Инструкция по настройке автоматизированного рабочего места для работы с электронной подписью (СКЗИ КриптоПро CSP, ключевой носитель JaCarta LT или Рутокен Lite)

Листов 19

Инфотекс Интернет Траст
2024 г.

Оглавление

I. Введение

✓ Документ предназначен для пользователей, осуществляющих самостоятельную установку средства криптографической защиты информации (СКЗИ) КриптоПро CSP[1] и настройку автоматизированного рабочего места для работы с электронной подписью (ЭП).

Самостоятельная настройка без специальных технических знаний может занять несколько дней и привести к неправильной работе программного обеспечения. Чтобы сохранить время и избежать ошибок, вы можете заказать услугу удалённой онлайн-настройки рабочего места.
Специалисты подключатся к вашему рабочему месту и настроят все параметры для начала работы с сертификатом.

✓ **С 1 января 2022 года получить квалифицированный сертификат электронной подписи руководителя юридического лица или индивидуального предпринимателя можно только в государственных удостоверяющих центрах (ФНС, Федеральной казначейство, Центральный банк РФ)[2]. В УЦ ИИТ можно получить сертификат на физическое лицо[3].**

✓ В удостоверяющем центре АО «ИнфоТеКС Интернет Траст» (далее – УЦ ИИТ) срок действия ключей и сертификата ЭП установлен равным 1 году.

✓ Для правильной работы СКЗИ ViPNet CSP необходимо выполнить все пункты данного руководства в указанной последовательности.

✓ Для корректной работы с электронной подписью (ЭП) на различных интернет-порталах (электронные торговые площадки, порталы контролирующих органов, различные федеральные информационные ресурсы и т.д.) в качестве интернет-обозревателя рекомендуется использовать **Chromium-Gost**.

✓ **Необходимо обращать особое внимание на примечания помеченные знаком ➧.**

Внимание! Вид окон может отличаться в зависимости от используемой операционной системы.

➧ **Всю необходимую документацию по услугам нашей компании вы можете загрузить на нашем сайте www.iitrust.ru раздел «Поддержка», кнопка «Пользовательская документация»**

---

[1] Если ваши ключи ЭП работают с СКЗИ ViPNet CSP выберите соответствующую инструкцию из представленных в разделе «Пользовательская документация».

[2] Согласно изменениям в 63-ФЗ «Об электронной подписи».

[3] При подписании электронных документов квалифицированной электронной подписью физического лица с целью подтверждения своих полномочий, действуя от имени юридического лица или ИП, необходимо оформить машиночитаемую доверенность (МЧД).

Внимание! Крайне не рекомендуется устанавливать СКЗИ КриптоПро CSP на компьютер, где уже установлено СКЗИ ViPNet CSP. В случае использовании двух СКЗИ на одном рабочем месте не гарантируется полноценная работа одного из них, вплоть до выхода операционной системы из строя. АО «ИнфоТеКС Интернет Траст» не несет ответственности за некорректную работу СКЗИ при несоблюдении пользователем данного условия.

II. Получение и установка КриптоПро CSP

1. Для получения КриптоПро CSP необходимо перейти на официальный сайт разработчика (https://www.cryptopro.ru/cryptopro/products/csp/default.htm) и затем к странице для загрузки файла с сайта: Скачать КриптоПро CSP.
2. Получение демо-версии КриптоПро CSP возможно только после предварительной регистрации. Это формальная, но обязательная процедура, абсолютно бесплатная. Пройдите регистрацию, заполнив все поля и согласившись с условиями лицензионного соглашения.
3. Скачайте дистрибутив КриптоПро CSP. Сохраните загружаемый файл на своем компьютере, а затем запустите установку программы файлом CSPSetup.exe.

Должна быть версия КриптоПро CSP 5.0 и выше с поддержкой ГОСТ Р 34.10-2012 / ГОСТ Р 34.11-2012

Перед началом установки КриптоПро CSP закройте все запущенные приложения.

Убедитесь, что вы обладаете достаточными правами для установки программ и записи информации в реестр (рекомендуется выполнять установку и настройку с правами локального администратора).

Выполняйте установку и настройку КриптоПро CSP локально на компьютере, а не через клиента удаленного доступа.

1. В появившемся окне нажмите кнопку «***Установить (рекомендуется)».***
2. Произойдет установка КриптоПро CSP. После установки обязательно перезагрузите компьютер.
3. Введите лицензию КриптоПро CSP. Запустите КриптоПро CSP. Откройте вкладку ***«Общие»*** и нажмите на кнопку ***«Ввод лицензии…»***. Затем заполните поля ***«Пользователь»***, ***«Организация»***, введите ***«Серийный номер»***[4] (серийный номер, полученный у организации-разработчика или организации, имеющей права на распространение продукта)[5] и нажмите кнопку ***«ОК»*** (Рисунок 1).

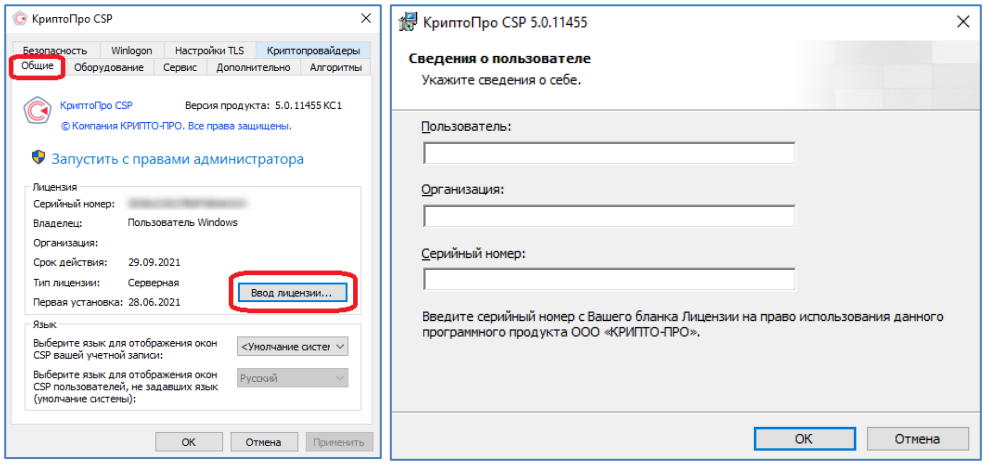

Рисунок 1

[4] При вводе серийного номера КриптоПро CSP все символы вводятся заглавными латинскими буквами. В серийном номере букв «О» нет – это цифра «0».

[5] Предоставление лицензии на КриптоПро CSP в перечень предоставляемых услуг АО «ИИТ» не входит.

III. Установка программного обеспечения для ключевых носителей

Установку программного обеспечения необходимо выполнить в зависимости от типа используемого ключевого носителя:

А. Если ЭП выпущена на носителях JaCarta LT, JaCarta-2 SE, JaCarta-2 ГОСТ, JaCarta-2 PKI/ГОСТ, JaCarta PK, произведите установку программного обеспечения для ключевых носителей JaCarta;

Б. Если ЭП выпущена на носителях Рутокен S, Рутокен Lite, Рутокен ЭЦП 2.0, произведите установку программного обеспечения для ключевых носителей Рутокен;

Опишем каждый из них подробнее, необходимо выполнить **подходящий**.

