

**Установка драйверов для ключевых носителей  
JaCarta и Рутокен  
Руководство пользователя**

**Версия: 1.1.3.4.**

**Дата: 04.03.2021**

## СОДЕРЖАНИЕ

<b>АННОТАЦИЯ .....</b>	<b>3</b>
<b>УСЛОВНЫЕ ОБОЗНАЧЕНИЯ .....</b>	<b>4</b>
<b>ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.....</b>	<b>5</b>
<b>1. УСТАНОВКА ДРАЙВЕРОВ JACARTA.....</b>	<b>6</b>
1.2. ИНТЕРФЕЙС ЕДИНОГО КЛИЕНТА JACARTA И JACARTASECURLOGON.....	10
1.3. ОСОБЕННОСТИ РАБОТЫ С ЕДИНЫМ КЛИЕНТОМ JACARTA И JACARTASECURLOGON .....	11
<b>2.УСТАНОВКА ДРАЙВЕРОВ RUTOKEN .....</b>	<b>12</b>
<b>3. НАСТРОЙКА СЧИТЫВАТЕЛЕЙ В СКЗИ КРИПТОПРОСР .....</b>	<b>16</b>
<b>4. ПРОВЕРКА КОРРЕКТНОСТИ УСТАНОВКИ ДРАЙВЕРОВ.....</b>	<b>20</b>
4.1. ПРОВЕРКА ПОСРЕДСТВОМ СКЗИ VIPNET CSP .....	20
4.2. ПРОВЕРКА ПОСРЕДСТВОМ СКЗИ КРИПТОПРО CSP.....	20
<b>ЗАКЛЮЧЕНИЕ .....</b>	<b>23</b>

## **Аннотация**

В настоящем документе представлена информация, позволяющая Пользователю продукта Астрал Отчет самостоятельно произвести установку драйверов для защищенных носителей JaCarta и RuToken и выполнить все необходимые настройки.

## Условные обозначения

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

## Термины и определения

**eToken** – персональное средство строгой аутентификации и хранения данных, аппаратно поддерживающее работу с цифровыми сертификатами и ЭП.

**JaCarta PKI** – это линейка PKI-токенов для аутентификации пользователей в корпоративных системах, безопасного хранения ключевых контейнеров, сертификатов и т.д.

**Рутокен** – программные и аппаратные средства для многофакторной аутентификации пользователей, электронной подписи и безопасного хранения криптографических ключей.

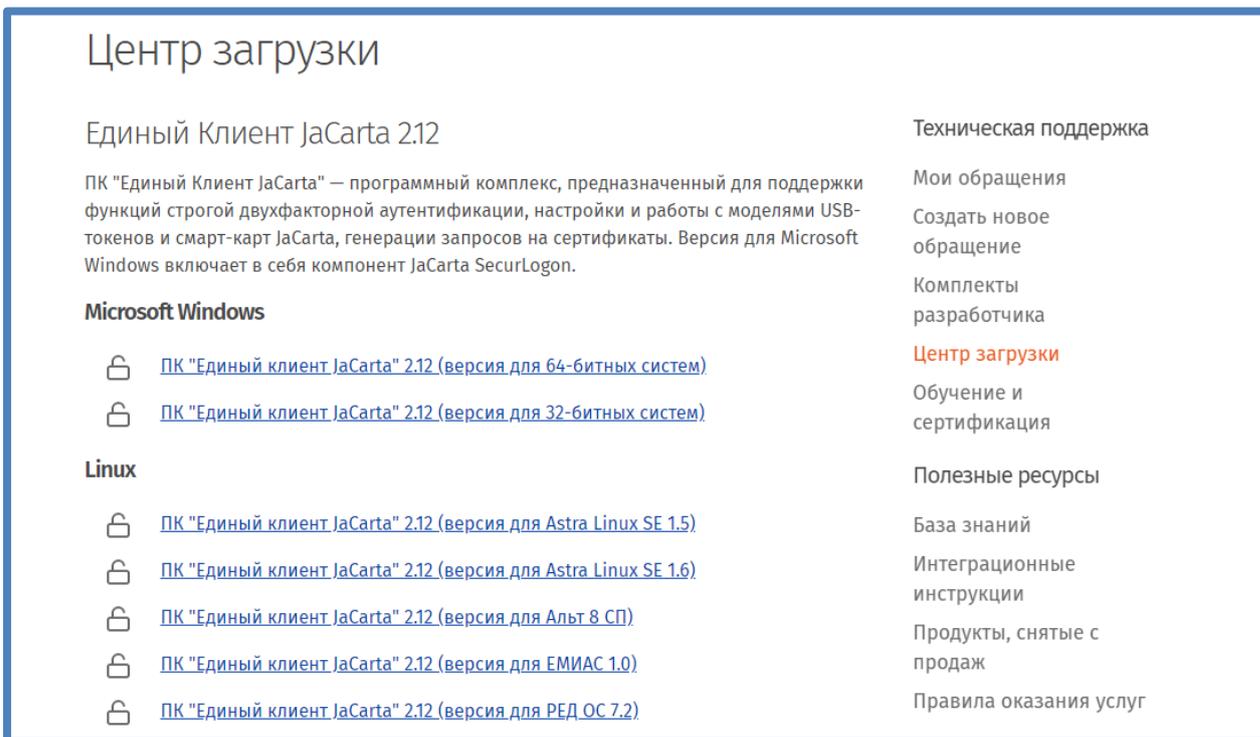
**Средство криптографической защиты, СКЗИ** – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем и осуществлять криптографическое преобразование информации для обеспечения ее безопасности.

**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 (п. 1 ст. 2 Федерального закона от № 63-ФЗ 06.04.2011 г.).

## 1. Установка драйверов JaCarta

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

Перейдите по ссылке <http://www.aladdin-rd.ru/support/downloads/jacarta/> и скачайте программу Единый Клиент JaCarta и JaCartaSecurLogon. Выберите версию 2.12 в зависимости от разрядности ос. (рис.1.).



Центр загрузки

Единый Клиент JaCarta 2.12

ПК "Единый Клиент JaCarta" – программный комплекс, предназначенный для поддержки функций строгой двухфакторной аутентификации, настройки и работы с моделями USB-токенов и смарт-карт JaCarta, генерации запросов на сертификаты. Версия для Microsoft Windows включает в себя компонент JaCarta SecurLogon.

**Microsoft Windows**

- ПК "Единый клиент JaCarta" 2.12 (версия для 64-битных систем)
- ПК "Единый клиент JaCarta" 2.12 (версия для 32-битных систем)

**Linux**

- ПК "Единый клиент JaCarta" 2.12 (версия для Astra Linux SE 1.5)
- ПК "Единый клиент JaCarta" 2.12 (версия для Astra Linux SE 1.6)
- ПК "Единый клиент JaCarta" 2.12 (версия для Альт 8 СП)
- ПК "Единый клиент JaCarta" 2.12 (версия для ЕМИАС 1.0)
- ПК "Единый клиент JaCarta" 2.12 (версия для РЕД ОС 7.2)

Техническая поддержка

- Мои обращения
- Создать новое обращение
- Комплекты разработчика
- Центр загрузки
- Обучение и сертификация

Полезные ресурсы

- База знаний
- Интеграционные инструкции
- Продукты, снятые с продаж
- Правила оказания услуг

Рис. 1.



Для установки программы Единый Клиент JaCarta и JaCartaSecurLogon на рабочем месте Пользователя должна быть установлена одна из следующих операционных систем:

- 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).

Из содержимого архива выберите дистрибутив, соответствующий разрядности Вашей операционной системы, и запустите его. В появившемся окне приветствия Мастера установки нажмите кнопку **Next** (рис. 2.).

