

Установка КОМПОНЕНТОВ,
необходимых для работы с
электронной подписью на
электронных торговых площадках
В2В

Оглавление

Установка СКЗИ КриптоПро CSP.....	3
Установка драйвера ключевого носителя РУТОКЕН	7
Установка ПО для ESMART Token.....	9
Установка драйвера ESMART Token.....	9
Установка ПО ESMART PKI Client для Windows	12
Установка ПО модуля поддержки КриптоПро CSP для Windows.....	15
Установка сертификата ключа подписи	19
Установка корневого сертификата.....	25
Установка библиотеки CAPICOM	29
Проверка работы электронной подписи на площадке В2В	33

Все программы и компоненты можно скачать по ссылке:

<http://www.esphere.ru/support/download/uc/>

либо на сайте площадки B2B в разделе ЭЦП. <http://www.b2b-energo.ru/signature/more-for-clients.html>

Установка СКЗИ КристоПро CSP

В соответствии с вашей операционной системой скачайте дистрибутив по ссылке

<http://www.esphere.ru/support/download/uc/> из раздела: Дистрибутивы для КристоПро CSP для Windows

1. Запустите установочный файл, который скачали;
2. В появившемся окне программы установки «КристоПРО CSP (в зависимости от версии окно выглядит по разному)» нажмите кнопку «Далее»;

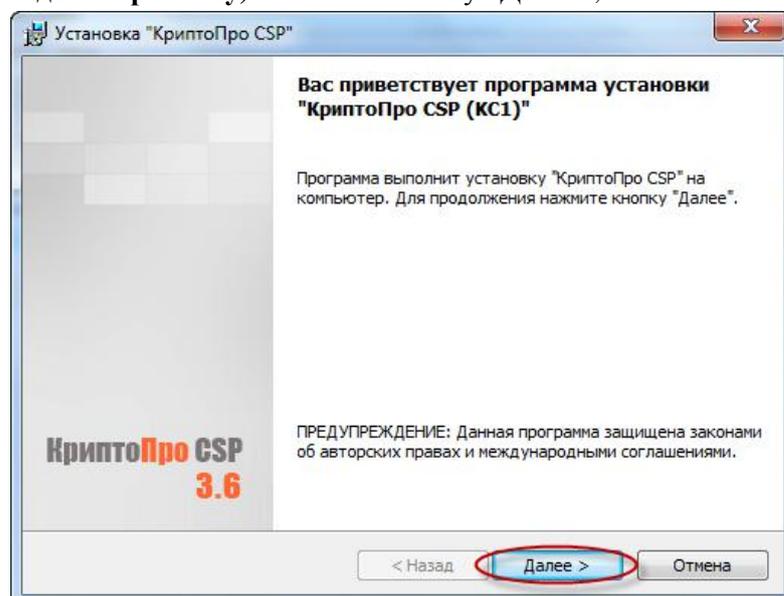


Рисунок 1. КристоПро CSP. Приветствие

3. Ознакомьтесь с текстом лицензионного соглашения, поставьте галочку «Я принимаю условия лицензионного соглашения» и нажмите кнопку «Далее»;

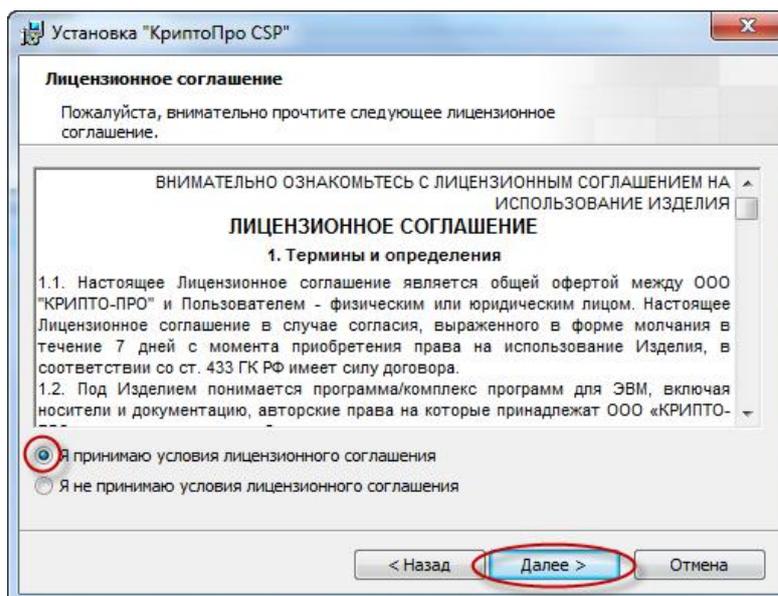


Рисунок 2. КриптоПро CSP. Лицензионное соглашение

4. В окне «Сведения о пользователе» введите имя, название организации, а также серийный номер, указанный в документе «Лицензия на использование программного продукта КриптоПро CSP» и нажмите кнопку «Далее»;

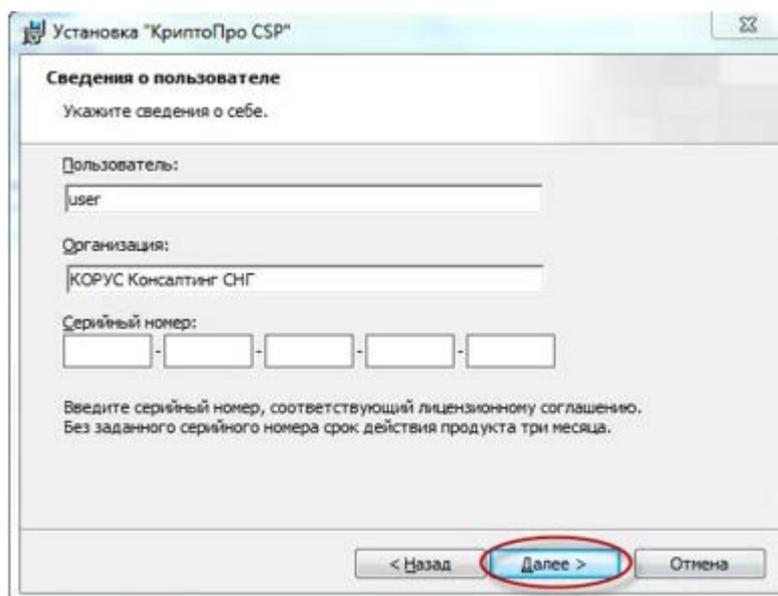


Рисунок 3. КриптоПро CSP. Сведения о пользователе

5. В следующем окне выберите обычный вид установки и нажмите кнопку «Далее».

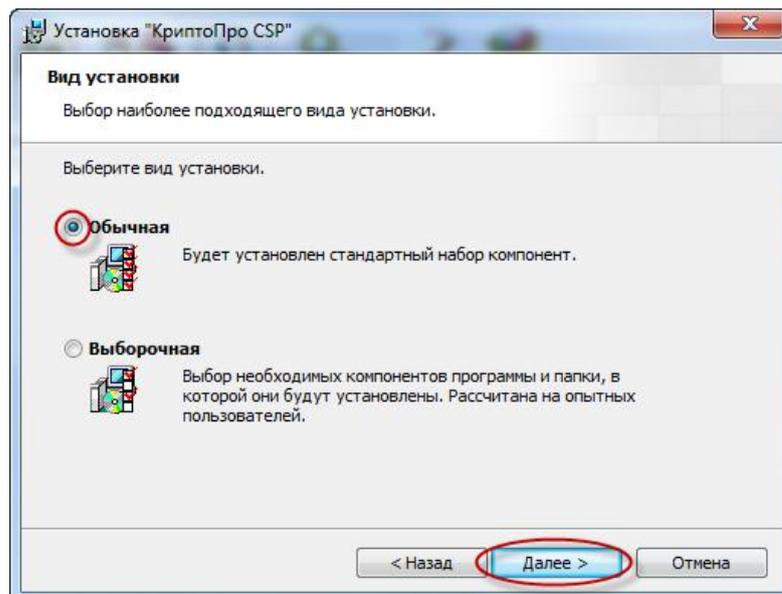


Рисунок 4. КриптоПро CSP. Вид установки

6. Укажите виды считывателей, которые необходимо зарегистрировать в «КриптоПро CSP». По умолчанию «Зарегистрировать считыватель смарт-карт» и «Зарегистрировать считыватель съемных носителей». Нажмите кнопку «Установить»;

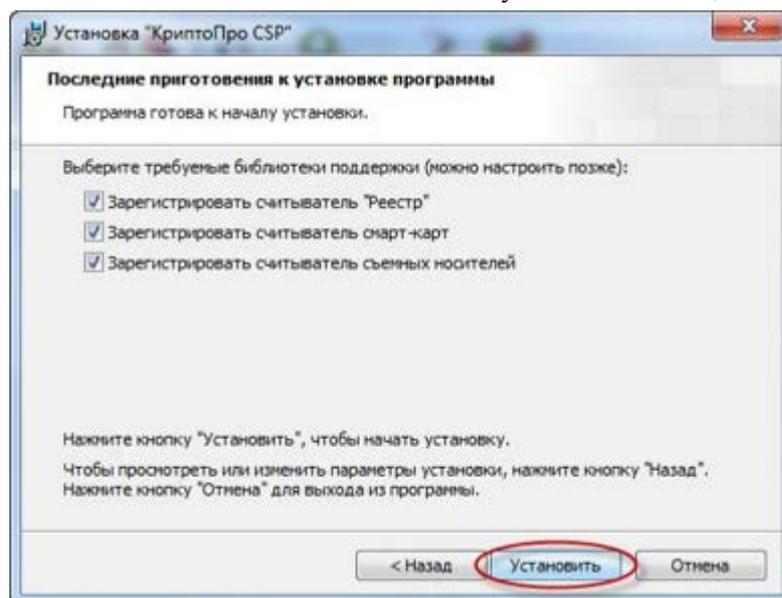


Рисунок 5. КриптоПро CSP. Последние приготовления к установке программы

7. По окончании установки нажмите кнопку «Готово».

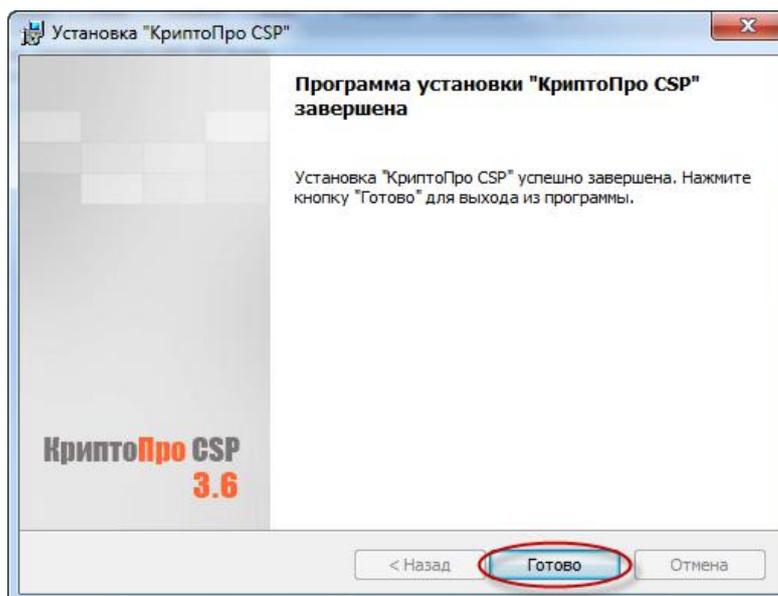


Рисунок 6. КриптоПро CSP. Завершение установки

8. Для завершения процесса установки программы необходимо перезагрузить компьютер. При появлении окна «Сведения о программе установки КриптоПро CSP» с предложением перезагрузки, следует нажать кнопку «Да»:

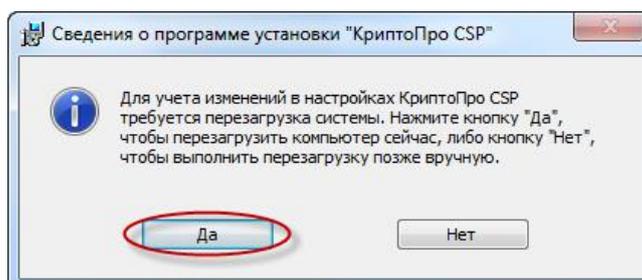


Рисунок 7. КриптоПро CSP. Перезагрузка системы

Установка драйвера ключевого носителя РУТОКЕН

Драйвер ключевого носителя Рутокен можно скачать по ссылке

<http://www.esphere.ru/support/download/uc/> в разделе [Дистрибутивы для РУТОКЕН](#)

Обратите внимание, что при установке драйвера ключевой носитель Рутокен **не должен** быть вставлен в USB-порт компьютера.