А. Установка программного обеспечения для ключевых носителей JaCarta

Внимание! Данный пункт инструкции следует использовать, ТОЛЬКО если КЭП выдана на JaCarta.

1. Для корректной работы ключевого носителей JaCarta под управлением операционной системы Microsoft Windows необходимо установить программное обеспечение, позволяющее выполнять базовые операции с электронными ключами JaCarta.

Для получения программного обеспечения актуальной версии необходимо зайти на страницу https://www.aladdin-rd.ru/support/downloads/jacarta_client, выбрать дистрибутив, подходящий разрядности вашей операционной системы, и нажать на кнопку ***«Скачать»*** (Рисунок 2).

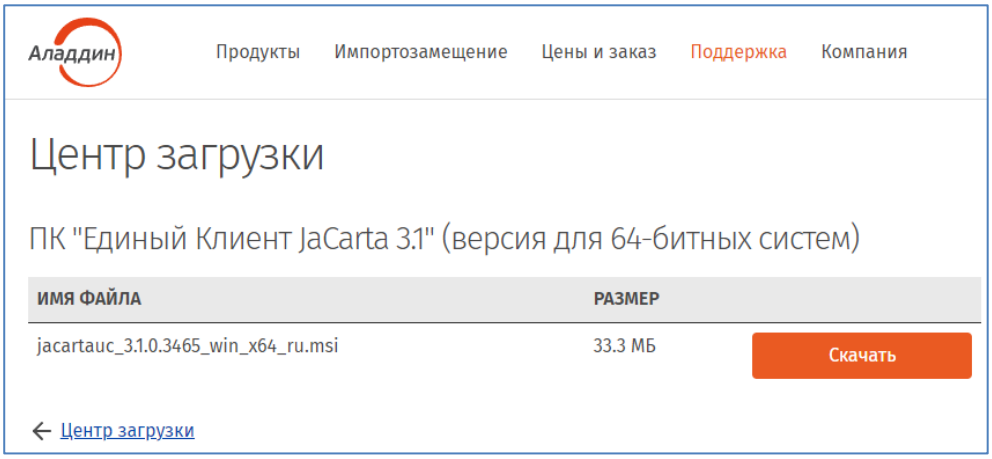

Рисунок 2

2. Загрузите дистрибутив в любое место компьютера и запустите установку утилиты. Выполните установку, следуя инструкциям мастера установки.
3. Перейти к IV главе: Установка личного сертификата

Б. Установка программного обеспечения для ключевых носителей Рутокен

Внимание! Данный пункт инструкции следует использовать, ТОЛЬКО если КЭП выдана на носителях Рутокен.

1. Для корректной работы ключевых носителей Рутокен под управлением операционной системы Microsoft Windows необходимо установить программное обеспечение, позволяющее выполнять базовые операции с электронными ключами: Рутокен.

Для получения программного обеспечения актуальной версии необходимо перейти на сайт компании «Актив», которая является разработчиком ключевых носителей Рутокен, в раздел «Драйверы для Windows» по данной ссылке: https://www.rutoken.ru/support/download/windows/ Нажмите кнопку «Драйверы Рутокен для Windows, EXE» (Рисунок 3).

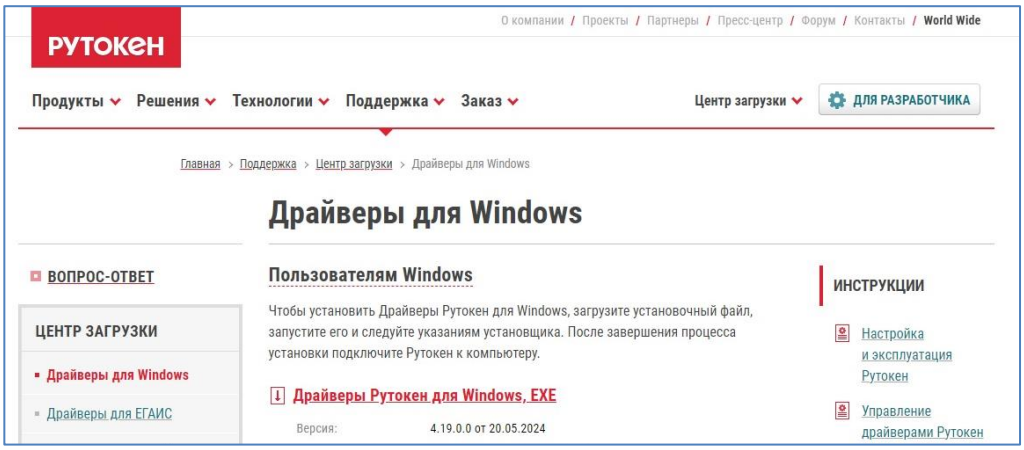

Рисунок 3

2. Загрузите архив с дистрибутивом в любое место компьютера, распакуйте его и запустите установку утилиты. Выполните установку, следуя инструкциям мастера установки.
3. Перейти к IV главе: Установка личного сертификата

IV. Установка личного сертификата

Установку личного сертификата возможно выполнить несколькими способами:

А. Установка личного сертификата с ключевого носителя

Б. Установка сертификата через личный кабинет https://iitrust.lk

В. Установка личного сертификата с дискового носителя

Опишем каждый из них подробнее, необходимо выполнить **подходящий**.

А. Установка личного сертификата с ключевого носителя

Внимание! Убедитесь, что ключевой носитель находится в USB-порту вашего компьютера

1. Запустите приложение КриптоПро CSP, перейдите на вкладку ***«Сервис»*** и нажмите кнопку ***«Просмотреть сертификаты в контейнере»*** (Рисунок 4, позиция А).

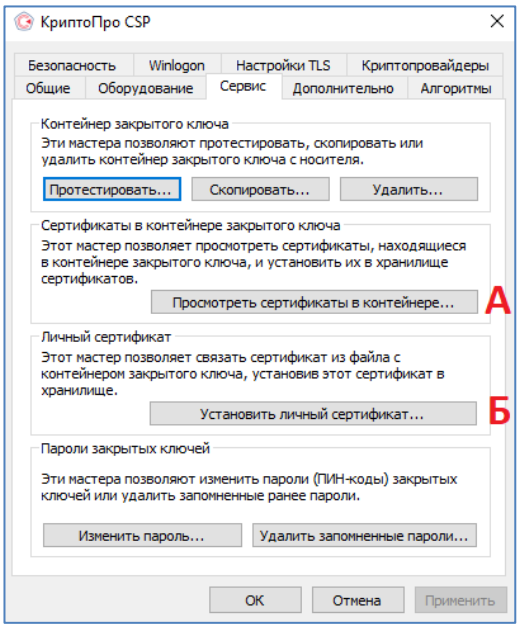

Рисунок 4

2. В открывшемся окне нажмите кнопку ***«Обзор»***, чтобы выбрать контейнер для просмотра. После выбора нужного контейнера нажмите кнопку ***«Ок»*** (Рисунок 5).

