Институт энергетических систем

Сайт «Конкурентный отбор мощности»

Инструкция по настройке ЭЦП

2010

Содержание

1. Установка ПО драйверов USB ключа eTokenPRO

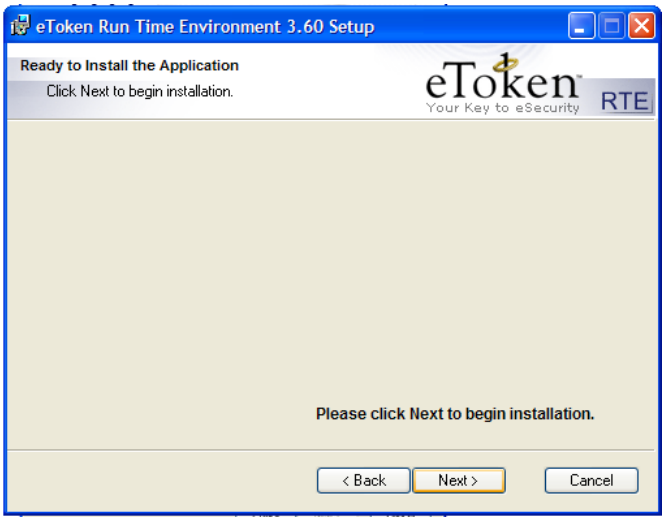
1.1 Установка драйверов USB ключа eTokenPRO

Запускаем файл rte_3.60.msi

нажимаем кнопку «Next»

Выбираем «I accept the license agreement»

нажимаем кнопку «Next»

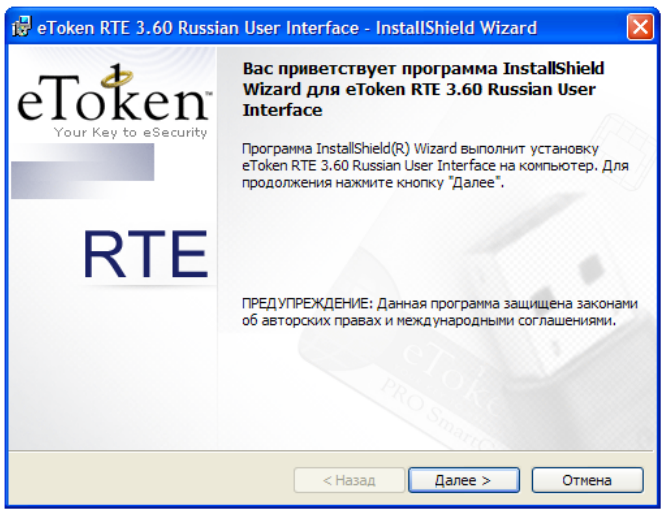


Извлекаем из USB портов все ключи и нажимаем кнопку «Next»

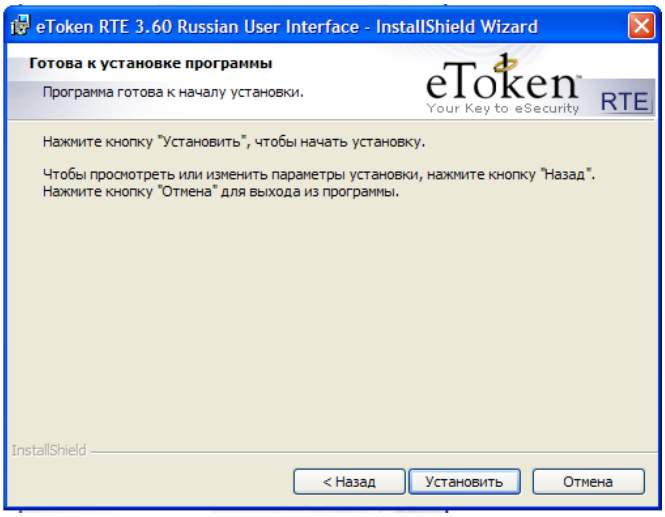
нажимаем кнопку «Finish»

1.2 Установка русскоязычного интерфейса драйверов USB ключа eTokenPRO

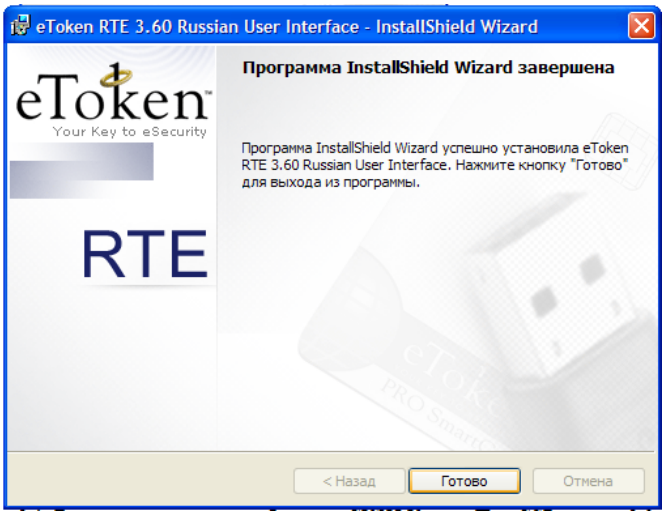
Запускаем файл rte_3.60.RUI.msi



Нажимаем кнопку «Далее»



Нажимаем кнопку «Установить»



Нажимаем кнопку «Готово»

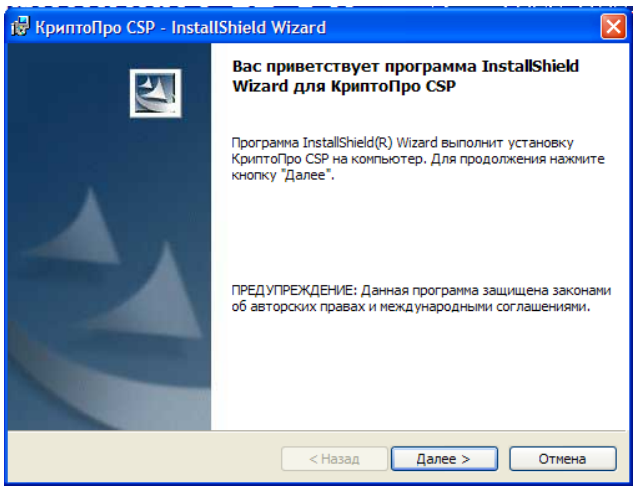
2. Установка СКЗИ КриптоПРО CSP

2.1 Установка ПО СКЗИ «КриптоПро CSP 3.0»

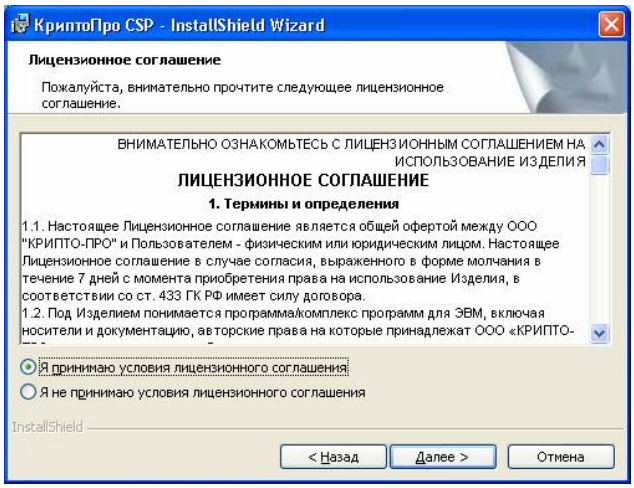
Вставить диск с дистрибутивом СКЗИ КриптоПро CSP версии 3.0;

Нажимаем кнопку «Установить CSP»

Выбираем версию «КриптоПро CSP 3.0 КС1 рус»

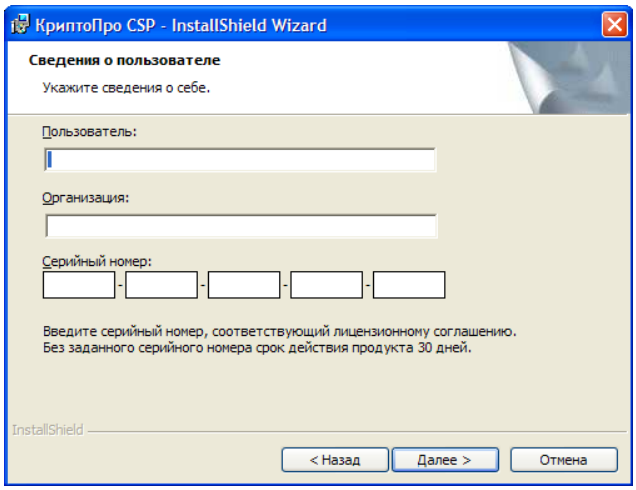


Нажимаем кнопку «Далее»



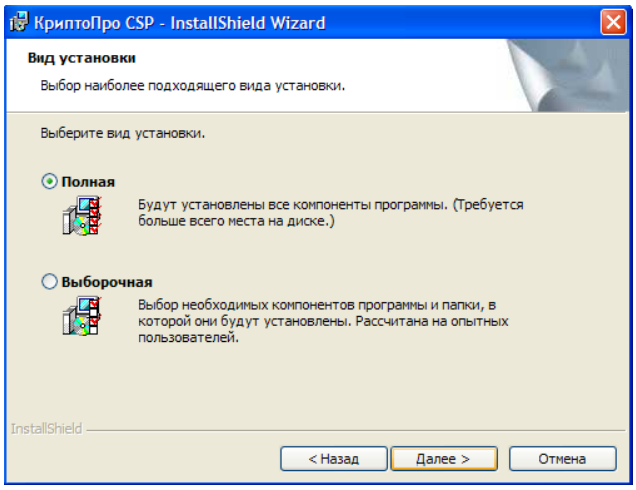
Выбираем «Я принимаю условия лицензионного соглашения»

Нажимаем кнопку «Далее»



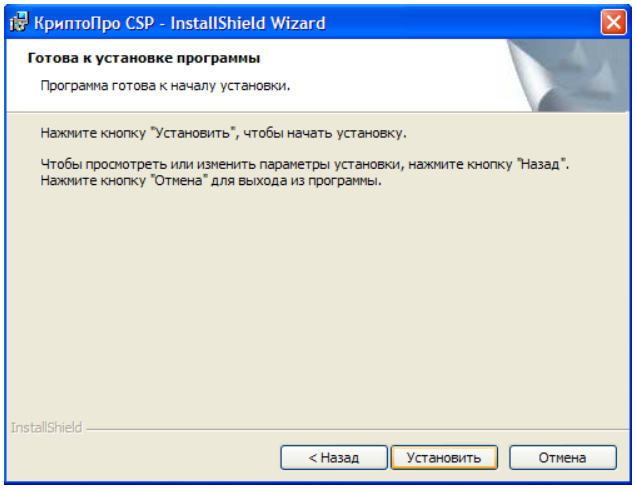
Вводим серийный номер лицензии на использование КриптоПро CSP 3.0.

Нажимаем кнопку «Далее»

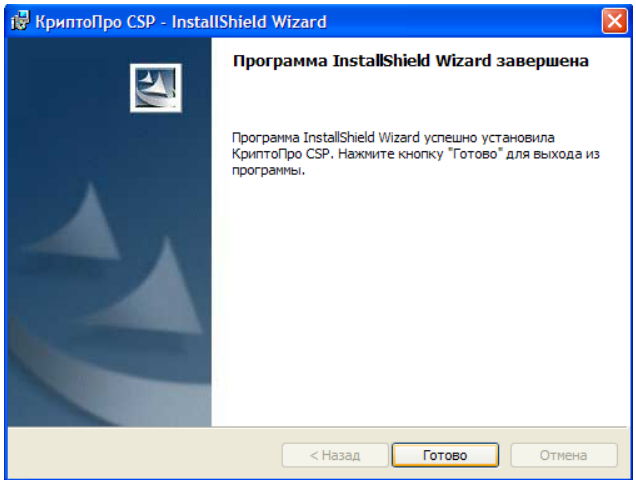


Выбираем полную версию СКЗИ

Нажимаем кнопку «Далее»



Нажимаем «Установить»



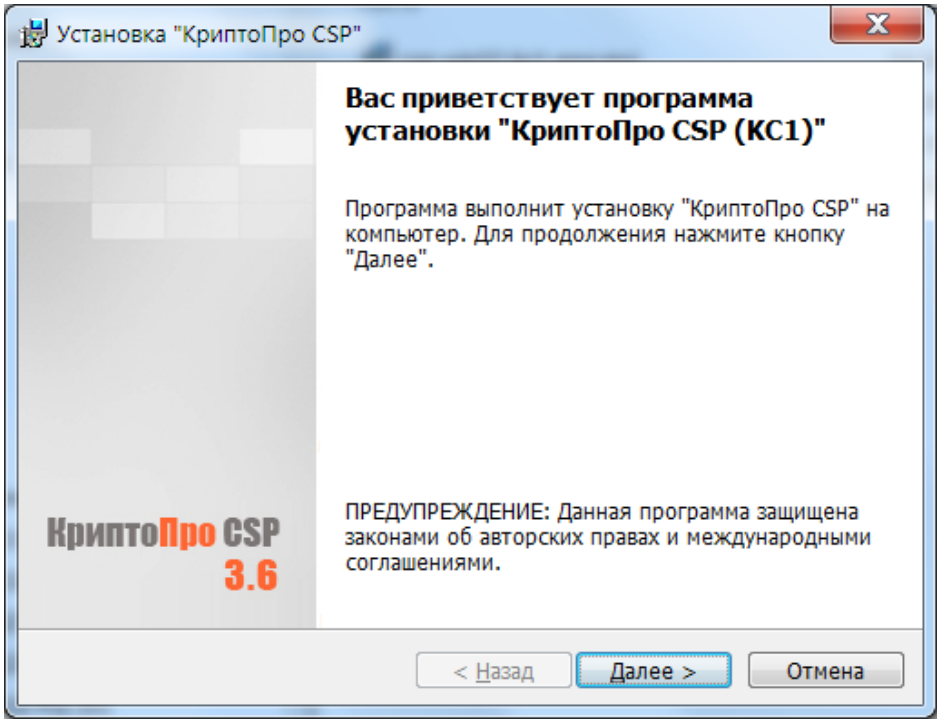
Нажимаем «Готово»