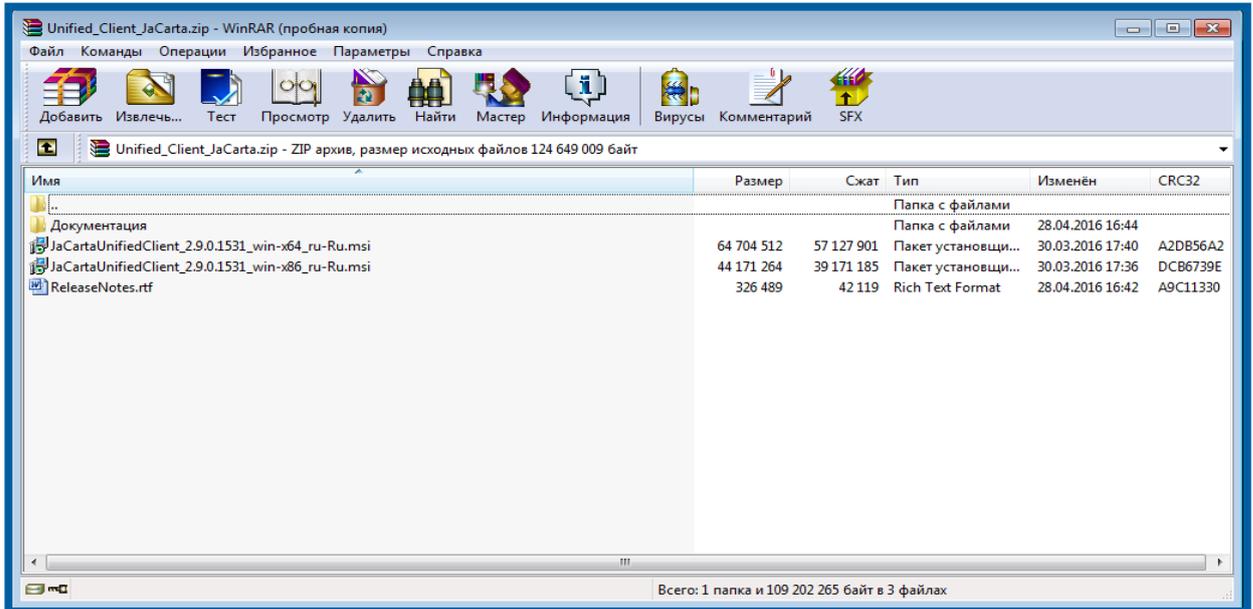


Рис. 2.

В окне приветствия Мастера установки нажмите кнопку **Далее** (рис. 3.).

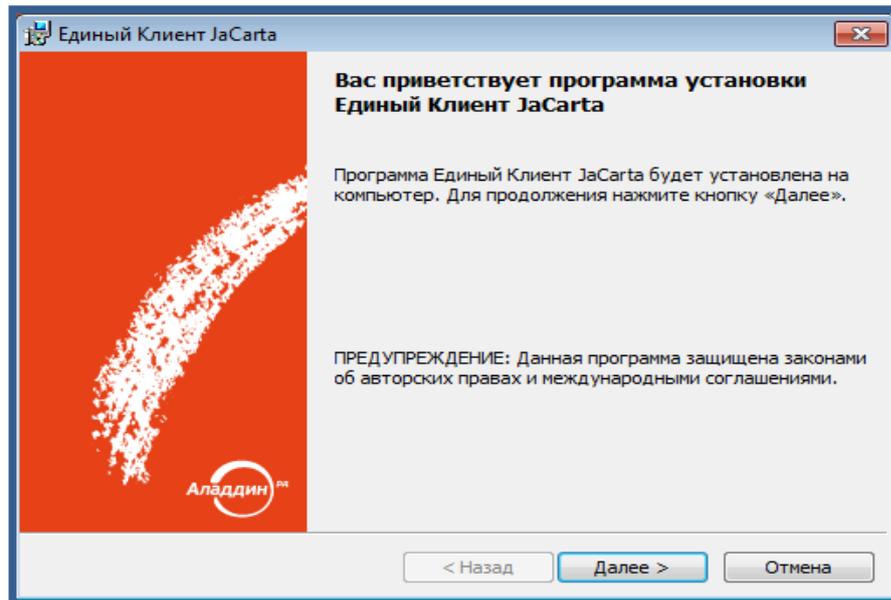
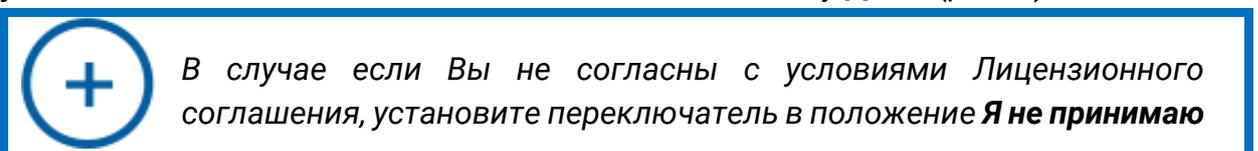


Рис. 3.

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.4.).



**условия лицензионного соглашения и нажмите кнопку **Далее**.**  
Установка программы будет прекращена.

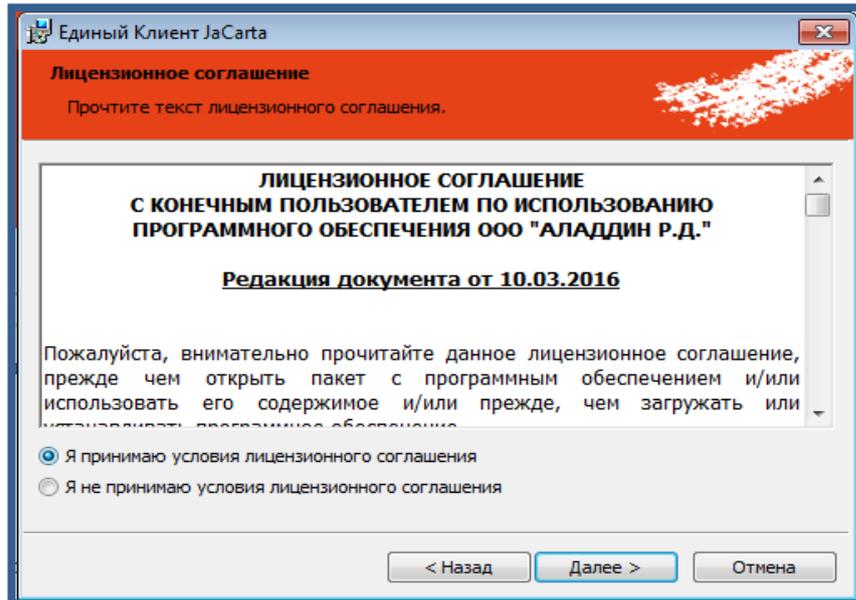


Рис. 4.

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.5.).

