

**Продукт «1С-ЭТП»  
Работа с электронной подписью  
Руководство пользователя**

**Версия: 1.0.1.3.  
Дата: 21.05.2020 г.**

## СОДЕРЖАНИЕ

<b>АННОТАЦИЯ</b> .....	<b>3</b>
<b>УСЛОВНЫЕ ОБОЗНАЧЕНИЯ</b> .....	<b>4</b>
<b>ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ</b> .....	<b>5</b>
<b>1. ОБЩАЯ ИНФОРМАЦИЯ</b> .....	<b>6</b>
<b>2. ТРЕБОВАНИЯ К РАБОЧЕМУ МЕСТУ</b> .....	<b>7</b>
<b>3. ПОДГОТОВКА К РАБОТЕ С ЭЛЕКТРОННОЙ ПОДПИСЬЮ</b> .....	<b>8</b>
3.1. УСТАНОВКА И НАСТРОЙКА КРИПТОПРОВАЙДЕРОВ .....	8
3.1.1. Установка СКЗИ Крипто ПРО CSP .....	8
3.1.2. Регистрация СКЗИ Крипто ПРО CSP .....	13
3.1.3. Установка СКЗИ ViPNet CSP .....	16
3.1.4. Регистрация СКЗИ ViPNet CSP .....	21
3.2. УСТАНОВКА ДРАЙВЕРОВ НОСИТЕЛЕЙ .....	24
3.2.1. Установка драйверов JaCarta .....	24
3.2.1.1. Интерфейс Единого клиента JaCarta и JaCarta SecurLogon .....	28
3.2.1.2. Особенности работы с Единым клиентом JaCarta .....	30
3.2.2. Установка драйверов RuToken .....	30
3.2.3. Настройка считывателей в СКЗИ КриптоПро CSP .....	34
3.3. УСТАНОВКА СЕРТИФИКАТОВ .....	38
3.3.1. Установка сертификатов Крипто ПРО CSP .....	38
3.3.1.1. Создание копии контейнера закрытого ключа КриптоПро CSP .....	43
3.3.2. Установка сертификатов ViPNet CSP .....	47
3.3.2.1. Создание копии контейнера закрытого ключа ViPNet CSP .....	51
3.4. УСТАНОВКА КОРНЕВЫХ СЕРТИФИКАТОВ .....	53
3.4.1. Установка корневых сертификатов с помощью программы автоматической установки .....	53
3.5. НАСТРОЙКА ИНТЕРНЕТ-БРАУЗЕРА .....	56
<b>4. РАБОТА С ЭЛЕКТРОННОЙ ПОДПИСЬЮ</b> .....	<b>62</b>
4.1. ОСОБЕННОСТИ РАБОТЫ С НАИБОЛЕЕ РАСПРОСТРАНЕННЫМИ САЙТАМИ С ПОМОЩЬЮ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ .....	62
4.1.1. ЗАО «Сбербанк-АСТ» .....	62
4.1.1.1. Регистрация на универсальной торговой платформе .....	62
4.1.1.2. Вход в личный кабинет Поставщика .....	62
4.1.2. Авторизация на портале Госуслуги с помощью КЭП .....	64
4.1.3. ГАС «Правосудие» .....	68
4.1.4. Вход на портал <i>tos.ru</i> .....	69
4.1.5. ГИС ЖКХ .....	70
4.1.6. Вход на портал Росреестра с помощью электронной подписи .....	71
4.2. ПРОВЕРКА ПОДПИСИ .....	72
4.2.1. Открытие сертификата через свойства браузера .....	72
4.2.2. Открытие сертификата с помощью СКЗИ .....	74
4.3. ДЕЙСТВИЯ ПРИ СМЕНЕ СЕРТИФИКАТА .....	80
<b>ЗАКЛЮЧЕНИЕ</b> .....	<b>81</b>

## **Аннотация**



Документ «Руководство Пользователя по работе с электронной подписью» содержит описание процесса подготовки рабочего места и работы с электронной подписью, полученной в точках выдачи АО «КАЛУГА АСТРАЛ».

В разделе «Требования к рабочему месту» приведены требования к техническому и программному обеспечению, необходимому для обеспечения корректной работы криптографических средств, драйверов носителей и интернет-браузеров.

В разделе «Подготовка к работе с электронной подписью» описаны действия Пользователя по установке криптопровайдеров, драйверов носителей, корневых сертификатов и сертификата Пользователя, а также настройка интернет-браузера.

Раздел «Работа с электронной подписью» содержит описание действий Пользователя при смене сертификата, проверке подписи или работе на популярных сайтах, для авторизации на которых требуется электронная подпись.

## Условные обозначения

Обозначение	Расшифровка
	<p><i>Блок «Внимание». Содержит информацию о важных моментах, на которые следует обратить внимание. А также о возможных нежелательных действиях и ошибочных ситуациях.</i></p>
	<p><i>Блок «Примечание». Содержит рекомендации и особые значения.</i></p>
<p><b>Текст</b></p>	<p><i>Обозначение компонентов интерфейса, требующих активного воздействия Пользователя (кнопки, флаги и т.д.).</i></p>

## Термины и определения

**Ключ электронной подписи** – уникальная последовательность символов, предназначенная для создания электронной подписи;

**Ключ проверки электронной подписи** – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи;

**Корневой сертификат Удостоверяющего Центра** – основной сертификат, на котором выстраивается цепочка доверия сертификатам;

**Сертификат ключа проверки электронной подписи** – электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи;

**Список отозванных сертификатов (СОС)** – созданный Удостоверяющим центром список сертификатов ключей проверки электронных подписей, отозванных до окончания срока их действия;

**СКЗИ (средство криптографической защиты информации)** – программа (служба), которая обеспечивает шифрование и дешифрование документов. Без нее не удастся использовать ЭП на компьютере;

**Средства электронной подписи** – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи;

**Удостоверяющий центр** – юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом;

**Электронная подпись (ЭП)** – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

## 1. Общая информация

Электронная подпись (ЭП) – аналог печати юридического лица, собственноручной подписи физического лица и индивидуального предпринимателя. Используется для идентификации личности владельца при совершении юридически значимых действий. Сюда входят авторизация на порталах аукционов, торгов, удаленное получение государственных, муниципальных услуг, электронная регистрация сделок и документооборота.

Порядок получения ЭП:

1. Обратитесь в Удостоверяющий Центр.
2. Выберите нужный вам вид электронной подписи.
3. Заполните заявление на получение ЭП.
4. Оплатите госпошину и счет.
5. Предоставьте пакет документов в УЦ.
6. Запишите Вашу ЭП на защищенный носитель Рутокен Lite 64 КБ, для того чтобы хранить ее в безопасности.
7. Получите ЭП на защищенном носителе.

## 2. Требования к рабочему месту

Требования к компьютеру:

- Процессор – Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более;
- Объем оперативной памяти – не менее 512 Мбайт;
- Свободное место на жестком диске – не менее 100 Мбайт;
- Любой современный интернет браузер, обновленный до последней версии;

Требования к операционным системам:

- Microsoft Windows 10 (32/64-бит);
- Microsoft Windows 8.1 (32/64-бит);
- Microsoft Windows 8 (32/64-бит);
- Microsoft Windows 7 SP1 (32/64-бит);
- Microsoft Windows Vista SP2 (32/64-бит);
- Microsoft Windows XP SP3 (32-бит), SP2 (64-бит);
- Microsoft Windows Server 2012 R2;
- Microsoft Windows Server 2012;
- Microsoft Windows Server 2008 R2 SP1;
- Microsoft Windows Server 2008 SP2 (32/64-бит);
- Microsoft Windows Server 2003 R2 SP2 (32/64-бит);
- Microsoft Windows Server 2003 SP2 (32/64-бит).

### 3. Подготовка к работе с электронной подписью

Подготовка к работе с электронной подписью включает выполнение следующих действий:

- установку требуемого криптопровайдера (ViPNet CSP либо КриптоПро CSP);
- регистрацию криптопровайдера;
- установку драйверов защищенных носителей;
- настройку считывателей в СКЗИ.

Подробная информация по выполнению данных действий представлена ниже.

#### 3.1. Установка и настройка криптопровайдеров

##### 3.1.1. Установка СКЗИ Крипто ПРО CSP



*С 1 января 2019 года для формирования электронной подписи на рабочем месте Вам необходимо будет иметь КриптоПро CSP версии 4.0.*

*Обновление криптопровайдера необходимо будет выполнить при продлении сертификата.*

*Для того чтобы избежать трудностей при формировании ЭП, начиная с 1 января 2019 года, рекомендуем Вам обновить версию Вашего СКЗИ в течение 2018 года.*



*Перед установкой, переустановкой или удалением СКЗИ рекомендуется создать точку восстановления системы.*



*Установка двух СКЗИ может повлечь нестабильную работу операционной системы.*

Для установки программного обеспечения «КриптоПРО CSP» перейдите на сайт ООО «КРИПТО-ПРО» по ссылке <http://cryptopro.ru/>.

На открывшейся странице сайта «КриптоПро» в главном меню выберите пункт **Продукты** → **СКЗИ КриптоПро CSP/TLS/JCP** → **Загрузка файлов** (рис. 3.1.1.1.).



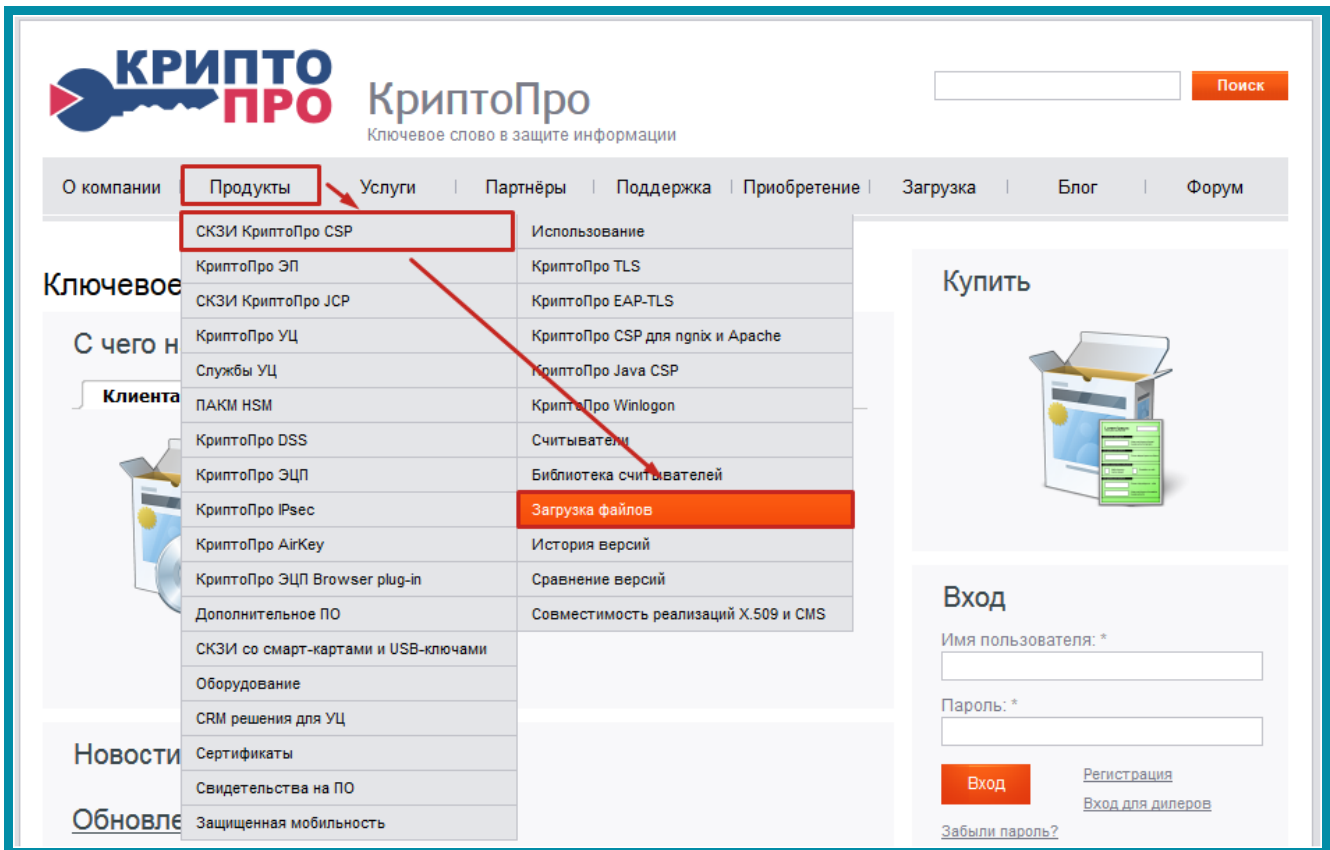


Рис. 3.1.1.1.

Перед Вами откроется раздел **Как загрузить дистрибутив?** Если Вы входите в систему в первый раз, необходимо зарегистрироваться, перейдя по ссылке **Предварительной регистрации**. Если Вы являетесь зарегистрированным пользователем, перейдите по ссылке **Войдите под вашей учетной записью** (рис. 3.1.1.2.).

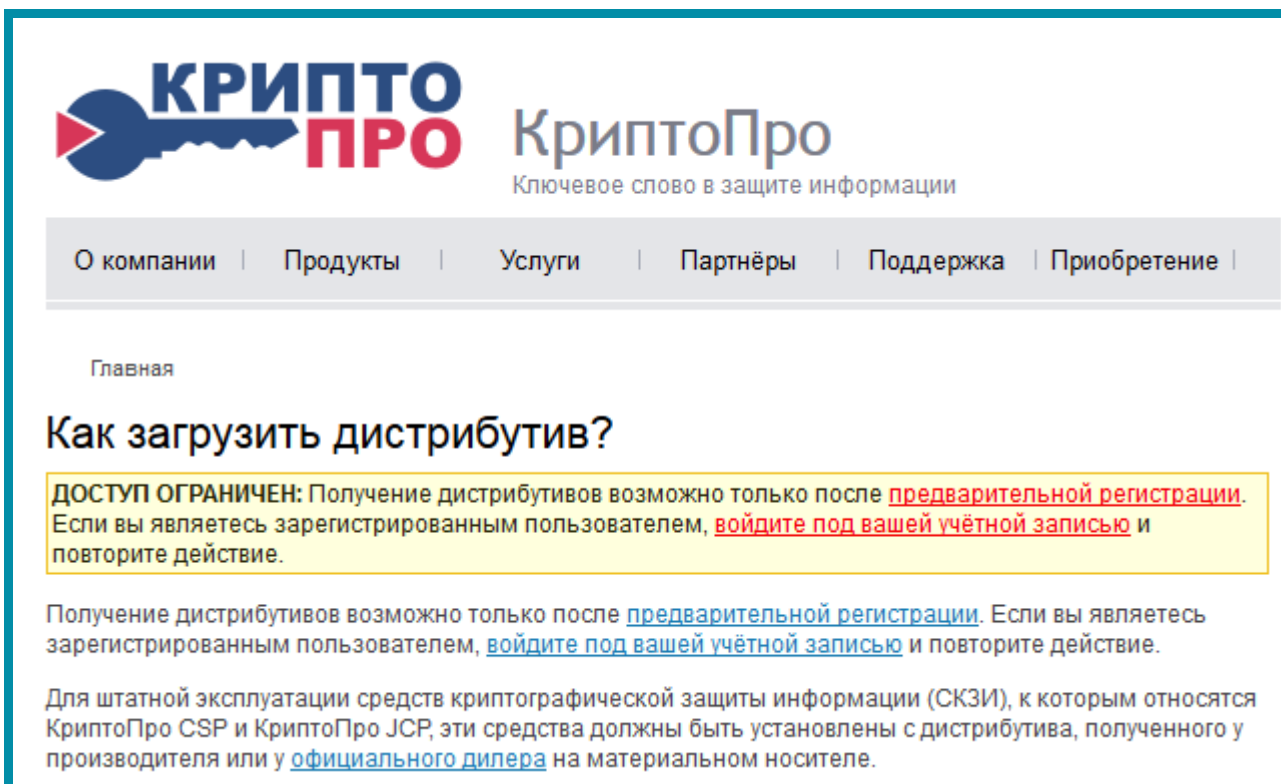


Рис. 3.1.1.2.

После авторизации на сайте на открывшейся странице перейдите по ссылке **Загрузка файлов** (рис. 3.1.1.3.).

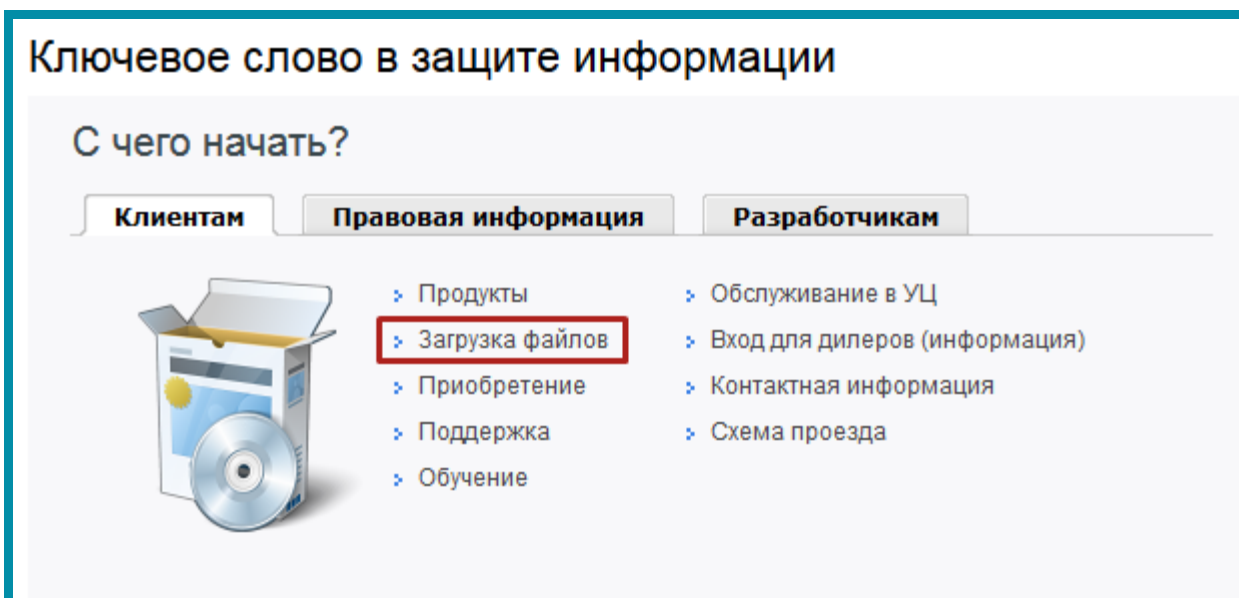


Рис. 3.1.1.3.

В центре загрузки выберите загружаемый продукт **КриптоПро CSP** (рис. 3.1.1.4.).

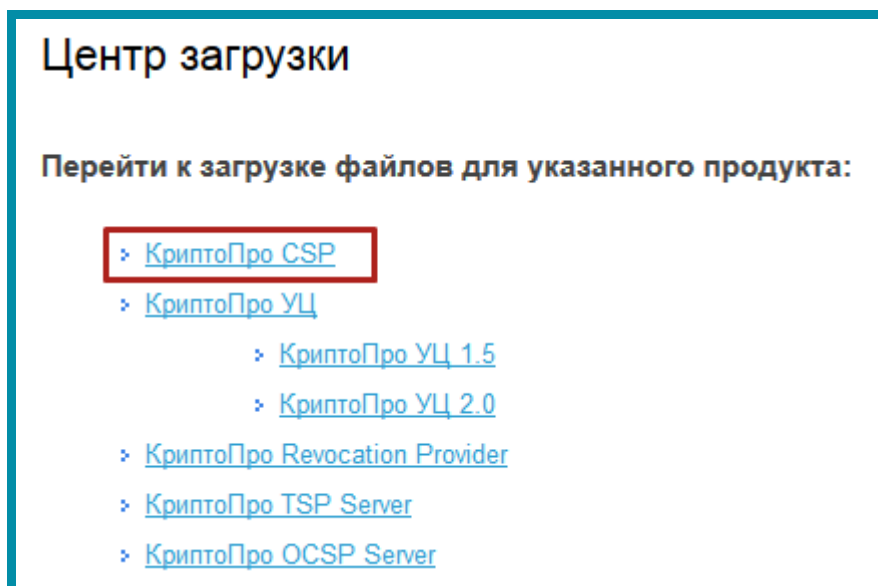
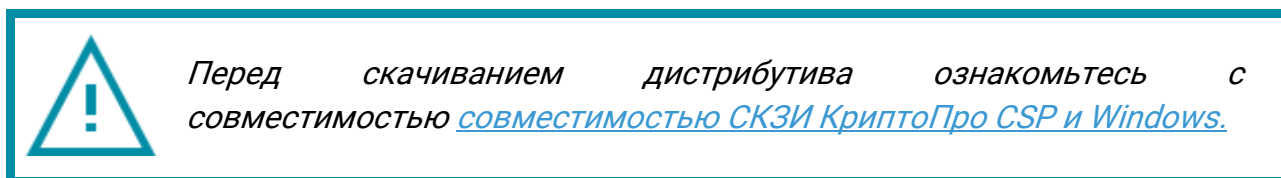


Рис. 3.1.1.4.



На открывшейся странице сайта выберите необходимый дистрибутив в соответствии с установленной у Вас операционной системой и ее разрядностью (рис. 3.1.1.5).

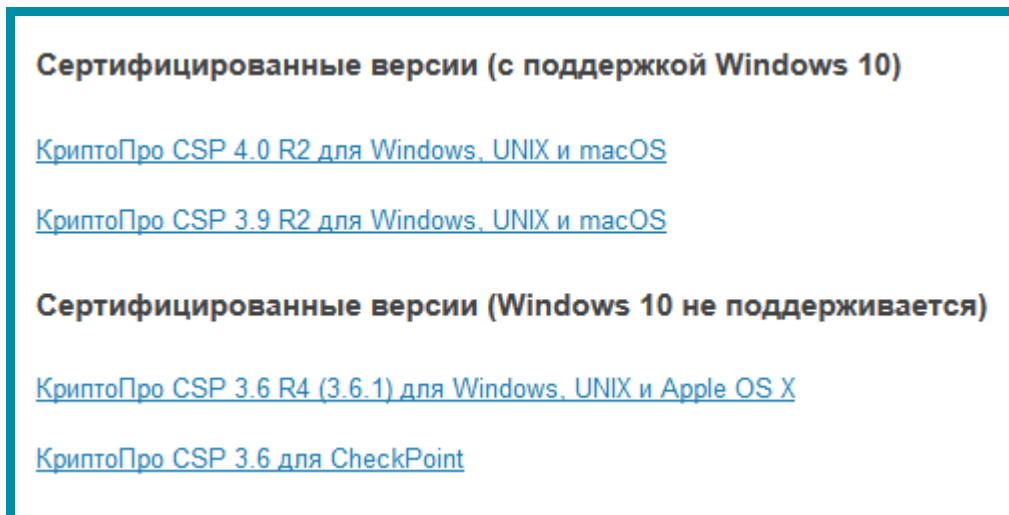


Рис. 3.1.1.5.

Далее Вам будет предложено сохранить выбранный дистрибутив в формате .msi на жесткий диск компьютера. Нажмите кнопку **Сохранить файл** (рис. 3.1.1.6).

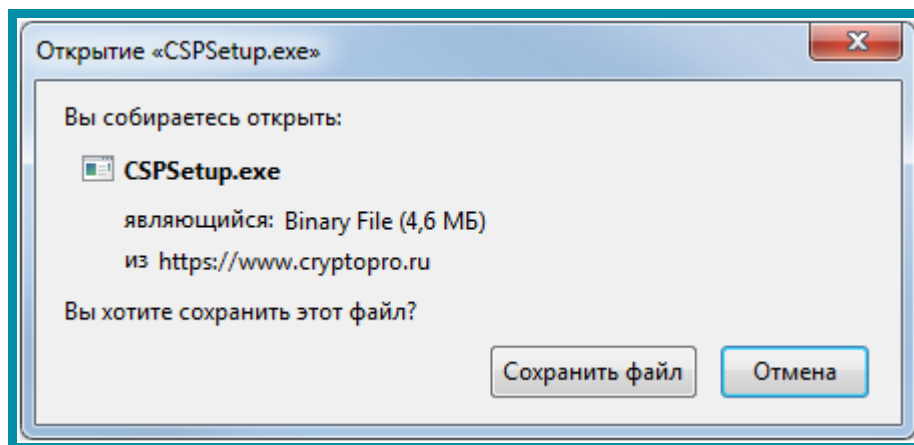


Рис. 3.1.1.6.



Перед установкой, переустановкой и удалением криптопровайдера рекомендуется [создать точку восстановления системы.](#)

Для начала установки запустите установочный файл программы. В открывшемся окне нажмите кнопку **Установить** (рис. 3.1.1.7).

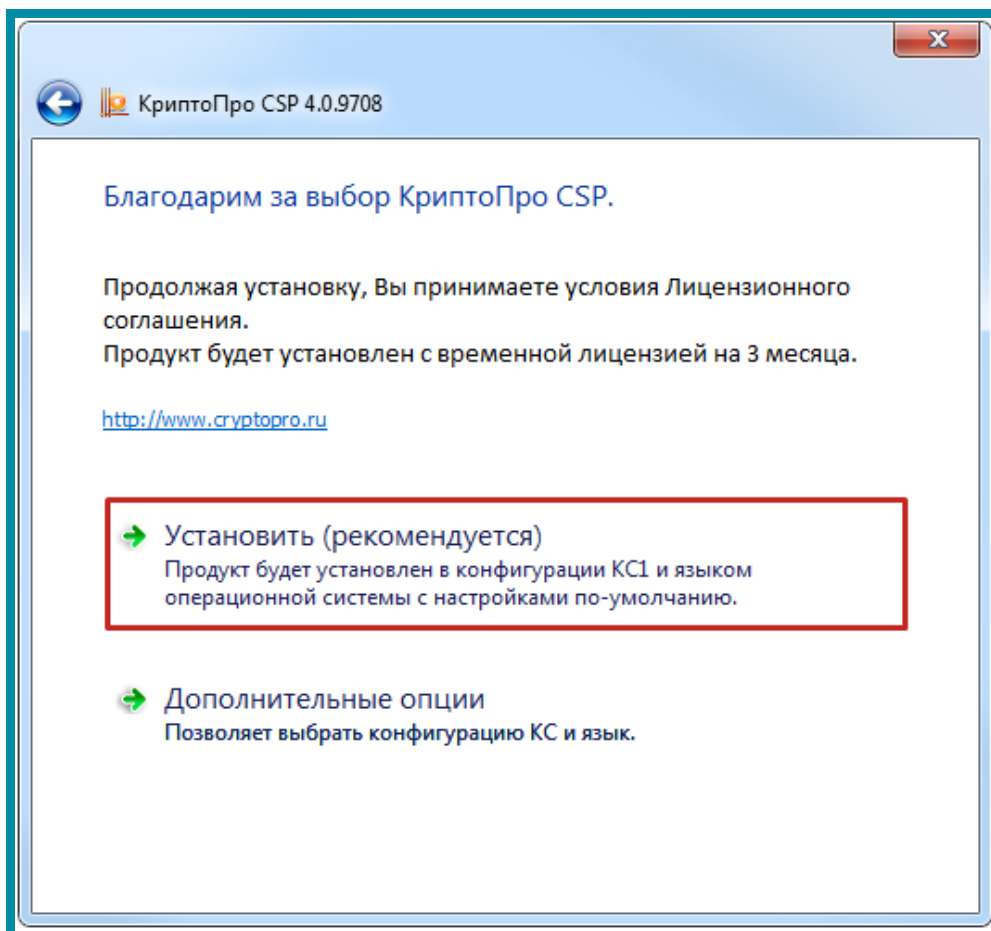


Рис. 3.1.1.7.

Начнется установка программы (рис. 3.1.1.8).

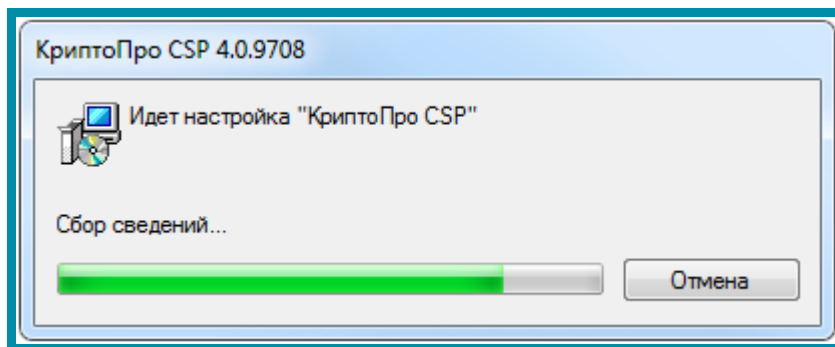


Рис. 3.1.1.8.

После того, как программа сообщит об успешном окончании установки КриптоПро CSP, нажмите кнопку **ОК** (рис. 3.1.1.9.).

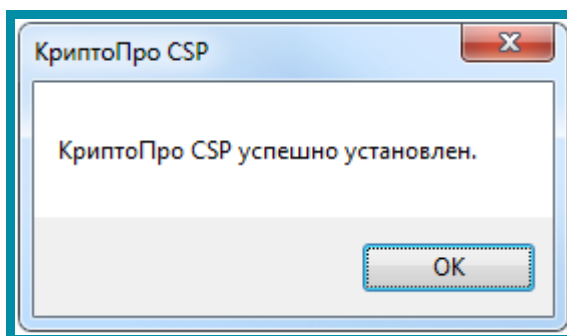


Рис. 3.1.1.9.



*После установки СКЗИ КриптоПро CSP необходимо выполнить перезагрузку ПК.*

После перезагрузки ПК, СКЗИ «КриптоПро CSP» будет готов к работе. СКЗИ «КриптоПро CSP» имеет демонстрационный период - 3 месяца, на протяжении которых СКЗИ будет работать в полнофункциональном режиме, после чего потребуется обязательная [регистрация продукта](#).

### 3.1.2. Регистрация СКЗИ Крипто ПРО CSP

После перезагрузки компьютера запустите программу КриптоПро CSP, нажав на ярлык программы на рабочем столе или выбрав «КриптоПро CSP» в меню «Пуск». Перед Вами появится окно следующего вида (рис. 3.1.2.1.).

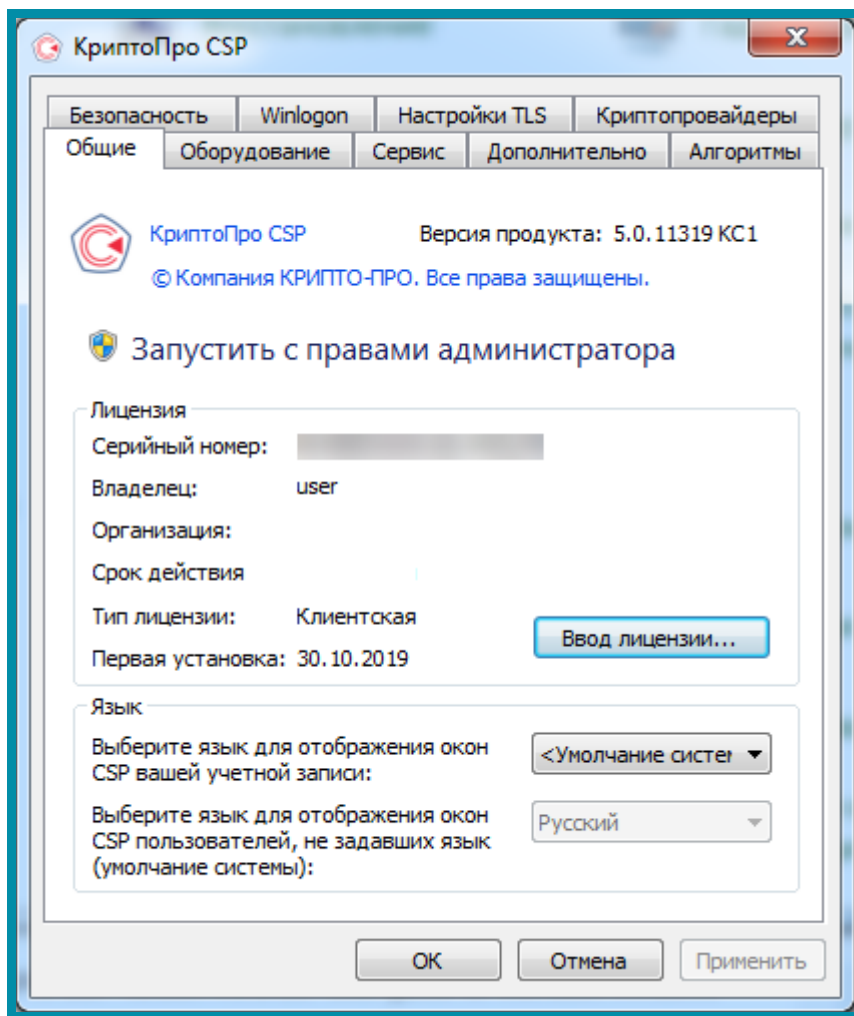


Рис. 3.1.2.1

Для регистрации программы нажмите кнопку **Ввод лицензии**. В открывшемся окне введите данные о владельце, серийный номер программы и нажмите **ОК** (рис. 3.1.2.2.).



*Демонстрационный период работы СКЗИ Крипто Про CSP составляет 90 дней. Для продолжения работы программы по истечении данного периода требуется ввод серийного номера, приобрести который Вы можете, обратившись в клиентскую службу.*

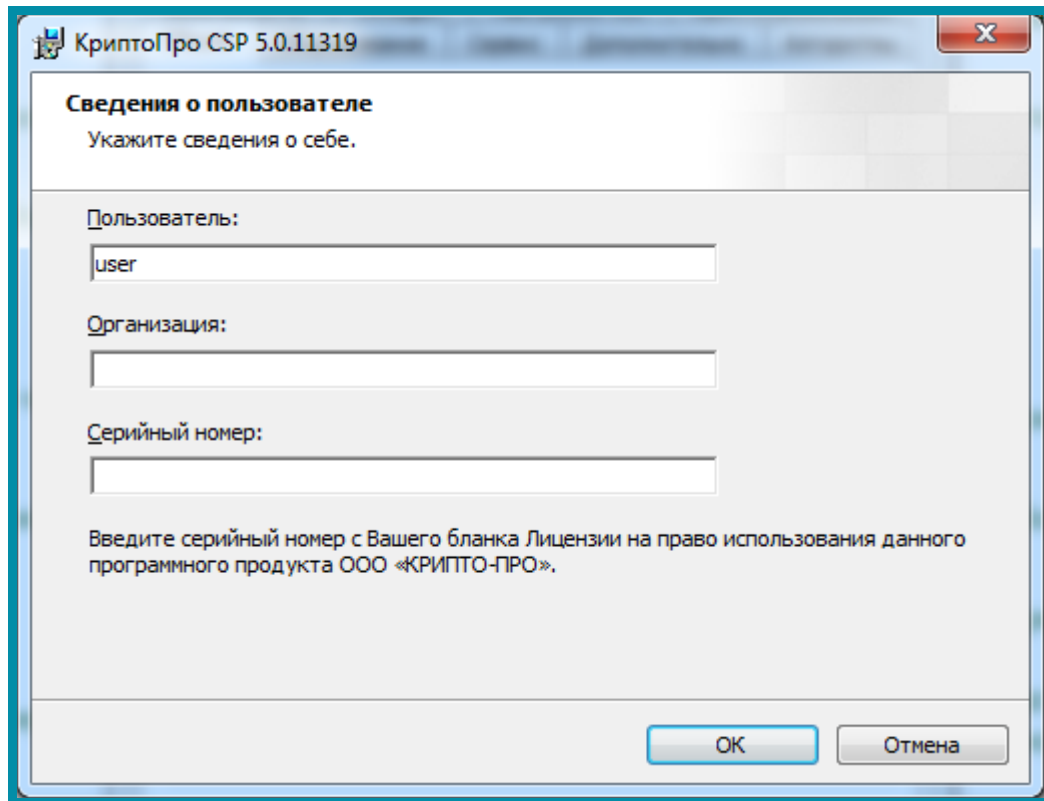


Рис. 3.1.2.2.