Перезагружаем компьютер

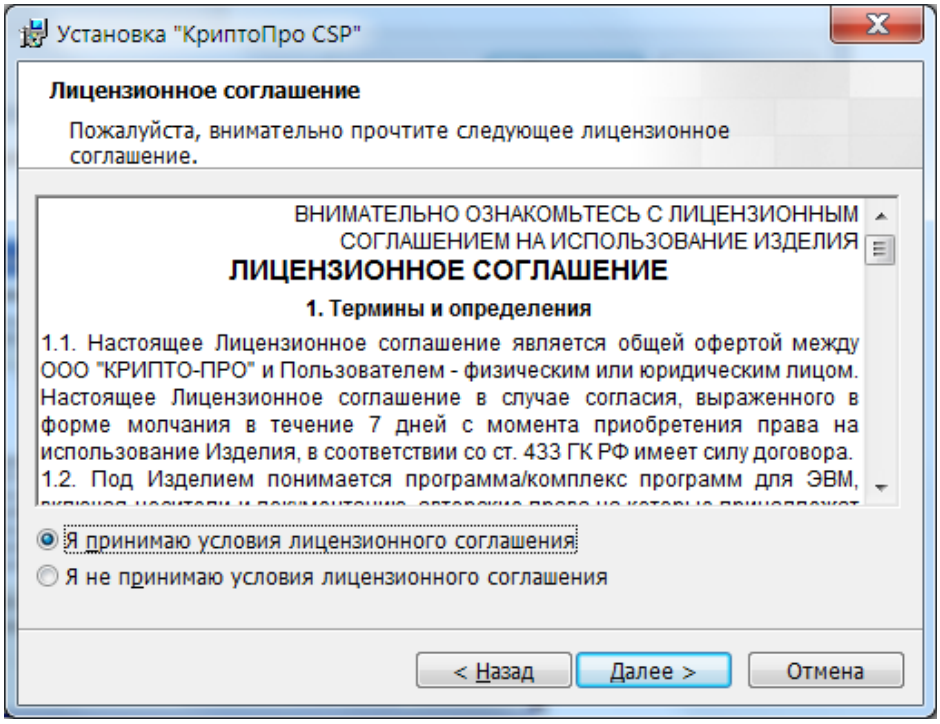
2.2 **Установка ПО СКЗИ «КриптоПро CSP 3.6»** для Windows x64 (XP x64, 2003 Server x64, Vista x64, 2008 Server x64, Windows 7 x64)**:**

Вставить диск с дистрибутивом СКЗИ КриптоПро CSP версии 3.6;

Выбираем и запускаем версию «КриптоПро CSP 3.6 x64 КС1 рус»

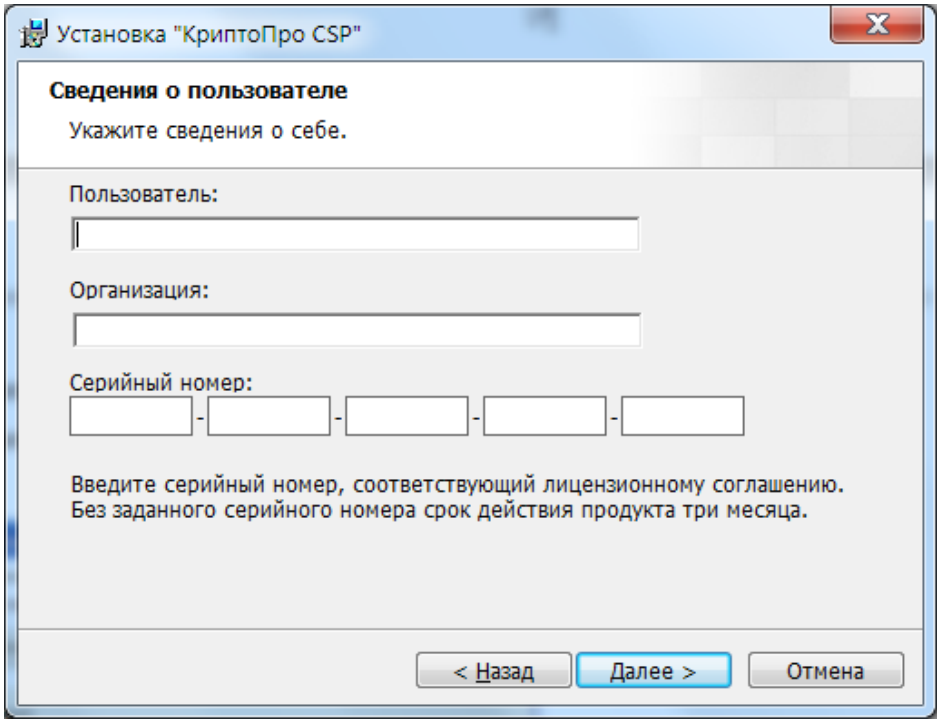


Нажимаем кнопку «Далее»



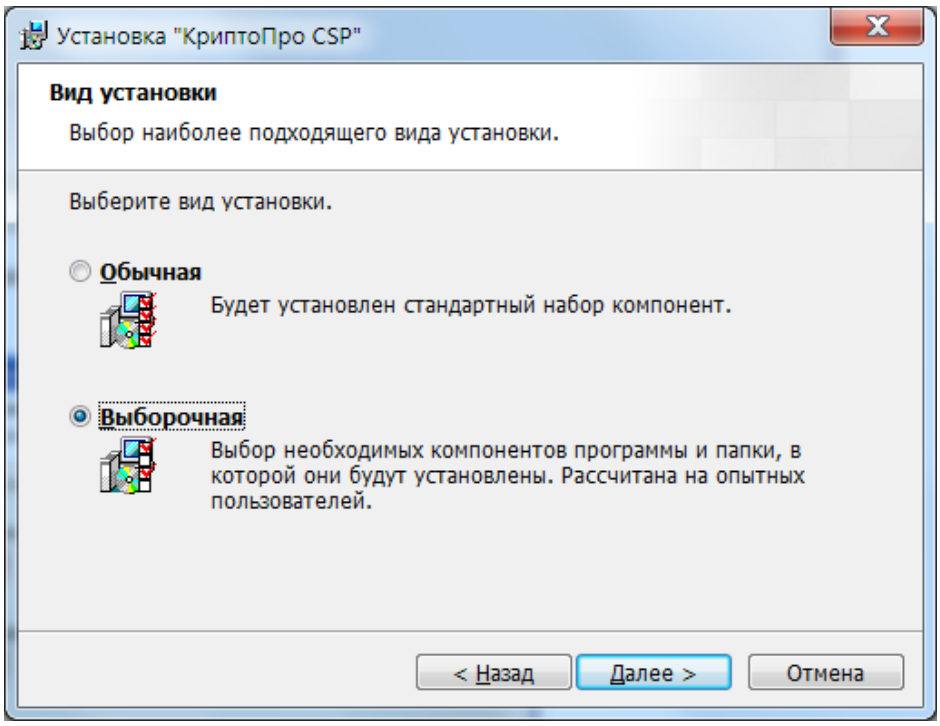
Выбираем «Я принимаю условия лицензионного соглашения»

Нажимаем кнопку «Далее»



Вводим серийный номер лицензии на использование КриптоПро CSP 3.6.

Нажимаем кнопку «Далее»

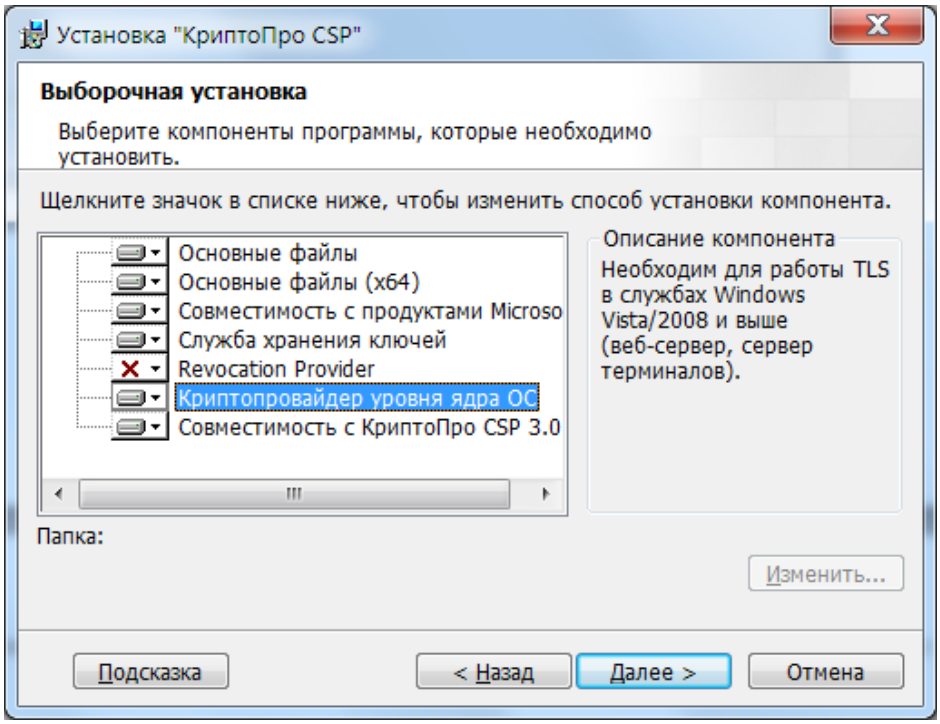


Выбираем выборочную версию СКЗИ

Нажимаем кнопку «Далее»

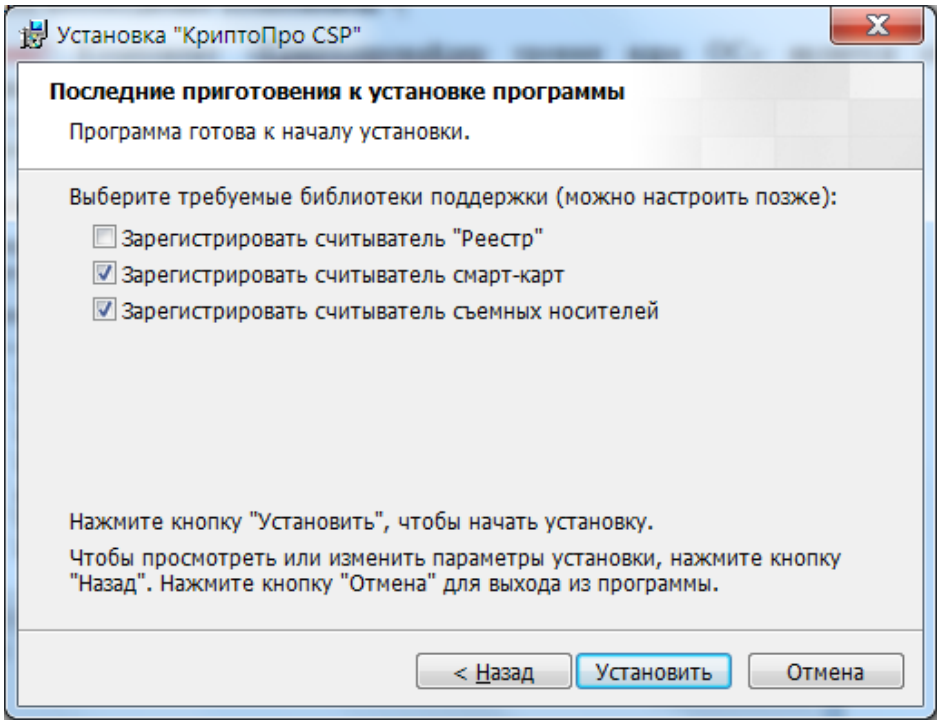
Выбираем необходимые компоненты.

Внимание! Компонент «Криптопровайдер уровня ядра ОС» является обязательным для установки.

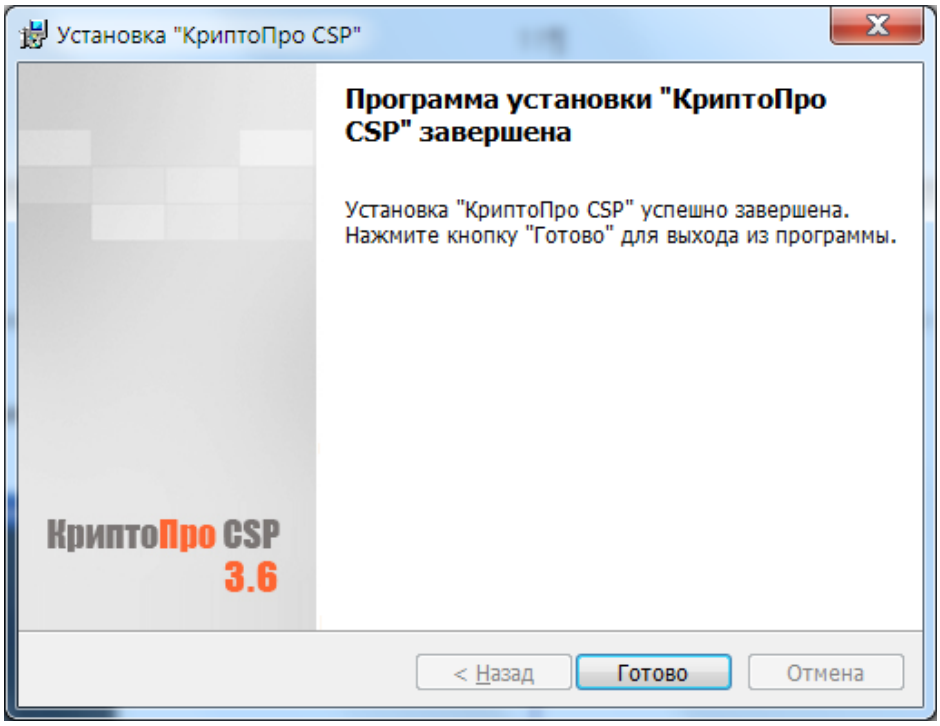


Нажимаем кнопку «Далее»

Выбираем требуемые библиотеки поддержки



Нажимаем кнопку «Установить»



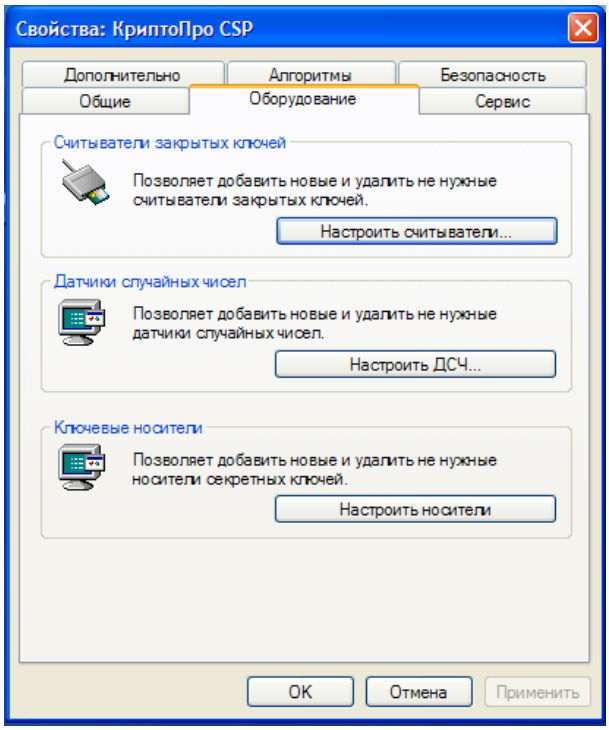
Нажимаем «Готово»

Перезагружаем компьютер

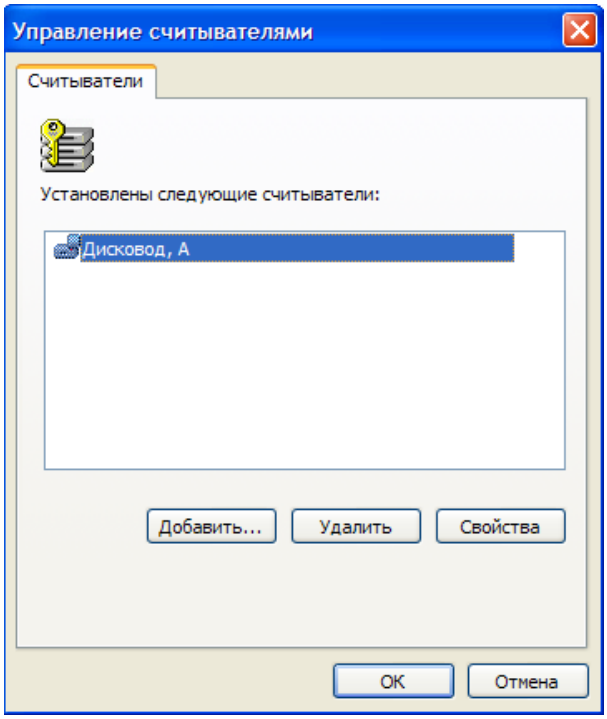
2.3 Настройка носителей и считывателей для работы eToken с криптопровайдером КриптоПРО.

