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

Листов 16

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].**

✓ Для правильной работы СКЗИ КриптоПро 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». Для удобства можно воспользоваться фильтром.

[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 ViPNet CSP при несоблюдении пользователем данного условия.

II. Получение и установка КриптоПро CSP

1. Для получения КриптоПро CSP необходимо перейти на официальный сайт разработчика (http://www.cryptopro.ru/cryptopro/products/csp/default.htm) и затем к странице для загрузки файла с сайта: Загрузить СКЗИ «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[4]. 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, пароль локального администратора должен быть не пустой).

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. Запустите КриптоПро CSP. Откройте вкладку ***«Общие»*** и нажмите на кнопку ***«Ввод лицензии…»***. Затем заполните поля ***«Пользователь»***, ***«Организация»***, введите ***«Серийный номер»***[5] (серийный номер, полученный у организации-разработчика или организации, имеющей права на распространение продукта)[6] и нажмите кнопку ***«ОК»*** (Рисунок 1).

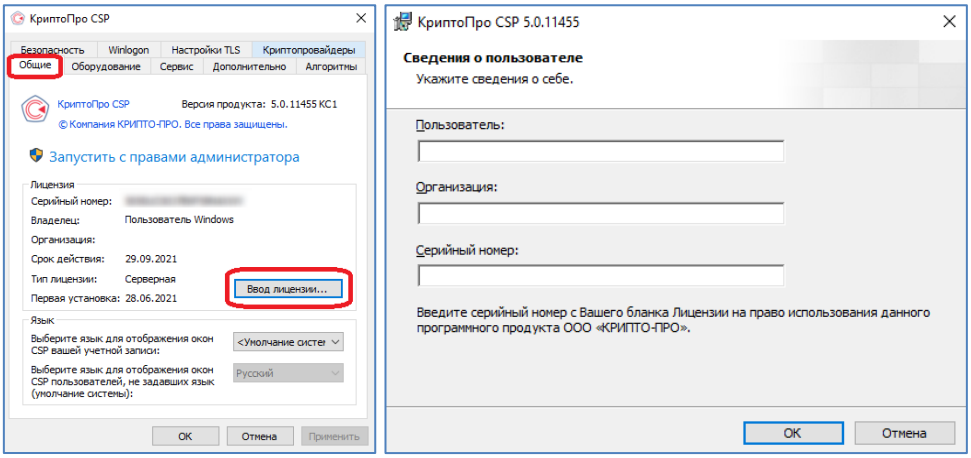

Рисунок 1

[4] В соответствии с выпиской из документа ФСБ России от 31 января 2014 г. №149/7/1/3-58 «О порядке перехода к использованию новых стандартов ЭЦП и функции хэширования», использование схемы подписи ГОСТ Р 34.10-2001 для формирования подписи после 31 декабря 2018 года не допускается. С 1 января 2019 года для формирования усиленной квалифицированной электронной подписи возможно использование только сертифицированных криптографических средств, реализующих ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012. Они реализуются в «КриптоПро CSP» версии 5.0 и выше.

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

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

III. Настройка КриптоПро CSP для работы с электронной подписью

Установку личного сертификата возможно выполнить несколькими способами:

А. Установка личного сертификата с ключевого носителя JaCarta LT

Б. Установка сертификата через личный кабинет

В. Установка личного сертификата с дискового носителя

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

А. Установка личного сертификата с ключевого носителя JaCarta LT[7]

Внимание! Данный пункт инструкции следует использовать, ТОЛЬКО если Вам выдали ключевой носитель JaCarta. Если Вы генерировали запрос через личный кабинет iitrust.lk или Вам выдали ключевой дистрибутив на диске, то Вам следует перейти к пунктам Б/В текущей инструкции.

1. Для корректной работы ключевого носителя 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).

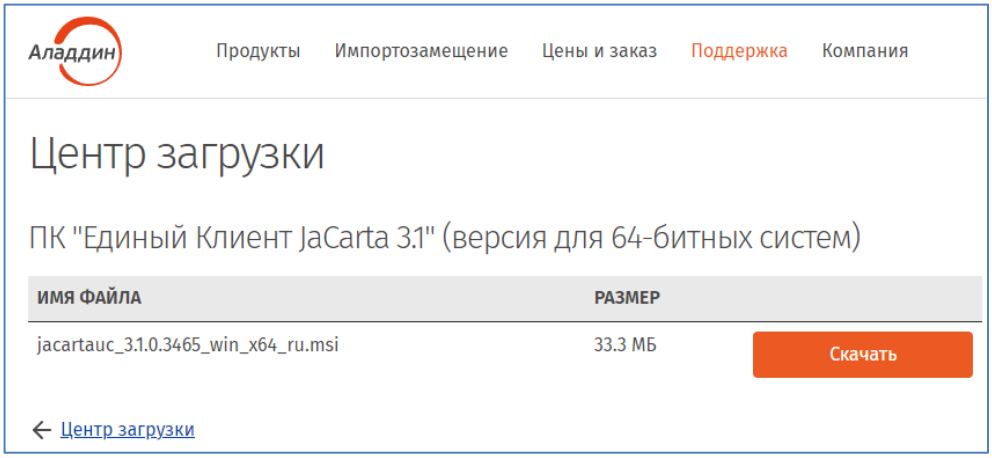

Рисунок 2

2. Загрузите дистрибутив в любое место компьютера и запустите установку утилиты. Выполните установку, следуя инструкциям мастера установки.