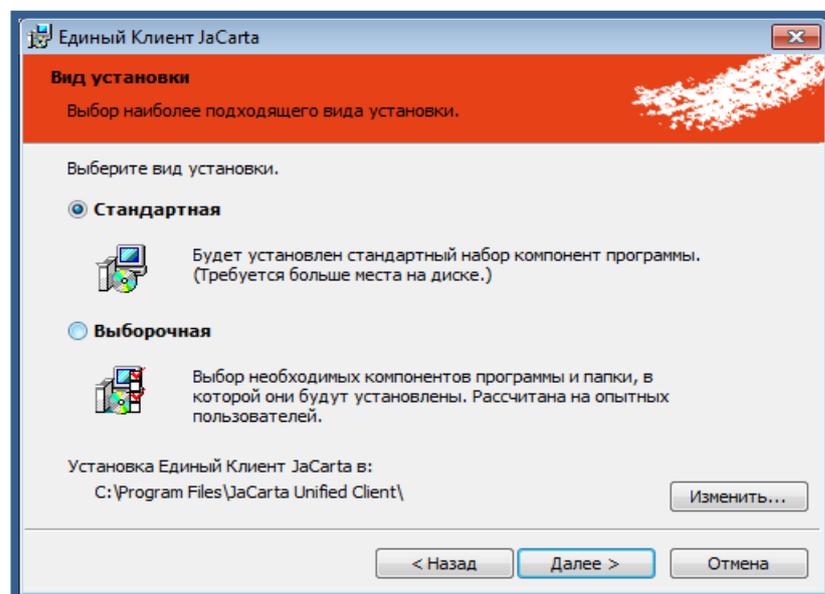


Рис. 5.

В следующем окне нажмите кнопку **Установить** (рис.6.).

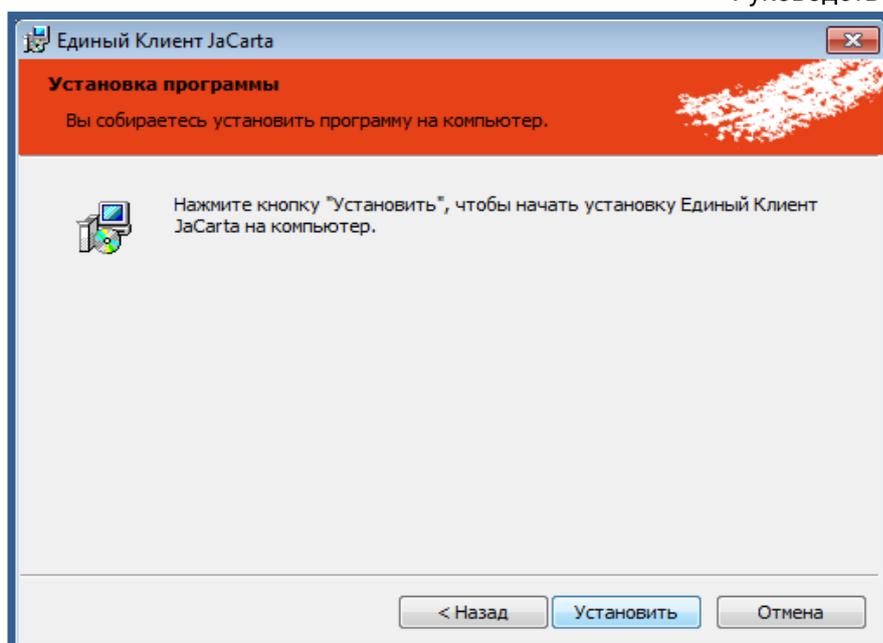


Рис. 6.

По завершению установки нажмите кнопку **Готово** (рис. 7.).

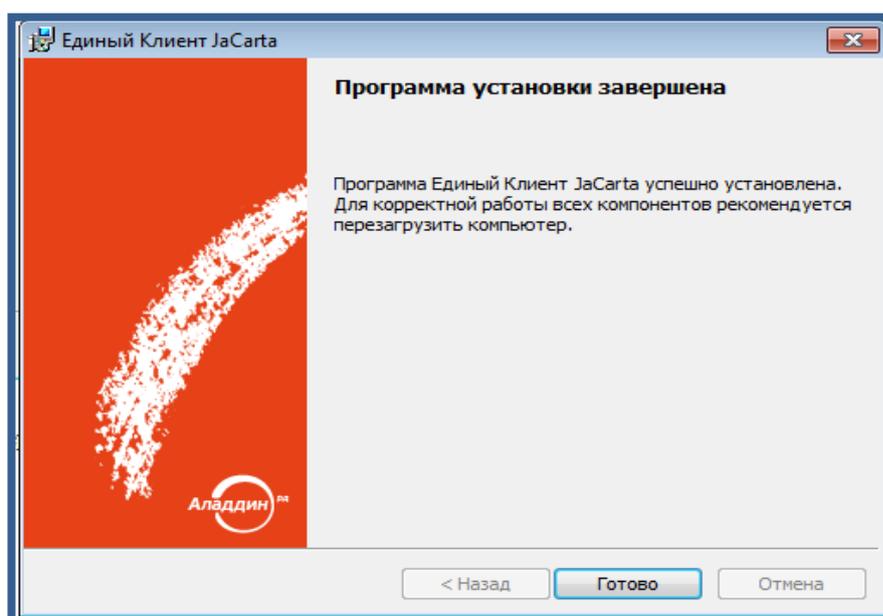


Рис. 7.

Перезагрузите компьютер.

## 1.2. Интерфейс Единого клиента JaCarta и JaCartaSecurLogon

В правом нижнем углу экрана Вашего компьютера расположена область уведомлений панели задач. Эта область содержит значок программы Единый клиент JaCarta и JaCartaSecurLogon (рис. 8).

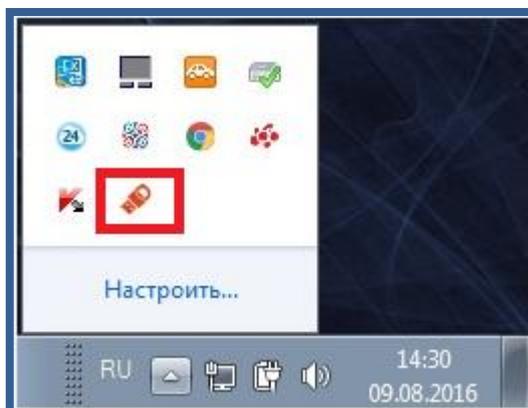


Рис. 8.

Для открытия меню программы Единый клиент JaCarta и JaCartaSecurLogon нажмите правой кнопкой на вышеобозначенном значке программы Единый клиент JaCarta и JaCartaSecurLogon в области уведомлений и выберите пункт **Единый Клиент JaCarta и JaCartaSecurLogon**.

В верхней части левой панели отображаются подсоединенные к компьютеру электронные ключи. Значок электронного ключа зависит от типа этого электронного ключа (рис. 9.).

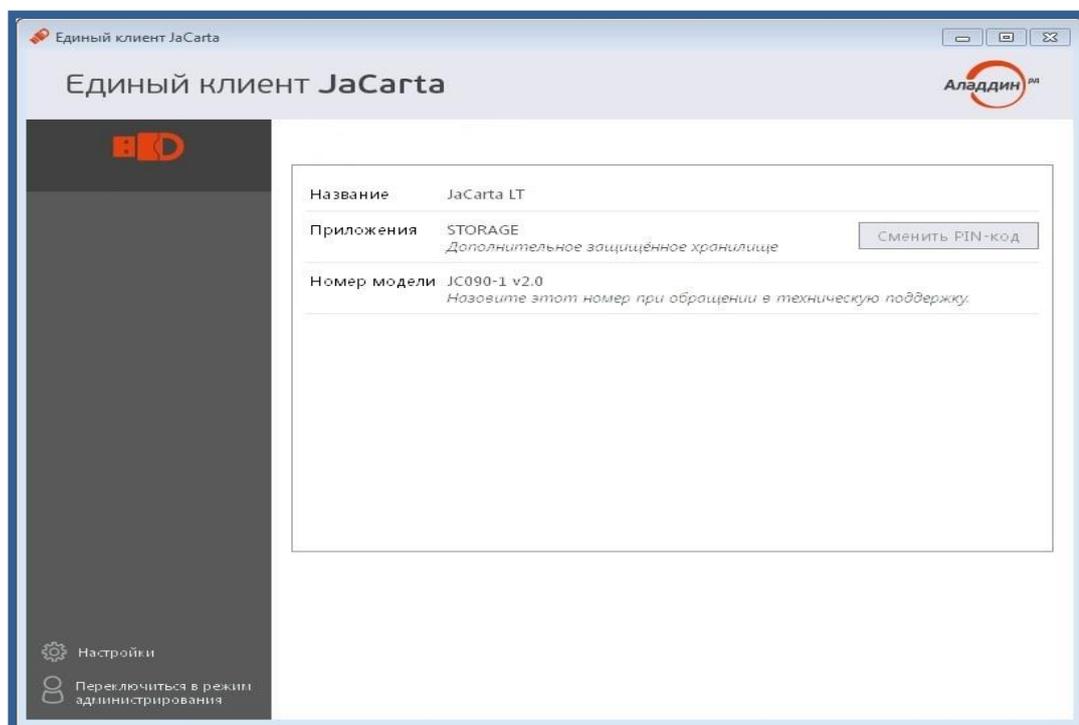


Рис. 9.