2.3.1.1 Настройка считывателей в КриптоПро CSP

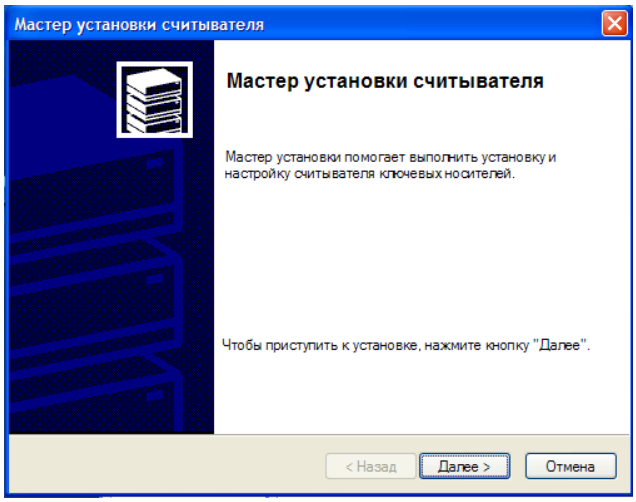
Заходим в Пуск – Настройка – Панель управления – КриптоПро - вкладка Оборудование



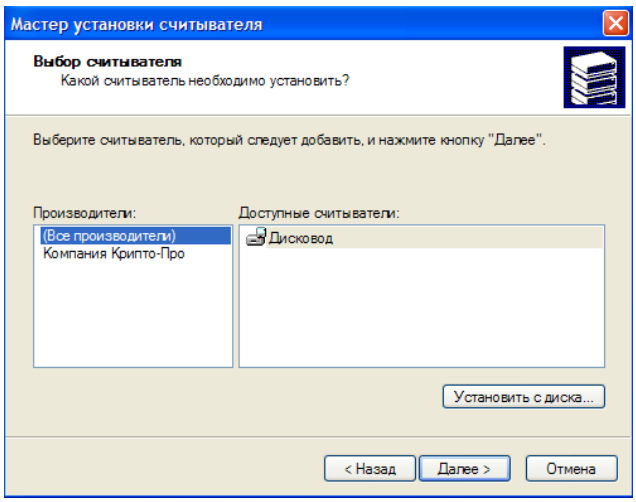
Нажимаем кнопку «Настроить считыватели»



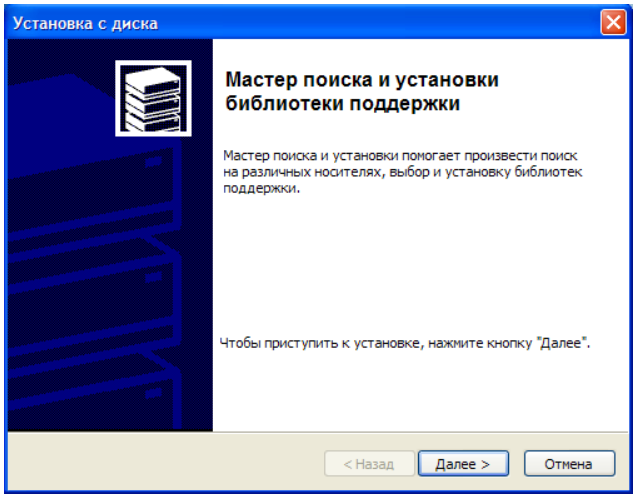
Нажимаем кнопку «Добавить»



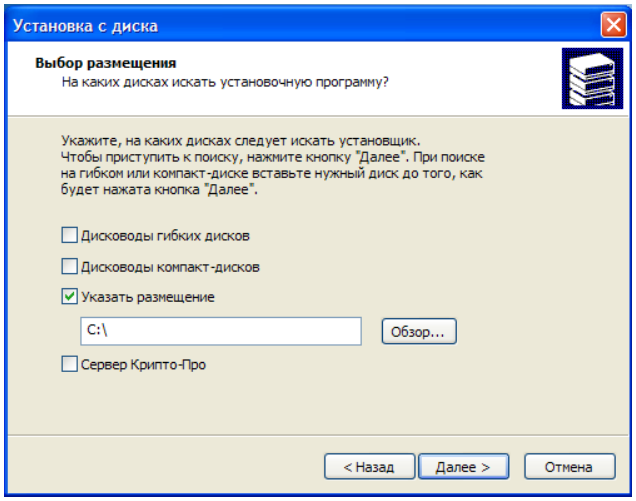
Нажимаем «Далее»



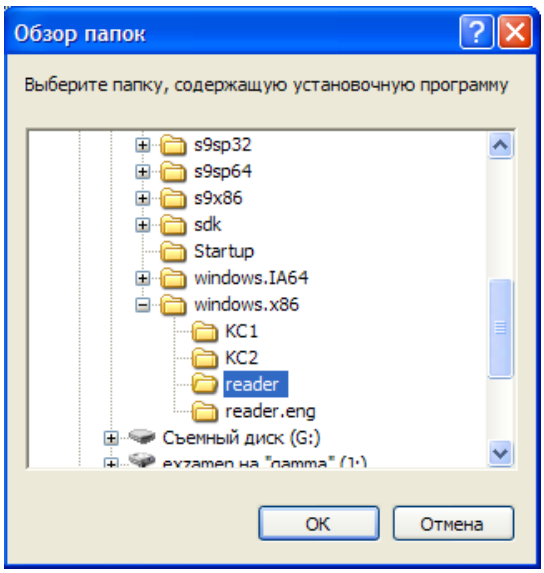
Нажимаем «Установить с диска»



Нажимаем «Далее»

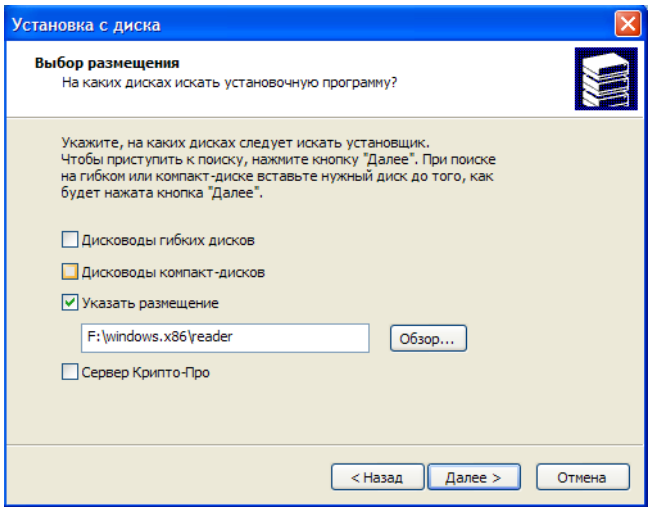


Нажимаем «Обзор…»

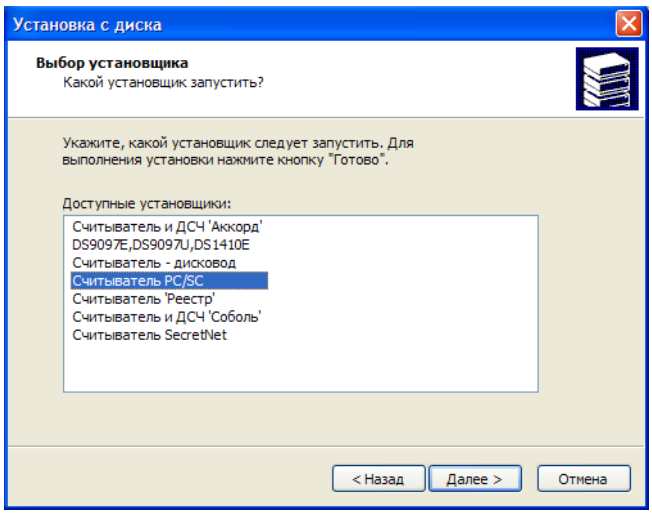


Выбираем папку, например, windows.x86/reader на инсталляционном диске для КриптоПро CSP 3.0

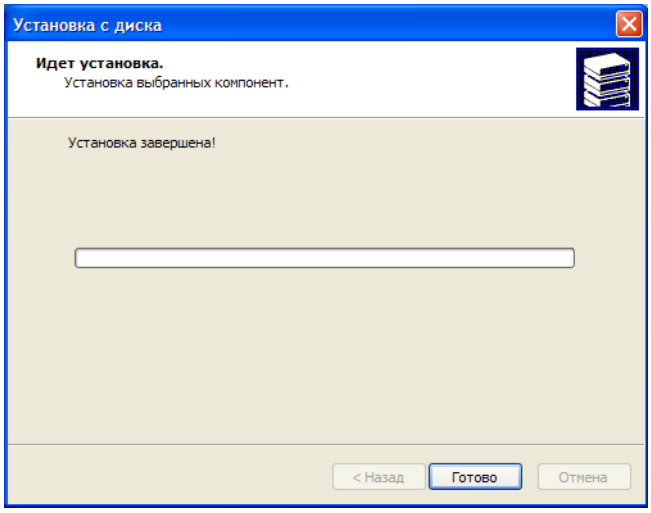
Нажимаем «ОК»



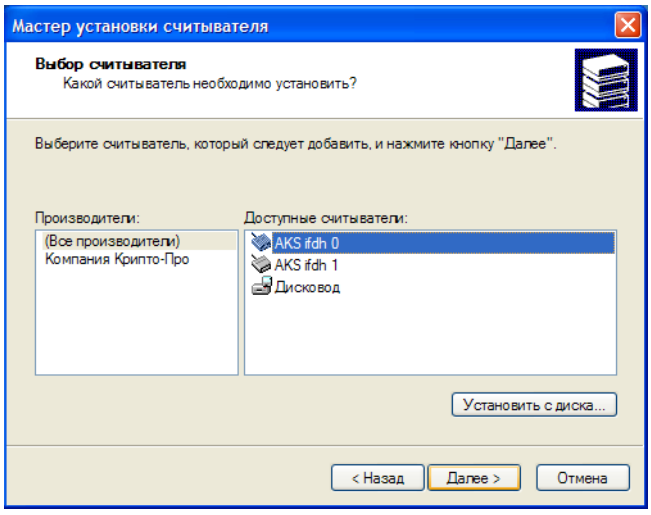
Нажимаем «Далее»



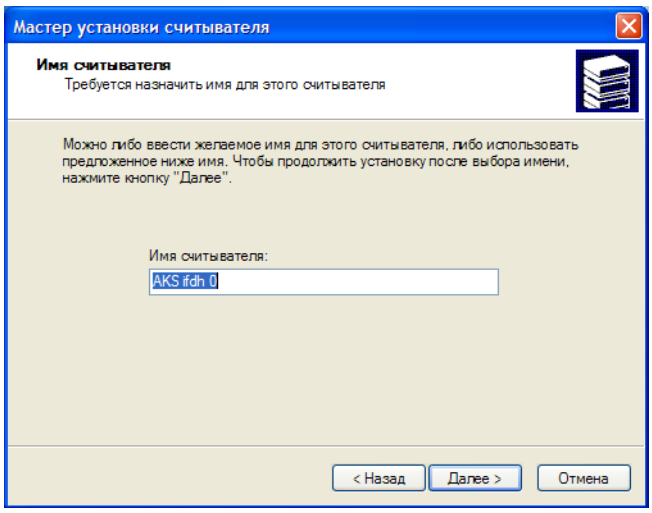
Выбираем «Считыватель PC/SC» и нажимаем кнопку «Далее»



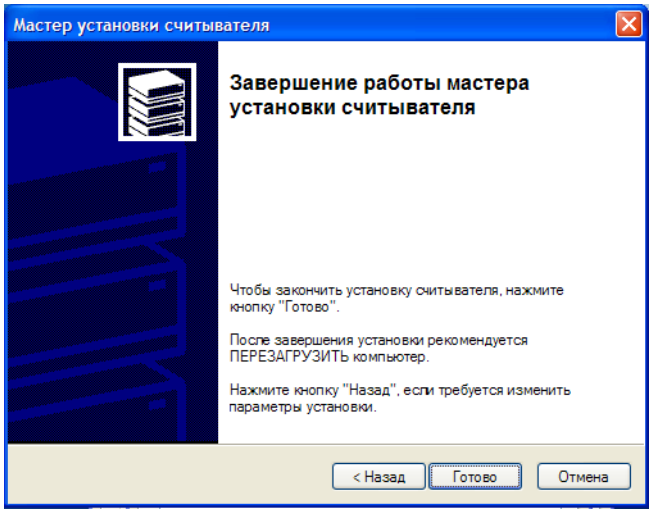
Нажимаем кнопку «Готово»