Сведения о лицензии отобразятся на вкладке **Общие**. Программное обеспечение СКЗИ КриптоПро CSP успешно установлено и настроено для дальнейшей работы (рис. 3.1.2.3.).

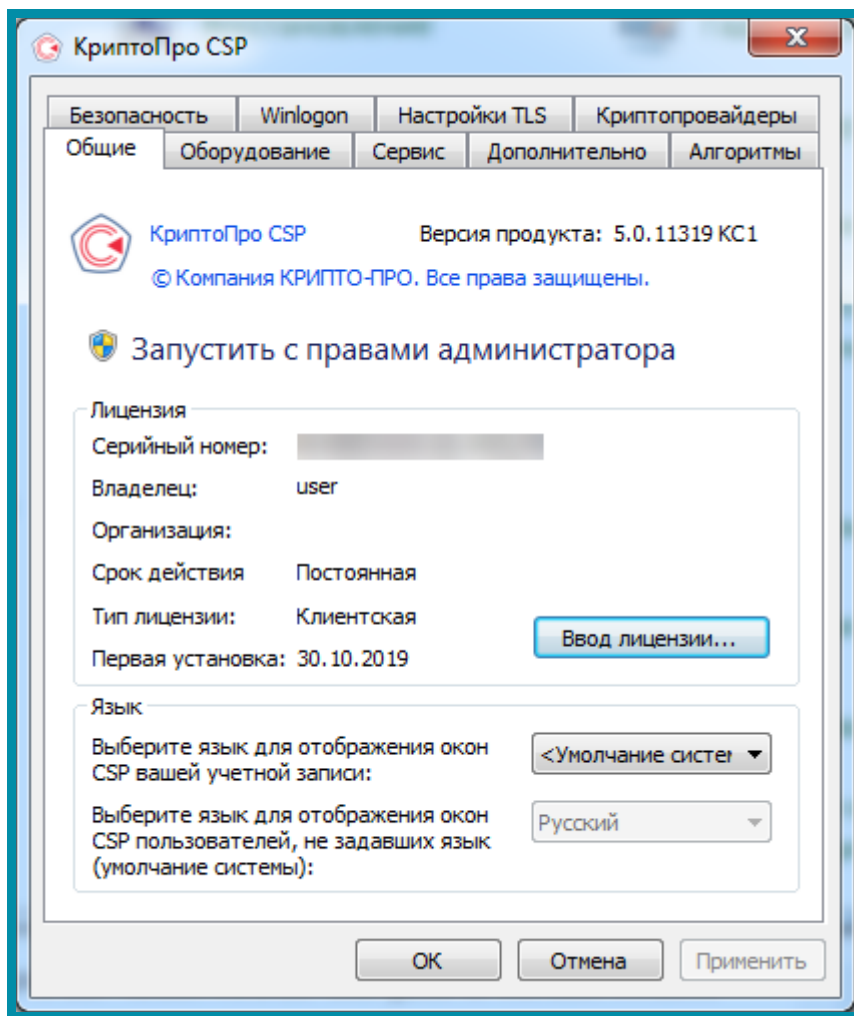


Рис. 3.1.2.3.

### 3.1.3. Установка СКЗИ ViPNet CSP



*С 1 января 2019 года для формирования электронной подписи на рабочем месте Вам необходимо будет иметь ViPNet CSP версии 4.2.*



*Перед установкой, переустановкой или удалением СКЗИ рекомендуется создать точку восстановления системы.*



*Установка двух СКЗИ может повлечь нестабильную работу операционной системы.*

Для установки программного обеспечения «ViPNet CSP» перейдите по ссылке <https://infotecs.ru/downloads/all>. Перед Вами появится список



дистрибутивов. Выберите необходимый дистрибутив в соответствии с версией и разрядностью Вашей операционной системы (рис. 3.1.3.1.).

Полнофункциональная версия	Версия	Размер
VIPNet CSP 4.2 Версия для Windows: 7(32/64-разрядная)/8 (64-разрядная)/8.1 (32/64-разрядная)/10 (32/64-разрядная) /2008 R2 64-разрядная)/2012 64-разрядная)/2012 R2 64-разрядная)/ Внимание! Криптопровайдер VIPNet CSP этой версии несовместим с антивирусным ПО Лаборатории Касперского. Рекомендуем использовать <a href="#">бета-версию</a> .	4.2 от 31.07.2018	32.35 Mb
VIPNet SysLocker (для варианта исполнения КСЗ) Версия для Windows: 7(32/64-разрядная)/ 8.1 (32/64-разрядная)/10 (32/64-разрядная) /Server 2008 R2 64-разрядная)/Server 2012 R2 (64-разрядная)/Server 2016 (64-разрядная)/	1.1 от 13.02.2019	10.93 Mb
VIPNet CSP 4 windows x32 rus Версия для ОС Windows XP Внимание! Данная версия не является сертифицированным СКЗИ и не предназначена для использования в системах ЮЗДО. Рекомендуем использовать CSP 4.2.	4 от 26.02.2014	21.31 Mb

Рис. 3.1.3.1.

Заполните нижеприведенную форму лицензионного соглашения и нажмите кнопку **Отправить заявку** (рис. 3.1.3.2.).

ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ С КОНЕЧНЫМ ПОЛЬЗОВАТЕЛЕМ НА ИСПОЛЬЗОВАНИЕ ПО VIPNET CSP

1. Определение понятий  
 1.1. Программа для ЭВМ – представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, а также эксплуатационная документация, предоставляемая в печатном и в электронном виде.  
 1.2. Программное обеспечение VipNet CSP (ПО) – программа для ЭВМ, производимая ОАО «ИнфоТеКС».  
 1.3. ОАО «ИнфоТеКС» (Правообладатель) – обладатель исключительных и имущественных авторских прав на ПО. Все авторские права на ПО защищены законодательством Российской Федерации о правах на результаты интеллектуальной деятельности. ПО является интеллектуальной собственностью ОАО «ИнфоТеКС».

Я согласен с условиями EULA \*

**Персональная информация**

ФИО полностью \*  
 Тестов Тест Тестович

Контактный e-mail \*  
 kozubova\_ma@astral.ru

**ОТПРАВИТЬ ЗАЯВКУ**

Рис. 3.1.3.2.

На указанную почту будет отправлено письмо со ссылкой на дистрибутив и серийным номером для регистрации продукта (рис. 3.1.3.3.).

На сайте компании [Инфотекс](#) 24.09.2019 15:41 была заполнена веб-форма на скачивание VipNet CSP 4.2 и указан [ваш e-мейл адрес](mailto:kozubova_ma@astral.ru) (kozubova\_ma@astral.ru).

Компания ИнфоТеКС благодарит за проявленный интерес к нашим продуктам

Данный продукт требует регистрации. Ваш серийный номер: **8WPH-EG8C-WWG4-XG3R**

Ваша ссылка на загрузку VipNet CSP 4.2: [https://files.infotecs.ru/dl/sess/vipnet\\_csp/full/330197582d94d086e17e59d496777040/vipnet\\_csp\\_4.2\\_cert.zip](https://files.infotecs.ru/dl/sess/vipnet_csp/full/330197582d94d086e17e59d496777040/vipnet_csp_4.2_cert.zip)

Размер загружаемого файла - 32.35 МБ, контрольная сумма файла дистрибутива (рассчитанная по алгоритму GOST R 34.11-2012/256) - DB7B9B970AFDA08E75F9BDC2C0790857B7401E5AA721446BE3F18A850527B78E

Для проверки контрольной суммы воспользуйтесь утилитой [VipNet HashCalc](#)

Внимание! Ссылка будет действительна в течение 5 дней с момента заполнения формы на скачивание файла!

Рис. 3.1.3.3.

Полученный серийный номер необходим для регистрации программного продукта VipNet CSP после его установки.

Перейдите по ссылке для скачивания программного продукта и запустите загруженный файл Setup.exe. После его запуска перед Вами откроется окно подготовки к установке приложения VipNet (рис. 3.1.3.4.).

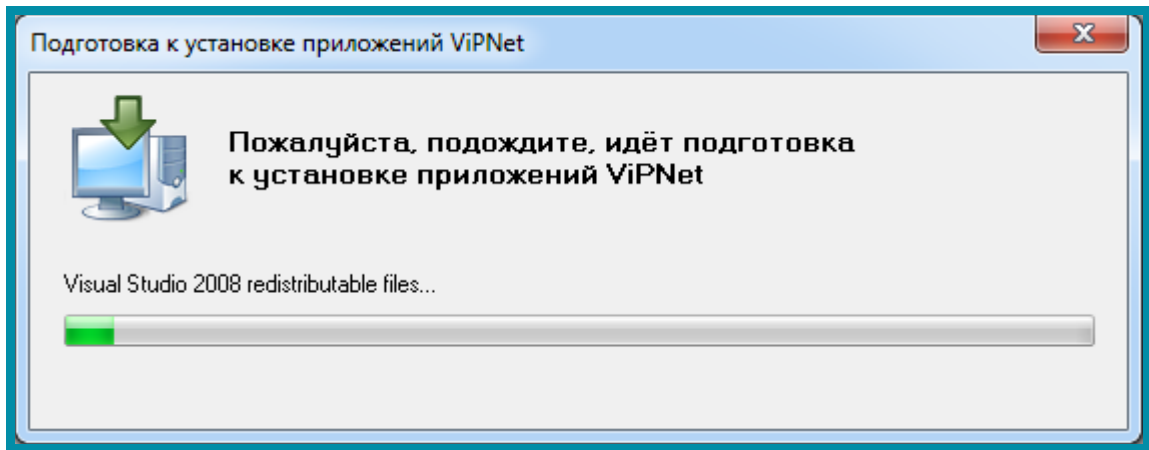


Рис. 3.1.3.4.

В окне **Способ установки** (рис. 3.1.3.5.) нажмите кнопку **Установить сейчас**.

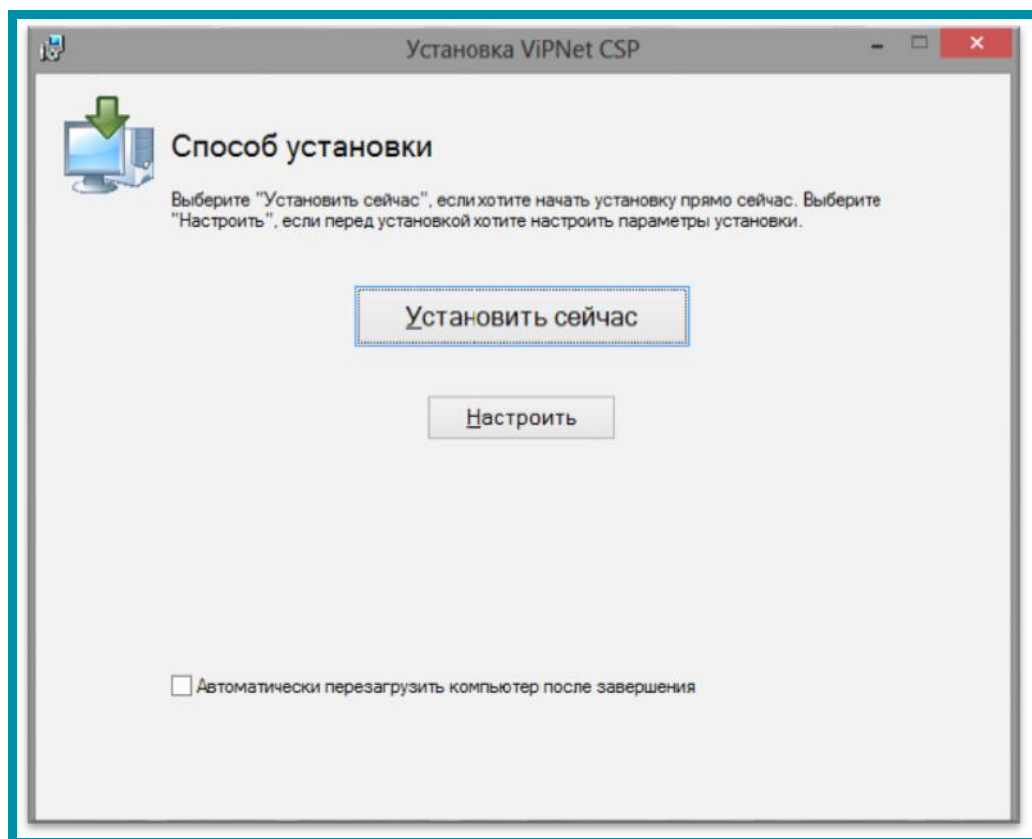


Рис. 3.1.3.5.

Начнется установка программного продукта ViPNet CSP (рис. 3.1.3.6.).

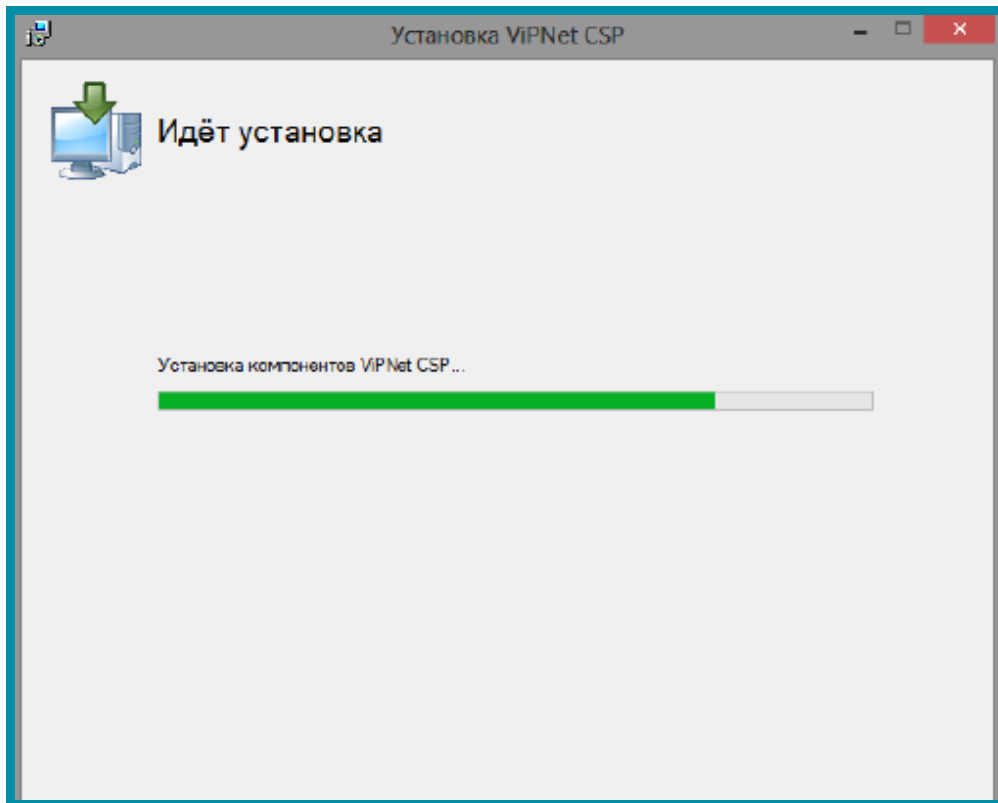


Рис. 3.1.3.6.

Программа сообщит об окончании установки СКЗИ ViPNet CSP, нажмите кнопку **Закреть** (рис. 3.1.3.7.).

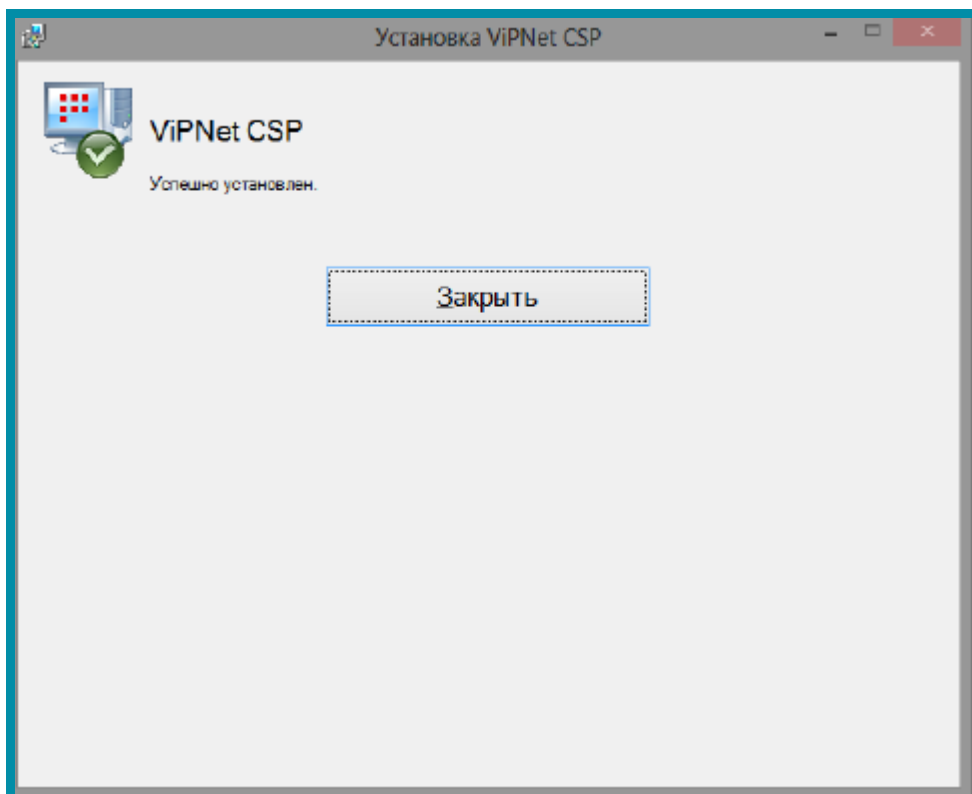


Рис. 3.1.3.7.

По окончании установки необходимо перезагрузить компьютер. Вы можете сделать это сразу, для этого нажмите кнопку **Да** (рис. 3.1.3.8.). Если Вы нажмете **Нет**, то перезагрузка компьютера отложится, Вам нужно будет перезагрузить компьютер вручную.

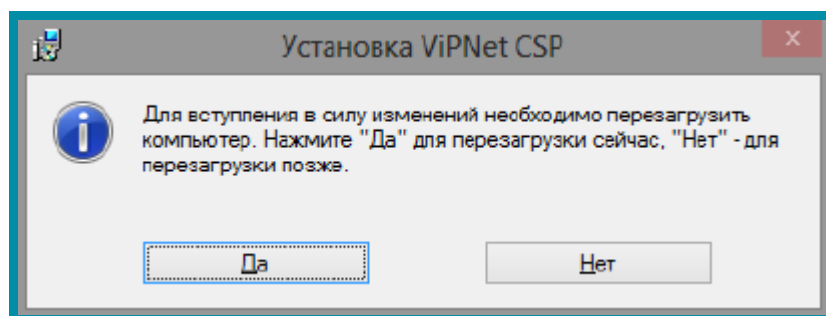


Рис. 3.1.3.8.

### 3.1.4. Регистрация СКЗИ ViPNet CSP

Настройка СКЗИ ViPNet CSP включает в себя регистрацию продукта. После перезагрузки компьютера перейдите в «Пуск» – «Все программы» – «ViPNet» – «ViPNet CSP» (рис. 3.1.4.1.).

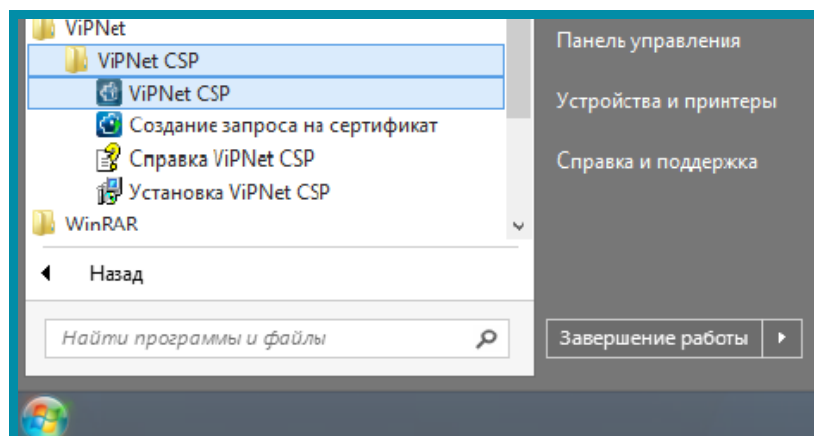


Рис. 3.1.4.1.

Перед Вами откроется окно следующего вида (рис. 3.1.4.2.), выберите пункт **Зарегистрировать ViPNet CSP** и нажмите кнопку **Далее**.

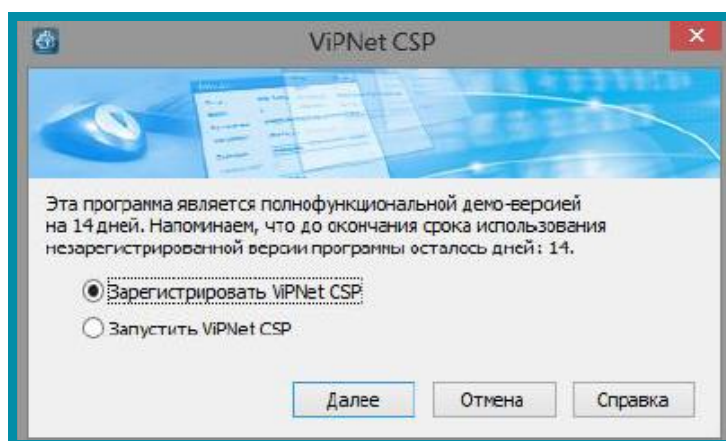


Рис. 3.1.4.2.

В следующем окне выберите пункт **Запрос на регистрацию (получить код регистрации)** и нажмите кнопку **Далее** (рис. 3.1.4.3.).

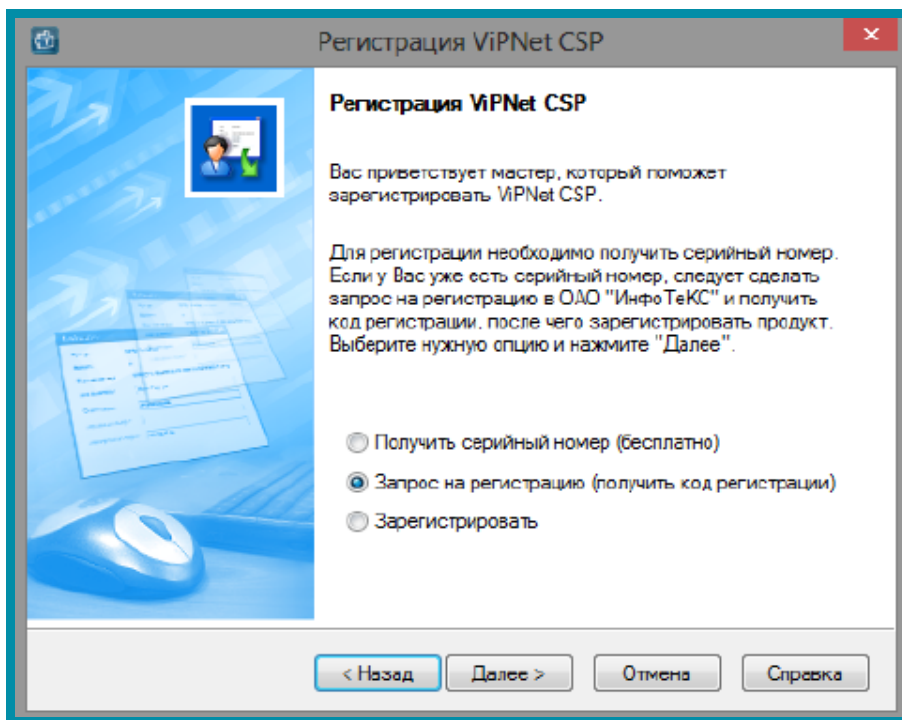


Рис. 3.1.4.3.

В окне **Способ запроса на регистрацию** (рис. 3.1.4.4.) выберите пункт **Через Интернет (online)**. При этом Ваш компьютер должен быть подключен к Интернету. Нажмите кнопку **Далее**.

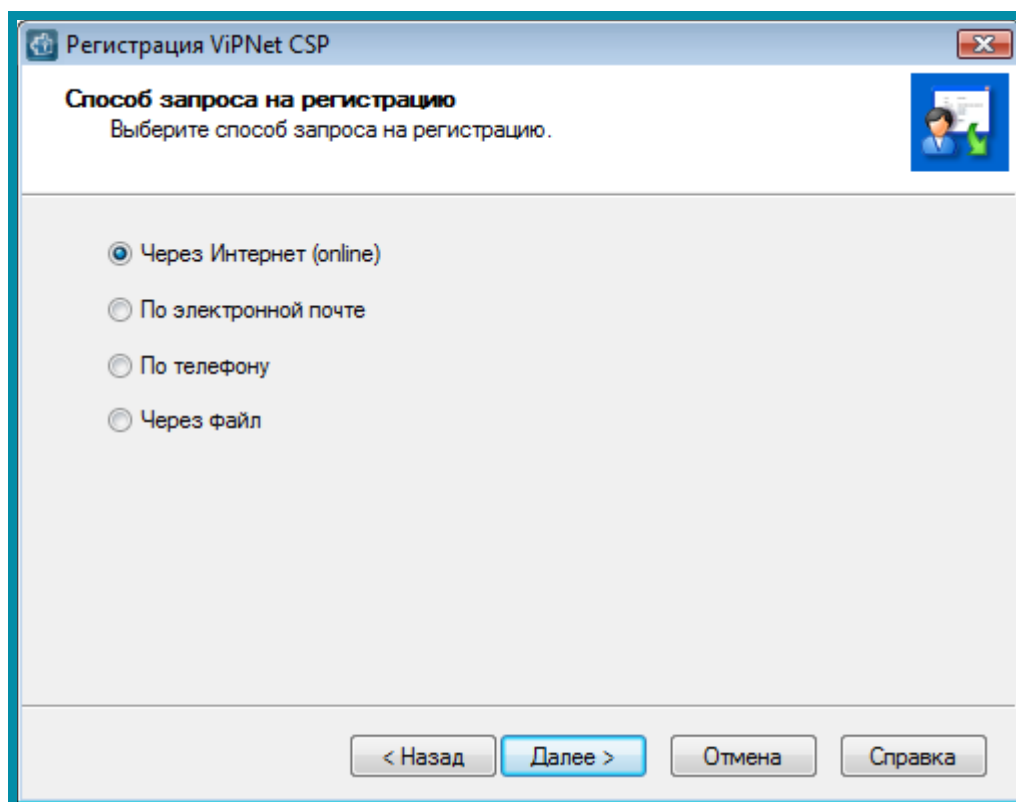
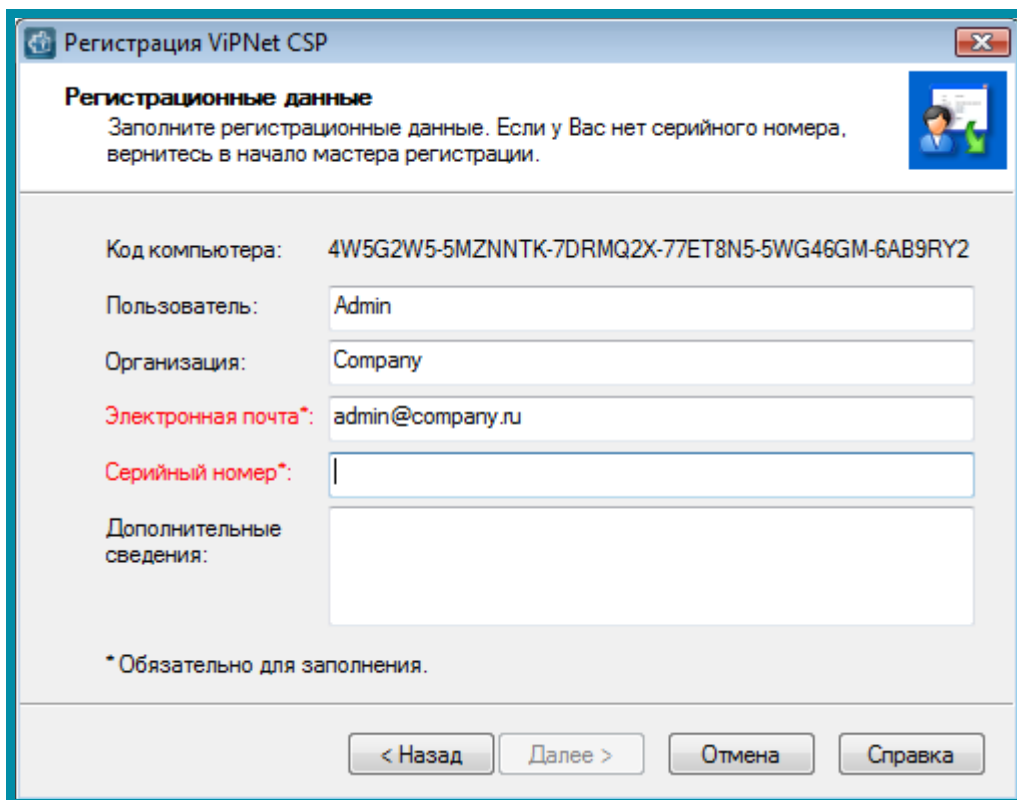


Рис. 3.1.4.4.

В окне **Регистрационные данные** (рис. 3.1.4.5.) заполните все поля и введите Ваш серийный номер для ViPNet CSP. Нажмите кнопку **Далее**.



The screenshot shows a window titled "Регистрация ViPNet CSP" with a close button in the top right corner. Below the title bar, the text "Регистрационные данные" is displayed, followed by instructions: "Заполните регистрационные данные. Если у Вас нет серийного номера, вернитесь в начало мастера регистрации." To the right of this text is a small icon of a person with a green checkmark. The main area contains several input fields: "Код компьютера:" with the value "4W5G2W5-5MZNNTK-7DRMQ2X-77ET8N5-5WG46GM-6AB9RY2"; "Пользователь:" with "Admin"; "Организация:" with "Company"; "Электронная почта\*:" with "admin@company.ru"; "Серийный номер\*:" which is empty; and "Дополнительные сведения:" which is a large empty text area. At the bottom left, there is a note: "\* Обязательно для заполнения." At the bottom right, there are four buttons: "< Назад", "Далее >", "Отмена", and "Справка".

Рис. 3.1.4.5.

Если регистрация прошла успешно, программа установки сообщит об этом (рис. 3.1.4.6.). Нажмите кнопку **Готово**.

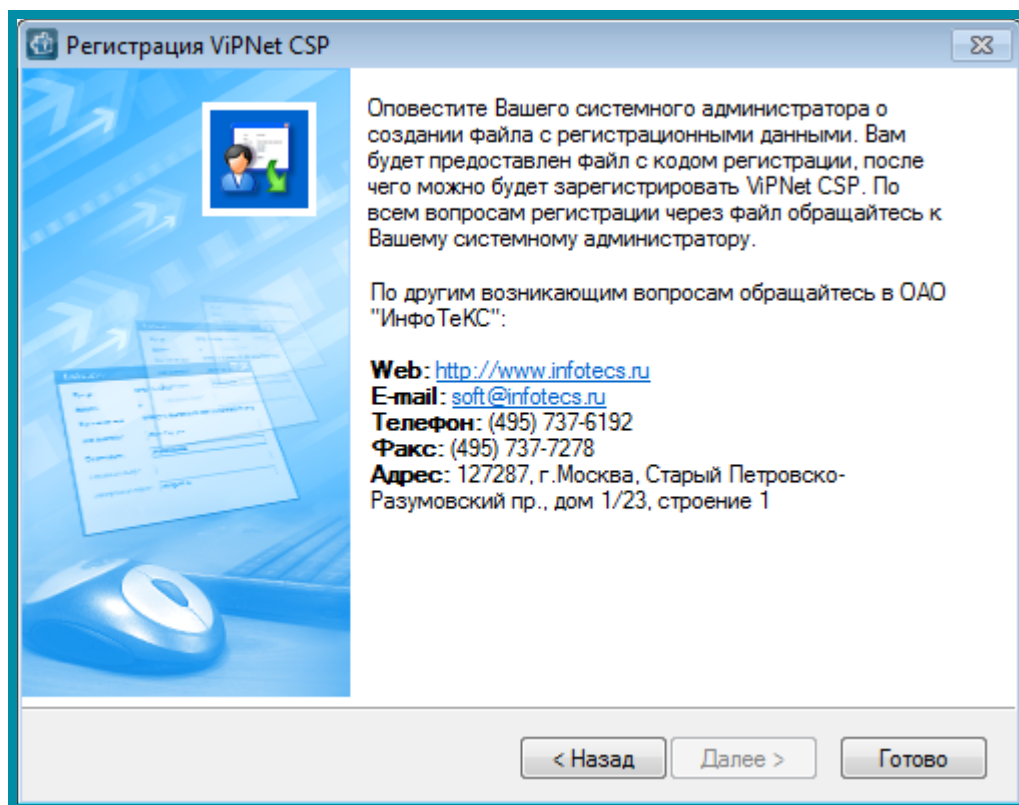


Рис. 3.1.4.6.

## 3.2. Установка драйверов носителей

### 3.2.1. Установка драйверов JaCarta

Для работы с носителем JaCarta необходима установка на рабочее место Пользователя специального программного обеспечения – программы Единый Клиент JaCarta и JaCarta SecurLogon.

Перейдите по ссылке <http://www.aladdin-rd.ru/support/downloads/jacarta/> и выберите программу ПК Единый Клиент JaCarta 2.12 (бета) в соответствии с разрядностью Вашей операционной системы (рис. 3.2.1.1.).



