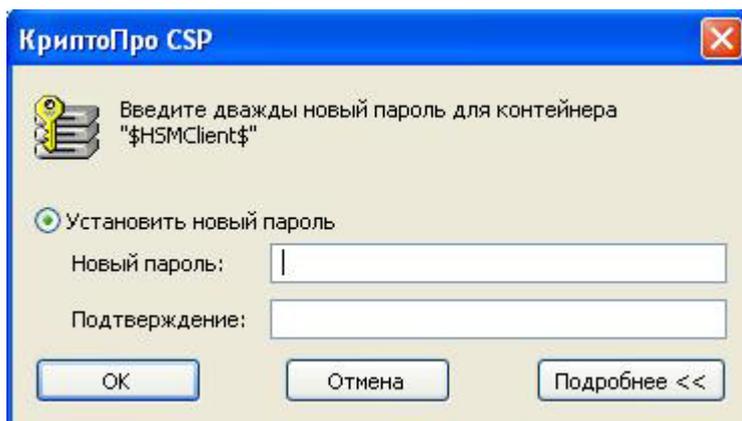


Если в хранилище доверенных корневых сертификатов ещё нет самоподписанного сертификата ПАКМ (обычно это происходит, когда связь еще ни разу не была установлена или когда произведена плановая смена ключа и сертификата ПАКМ), в окне просмотра сертификата появится информация, что сертификат не удалось проверить, проследив до доверенного центра сертификации. Чтобы установить самоподписанный сертификат ПАКМ в хранилище, необходимо установить связь с ПАКМ (см. пункт 7).

Для смены пароля контейнера закрытого ключа необходимо нажать «Сменить пароль...». После этого появится предложение ввести текущий пароль контейнера:



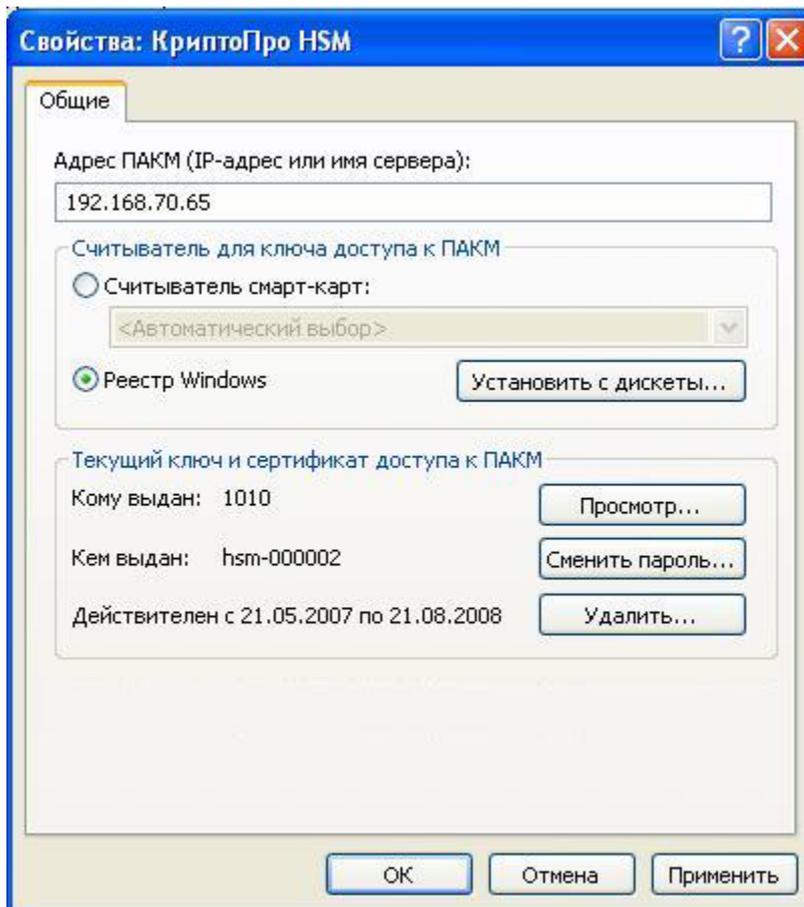
После ввода пароля появится предложение ввести новый пароль:



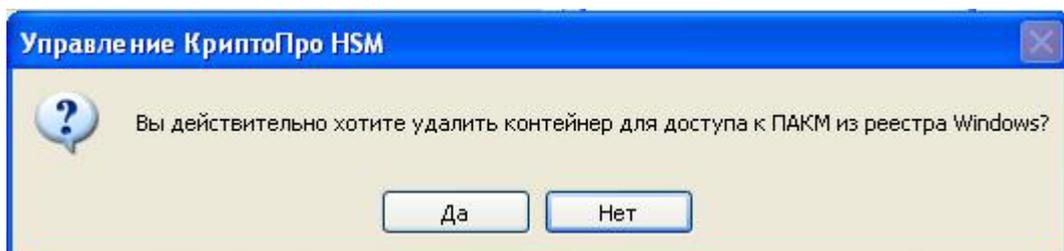
Пароль контейнера закрытого ключа доступа к ПАКМ, установленного в реестр, индивидуален для каждого пользователя.

Внимание. При формировании Администратором ПАКМ ключа доступа пользователя прямо в ПАКМ, а не на удаленном рабочем месте Администратора, класс защиты ключа устанавливается в соответствии с уровнем безопасности защиты СКЗИ ПАКМ. Если уровень безопасности ПО «Клиент HSM», работающего со смарт-картой пользователя ниже уровня безопасности ПАКМ, то класс защиты ключа на смарт-карте должен быть понижен до необходимого уровня. Это можно сделать процедурой изменения пин-кода на смарт-карте на рабочем месте пользователя, описанной выше. Если этого не сделать, то ПО «Клиент HSM» не сможет установить связь с ПАКМ.

Удаление ключа и сертификата доступа к ПАКМ возможно, только если ключ установлен в реестре.



Для удаления контейнера ключа необходимо нажать кнопку «Удалить...». После этого появится окно с просьбой подтвердить удаление:



Если нажать «Да», сертификат и контейнер ключа доступа к ПАКМ будет удален.

7. УСТАНОВКА СВЯЗИ С ПАКМ.

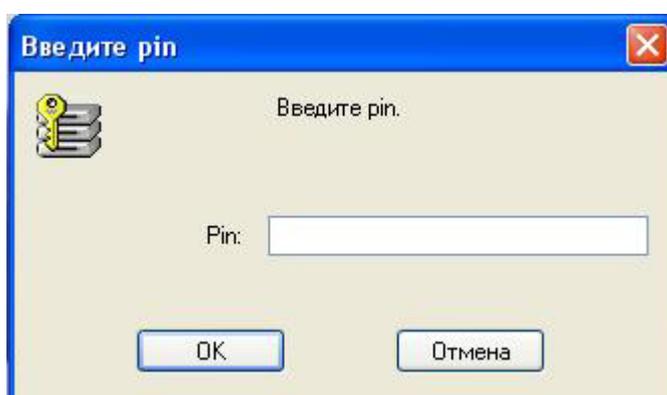
Для успешной установки связи с ПАКМ предварительно должны быть произведены необходимые настройки, как описано в главе 6.

Для установки связи необходимо щелкнуть мышью на значке «Клиент КриптоПро HSM» в системном трее на панели задач Windows.

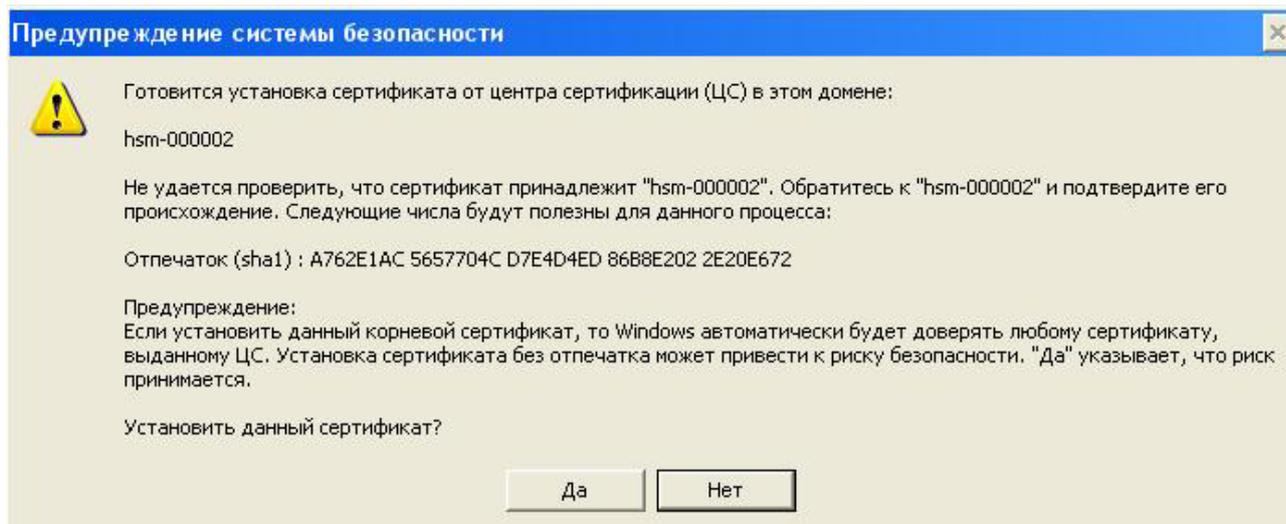


Если ключ доступа находится на смарт-карте следует вставить карту в считыватель.