Внимание! Убедитесь, что ключевой носитель JaCarta LT находится в USB-порту Вашего компьютера

3. В основном окне КриптоПро CSP, перейдите на вкладку ***«Сервис»*** и нажмите кнопку ***«Просмотреть сертификаты в контейнере»*** (Рисунок 3, позиция А).

[7] Если вы используете ключевой носитель Rutoken, то вам необходимо установить программное обеспечение компании «Актив» по ссылке https://www.rutoken.ru/support/download/windows/.
Если вы используете ключевой носитель eToken, то вам необходимо установить программное обеспечение компании Аладдин РД ***«eToken PKI Client»*** по ссылкам:
- для 64-разрядной системы;
- для 32-разрядной системы.

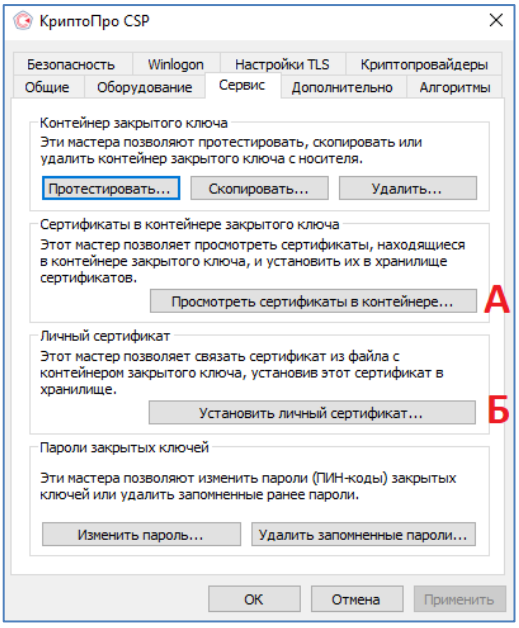

Рисунок 3

4. В открывшемся окне нажмите кнопку ***«Обзор»***, чтобы выбрать контейнер для просмотра. После выбора нужного контейнера нажмите кнопку ***«Ок»*** (Рисунок 4).

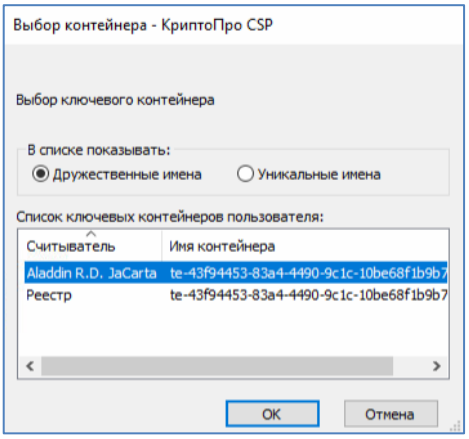

Рисунок 4

5. В следующем окне нажмите кнопку ***«Далее».*** Если запросит пароль, введите[8].

Если после нажатия кнопки «Далее» появляется сообщение «В контейнере закрытого ключа отсутствует открытый ключ шифрования», необходимо перейти к установке сертификата с помощью Варианта Б.

6. В открывшемся окне следует нажать кнопку ***«Установить»*** (Рисунок 5), после чего утвердительно ответить на уведомление о замене сертификата, если оно появится (Рисунок 6).

[8] По умолчанию PIN-код пользователя на устройство JaCarta LT:

- если носитель получен до 15.01.2019: **1eToken**
- с 15.01.19 года PIN -код устанавливается **1234567890**

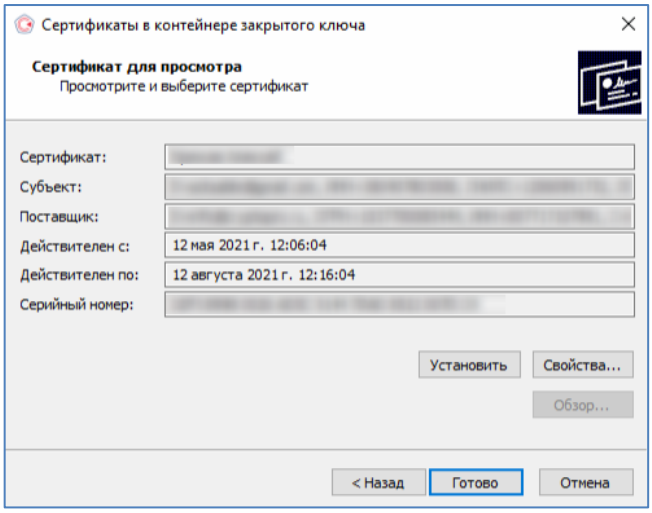

Рисунок 5

7. Если сертификат ранее уже был установлен, появится следующее информационное окно, нажмите кнопку ***«Да»*** (Рисунок 6).