1. Запустите установочный файл драйвера
2. В открывшемся окне установки нажмите кнопку «Далее»;

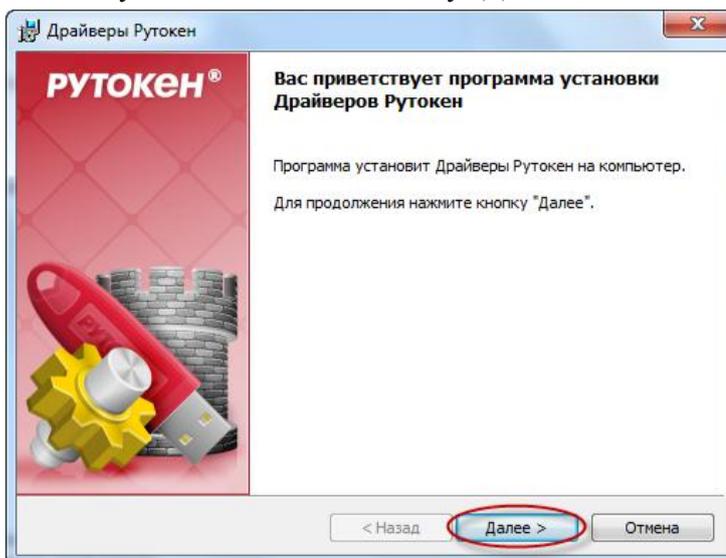


Рисунок 8. Драйвер Рутокен. Начало установки

3. Для запуска установки драйвера Рутокен нажмите «Установить»;

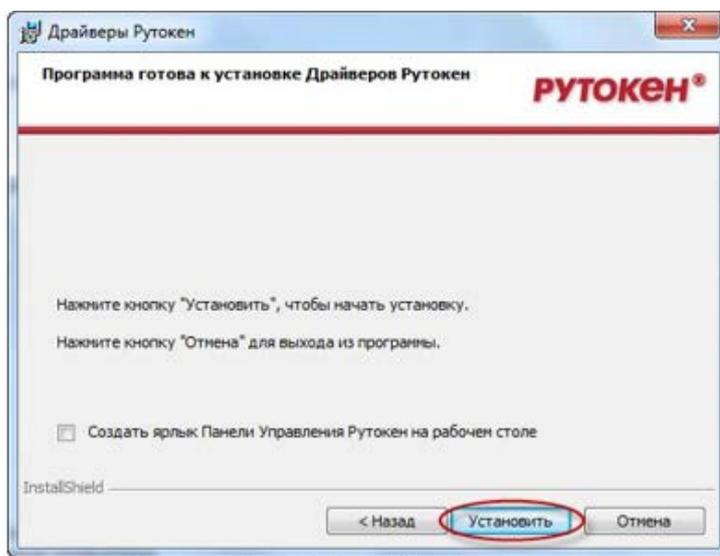


Рисунок 9. Драйвер Рутокен. Запуск установки

4. Для завершения установки драйвера нажмите кнопку «Готово».

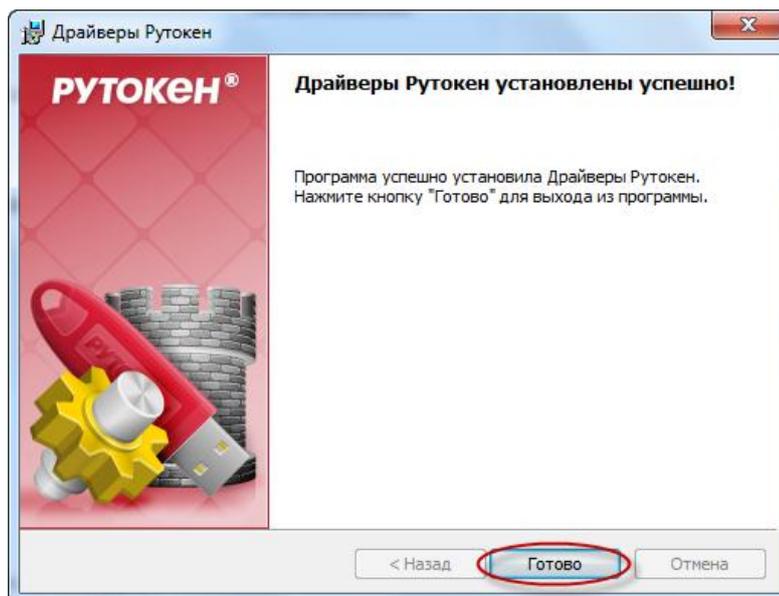


Рисунок 10. Драйвер Рутокен. Завершение установки.

Установка ПО для ESMART Token

Установка драйвера ESMART Token

Драйвер ESMART Token можно скачать по ссылке <http://www.esphere.ru/support/download/uc/> из раздела <http://www.esmart.ru/download/> или с сайта (<http://www.esmart.ru/download/>).

Дистрибутивы для ESMART Token

Системные требования драйверов ключевого ESMART Token представлены в таблице 1.

Таблица 1.

Операционная система	Драйверы ESMART Token
Windows Server 2012 R2	+
Windows 8.1	+
Windows Server 2012	+
Windows 8	+
Windows Server 2008 R2	+
Windows 7	+
Windows Server 2008	+
Windows Vista	+
Windows Server 2003 R2	+
Windows Server 2003	+
Windows XP	+

Для установки драйвера ESMART Token необходимо выполнить следующие действия:

1. Запустить ПО драйвера ESMART Token. В появившемся окне нажать кнопку «ОК»

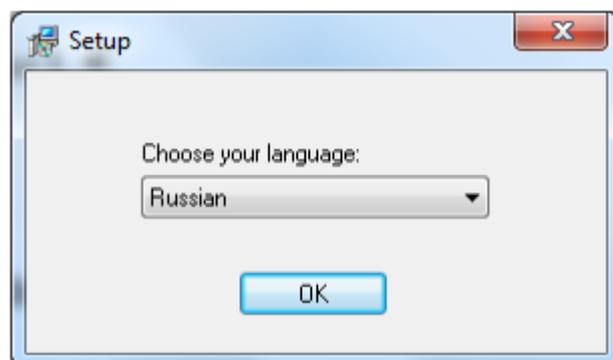


Рисунок 11. Драйвер ESMART Token. Начало установки

2. В окне нажать кнопку «Далее».

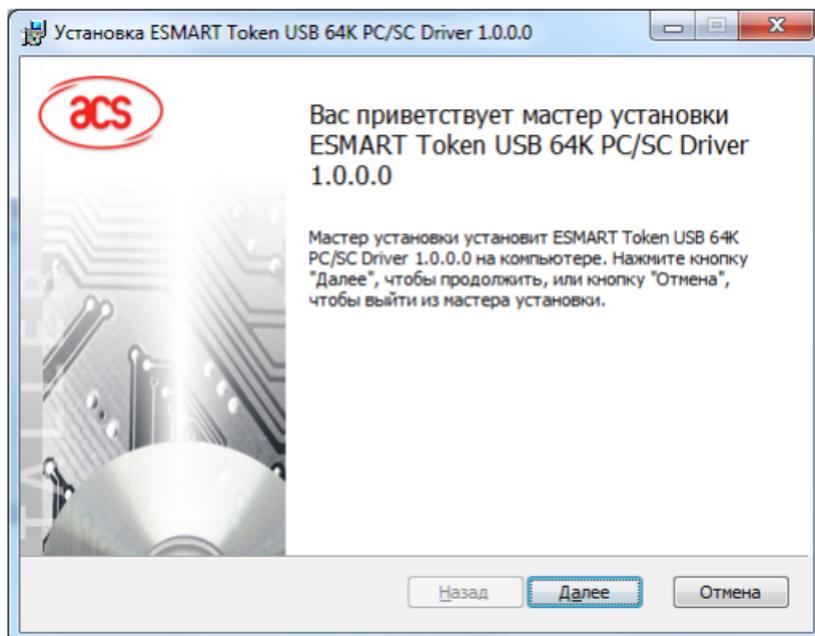


Рисунок 12. Мастер установки ESMART Token

3. В окне нажать кнопку «Далее».

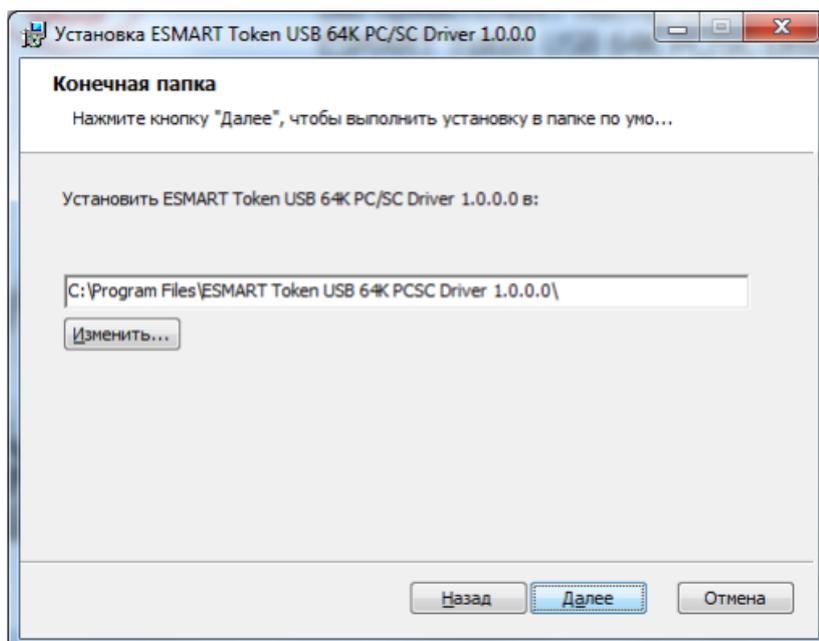


Рисунок 13. Установка ESMART Token

4. В окне нажать кнопку «Установить».

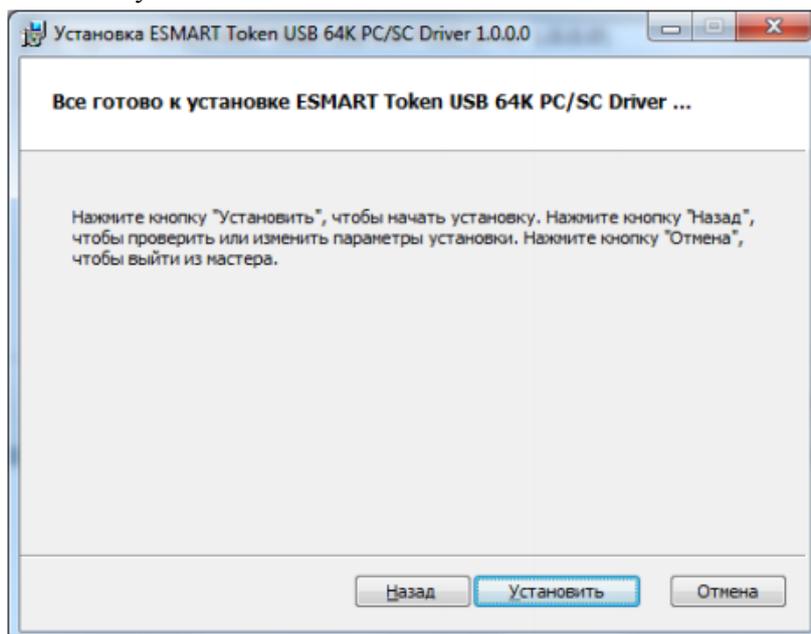


Рисунок 14. Установка ESMART Token

5. В окне нажать кнопку «Готово».

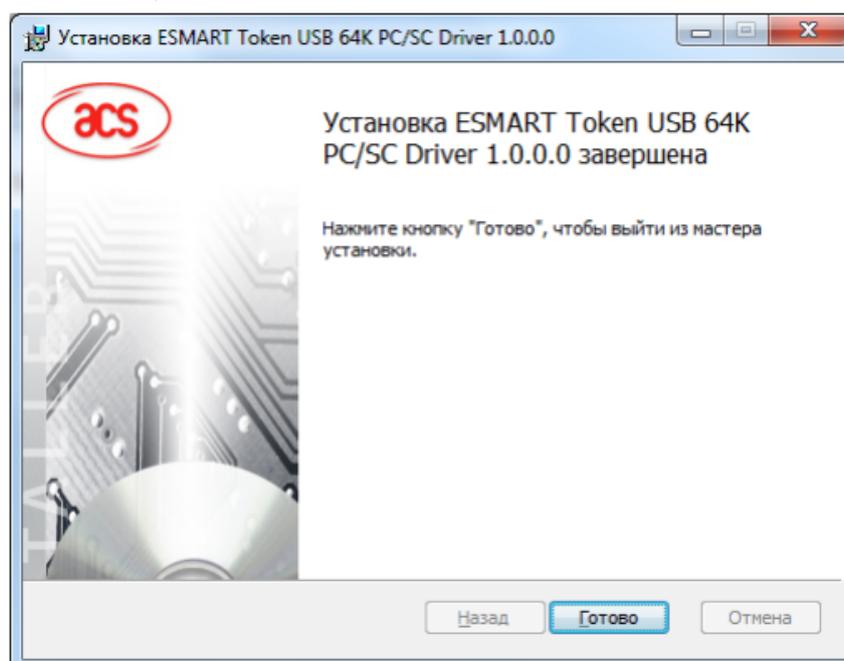


Рисунок 15. Завершение установки ESMART Token

Установка ПО ESMART PKI Client для Windows

Драйвер ESMART Token можно скачать по ссылке <http://www.esphere.ru/support/download/uc/> из раздела [Дистрибутивы для ESMART Token](#) или с сайта (<http://www.esmart.ru/download/>).