В окне меню программы доступен функционал настройки и переключения в режим Администратора/Пользователя.

### **1.3. Особенности работы с Единым клиентом JaCarta и JaCartaSecurLogon**

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

Носитель JaCarta работает только с СКЗИ КриптоПро CSP 4.0R3.

Носитель JaCarta с криптопровайдером ViPNet CSP может некорректно работать на операционной системе Windows 10, поскольку версия ViPNetCSP для Windows 10 на данный момент находится на стадии бета-тестирования.

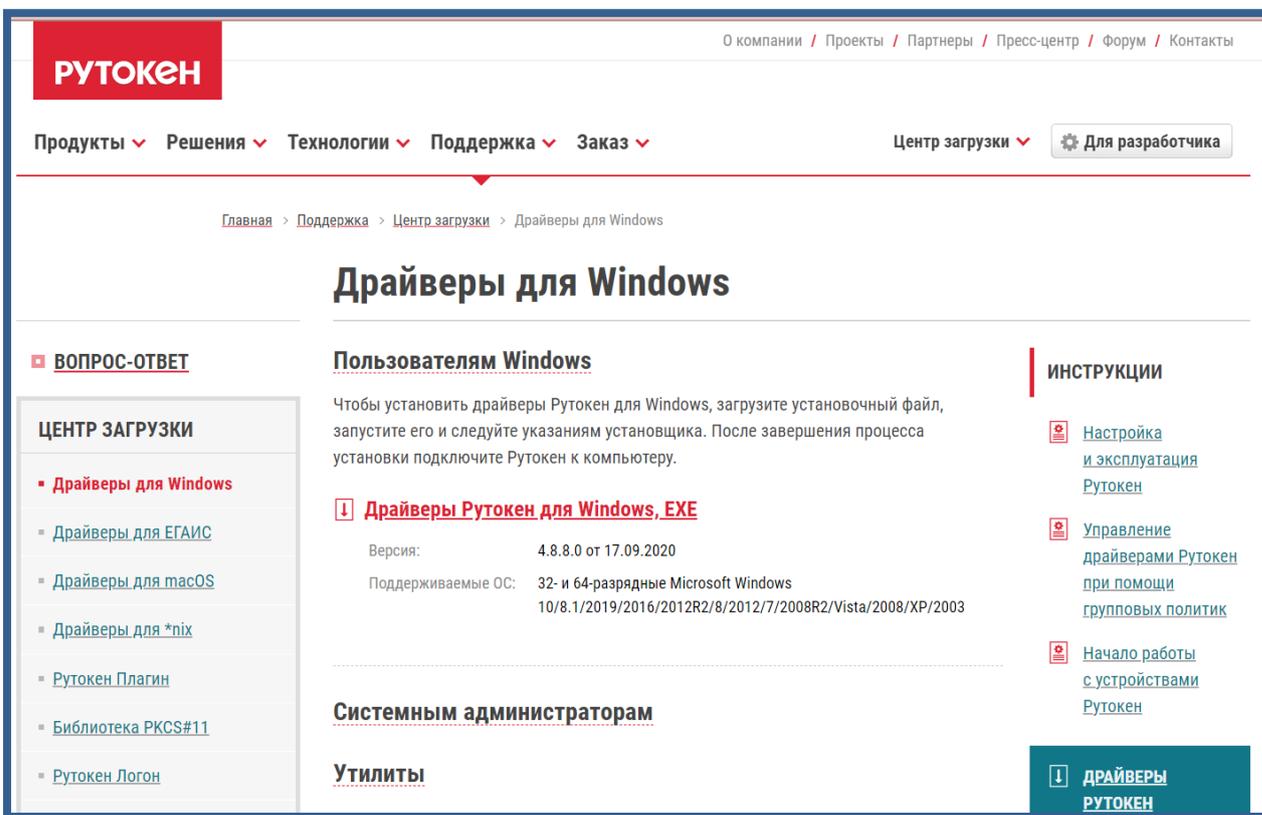
После установки программы Единый Клиент JaCarta установка на это же рабочее место JC-Client не допускается.

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

## 2. Установка драйверов RuToken

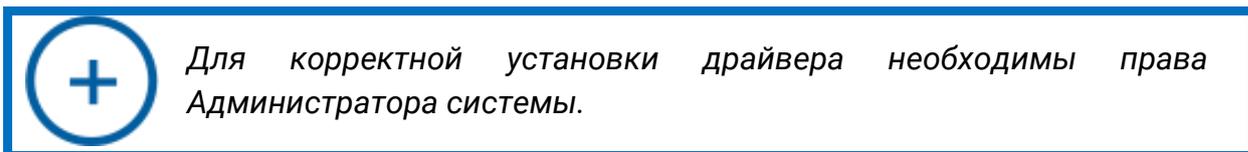
Для работы с носителем Рутокен необходима установка на рабочее место соответствующих драйверов. Для установки произведите следующие действия.

Перейдите по ссылке <http://www.rutoken.ru/support/download/drivers-for-windows/> и скачайте драйвер (рис. 10).



The screenshot shows the RuToken website's support page for Windows drivers. The page is titled "Драйверы для Windows" and includes a navigation menu with categories like "Продукты", "Решения", "Технологии", "Поддержка", and "Заказ". A sidebar on the left contains a "ЦЕНТР ЗАГРУЗКИ" (Download Center) with links for various operating systems and device types. The main content area features a "Пользователям Windows" (For Windows Users) section with instructions on how to install the drivers, a download link for "Драйверы Рутокен для Windows, EXE", and technical details such as version (4.8.8.0) and supported OS versions (32-bit and 64-bit Microsoft Windows from 10/8.1 to 2003). A right sidebar contains "ИНСТРУКЦИИ" (Instructions) with links for setup, management, and starting work with devices. A prominent blue button labeled "ДРАЙВЕРЫ РУТОКЕН" is located at the bottom right of the main content area.

Рис. 10.



Для корректной установки драйвера необходимы права Администратора системы.

Отсоедините Рутокен от USB-порта компьютера, запустите программу установки и нажмите кнопку **Установить** (рис.11.).