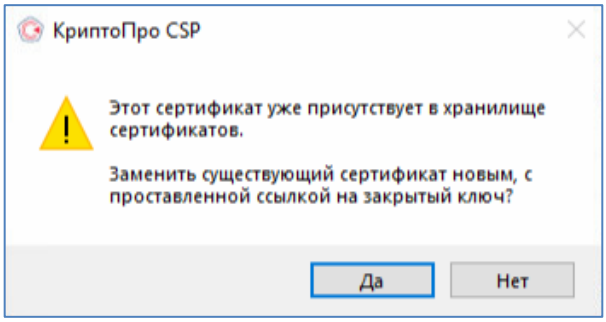

Рисунок 6

8. Если ранее сертификат не был установлен, то появится информационное окно, что сертификат был успешно установлен в хранилище «Личное» текущего пользователя (Рисунок 7).

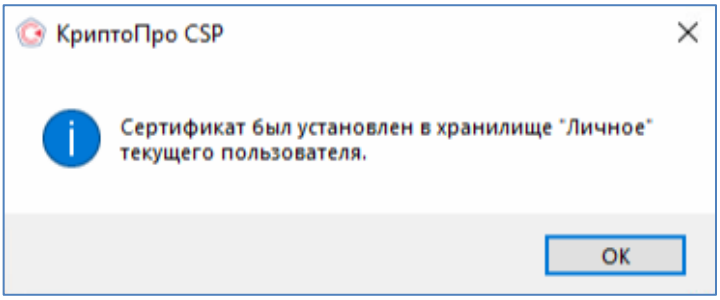

Рисунок 7

9. Перейти к 5 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 8).

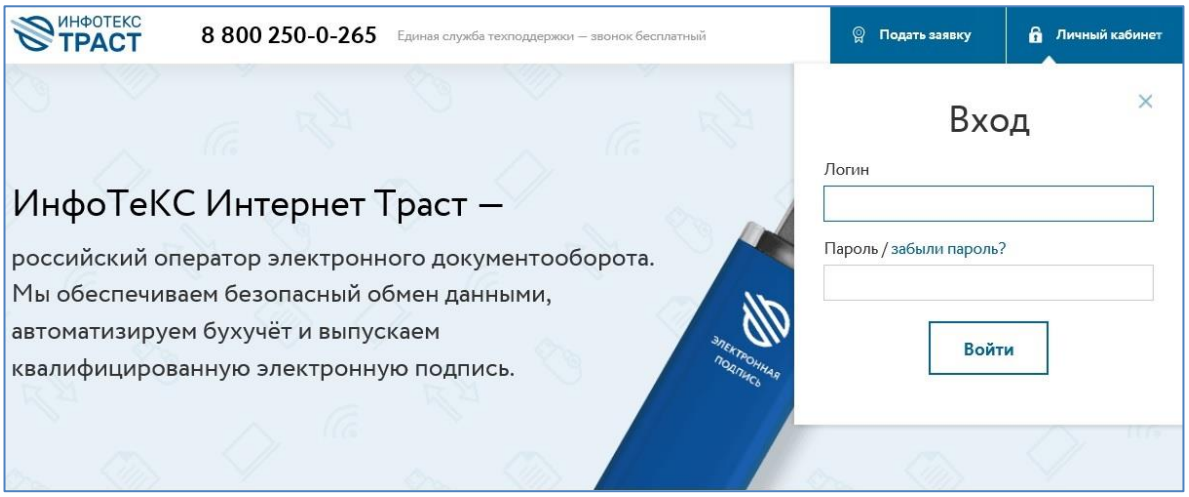

Рисунок 8

В списке заявок выберите заявку в статусе ***«Завершена»*** и нажмите на ее номер/строчку (Рисунок 9).

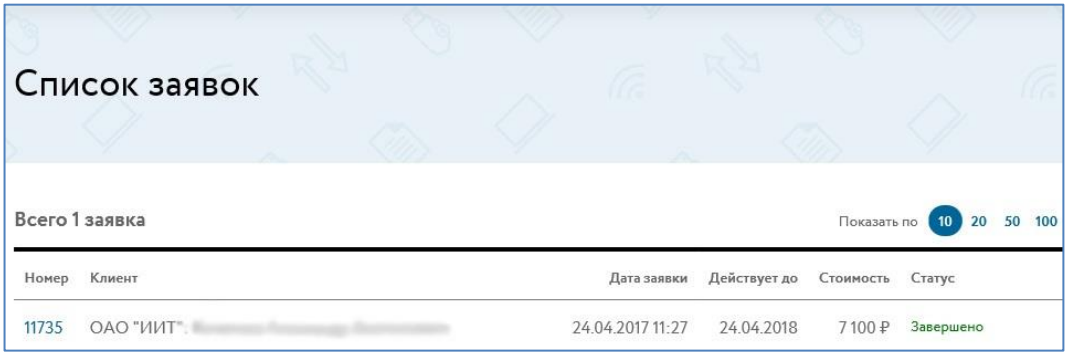

Рисунок 9

На странице нажмите кнопку ***«Установить»***[9] (Рисунок 10). Сертификат будет успешно установлен в контейнер[10]. (Рисунок 11).