Системные требования к ПО ESMART PKI Client для Windows представлены в таблице 2. Таблица 2.

Операционная система	ПО ESMART PKI Client для Windows
Windows Server 2012 R2	+
Windows 8.1	+
Windows Server 2012	+
Windows 8	+
Windows Server 2008 R2	+
Windows 7	+
Windows Server 2008	+
Windows Vista	+
Windows Server 2003 R2	+
Windows Server 2003	+
Windows XP	+

Для установки ПО ESMART PKI Client для Windows необходимо выполнить следующие действия:

1. Запустить ПО ESMART PKI Client для Windows. В появившемся окне нажать кнопку «Далее».

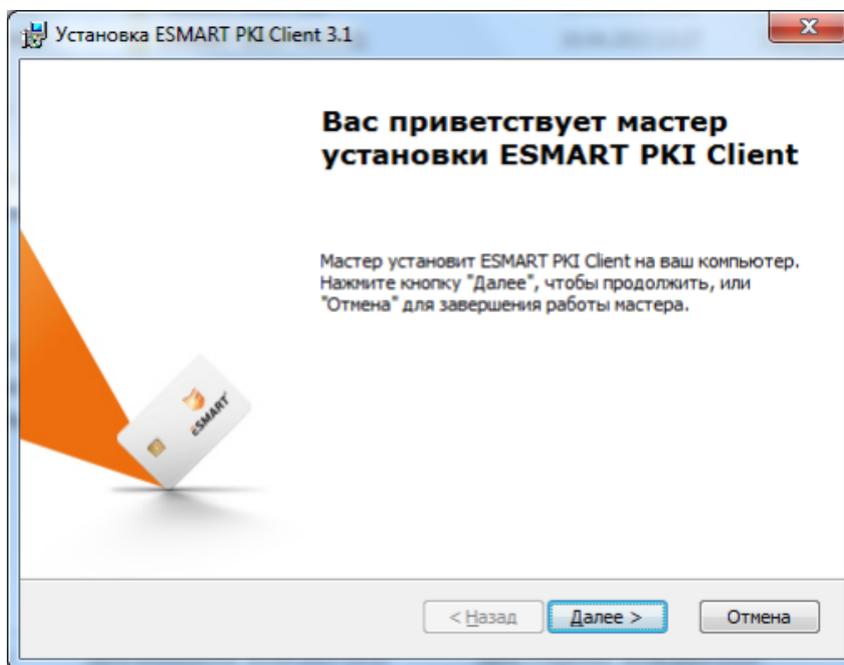


Рисунок 16. Начало установки ESMART PKI Client

2. В окне нажать кнопку «Далее».

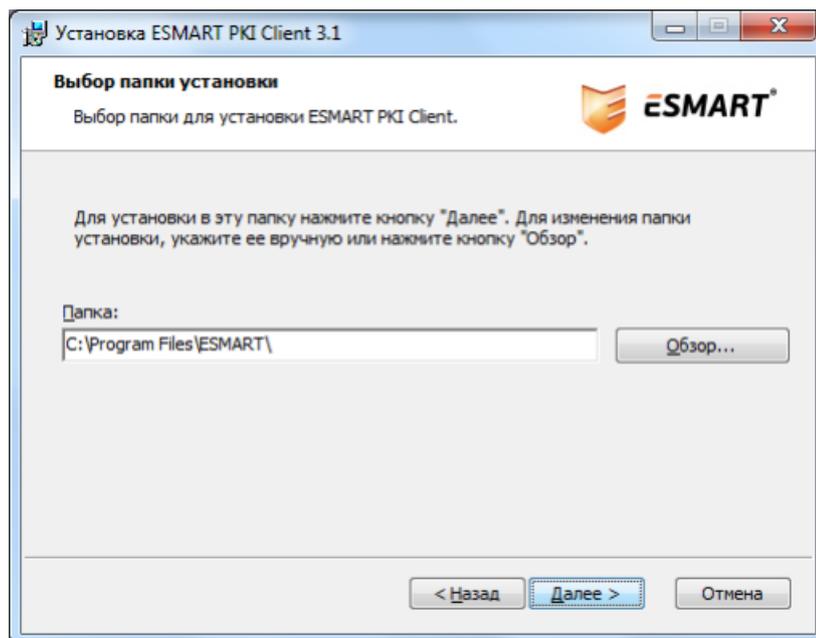


Рисунок 17. Выбор папки установки ESMART PKI Client

3. В окне нажать кнопку «Установить».

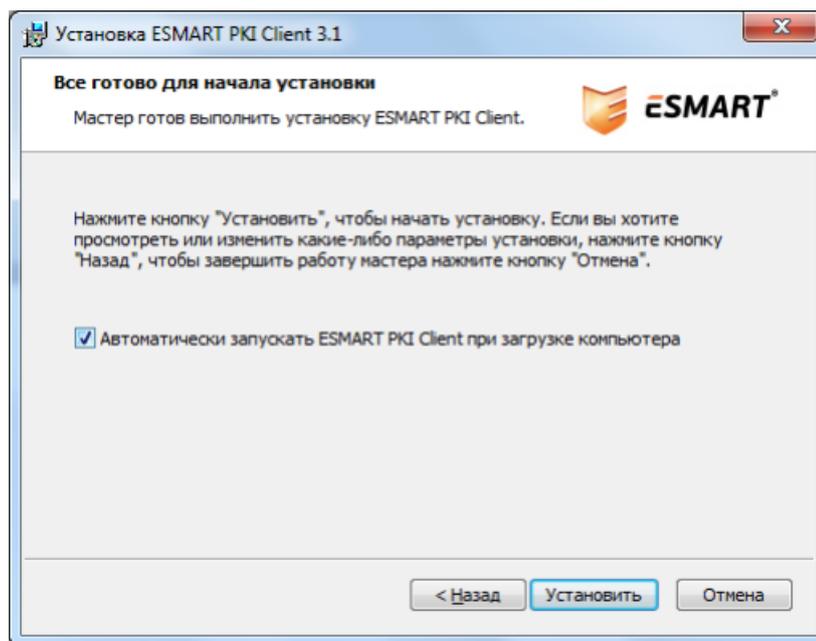


Рисунок 18. Установка ESMART PKI Client

4. В окне нажать кнопку «Установить».

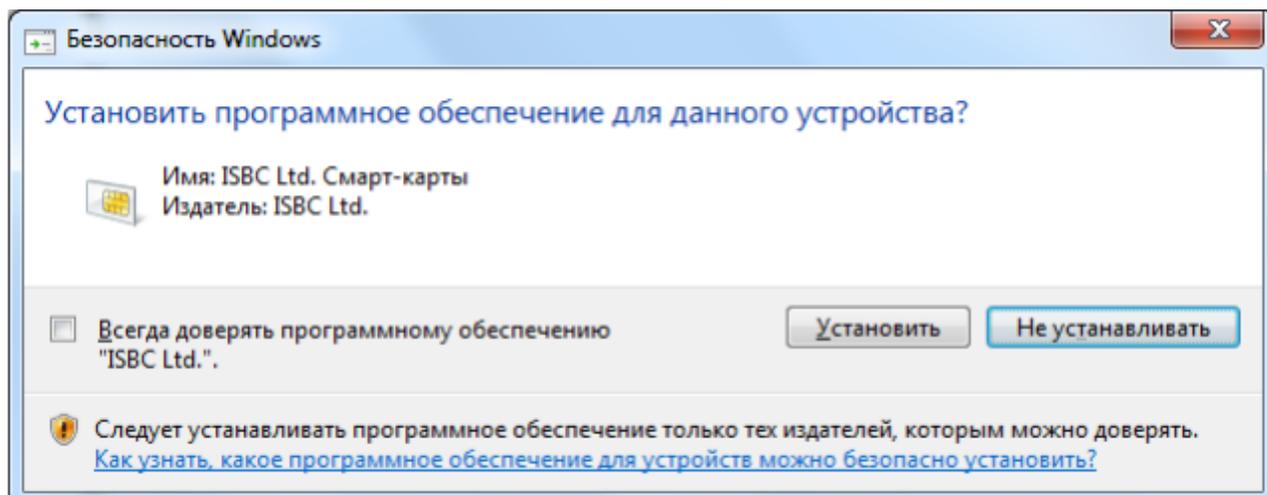


Рисунок 19. Установка ESMART PKI Client

5. В окне нажать кнопку «Готово»

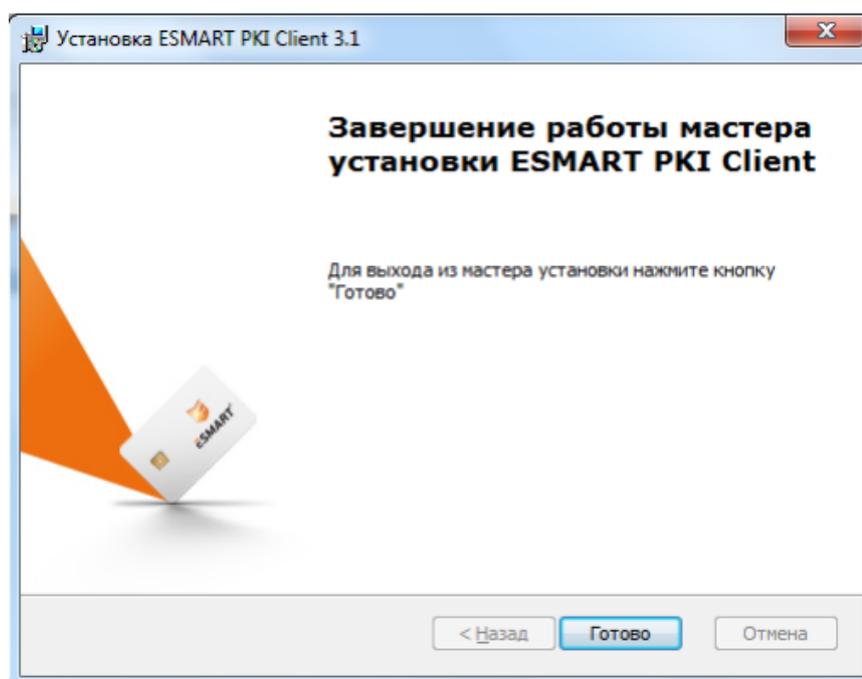


Рисунок 20. Завершение установки ESMART PKI Client

Установка ПО модуля поддержки КриптоПро CSP для Windows

Драйвер ESMART Token можно скачать по ссылке <http://www.esphere.ru/support/download/uc/> из раздела или с сайта (<http://www.esmart.ru/download/>).

Дистрибутивы для ESMART Token

Для установки ПО модуля поддержки КриптоПро CSP для Windows необходимо выполнить следующие действия:

1. Запустить ПО модуля поддержки КриптоПро CSP для Windows. В появившемся окне нажать кнопку «ОК».

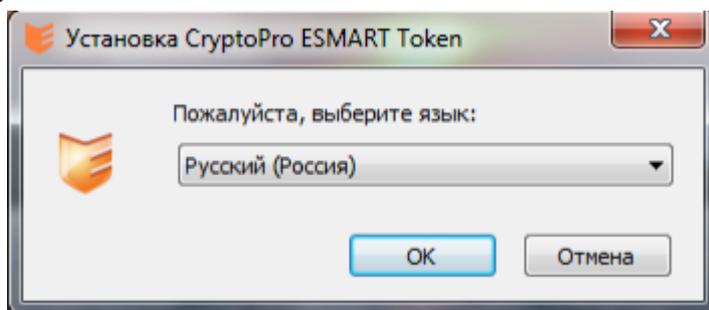


Рисунок 21. Начало установки модуля поддержки КриптоПро CSP для Windows

2. В окне нажать кнопку «Далее».