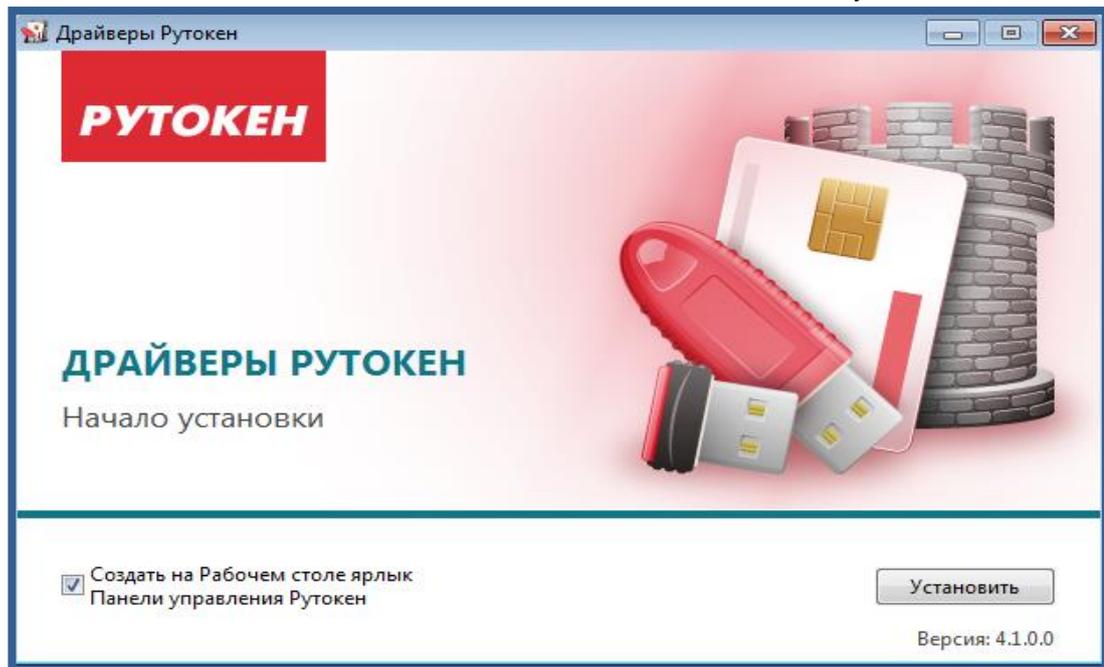


Рис. 11.

После начала установки может потребоваться перезагрузка компьютера. После перезагрузки программа продолжит установку автоматически. Дождитесь окончания установки драйверов (рис. 12.).

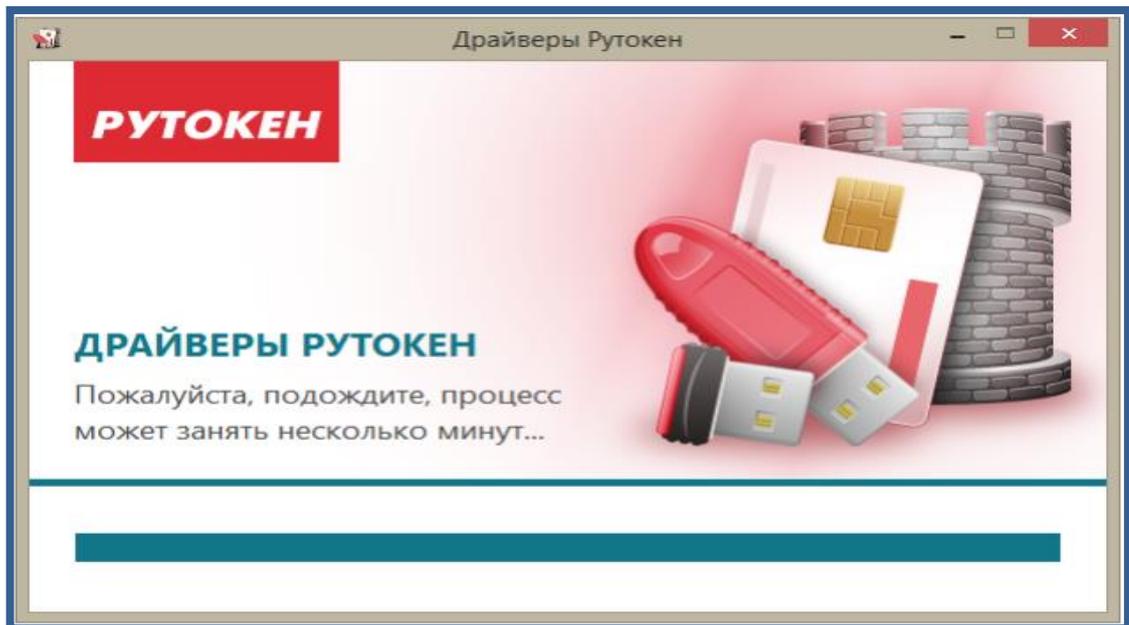


Рис.12.

После завершения установки драйвера вставьте Рутокен в USB-порт компьютера. Рутокен определится, после чего система установит для него драйвер (рис.13.).

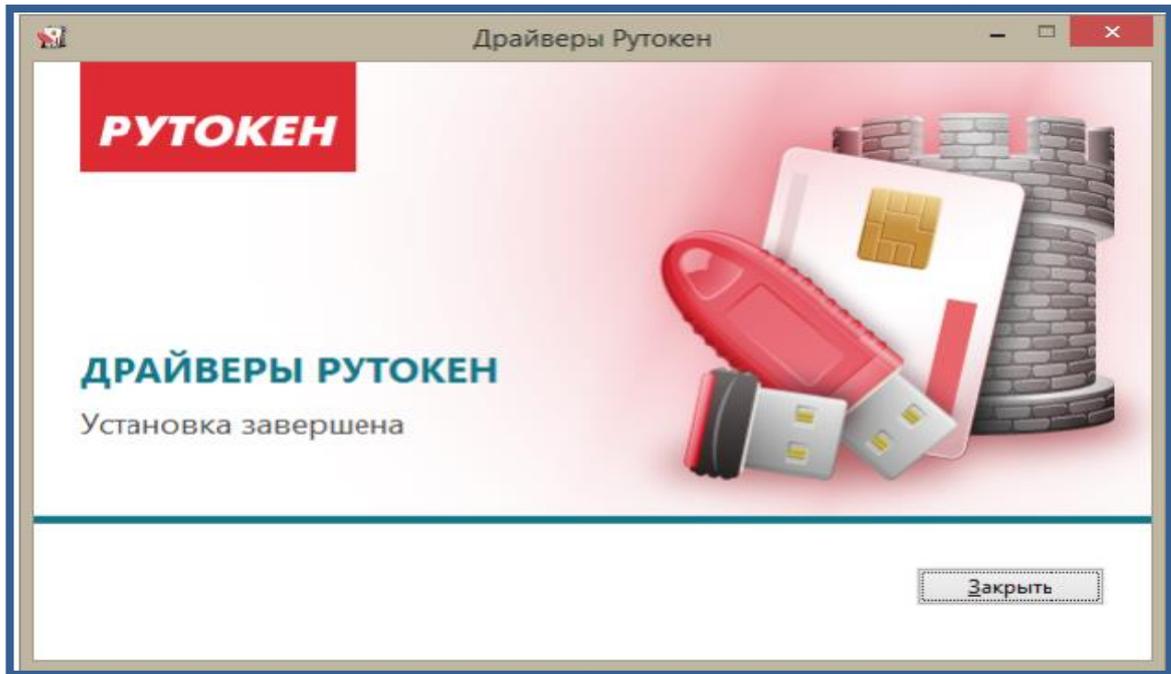


Рис. 13.

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.14.).