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

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

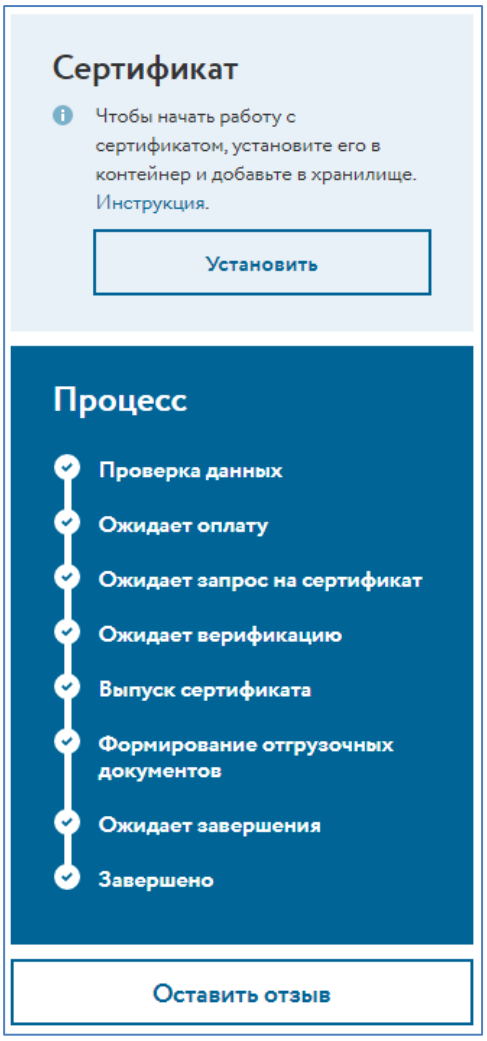

Рисунок 10

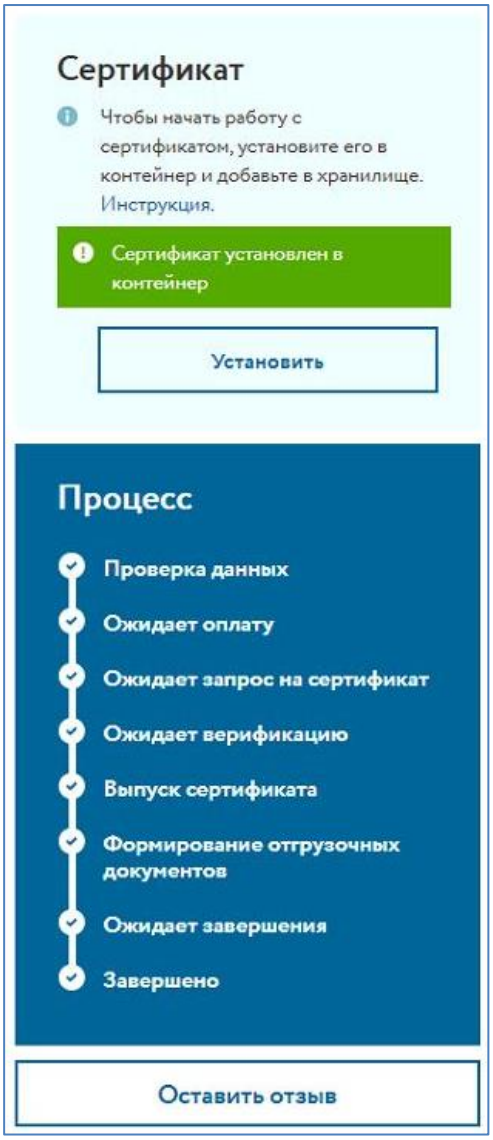

Рисунок 11

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 12).