В открывшемся окне необходимо ввести пароль для контейнера ключа доступа.



При правильно введенном пароле ПО «Клиент HSM» попытается установить связь с ПАКМ. Если в хранилище доверенных корневых сертификатов ещё нет самоподписанного сертификата ПАКМ (обычно, когда связь устанавливается в первый раз или когда произведена плановая смена ключа и сертификата ПАКМ), необходимого для проверки сертификатов ключа доступа пользователя и TLS сервера ПАКМ, то система попытается его установить. При этом самоподписанный сертификат ПАКМ извлекается из контейнера ключа доступа пользователя и на экран выдается стандартное окно ОС Windows с предложением установить сертификат в хранилище доверенных корневых центров сертификации.



Если ответить «Да», корневой сертификат будет установлен в локальное хранилище пользователя.

При установлении связи с ПАКМ «Клиент HSM» получает текущий сертификат TLS-сервера ПАКМ и пытается его проверить с помощью корневых сертификатов, установленных в хранилище доверенных сертификатов данного пользователя. Аналогичная проверка сертификата доступа к ПАКМ производится на ПАКМ. Если обе проверки будут успешными, связь будет установлена, и значок на панели задач изменит вид на указанный ниже:



В дальнейшем запрос на установку корневого сертификата может быть повторен ПО «Клиент HSM» лишь в случае удаления корневого сертификата ПАКМ из хранилища доверенных сертификатов, либо после перевыпуска ключа и сертификата ПАКМ.

В случае перевыпуска корневого сертификата на ПАКМ и последующего выпуска нового сертификата TLS-сервера Администратор ПАКМ должен перевыпустить ключи и сертификаты доступа пользователей. После этого процедура установки корневого сертификата ПАКМ будет повторена.

Для отключения связи с ПАКМ необходимо снова щелкнуть на значке «Клиент КриптоПро HSM». После этого связь будет прекращена и значок примет прежний вид.



После успешной установки связи с ПАКМ в оперативной памяти компьютера открывается контекст ключа доступа к ПАКМ, который будет закрыт после выхода из сеанса пользователя или после перезагрузки компьютера. При открытом контексте ключа для работы с контейнером ключа pin-код не требуется, поэтому при повторной установке связи с ПАКМ окно с просьбой ввести пароль не появится.

Если долго не используется установленное соединение между рабочей станцией пользователя и ПАКМ «КриптоПро HSM», то ПАКМ может «закрыть» это соединение, чтобы дать

возможность другим, активным пользователям доступ к криптографическому сервису ПАКМ. При этом приложение пользователя, которое попытается обратиться через «закрытое» соединение выдаст сообщение об ошибке. Иконка в системном трее изменится на



(соединение не установлено). Чтобы продолжить работу с криптографическим сервисом необходимо инициировать установление нового соединения, как было описано выше.

При очень высокой загрузке ПАКМ «КриптоПро HSM» (интенсивная работа десятков тысяч пользователей с криптографическими сервисами ПАКМ) время ожидания отклика от ПАКМ может возрасти и превысить заданное по умолчанию максимальное время отклика (таймаут). При этом криптографический вызов может закончиться неудачей. Если такое наблюдается довольно часто, то необходимо обратиться к Администратору безопасности предприятия для устранения проблемы. Увеличение максимального времени ожидания отклика от ПАКМ описано в документе «ЖТЯИ.00046-01 90 02 КриптоПро HSM. Правила пользования».

8. Управление ключами ЭЦП и сертификатами ключей ЭЦП.

Консоль управления КриптоПро PKI реализует некоторые сервисные функции, позволяющие пользователю управлять своими ключами электронной цифровой подписи и сертификатами ключей ЭЦП.

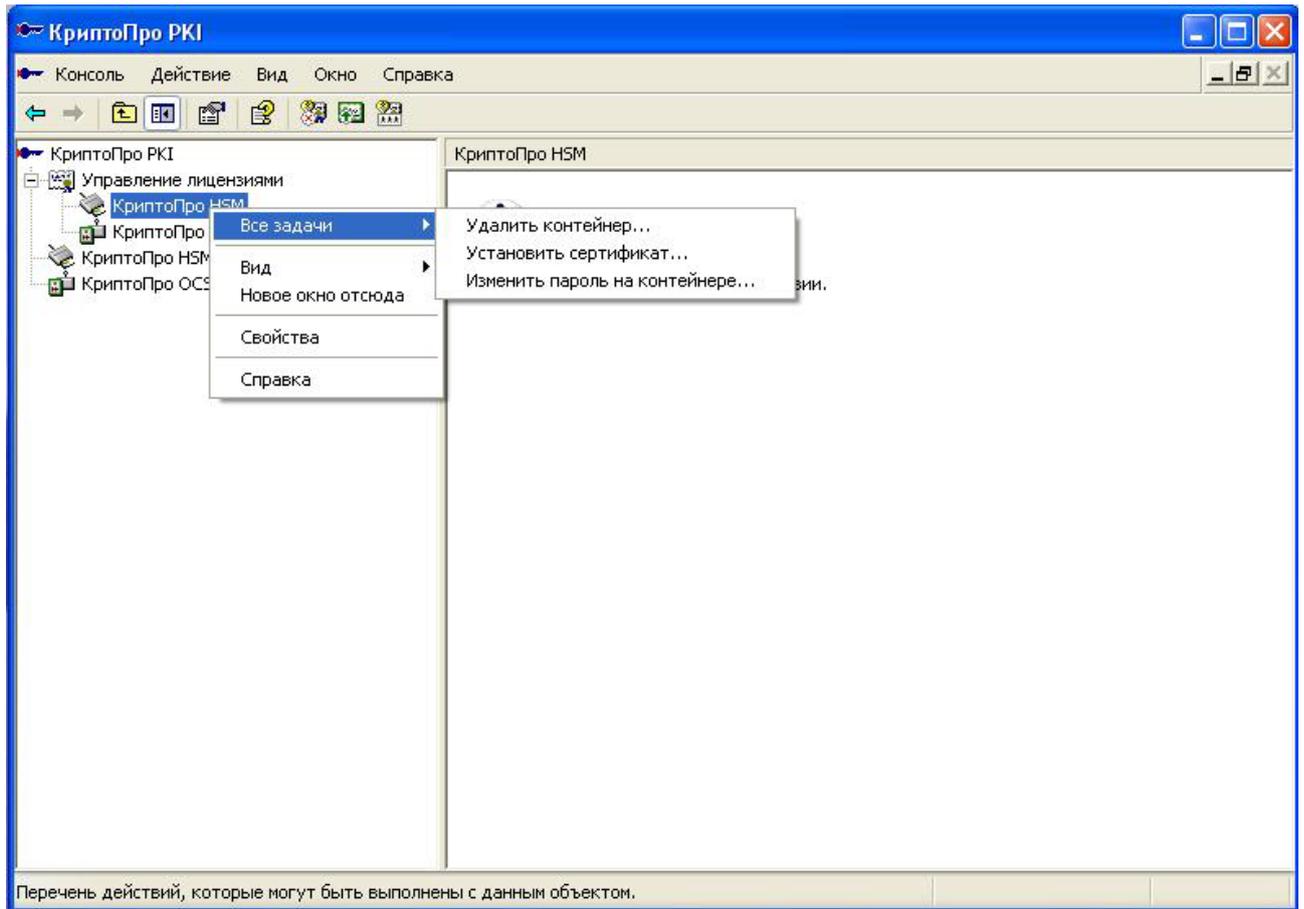
В процессе работы пользователь при помощи специализированных приложений формирует ключи подписи в ПАКМ, формирует запросы на сертификаты ключей подписей, отправляя их в удостоверяющие центры (УЦ), получает из УЦ готовые сертификаты ключей ЭЦП и устанавливает их у себя. После этого он может формировать ЭЦП под документами.