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

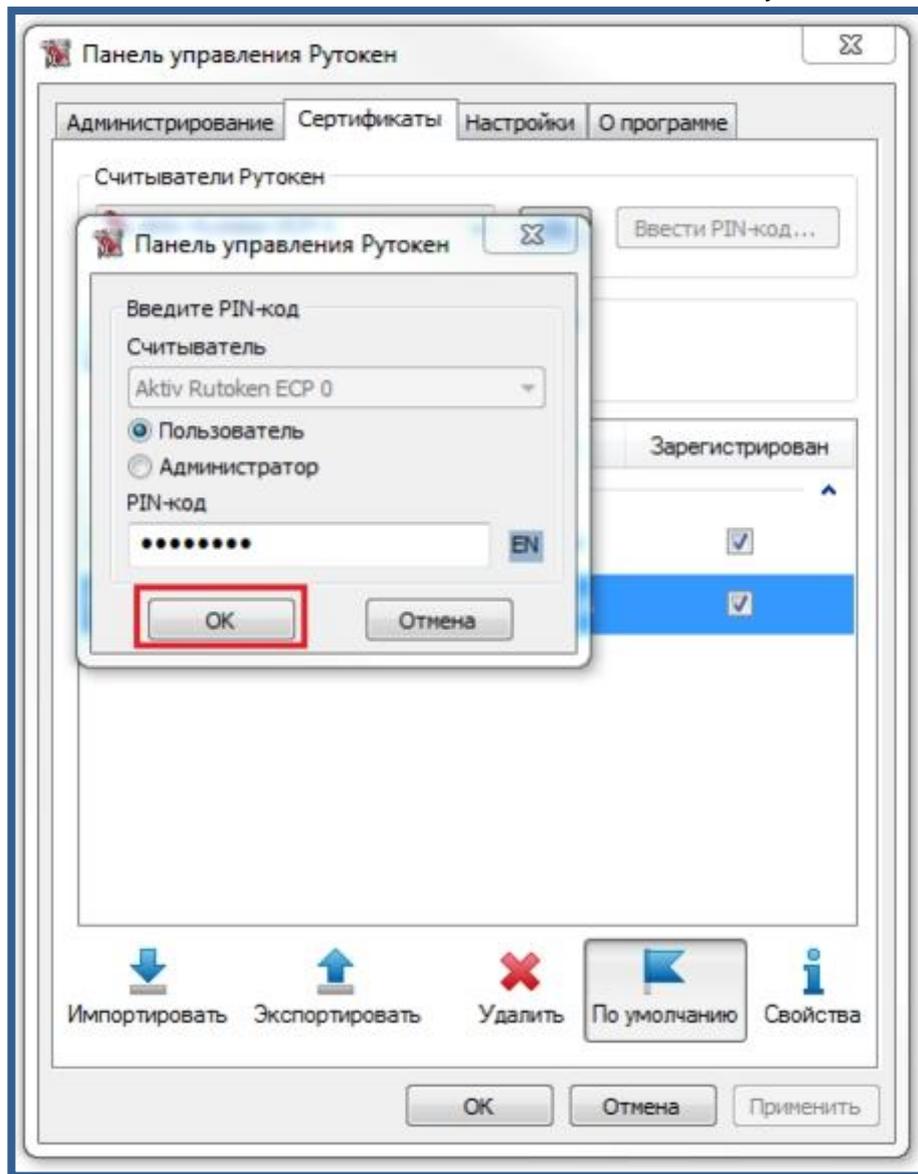


Рис. 14.

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

### 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. 15.).

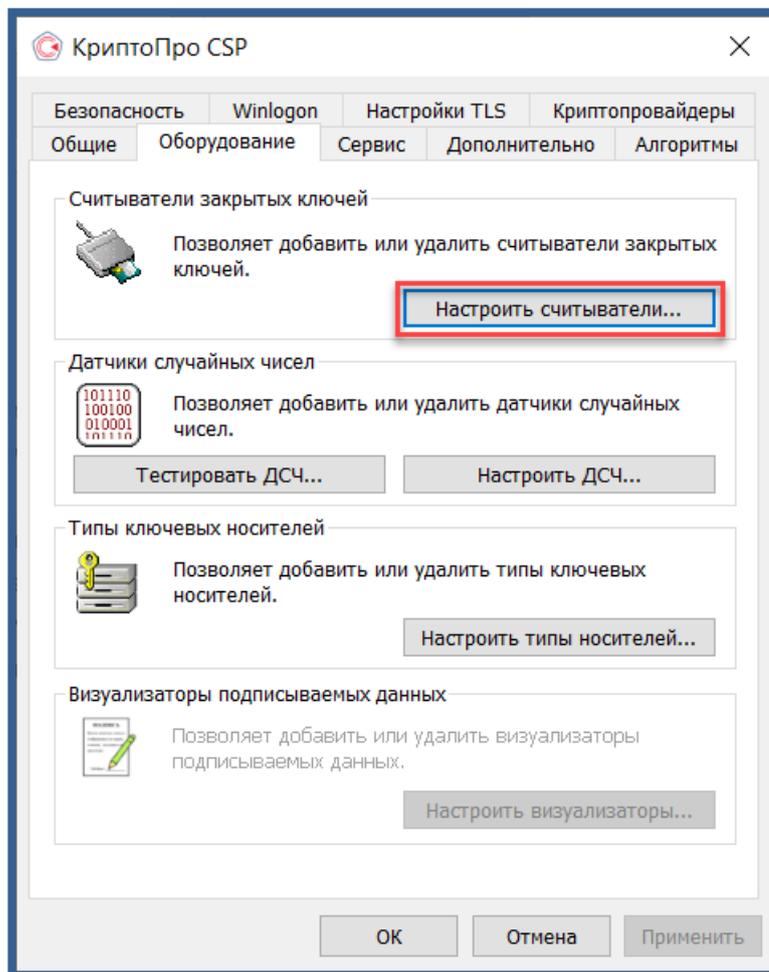


Рис. 15.

Перед Вами откроется окно со списком установленных считывателей (рис. 16.). В случае если в списке нет считывателя «Все считыватели смарт-карт», нажмите кнопку **Добавить**.

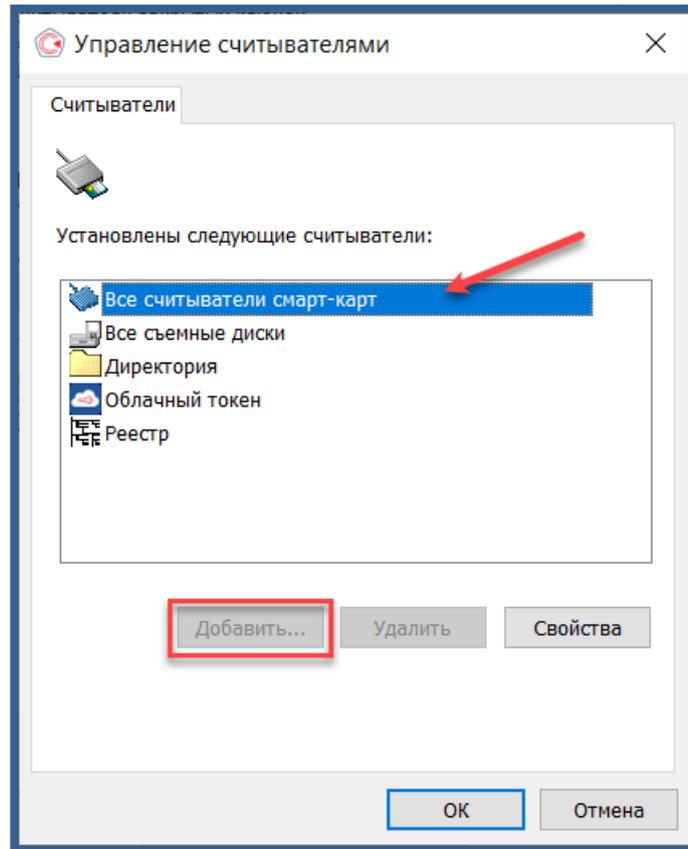


Рис. 16.

 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.17.).