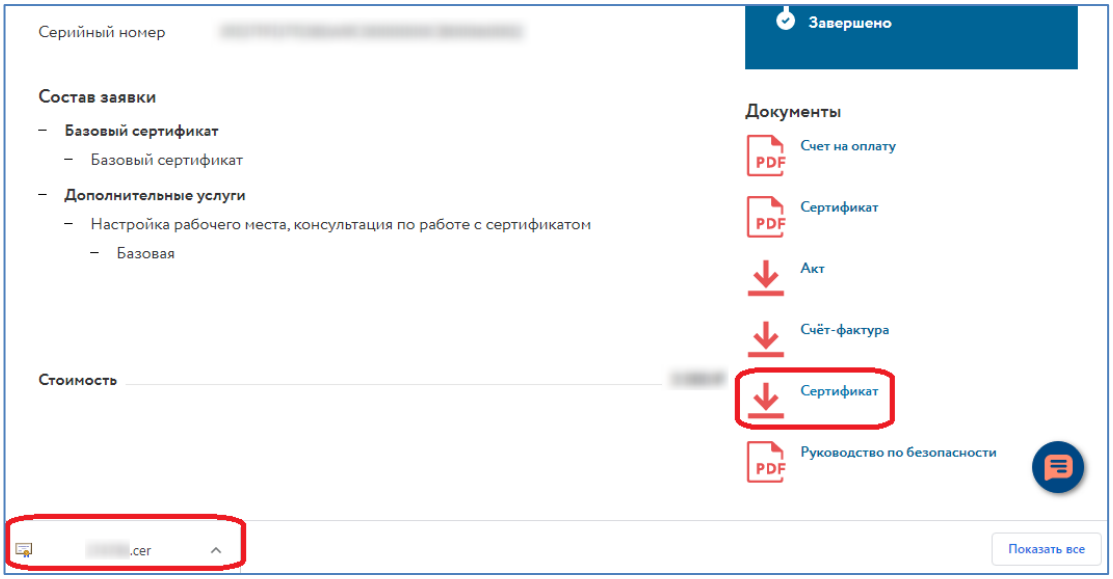

Рисунок 12

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 13)**.**

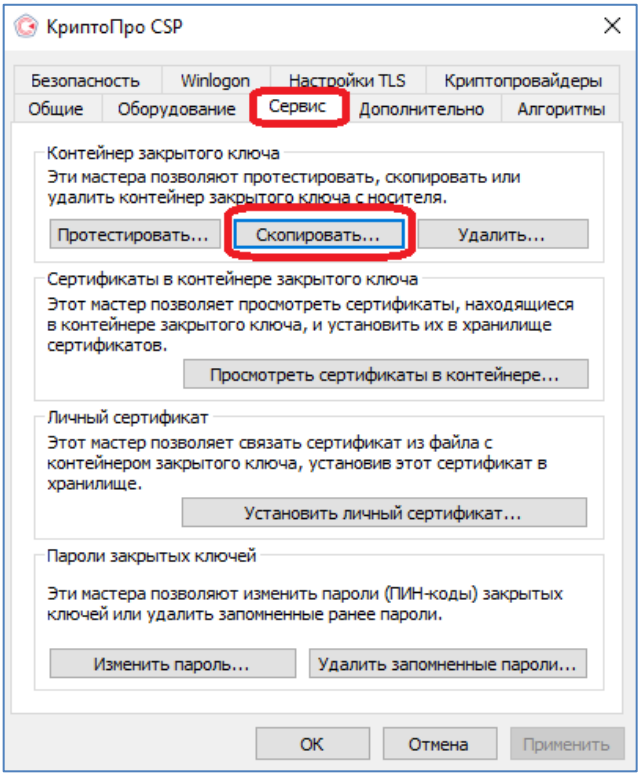

Рисунок 13

4. Нажмите кнопку ***«Обзор…»*** для выбора контейнера закрытого ключа, выберите нужный контейнер и нажмите кнопку ***«ОК»*** (Рисунки 14-15).

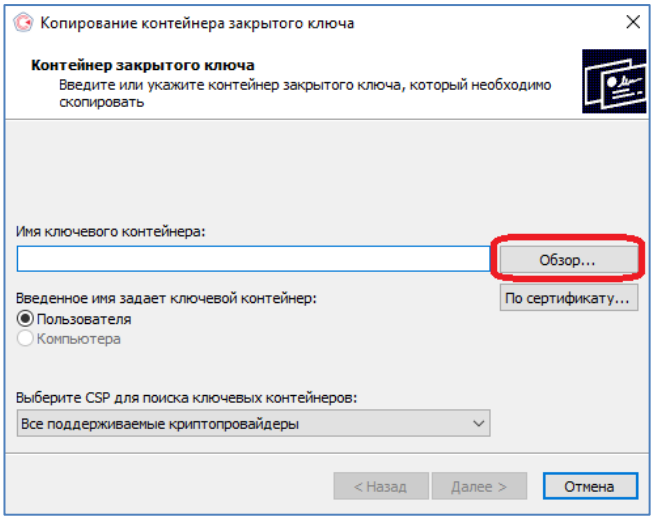

Рисунок 14

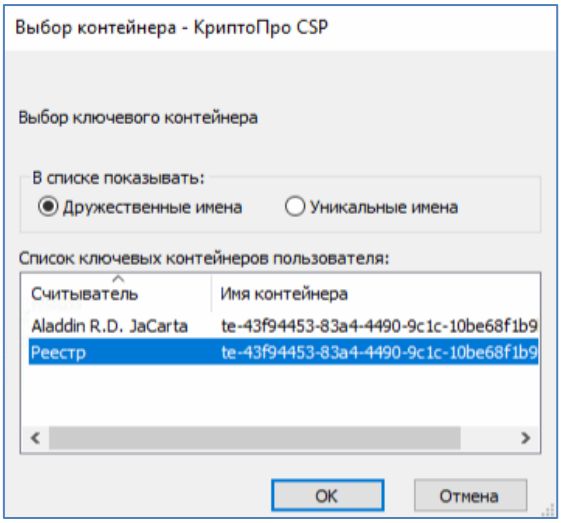

Рисунок 15

5. При необходимости введите пароль к контейнеру закрытого ключа[11] (Рисунок 16).

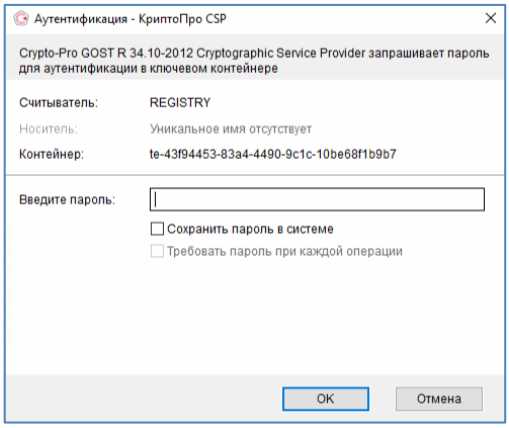

Рисунок 16

6. Задайте имя контейнера, который будет храниться на JaCarta LT, и нажмите ***«Готово»*** (Рисунок 17).