Периодически необходимо менять пароли на контейнеры ключей ЭЦП, хранящихся в ПАКМ, а при окончании срока действия ключей уничтожать их.

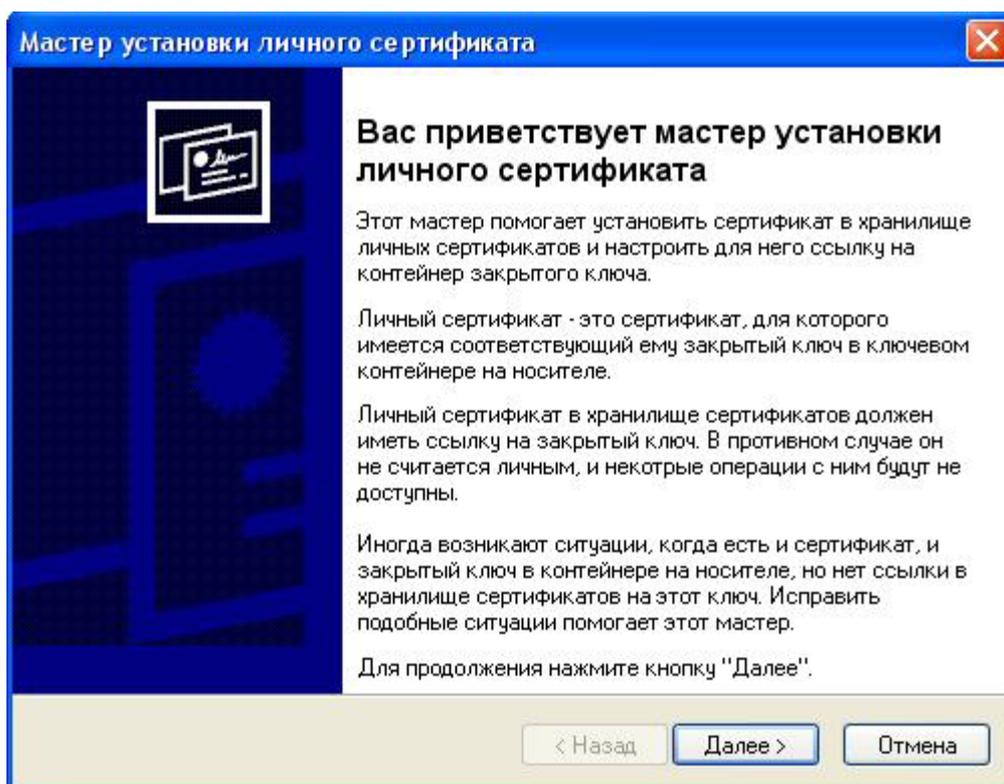
8.1. Установка личного сертификата.

Для установки личного сертификата пользователя в хранилище личных сертификатов на компьютере и создания связки сертификата с контейнером закрытого ключа на ПАКМ, необходимо открыть сеанс данного пользователя и установить связь с ПАКМ (как описано в главе 7).

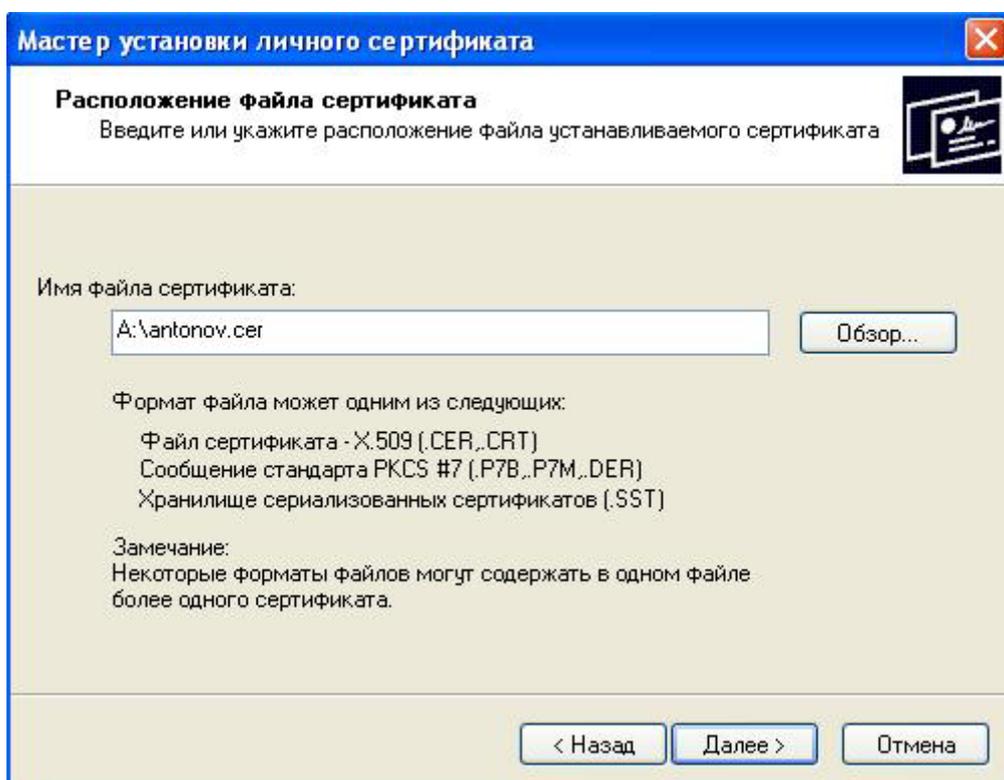
Затем необходимо открыть окно «КриптоПро PKI», щелкнув правой кнопкой мыши на значке «Клиент КриптоПро HSM», и в выпадающем меню выбрав пункт «КриптоПро PKI». В окне «КриптоПро PKI» необходимо щелкнуть правой кнопкой мыши на пункте «КриптоПро HSM» в левой части окна и в выпадающем меню выбрать пункт «Все задачи» → «Установить сертификат»:



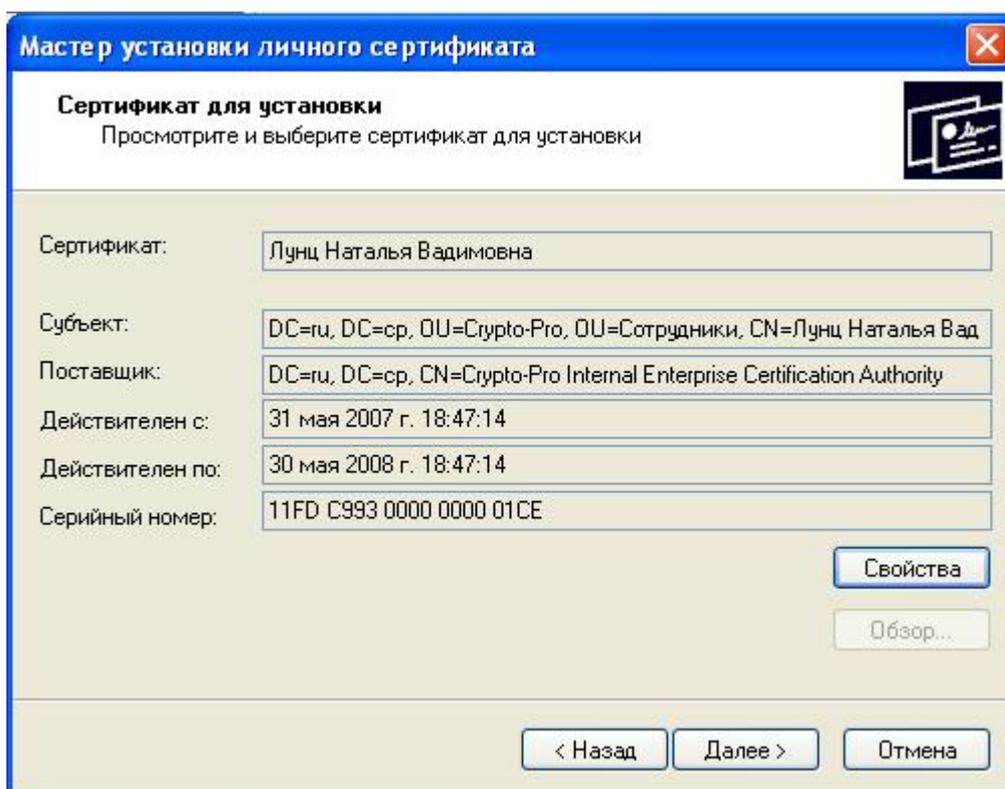
После этого откроется окно Мастера установки личного сертификата.