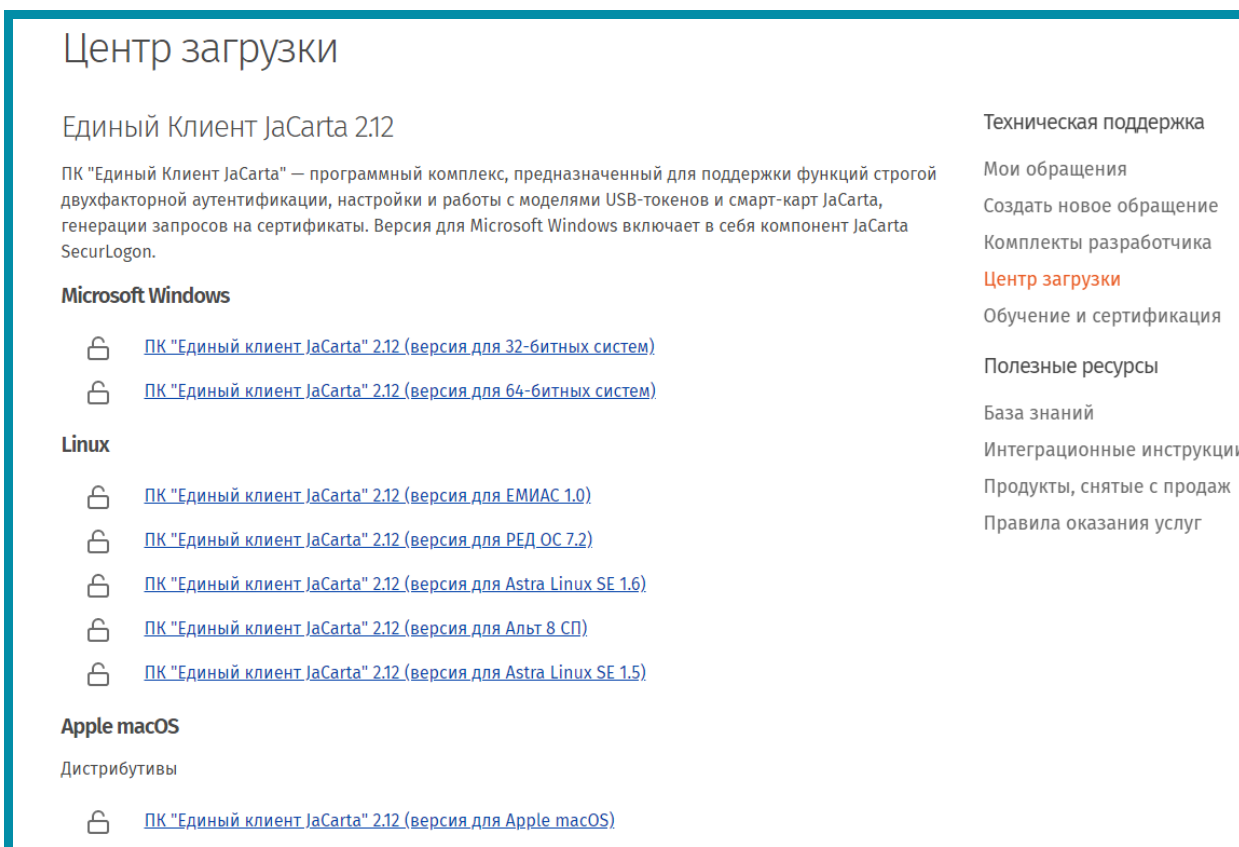


Рис. 3.2.1.1.

При нажатии на ссылку откроется новое окно, здесь нажмите **Скачать** (рис. 3.2.1.2.).

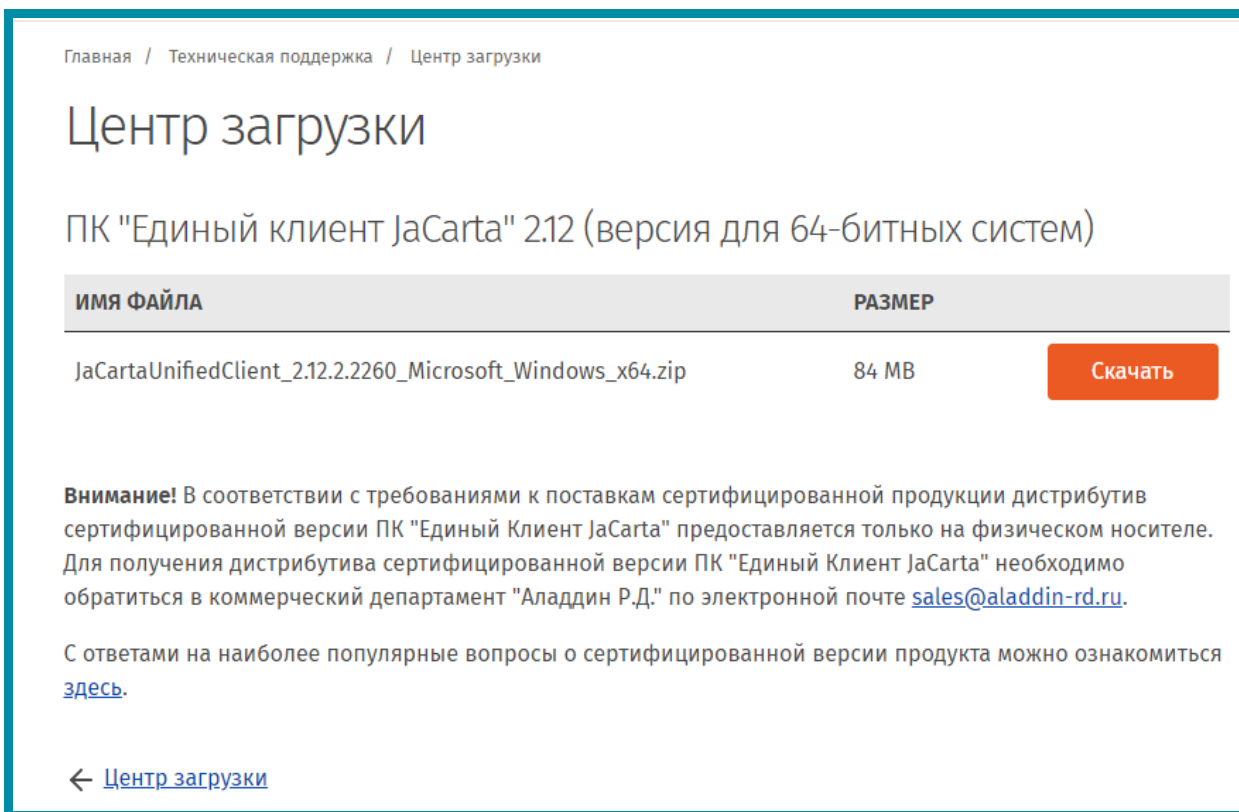


Рис. 3.2.1.2.

В окне приветствия Мастера установки нажмите кнопку **Далее** (рис. 3.2.1.3).

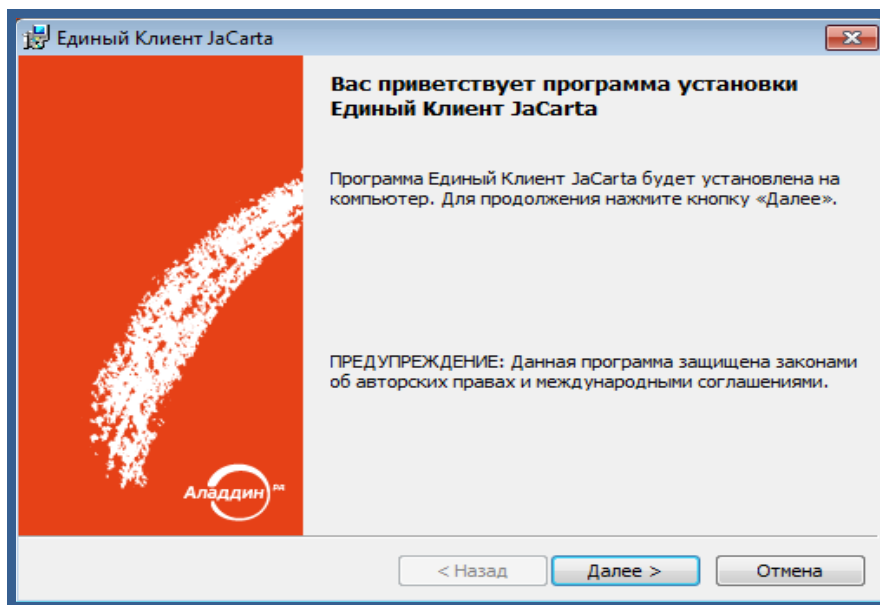


Рис. 3.2.1.3.

Ознакомьтесь с текстом Лицензионного соглашения. В случае если Вы согласны с его условиями, установите переключатель в положение **Я принимаю условия лицензионного соглашения** и нажмите кнопку **Далее** (рис. 3.2.1.4).

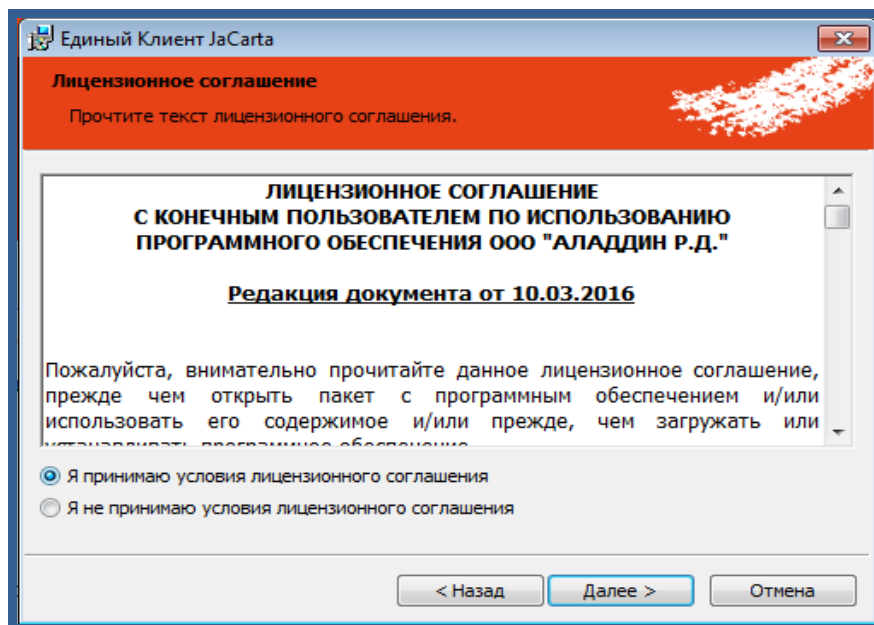


Рис. 3.2.1.4.

В следующем окне установите переключатель вида установки в положение **Стандартная**, выберите директорию установки программы либо оставьте значение директории по умолчанию (рекомендуется) и нажмите кнопку **Далее** (рис. 3.2.1.5).

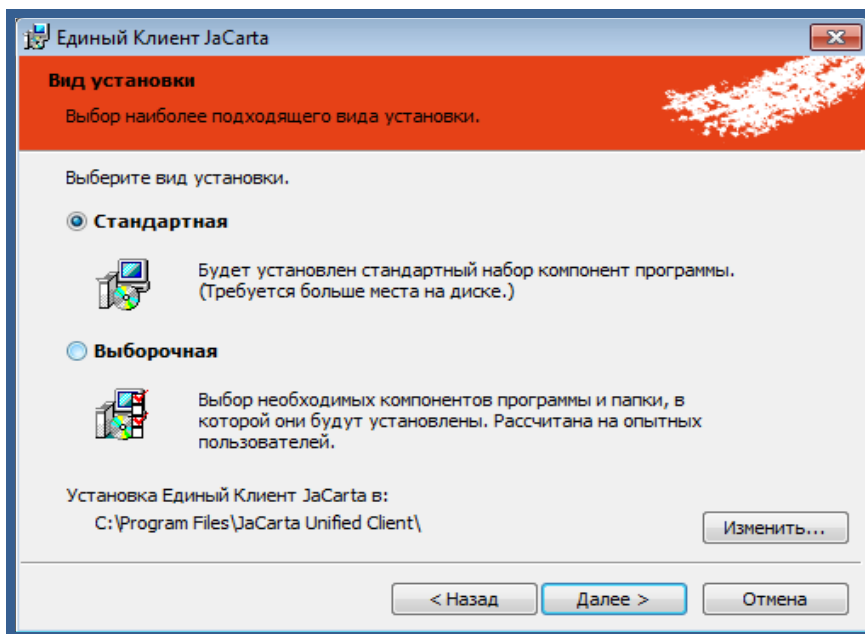


Рис. 3.2.1.5.

В следующем окне нажмите кнопку **Установить** (рис. 3.2.1.6.).

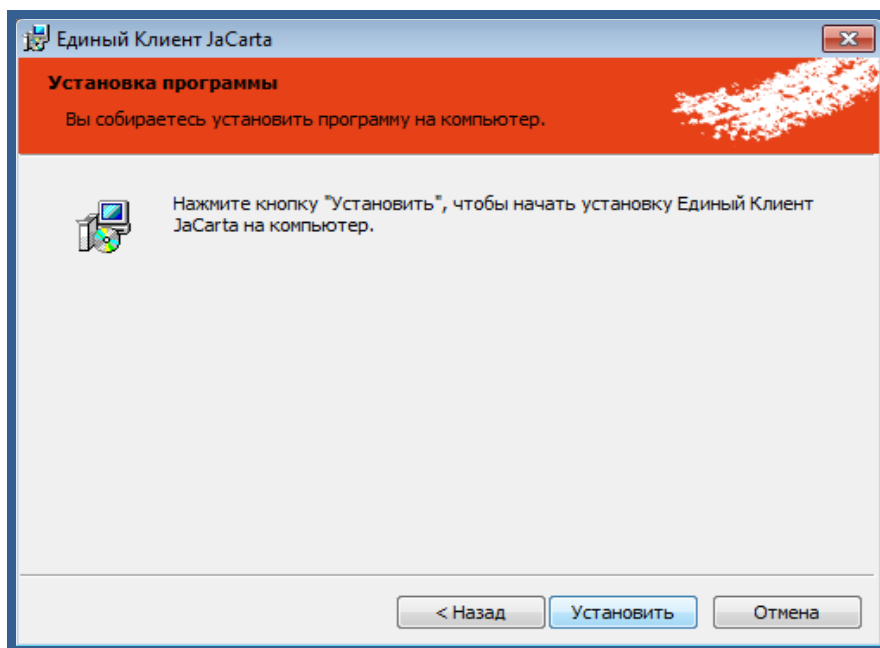
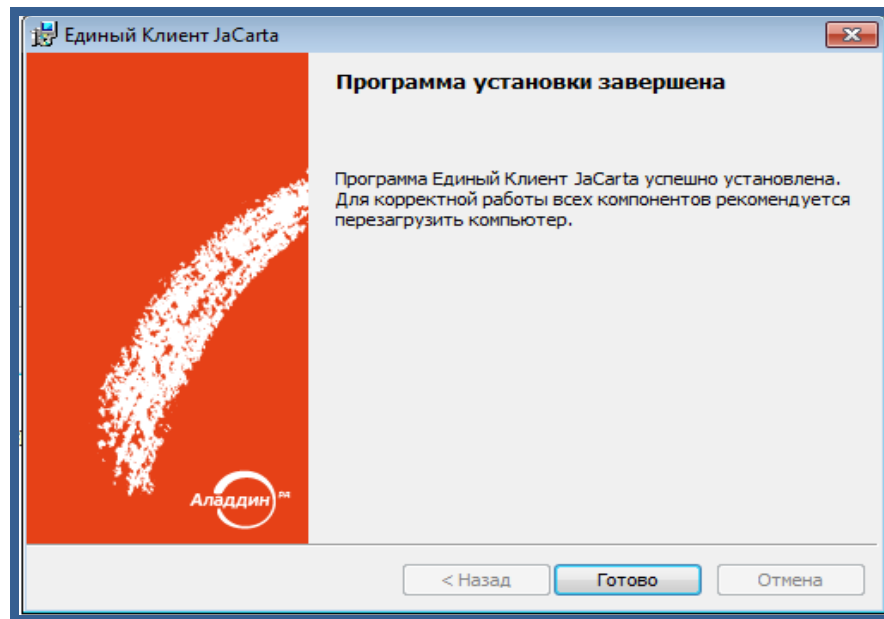


Рис. 3.2.1.6.

После завершения установки нажмите кнопку **Готово** (рис. 3.2.1.7.).



*Рис. 3.2.1.7.*

Перезагрузите компьютер.

### 3.2.1.1. Интерфейс Единого клиента JaCarta и JaCarta SecurLogon

Чтобы открыть программу выполните Пуск -> папка Аладдин Р.Д. -> Единый клиент JaCarta (*рис. 3.2.1.1.1.*).

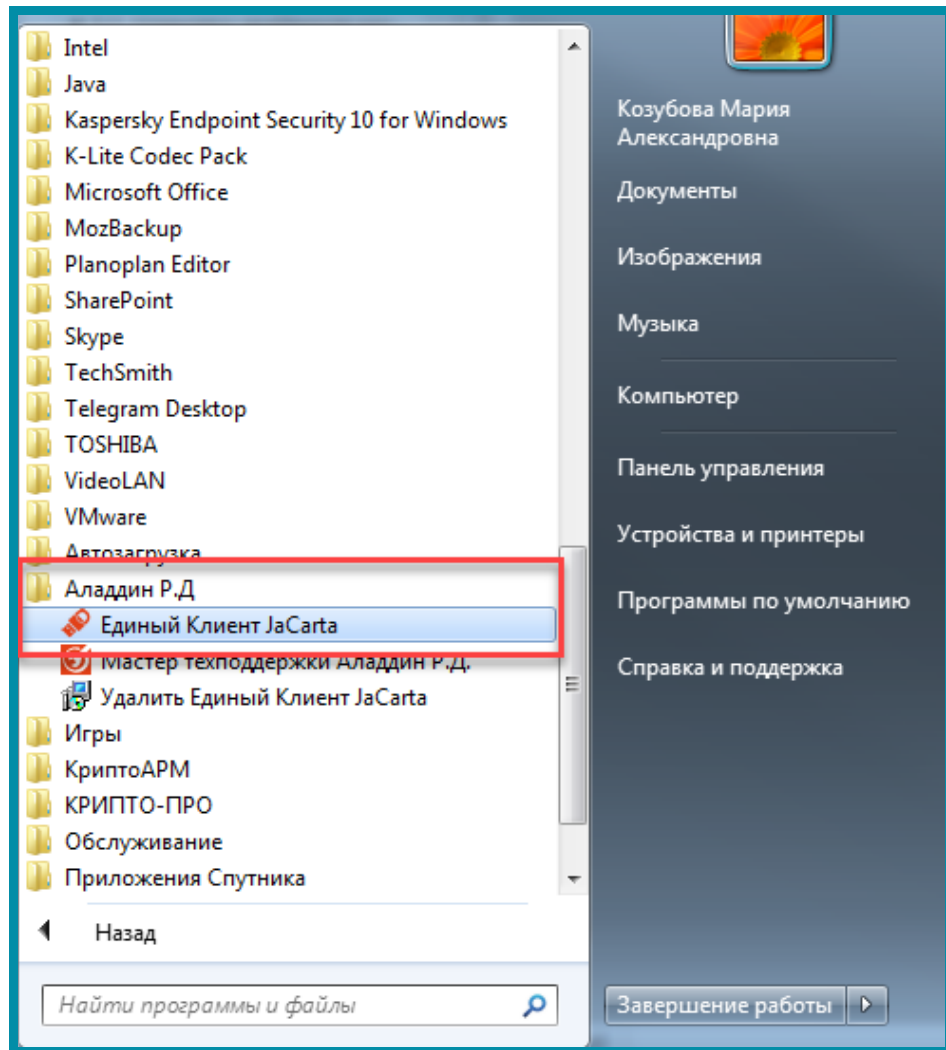


Рис. 3.2.1.1.1.

В верхней части левой панели отображаются подсоединенные к компьютеру электронные ключи. Значок электронного ключа зависит от типа этого электронного ключа (рис. 3.2.1.1.2.).

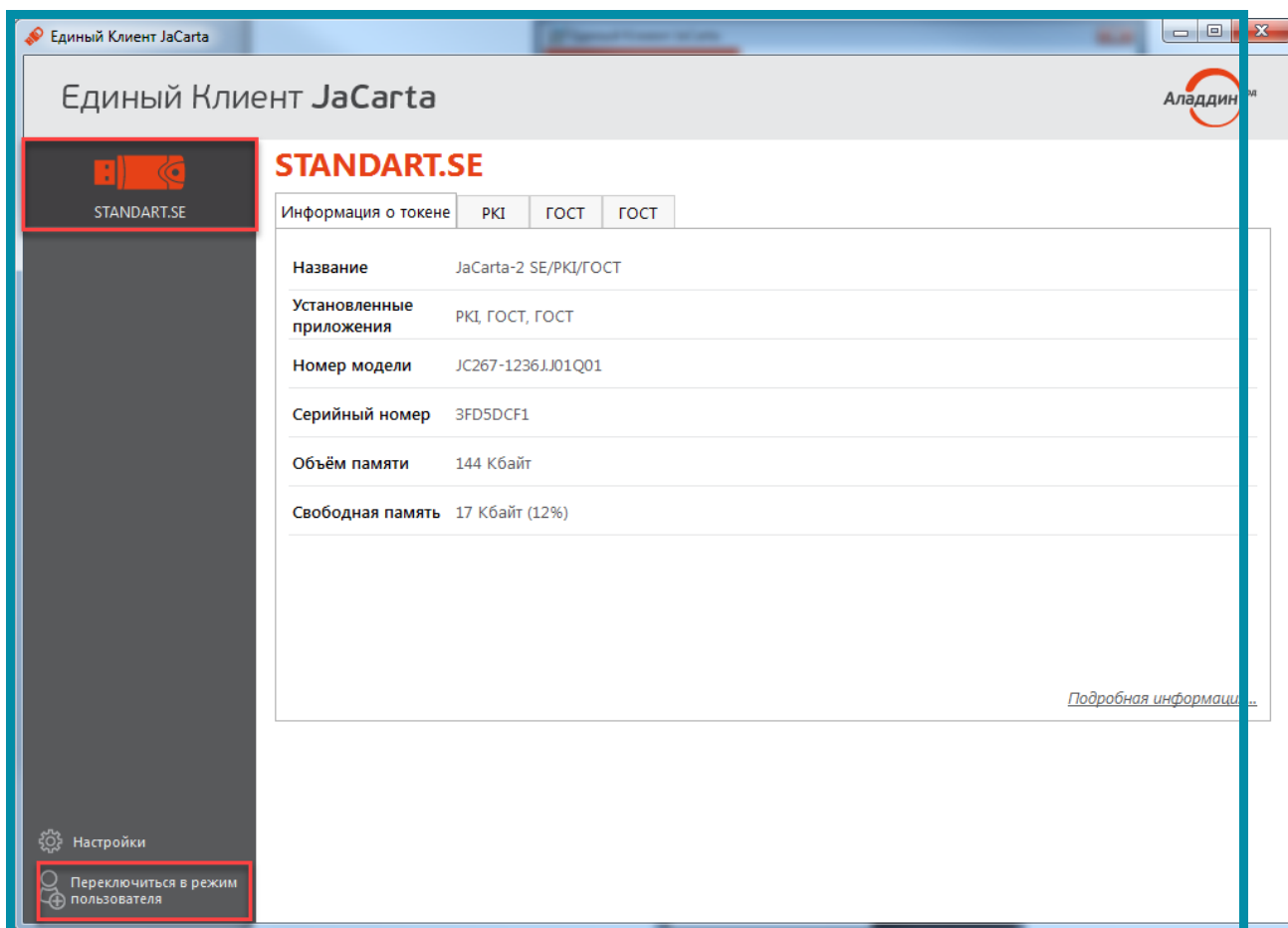


Рис. 3.2.1.1.2.

В нижнем левом углу окна программы доступны функции настройки и переключения в режим Администратора/Пользователя.

### 3.2.1.2. Особенности работы с Единым клиентом JaCarta

По умолчанию на носители JaCarta устанавливается ПИН-код 1234567890. Предусмотрена возможность смены стандартного ПИН-кода.

Носитель JaCarta работает только с СКЗИ КриптоПро CSP 3.6.7777 (предыдущие версии не отображает контейнеров).

После установки программы Единый Клиент JaCarta установка на это же рабочее место JC-Client не допускается.

При переустановке JC-Client после удаления программы Единый Клиент JaCarta необходимо перезагрузить компьютер.

### 3.2.2. Установка драйверов RuToken

Для работы с носителем Рутокен необходима установка на рабочее место соответствующих драйверов. Для установки произведите следующие действия.

Перейдите по ссылке <http://www.rutoken.ru/support/download/drivers-for-windows/> и скачайте драйвер (рис. 3.2.2.1).



Рис. 3.2.2.1.

Ознакомьтесь с лицензионным соглашением установите флажок «Условия Лицензионного соглашения прочитаны...» и нажмите **Условия приняты** (рис. 3.2.2.2.).

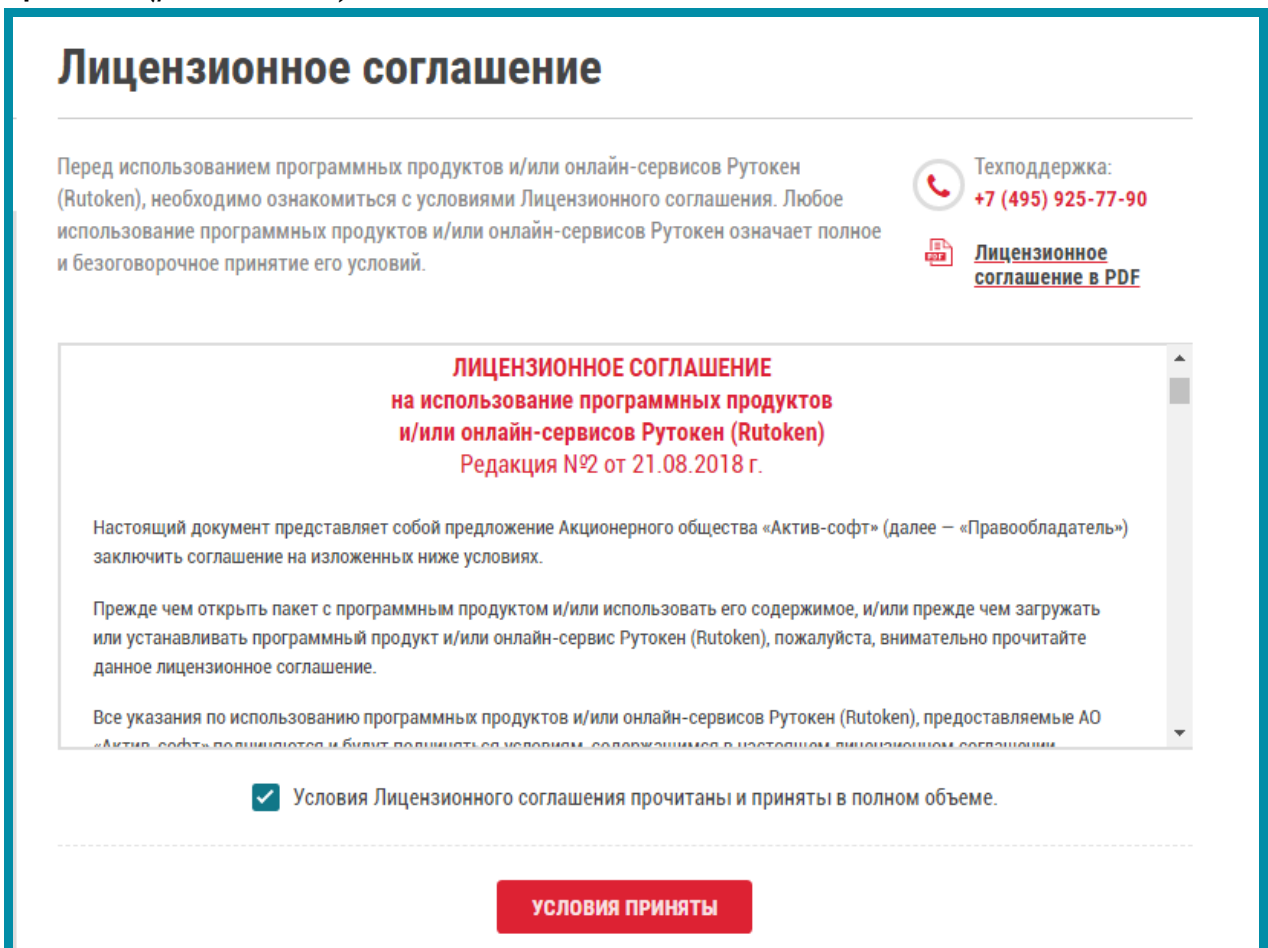


Рис. 3.2.2.2.



Для корректной установки драйвера необходимы права Администратора системы.

Когда дистрибутив будет скачен отсоедините Рутокен от USB-порта компьютера, запустите программу установки и нажмите кнопку **Установить** (рис. 3.2.2.3.).

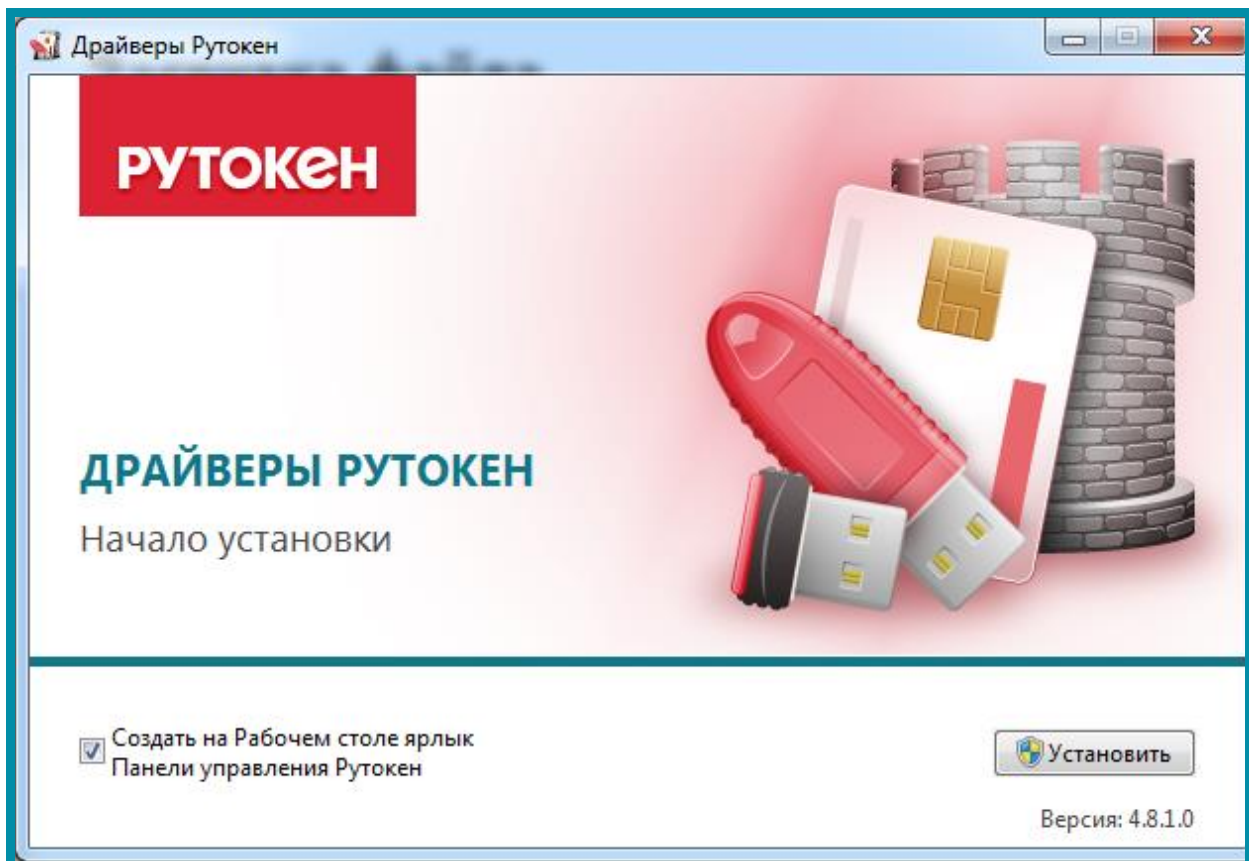


Рис. 3.2.2.3.

После начала установки может потребоваться перезагрузка компьютера. После перезагрузки программа продолжит установку автоматически. Дождитесь окончания установки драйверов (рис. 3.2.2.4.).



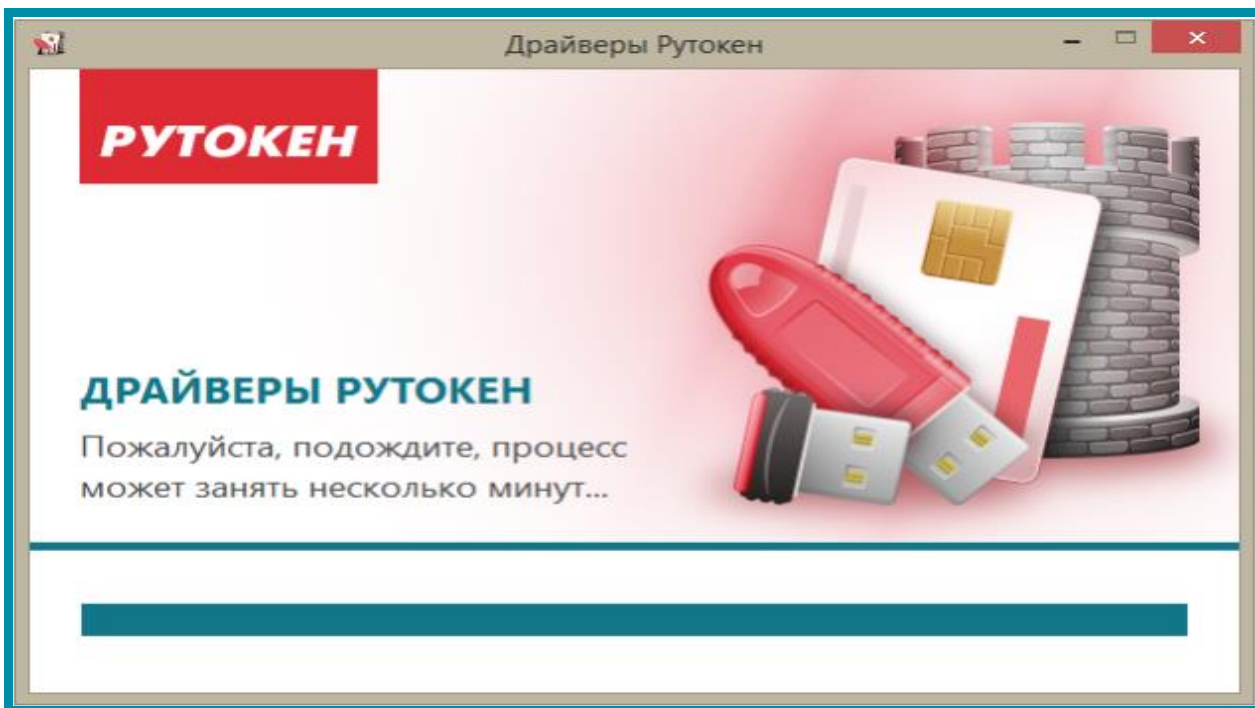


Рис. 3.2.2.4.

После завершения установки драйвера вставьте РуТокен в USB-порт компьютера. Рутокен определится, после чего система установит для него драйвер (рис. 3.2.2.5.).