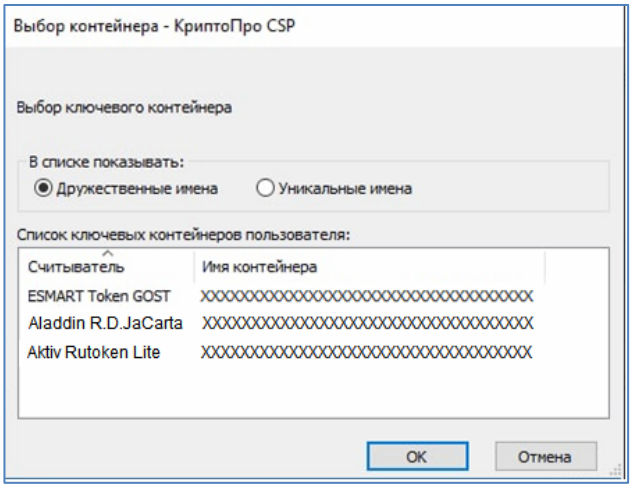

Рисунок 5

3. В следующем окне нажмите кнопку ***«Далее».*** Если запросит пароль, введите пин-код вашего

ключевого носителя.

4. В открывшемся окне следует нажать кнопку ***«Установить»*** (Рисунок 6).

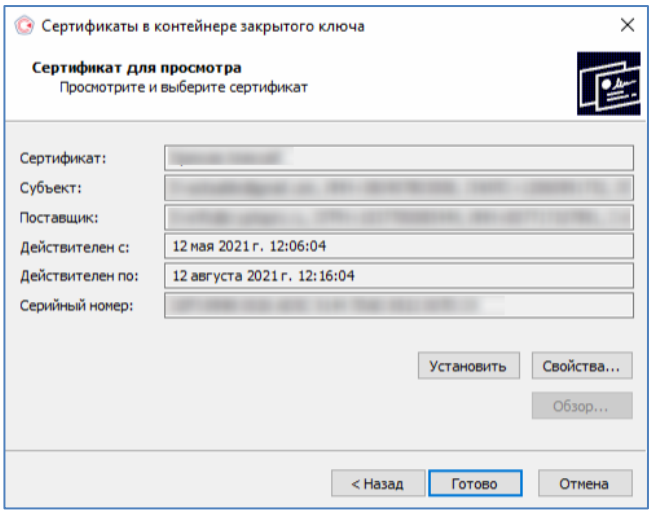

Рисунок 6

5. Если сертификат ранее уже был установлен, появится следующее информационное окно, нажмите кнопку ***«Да»*** (Рисунок 7).

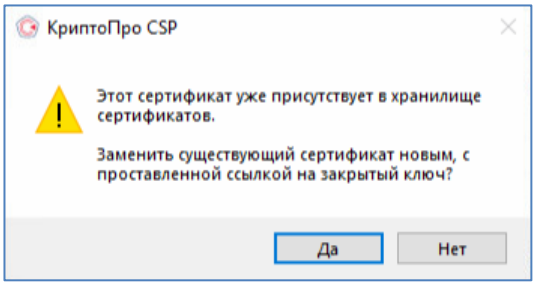

Рисунок 7

6. Если ранее сертификат не был установлен, то появится информационное окно, что сертификат был успешно установлен в хранилище «Личное» текущего пользователя (Рисунок 8).

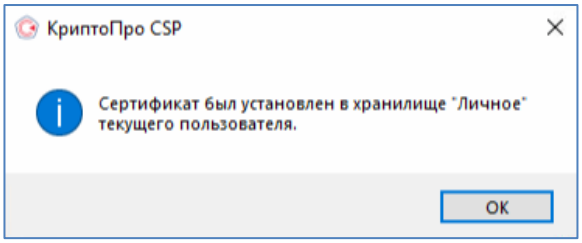

Рисунок 8

По умолчанию PIN-код на JaCarta LT: до 15.01.2019 устанавливался 1eToken, с 21.01.19 года устанавливается 1234567890. Рекомендуется сменить PIN-код доступа к JaCarta LT со стандартного на более устойчивый, который будете знать только вы. Для смены PIN-кода следуйте указаниям раздела V настоящей Инструкции.

По умолчанию PIN-код на Рутокен: 12345678. Рекомендуется сменить PIN-код доступа к Рутокену со стандартного на более устойчивый, который будете знать только вы. Для смены PIN-кода следуйте указаниям раздела VI настоящей Инструкции.

7. Перейти к 4 главе: Построение цепочки сертификатов до головного удостоверяющего центра Министерства связи и массовых коммуникаций».

Б. Установка сертификата через личный кабинет

Внимание! Данный пункт инструкции следует использовать, ТОЛЬКО если Вы создавали запрос на выпуск сертификата через Личный кабинет (https://iitrust.lk).

Внимание! Настоятельно рекомендуем скопировать контейнер на ключевой носитель JaCarta LT. Утеря контейнера ведет к внеплановой смене электронной подписи, что в свою очередь является платной услугой с обязательным личным прибытием в УЦ ИИТ.

Перейдите в личный кабинет по ссылке **https://iitrust.lk** и введите логин и пароль в соответствующие поля (Рисунок 9).

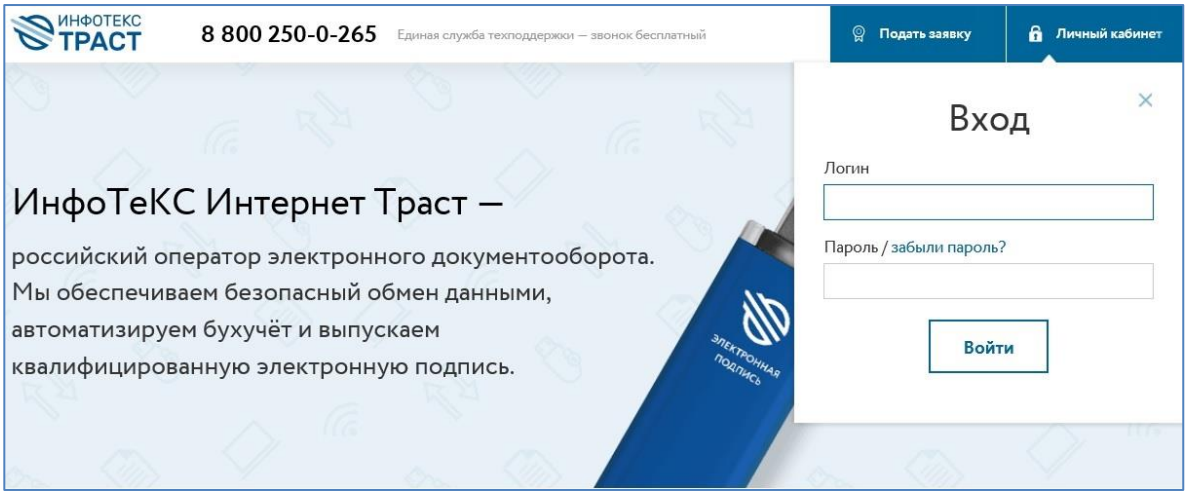

Рисунок 9

В списке заявок выберите заявку в статусе ***«Завершена»*** и нажмите на ее номер/строчку (Рисунок 10).

