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

Листов 22

Инфотекс Интернет Траст
2025 г.

Оглавление

I. Введение

✓ Документ предназначен для пользователей, осуществляющих самостоятельную установку средства криптографической защиты информации (СКЗИ) ViPNet 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 КриптоПро 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 ViPNet CSP на компьютер, где уже установлено СКЗИ «КриптоПро CSP». В случае использования 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 ViPNet CSP

1. Для получения ViPNet CSP необходимо перейти на официальный сайт разработчика по адресу: https://infotecs.ru/downloads/latest/?product=vipnet_csp&type=full и скачать актуальную версию.
2. Пройдите установленную процедуру регистрации, согласившись с условиями лицензионного соглашения (EULA) и заполнив обязательные поля.
3. Ссылка для скачивания продукта и серийный номер будут отправлены на указанный Вами адрес электронной почты при регистрации. Перейдите по полученной ссылке для скачивания, сохраните загруженный архив с дистрибутивом на своем компьютере, распакуйте архив, затем запустите установку ViPNet CSP exe-файлом.
4. Выполните установку ViPNet CSP, следуя инструкциям мастера установки.
5. После перезагрузки компьютера запустите настройку ViPNet CSP из панели ***«Пуск».***

✓ Выберите пункт ***«Зарегистрировать ViPNet CSP»*** и нажмите кнопку ***«Далее»*** (Рисунок 1)[4].

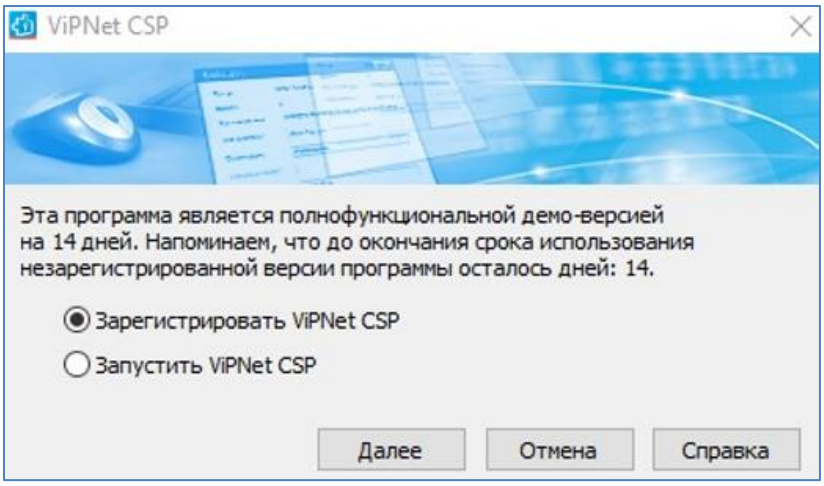

Рисунок 1

✓ Выберите пункт ***«Запрос на регистрацию (получить код регистрации)»*** и нажмите кнопку ***«Далее»*** (Рисунок 2).

[4] Без регистрации ViPNet CSP будет функционировать в течение 14 дней и не сможет обеспечить юридической значимости электронной подписи.