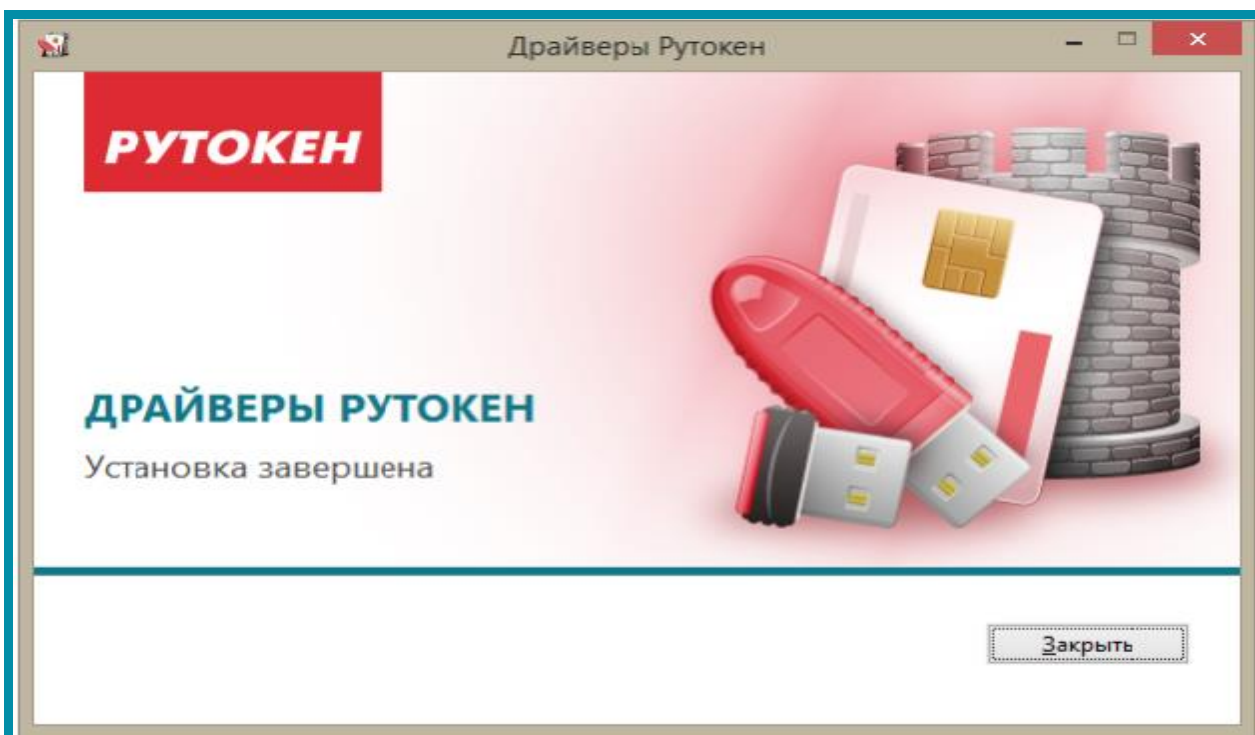


Рис. 3.2.2.5.

Определить корректность работы носителя Рутокен можно по светодиоду либо в панели управления Рутокен. Для этого откройте программу и на вкладке «Сертификаты» в пункте «Считыватели Рутокен» будет отображаться устройство (рис. 3.2.2.6.).



При каком-либо действии с носителем Рутокен программа запрашивает пароль. Пароль по умолчанию 12345678.

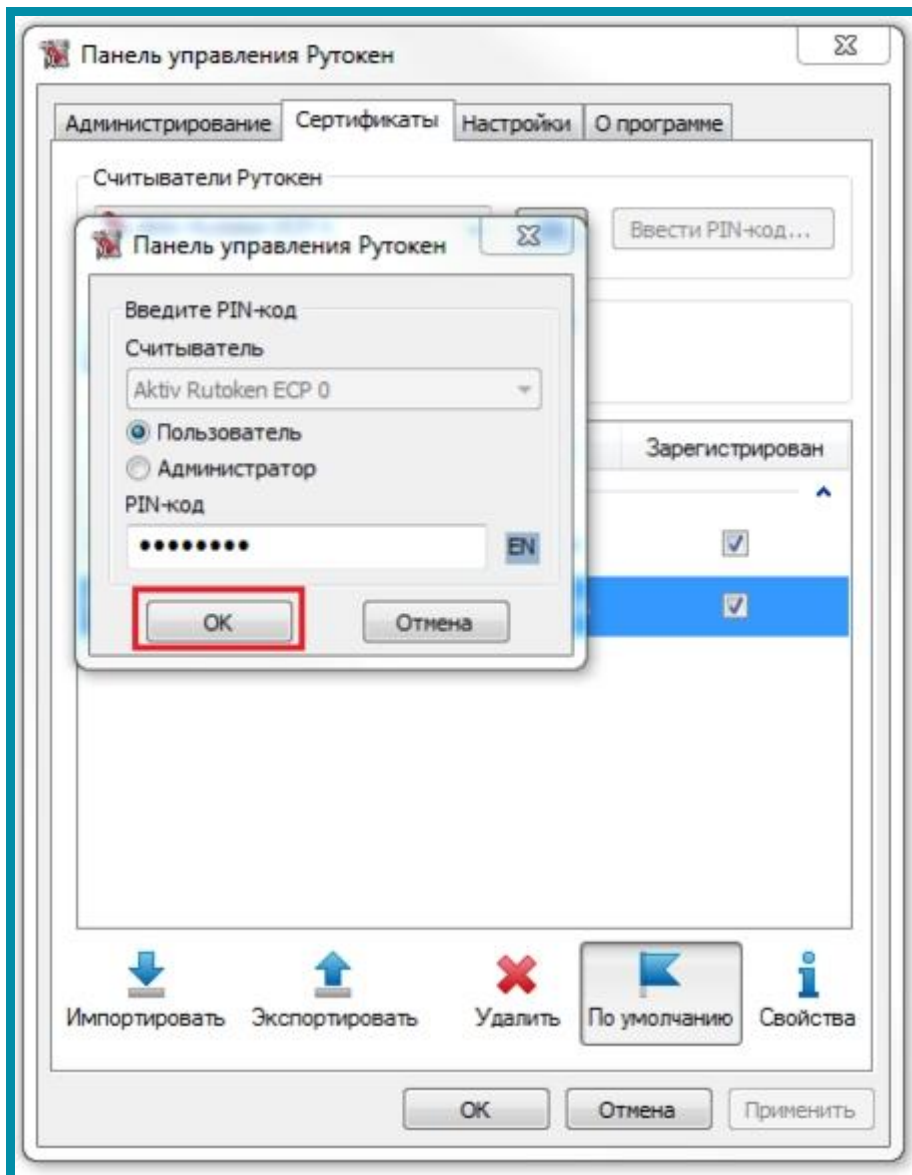


Рис. 3.2.2.6.

Рутокен одинаково корректно работает с СКЗИ ViPNet CSP и КриптоПро CSP при наличии установленного драйвера.

### 3.2.3. Настройка считывателей в СКЗИ КриптоПро CSP

Вставьте защищенный носитель в USB-порт Вашего компьютера.

Перейдите в пункт меню Пуск – Настройка – Панель управления и запустите СКЗИ КриптоПро CSP.

В открывшемся окне перейдите на вкладку «Оборудование» и нажмите кнопку **Настроить считыватели...** (рис. 3.2.3.1.).

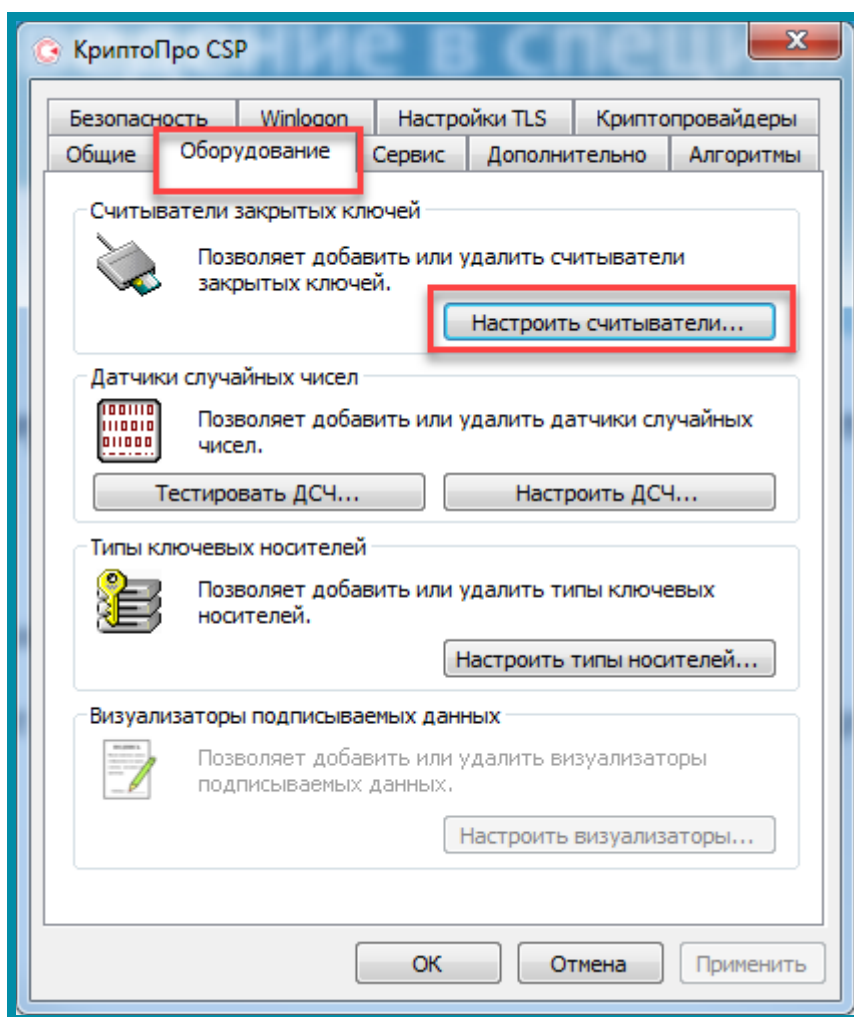


Рис. 3.2.3.1.

Перед Вами откроется окно со списком установленных считывателей (рис. 3.2.3.2.). В случае если в списке нет считывателя «Все считыватели смарт-карт», нажмите кнопку **Добавить**.

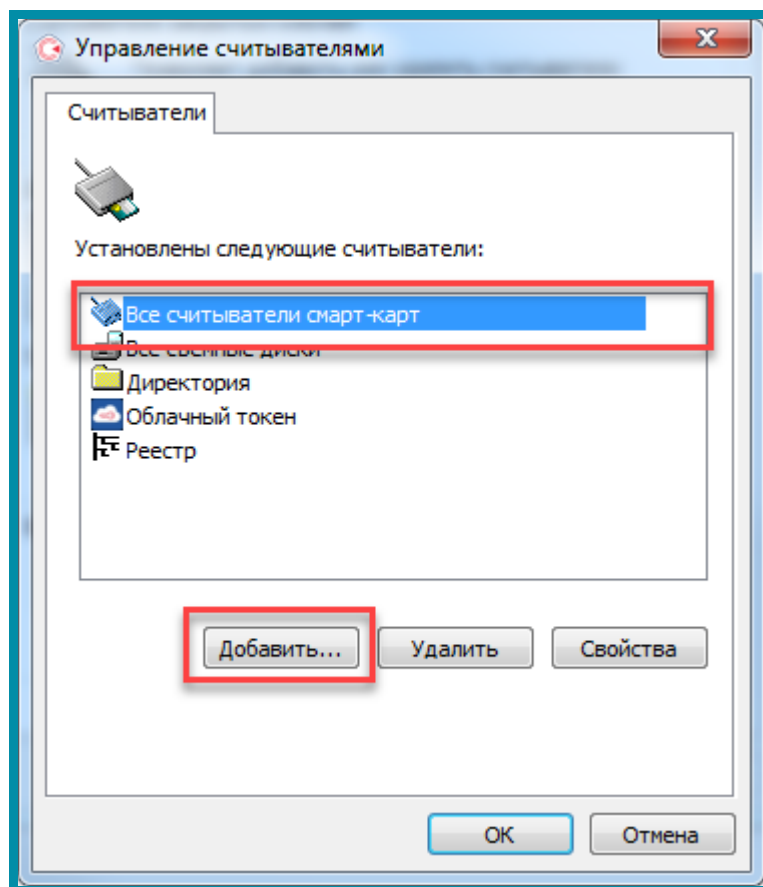


Рис. 3.2.3.2.



*В случае если кнопка «Добавить» неактивна, перейдите на вкладку «Общие» и нажмите ссылку **Запустить с правами администратора**.*

В открывшемся окне выберите пункт «Все считыватели смарт-карт» и нажмите кнопку **Далее** (рис. 3.2.3.3.).

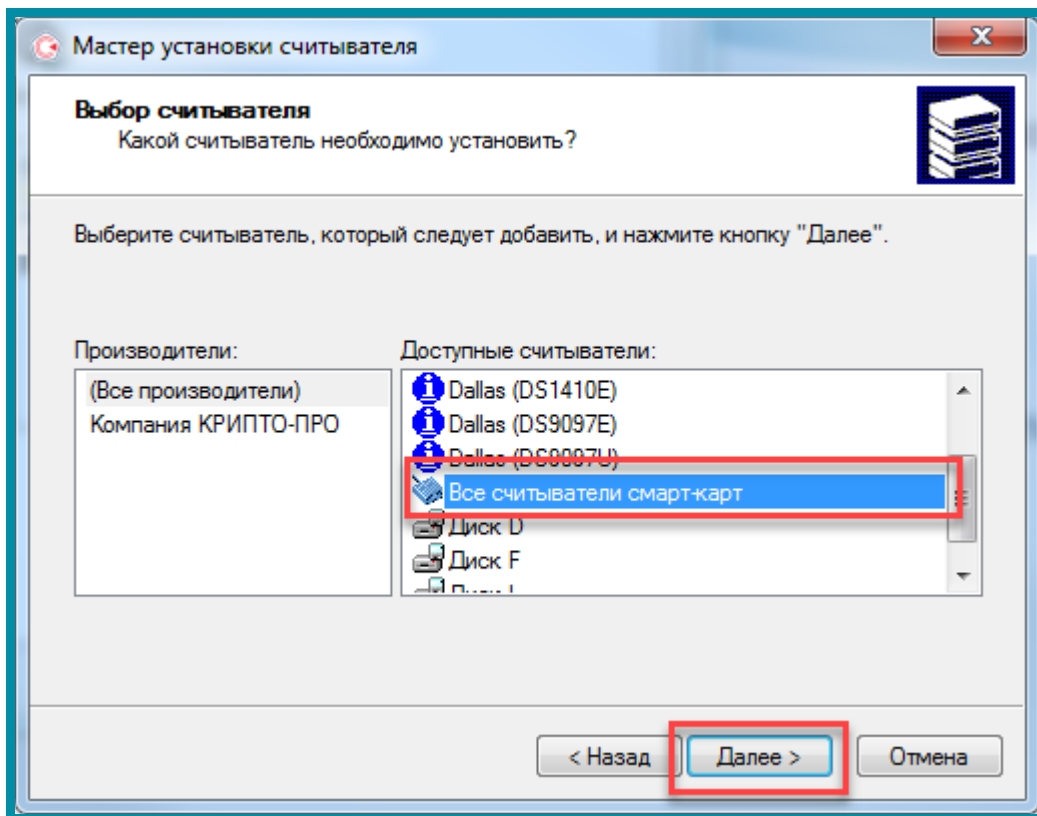


Рис. 3.2.3.3.

Для продолжения установки нажмите кнопку **Далее** (рис. 3.2.3.4.).

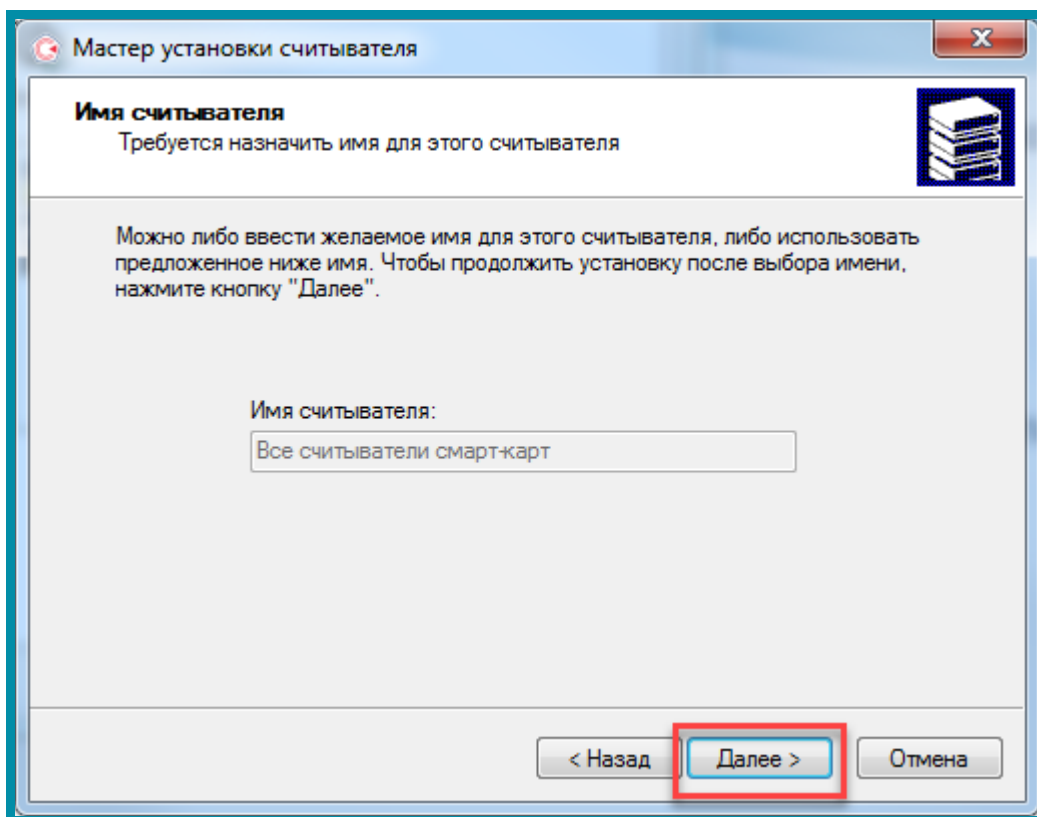


Рис. 3.2.3.4.

После установки в Вашем списке появится считыватель «Все считыватели смарт-карт». Нажмите кнопку **Готово**.

На вкладке «Оборудование» нажмите кнопку **Настроить типы носителей**. В следующем окне проверьте наличие необходимого носителя и нажмите кнопку **ОК** (рис. 3.2.3.5).

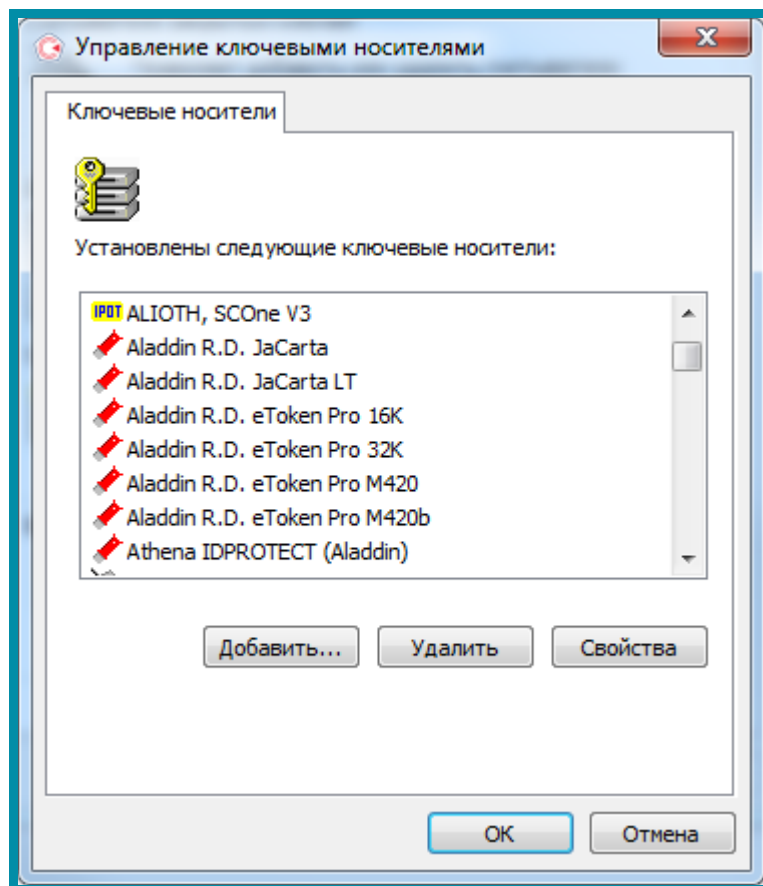


Рис. 3.2.3.5.



*В случае если в окне «Управление ключевыми носителями» нет необходимого носителя, нажмите кнопку **Добавить** и добавьте его.*

Настройка считывателя завершена.

### 3.3. Установка сертификатов

#### 3.3.1. Установка сертификатов Крипто ПРО CSP

Для установки сертификатов перейдите в пункт меню «Пуск» – «КРИПТО-ПРО» – «КриптоПро CSP» (рис. 3.3.1.1.).

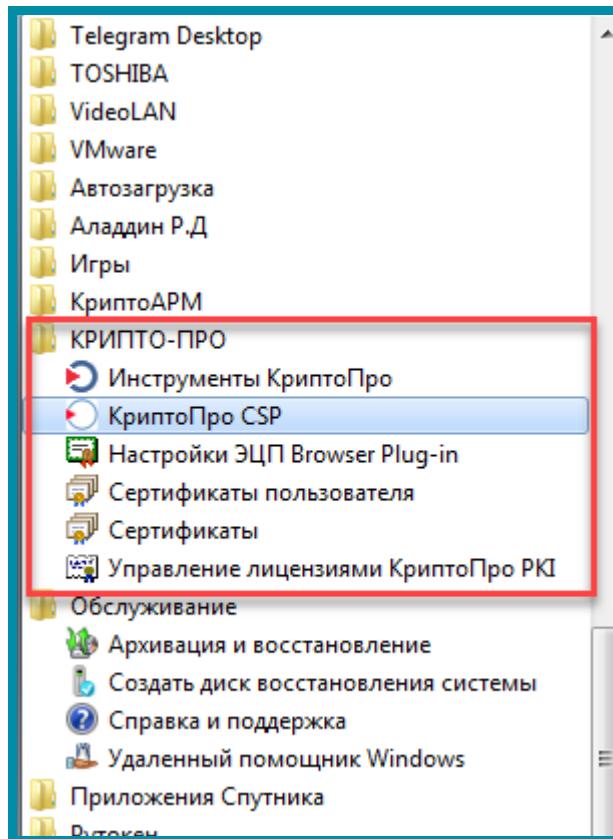


Рис. 3.3.1.1.

После запуска СКЗИ КриптоПро CSP перейдите на вкладку «Сервис» и нажмите кнопку **Просмотреть сертификаты в контейнере** (рис. 3.3.1.2.).

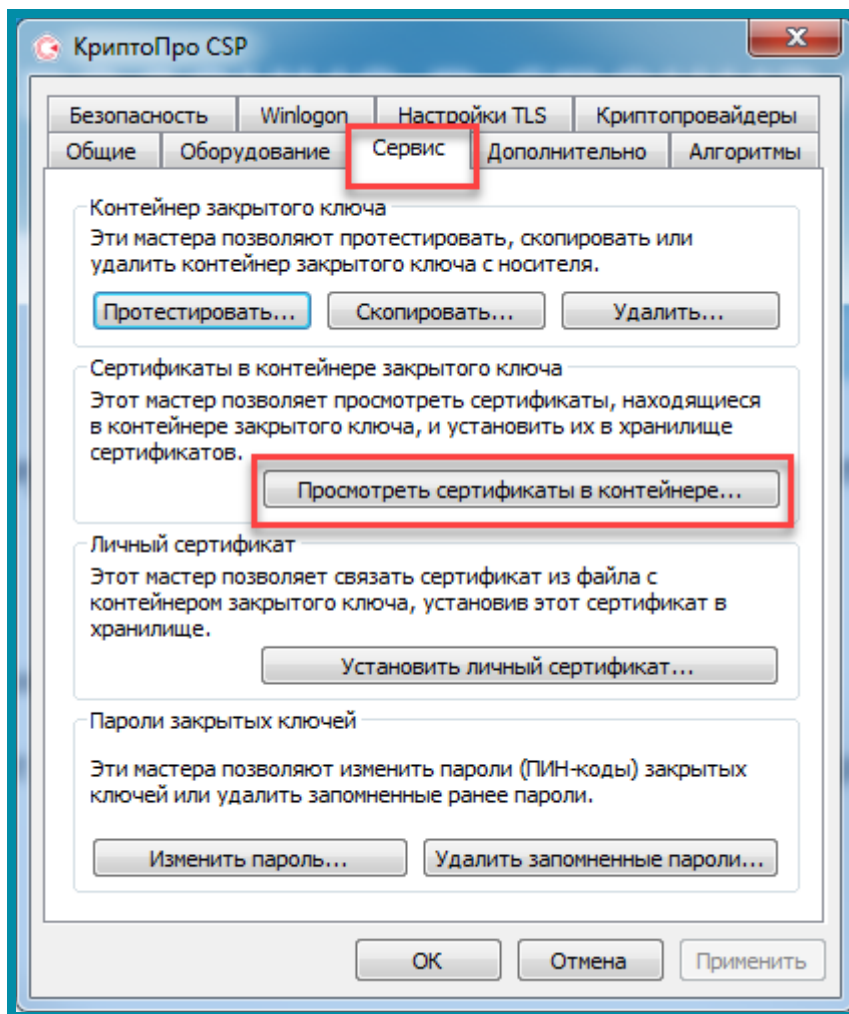


Рис. 3.3.1.2.

В окне «Контейнер закрытого ключа» нажмите кнопку **Обзор** (рис. 3.3.1.3.) и выберите Ваш контейнер из списка, после выбора нажмите кнопку **ОК** (рис. 3.3.1.4.).



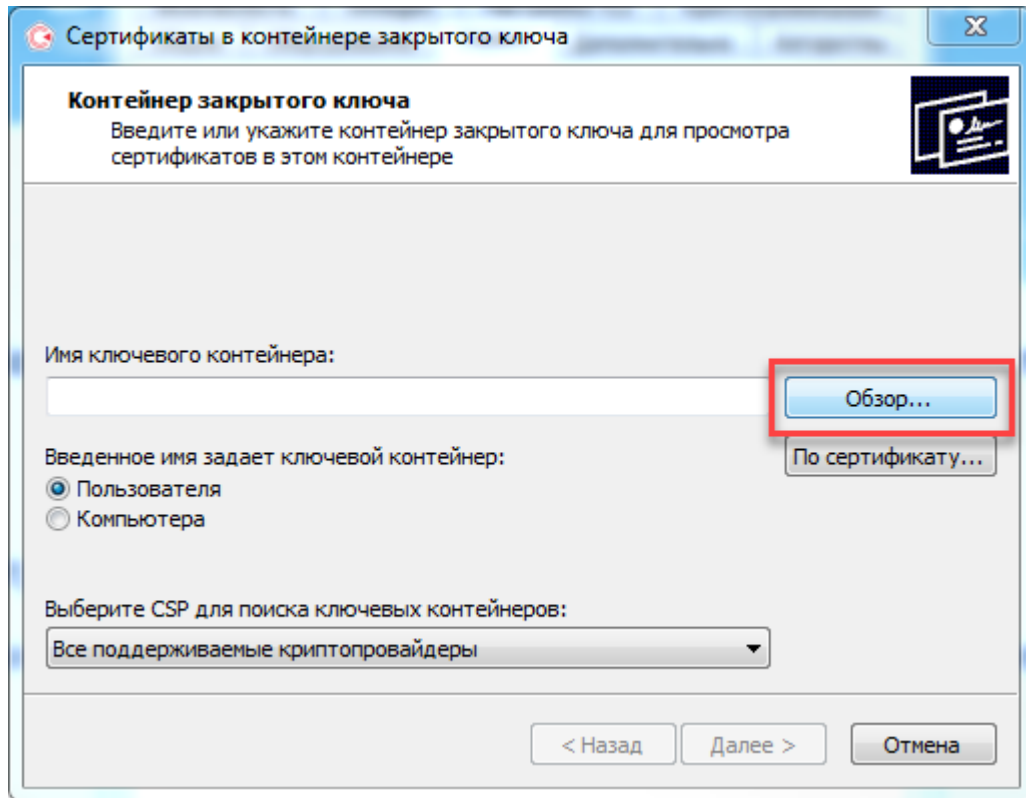


Рис. 3.3.1.3.

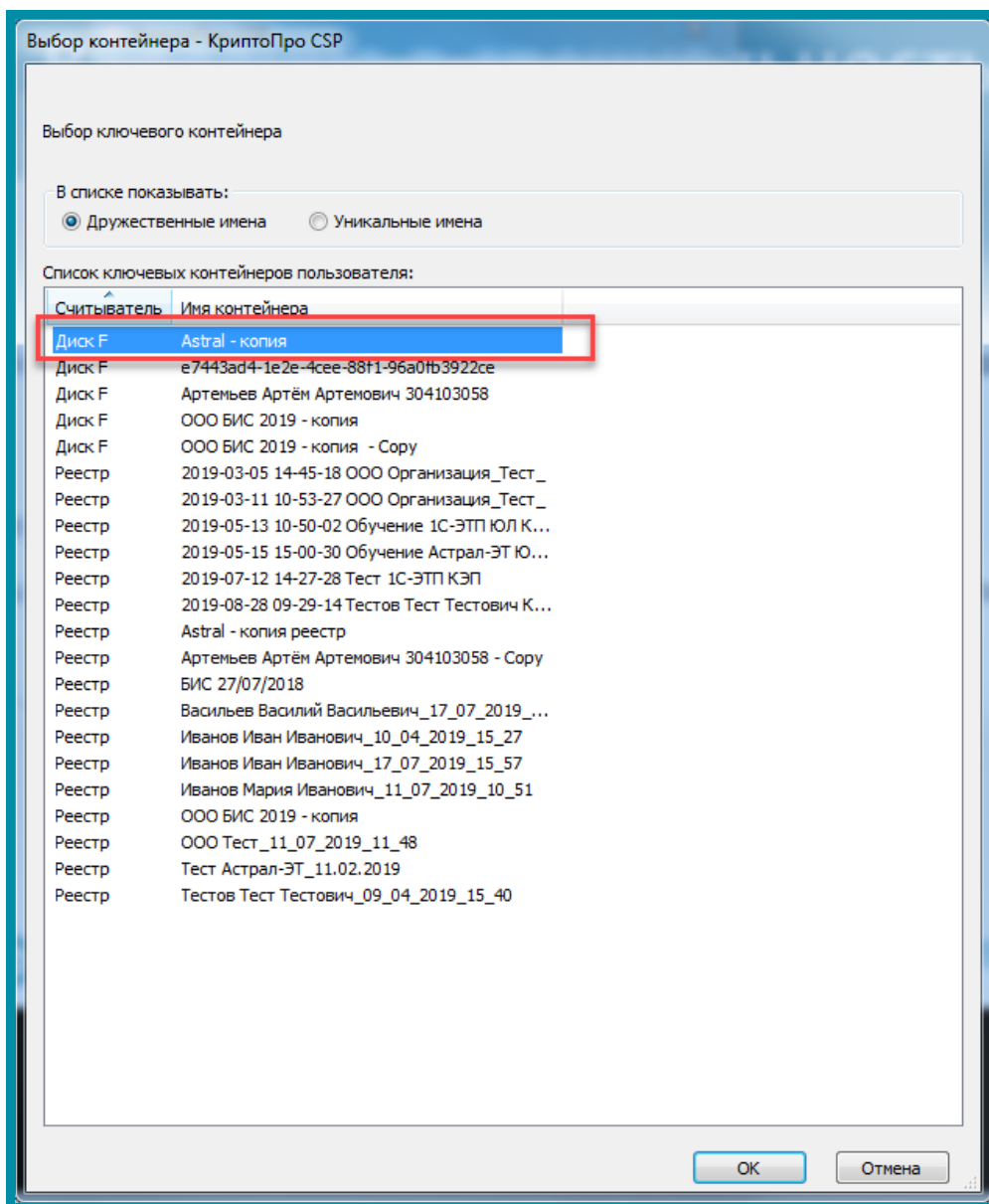


Рис. 3.3.1.4.

Перед Вами откроется окно «Сертификат для просмотра», нажмите кнопку **Установить** (рис. 3.3.1.6).

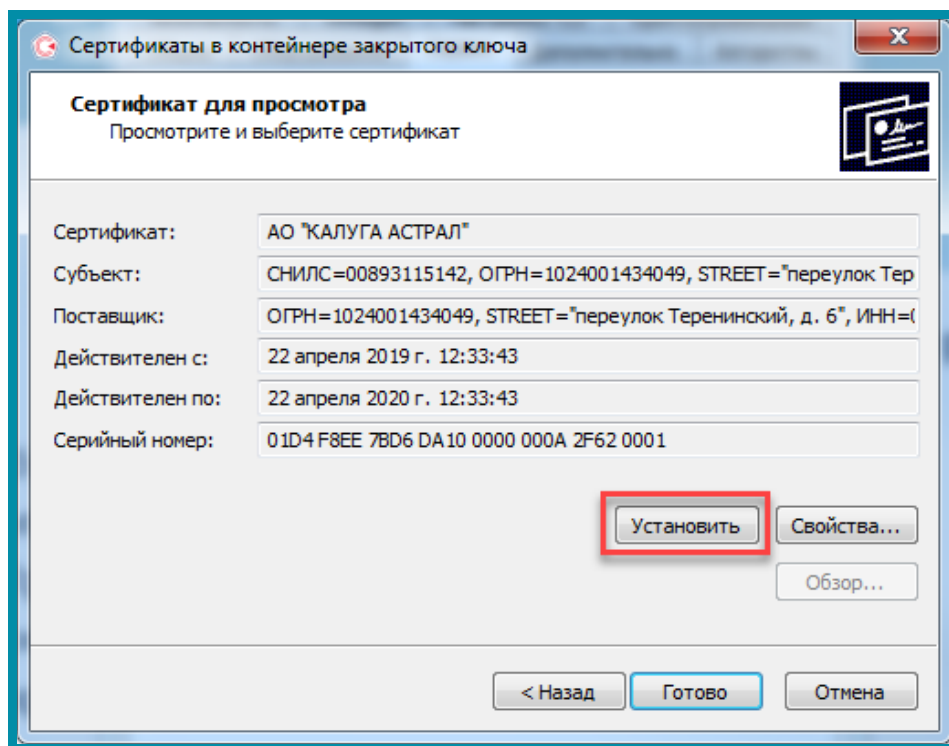


Рис. 3.3.1.6.

После этого появится сообщение «Сертификат был установлен в хранилище «Личные» текущего Пользователя». Закройте его нажатием кнопки ОК (рис. 3.3.1.7.).

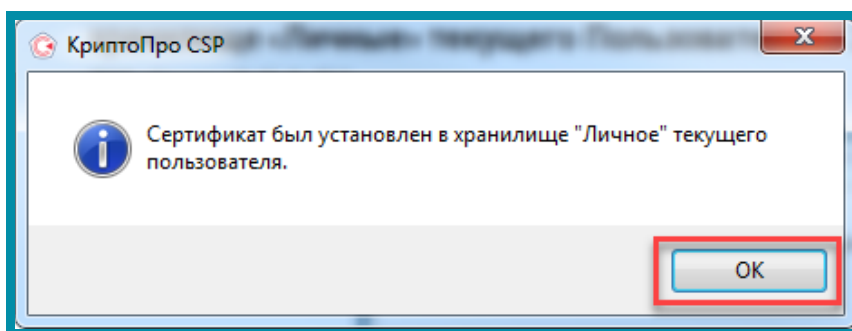


Рис. 3.3.1.7.