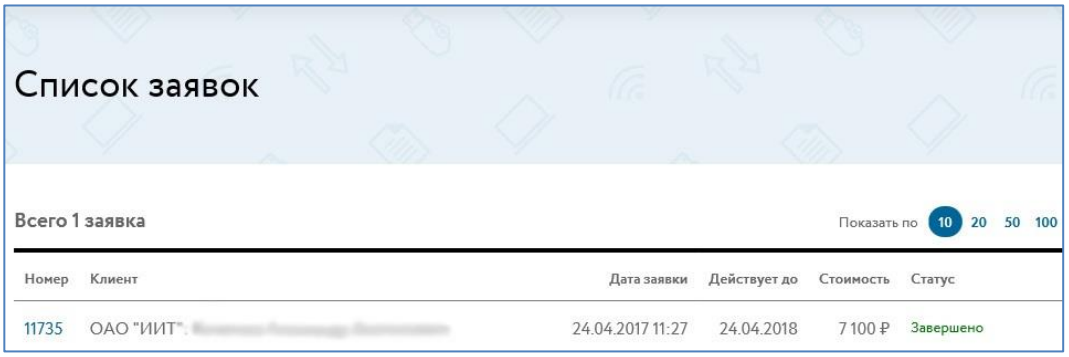

Рисунок 10

На странице нажмите кнопку ***«Установить»***[6] (Рисунок 11). Сертификат будет успешно установлен в контейнер[7]. (Рисунок 12).

[6] Должно быть установлено и запущено дополнительное ПО «TRUST Plugin» с расширением для браузера.

[7] Если при создании пароля доступа к контейнеру ключей вы не отметили флажок «Сохранить пароль», то при запросе пароля введите его.

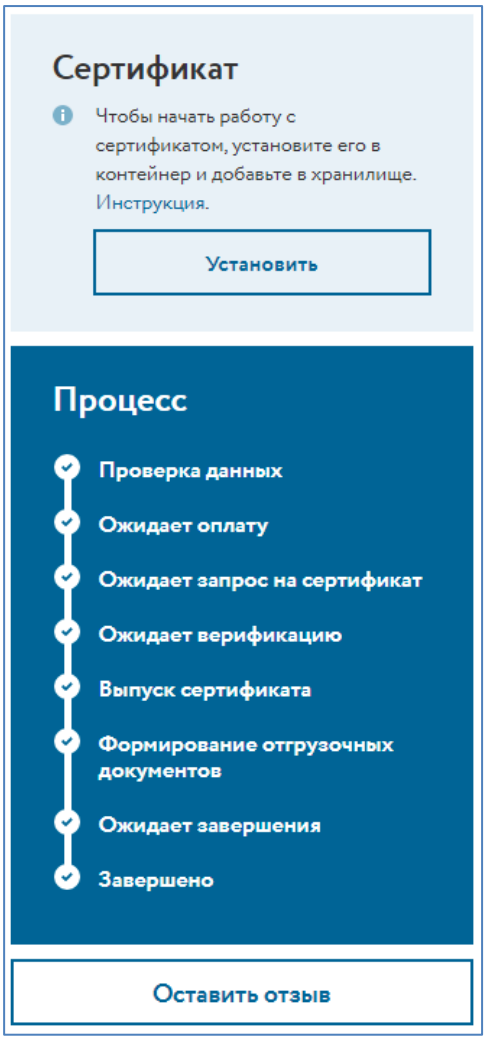

Рисунок 11

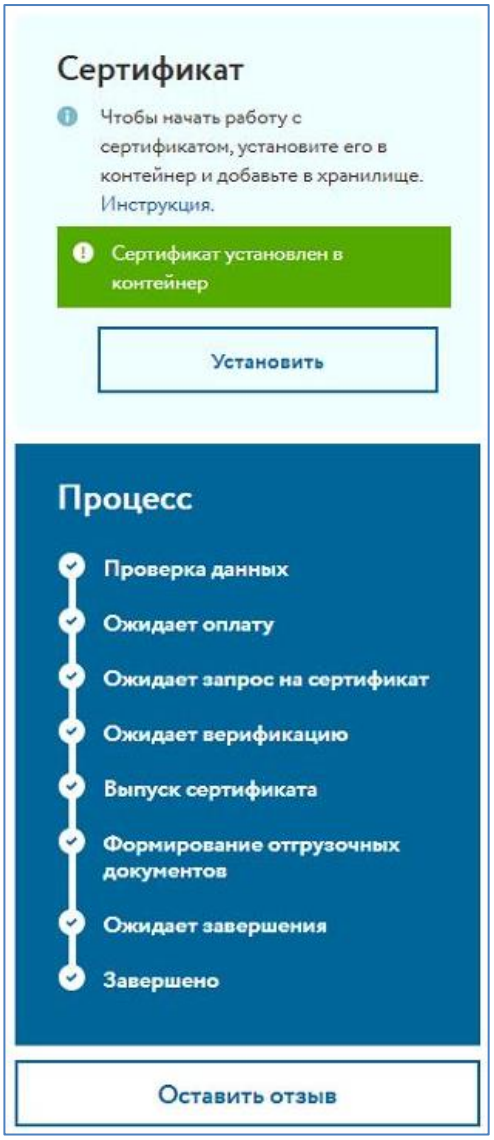

Рисунок 12

Если при создании пароля доступа к контейнеру ключей вы не отметили флажок **«Сохранить пароль»**, то при запросе пароля введите его.

Затем **обязательно установите сертификат в системное хранилище**, процесс установки личного сертификата приведен в **разделе А**.

Если при генерации контейнера использовался нестандартный путь для сохранения (или контейнер был сохранен на носитель) установите сертификат самостоятельно, загрузив его из личного кабинета, нажав на кнопку **«Сертификат»** (Рисунок 13).

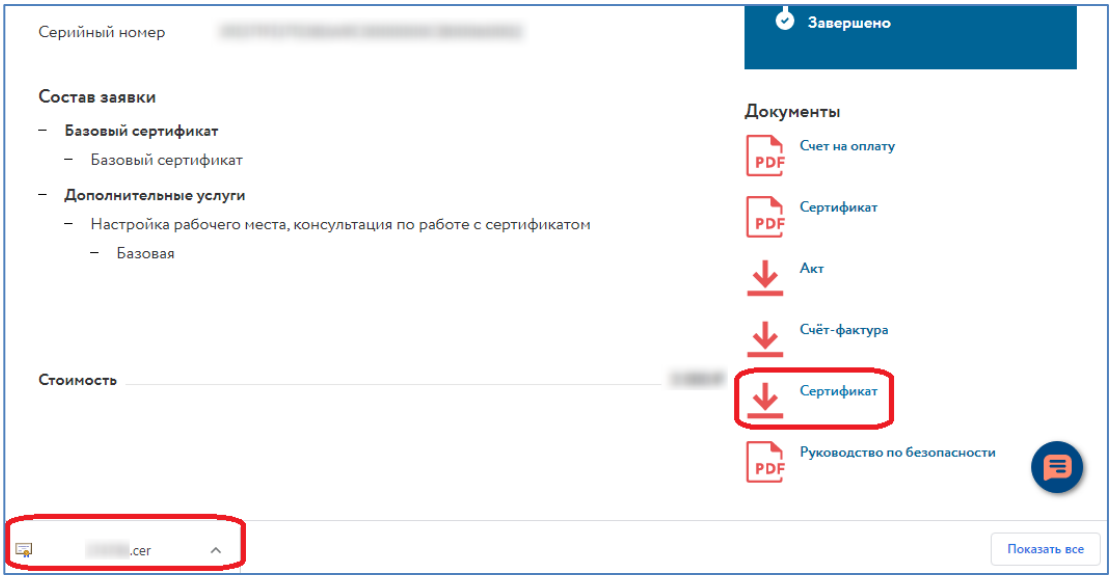

Рисунок 13

Процесс установки сертификата описан в **разделе В** данной инструкции.