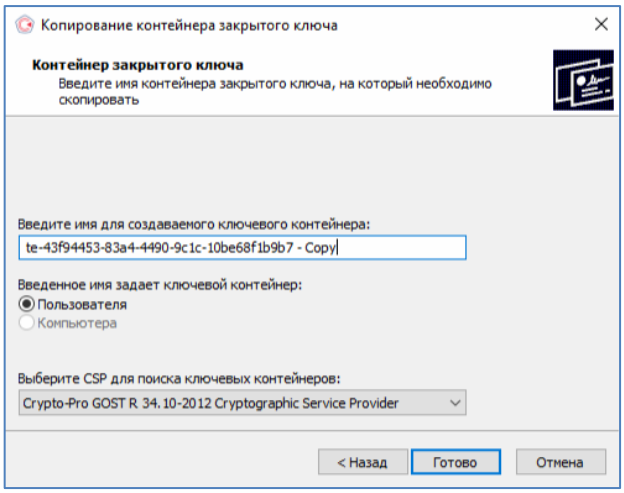

Рисунок 17

В окне выбора носителя укажите JaCarta LT ***Aladdin JaCarta*** и нажмите ***«ОК»***, при необходимости введите пароль для устройства JaCarta LT (Рисунок 18).

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

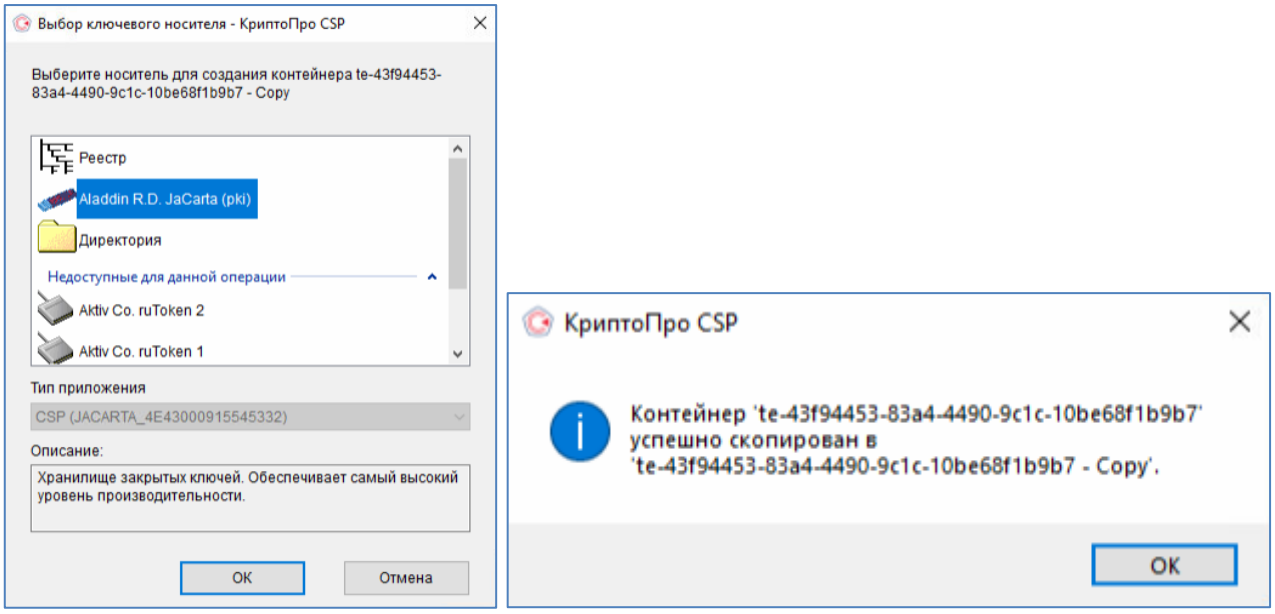

Рисунок 18

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 19).

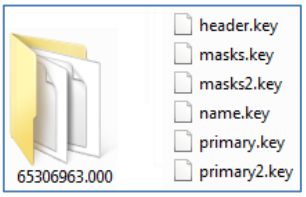

Рисунок 19

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 20).

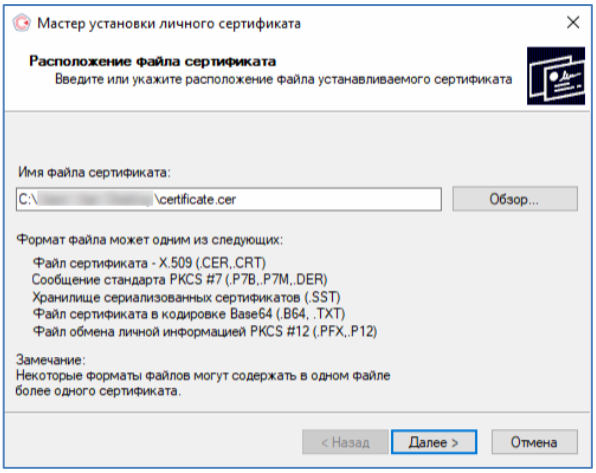

Рисунок 20

3. В следующем окне кликнуть по кнопке ***«Далее»*** (Рисунок 21).