Для продолжения необходимо нажать кнопку «Далее», и в следующем окне указать расположение файла с сертификатом:

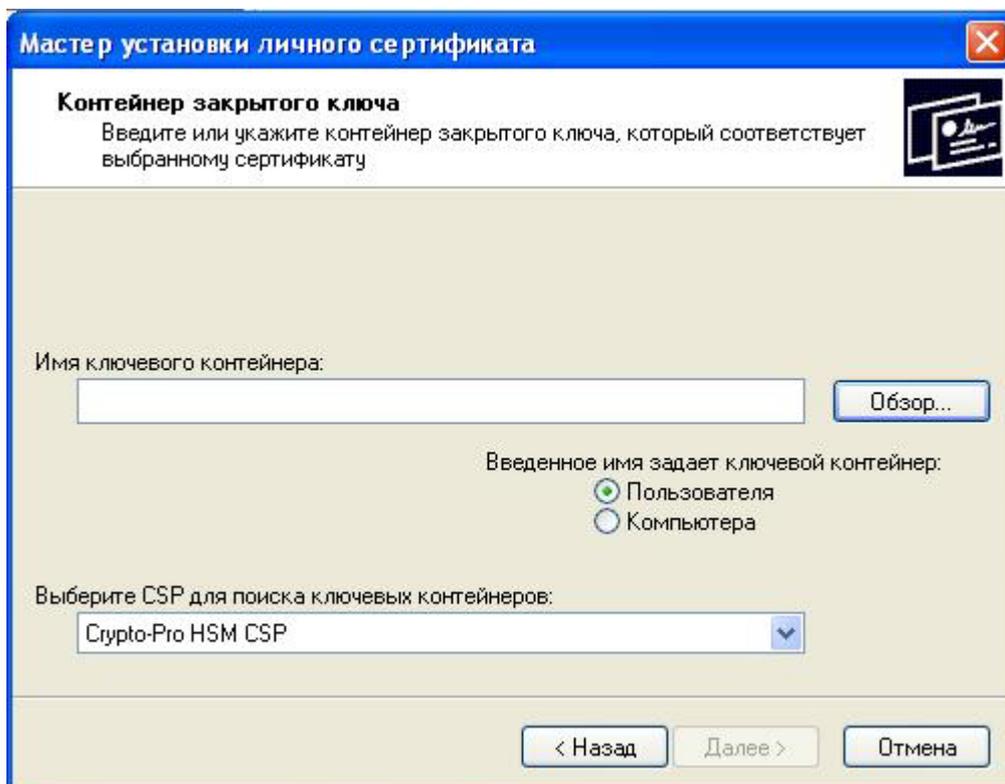


Следующее окно содержит информацию об устанавливаемом сертификате:

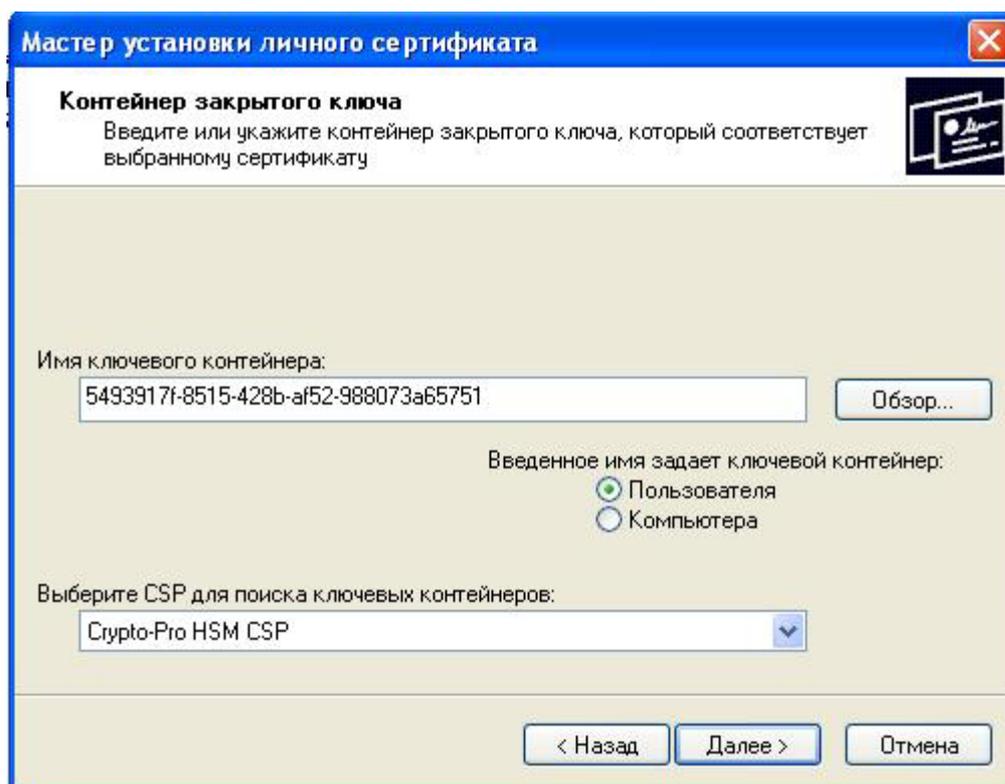
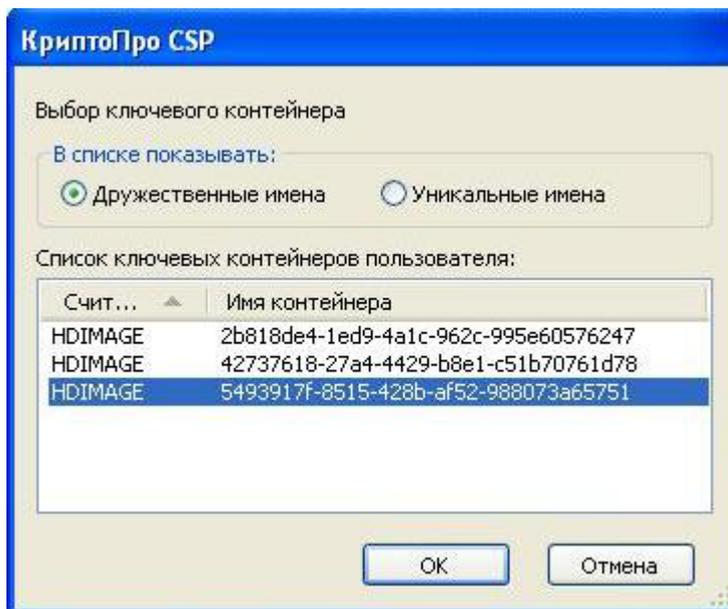


Если нажать «Свойства», появится стандартное окно просмотра сертификата.

В следующем окне необходимо ввести имя ключевого контейнера в ПАКМ, который соответствует устанавливаемому сертификату:

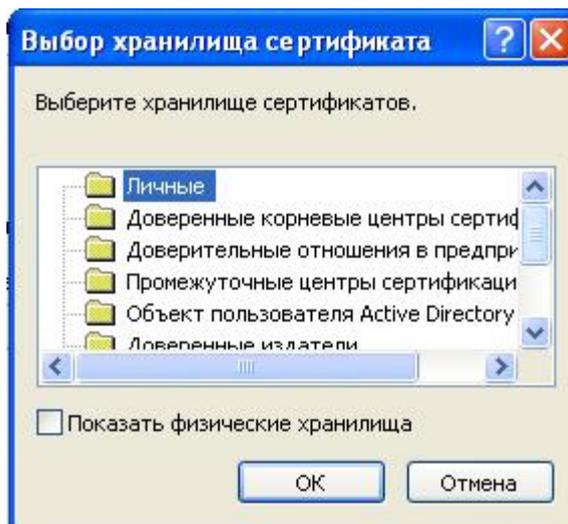
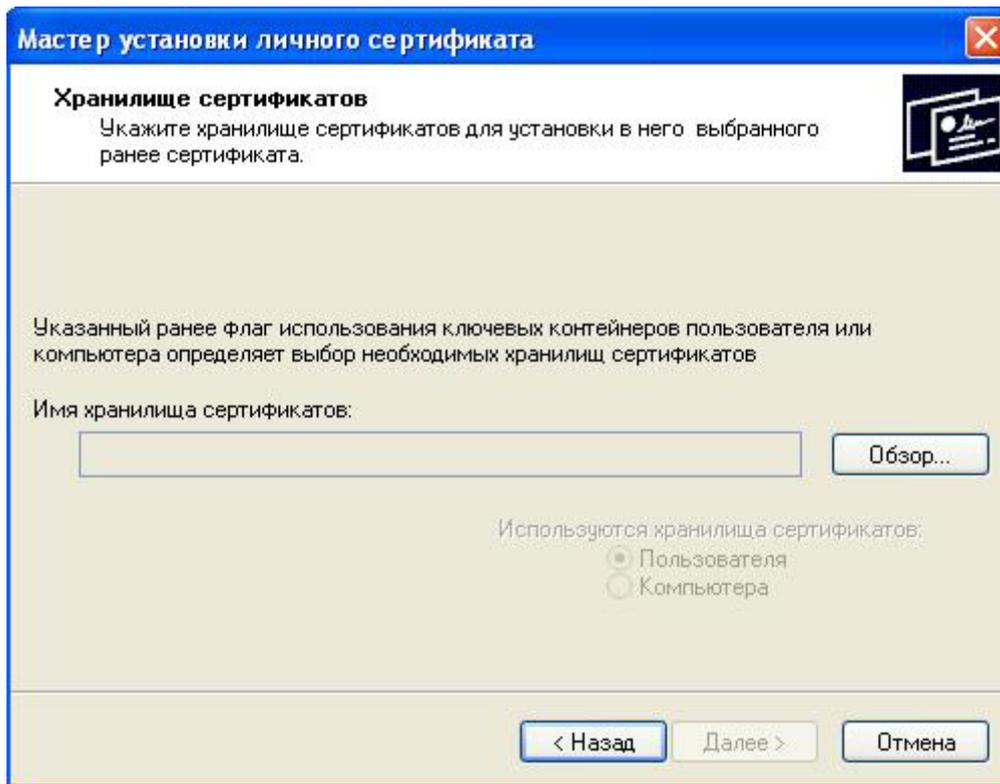


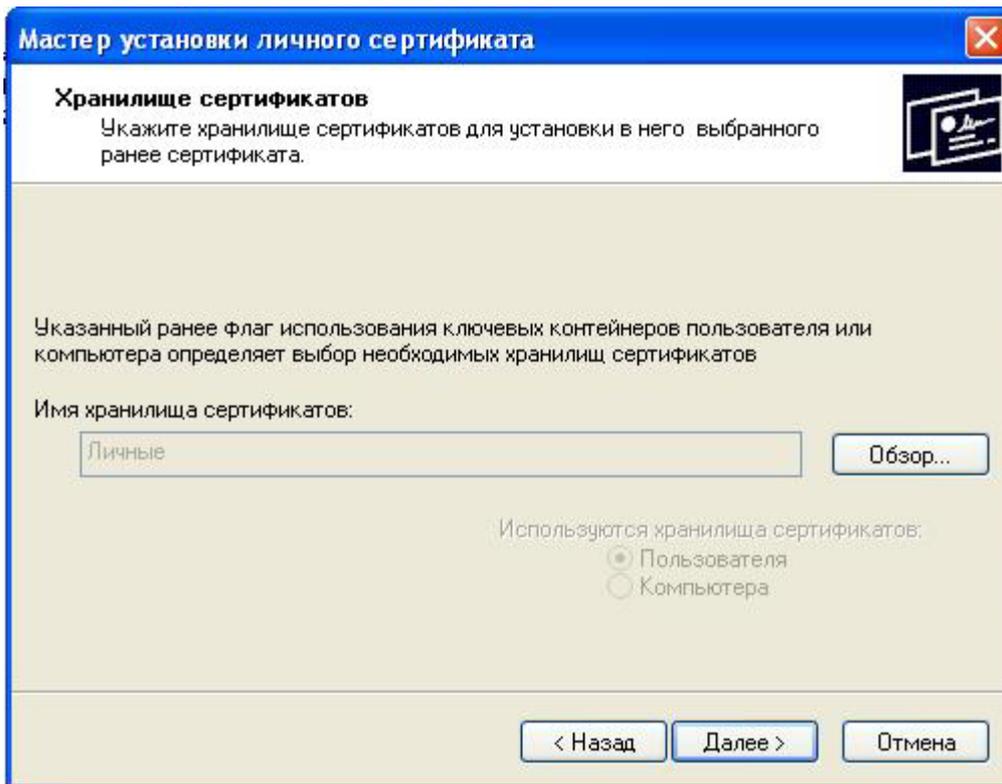
Для выбора контейнера из списка ключевых контейнеров пользователя необходимо нажать кнопку «Обзор...» и выбрать имя контейнера в появившемся окне:



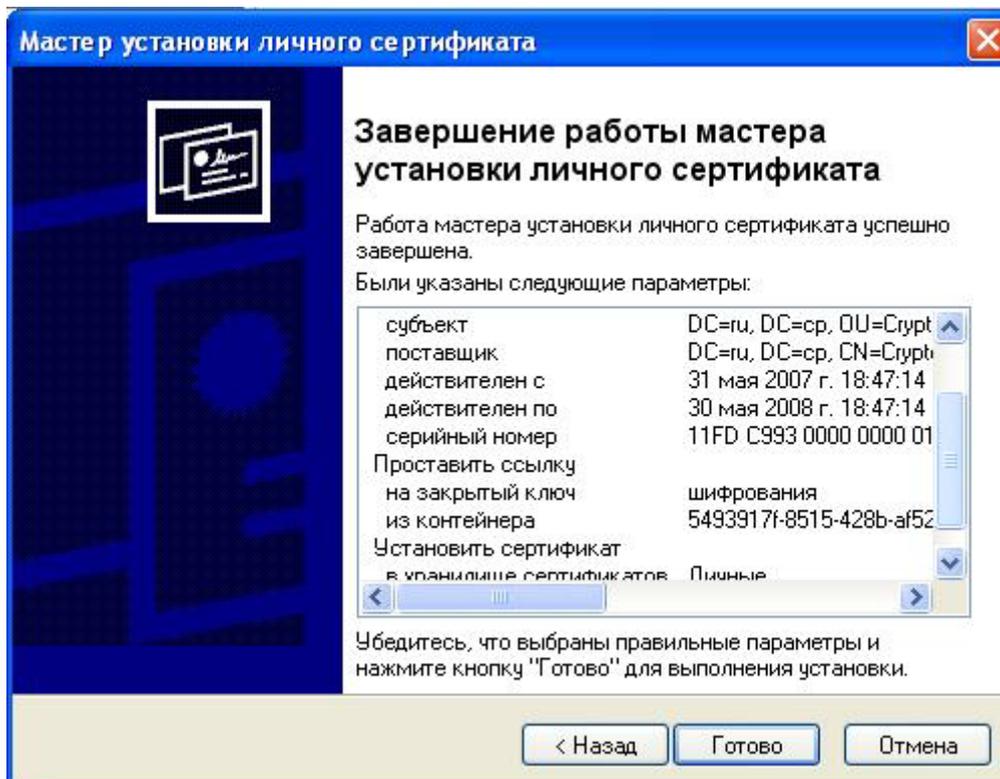
После нажатия кнопки «Далее» появится окно с предложением ввести пароль для контейнера закрытого ключа. Если закрытый ключ на указанном контейнере не соответствует открытому ключу в сертификате, после ввода пароля для контейнера появится сообщение об ошибке.