Если вы генерировали контейнер в реестр и хотите скопировать его на приобретенный носитель JaCarta LT - запустите криптопровайдер ***КриптоПро CSP*** из ***«Панели управления»*** или из кнопки меню ***«Пуск».***

Перейдите на вкладку ***«Сервис»*** и нажмите кнопку ***«Скопировать…»*** (Рисунок 14)**.**

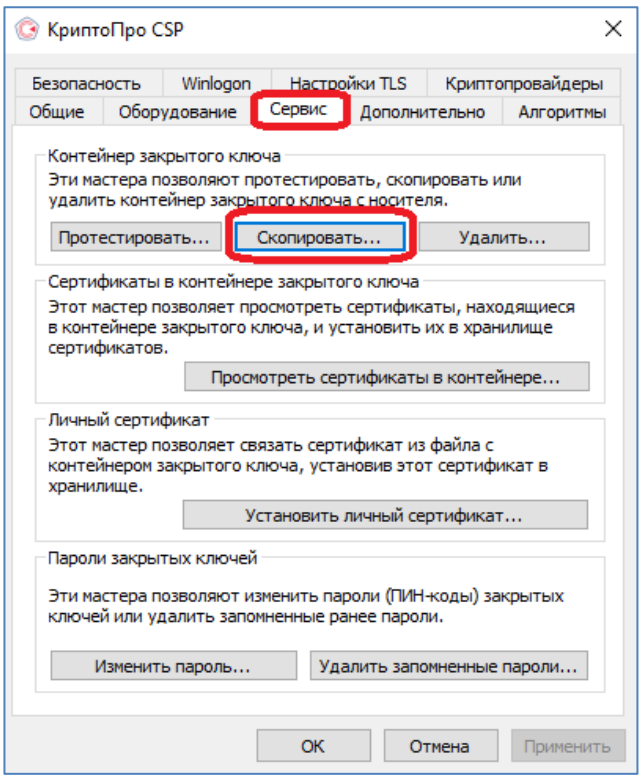

Рисунок 14

4. Нажмите кнопку ***«Обзор…»*** для выбора контейнера закрытого ключа, выберите нужный контейнер и нажмите кнопку ***«ОК»*** (Рисунки 15-16).

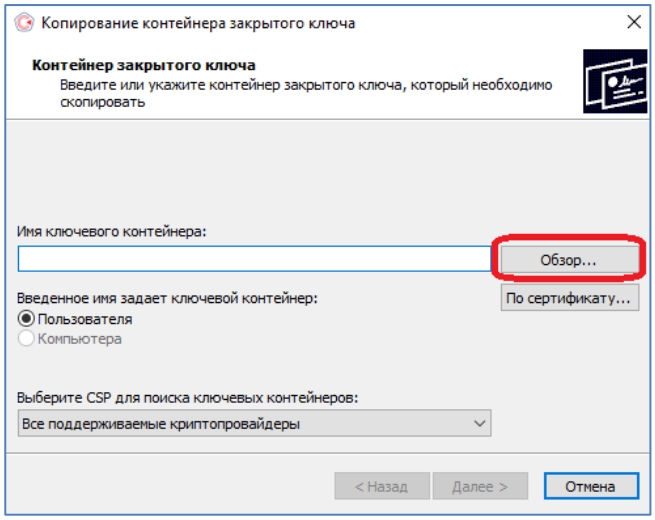

Рисунок 15

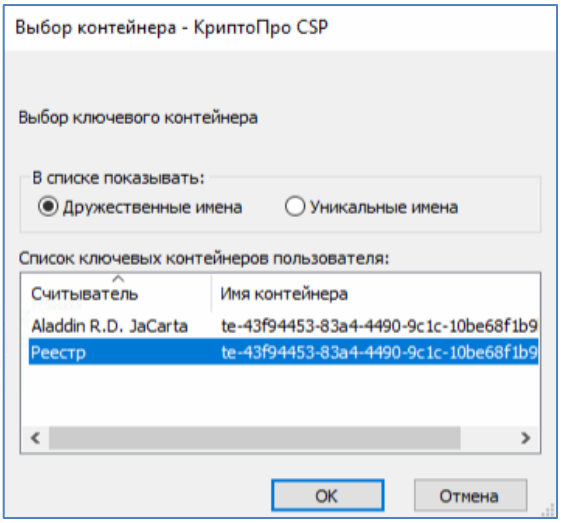

Рисунок 16

5. При необходимости введите пароль к контейнеру закрытого ключа[8] (Рисунок 17).

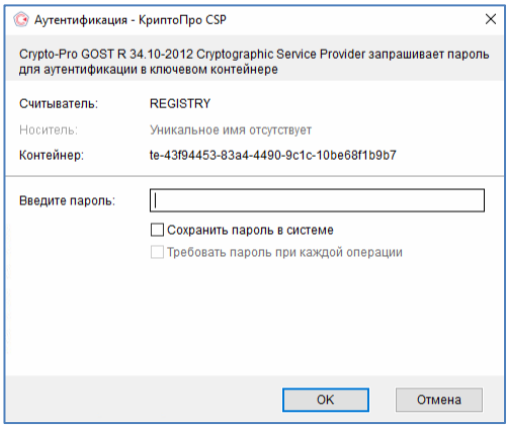

Рисунок 17

6. Задайте имя контейнера, который будет храниться на JaCarta LT или Рутокене, и нажмите ***«Готово»*** (Рисунок 18).

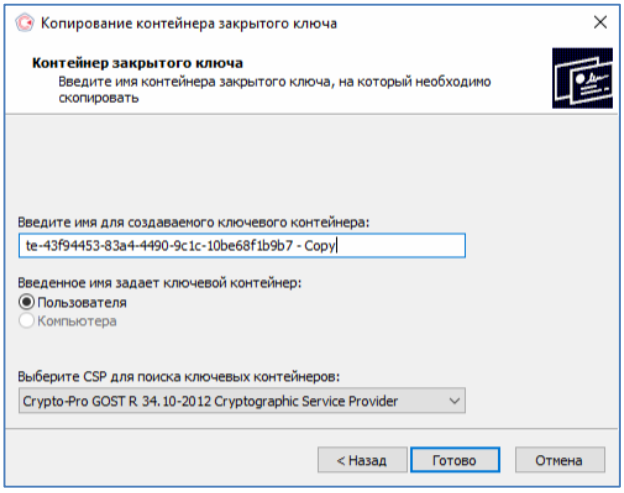

Рисунок 18

[8] По умолчанию пин-код пользователя для контейнера: **123456**

В окне выбора носителя укажите JaCarta LT ***Aladdin JaCarta или Рутокен*** и нажмите ***«ОК»***, при необходимости введите пароль для устройства (Рисунок 19).