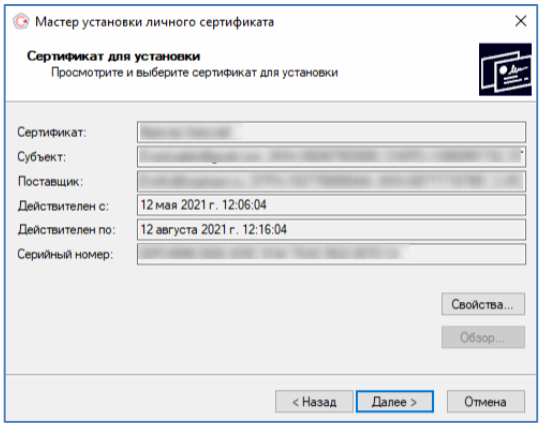

Рисунок 21

4. Укажите пункт ***«Найти контейнер автоматически»*** (Рисунки 22 - 23).

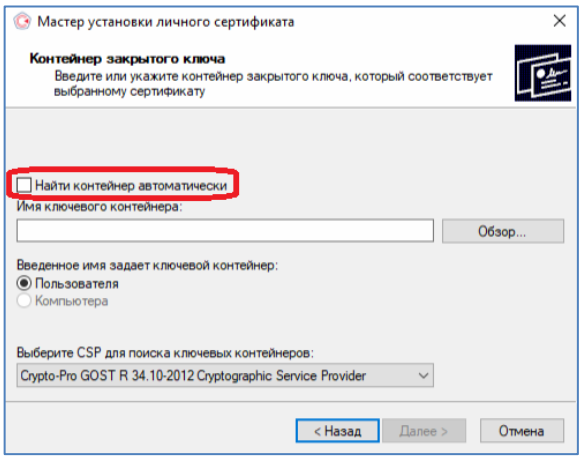

Рисунок 22

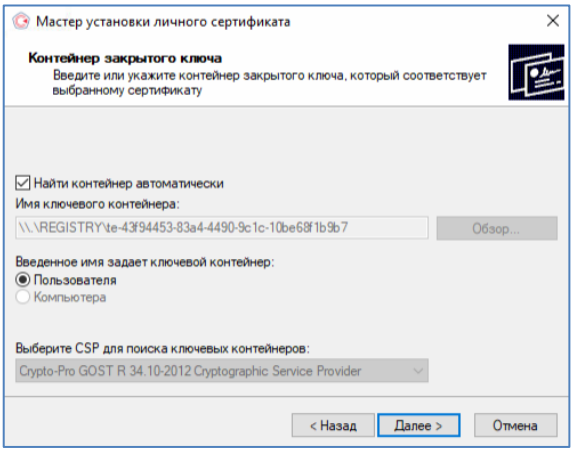

Рисунок 23

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, стандартный пароль к контейнеру, полученному на диске: 123456. Рекомендуется сменить ПИН доступа к JaCarta LT 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 24).

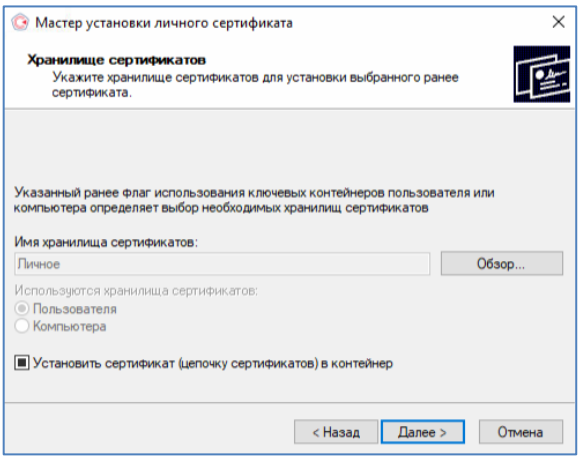

Рисунок 24

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 25).

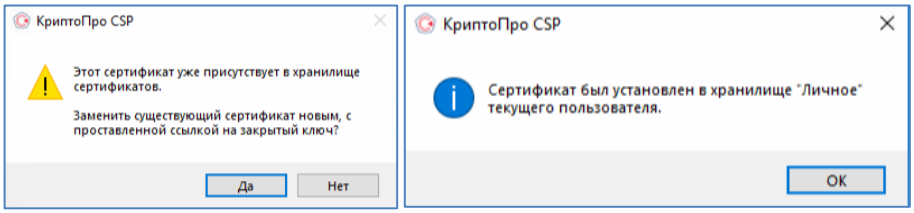

Рисунок 25

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

- ✓ Загрузить головные сертификаты удостоверяющего центра Министерства связи и массовых коммуникаций (далее по тексту - ***Головной УЦ***) можно самостоятельно с официального сайта[12], либо по ссылкам:
  - **http://reestr-pki.ru/cdp/guc_gost12.crt**[13]
  - **http://reestr-pki.ru/cdp/guc2021.crt**[14]
  - **http://reestr-pki.ru/cdp/guc2022.crt**[15]
- ✓ Откройте загруженный сертификат и нажмите ***«Установить сертификат»*** (Рисунок 26).
- ✓ 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 27, позиция А), нажать ***«Обзор»*** (Рисунок 27, позиция Б), выбрать ***«Доверенные корневые центры сертификации»*** (Рисунок 27, позиция В), нажать ***«Далее»*** (Рисунок 27, позиция Г).