### 3.3.1.1. Создание копии контейнера закрытого ключа КриптоПро CSP

Для того чтобы скопировать контейнер закрытого ключа, нажмите «Пуск» – «Программы» – «КриптоПро» – «КриптоПро CSP», перейдите на вкладку «Сервис» и нажмите кнопку **Скопировать** (рис. 3.3.1.1.1.).

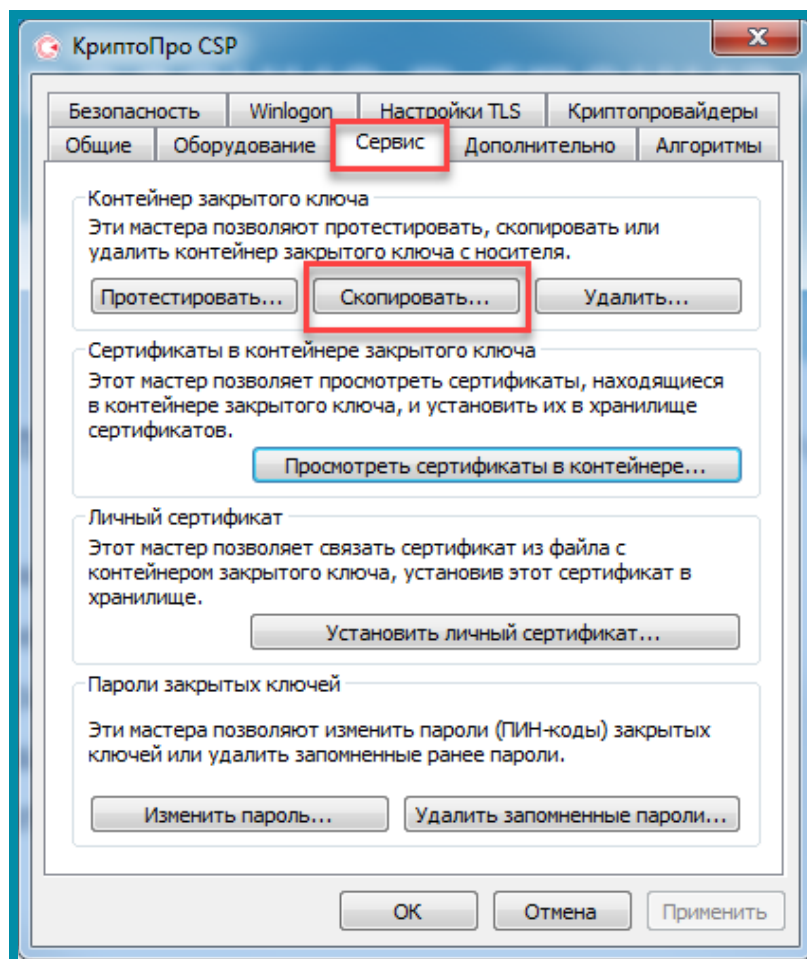


Рис. 3.3.1.1.1.

После нажатия кнопки **Обзор** выберите необходимый для копирования ключевой контейнер и нажмите **ОК** (рис. 3.3.1.1.3., рис. 3.3.1.1.4.).

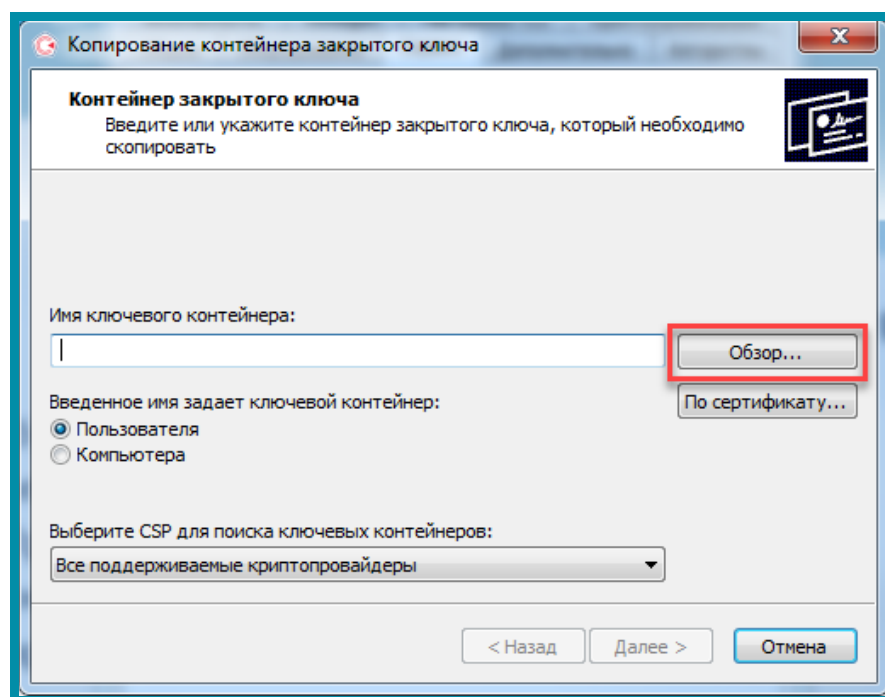


Рис. 3.3.1.1.3.

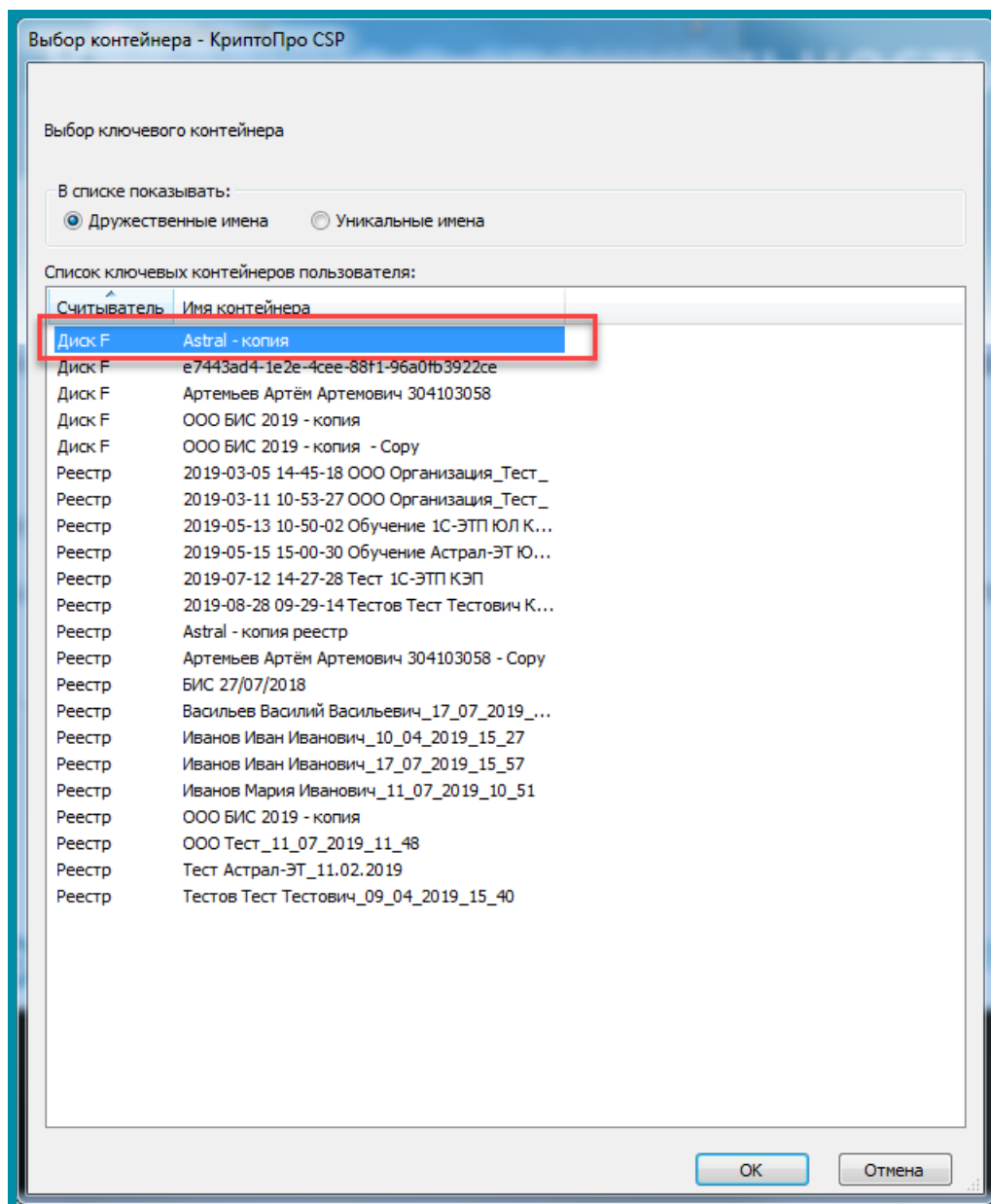


Рис. 3.3.1.1.4.

Система отобразит окно «Копирование контейнера закрытого ключа» (рис. 3.3.1.1.5.), в котором необходимо ввести имя нового ключевого контейнера.

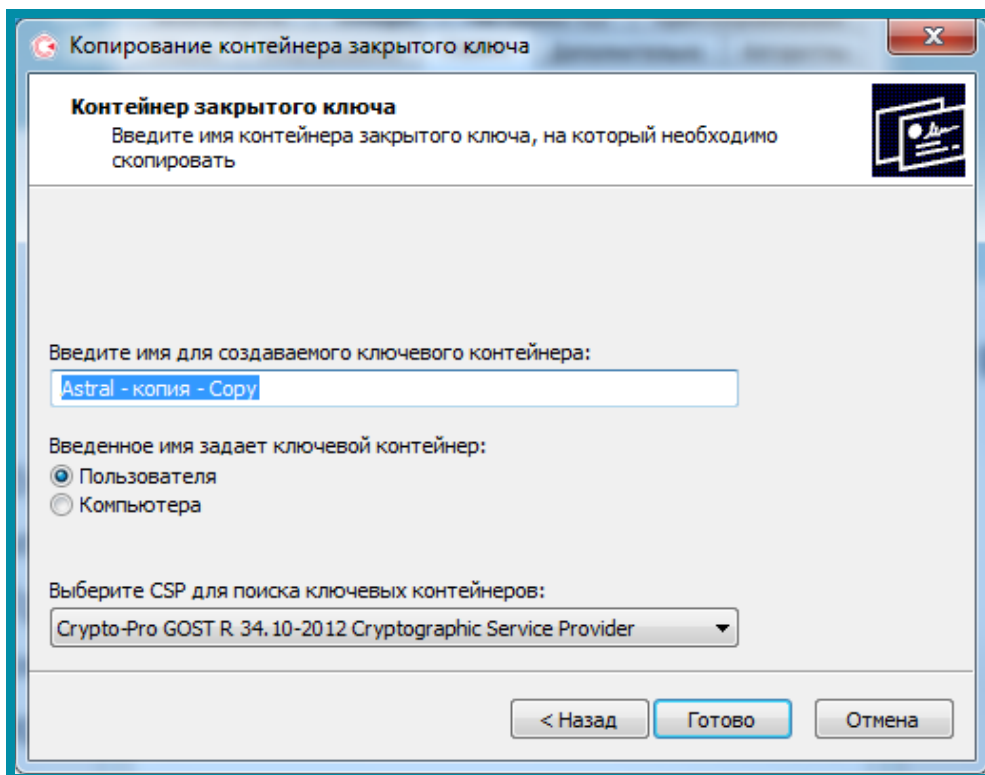


Рис. 3.3.1.1.5.

После ввода нажмите кнопку **Готово**. Система отобразит окно, в котором выбираем носитель для копированного контейнера (рис. 3.3.1.1.6.).

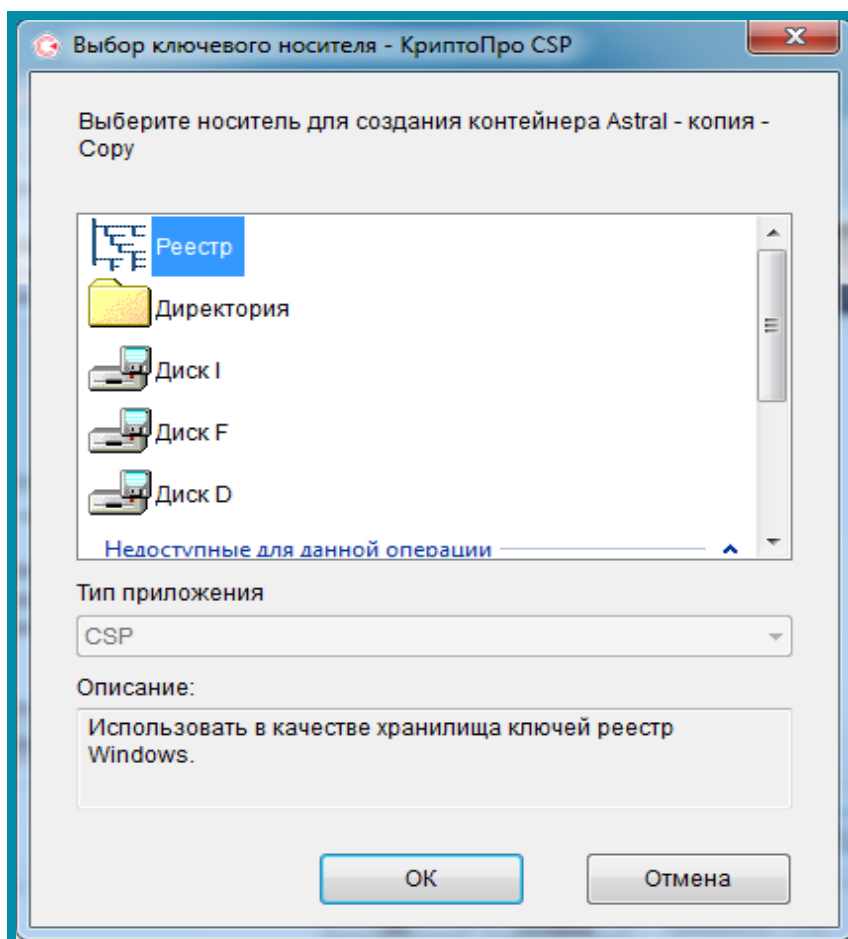


Рис. 3.3.1.1.6.

Вставьте носитель в считыватель и нажмите кнопку **ОК**. Система отобразит окно установки пароля на доступ к закрытому ключу (рис. 3.3.1.1.7.). Введите пароль, подтвердите его, при необходимости установите флаг «Запомнить пароль» (если данный флаг будет установлен, пароль сохранится в специальном хранилище на локальном компьютере, и при обращении к закрытому ключу пароль будет автоматически считываться из этого хранилища, а не вводиться Пользователем).

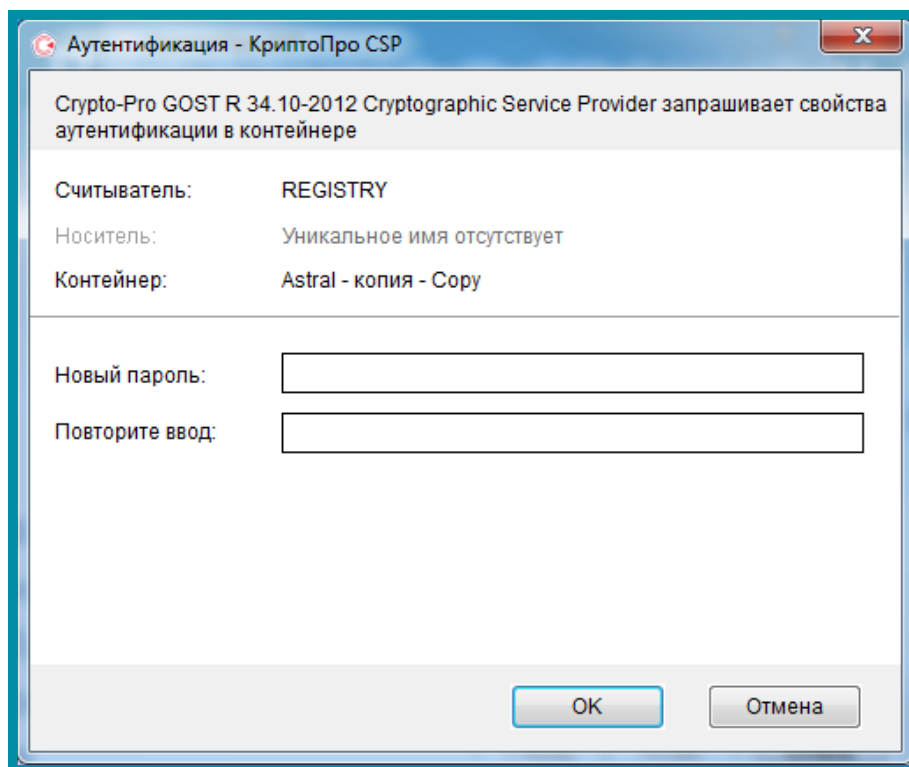


Рис. 3.3.1.1.7.

После ввода необходимых данных нажмите кнопку **ОК**. СКЗИ «КриптоПро CSP» осуществит копирование контейнера закрытого ключа.

### 3.3.2. Установка сертификатов VipNet CSP

Дважды щелкните левой кнопкой мыши по ярлыку программы. Перед Вами откроется окно **Настройка VipNet CSP**. Перейдите на вкладку **Контейнеры ключей** (рис. 3.3.2.1.).

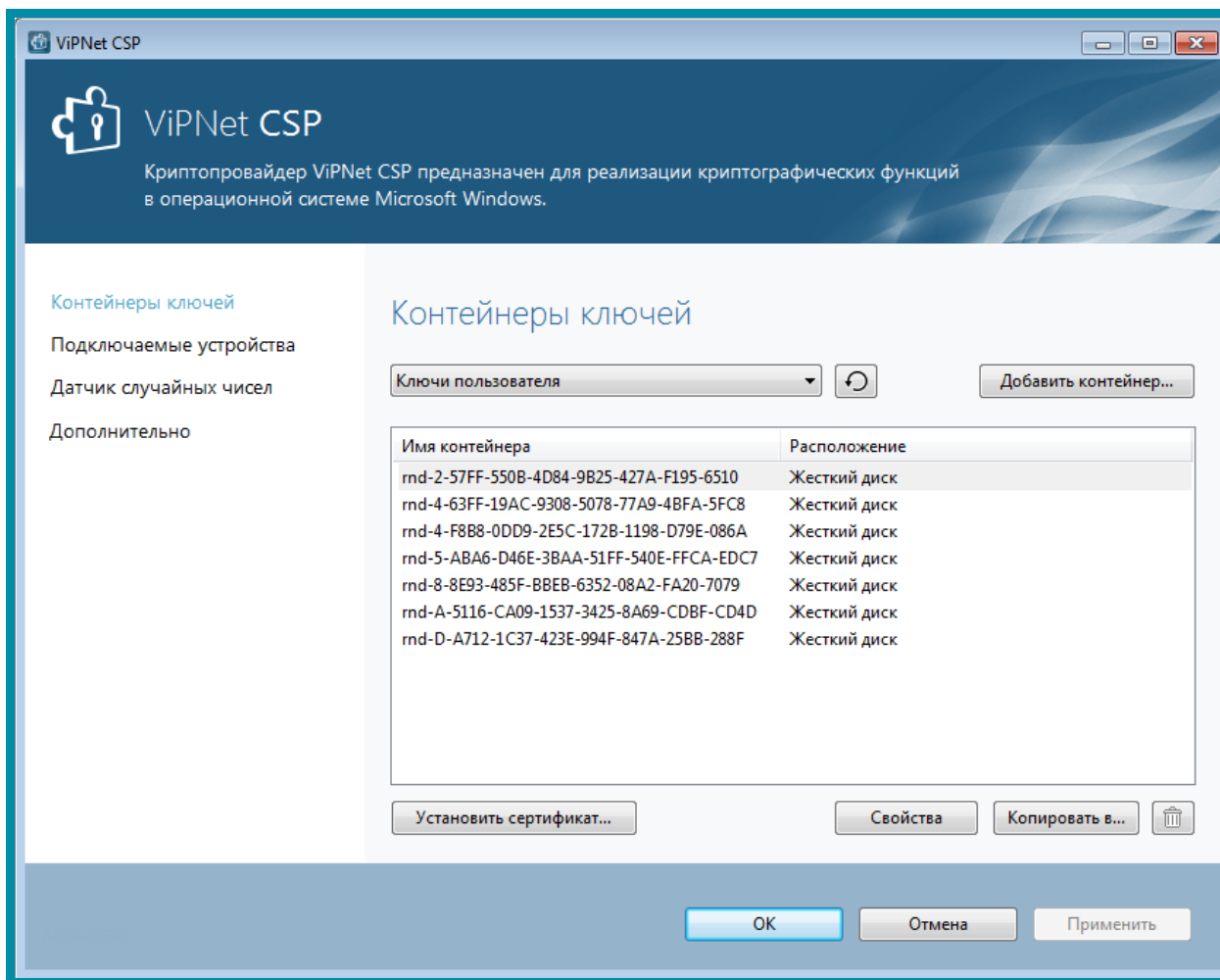


Рис. 3.3.2.1.

Программа автоматически найдет созданные ранее контейнеры. Если необходимого контейнера нет в списке, нажмите кнопку **Добавить контейнер**.

Перед Вами откроется окно, где необходимо указать контейнер закрытого ключа (рис. 3.3.2.2.).

Нажмите кнопку **Обзор**, выберите Ваш ключ и нажмите кнопку **OK**.



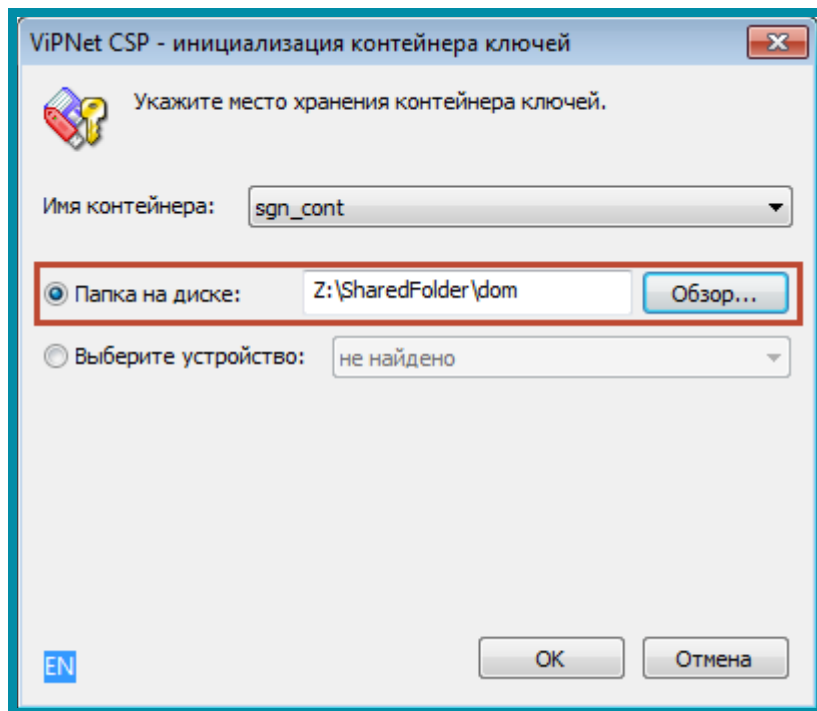
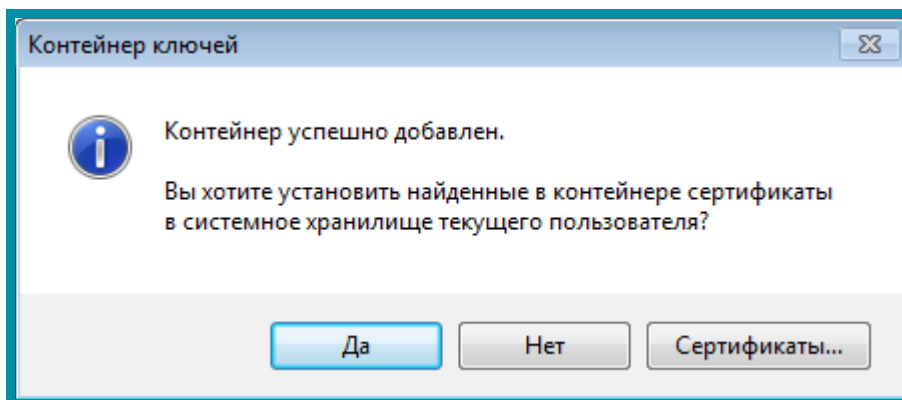


Рис. 3.3.2.2.

В окне **Контейнер ключей** появится сообщение об успешном добавлении контейнера ключей и предложение установить сертификат в системное хранилище (рис. 3.3.2.3.).



Теперь Вам необходимо установить сертификат из контейнера в системное хранилище **Личные сертификаты**. Для этого выделите контейнер в списке и нажмите кнопку **Свойства** либо дважды щелкните на нужный контейнер (рис. 3.3.2.3.).

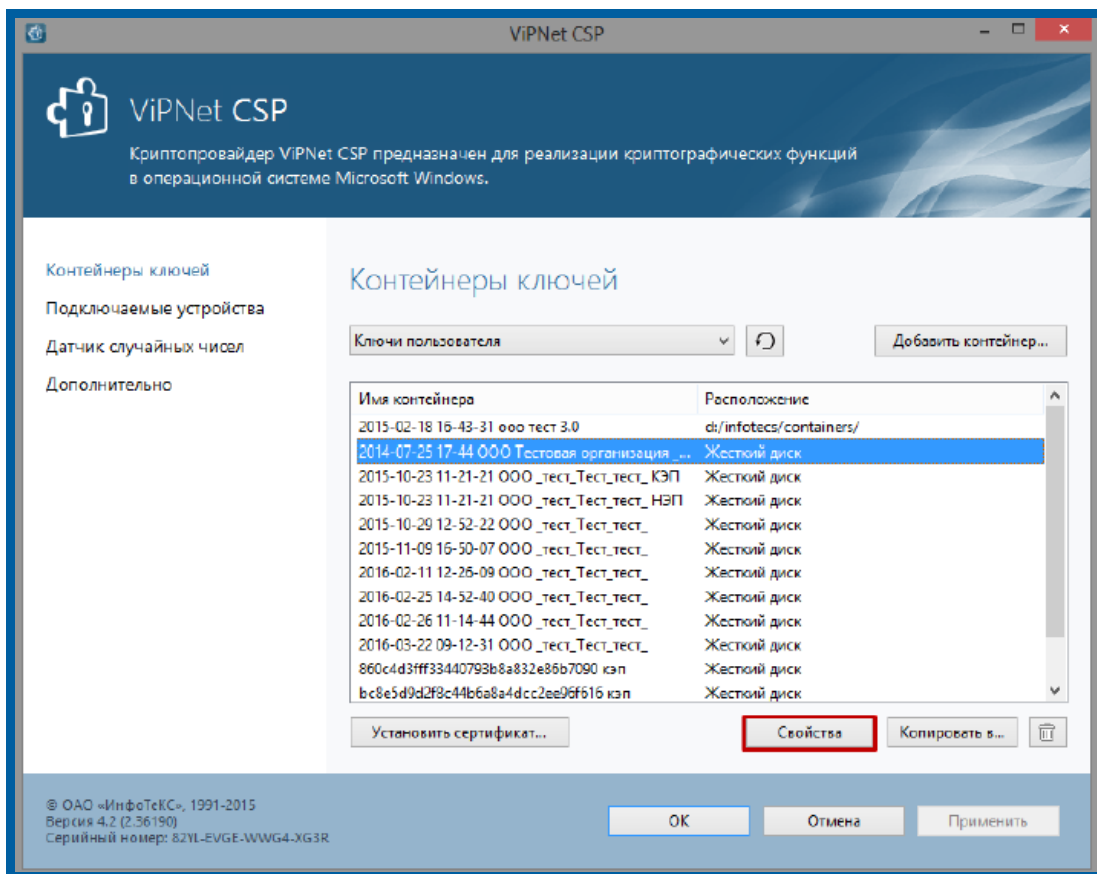


Рис. 3.3.2.3.

В окне «Свойства контейнера ключей» нажмите кнопку **Добавить сертификат из файла.** (рис. 3.3.2.4).

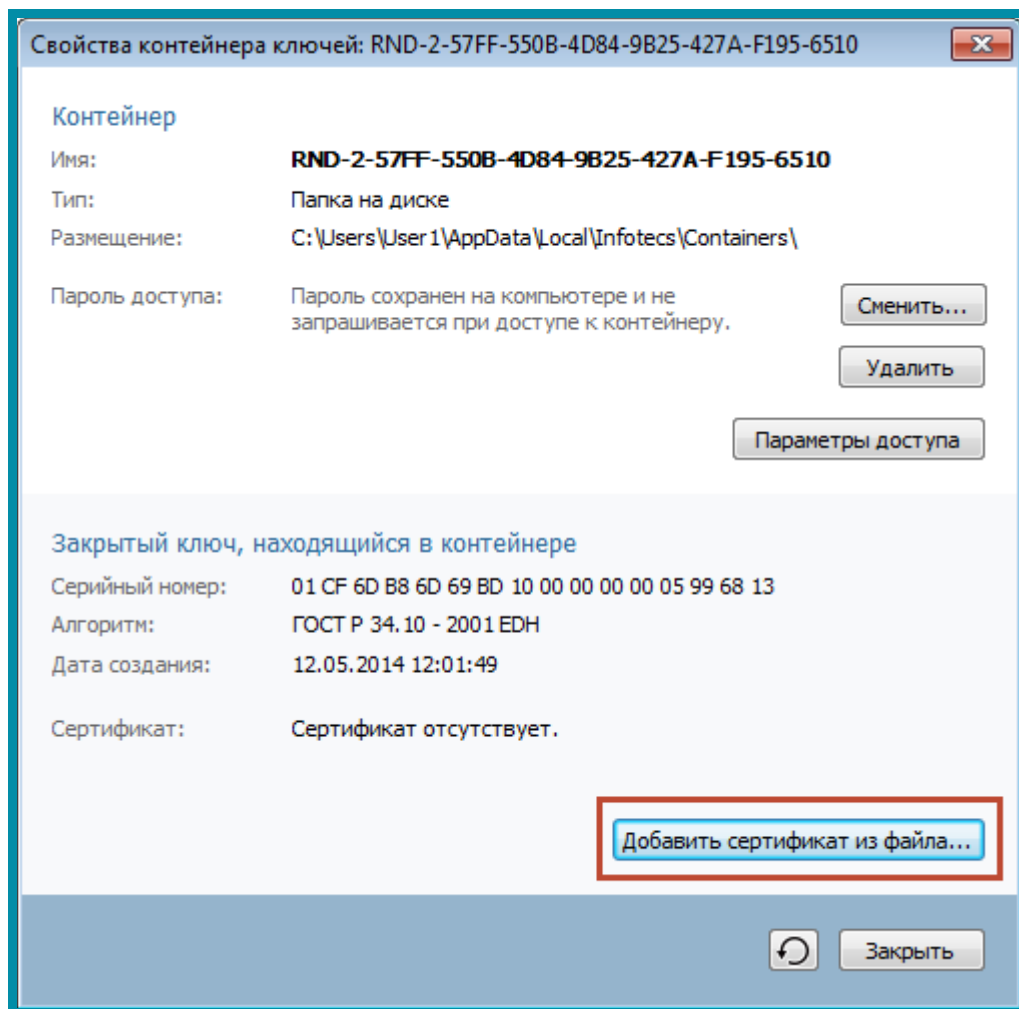


Рис. 3.3.2.4.

Пройдите по шагам мастера установки сертификата, нажимая кнопки **Установить сертификат – Далее – Далее – Готово** (рис. 3.3.2.5.).

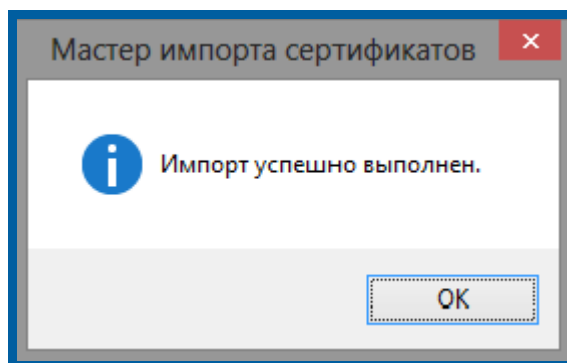


Рис. 3.3.2.5.

### 3.3.2.1. Создание копии контейнера закрытого ключа ViPNet CSP

Откройте программу ViPNet CSP. Для этого перейдите в меню «Пуск» – «Все программы» – «ViPNet» – «ViPNet CSP» (рис. 3.3.2.1.1.).

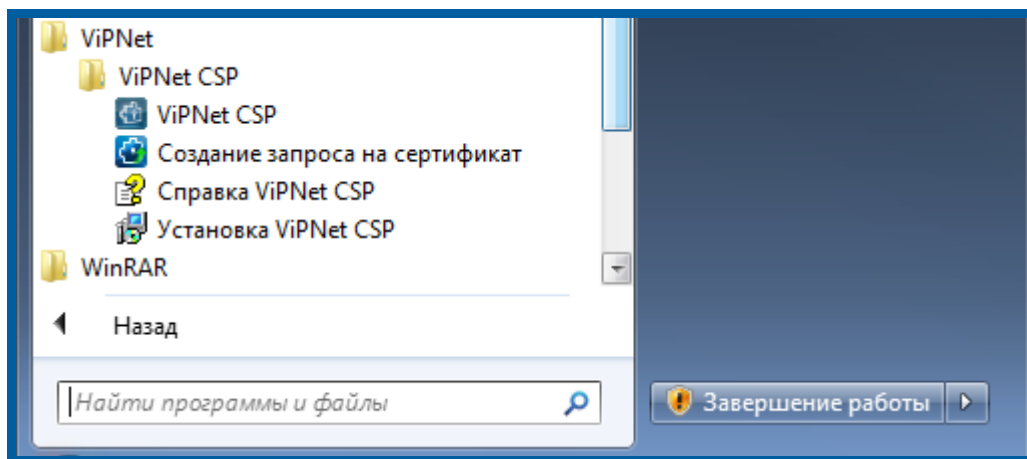


Рис. 3.3.2.1.1.

В открывшемся окне перейдите на вкладку «Контейнеры», выделите нужный контейнер одним нажатием левой кнопки мыши и нажмите кнопку **Копировать** (рис. 3.3.2.1.2.).