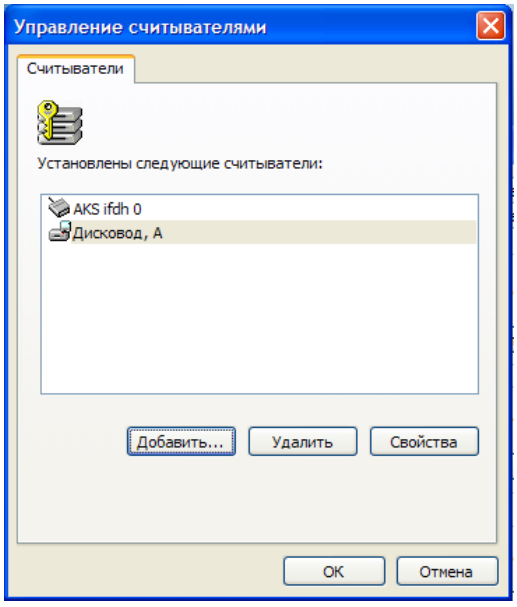
Выбираем из доступных считывателей «AKS ifdh 0» и нажимаем кнопку «Далее»



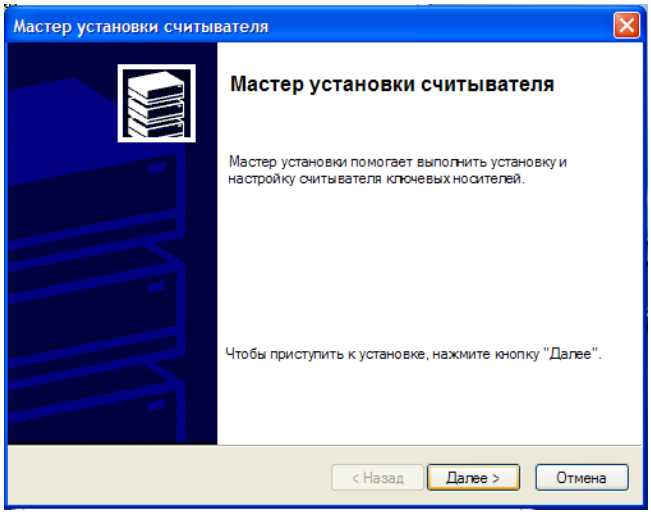
Нажимаем кнопку «Далее»



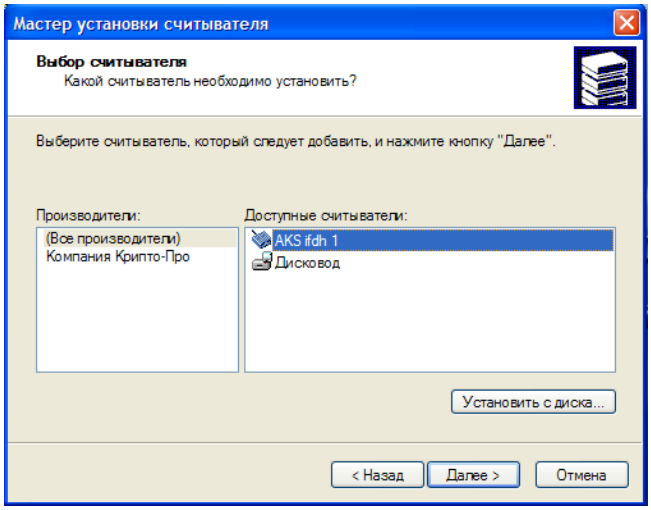
Нажимаем кнопку «Готово»



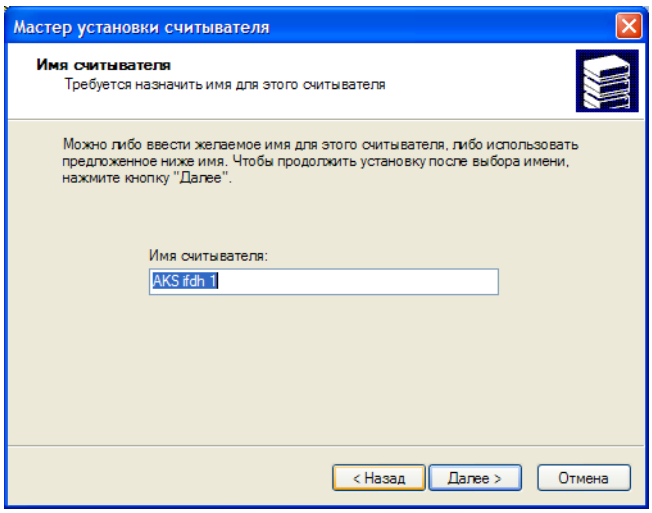
Нажимаем кнопку «Добавить»



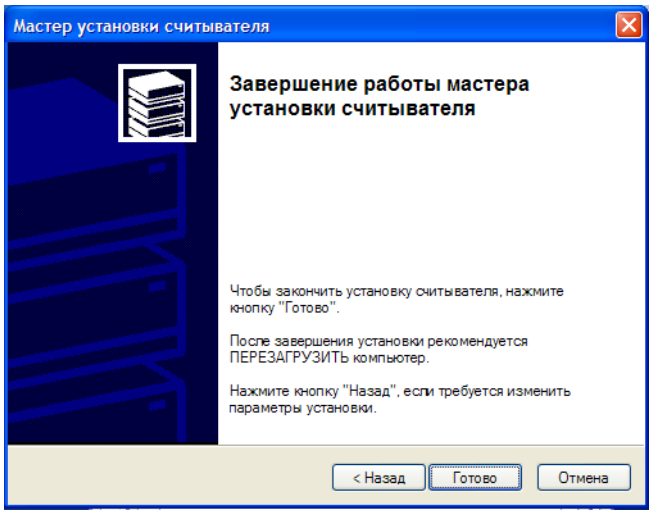
Нажимаем «Далее»



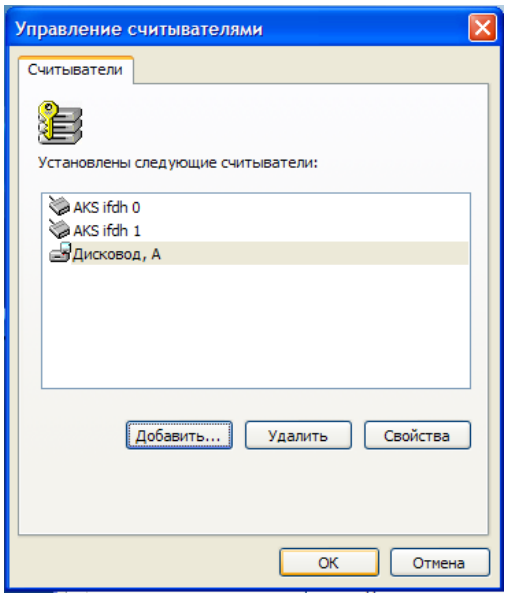
Выбираем из доступных считывателей «AKS ifdh 1» и нажимаем кнопку «Далее»



Нажимаем кнопку «Далее»



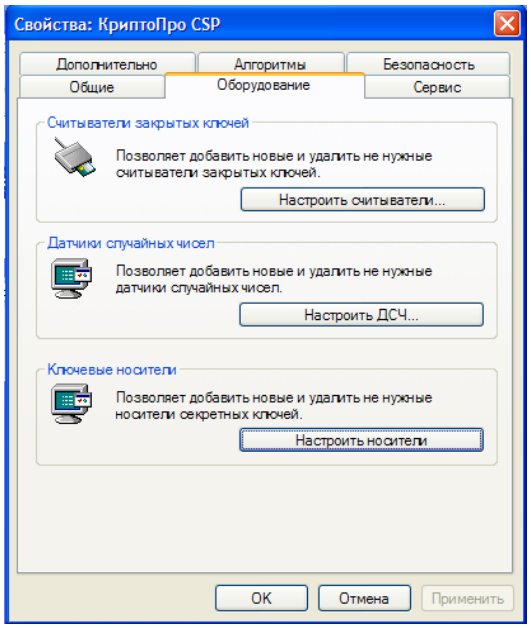
Нажимаем кнопку «Готово»



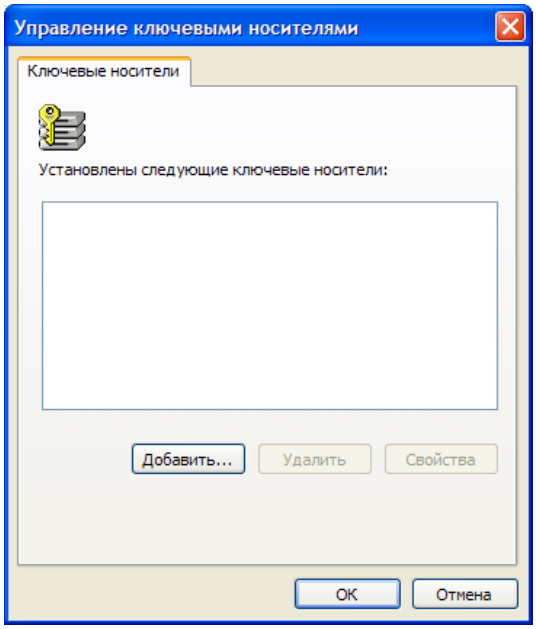
Нажимаем «ОК»

2.3.1.2 Настройка носителей в КриптоПро CSP

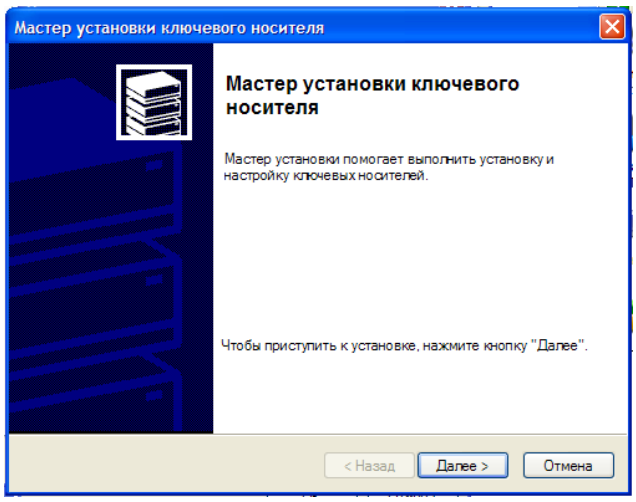
Заходим в Пуск – Настройка – Панель управления – КриптоПро - вкладка Оборудование



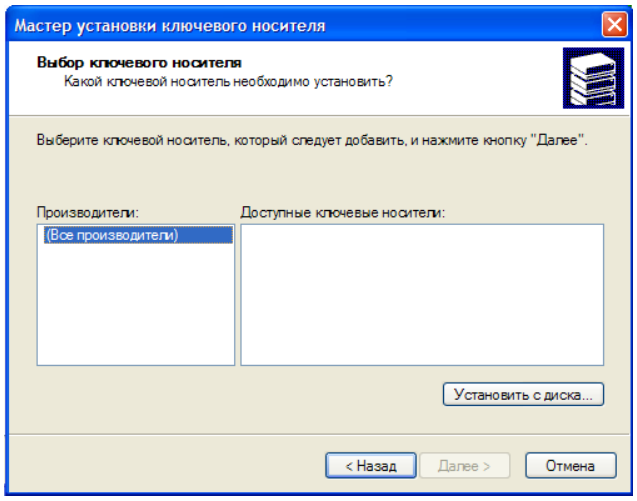
Нажимаем кнопку «Настроить носители»



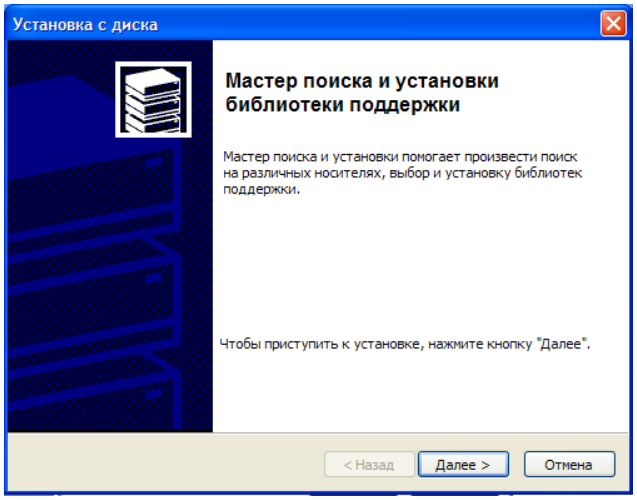
Нажимаем кнопку «Добавить»



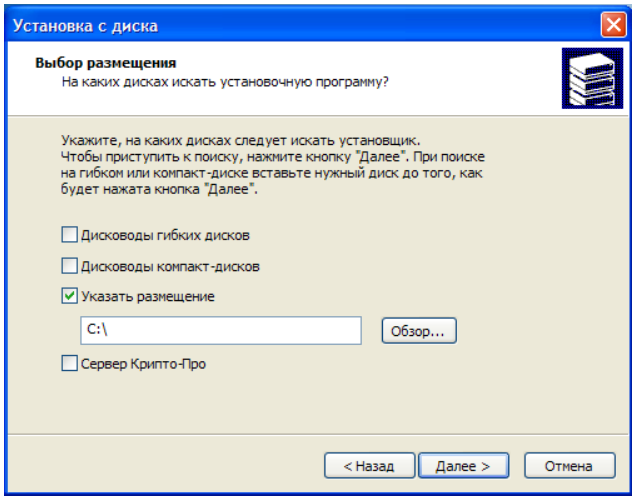
Нажимаем кнопку «Далее»



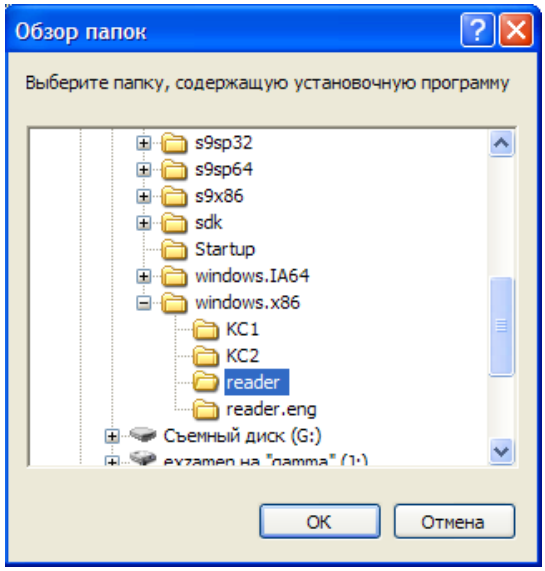
Нажимаем кнопку «Установить с диска…»