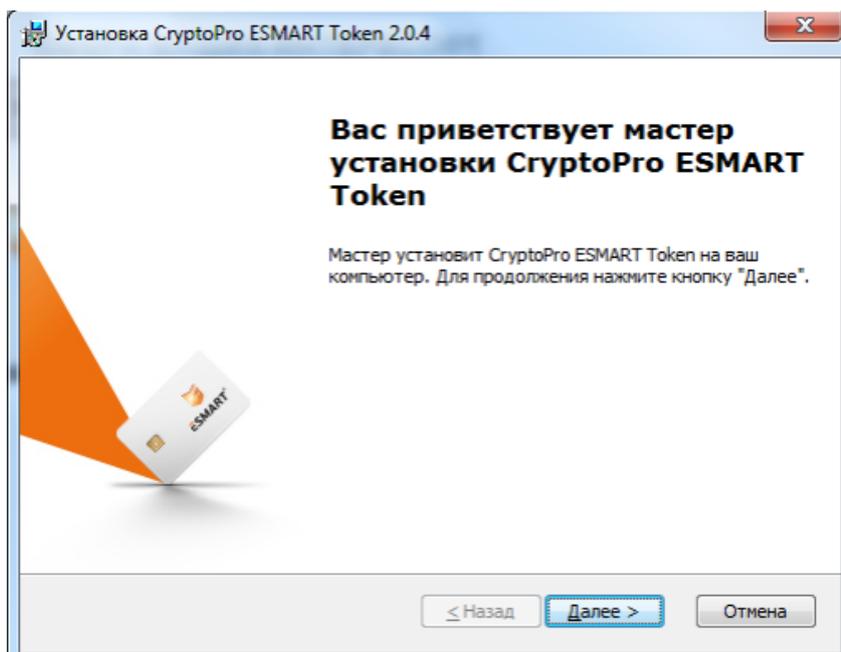


Рисунок 22. Начало установки модуля поддержки КриптоПро CSP для Windows

3. В окне нажать кнопку «Далее».

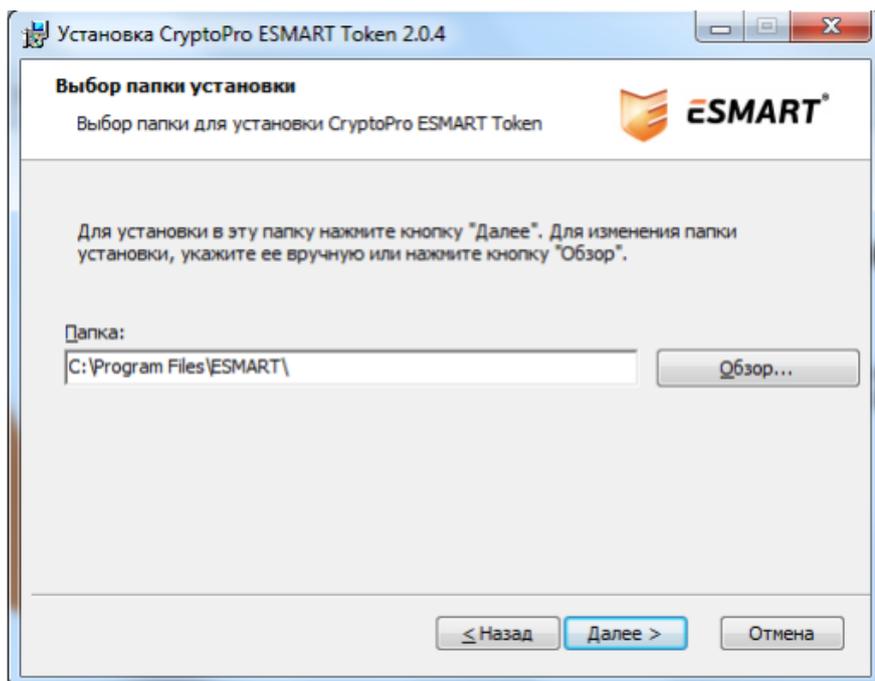


Рисунок 23. Выбор папки установки модуля поддержки КриптоПро CSP для Windows

4. В окне нажать кнопку «Далее»

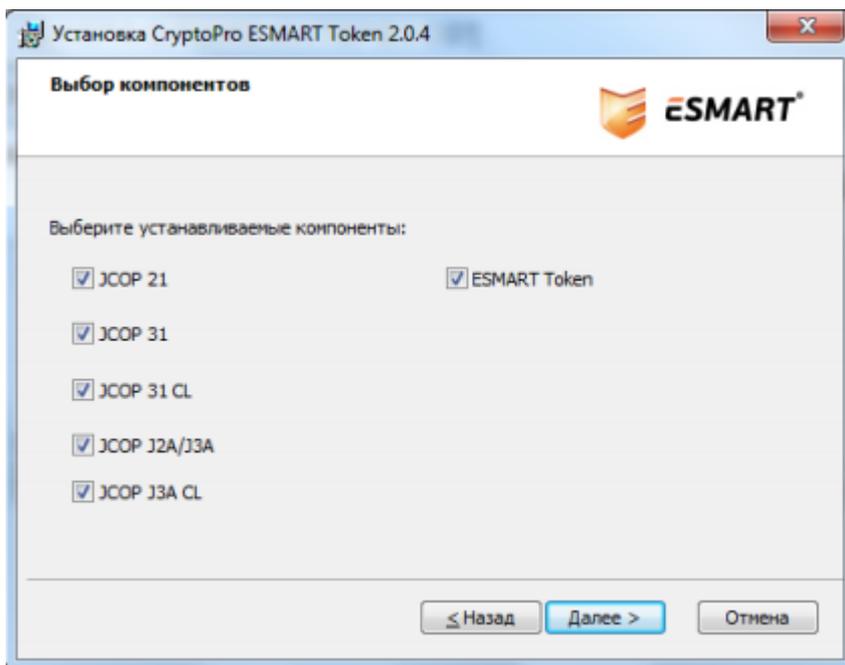


Рисунок 24. Параметры установки модуля поддержки КриптоПро CSP для Windows

5. В окне нажать кнопку «Далее».

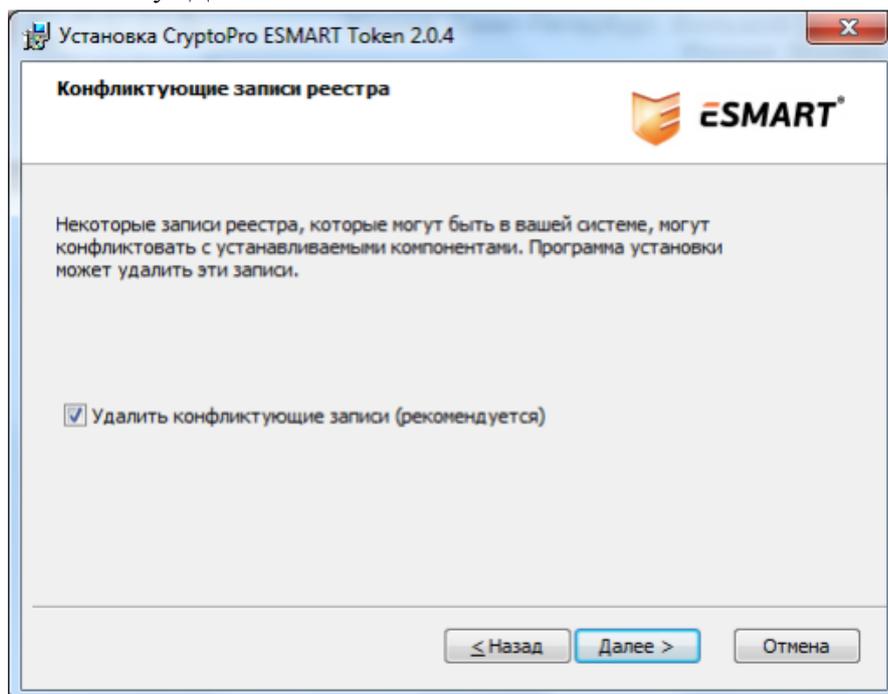


Рисунок 25. Параметры установки модуля поддержки КриптоПро CSP для Windows

6. В окне нажать кнопку «Установить».

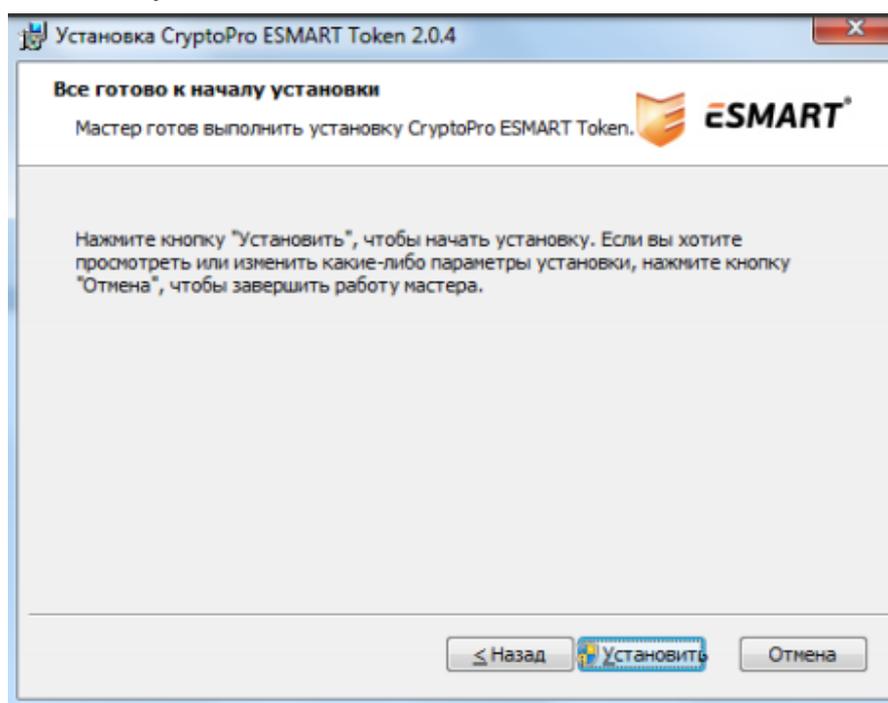


Рисунок 26. Установка модуля поддержки КриптоПро CSP для Windows

7. В окне нажать кнопку «Готово».

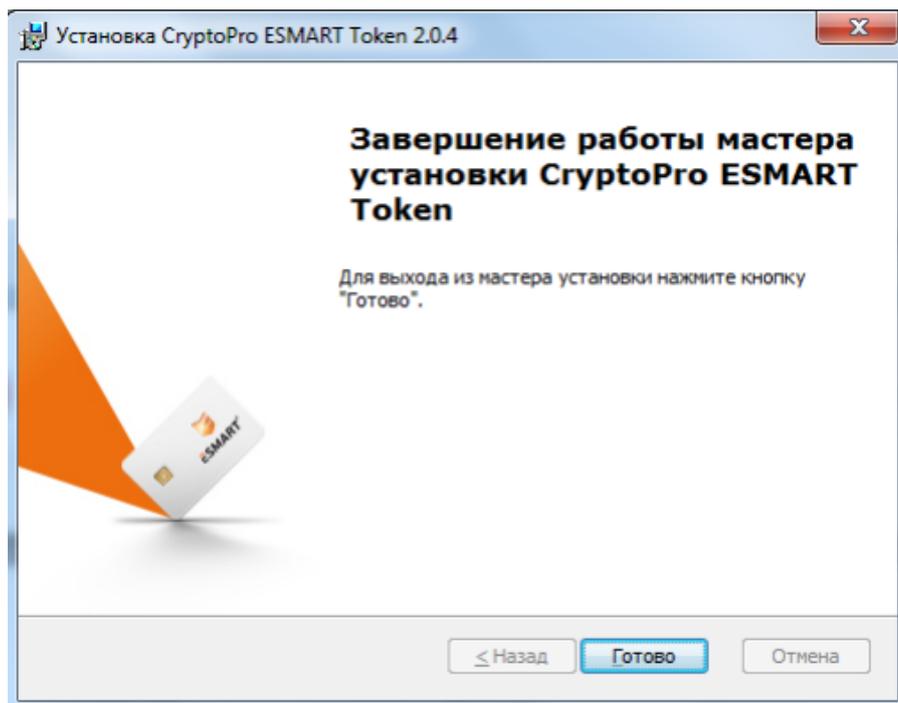


Рисунок 27. Завершение установки модуля поддержки КриптоПро CSP для Windows

Установка сертификата ключа подписи

Перед установкой сертификата ключа подписи необходимо вставить ключевой носитель Рутокен/ESMART в USB-порт компьютера.