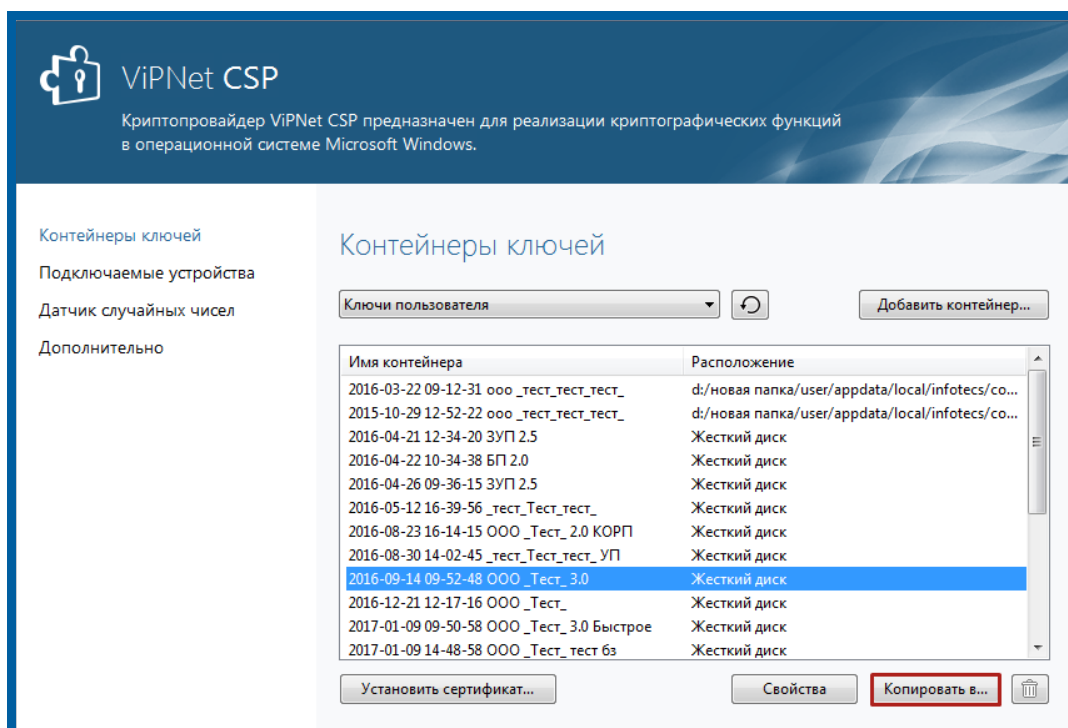


Рис. 3.3.2.1.2.

Далее выберите путь сохранения копии контейнера ключа. Для этого нажмите кнопку **Обзор** (рис. 3.3.2.1.3.).

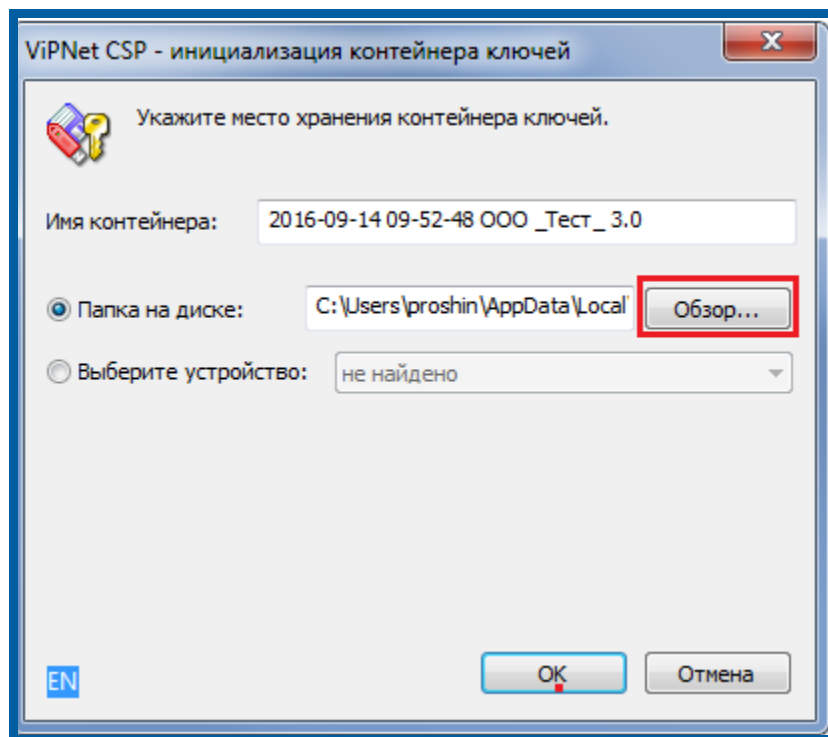


Рис. 3.3.2.1.3.

Укажите папку, в которую хотите поместить копию контейнера ключа, и нажмите **ОК**. Введите пароль контейнера ключа, после чего задайте новый пароль и подтвердите его. Пароль должен содержать в себе не менее 6 символов.

На вкладке Контейнеры появится копия Вашего контейнера с указанием места хранения.

### 3.4. Установка корневых сертификатов

#### 3.4.1. Установка корневых сертификатов с помощью программы автоматической установки

Для корректного построения пути сертификации любого сертификата, выданного АО «КАЛУГА АСТРАЛ» можно воспользоваться программой автоматической установки корневых сертификатов.

Для скачивания программы перейдите на официальный сайт <http://astral.ru>. Выберите раздел сайта «Продукты» – «1С-ЭТП» (рис. 3.4.1.1.).

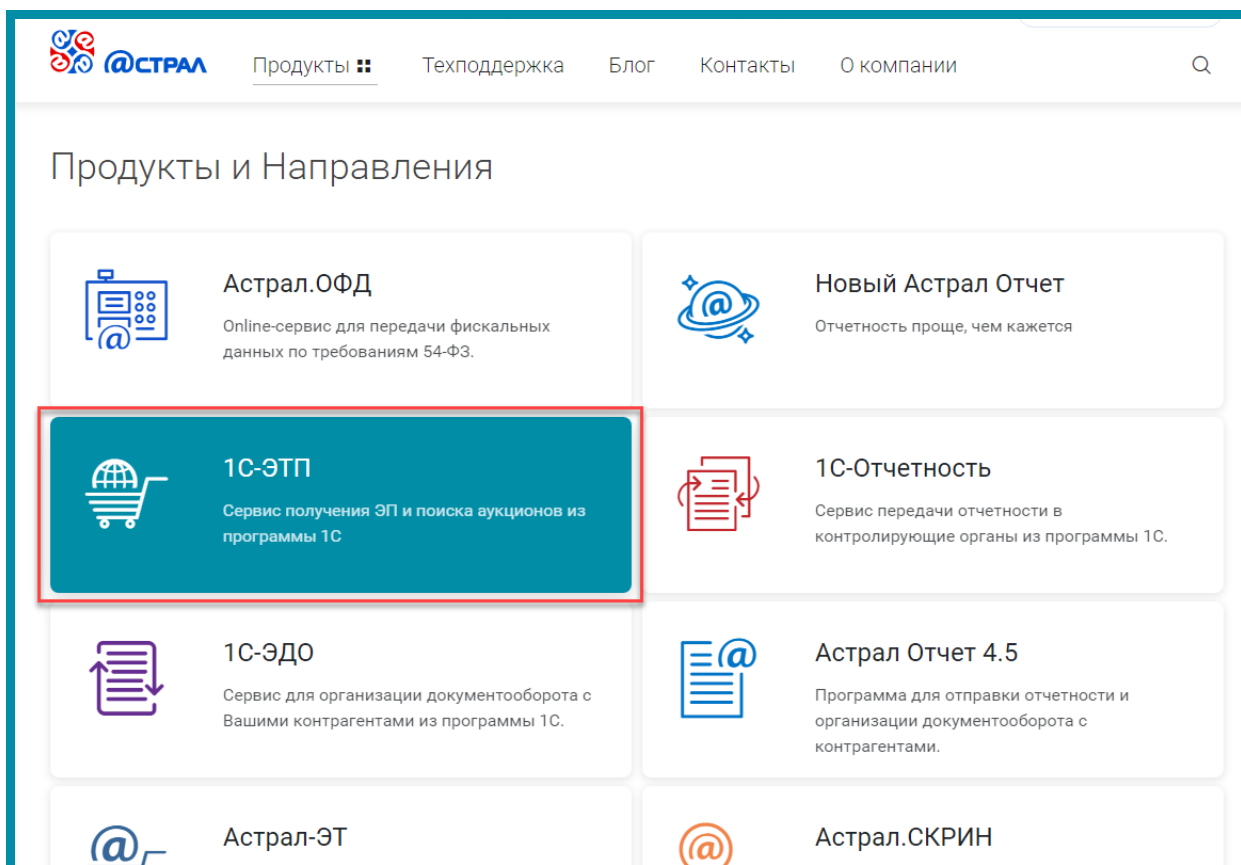


Рис. 3.4.1.1.

Перейдите на вкладку «Техническая поддержка» и выберите ссылку «Автоматическая установка корневых сертификатов» (рис. 3.4.1.2.).

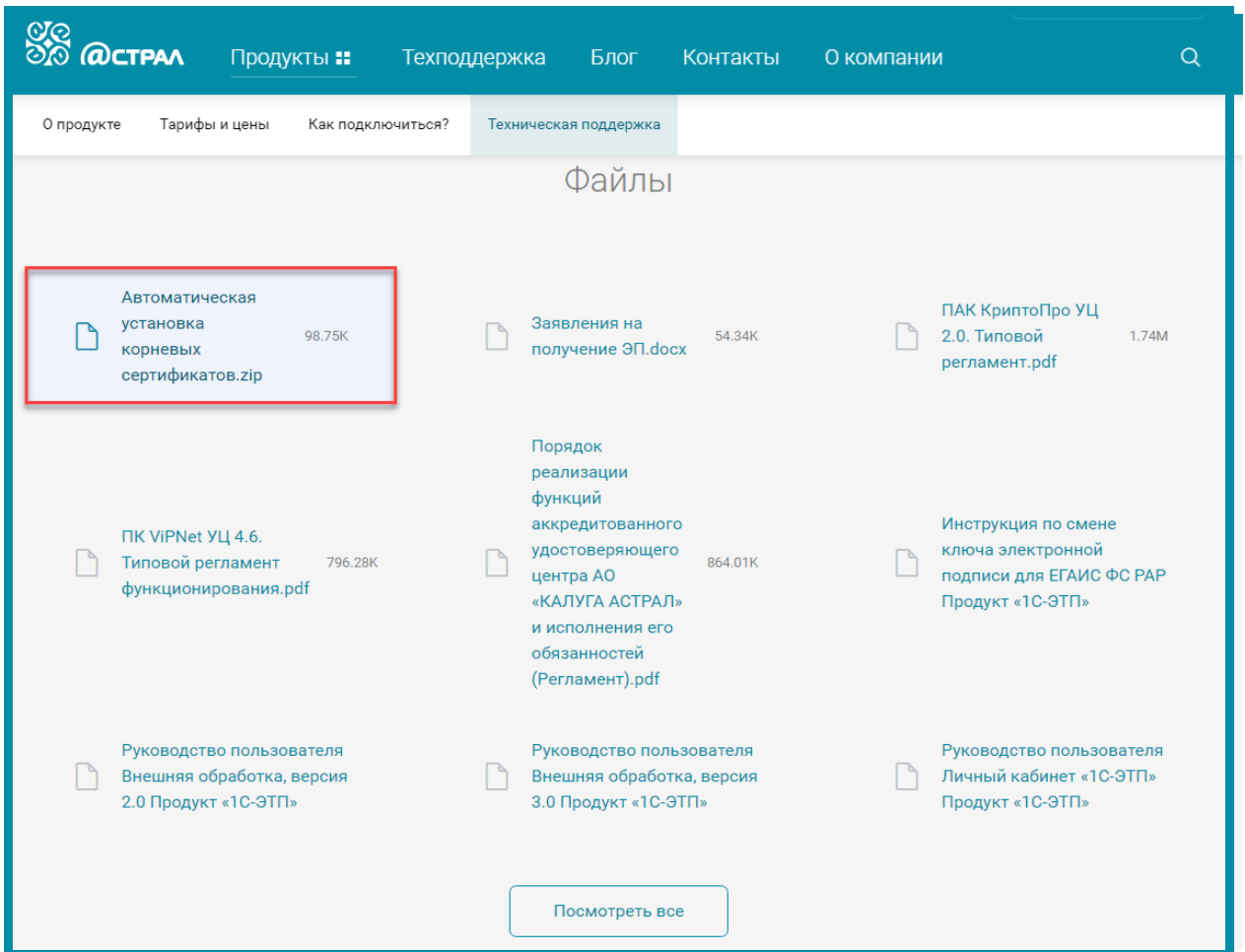


Рис. 3.4.1.2.

Распакуйте скачанный архив и запустите файл InstallSertsAstral.exe. Начнется процедура автоматической установки корневых сертификатов (рис. 3.4.1.3.).

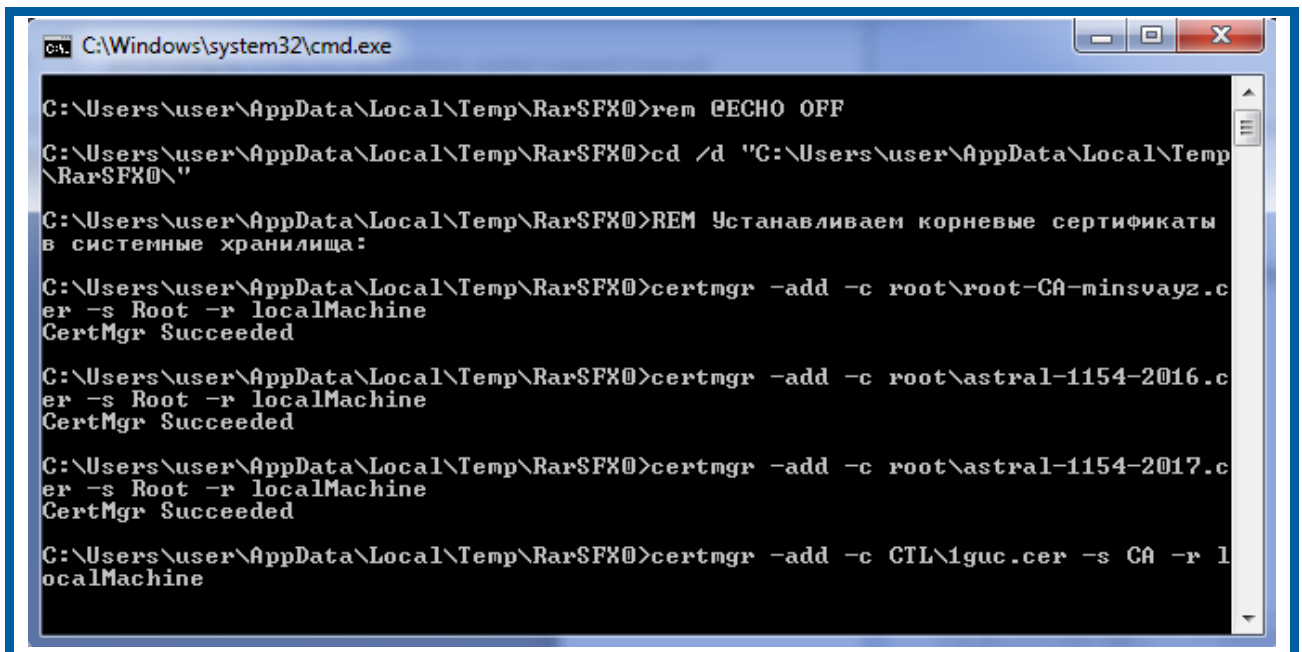


Рис. 3.4.1.3.

### 3.5. Настройка интернет-браузера

Для корректной работы интернет-браузера при использовании электронной подписи произведите следующие настройки: Откройте окно интернет-браузера Internet Explorer и перейдите в пункт меню «Сервис» – «Свойства обозревателя» (рис. 3.5.1).

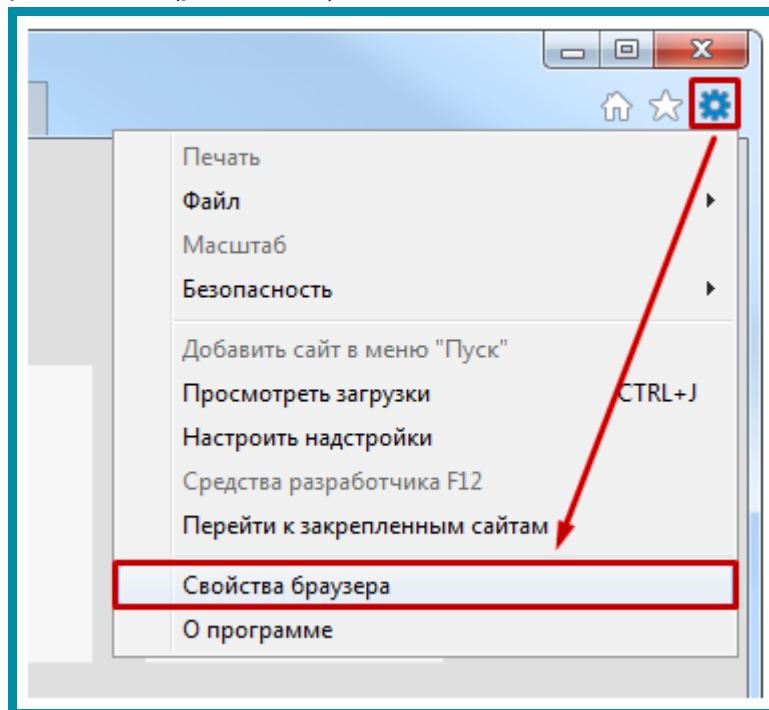


Рис. 3.5.1.

В открывшемся окне перейдите на вкладку «Безопасность». Выделите пункт «Надежные сайты» и нажмите кнопку **Сайты** (рис. 3.5.2).



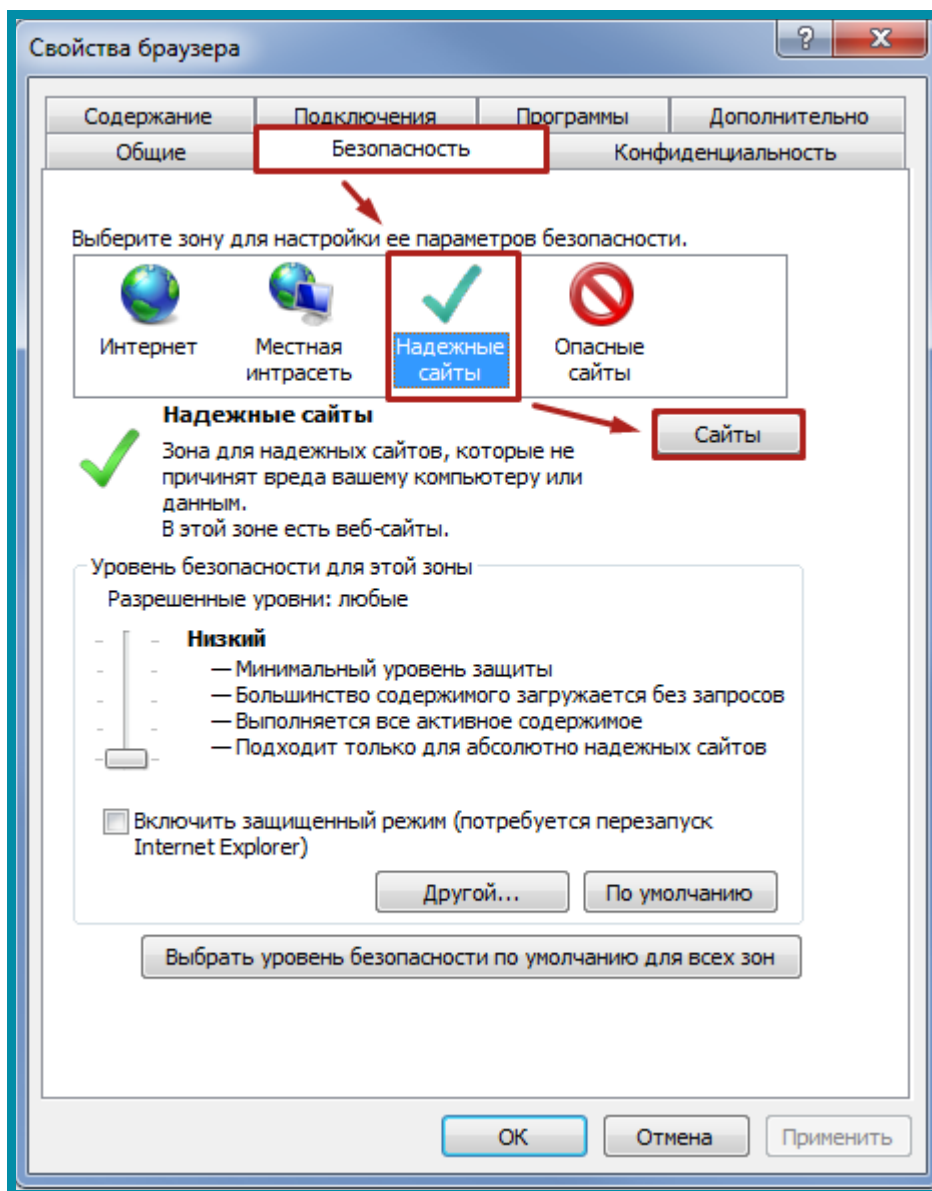


Рис. 3.5.2.

Впишите адрес электронной торговой площадки или ресурса, на котором предполагается работа, и нажмите кнопку **Добавить**. Отметку в поле **Для всех узлов этой зоны требуется проверка серверов (https:)** необходимо убрать, далее нажмите кнопку **Заккрыть** (рис. 3.5.3.).

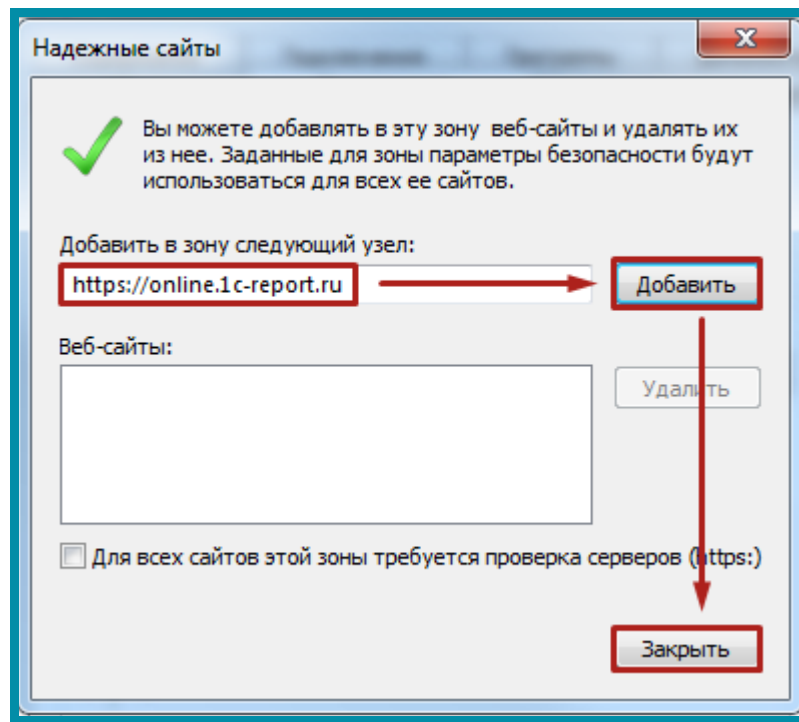


Рис. 3.5.3.

На вкладке «Безопасность» нажмите кнопку **Другой**. В открывшемся окне «Параметры безопасности» в поле Сброс особых параметров выберите режим **Низкий** и нажмите кнопку **Сбросить**. Далее включите/разрешите (в зависимости от версии Internet Explorer) все элементы ActiveX (рис. 3.5.4.).

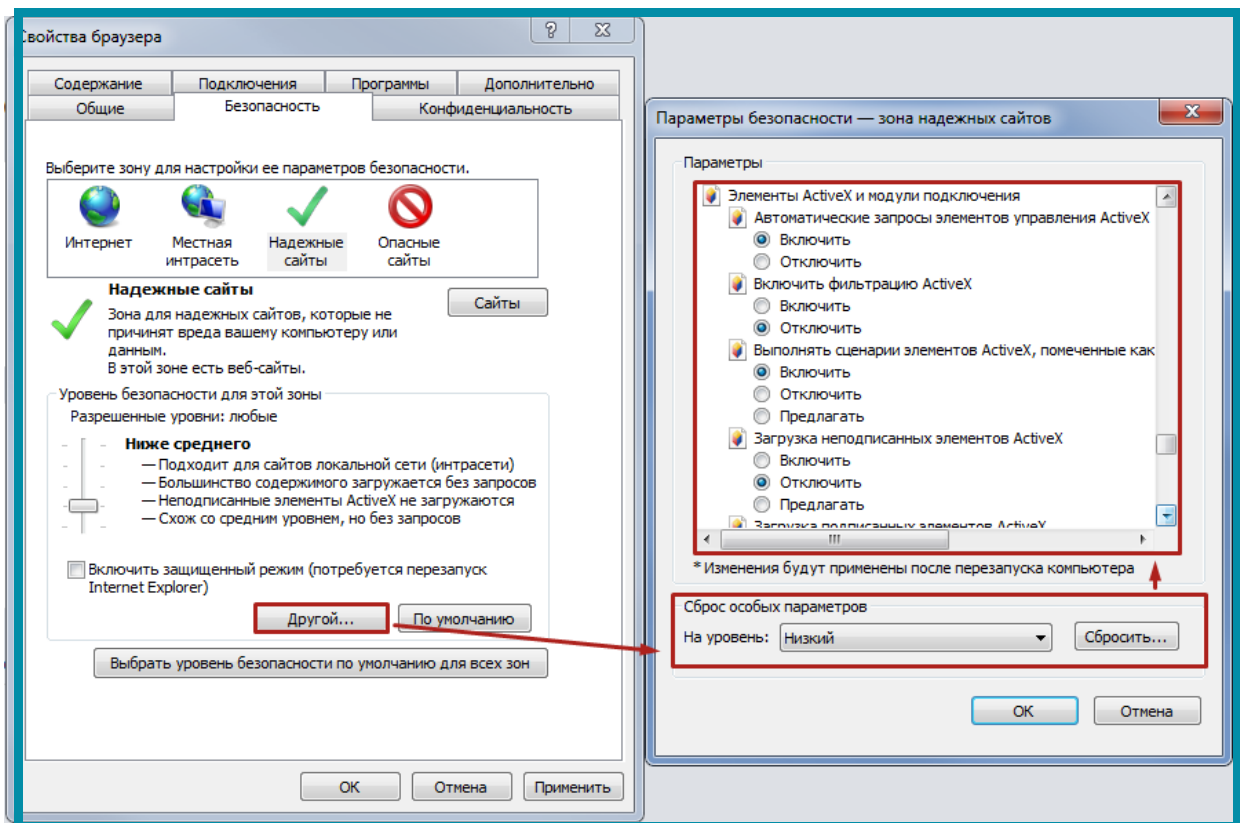


Рис. 3.5.4.

Также в разделе «Разное» включите «Отображение разнородного содержимого» (рис. 3.5.5).

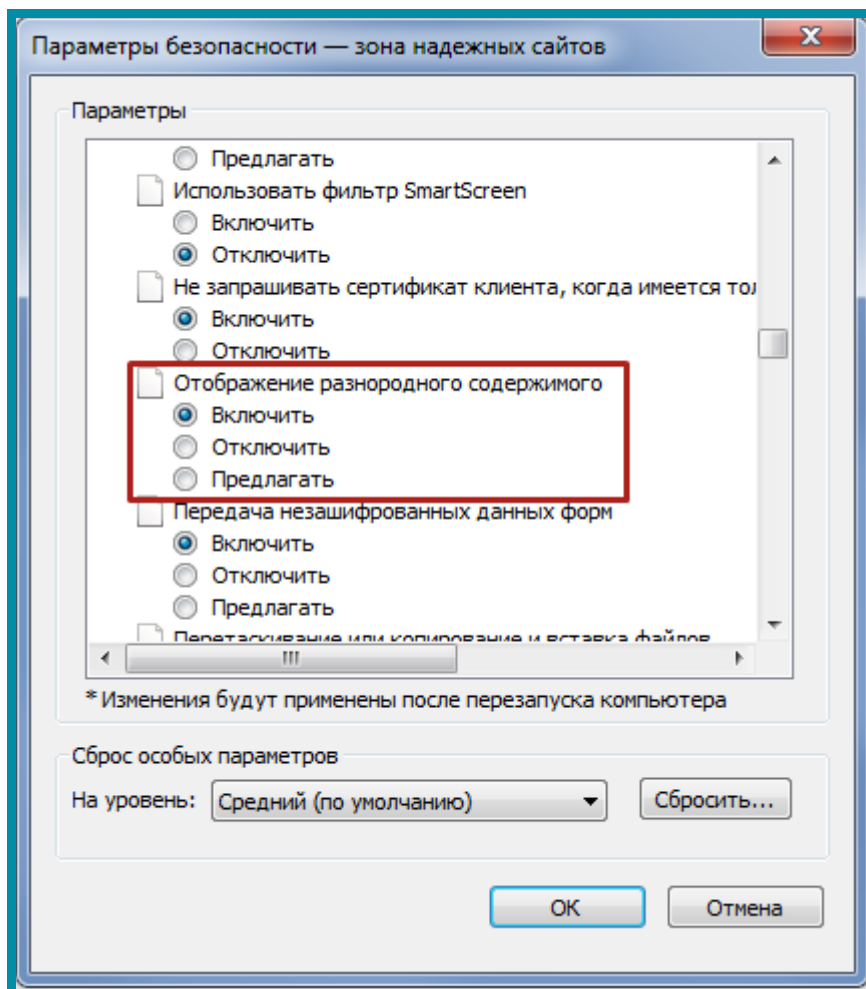


Рис. 3.5.5.

Отключите Блокировку всплывающих окон. После этого нажмите кнопку **Ок** (рис. 3.5.6).

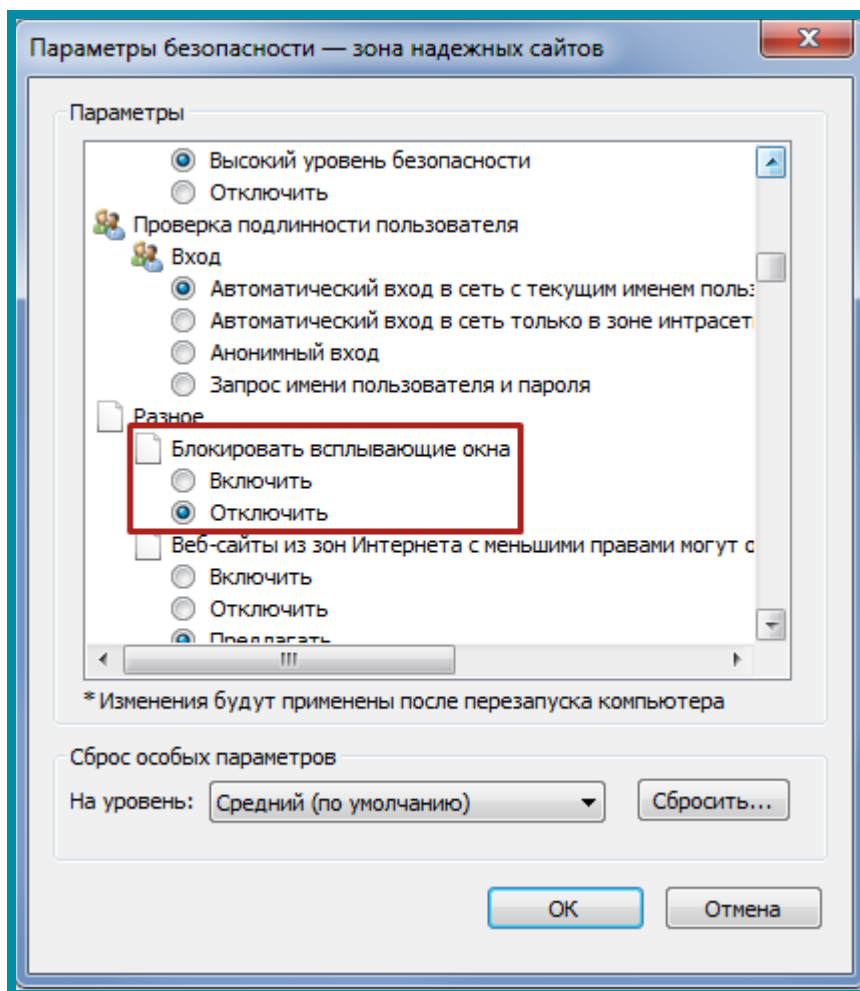


Рис. 3.5.6.

Перейдите на вкладку «Конфиденциальность» и выберите Средний (или Умеренно высокий) уровень безопасности для зоны Интернета. Далее снимите флажок с пункта **Включить блокирование всплывающих окон** или добавьте используемый сайт в исключения, нажав на кнопку **Параметры** (рис. 3.5.7).

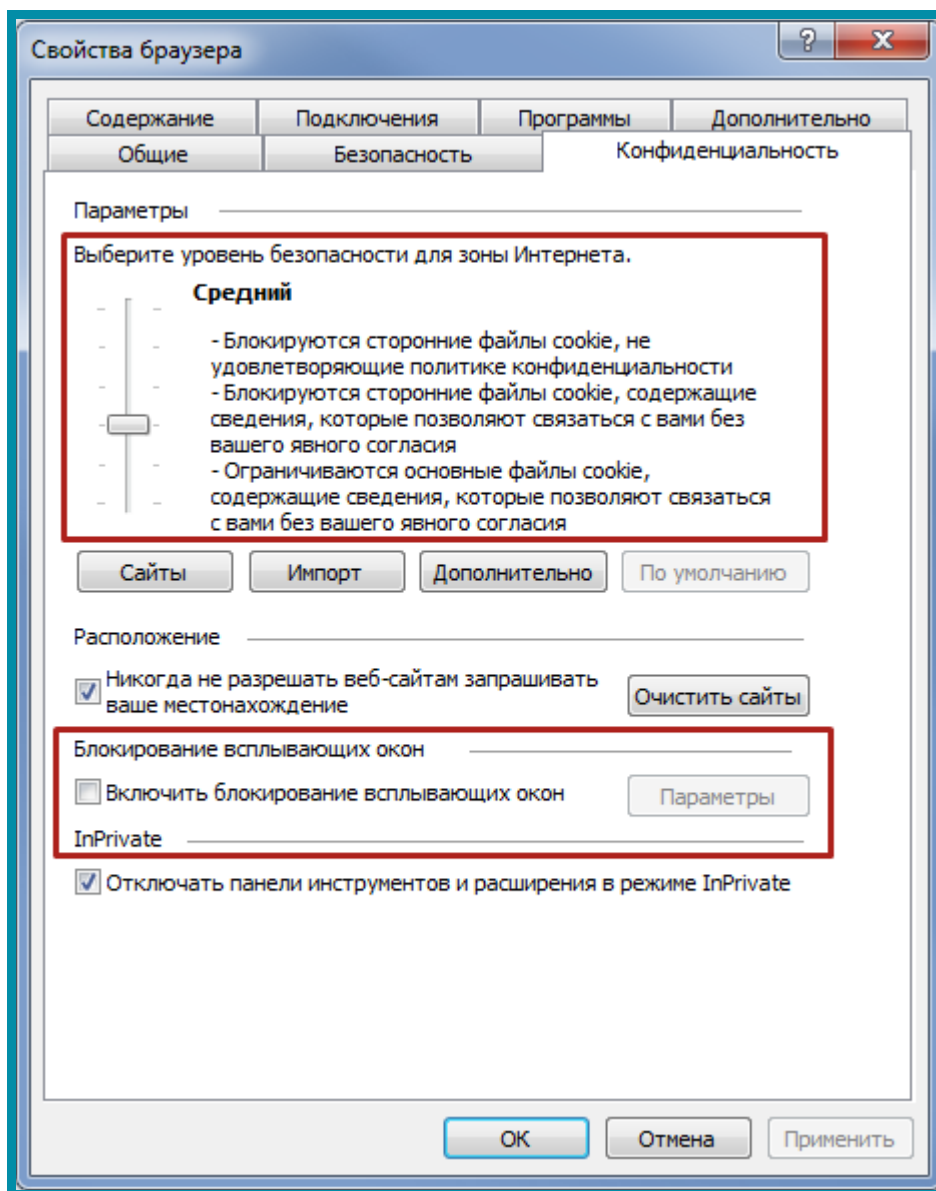


Рис. 3.5.7.