В следующем окне необходимо нажать кнопку «Обзор...» и выбрать хранилище для установки сертификата:





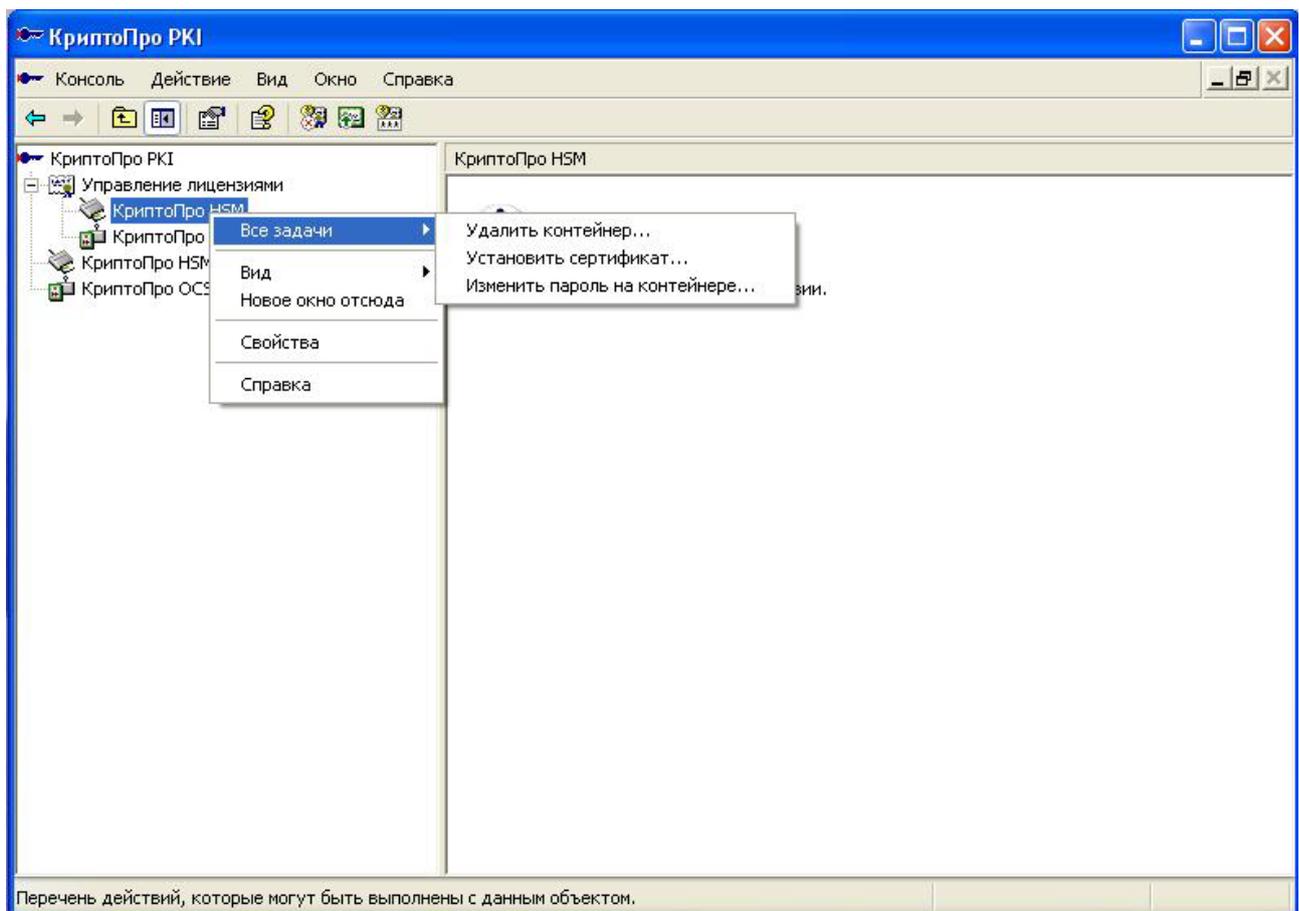
В следующем окне необходимо просмотреть параметры устанавливаемого сертификата и нажать кнопку «Готово».



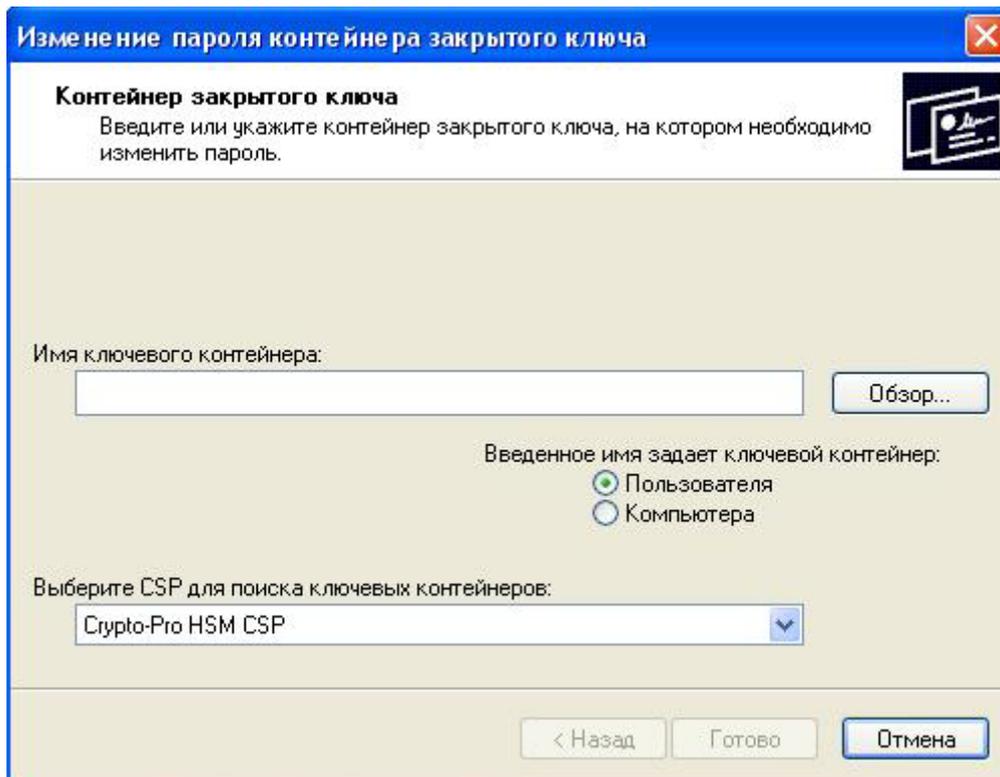
8.2. Изменение пароля на контейнере личного ключа.

Для изменения пароля на контейнере закрытого личного ключа на ПАКМ необходимо открыть сеанс пользователя – владельца ключа и установить связь с ПАКМ (как описано в главе 7).

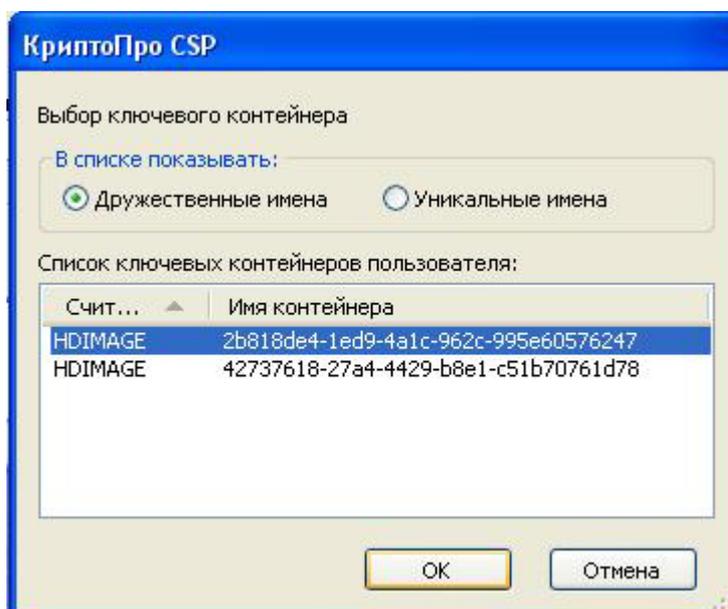
Затем необходимо открыть окно «КриптоПро PKI», щелкнув правой кнопкой мыши на значке «Клиент КриптоПро HSM» на панели задач, и в выпадающем меню выбрав пункт «КриптоПро PKI». В окне «КриптоПро PKI» необходимо щелкнуть правой кнопкой мыши на пункте «КриптоПро HSM» в левой части окна и в выпадающем меню выбрать пункт «Все задачи»→«Изменить пароль на контейнере».