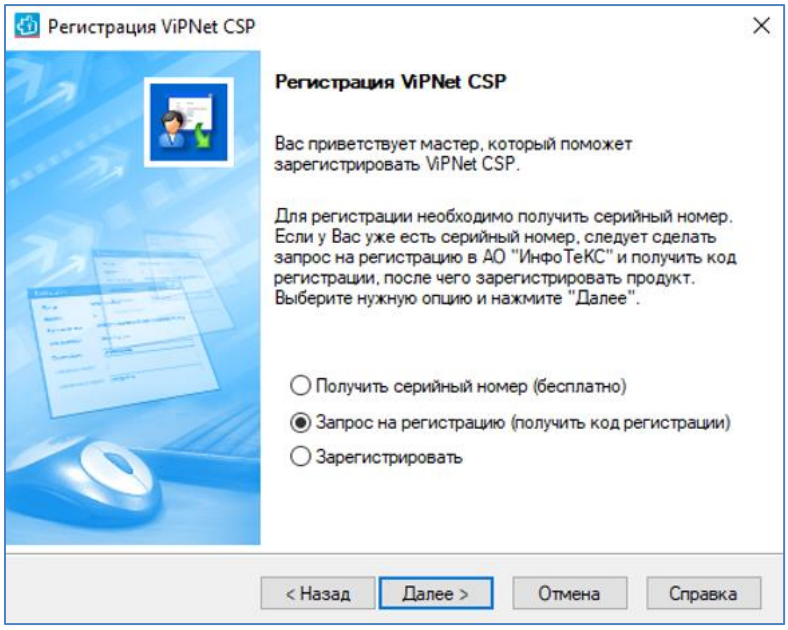

Рисунок 2

✓ Выберите пункт ***«Через Интернет (online)»*** и нажмите кнопку ***«Далее»*** (Рисунок 3).

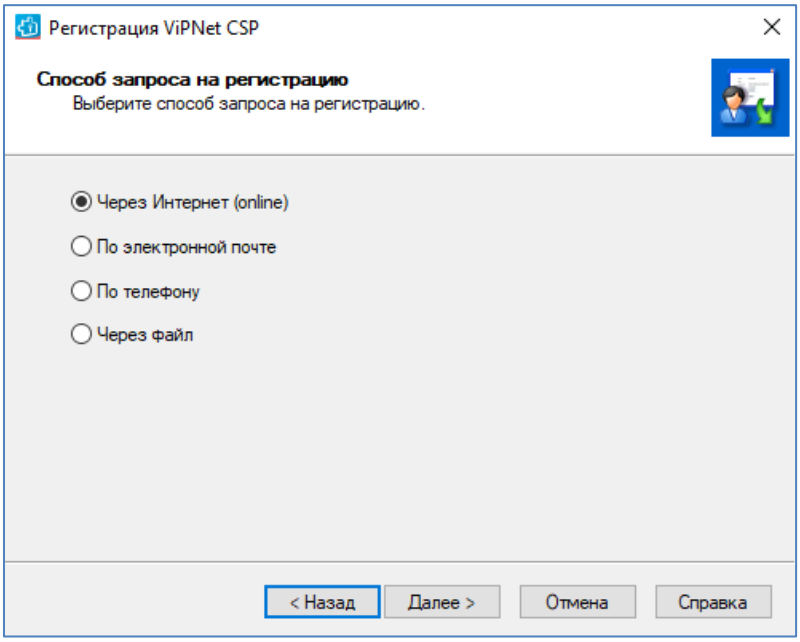

Рисунок 3

✓ Заполните форму своими регистрационными данными, включая ***«Серийный номер»*** ViPNet CSP, полученный при регистрации на ваш E-mail и нажмите кнопку ***«Далее»*** (Рисунок 4).