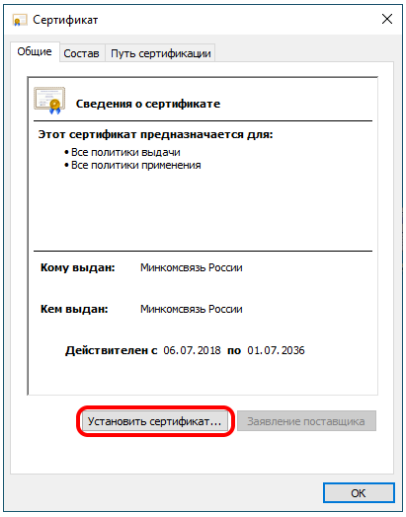

Рисунок 26

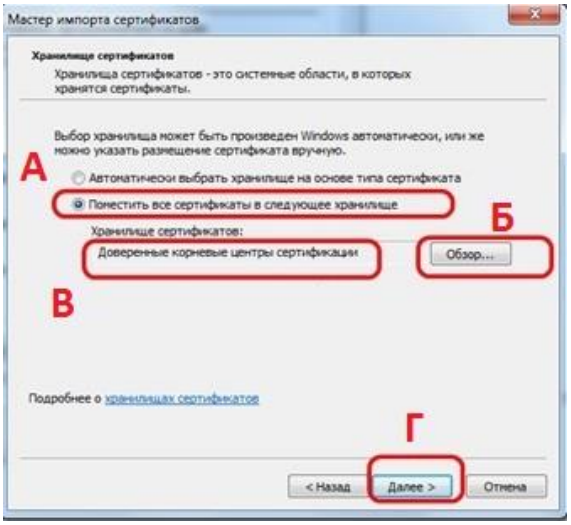

Рисунок 27

- ✓ Далее на все запросы мастера импорта сертификатов об установке сертификата ***«Далее»/«Да»/«ОК»*** - соглашаетесь.
- ✓ Установите оба сертификата.
- ✓ Для сертификатов, выпущенных в УЦ ФНС после 05.05.2022 года, установите подчиненный сертификат УЦ ФНС России[16] в хранилище «Промежуточные центры сертификации».

---

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

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

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

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

[16] URL: https://e-trust.gosuslugi.ru/app/scc/portal/api/v1/portal/ca/download/021B60DA90EDB6DCE479528359057BE69D4D4884

V. Смена PIN-кода на доступ к содержимому устройству 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 28).
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 29).
7. Нажмите кнопку ***«Выполнить»***. При успешной установке нового PIN-кода пользователя появится соответствующее сообщение (Рисунок 30).

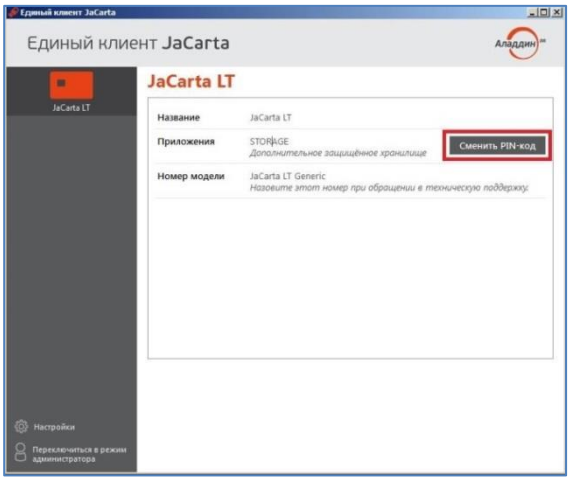

Рисунок 28

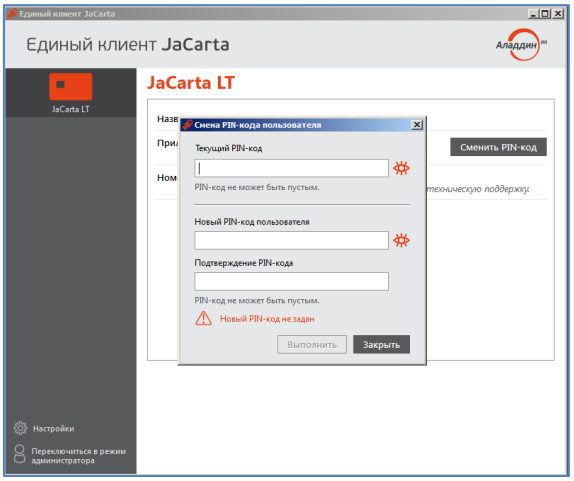

Рисунок 29

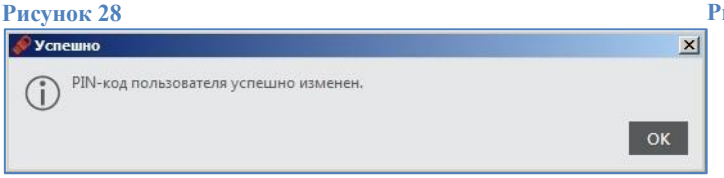

Рисунок 30

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.