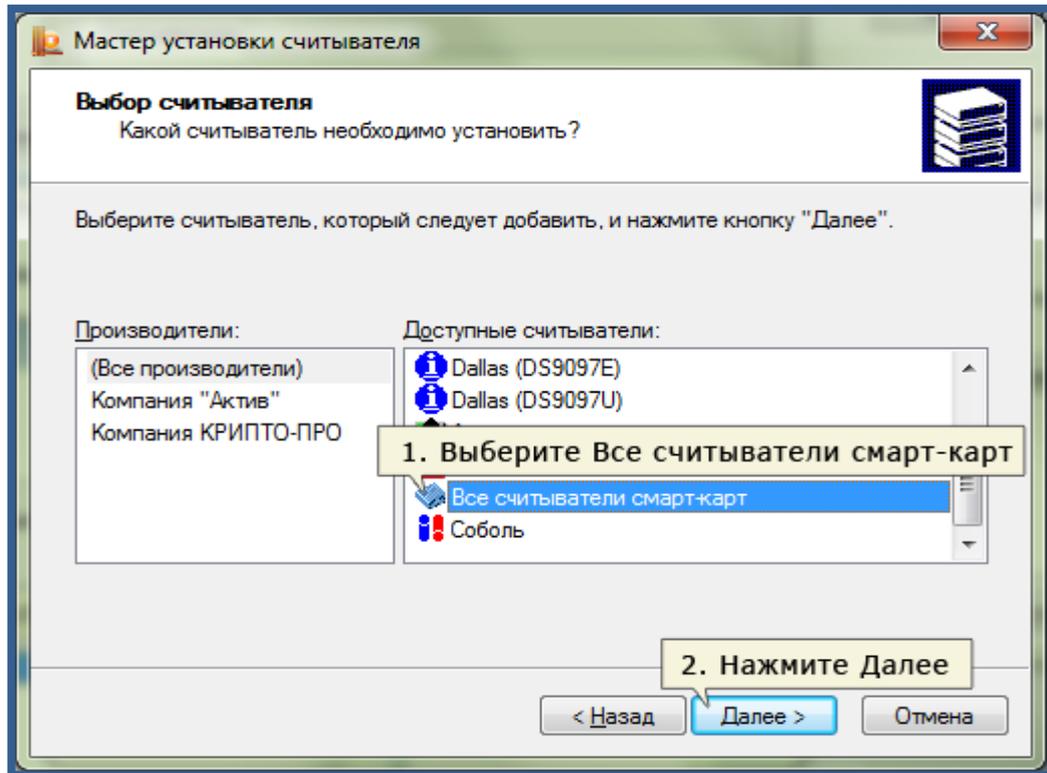


Рис. 17.

Для продолжения установки нажмите кнопку **Далее** (рис.18.).

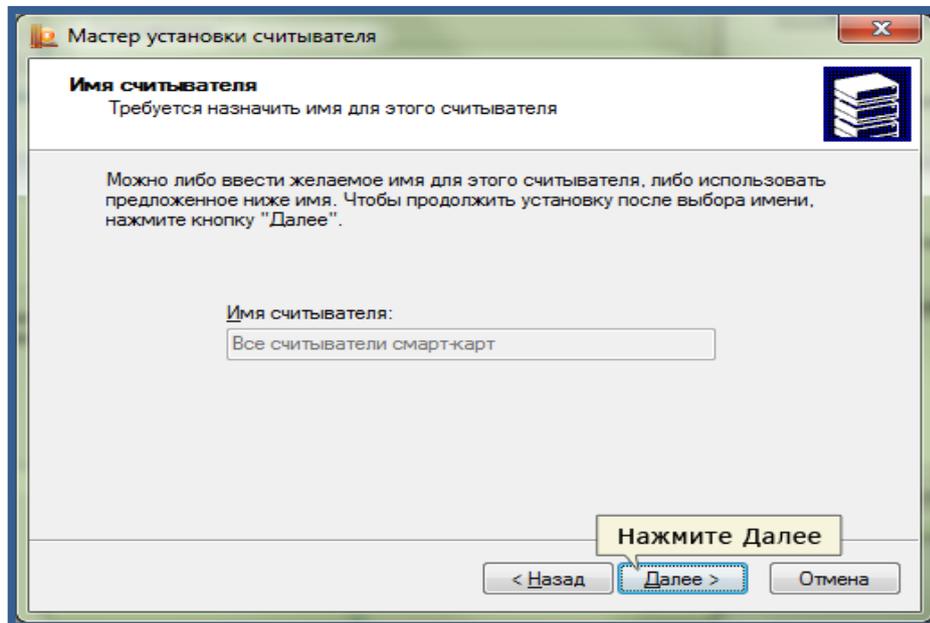


Рис. 18.

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

На вкладке «Оборудование» нажмите кнопку **Настроить типы носителей**. В следующем окне проверьте наличие необходимого носителя и нажмите кнопку **ОК** (рис. 19.).

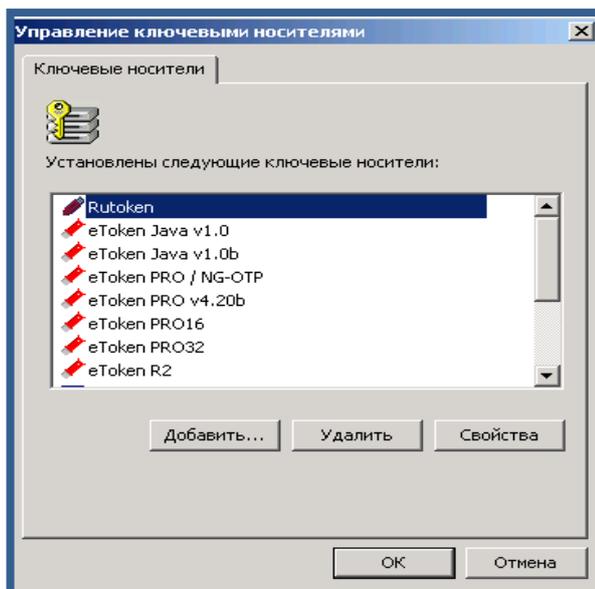


Рис. 19.



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

Настройка считывателя завершена.

#### 4. Проверка корректности установки драйверов

Корректность установки драйверов можно проверить посредством СКЗИ ViPNetCSP либо КриптоПро CSP, в зависимости, от того под каким СКЗИ выпущен сертификат.



*При использовании сертификата для работы с порталом ЕГАИС установка СКЗИ не требуется.*

##### 4.1. Проверка посредством СКЗИ ViPNet CSP

Вставьте защищенный носитель в USB-порт Вашего компьютера.

Перейдите в пункт меню **Пуск – Все программы – ViPNet – ViPNet CSP**.

Перейдите во вкладку «Устройства».

В окне «Подключенные устройства» должен отобразиться подключенный защищенный носитель (рис. 20.).