Нажимаем «Далее»

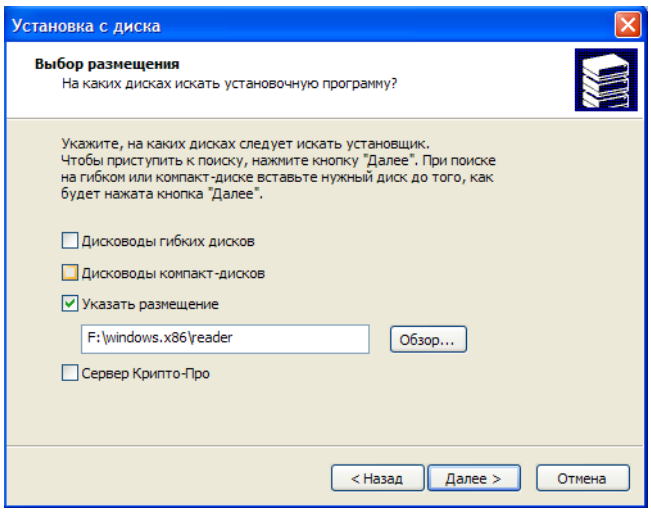


Нажимаем «Обзор…»

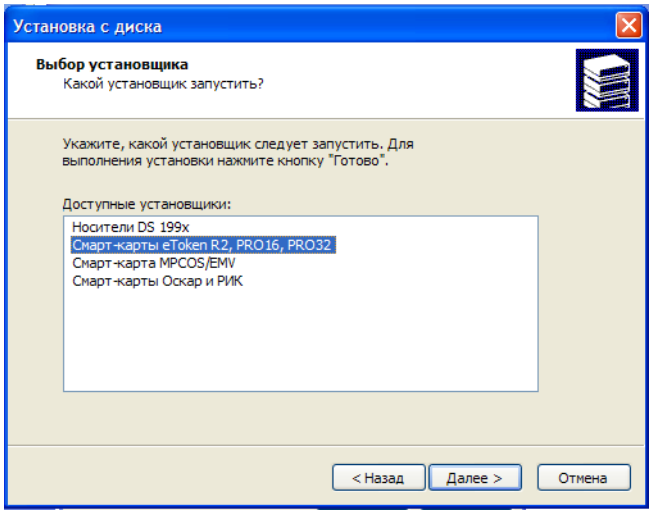


Выбираем папку, например, windows.x86/reader на инсталляционном диске для КриптоПро CSP 3.0

Нажимаем «ОК»

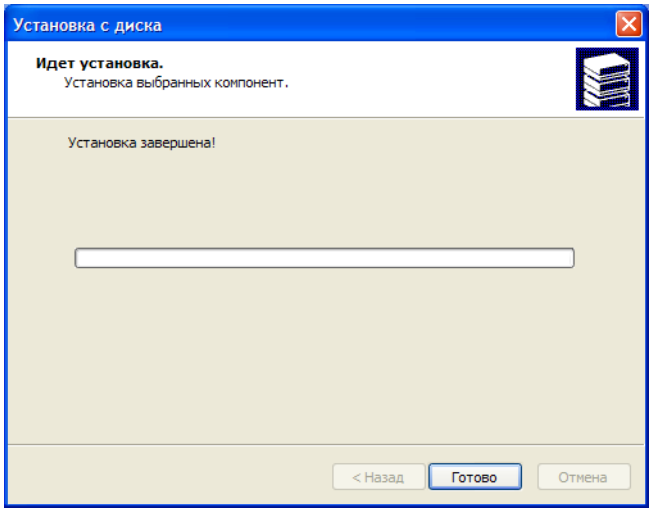


Нажимаем «Далее»

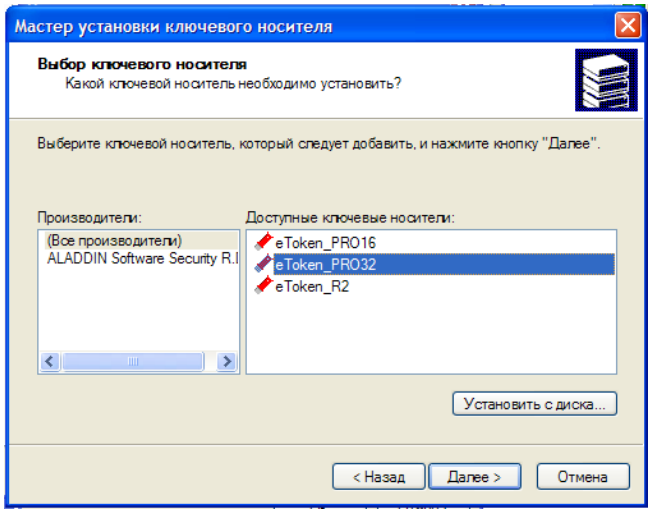


Выбираем «Смарт-карты e-Token R2, PRO16, PRO32»

Нажимаем «Далее»

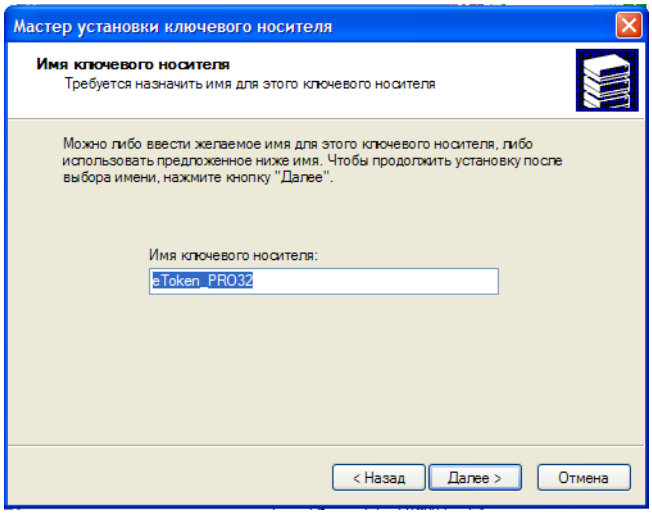


Нажимаем «Готово»

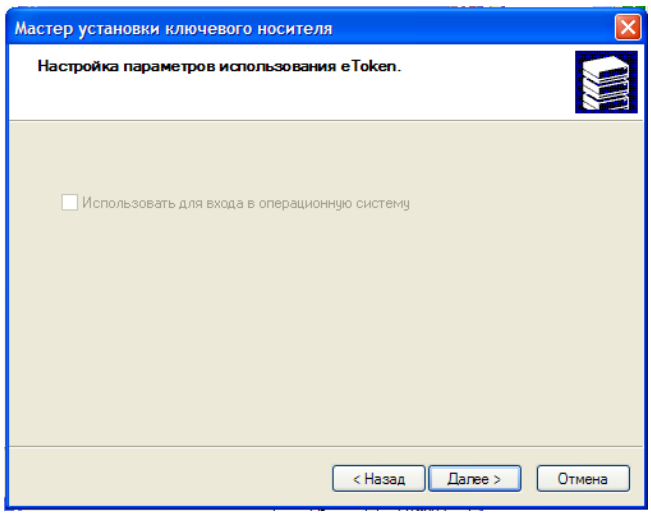


Из доступных ключевых носителей выбираем «eToken_PRO32»

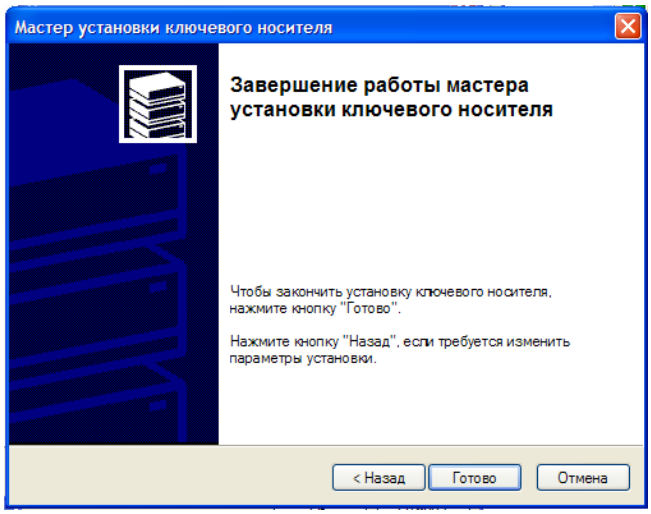
Нажимаем «Далее»



Нажимаем «Далее»



Нажимаем «Далее»



Нажимаем «Готово»

3. Установка библиотеки CAPICOM 2.1.0.2

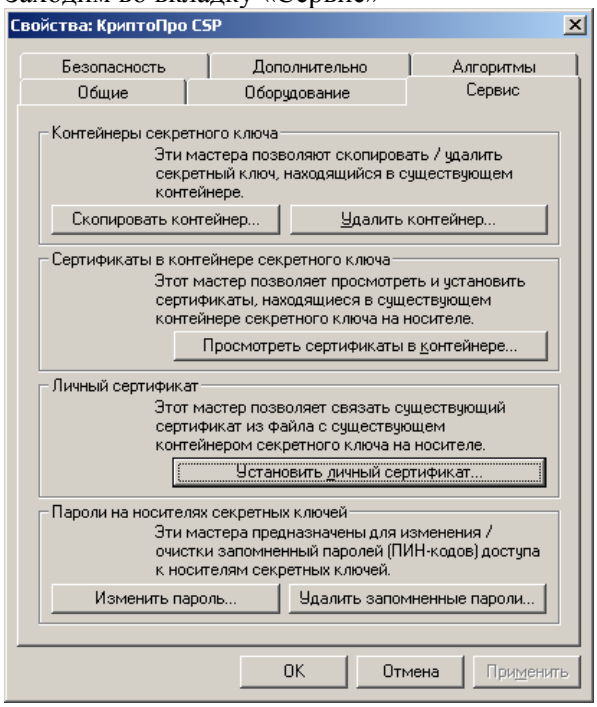
Загрузить файл библиотеки capicom.dll версии 2.1.0.2 с сайта Microsoft (http://www.microsoft.com/downloads/details.aspx?FamilyId=860EE43A-A843-462F-ABB5-FF88EA5896F6&displaylang=en) и скопировать его в папку C:\WINDOWS\system32\

В командной строке выполнить команду «regsvr32 capicom.dll».

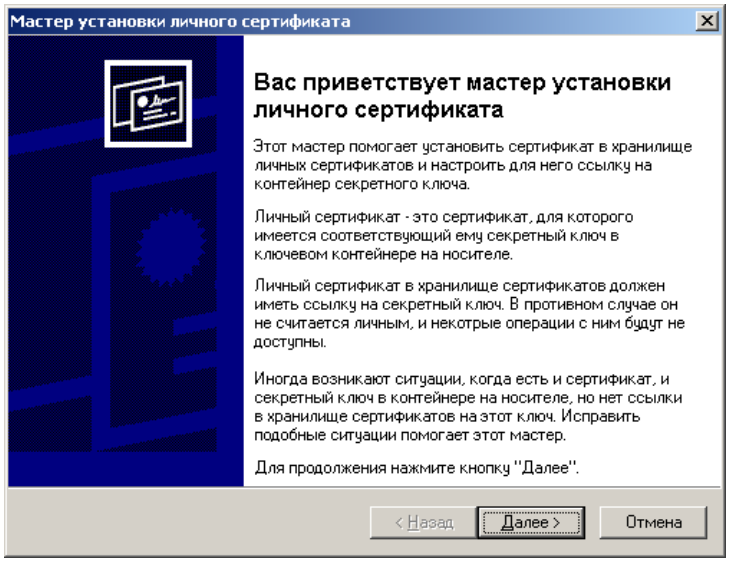
4. Установка личного сертификата пользователя в систему

Вставляем ключ eToken PRO с личным сертификатом пользователя в USB порт.
Открываем панель управления «КриптоПРО CSP».

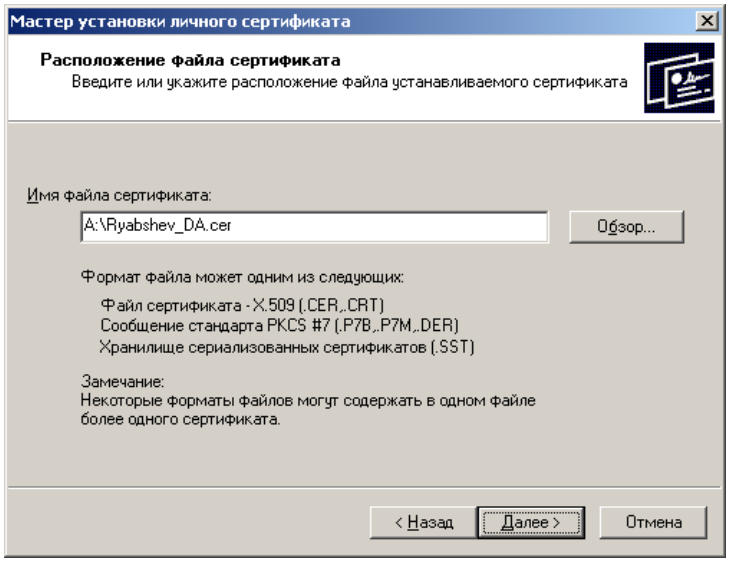
Заходим во вкладку «Сервис»



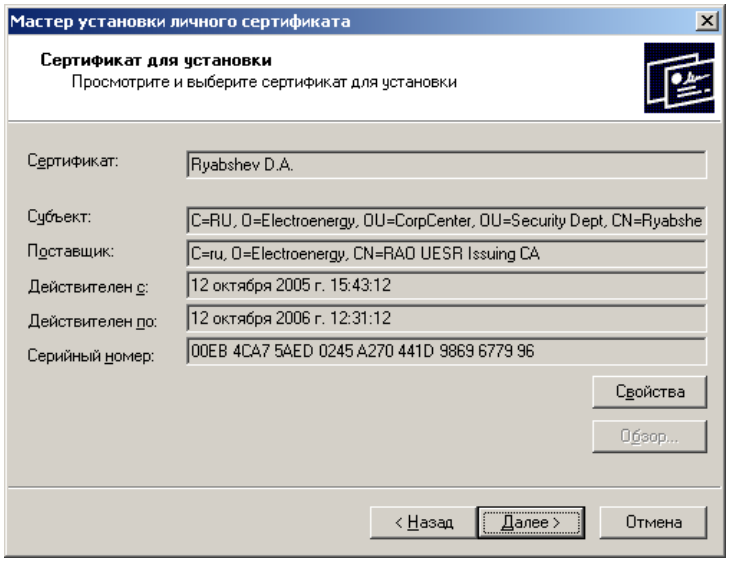
Нажимаем кнопку «Установить личный сертификат…»