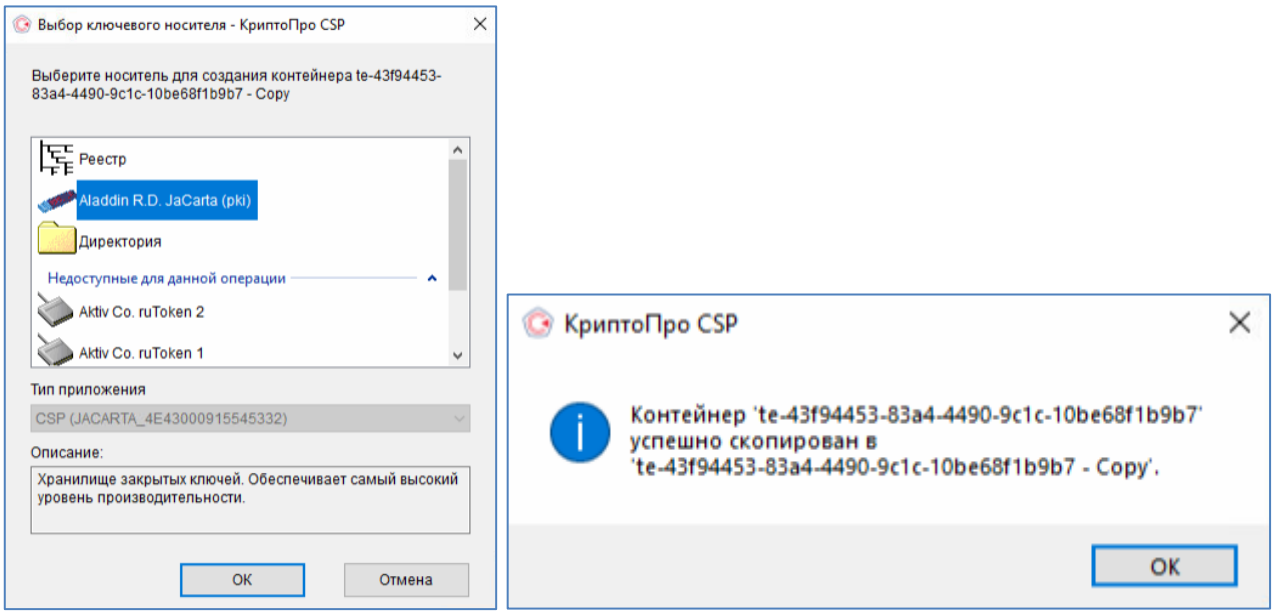

Рисунок 19

Установите сертификат в личное хранилище, описание процесса установки в **разделе А.**

В. Установка личного сертификата, хранящегося на диске

Внимание! Данный пункт инструкции следует использовать, ТОЛЬКО если Вам выдали ключевой дистрибутив на диске.

Папку с закрытым ключом (и файл сертификата, если он есть) необходимо скопировать с диска в корень дискеты (flash-накопителя). Название папки при копировании изменять нельзя. Папка с закрытым ключом должна содержать 6 файлов с расширением.key (Рисунок 20).

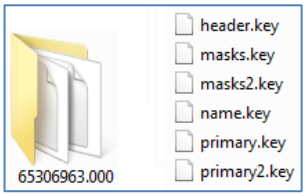

Рисунок 20

Как правило, в закрытом ключе присутствует открытый ключ (файл header.key в этом случае будет весить больше 1 Кб). В этом случае копирование открытого ключа выполнять необязательно.

1. Запустите ***КриптоПро CSP*** **через** ***Пуск → Все программы → КРИПТО-ПРО → КриптоПро CSP***. В окне ***«Свойства КриптоПро CSP»*** перейти на вкладку ***«Сервис»*** и кликнуть по кнопке ***«Установить личный сертификат»*** **(Рисунок 3, позиция Б).**
2. В окне ***«Мастер импорта сертификатов»*** **нажмите на кнопку** ***«Обзор»***, чтобы выбрать файл сертификата с расширением **.cer** (Рисунок 21).

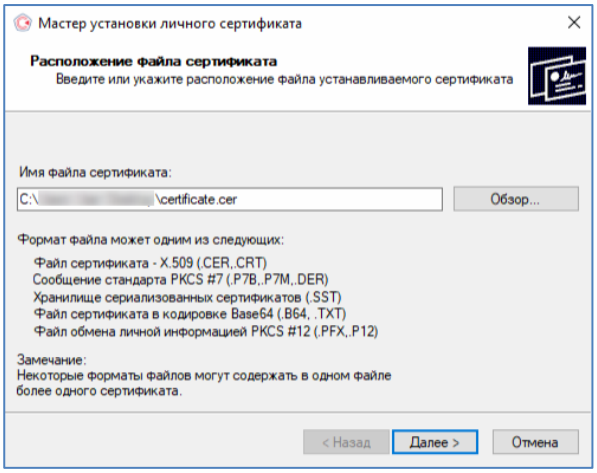

Рисунок 21

3. В следующем окне кликнуть по кнопке ***«Далее»*** **(Рисунок 22).**

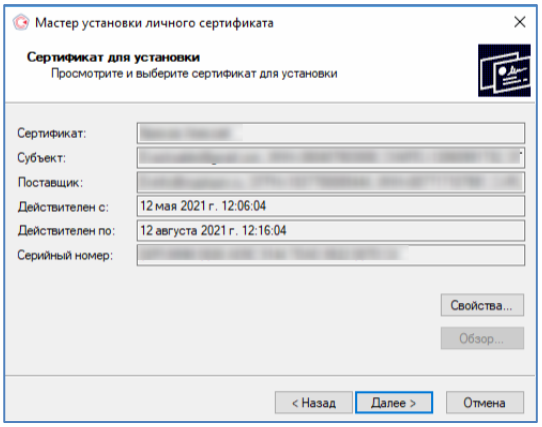

Рисунок 22

4. Укажите пункт ***«Найти контейнер автоматически»*** **(Рисунки 23 - 24).**

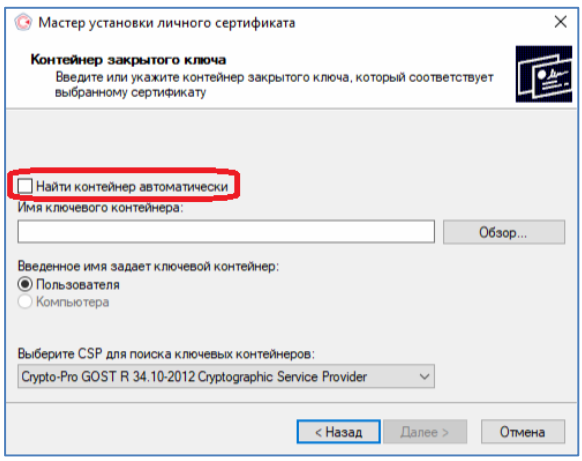

Рисунок 23

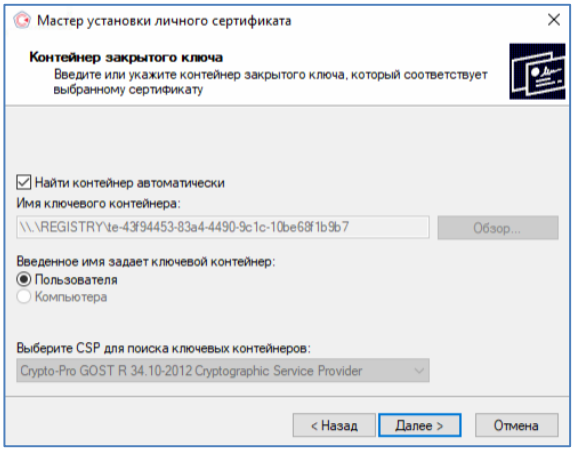

Рисунок 24

5. После выбора контейнера следует нажать на кнопку ***«Далее»*****.** Если на доступ к закрытому ключу установлен пароль, то система попросит ввести его. Введите пароль и нажмите кнопку ***«Ок»***.