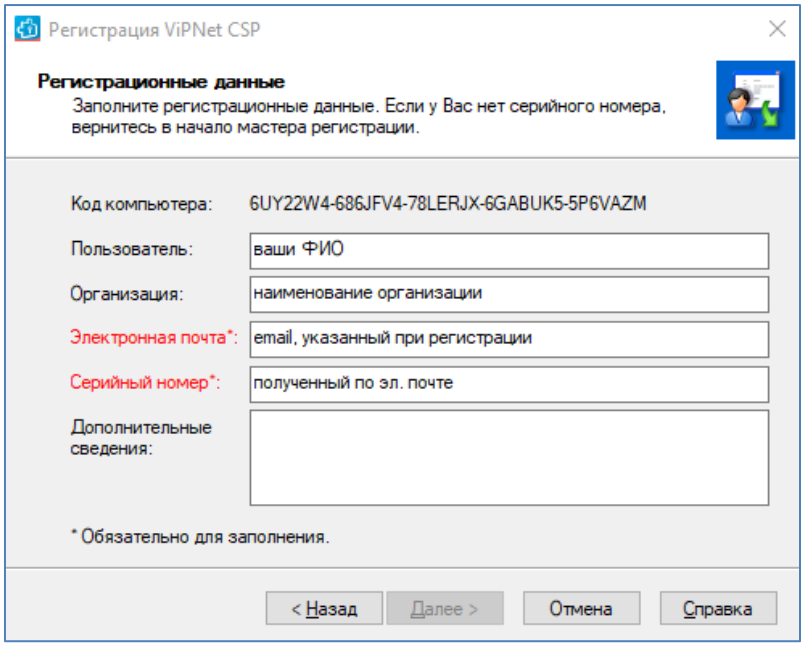

Рисунок 4

✓ После завершения процесса регистрации нажмите кнопку ***«Готово»*** (Рисунок 5).

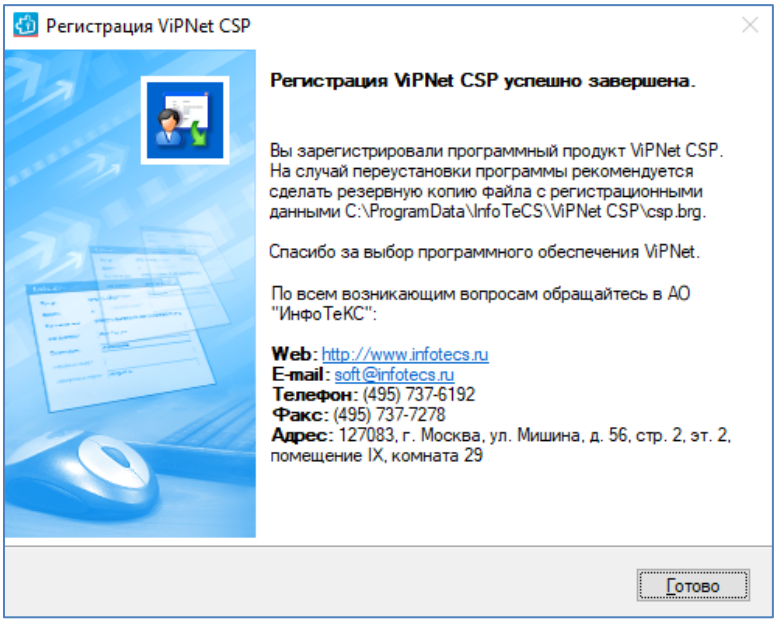

Рисунок 5

✓ На вопрос ***«Запустить ViPNet CSP сейчас?»*** нажмите кнопку ***«Да»*** или запустите ViPNet CSP позже из панели ***«Пуск».***

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 2.0/3.0, 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 6).

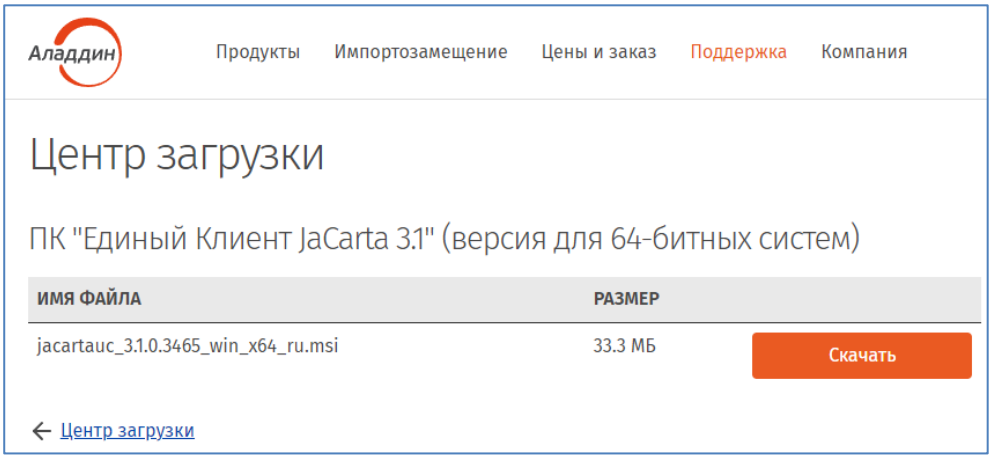

Рисунок 6

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 7).