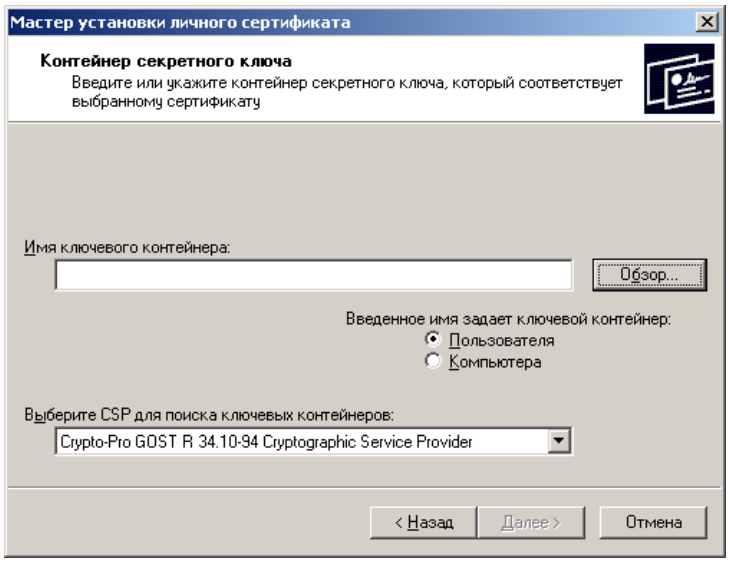
Нажимаем кнопку «Далее»



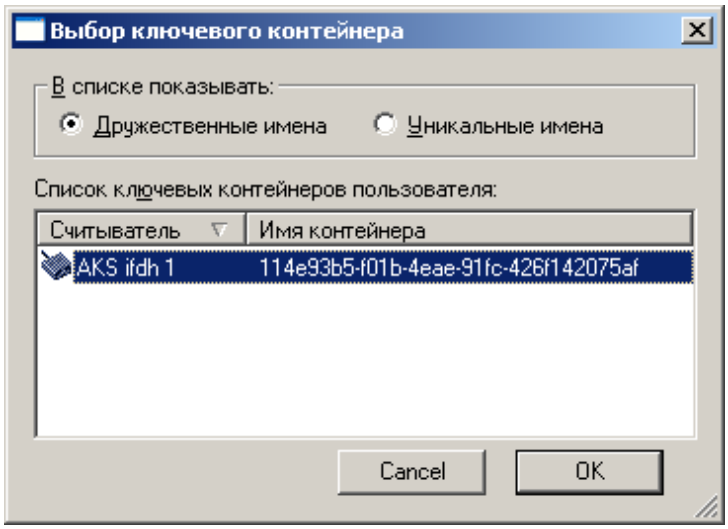
Находим файл личного сертификата, используя кнопку «Обзор…», нажимаем кнопку «Далее»



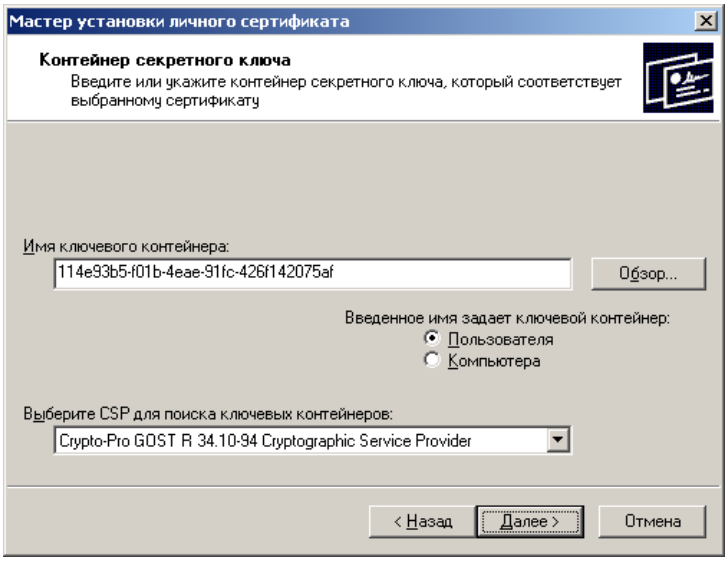
Нажимаем кнопку «Далее»



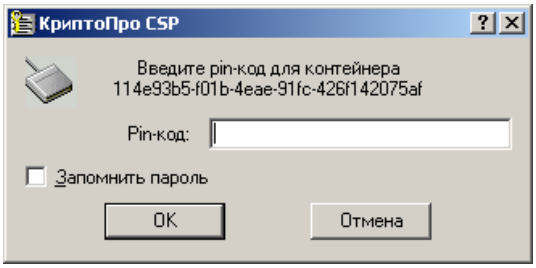
Находим ключевой контейнер, используя кнопку «Обзор…»



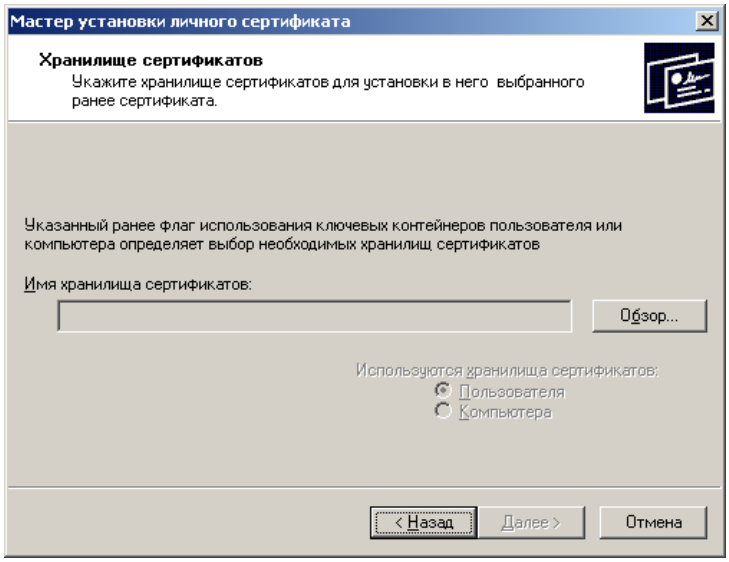
Нажимаем кнопку «ОК»



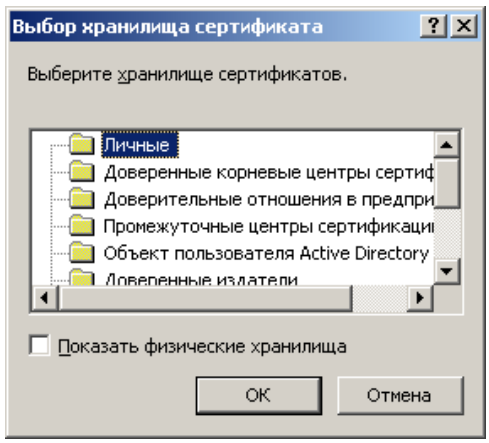
Нажимаем кнопку «Далее»



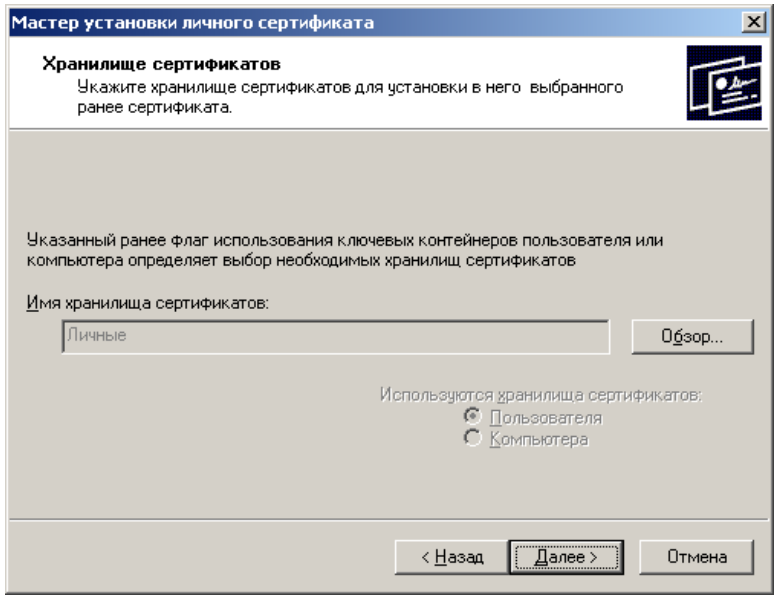
Набираем пин-код ключевого контейнера (по умолчанию – 1234567890)



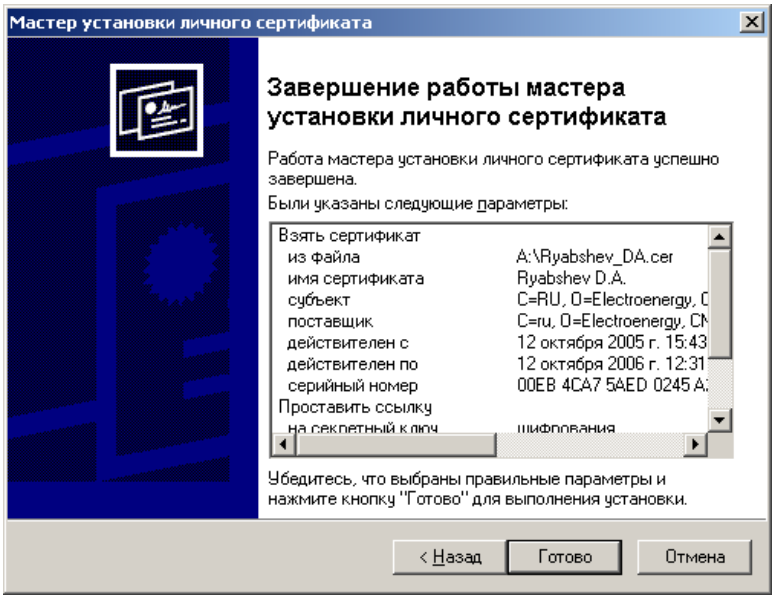
Нажимаем кнопку «Обзор…»



Выбираем папку «Личные», Нажимаем кнопку «ОК»



Нажимаем кнопку «Далее»

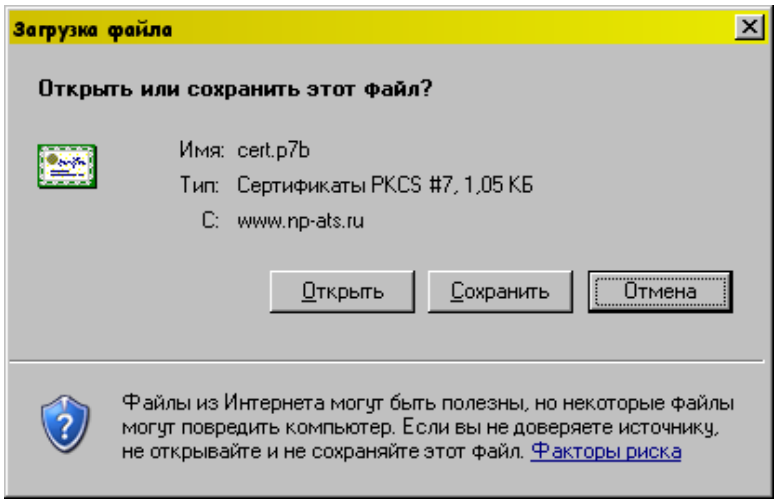


Нажимаем кнопку «Готово»

5. Установка корневых и выпускающих сертификатов Удостоверяющих центров

Корневые сертификата удостоверяющего центра ОАО «АТС» опубликованы на сайте ОАО «АТС» в разделе «Удостоверяющий центр ОАО «АТС» по адресу http://www.atsenergo.ru/. Скачать их можно по ссылке:

http://www.atsenergo.ru/idc/groups/adm_certification/documents/ats_download/ats055555.p7b

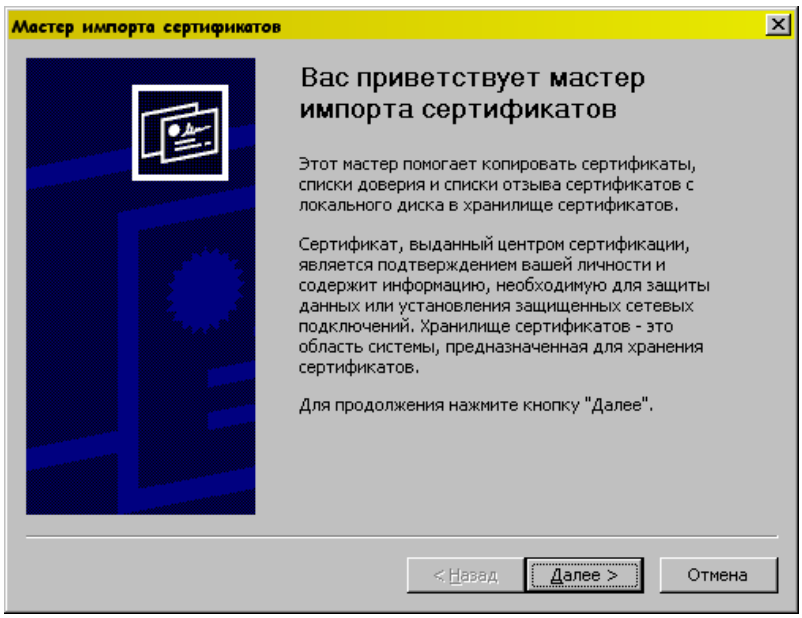


Нажимаем кнопку «Сохранить» и указываем путь для сохранения корневого сертификата.