## 4. Работа с электронной подписью

### 4.1. Особенности работы с наиболее распространенными сайтами с помощью электронной цифровой подписи

#### 4.1.1. ЗАО «Сбербанк-АСТ»

##### 4.1.1.1. Регистрация на универсальной торговой платформе

Адрес площадки - <http://www.sberbank-ast.ru/>.

Порядок регистрации на УТП указан в [инструкции](#).

С порядком регистрации на УТП без ЭП можно ознакомиться [здесь](#).

##### 4.1.1.2. Вход в личный кабинет Поставщика

Адрес площадки – <http://www.sberbank-ast.ru/>.

Правила входа в личный кабинет Поставщика – <http://www.sberbank-ast.ru/Docs/faq/Поставщик.pdf>.

Регистрация Пользователей осуществляется из открытой части площадки. Для этого нажмите кнопку **Войти** (4.1.1.2.1.),

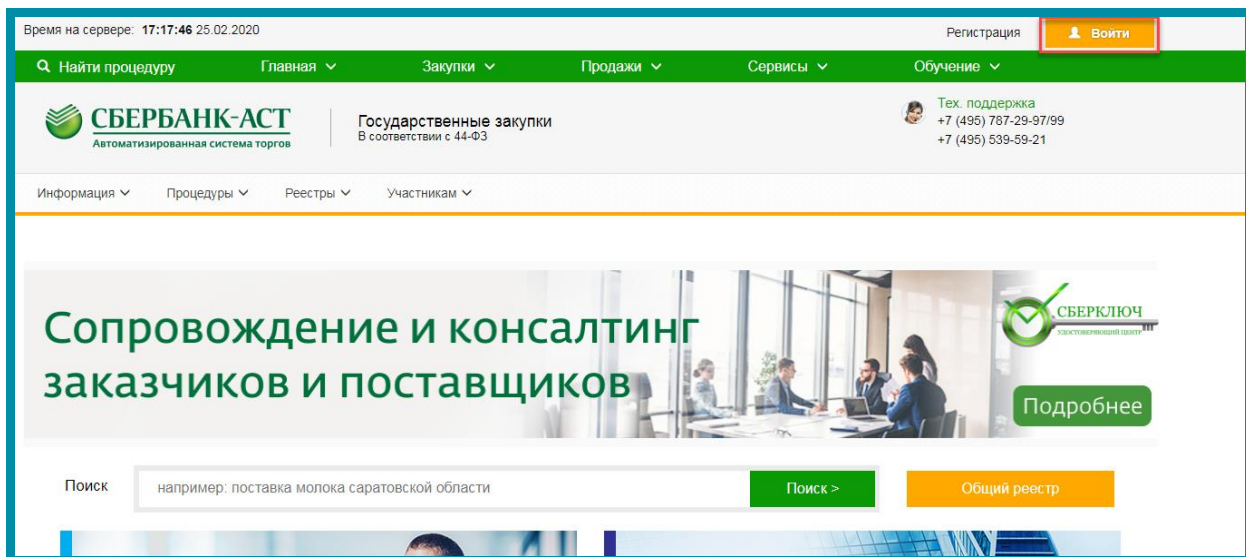


Рис. 4.1.1.2.1.

В открывшемся окне выберите сертификат в поле **Сертификат** и нажмите **Войти** (рис. 4.1.1.2.2.).

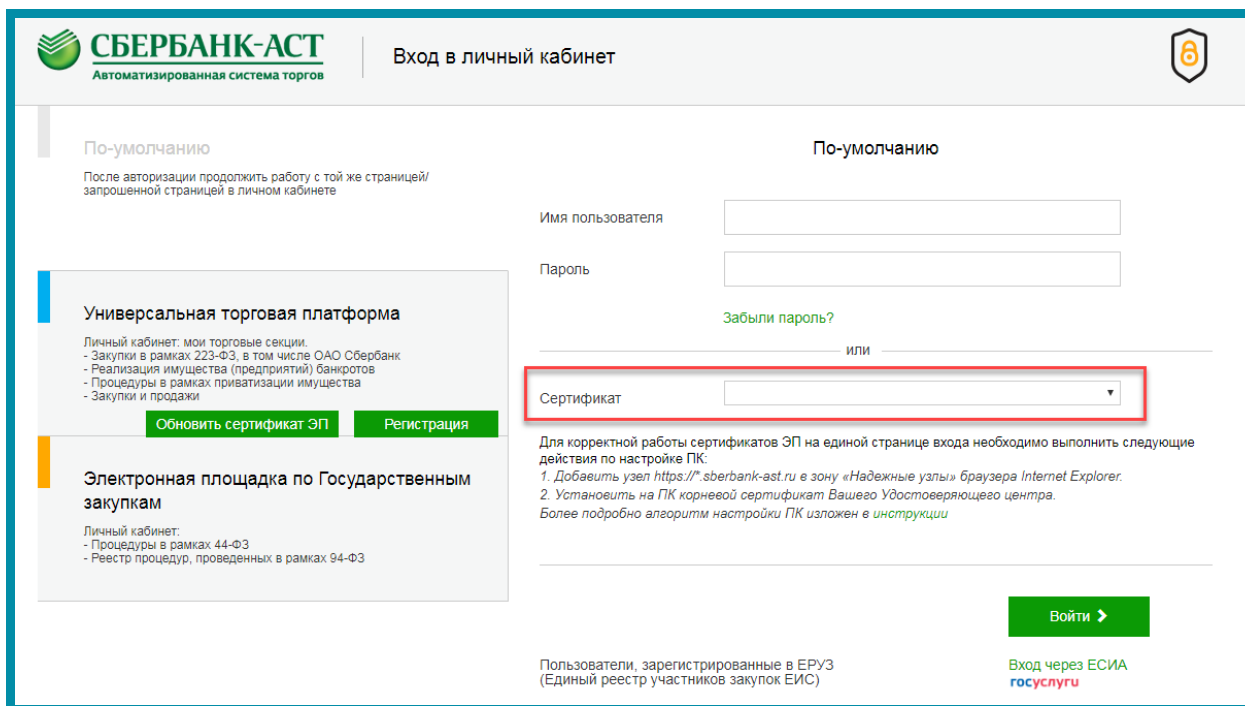


Рис. 4.1.1.2.2.

Для регистрации на площадке без квалифицированной электронной подписи выберите на главном меню **Участникам – Регистрация** (рис. 4.1.1.2.3.).

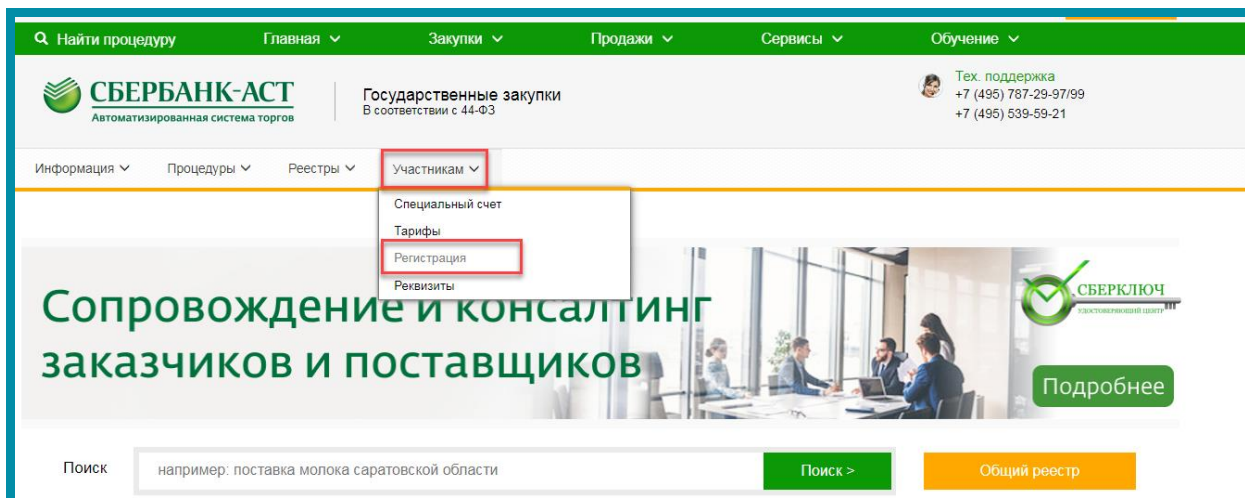


Рис. 4.1.1.2.3.

Нажмите кнопку **Выбрать** в поле «Регистрация пользователя участника (не имеющего квалифицированной электронной подписи)», затем нажмите кнопку **Подать заявку** (рис. 4.1.1.2.3.).

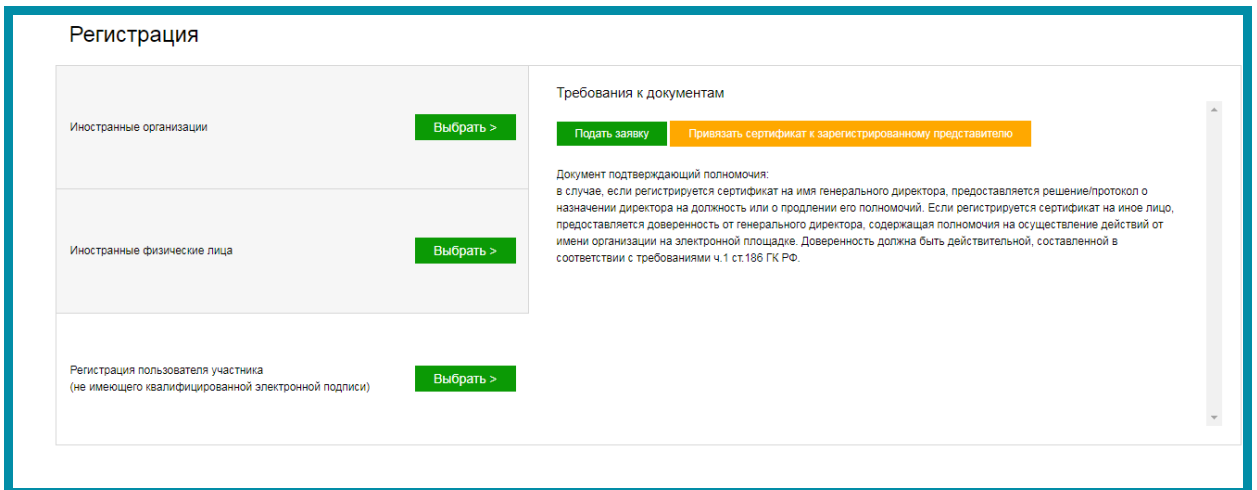


Рис. 4.1.1.2.3.

Выберите из списка Ваш сертификат электронной подписи и нажмите кнопку **Заполнить регистрационную форму**, после чего некоторые поля (ИНН, КПП, ОГРН, Ф. И. О и т.д.) заполнятся автоматически. Остальные поля заполняются вручную, поля, отмеченные звездочкой (\*) являются обязательными для заполнения. В системе электронной площадки ЗАО «Сбербанк-АСТ» осуществляется проверка на уникальность логинов, поэтому заполняя поле «Логин», необходимо указывать новый логин (при указании существующего логина система выдаст сообщение об ошибке). Логин должен содержать только латинские буквы и цифры в любом сочетании, заглавный и строчной регистр.

После успешного формирования заявки на регистрацию Пользователя:

- если в регистрируемом сертификате электронная подпись имеет значение «Администратор организации», заявка принимается автоматически;
- если в сертификате электронной подписи отсутствует роль «Администратор организации»:
  - при наличии в организации другого зарегистрированного пользователя с правами «Администратор организации» и действующим сертификатом электронной подписи такой Пользователь может самостоятельно одобрить заявку в своем личном кабинете (раздел меню «Личный кабинет» – «Заявка на регистрацию пользователей»).
  - при отсутствии возможности самостоятельно принять заявку необходимо написать письмо на адрес [info@sberbank-ast.ru](mailto:info@sberbank-ast.ru) с просьбой одобрить заявку.

#### 4.1.2. Авторизация на портале Госуслуги с помощью КЭП

Адрес – <https://www.gosuslugi.ru/legal-entity>.

Для авторизации на портале Госуслуги с помощью электронной подписи перейдите на сайт Госуслуги. В разделе «Вход в Госуслуги» нажмите на кнопку **Войти** (рис. 4.1.2.1.).



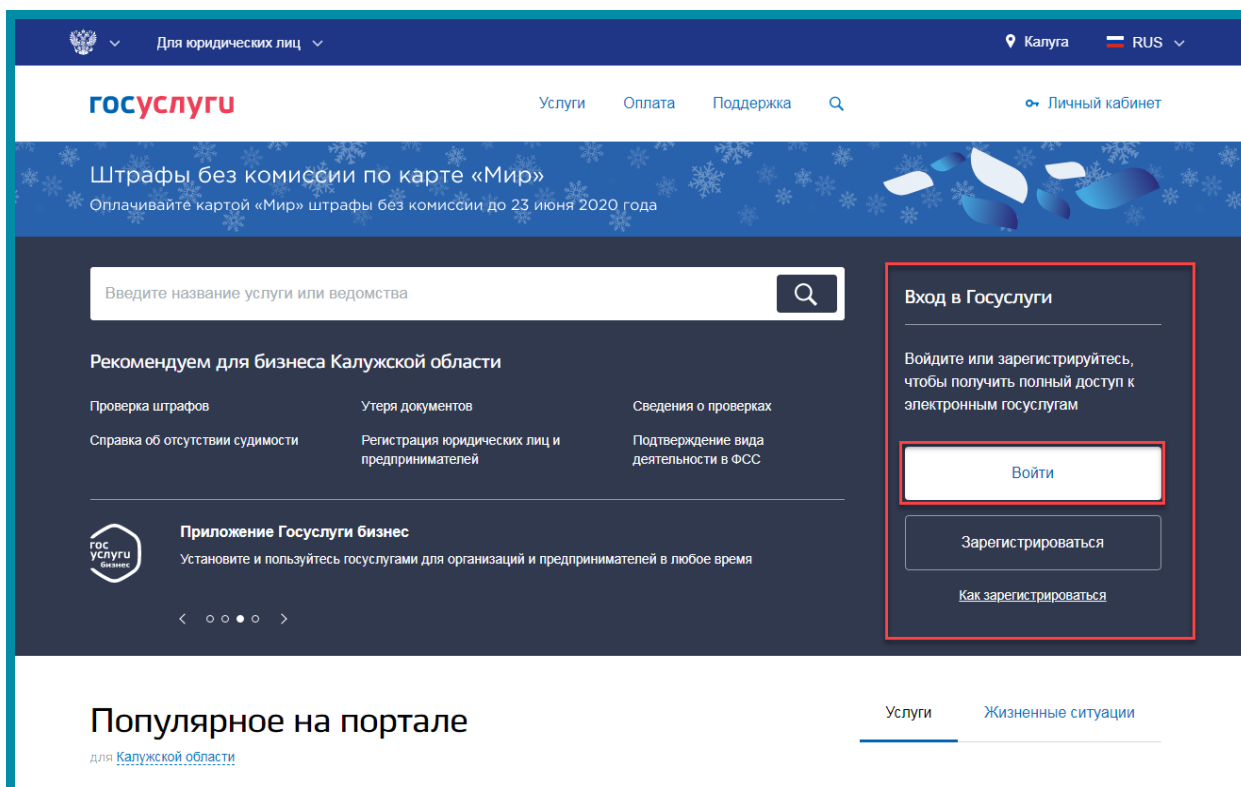


Рис. 4.1.2.1.

В открывшемся окне нажмите на кнопку Вход с помощью электронной подписи (рис. 4.1.2.2.).

госуслуги Единая система идентификации и аутентификации

## Вход

для портала Госуслуг

**Телефон или почта** СНИЛС

Мобильный телефон или почта

Пароль [Показать](#)

Чужой компьютер

**Войти**

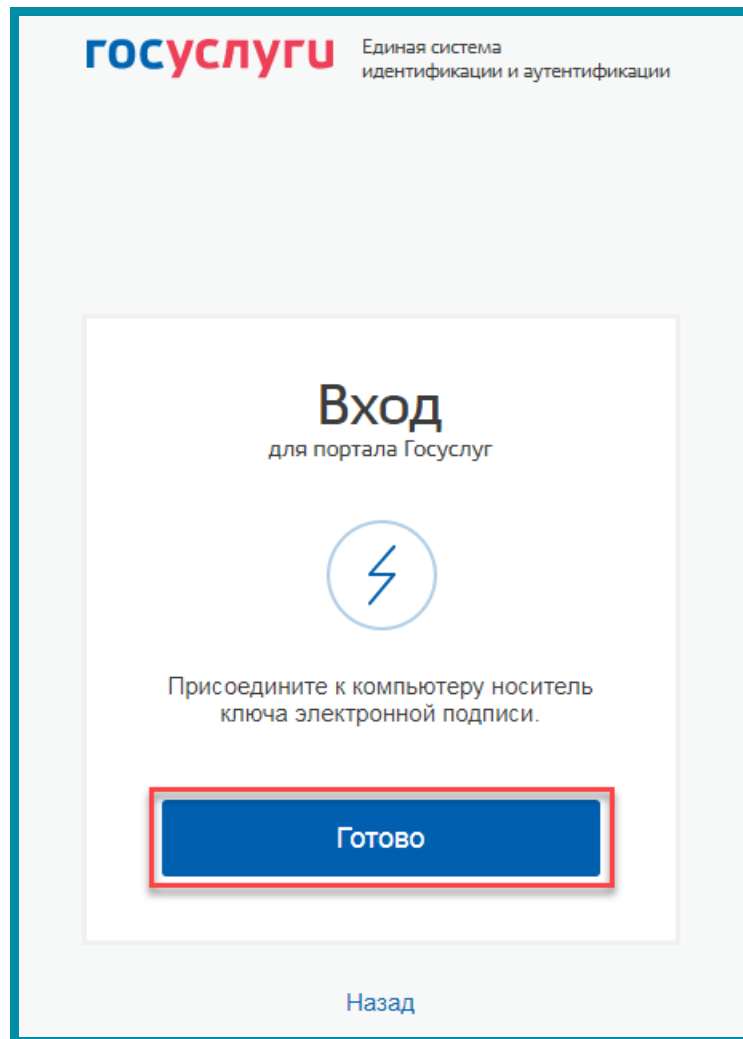
[Я не знаю пароль](#)

Зарегистрируйтесь для полного доступа к сервисам

[Вход с помощью электронной подписи](#)

Рис. 4.1.2.2.

На следующем шаге убедитесь, что носитель ключа электронной подписи подключен к компьютеру (если сертификат храниться в реестре подключать не нужно ничего), после нажмите **Готово** (рис. 4.1.2.3.).



*Рис. 4.1.2.3.*

В открывшемся окне выберите сертификат ключа проверки электронной подписи нажав на него левой кнопкой мыши (*рис. 4.1.2.4.*).

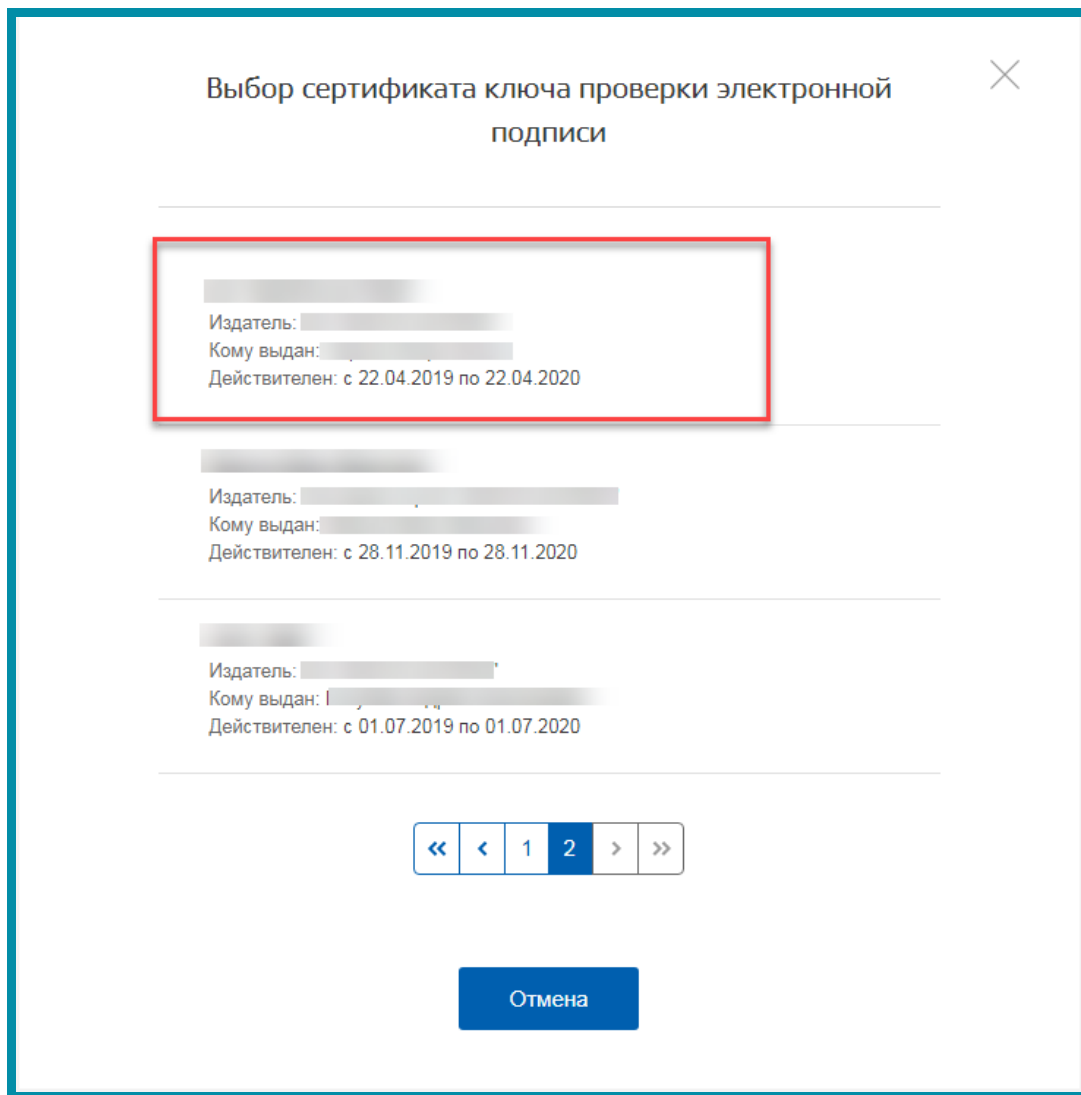


Рис. 4.1.2.4.

#### 4.1.3. ГАС «Правосудие»

Адрес – <https://ej.sudrf.ru/>.

Справочная информация по регистрации на портале - <https://ej.sudrf.ru/info>.

Доступ к сервису ЭП предоставляется физическим лицам, имеющим уровень достоверности идентификации пользователя не ниже чем «подтвержденная учетная запись» в ЕСИА или усиленная электронная цифровая подпись (далее – УКЭП), построенная на алгоритмах шифрования ГОСТ.

Для того чтобы зарегистрироваться на главном окне портала нажмите кнопку **Вход** (рис. 4.1.3.1.).

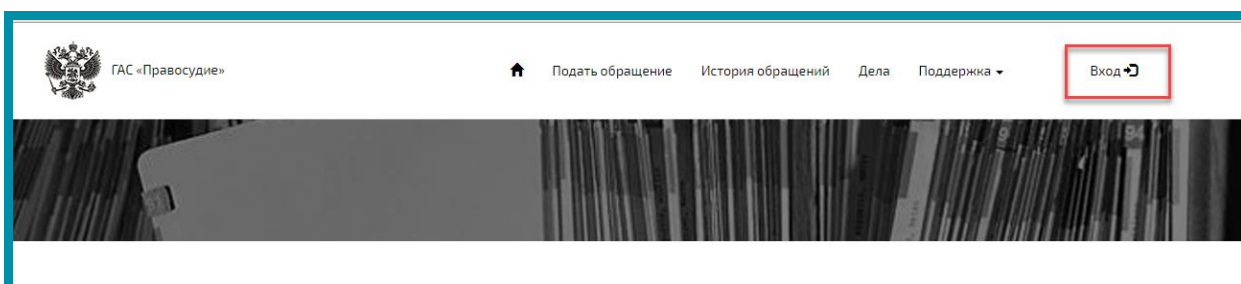


Рис. 4.1.3.1.

В открывшемся окне ознакомьтесь с документом «Пользовательское соглашение» и установите соответствующий флажок (рис. 4.1.3.2., 1) затем нажмите кнопку **Войти** (рис. 4.1.3.2., 2), если уже зарегистрированы в ЕСИА либо **Пройти регистрацию в ЕСИА** (рис. 4.1.3.2., 3).

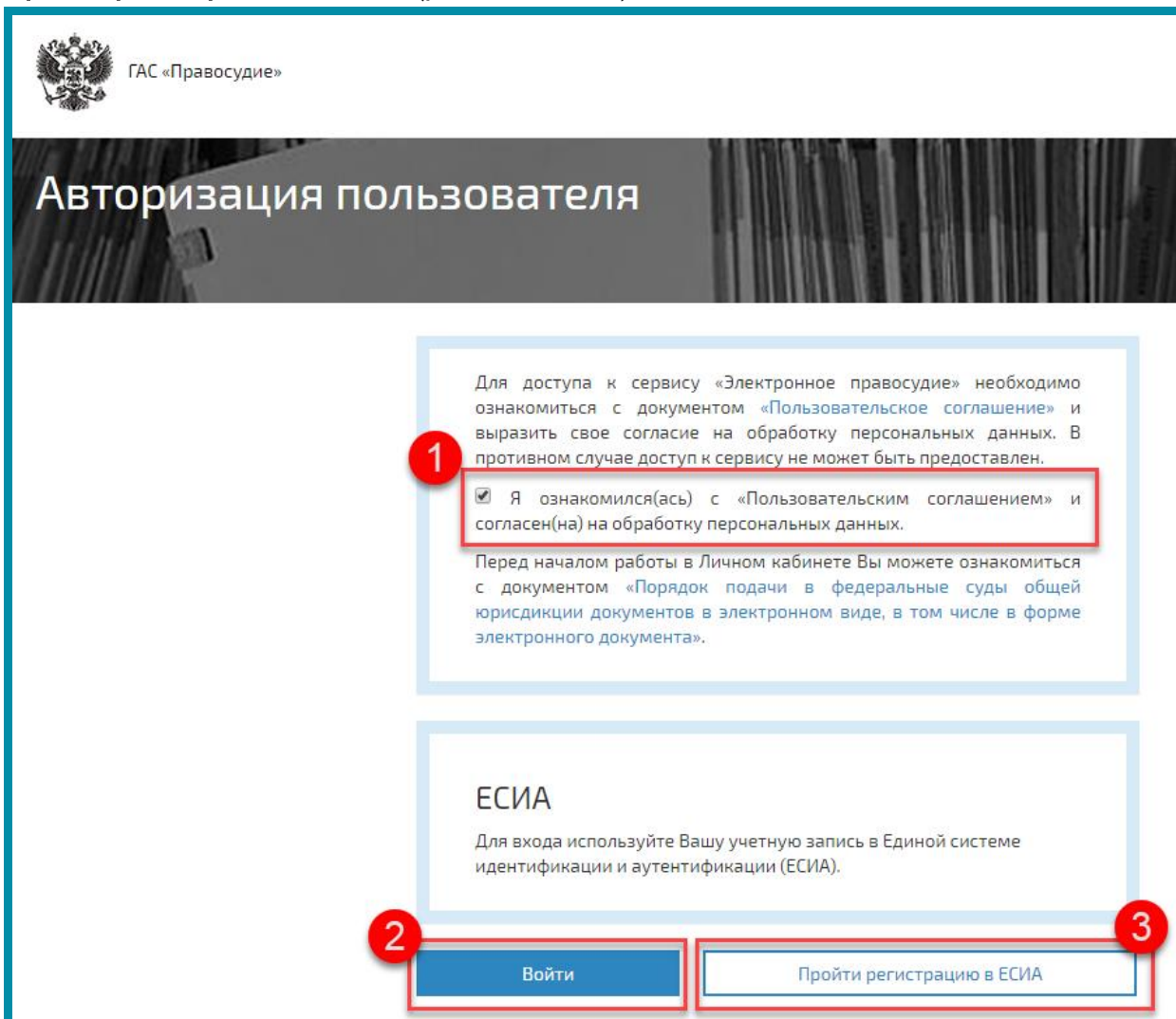


Рис. 4.1.3.2.



Доступ к ЛК ЭП посредством усиленной квалифицированной подписи возможен только в браузере Internet Explorer, версии не ниже 11.0.9.

#### 4.1.4. Вход на портал mos.ru

Адрес – <https://oauth20.mos.ru/sps/login.jsp>.

Подробное описание – [https://www.mos.ru/pgu/common/legal\\_new.pdf](https://www.mos.ru/pgu/common/legal_new.pdf).

Для авторизации на портале перейдите по ссылке <https://www.mos.ru/> и нажмите кнопку **Войти** (рис. 4.1.4.1.).

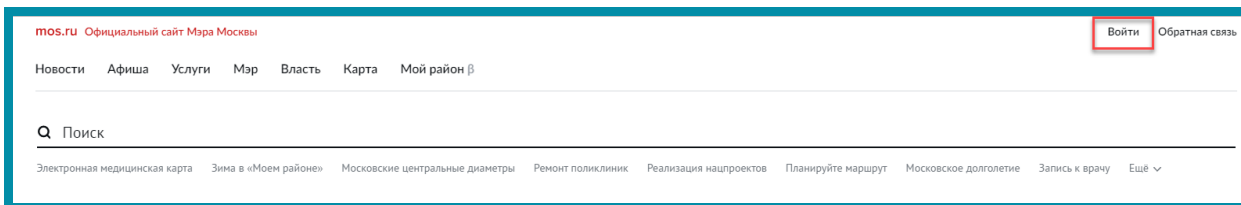


Рис. 4.1.4.1.

В открывшемся окне выберите способ авторизации **Войти по электронной подписи** либо **Госуслуги** (если авторизованы в системе ЕСИА) (рис. 4.1.4.2.).

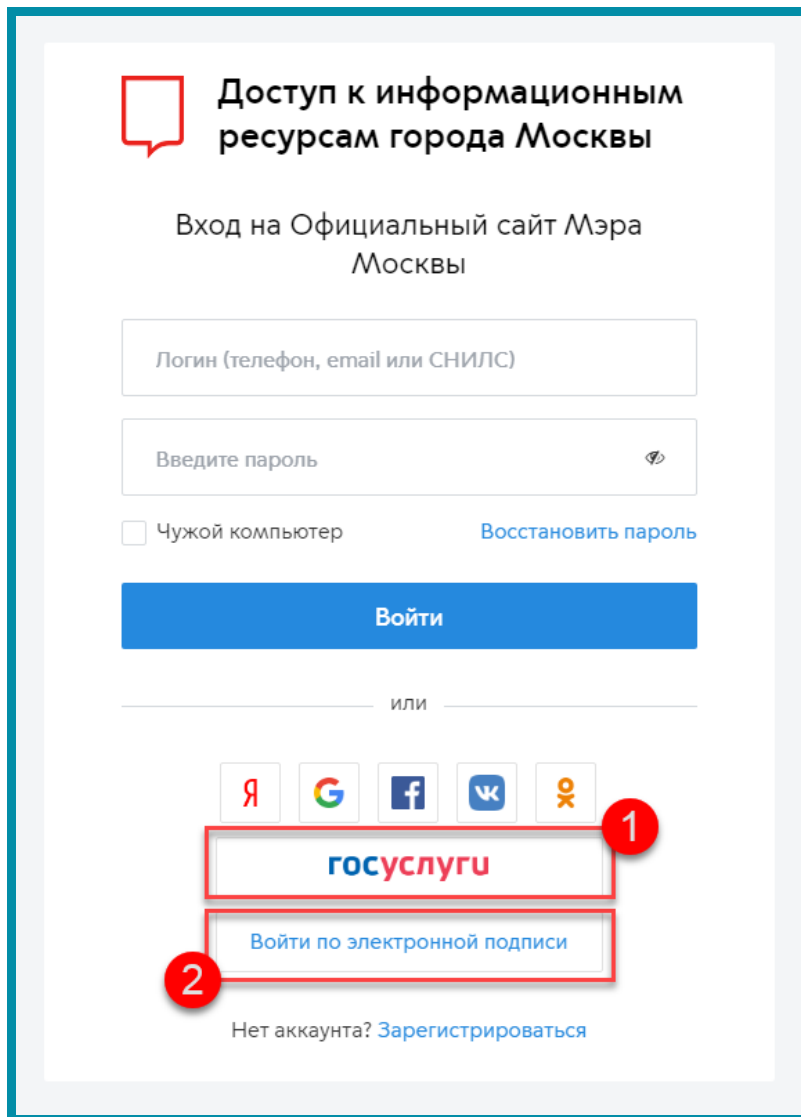


Рис. 4.1.4.2.



*В соответствии с выбранным способом регистрации следуйте указаниям для авторизации.*

#### 4.1.5. ГИС ЖКХ

Адрес – <https://dom.gosuslugi.ru/#!/main>

Для входа в личный кабинет перейдите на сайт ГИС ЖКХ и нажмите кнопку **Войти** на главном меню (рис. 4.1.5.1.).

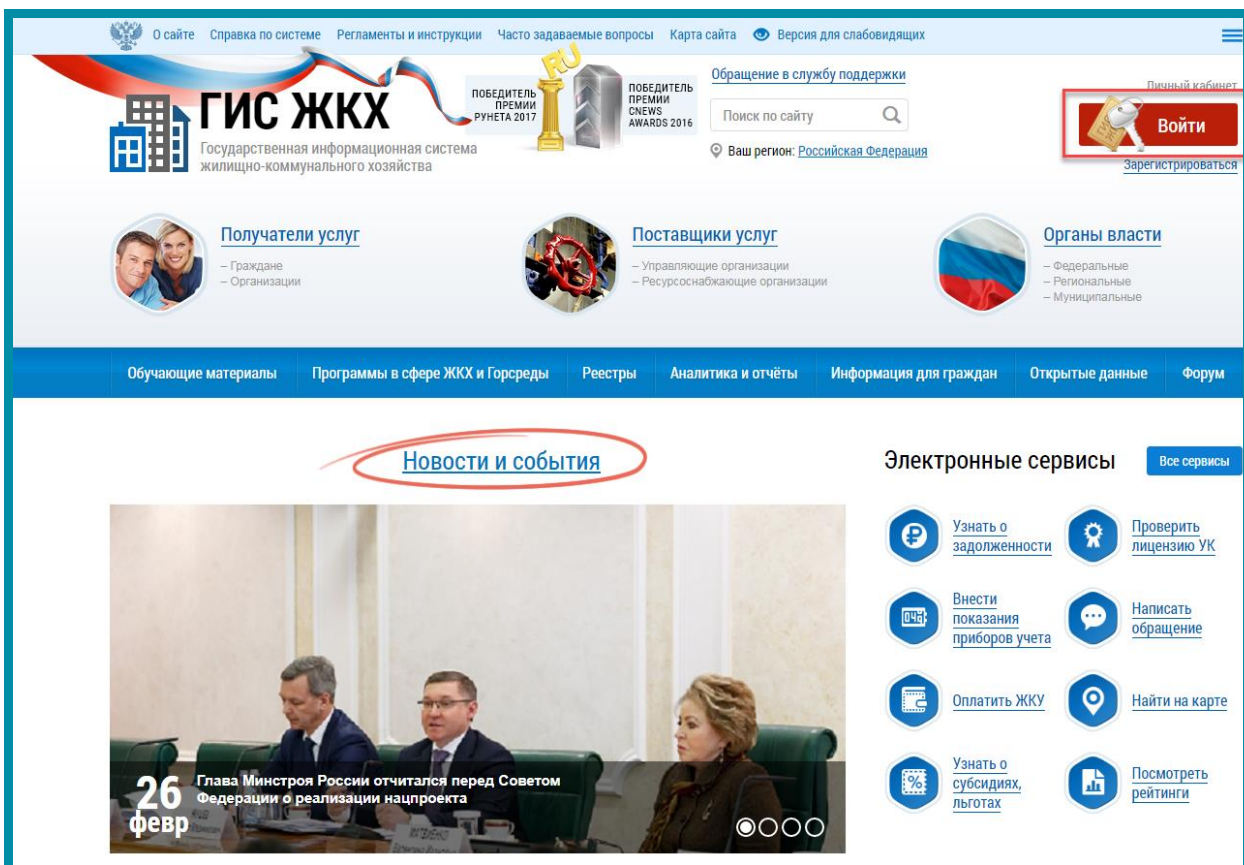


Рис. 4.1.5.1.