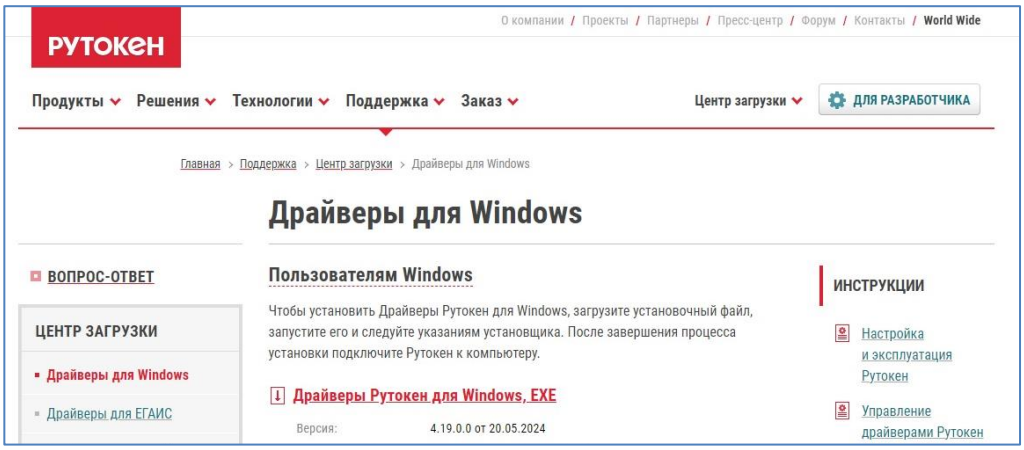

Рисунок 7

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 ViPNet CSP и убедитесь, что в разделе ***«Дополнительно»*** включена опция ***«Поддержка работы ViPNet CSP через Microsoft CryptoAPI»*** (Рисунок 8).