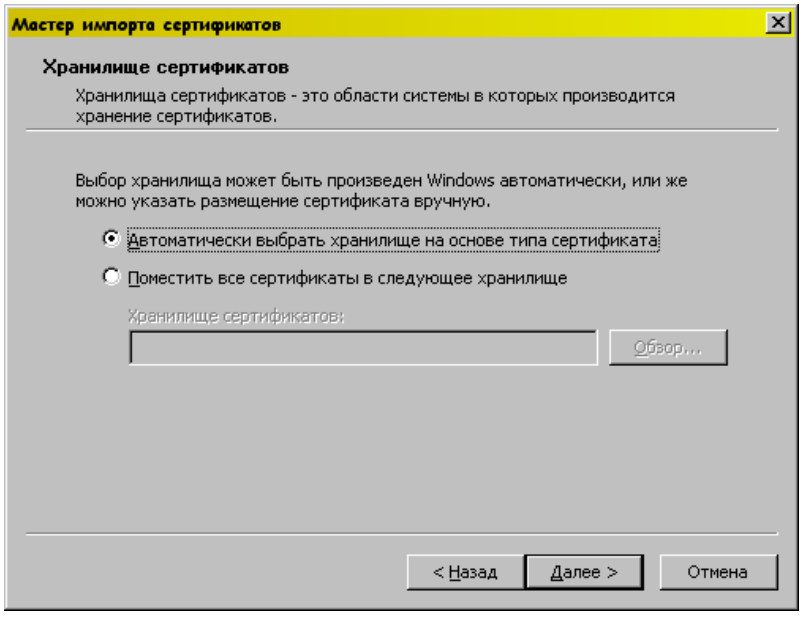
Нажимаем правую кнопку мыши на сохраненном файле

Заходим с раздел «Сертификаты», выбираем сертификат и нажимаем правую к

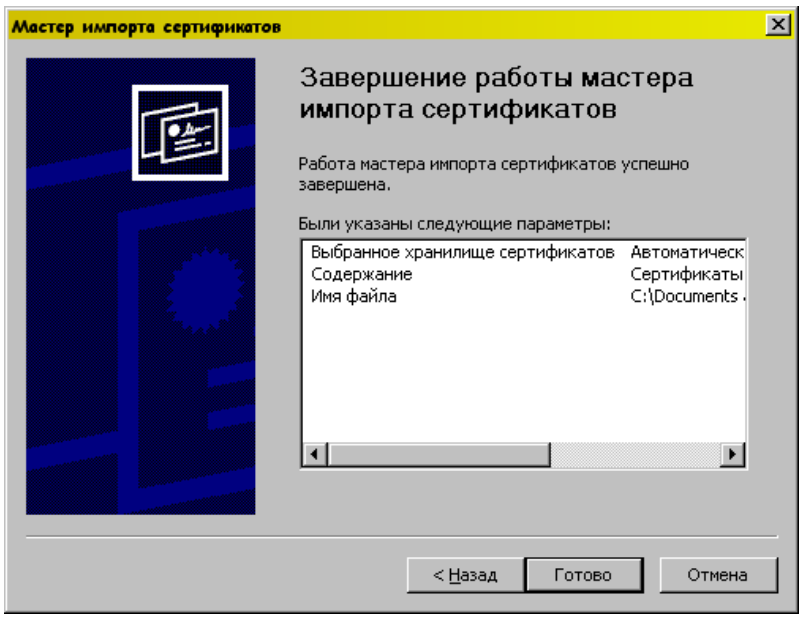
Выбираем «Установить сертификат»



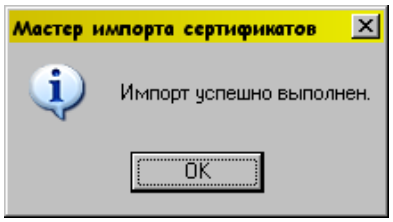
Нажимаем кнопку «Далее»



Нажимаем кнопку «Далее»



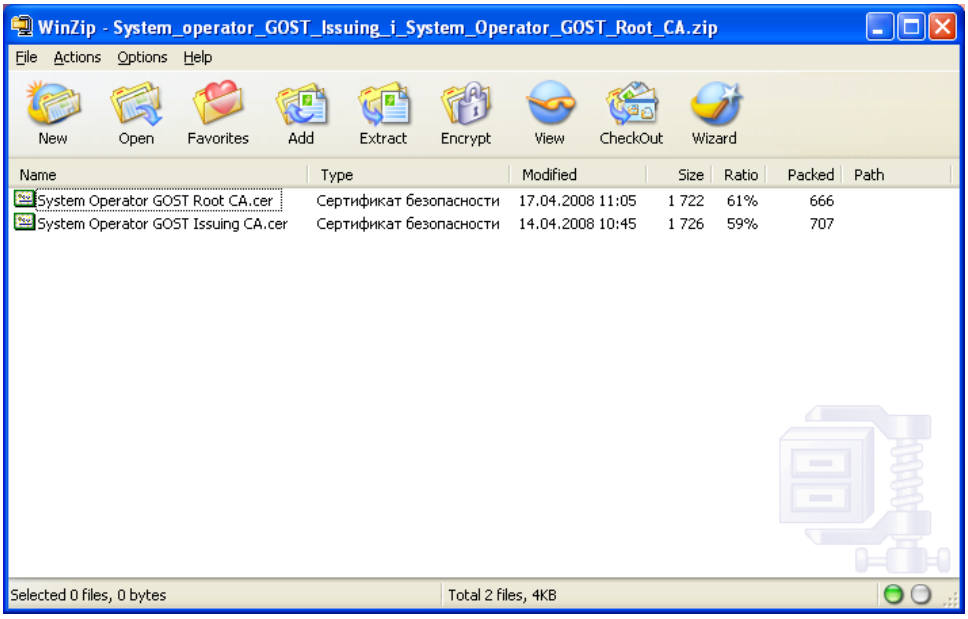
Нажимаем кнопку «Готово»



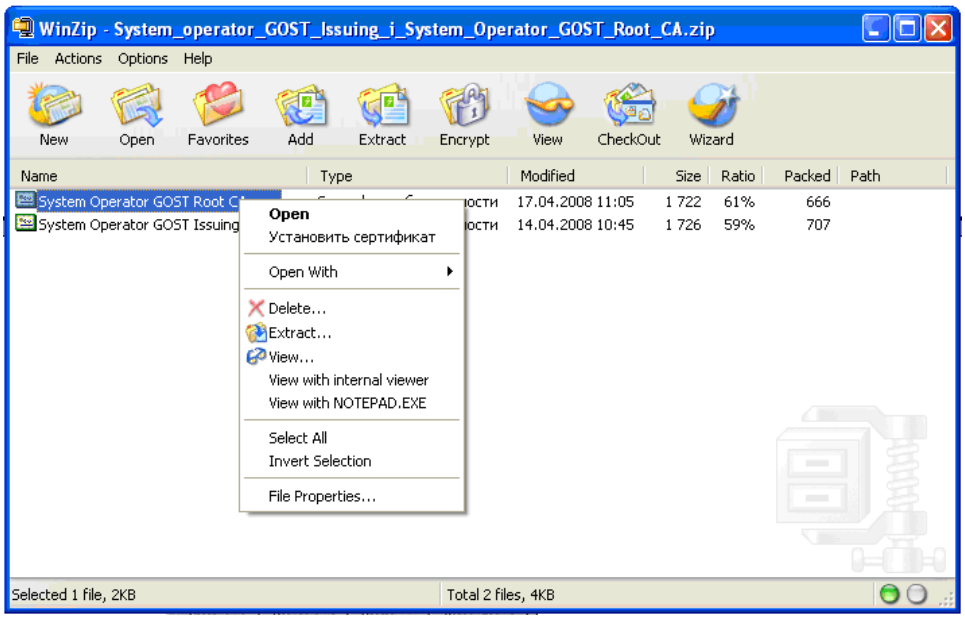
Нажимаем кнопку «ОК»

Корневой и выпускающий сертификаты Удостоверяющего центра ОАО «СО ЕЭС» необходимы для авторизации по логин-паролю и опубликованы на сайте «Балансирующего рынка» по адресу http://br.so-ups.ru/ в разделе «Документы», а также на официальном сайте ОАО «СО ЕЭС» по адресу http://www.so-ups.ru/ в разделе «Контакты и реквизиты » – «Удостоверяющий центр» архив «System Operator RSA Issuing CA и System Operator RSA Root CA».

Сохранить корневой и выпускающий сертификаты Удостоверяющего центра ОАО «СО ЕЭС», открыть архив:



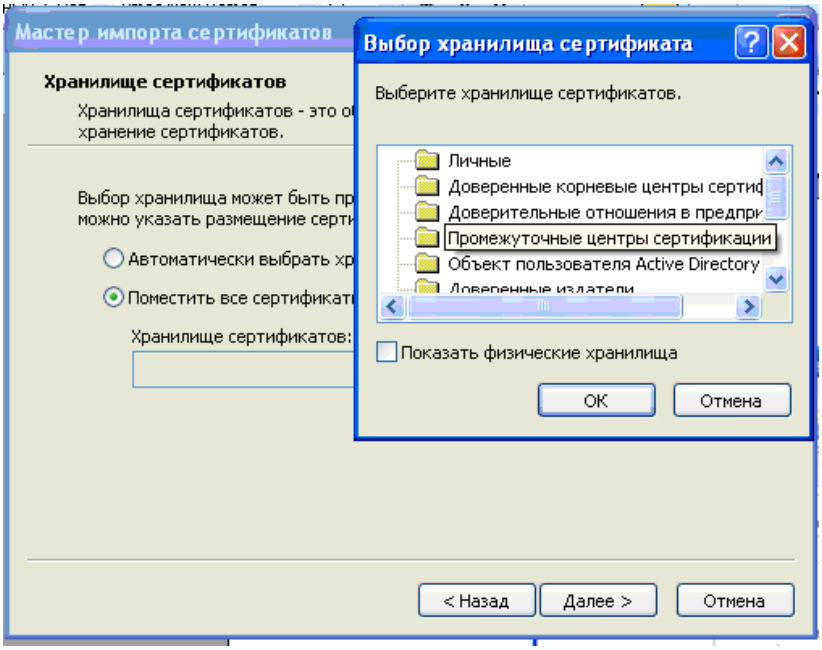
Нажать правую кнопку мыши на System Operator RSA Root CA.cer и выбрать «Установить сертификат»:



Нажать кнопку «Далее» и выполнить действия, аналогичные с описанными ранее для сертификатов Удостоверяющего центра ОАО «АТС».

Далее нажать правую кнопку мыши на System Operator RSA Issuing CA.cer и выбрать «Установить сертификат».

Данный сертификат при установке необходимо поместить в «Промежуточные центры сертификации».

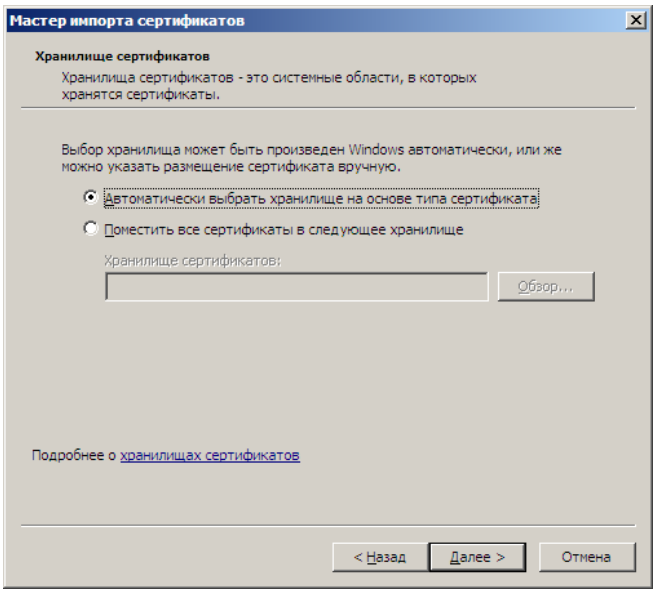


Нажать кнопку «Далее» и кнопку «Готово».

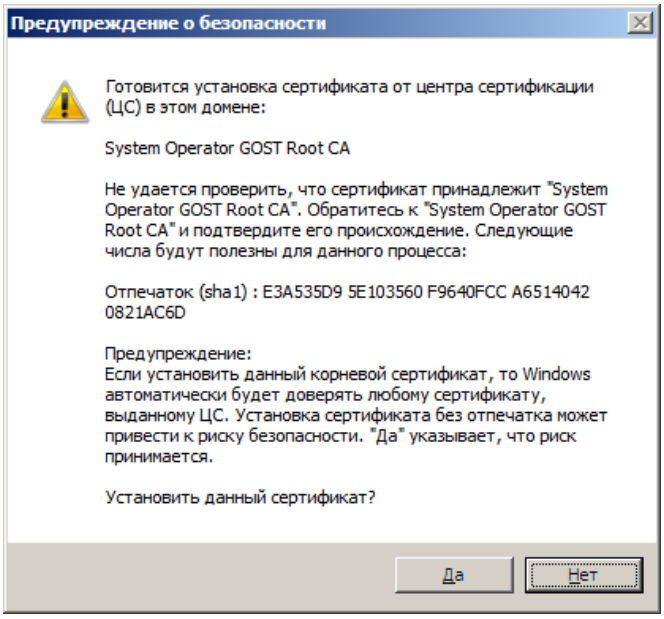
Некоторые нюансы установки сертификатов в Windows 7, которых не было в Windows XP.

Установка корневых сертификатов.

При установке корневого сертификата, если оставить автоматический выбор хранилища,



то в WinXP выдавался запрос



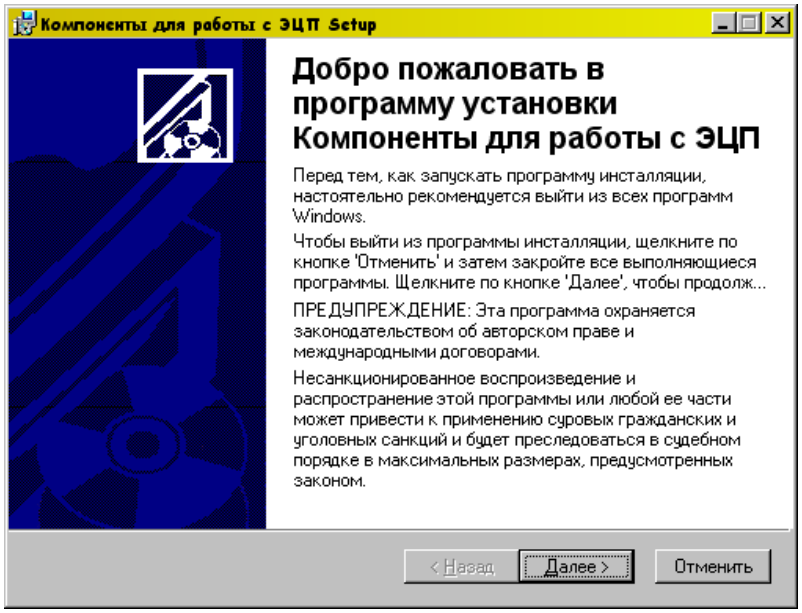
и корневой сертификат устанавливался в хранилище в «Доверенные корневые центры сертификации».