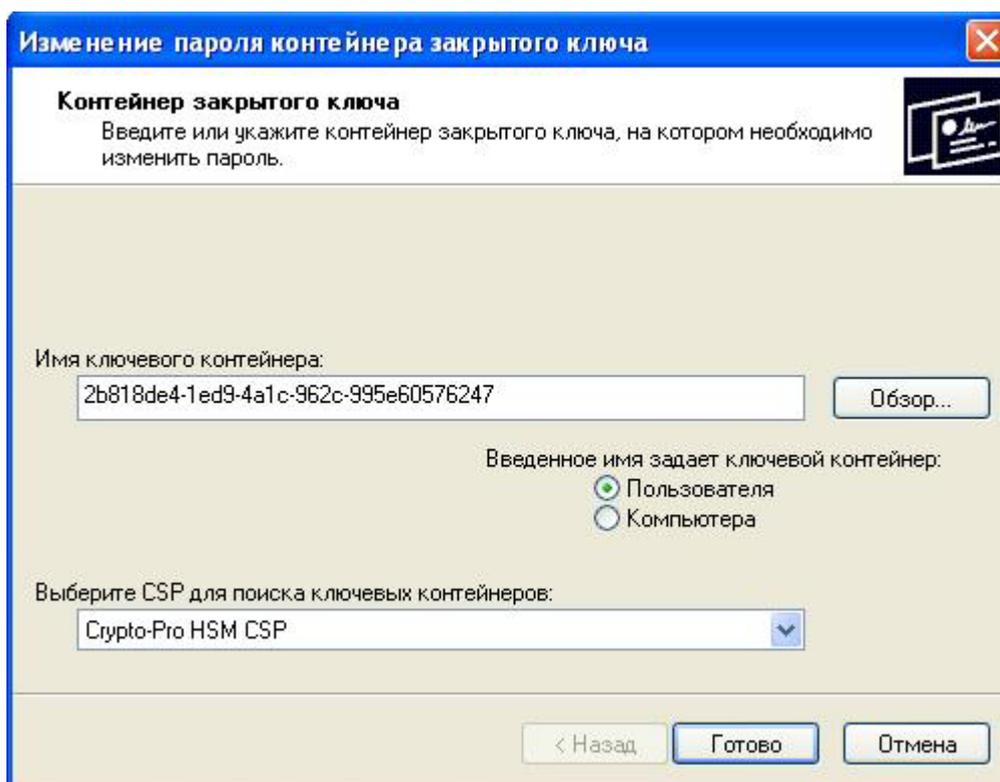
В открывшемся окне необходимо ввести имя ключевого контейнера.



Для выбора контейнера из списка ключевых контейнеров пользователя необходимо нажать кнопку «Обзор...» и выбрать имя контейнера в появившемся окне:



После выбора контейнера необходимо нажать «Готово».



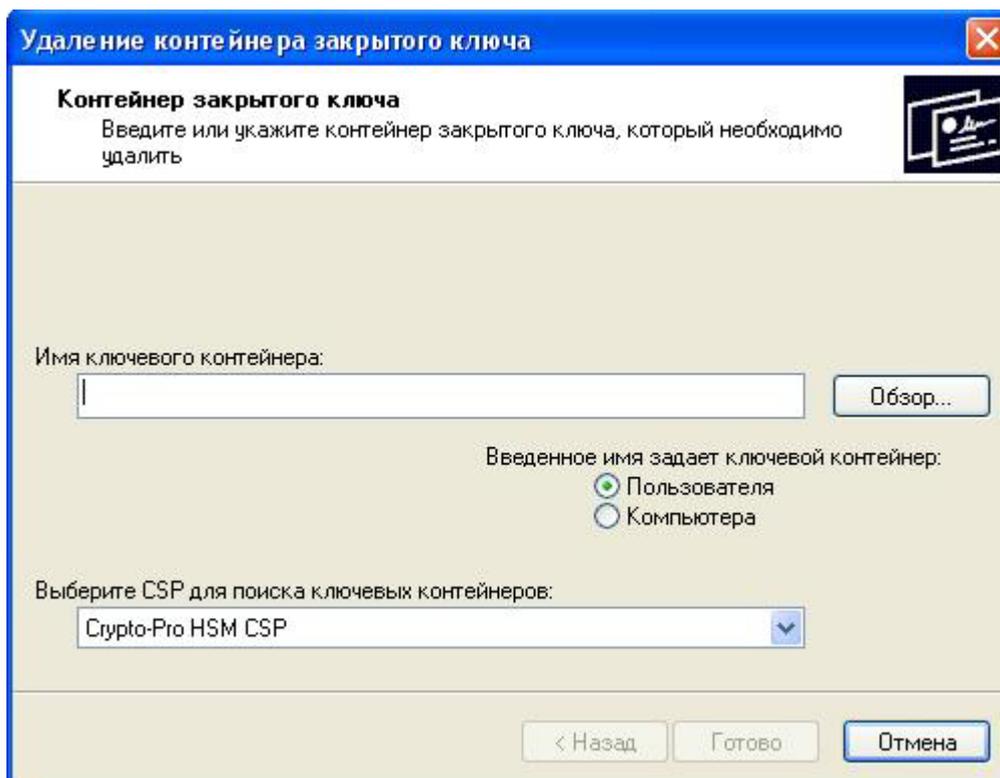
После этого появится окно, в котором необходимо ввести старый пароль контейнера, и затем окно, в котором дважды необходимо будет ввести новый пароль.

8.3. Удаление контейнера личного ключа.

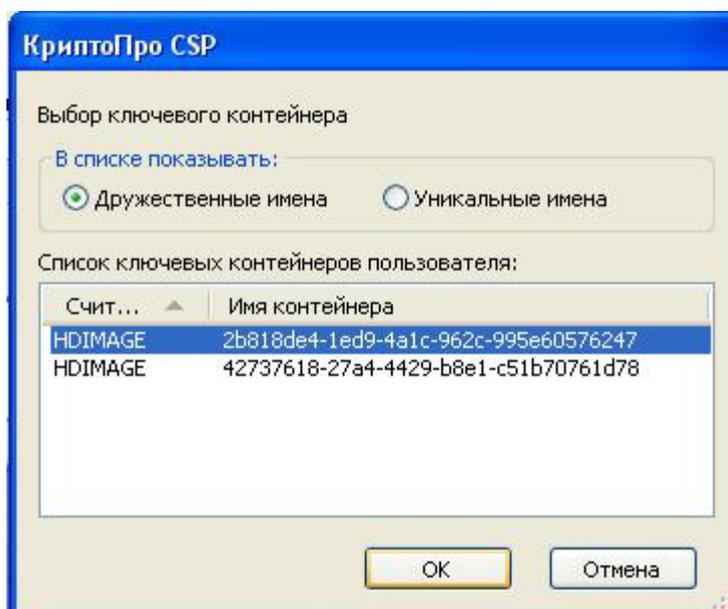
Для удаления контейнера закрытого личного ключа на ПАКМ необходимо открыть сеанс пользователя – владельца ключа и установить связь с ПАКМ (как описано в главе 7).

Затем необходимо открыть окно «КриптоПро PKI», щелкнув правой кнопкой мыши на значке «Клиент КриптоПро HSM» на панели задач, и в выпадающем меню выбрав пункт «КриптоПро PKI». В окне «КриптоПро PKI» необходимо щелкнуть правой кнопкой мыши на пункте «КриптоПро HSM» в левой части окна и в выпадающем меню выбрать пункт «Все задачи» → «Удалить контейнер».

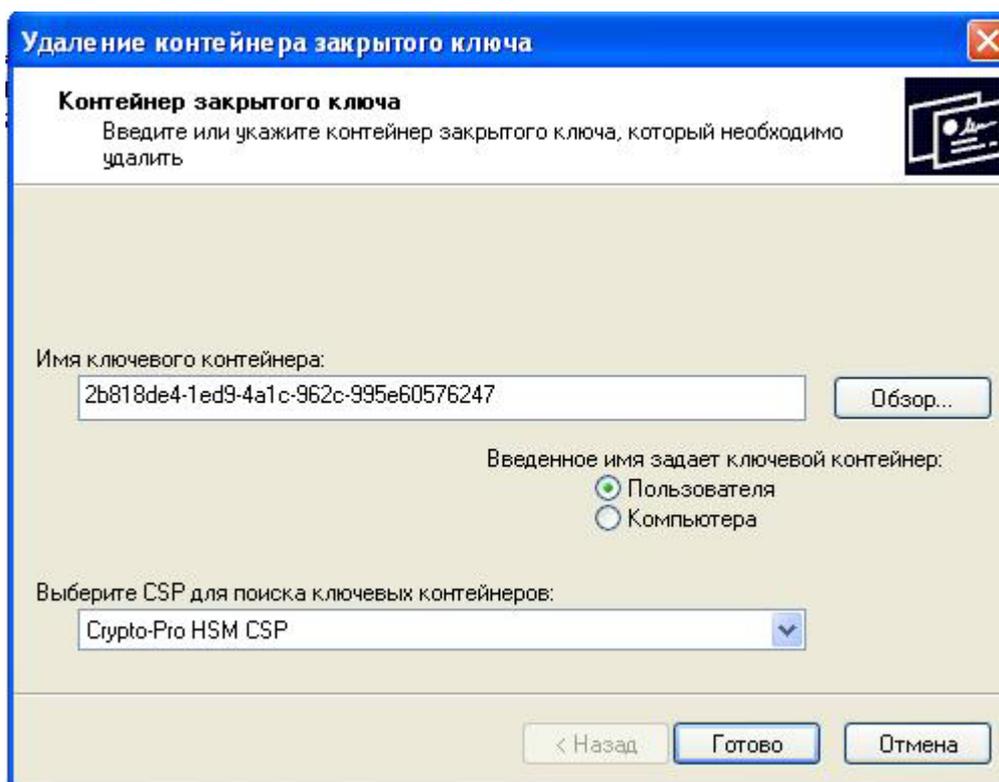
В открывшемся окне необходимо ввести имя ключевого контейнера.