1. Запустите **КриптоПро CSP** (Пуск -> Панель Управления -> КриптоПро CSP);

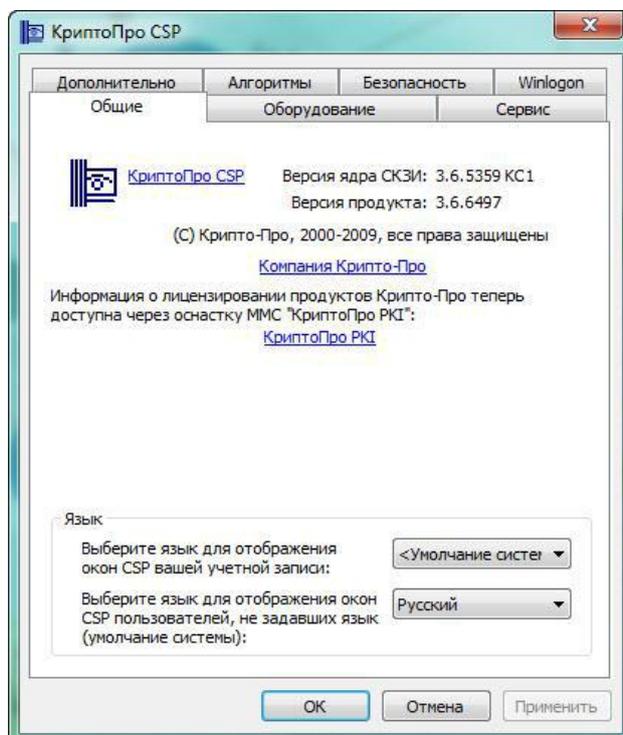


Рисунок 28. Установка открытого ключа сертификата пользователя. Вкладка «Общие»

2. Выберите вкладку «Сервис» и нажмите кнопку «Просмотреть сертификаты в контейнере»:

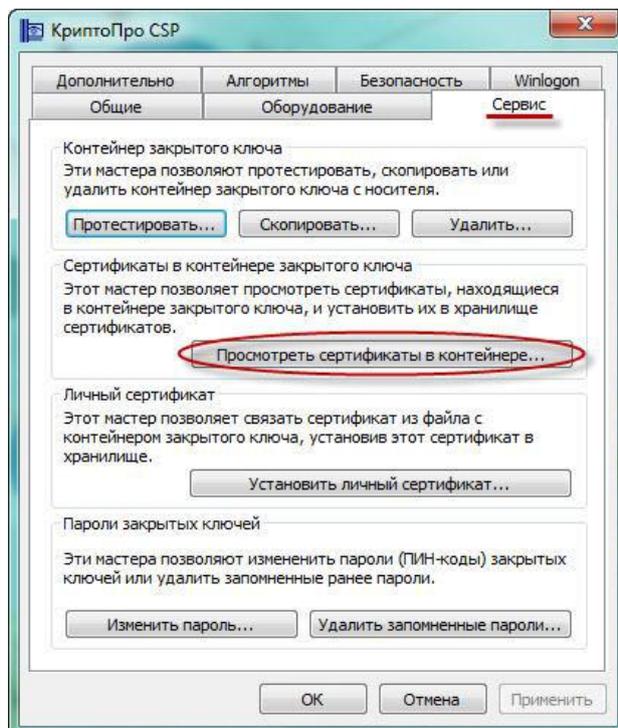


Рисунок 29. Установка открытого ключа сертификата пользователя. Вкладка «Сервис»

3. В окне «Сертификаты в контейнере закрытого ключа» нажмите кнопку «Обзор»;

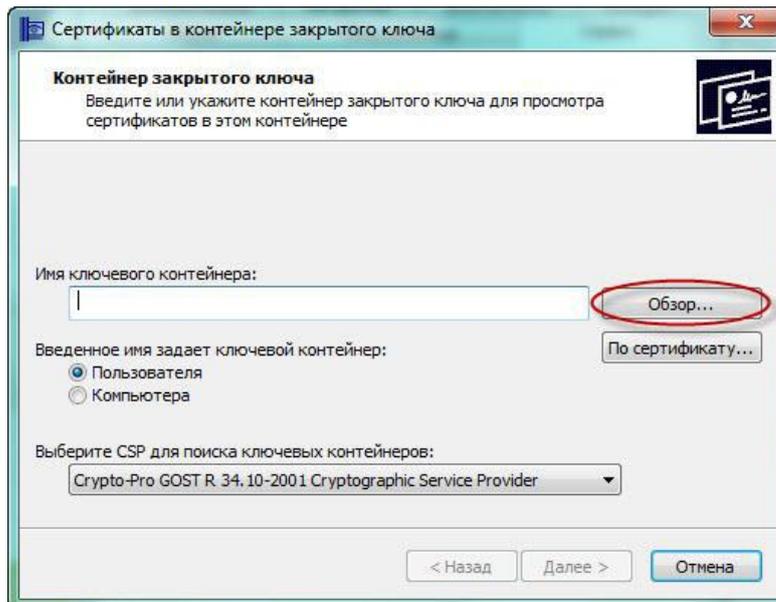


Рисунок 30. Установка открытого ключа сертификата пользователя. Сертификаты в контейнере закрытого ключа

4. В списке ключевых носителей выберите нужный личный сертификат и нажмите «ОК»;

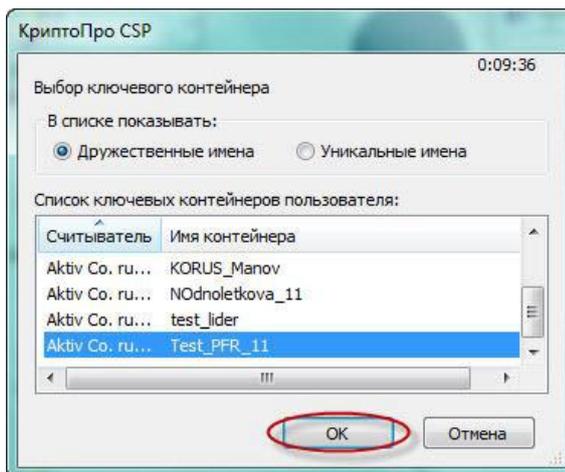


Рисунок 31. Установка открытого ключа сертификата пользователя. Список ключевых контейнеров пользователя

5. Нажмите кнопку «Далее» для продолжения установки;

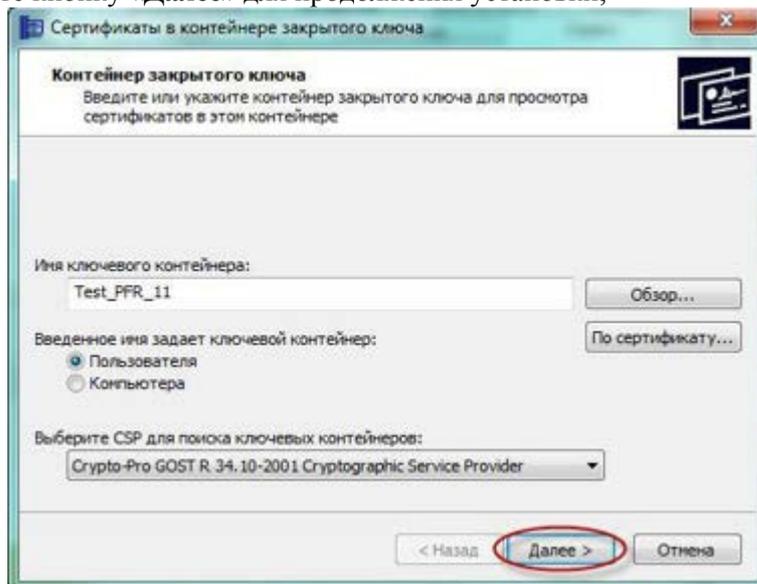


Рисунок 32. Установка открытого ключа сертификата пользователя. Имя ключевого контейнера

6. В информации о выбранном сертификате нажмите кнопку «Свойства»;

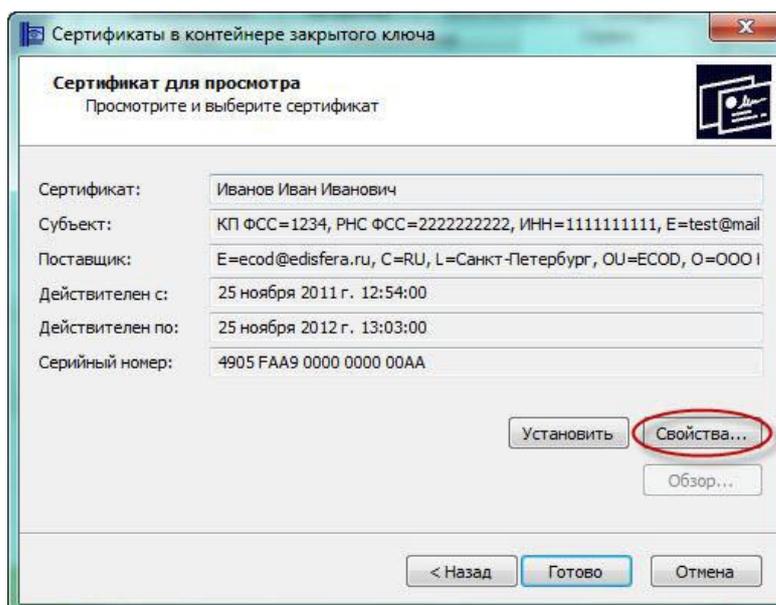
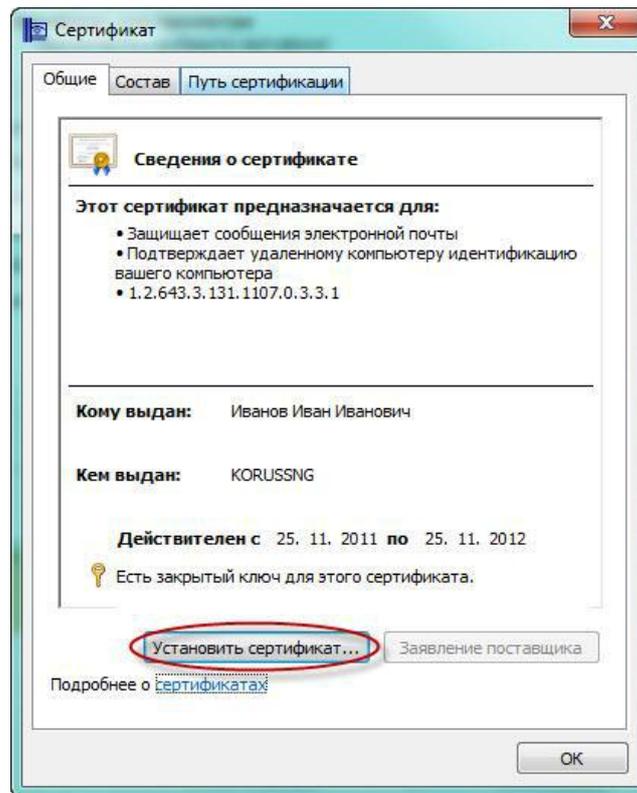


Рисунок 33. Установка открытого ключа сертификата пользователя. Сертификат для просмотра

7. Далее в появившемся окне сертификата нажмите кнопку «Установить сертификат»;



8. После этого запустится «Мастер импорта сертификатов». Для продолжения установки нажмите «Далее»;

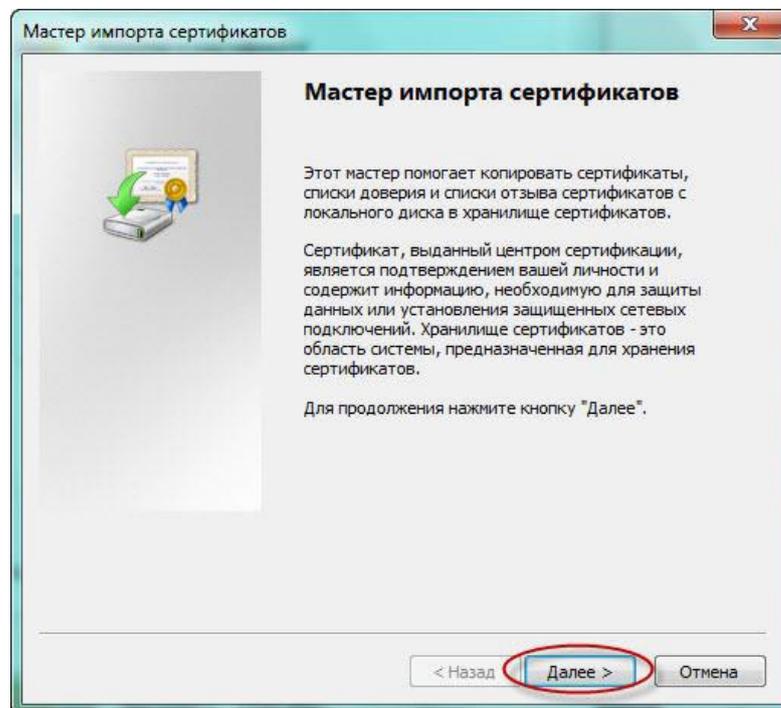


Рисунок 35. Установка открытого ключа сертификата пользователя. Мастер импорта сертификатов

9. В появившемся окне, поставьте галочку «Поместить все сертификаты в следующее хранилище» и нажмите кнопку «Обзор»;