В Windows 7 запрос не выдается и по умолчанию корневой сертификат помещается в «Промежуточные центры сертификации» и, как следствие, получаем отсутствие доверия к сертификатам, поэтому необходимо указывать конкретное хранилище «Доверенные корневые сертификаты».

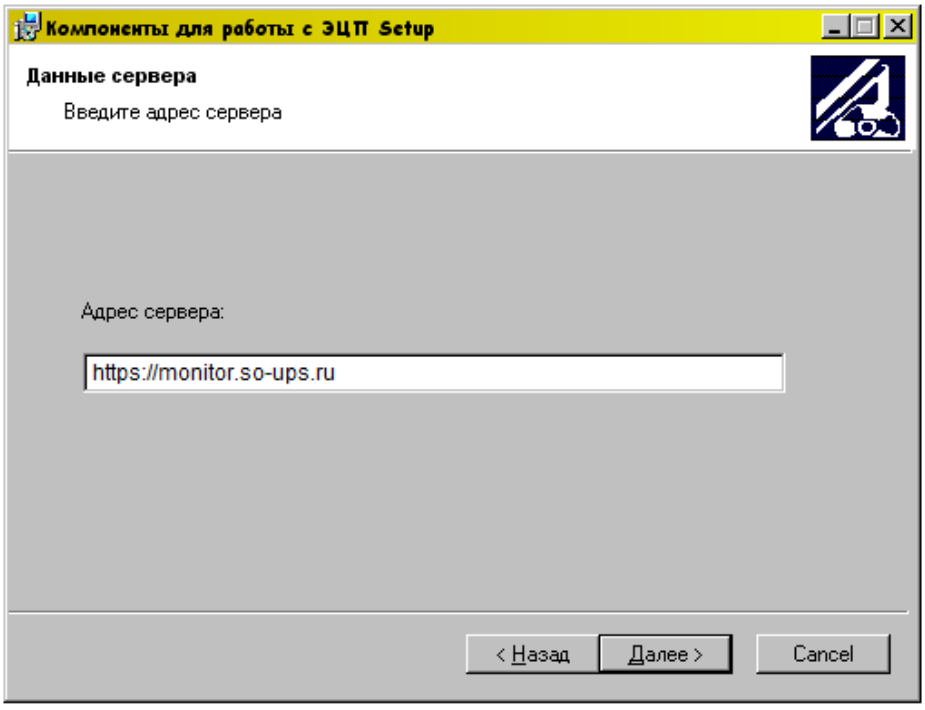
6. Настройка браузера IE 6.0 и выше

6.1 Устанавливаем «Компоненты для работы с ЭЦП»:

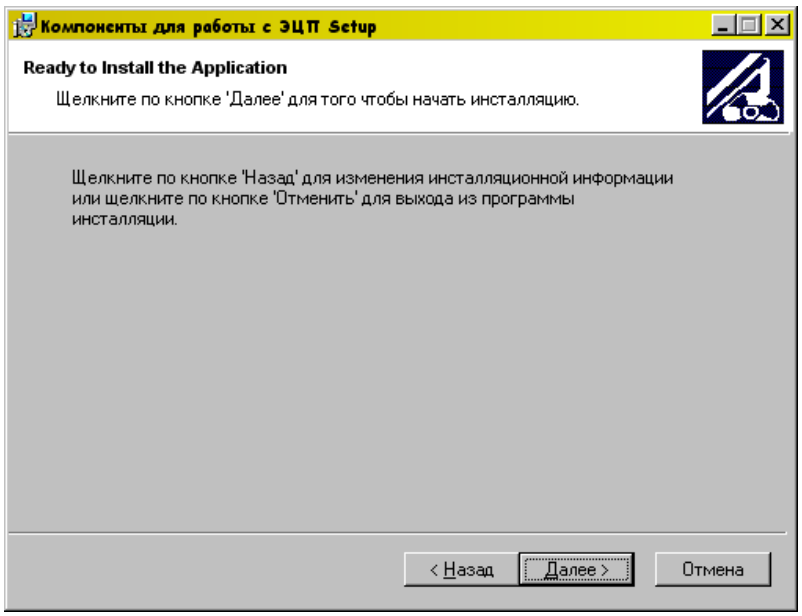
Запускаем утилиту для настройки браузера IE 6.0 и выше - setup.bat



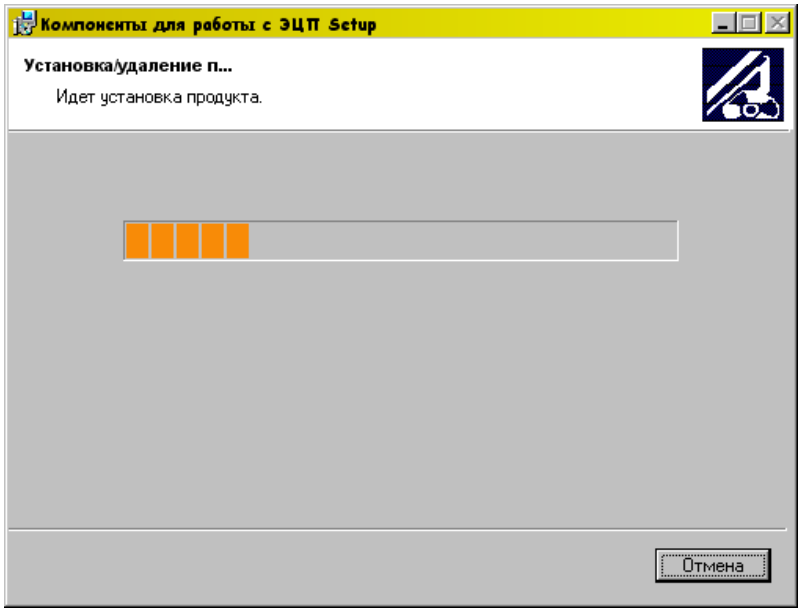
Нажимаем «Далее»

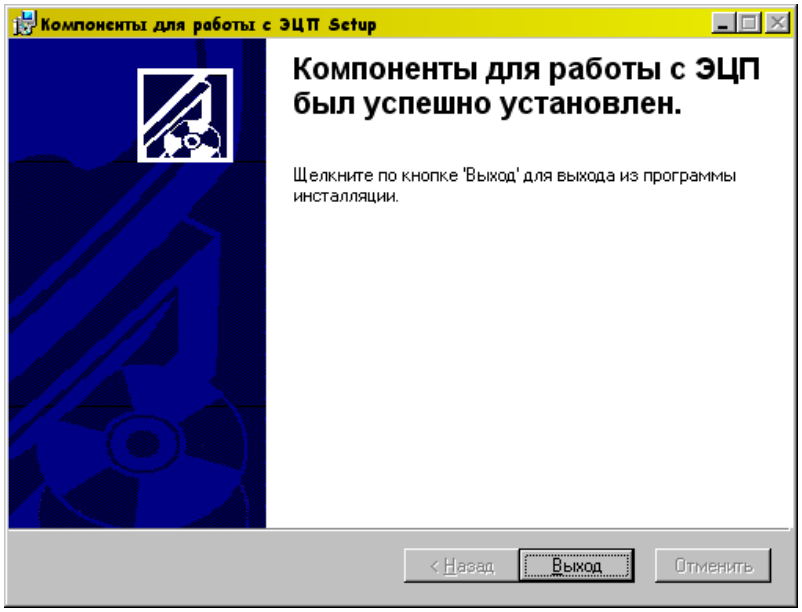


В поле «Адрес сервера» вводим адрес сайта балансирующего рынка по защищенному соединению https://monitor.so-ups.ru/



Нажимаем «Далее»

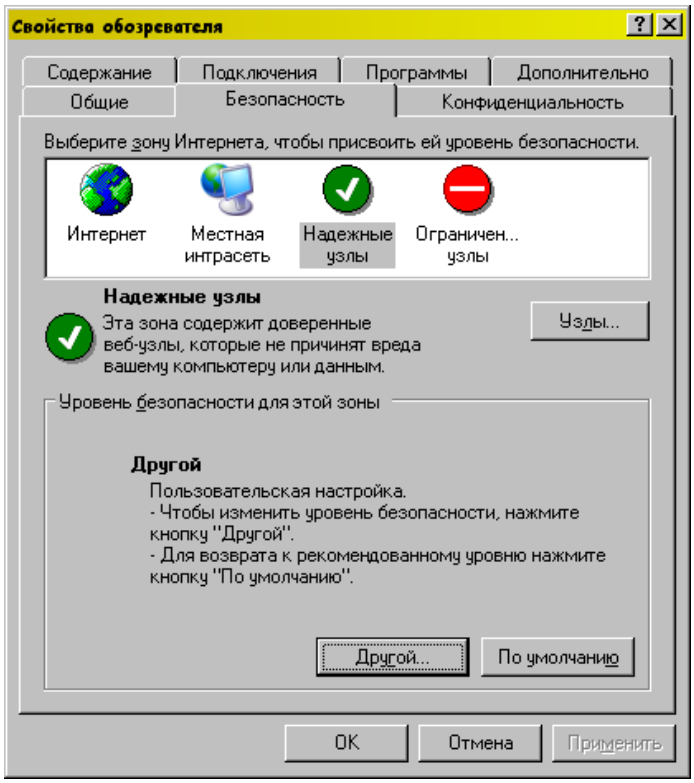




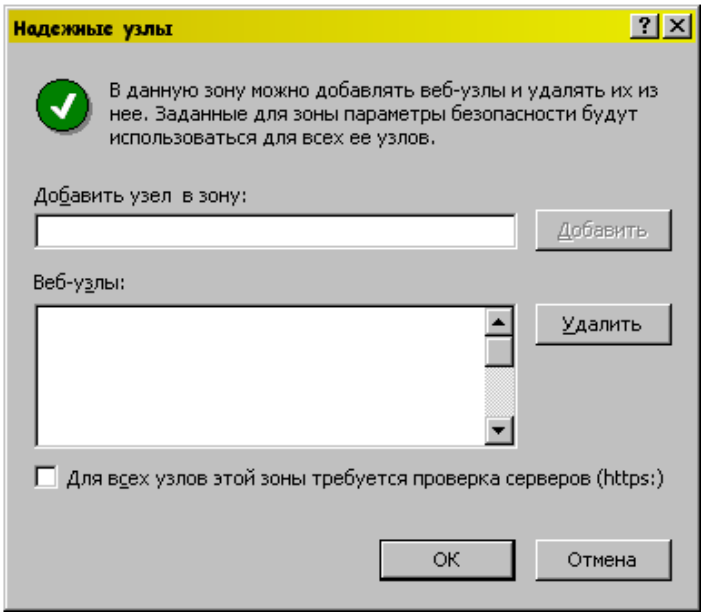
Нажимаем «Выход».

6.2 Проверка наличия защищенного адреса сайта балансирующего рынка в «надежных узлах» браузера и разрешения использования элементов ActiveX, не помеченных как безопасные

Запускаем браузер IE 6.0 или выше, нажимаем меню «Сервис» - «Свойства обозревателя», закладка «Безопасность».



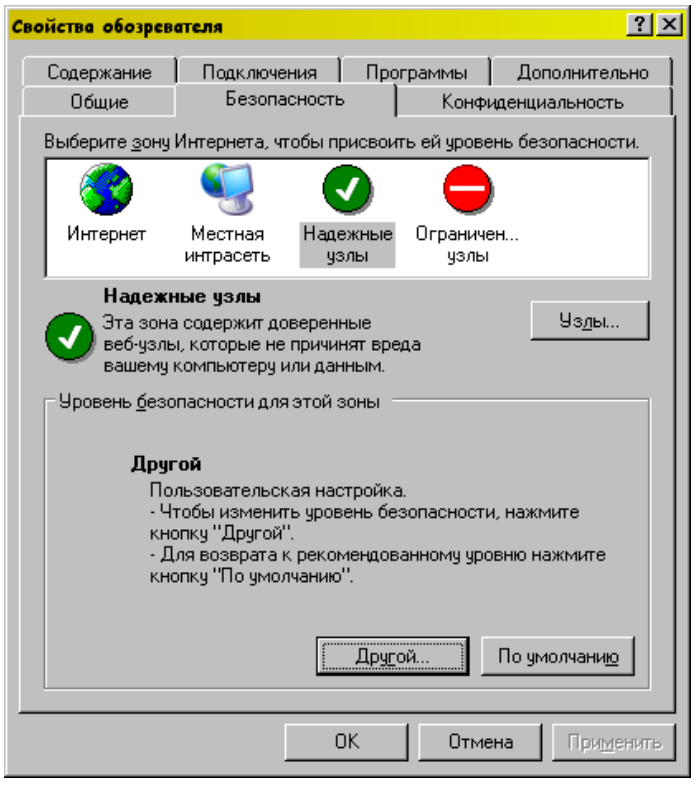
Выбираем «Надежные узлы» и нажимаем кнопку «Узлы».



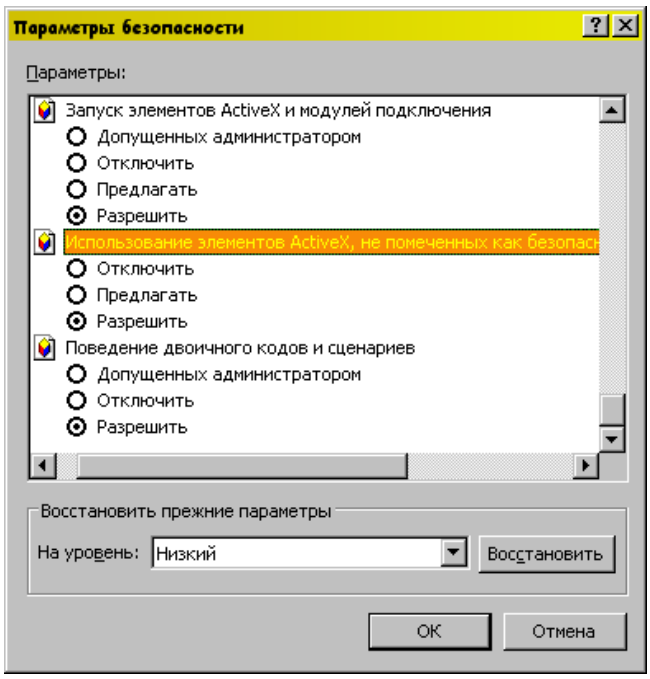
Проверяем наличие адреса https://monitor.so-ups.ru

При его отсутствии добавляем адрес https://monitor.so-ups.ru в надежные узлы.

Нажимаем «ОК».



Нажимаем кнопку «Другой…»



Проверяем, что для «Использование элементов ActiveX, не помеченных как безопасные» установлено «Разрешить»