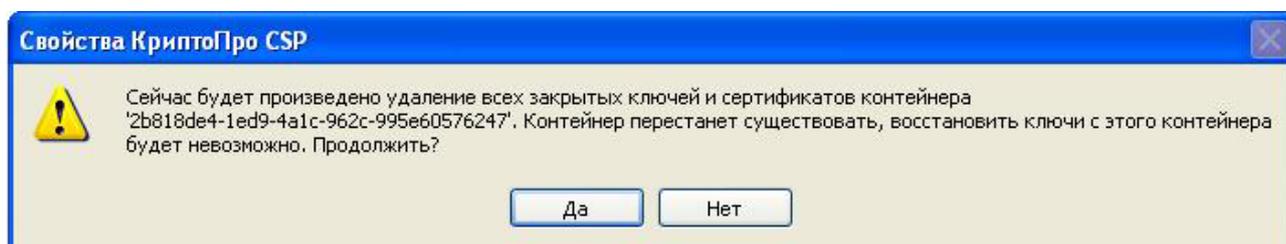
Для выбора контейнера из списка ключевых контейнеров пользователя необходимо нажать кнопку «Обзор...» и выбрать имя контейнера в появившемся окне:



После выбора контейнера необходимо нажать «Готово».



После этого появится предупреждение об удалении ключевого контейнера на ПАКМ:



Если нажать «Да», контейнер будет удален.

Если какое-либо приложение, работающее с данным ключом, было некорректно завершено, и контекст ключа на ПАКМ не был закрыт, при попытке удалить контейнер может появиться сообщение «ошибка обращения к контейнеру: требуемый ресурс занят». В этом случае следует обратиться к администратору ПАКМ.

9. УСТАНОВЛИВАЕМЫЕ КРИПТОПРОВАЙДЕРЫ

В процессе установки дистрибутива ПО «Клиент HSM» в Реестре ОС Windows регистрируются следующие криптопровайдеры:

- **"Crypto-Pro HSM CSP" (тип 75)**
- **"Crypto-Pro HSM Svc CSP" (тип 75)**
- **"Crypto-Pro HSM RSA CSP" (тип 1)**
- **"Crypto-Pro HSM RSA Svc CSP" (тип 1)**

Криптопровайдер "Crypto-Pro HSM CSP" (тип 75) основной криптопровайдер, который должен использоваться внешними приложениями. Он реализует:

- выполнение функций создания и проверки электронной цифровой подписи (ЭЦП) согласно ГОСТ Р 34.10-2001, возможность вычисления хэш-функции согласно ГОСТ Р 34.11-94;
- возможность шифрования и имитозащиты согласно ГОСТ 28147-89;

Для генерации и хранения ключей используется внутренний считыватель ПАКМ с именем «HSM». Его отличительной особенностью является то, что все закрытые ключи шифруются на ключах шифрования ПАКМ.

Криптопровайдер "Crypto-Pro HSM Svc CSP" (тип 75) отличается от криптопровайдера «Crypto-Pro HSM CSP» тем, что позволяет выводить запросы на ввод пин-кодов для ключей пользователей не на «рабочий стол» рабочей станции пользователя, а на LCD панель ПАКМ. Кроме этого он позволяет организовать обмен между сервером и ПАКМ по более производительному нешифрованному каналу, при условии осуществления однозначной двусторонней аутентификации «сервер<->ПАКМ», нахождении сервера и ПАКМ в одной контролируемой зоне и условии, что используется специальный сертификат ключа доступа, включающий расширение (extended key usage - ECU) «Администратор сервера (1.2.643.2.2.34.22)».

Именно этот криптопровайдер должен использоваться в серверных конфигурациях серверами приложений, работающими в фоновом режиме и не имеющими консоли для вывода сообщений и/или запроса пин кодов.

Опционально в ПАКМ «КриптоПро HSM» устанавливаются криптопровайдеры **"Crypto-Pro HSM RSA CSP" (тип 1)** и **"Crypto-Pro HSM RSA Svc CSP" (тип 1)**, которые реализуют алгоритмы электронной цифровой подписи RSA:

- генерацию ключевых пар с размером открытого ключа до 16K
- формирование и проверку ЭЦП (RSA)
- вычисление Hash функции с использованием алгоритмов SHA1, MD5.

Между криптопровайдерами "Crypto-Pro HSM RSA CSP" и "Crypto-Pro HSM RSA Svc CSP" действуют те же различия, что и между «Crypto-Pro HSM CSP» и «Crypto-Pro HSM Svc CSP».

Криптопровайдером по умолчанию для типа 75 является криптопровайдер «Crypto-Pro HSM CSP». Обычному пользователю не следует использовать криптопровайдер «"Crypto-Pro HSM Svc CSP"». Система всё равно не позволит ему работать с данным провайдером, если в сертификате ключа доступа к ПАКМ нет соответствующего расширения.

Администраторам серверов при использовании ПАКМ «КриптоПро HSM» с такими сервисами как Microsoft CA, «КриптоПро УЦ», Microsoft IIS и другими, реализованными в виде служб ОС Windows необходимо использовать криптопровайдер «Crypto-Pro HSM Svc CSP». Клиентская часть данного провайдера (на машине клиента ПАКМ «КриптоПро HSM») реализована в виде службы ОС Windows, которая запускается в момент загрузки ОС и может обслуживать криптографические запросы других служб даже, если никто из пользователей не открыл Windows сессию (простым языком – «не залогинился»).

Клиентская же часть данного провайдера «Crypto-Pro HSM CSP» реализована в виде обычного пользовательского приложения, которое грузится в момент входа («логон-а») пользователя, и отображается в виде иконки в системном трее. Таким образом, если на ПЭВМ с установленным ПО «Клиент HSM» нет активной Windows сессии (ни одного «залогиненного» пользователя), то никто не сможет обслужить криптографические запросы, обращенные к криптопровайдеру «Crypto-Pro HSM CSP».

Администраторам серверов, наоборот, рекомендуется установить для провайдера 75 типа криптопровайдером по-умолчанию «Crypto-Pro HSM Svc CSP», т.к. некоторые вызовы сервисы Windows делают через провайдеры «по-умолчанию».

Процесс установки дистрибутива ПО «Клиент HSM» не изменяет значение провайдера «по-умолчанию» для «1»-го типа. Обычно, в ОС Windows им является криптопровайдер «Microsoft Strong Cryptographic Provider».

10. ЛИТЕРАТУРА

1. ГОСТ 28147-89. Государственный стандарт Российской Федерации. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
 2. ГОСТ Р 34.10-94. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.
 3. ГОСТ Р 34.10-2001. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
 4. ГОСТ Р 34.11-94. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция хэширования.
 5. ЖТЯИ.00020-01 30 01. «КриптоПро HSM». Формуляр.
 6. ЖТЯИ.00046-01 90 02. КриптоПро HSM. Правила пользования.
 7. ЖТЯИ.00020-01 30 03. «КриптоПро HSM». Руководство Администратора безопасности.
 8. ЖТЯИ.00046-01 90 04. КриптоПро HSM. Руководство программиста.
 9. [X.680-X.699]. OSI NETWORKING AND SYSTEM ASPECTS. Abstract Syntax Notation One (ASN.1)
 10. [X.509]. ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997.
 11. [PKIX]. RFC 2459. Housley, W. Ford, W. Polk, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", January 1999.
 12. Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005).
-