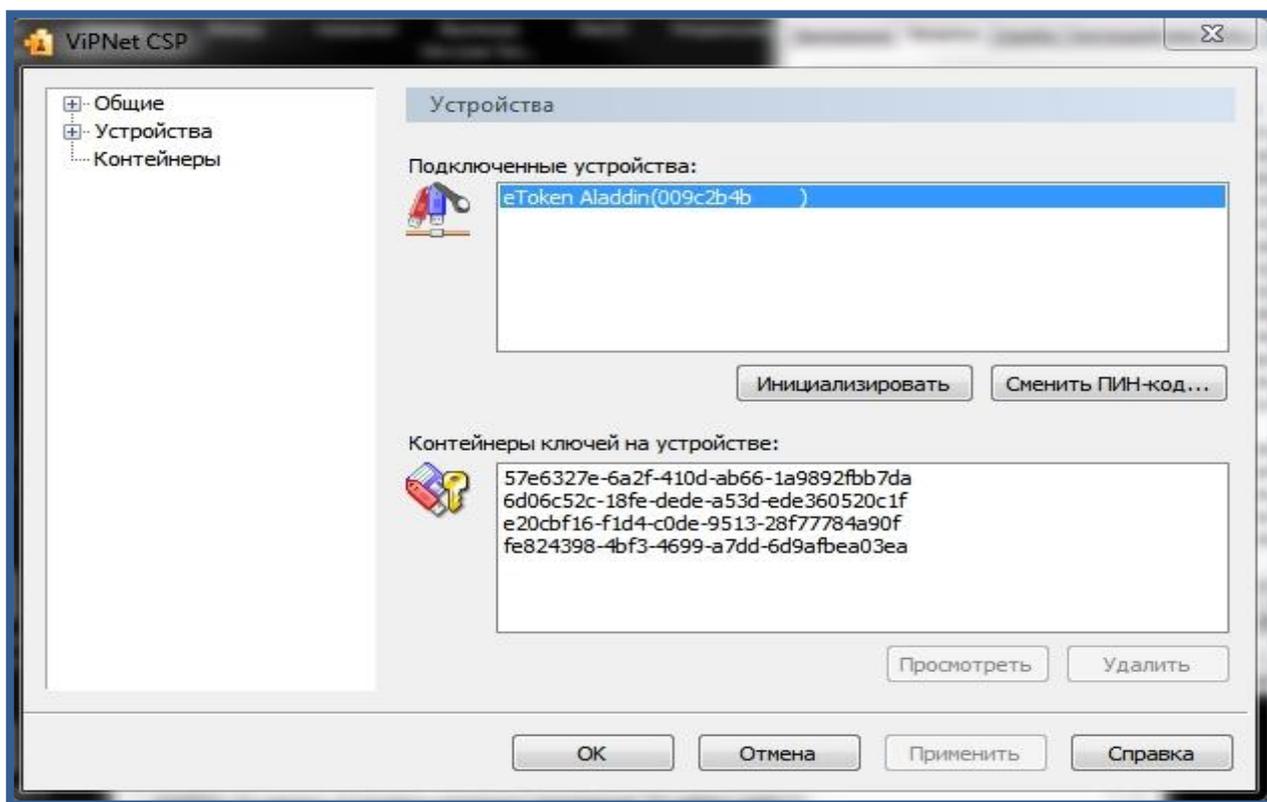


Рис. 20.

##### 4.2. Проверка посредством СКЗИ КриптоПро CSP

Вставьте защищенный носитель в USB-порт Вашего компьютера.

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

Выберите вкладку **Сервис – Просмотреть сертификаты в контейнере** (рис. 21.).

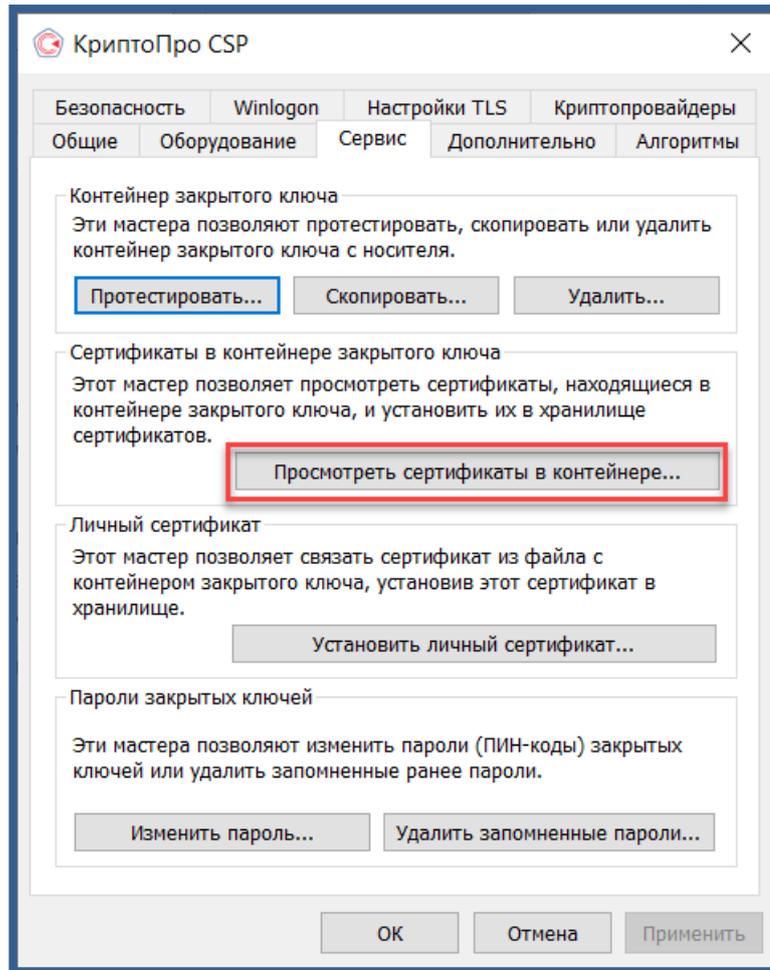


Рис. 21.

Нажмите кнопку **Обзор**. В появившемся окне должен отображаться защищенный носитель (рис.22.).

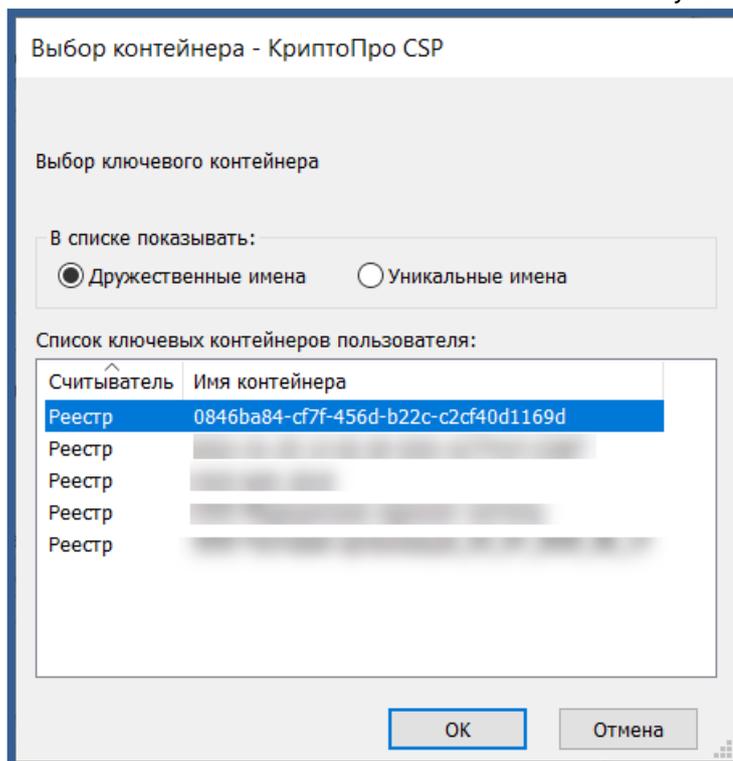


Рис. 22.

## **Заключение**

Все перечисленные шаги помогут Вам корректно произвести необходимые настройки на Вашем рабочем месте для работы с защищенными носителями.

Если в процессе установки у Вас возникли вопросы, не обозначенные в данной инструкции, Вы можете обратиться в службу технической поддержки по телефонам:

- Калуга (4842) 788-999;
- Москва (495) 663-73-58;
- Санкт-Петербург (812) 309-29-23.