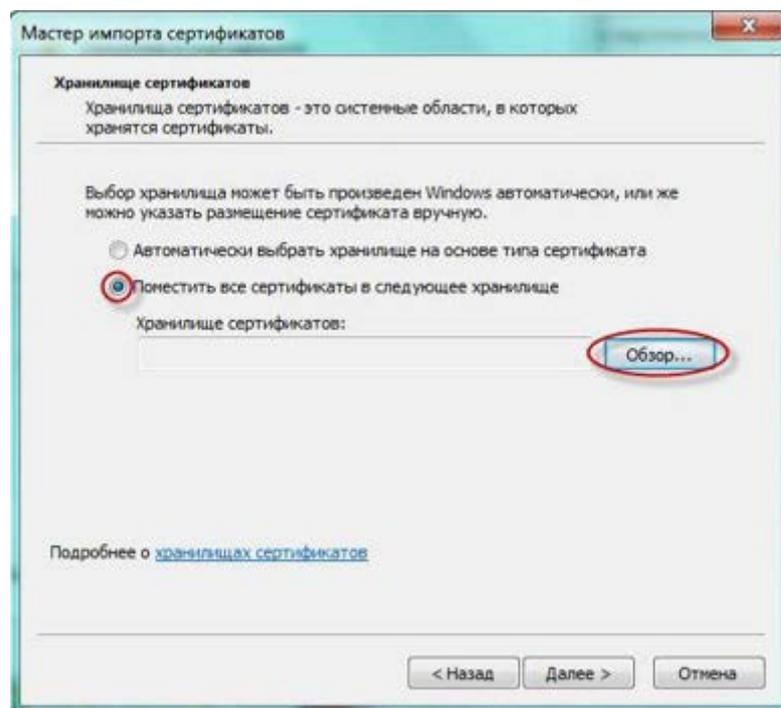


Рисунок 36. Установка открытого ключа сертификата пользователя. Выбор хранилища сертификатов

10. В списке хранилищ выберите хранилище «Личное», нажмите «ОК» и «Далее»;

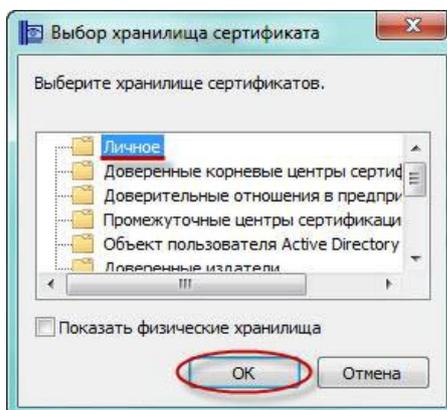


Рисунок 37. Установка открытого ключа сертификата пользователя. Хранилища сертификатов

11. Для завершения установки нажмите кнопку «Готово».

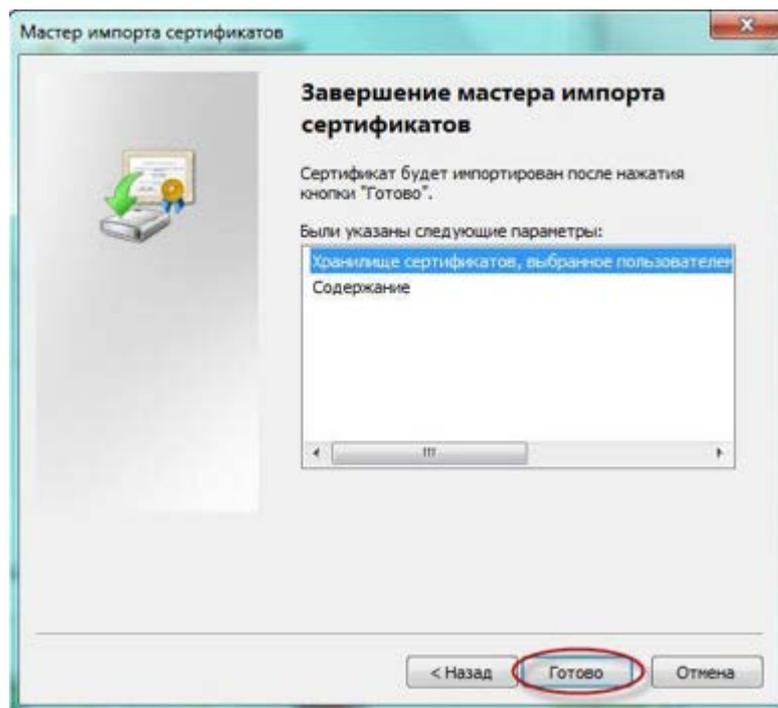


Рисунок 38. Установка открытого ключа сертификата пользователя. Завершение установки сертификата

12. Об успешном импорте сертификата в хранилище будет выдано сообщение «Импорт успешно выполнен»:

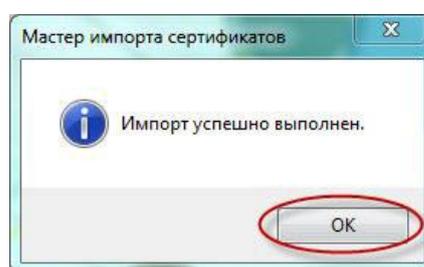


Рисунок 39. Установка открытого ключа сертификата пользователя. Подтверждение успешной установки

Установка корневого сертификата

1. Установка Корневого сертификата Головного удостоверяющего центра
2. Скачайте и откройте **файл Головной удостоверяющий центр**, в появившемся окне сертификата нажмите кнопку «**Установить сертификат**».

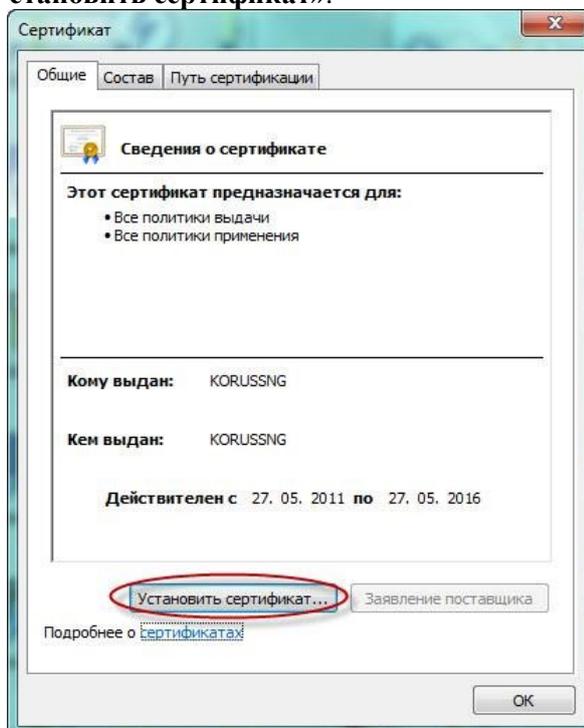


Рисунок 40. Установка корневого сертификата Головного удостоверяющего центра

3. После этого запустится «**Мастер импорта сертификатов**». Для продолжения установки выберите расположение хранилища: **Локальный компьютер**. Нажать «**Далее**».

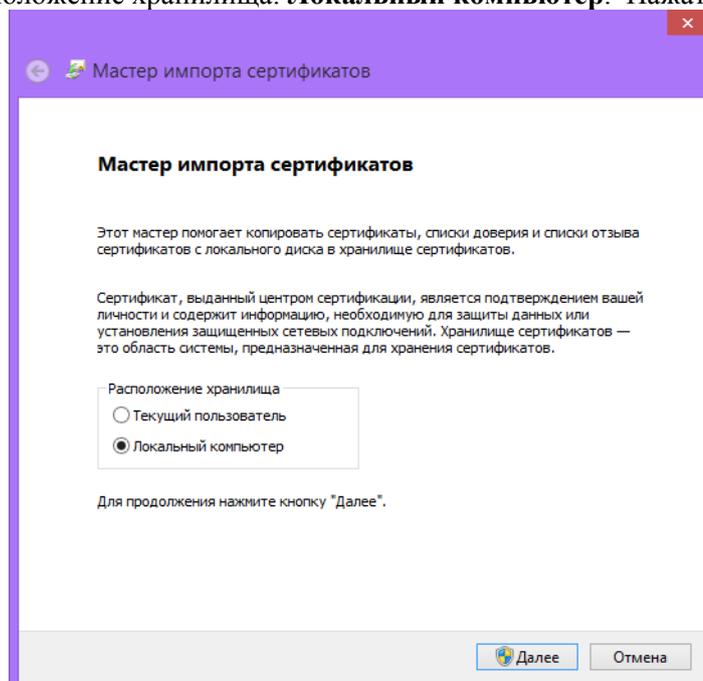


Рисунок 41. Мастер импорта сертификатов

4. В появившемся окне, поставьте галочку «Поместить все сертификаты в следующее хранилище» и нажмите кнопку «Обзор».

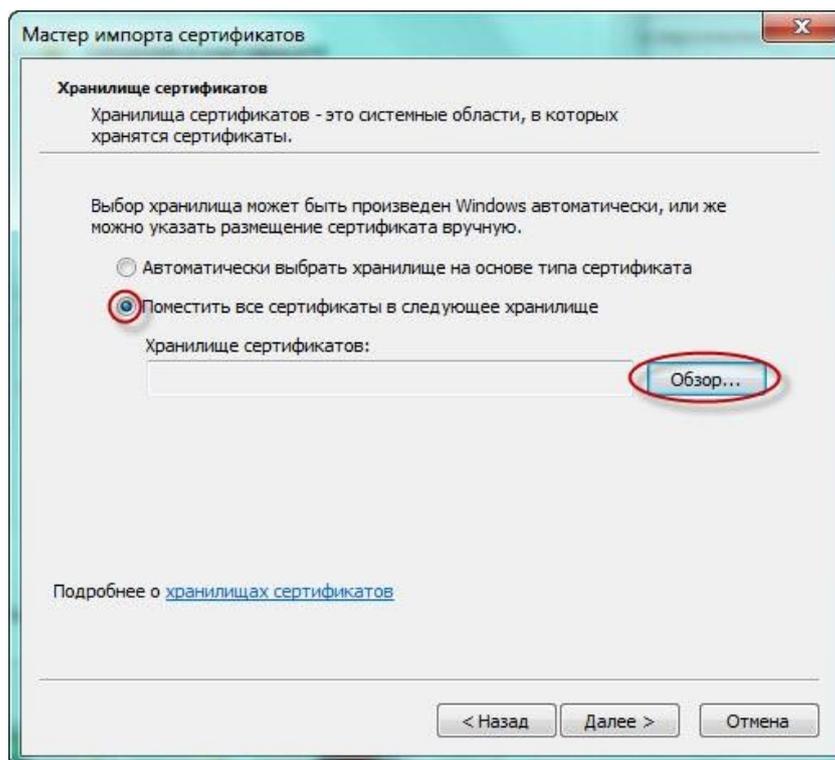


Рисунок 42. Установка корневого сертификата Головного удостоверяющего центра

5. В списке хранилищ выберите хранилище «Доверенные корневые центры сертификации», нажмите «ОК» и «Далее».

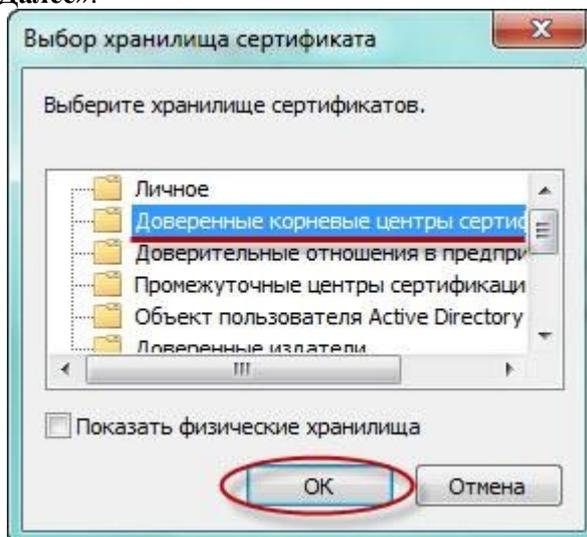


Рисунок 43. Выбор хранилища сертификата

6. Для завершения установки сертификата нажмите кнопку «Готово».