Авторизация на портале ГИС ЖКХ осуществляется через портал государственных услуг. Инструкцию по авторизации на сайте Госуслуги см. в [п. 4.1.2.](#)

После авторизации на сайте Госуслуги будет выполнено перенаправление на главную страницу личного кабинета портала ГИС ЖКХ.

#### 4.1.6. Вход на портал Росреестра с помощью электронной подписи

Адрес – <https://rosreestr.ru/site/fiz/>.

Для входа в личный кабинет Росреестра перейдите по ссылке <https://rosreestr.ru/> и нажмите кнопку **Личный кабинет** (рис. 4.1.6.1.).

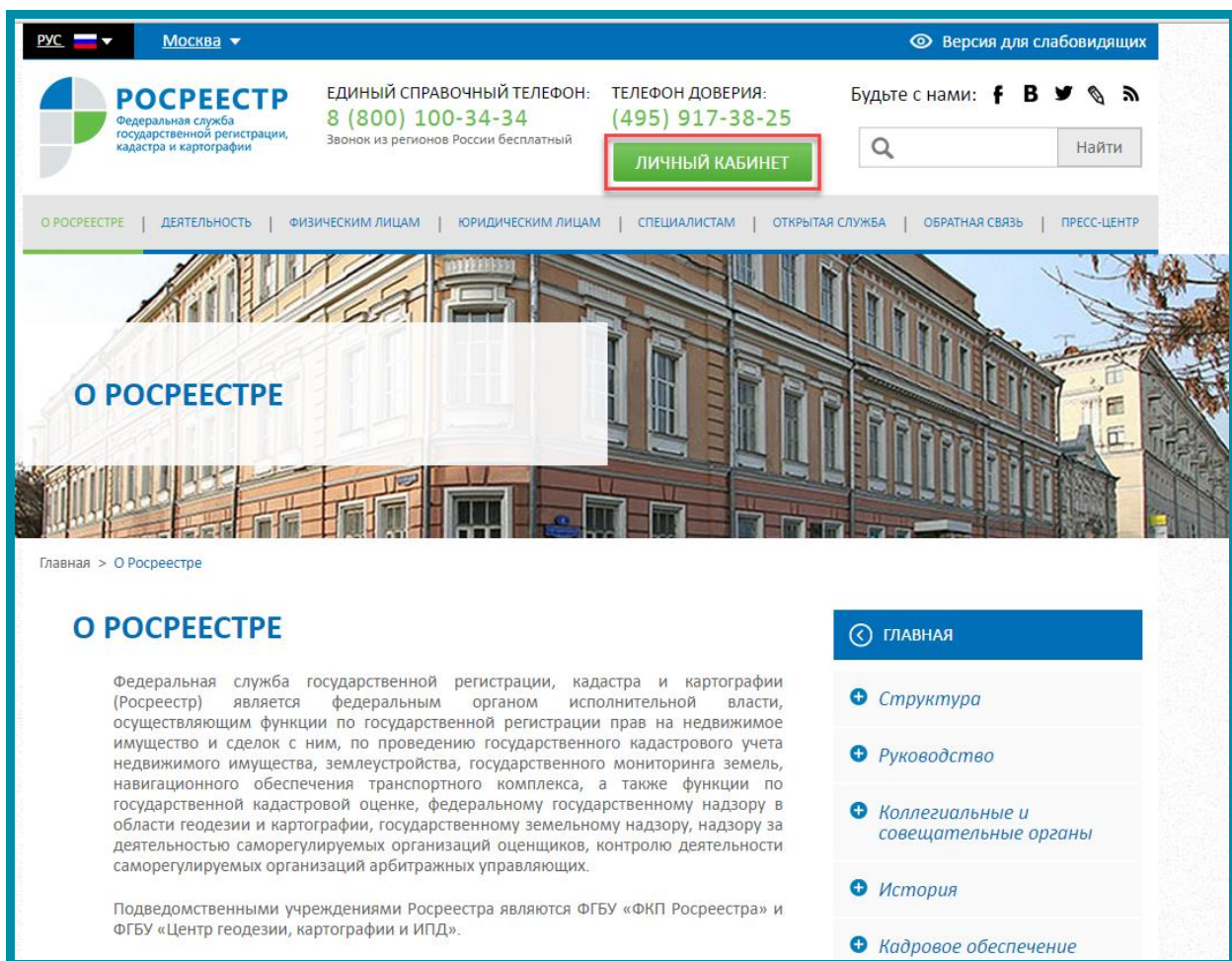


Рис. 4.1.6.1.

Авторизация на портале Росреестр осуществляется через портал государственных услуг. Инструкцию по авторизации на сайте Госуслуги см. в [п. 4.1.2.](#)

После авторизации Вы будете переадресованы на главную страницу личного кабинета портала Росреестра.

## 4.2. Проверка подписи

Для определения даты сертификата ЭП и сети, в которой он выпущен, откройте сертификат и ознакомьтесь с данной информацией. Это можно сделать способами, описанными ниже.

### 4.2.1. Открытие сертификата через свойства браузера

Зайдите в меню «Пуск» – «Панель управления» и выберите раздел **Свойства браузера** (Свойства обозревателя) (рис. 4.2.1.1.). Для удобства навигации установите тип просмотра «Мелкие значки».



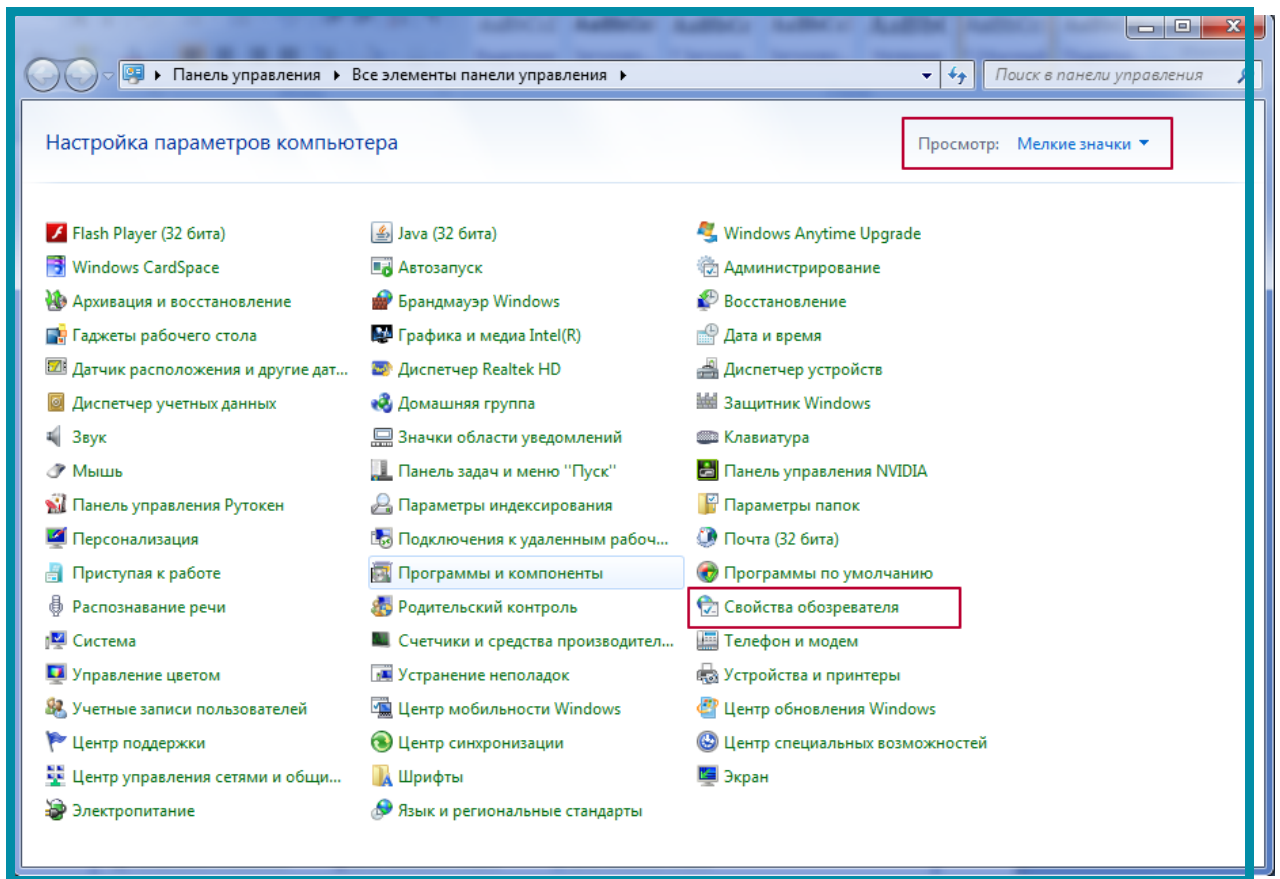


Рис. 4.2.1.1.

Перейдите во вкладку «Содержание» и нажмите кнопку **Сертификаты** (рис. 4.2.1.2.).

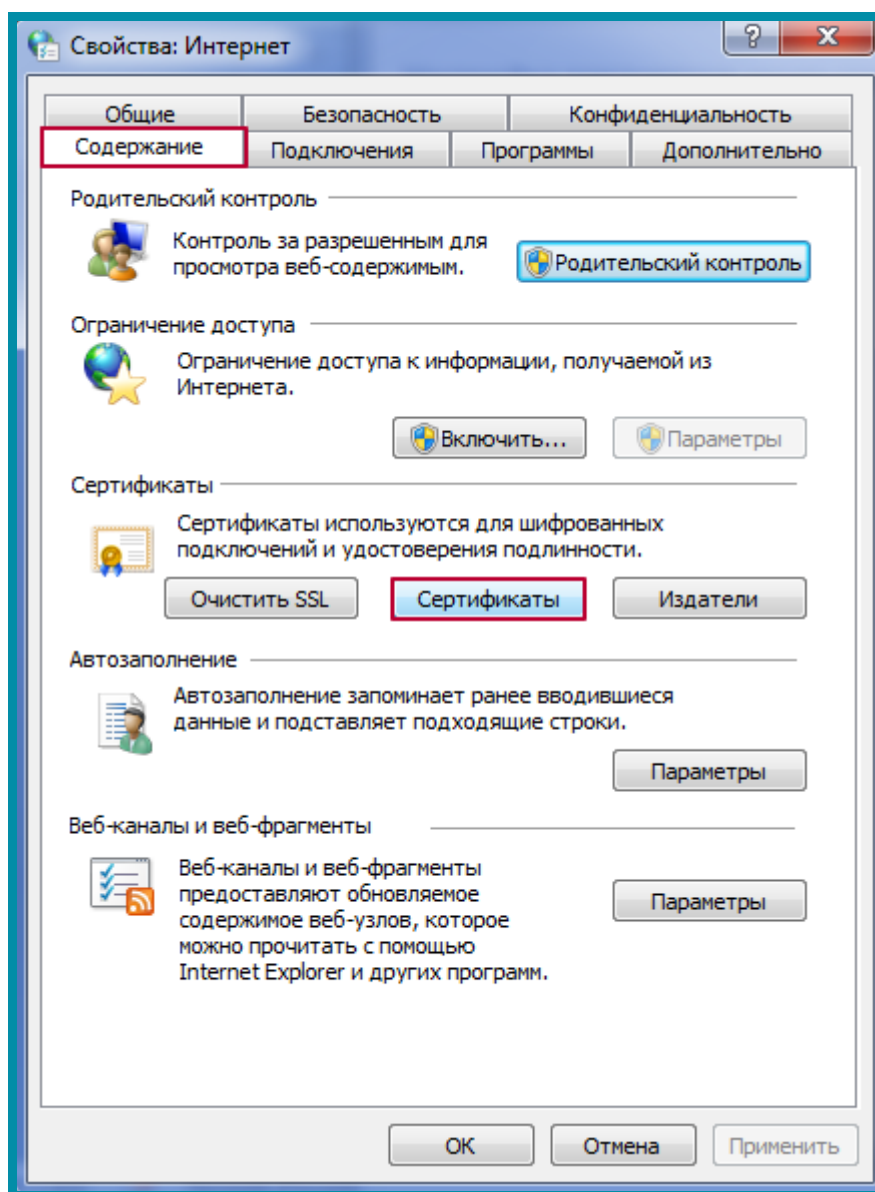


Рис. 4.2.1.2.

В открывшемся списке сертификатов выберите требуемый и откройте его двойным щелчком левой кнопки мыши.

#### 4.2.2. Открытие сертификата с помощью СКЗИ

Открыть сертификат ЭП возможно с помощью СКЗИ, установленного на компьютере.

Если Вы используете ViPNet CSP, запустите программу, перейдите во вкладку «Контейнеры ключей» и дважды щелкните левой кнопкой мыши по интересующему Вас контейнеру (рис. 4.2.2.1.).

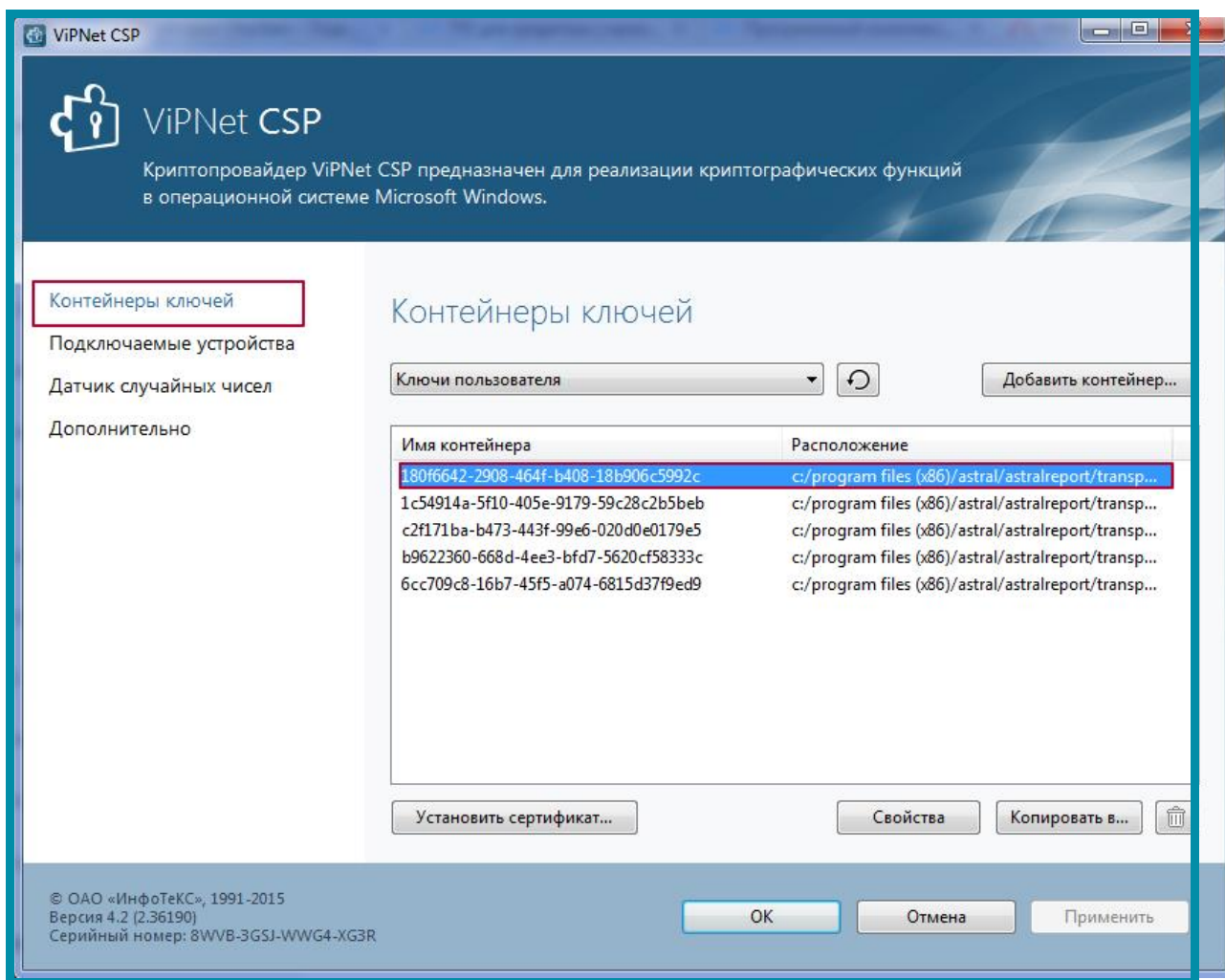


Рис. 4.2.2.1.

В появившемся окне нажмите кнопку **Открыть** либо изучите необходимую информацию внизу окна в поле **Сертификат** (рис. 4.2.2.2.).

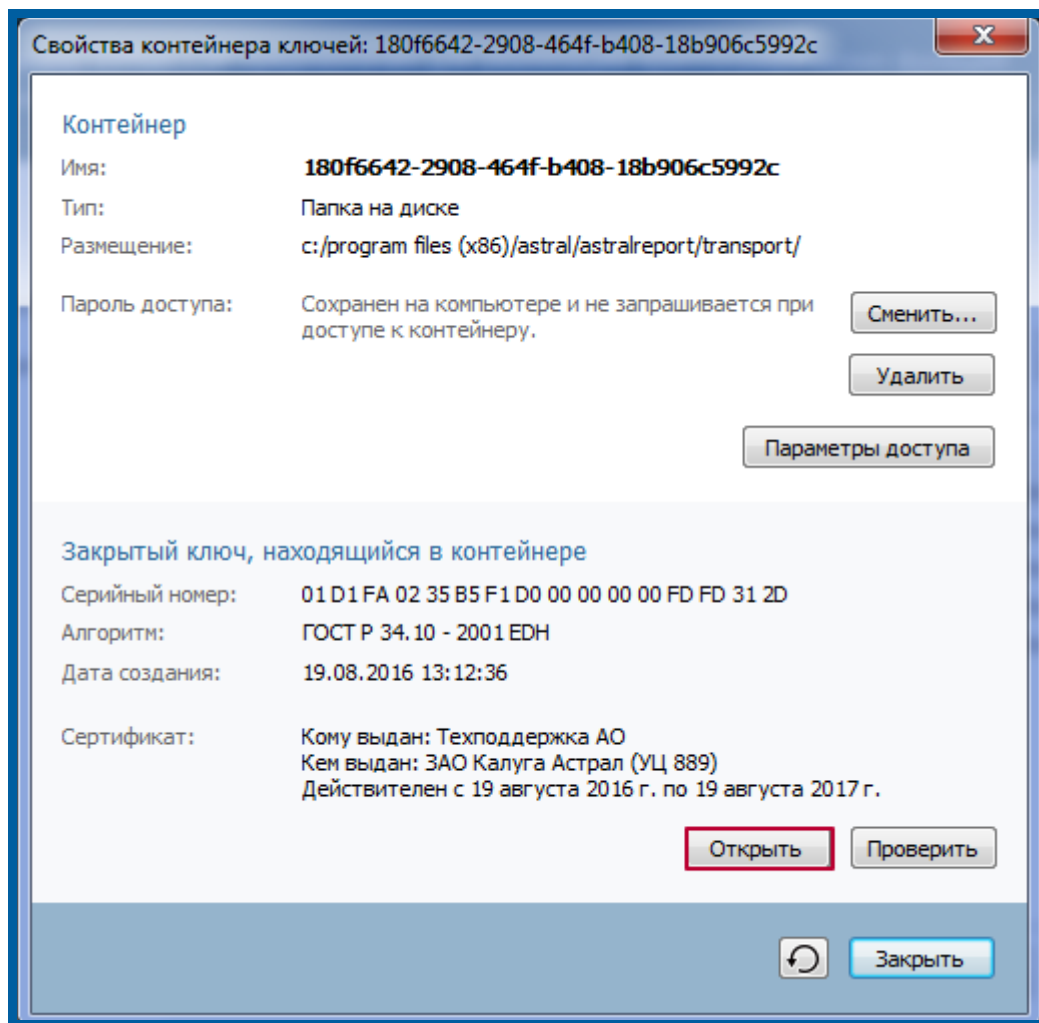


Рис. 4.2.2.2.

Если Вы используете КриптоПро CSP, запустите программу, перейдите на вкладку «Сервис» и нажмите кнопку **Просмотреть сертификаты в контейнере** (рис. 4.2.2.3.).

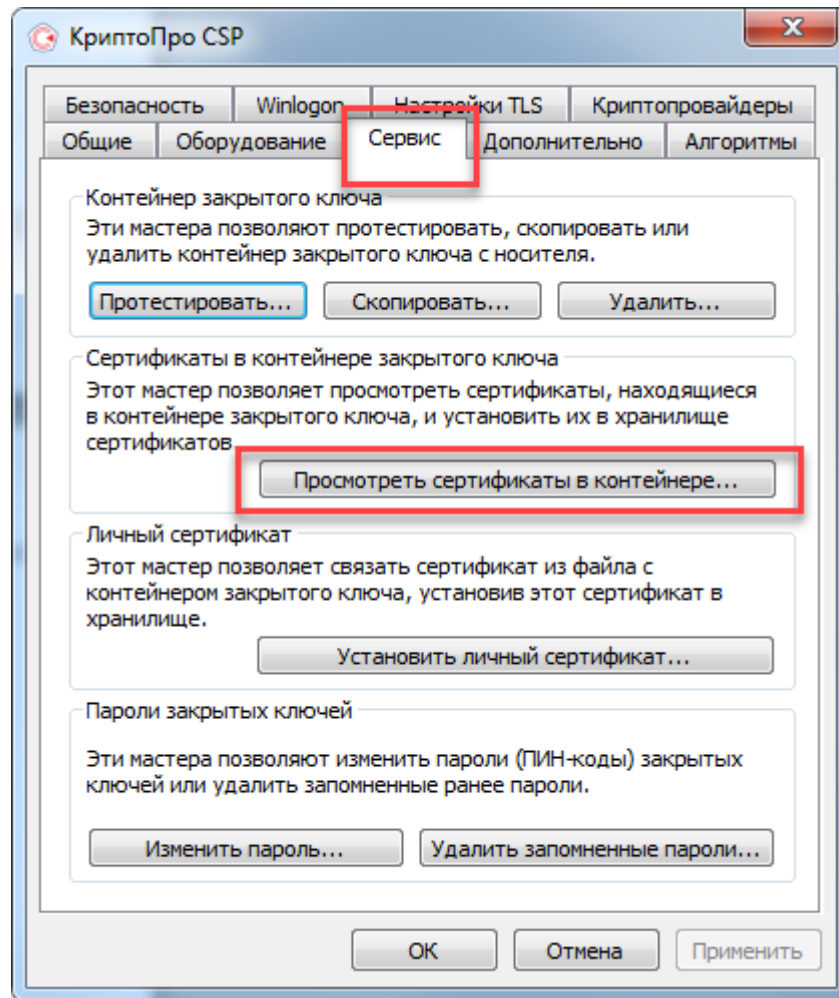


Рис. 4.2.2.3.

Затем нажмите кнопку **Обзор** (рис. 4.2.2.4.).

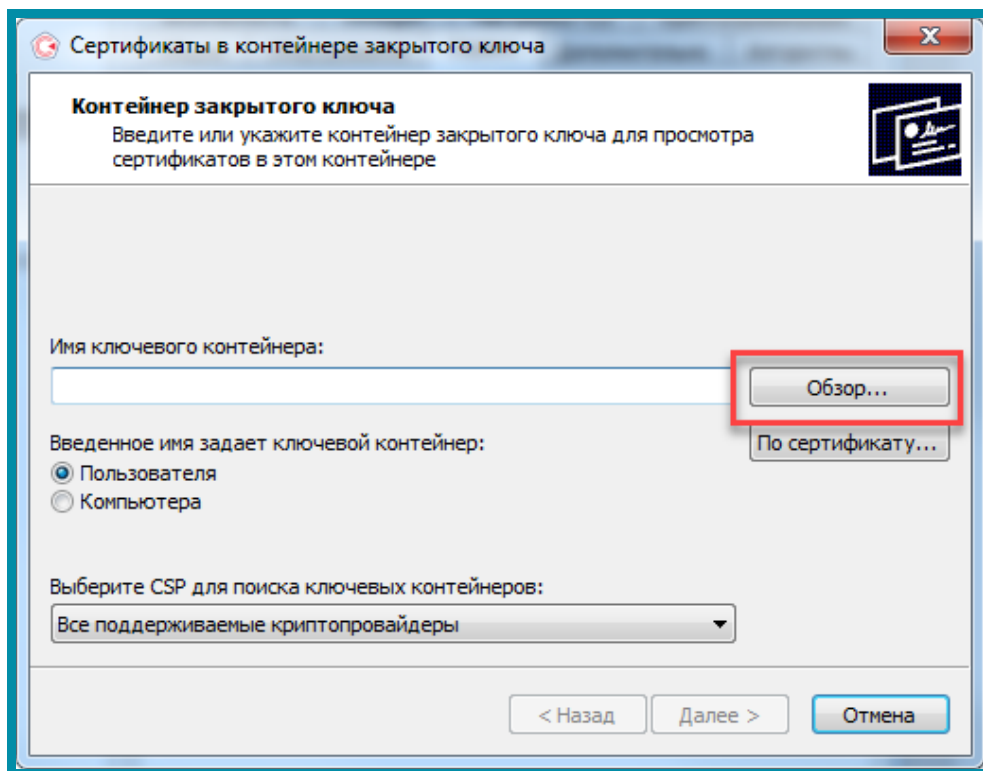


Рис. 4.2.2.4.

Из списка контейнеров выберите необходимый контейнер и нажмите кнопку ОК (рис. 4.2.2.5).

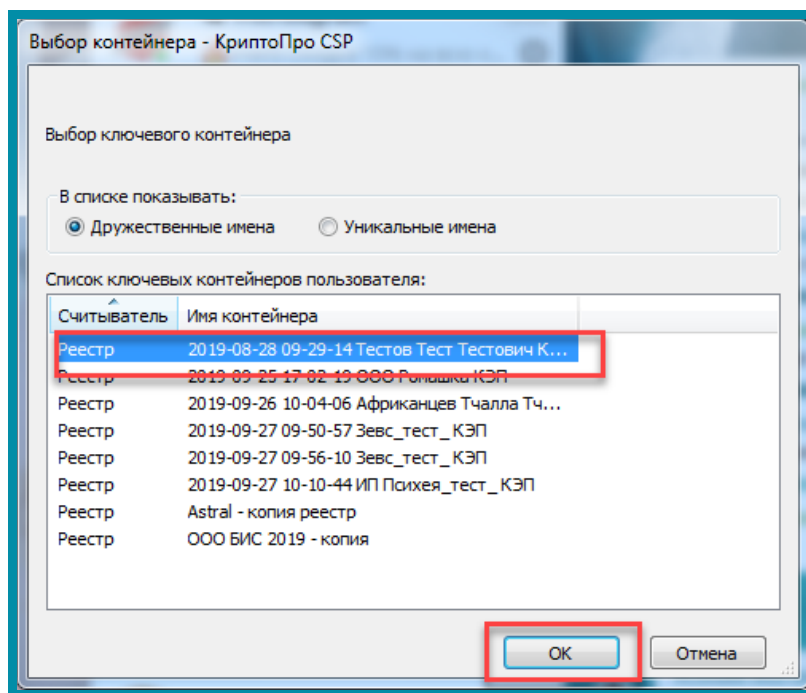


Рис. 4.2.2.5.

В открывшемся окне нажмите кнопку **Свойства** (рис. 4.2.2.6.).

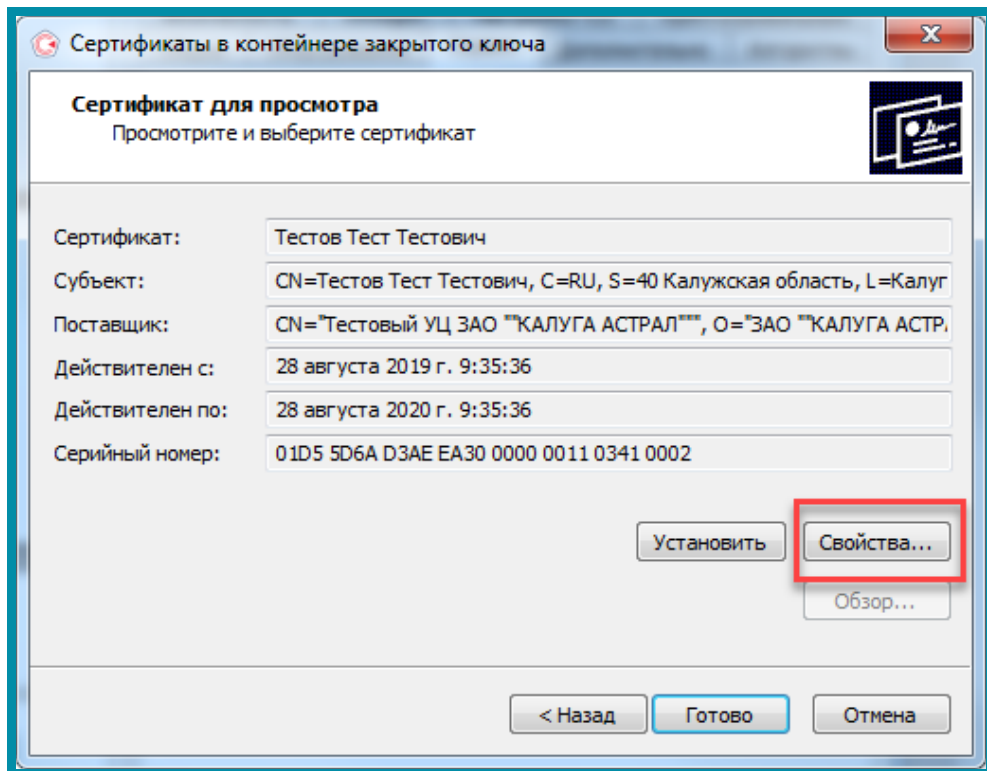


Рис. 4.2.2.6.

После открытия сертификата электронной подписи обратите внимание на срок его действия (рис. 4.2.2.7.).

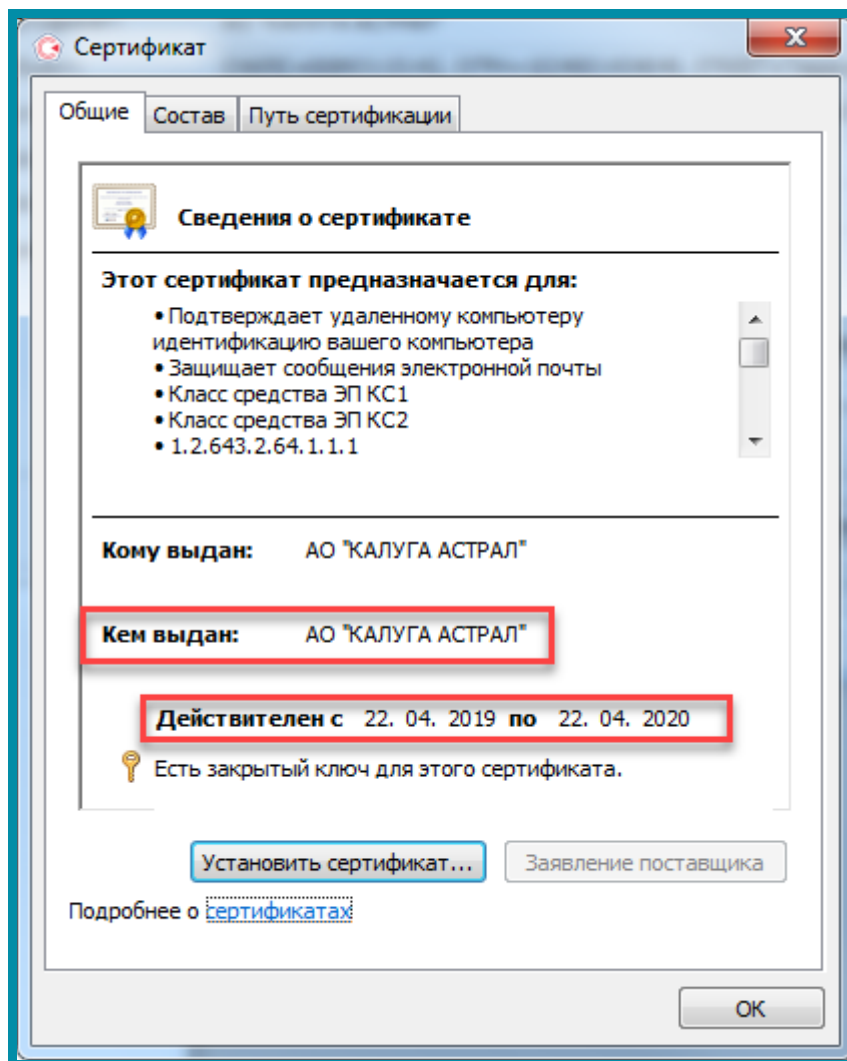


Рис. 4.2.2.7.

### 4.3. Действия при смене сертификата

Для перевыпуска электронной подписи за 20-30 дней до окончания срока действия текущей электронной подписи обратитесь [в точку выдачи](#) ЭП АО «КАЛУГА АСТРАЛ» по региону. Если точка выдачи в Вашем регионе отсутствует, обратитесь в ближайшую точку выдачи.

Процедура перевыпуска электронной подписи сводится к обращению в удостоверяющий центр и предоставлению необходимых документов. Если Вы ранее обращались в УЦ, вся информация там уже сохранена. Если не было никаких изменений в документах, достаточно будет заполнить заявление на продление и оплатить стоимость продления. Если обращение в УЦ было осуществлено после истечения срока действия электронной подписи, регистрация выполняется заново.

Повторно приобретать защищенные носители eToken или Rutoken, СКЗИ «КриптоПро CSP» не требуется. При условии, что на СКЗИ не истекает срок действия лицензии.



## **Заключение**

В настоящем документе приведена основная информация, необходимая Абонентам для получения и работы с электронной подписью, полученной в точках выдачи АО «КАЛУГА АСТРАЛ».