По умолчанию ПИН-код на JaCarta LT: до 15.01.2019 устанавливался 1eToken, с 21.01.19 года устанавливается 1234567890, ПИН-код для Рутокена: 12345678, стандартный пароль к контейнеру, полученному на диске: 123456. Рекомендуется сменить ПИН доступа к ключевому носителю со стандартного на более устойчивый, который будете знать только Вы.

6. В окне ***«Выбор хранилища сертификатов»*** кликнуть по кнопке ***«Обзор».*** Необходимо выбрать хранилище ***«Личные»*** и нажать ***«Ок»*** **(Рисунок 25).**

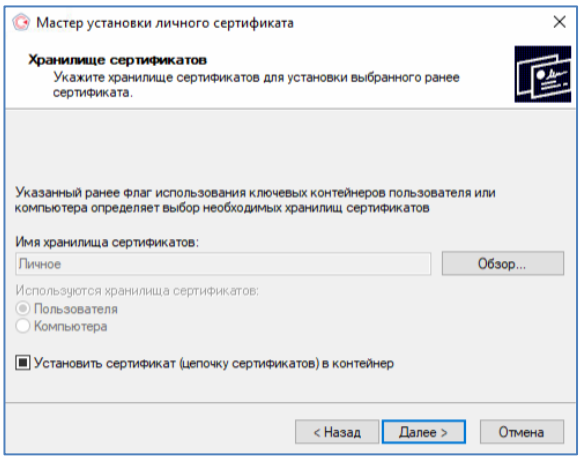

Рисунок 25

7. После выбора хранилища следует нажать на кнопку ***«Далее»***, затем ***«Готово»***. Появится одно из двух окон в зависимости от того, был ли ранее установлен сертификат в систему или нет (Рисунок 26).

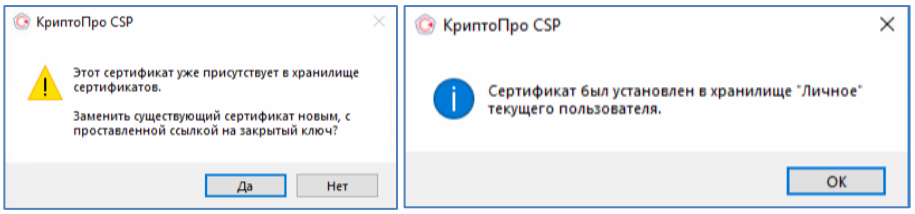

Рисунок 26

IV.Построение цепочки сертификатов до головного удостоверяющего центра Министерства цифрового развития, связи и массовых коммуникаций

- ✓ Загрузить головные сертификаты удостоверяющего центра Министерства цифрового развития, связи и массовых коммуникаций РФ (далее по тексту - ***Головной УЦ***) можно самостоятельно с официального сайта[9], либо по ссылкам:
  - http://reestr-pki.ru/cdp/guc_gost12.crt[10]
  - http://reestr-pki.ru/cdp/guc2021.crt[11]
  - http://reestr-pki.ru/cdp/guc2022.crt[12]
- ✓ Откройте загруженный сертификат и нажмите ***«Установить сертификат»*** (Рисунок 27).
- ✓ Запустится мастер импорта сертификатов, нажмите ***«Далее»***.
- ✓ При установке корневого сертификата Головного УЦ в окне выбора хранилища, необходимо хранилище указать вручную, для этого выбрать ***«Поместить все сертификаты в следующее хранилище»*** (Рисунок 28, позиция А), нажать ***«Обзор»*** (Рисунок 28, позиция Б), выбрать ***«Доверенные корневые центры сертификации»*** (Рисунок 28, позиция В), нажать ***«Далее»*** (Рисунок 28, позиция Г).

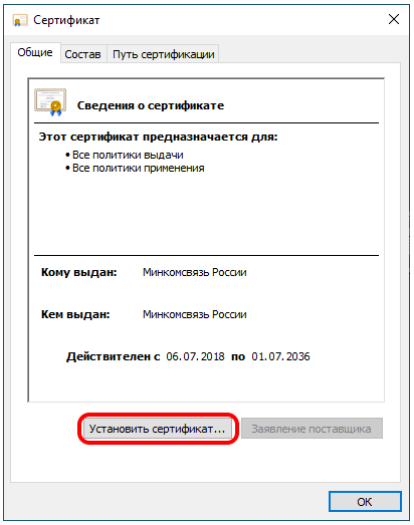

Рисунок 27

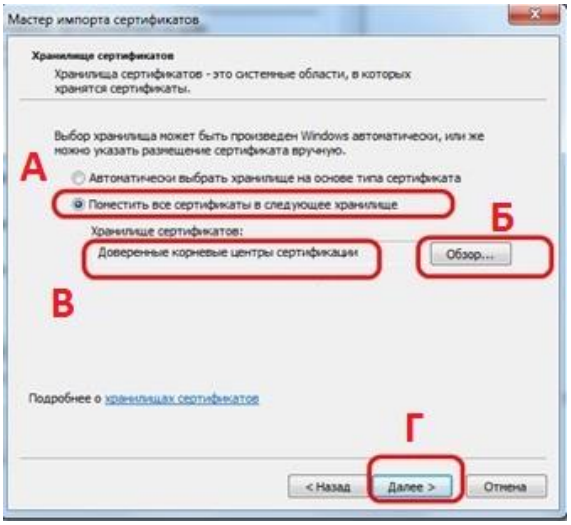

Рисунок 1

- ✓ Далее на все запросы мастера импорта сертификатов об установке сертификата ***«Далее»/«Да»/«ОК»*** - соглашаетесь.
- ✓ Установите все сертификаты.

---

[9] URL: https://e-trust.gosuslugi.ru/#/portal/mainca

[10] При необходимости проверить контрольную сумму сертификата можно с помощью командной строки - **certutil –hashfile [путь до сертификата]**. Отпечаток сертификата: **4bc6dc14d97010c41a26e058ad851f81c842415a**

[11] При необходимости проверить контрольную сумму сертификата можно с помощью командной строки - **certutil –hashfile [путь до сертификата]**. Отпечаток сертификата: **aff05c9e2464941e7ec2ab15c91539360b79aa9d**

[12] При необходимости проверить контрольную сумму сертификата можно с помощью командной строки - **certutil –hashfile [путь до сертификата]**. Отпечаток сертификата: **2F0CB09BE3550EF17EC4F29C90ABD18BFCAAD63A**

V. Смена PIN-кода на доступ к содержимому устройства JaCarta LT.

1. Вставьте JaCarta LT, на котором необходимо установить\сменить PIN-код пользователя, в USB-порт компьютера.
2. Откройте Единый клиент JaCarta (или запустите из панели ***Пуск\Все программы\Аладдин Р.Д\ Единый клиент JaCarta***).
3. Если к компьютеру подсоединено несколько электронных ключей, в левой панели Единого клиента JaCarta выберите нужный электронный ключ.
4. В главном окне нажмите кнопку ***«Сменить PIN-код»*** (Рисунок 29).
5. В поле ***«Текущий PIN-код»*** введите текущий PIN-код пользователя.
6. В полях ***«Новый PIN-код пользователя»*** и ***«Подтверждение PIN-код пользователя»*** введите новый PIN-код пользователя (Рисунок 30).
7. Нажмите кнопку ***«Выполнить»***. При успешной установке нового PIN-кода пользователя появится соответствующее сообщение (Рисунок 2).