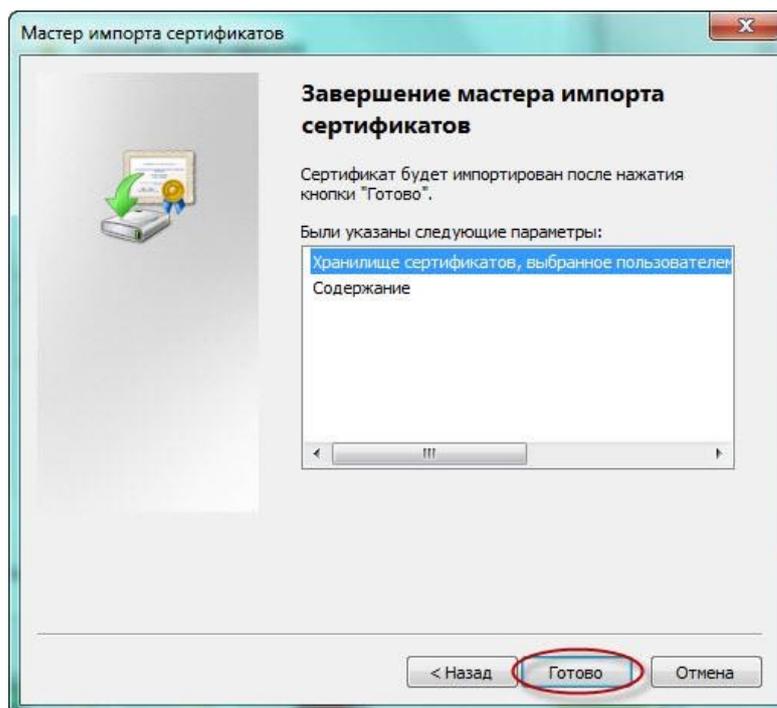


Рисунок 44. Завершение мастера импорта сертификатов

7. При запросе системы подтвердить доверие данному издателю сертификата, необходимо нажать «Да».

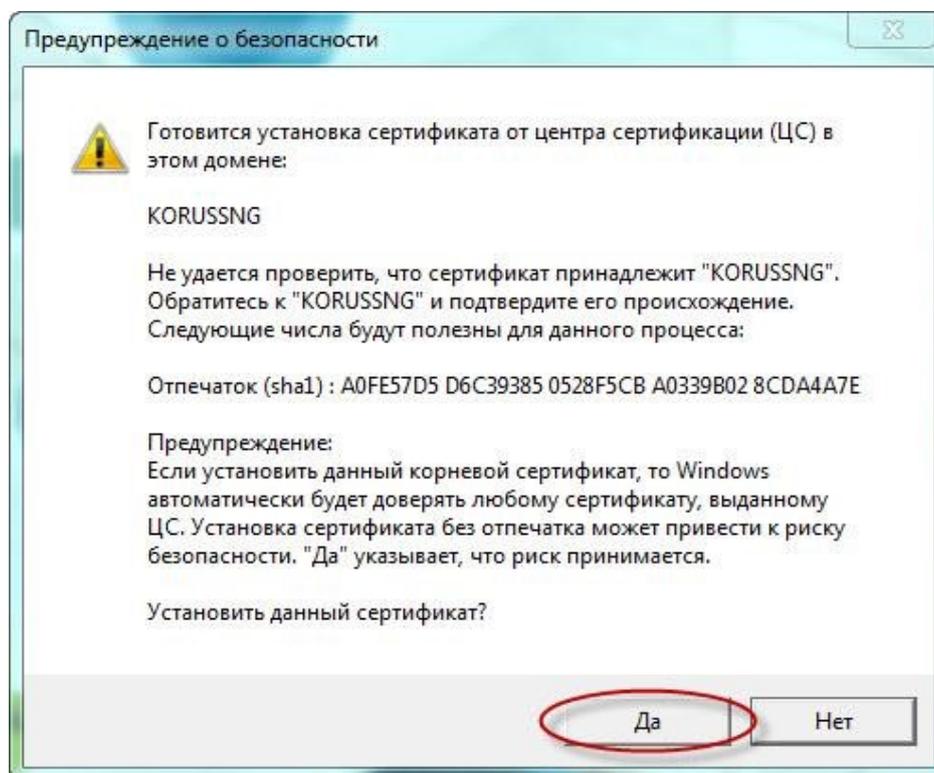


Рисунок 45. Предупреждение о безопасности

8. Об успешном импорте сертификата в хранилище будет выдано сообщение «Импорт успешно выполнен».

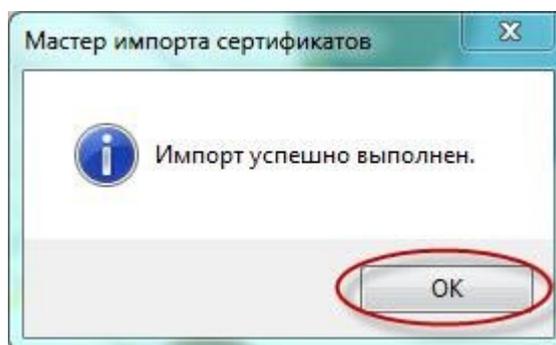


Рисунок 46. Успешное завершение импорта

9. Установка сертификата УЦ 1 ИС ГУЦ
Процесс установки сертификата ([скачать](#)) производится аналогично пункту 2-8, однако, сертификат «УЦ 1 ИС ГУЦ» следует установить в хранилище **«Промежуточные центры сертификации»**.
10. Установка сертификата, аккредитованного УЦ ООО «КОРУС Консалтинг СНГ».
Установка сертификата «ООО КОРУС Консалтинг СНГ» ([скачать](#)) производится аналогично пункту 2-8, но сертификат устанавливается в хранилище **«Промежуточные центры сертификации»**.

Установка библиотеки CARICOM

Библиотеку CARICOM можно скачать на площадке В2В по ссылке

<http://www.b2b-energo.ru/signature/more-for-clients.html> и установить утилиту для установки библиотеки CARICOM, настройки браузера Internet Explorer и установки КриптоПро ЭЦП Browser plug-in.

Утилита для установки библиотеки CARICOM, настройки браузера и установки КриптоПро ЭЦП plug-in

Утилита для установки библиотеки CARICOM, настройки браузера Internet Explorer и установки КриптоПро ЭЦП Browser plug-in (4.5 МБ)

Рисунок 47. Площадка В2В-energo. Утилита для установки библиотеки CARICOM

1. Кликните на ссылку для установки утилиты, нажмите **«Выполнить»**;



Рисунок 48. Установка утилиты

2. В окне с предупреждением системы безопасности нажмите **«Выполнить»**;

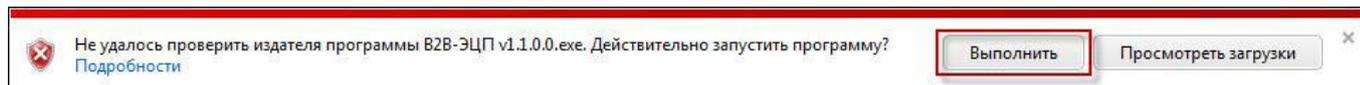


Рисунок 49. Предупреждение системы безопасности

3. После этого запустится **«Мастер установки В2В-ЭЦП»**. Для продолжения установки нажмите **«Далее»**;

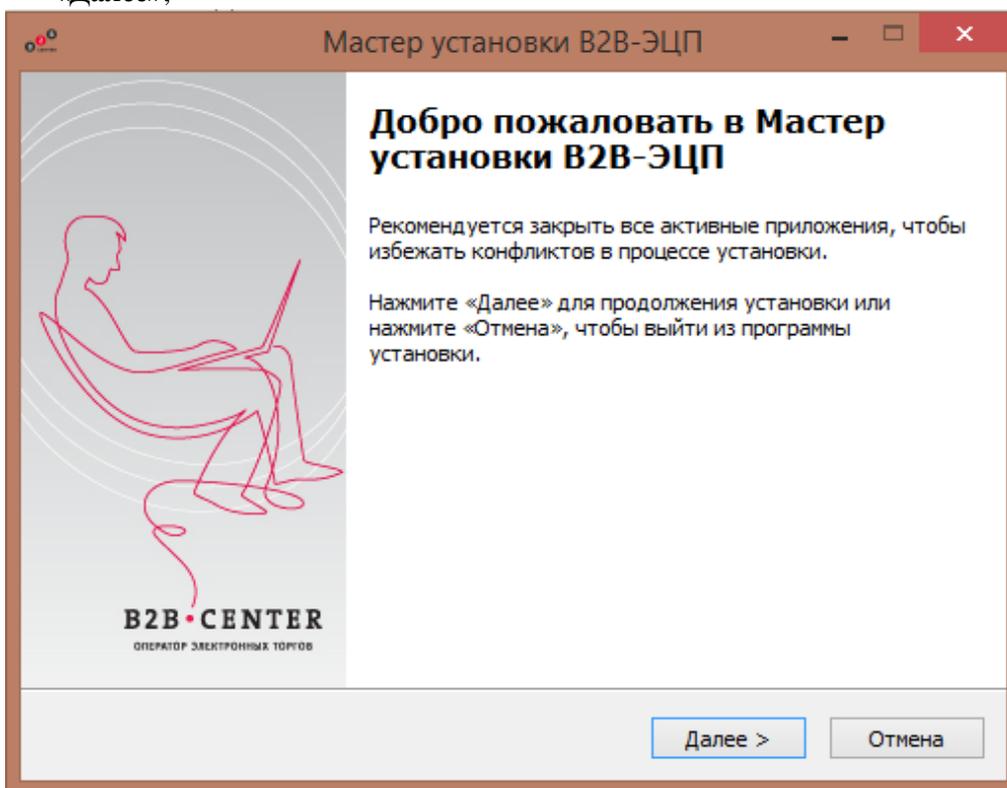


Рисунок 50. Мастер установки В2В-ЭЦП. Приветствие

4. Выберите компоненты для установки и нажмите «Далее»;

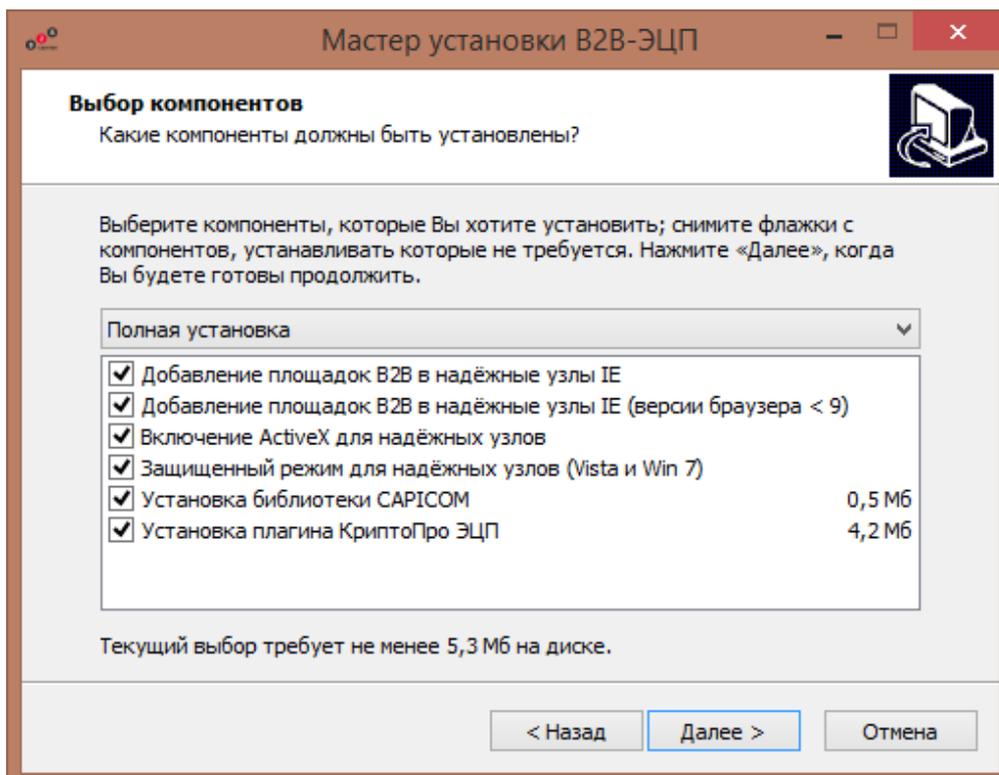


Рисунок 51. Мастер установки В2В-ЭЦП. Выбор компонентов для установки

4. Отметьте электронные площадки, на которых Вы собираетесь работать, нажмите «Далее»;