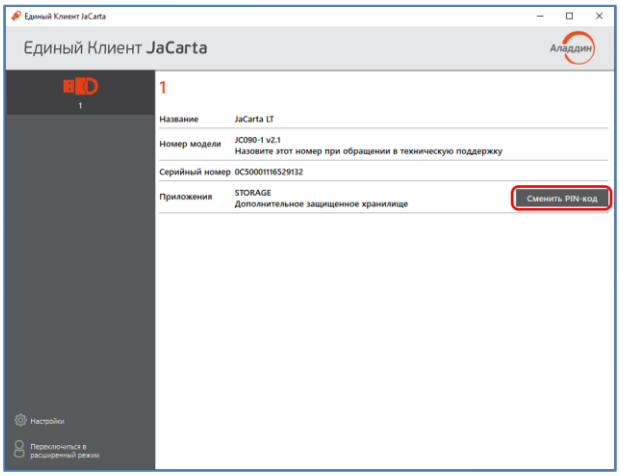

Рисунок 29

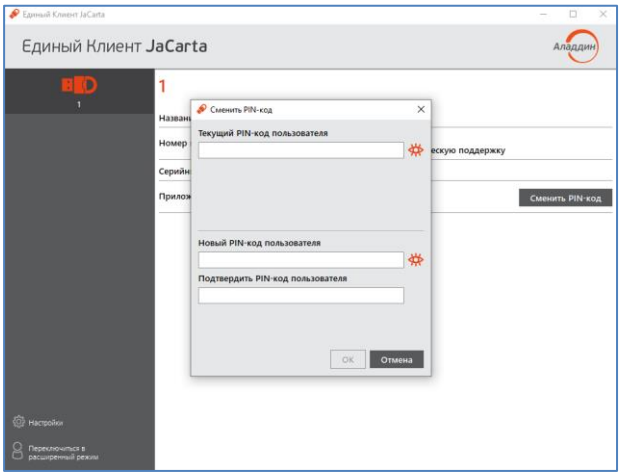

Рисунок 30

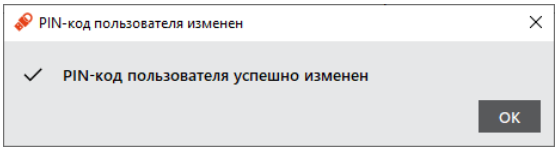

Рисунок 2

В случае если пароль (PIN-код) будет утерян (забыт) доступ к ключевой информации будет невозможен, что в свою очередь приведет к внеплановой смене ключевого дистрибутива, что является платной услугой, согласно регламенту Удостоверяющего центра, размещенного на сайте.

Количество ввода неправильного пароля (PIN-кода) для доступа к ключам электронной подписи на JaCarta LT ограничено (по умолчанию 10), после чего доступ к информации на JaCarta LT блокируется. Блокировка доступа к информации на JaCarta LT является необратимой аппаратной функцией. Никогда не используйте для решения технических проблем, возникающих при использовании JaCarta LT, процедуру инициализации JaCarta LT. Необходимо учитывать, что инициализация JaCarta LT ведет в потере всей информации в памяти ключа.

VI. Смена PIN-кода на доступ к содержимому устройства Рутокен Lite.

1. Вставьте Рутокен Lite, на котором необходимо установить\сменить PIN-код пользователя, в USB-порт компьютера.
2. Откройте ***Панель управления Рутокен*** (или запустите из панели ***Пуск\Все программы\Рутокен\ Панель управления Рутокен***) (Рисунок 32).

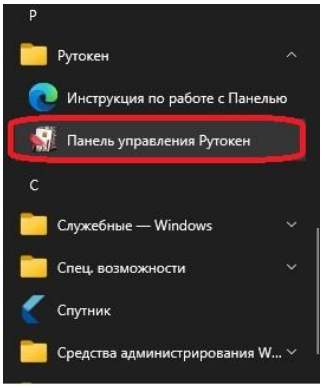

Рисунок 32

3. Если к компьютеру подсоединено несколько электронных ключей, во вкладке ***Администрирование*** в выпадающем списке ***Подключенные Рутокены*** выберите нужный электронный ключ (Рисунок 33).

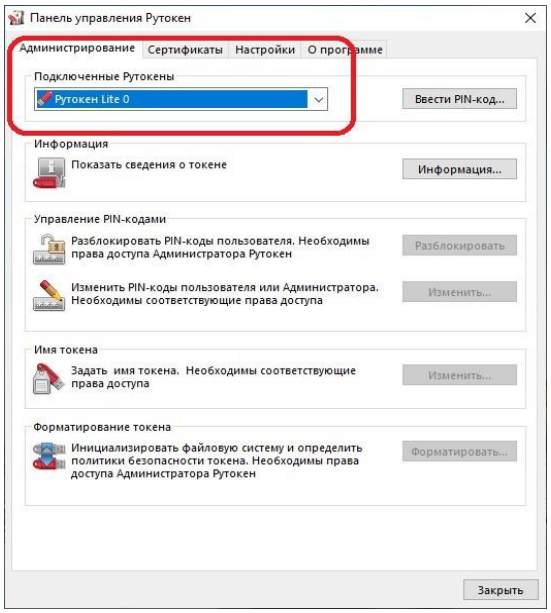

Рисунок 33

4. Во вкладке ***Администрирование*** нажмите кнопку ***«Ввести PIN-код…»***. Для смены Pin-кода пользователя необходимо ввести PIN-код пользователя[13] (Рисунок 34).

[13] По умолчанию PIN-код пользователя на устройство Рутокен Lite: **12345678**

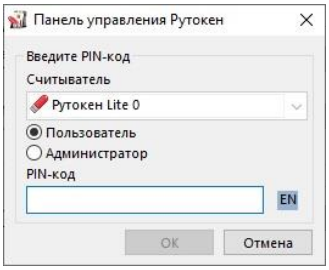

Рисунок 34

8. В полях ***«Введите новый PIN-код»*** и ***«Подтвердите новый PIN-код»*** введите новый PIN-код пользователя или администратора (Рисунок 35).

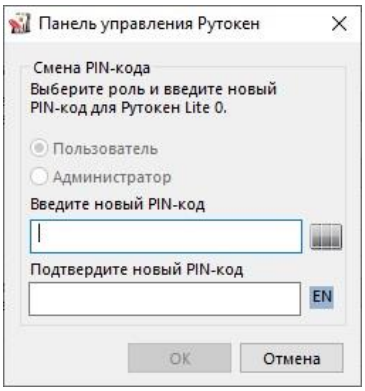

Рисунок 35

9. Нажмите кнопку ***«Ок»***. PIN-код успешно изменен.

➧ ***В случае если пароль (PIN-код) будет утерян (забыт) доступ к ключевой информации будет невозможен, что в свою очередь приведет к внеплановой смене ключевого дистрибутива, что является платной услугой, согласно регламенту Удостоверяющего центра, размещенного на сайте.***

➧ ***Количество ввода неправильного пароля (PIN-кода) для доступа к ключам электронной подписи на Рутокен Lite ограничено (по умолчанию 10), после чего доступ к информации на Рутокен Lite блокируется. Никогда не используйте для решения технических проблем, возникающих при использовании Рутокен Lite, процедуру инициализации Рутокен Lite. Необходимо учитывать, что инициализация Рутокен Lite ведет в потере всей информации в памяти ключа.***