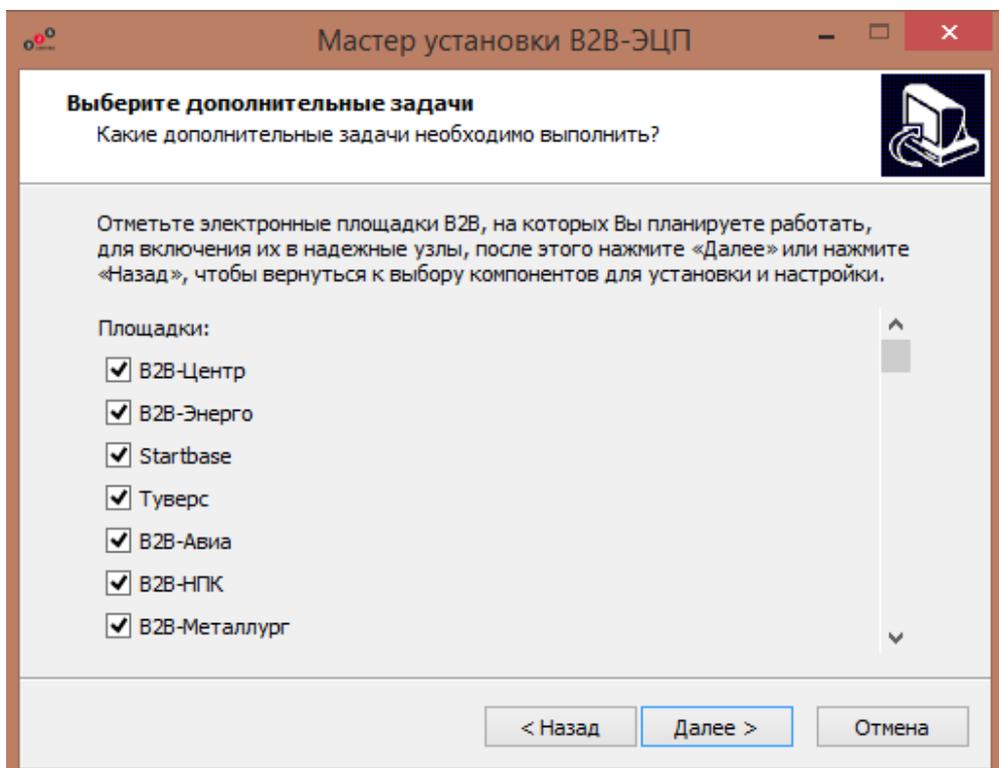


Рисунок 52. Мастер установки В2В-ЭЦП. Выбор площадок для работы

6. Нажмите кнопку «Установить»;

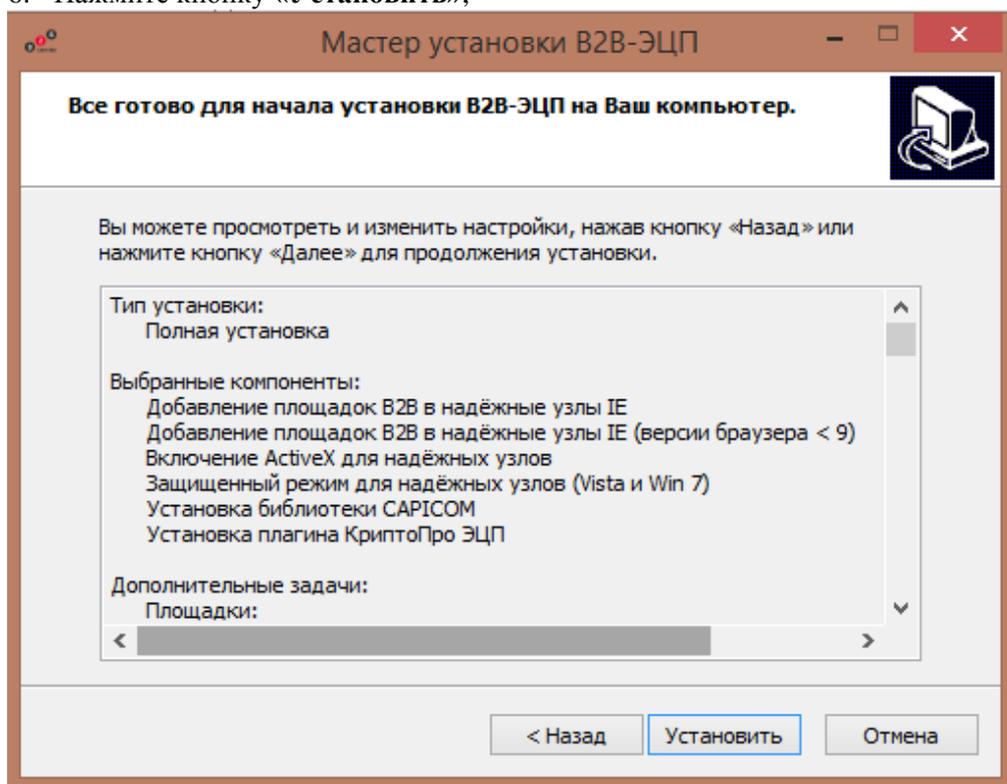


Рисунок 53. Мастер установки В2В-ЭЦП. Начало установки

7. Для установки **КриптоПро ЭЦП Browser plug-in** нажмите «Да»;

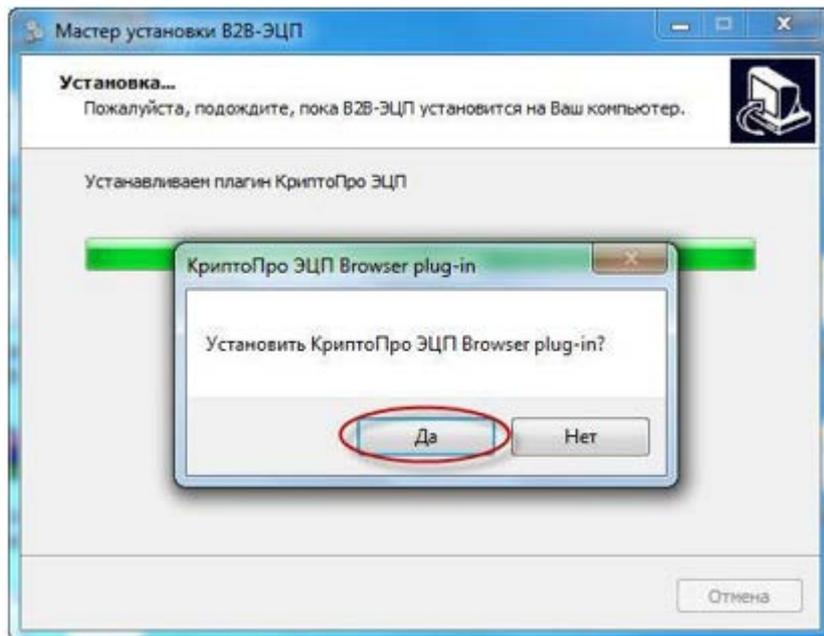


Рисунок 54. Мастер установки В2В-ЭЦП. Установка КриптоПро ЭЦП Browser plug-in

8. Нажмите «Да», чтобы перезагрузить систему;

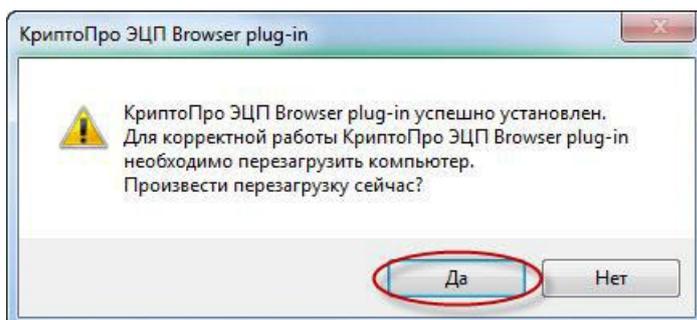


Рисунок 55. КриптоПро ЭЦП Browser plug-in. Перезагрузка системы

9. Для завершения работы мастера нажмите кнопку «**Завершить**»;

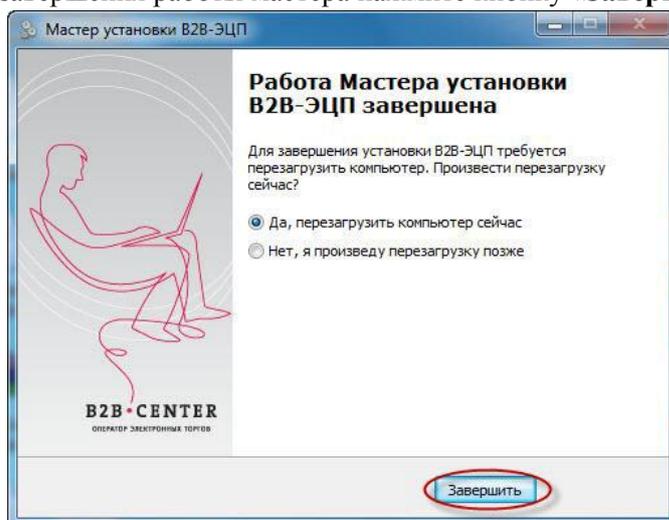


Рисунок 56. Перезагрузка компьютера.

Проверка работы электронной подписи на площадке В2В

1. Зайдите в Ваш личный кабинет на площадке В2В
2. Перейдите в раздел Электронная Цифровая подпись по ссылке <http://www.b2b-energo.ru/signature/> и выберите сервис «Проверка работы ЭЦП» по ссылке <http://www.b2b-energo.ru/signature/test.html>

Электронная цифровая подпись

Внимание! Указанные в разделе "Электронная цифровая подпись" цены на услуги по выпуску электронной подписи не являются офертой. Пожалуйста, уточните стоимость электронной подписи в выбранном Вами пункте выдачи.

[Получение и регистрация ЭЦП](#) [Регистрация сертификатов](#) [Проверка работы ЭЦП](#) [Центр проверки электронных документов](#) [Удостоверяющие центры](#) [Частые вопросы-ответы](#)

Данный раздел предназначен для проверки работы средств электронной цифровой подписи, полученных и настроенных для работы пользователей в системе.

Оператор Системы электронного документооборота В2В-Center **настоятельно рекомендует** главным пользователям проверять работоспособность электронной подписи, **прежде чем использовать** электронную подпись в торговых процедурах.

На главном пользователе организации лежит ответственность **постоянно поддерживать работоспособность электронной подписи** в процессе эксплуатации на своем рабочем компьютере, в том числе, дополнительно убедиться, что электронная подпись функционирует нормально:

- после проведения работ по установке, обновлению, удалению и настройке на рабочем компьютере системного и прикладного программного обеспечения;
- за 1-2 дня до планируемого использования электронной подписи в процедуре, особенно при загрузке конкурсных заявок.

Оператор Системы электронного документооборота В2В-Center **не несет ответственности** за нарушения в работе электронной подписи, которые имели место на рабочем компьютере организации и которые привели к проблемам в подписании электронных документов.

[Решение проблем, возникающих при работе с ЭЦП \(257 КБ\)](#)

[Утилита для установки библиотеки CAPICOM, настройки браузера Internet Explorer и установки КриптоПро ЭЦП Browser plug-in \(4.5 МБ\)](#)

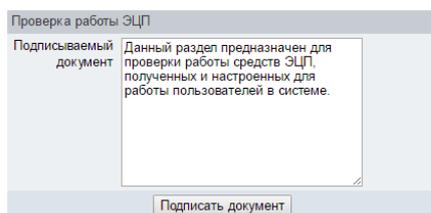


Рисунок 57. Площадка В2В-energo. Раздел ЭЦП. Проверка работы ЭЦП

3. Нажмите кнопку «Подписать документ» для подписания тестового документа

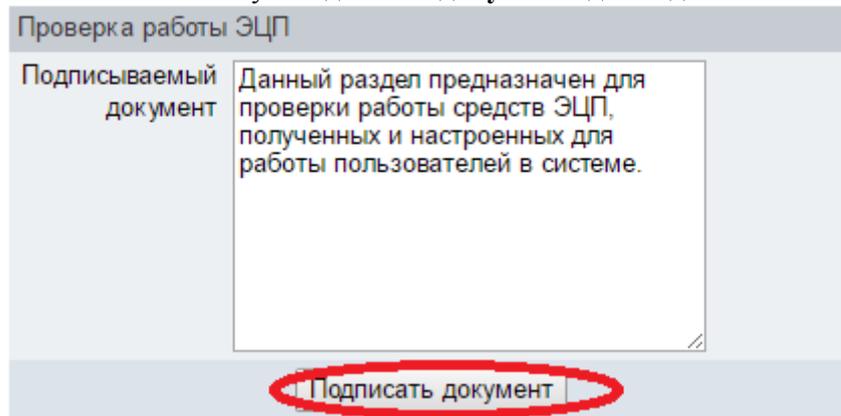


Рисунок 58. Площадка В2В-energo. Проверка работы ЭЦП. Подписание тестового документа

4. При подписании тестового документа система запросит пин-код для контейнера закрытого ключа (пин-код сообщается в Удостоверяющем центре при получении электронной подписи). Введите пин-код и нажмите «ОК».
5. В случае корректной установки всех компонентов, появится сообщение о том, что документ успешно подписан.

Если на этапе подписания возникают какие-либо ошибки, проверьте, что все компоненты корректно установлены, и обратитесь в службу технической поддержки по телефону:

8 (800)100-8-812 (Бесплатно по РФ), либо по электронной почте: help@esphere.ru