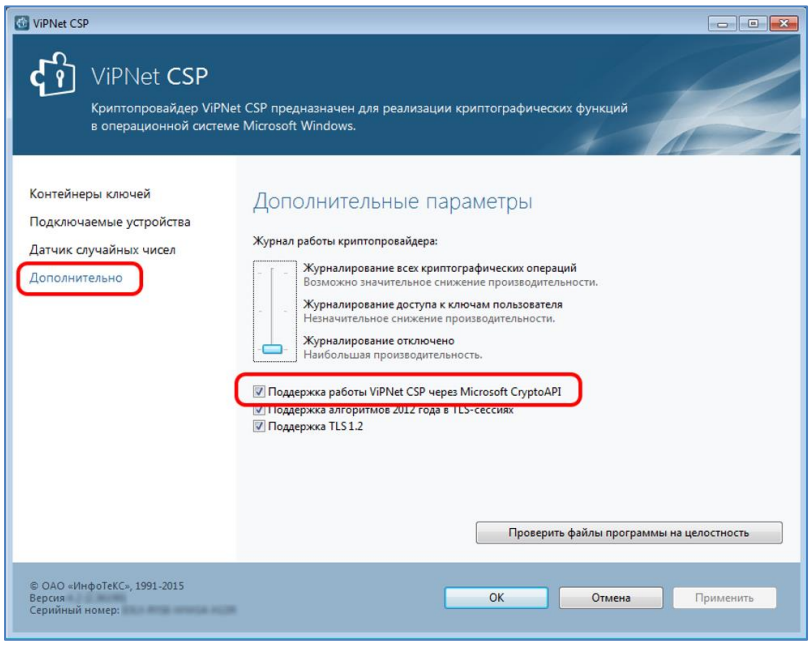

Рисунок 8

2. Перейдите в раздел ***«Контейнеры ключей».*** В выпадающем списке выберите подключенный защищенный носитель JaCarta или Рутокен, а в разделе ***«Имя контейнера»*** – контейнер ключей ***«XX-XXXX-XXXX-XXXX-XXXX»***. Затем нажмите кнопку ***«Свойства»*** (Рисунок). Если выпадающего списка нет, вероятно носитель «пустой» и вы генерировали контейнер самостоятельно через личный кабинет ИИТ. Процесс переноса контейнера на ключевой носитель описан на странице 17 данной инструкции.

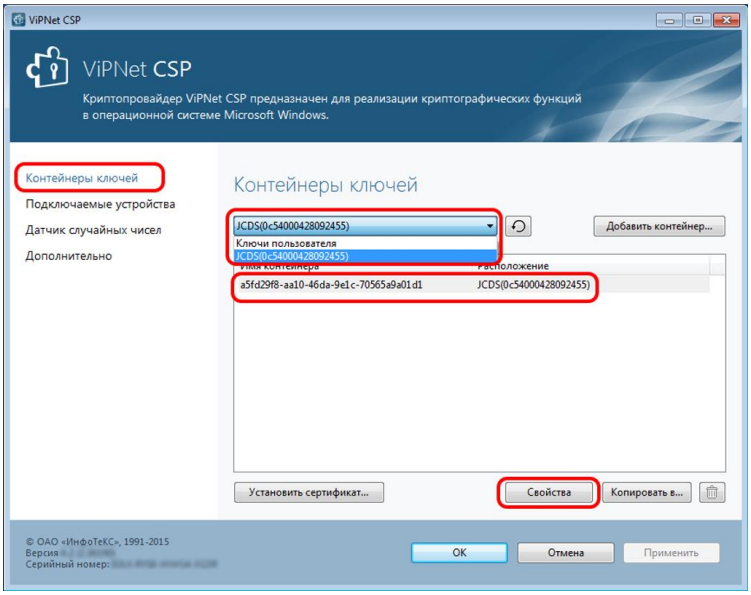

Рисунок 9

3. В окне свойств контейнера ключей (Рисунок 10 для Jacarta и Рисунок 11 для Рутокена) в разделе ***«Закрытый ключ, находящийся в контейнере»*** нажмите кнопку ***«Открыть»***.

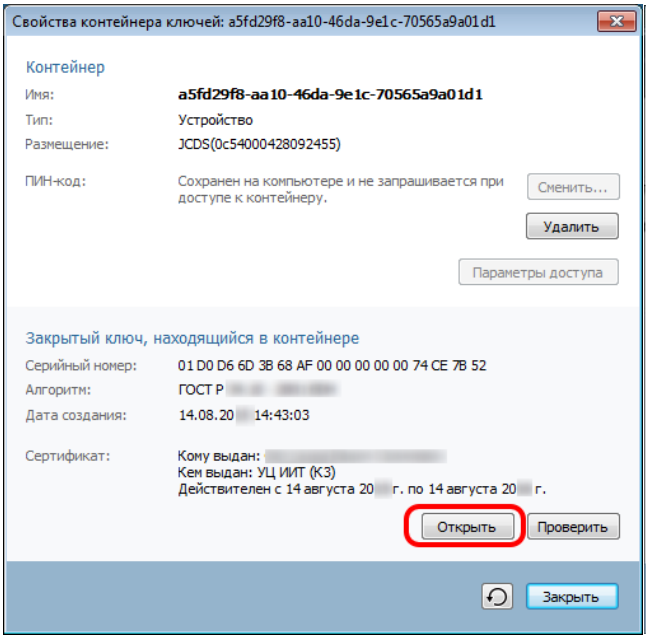

Рисунок 10

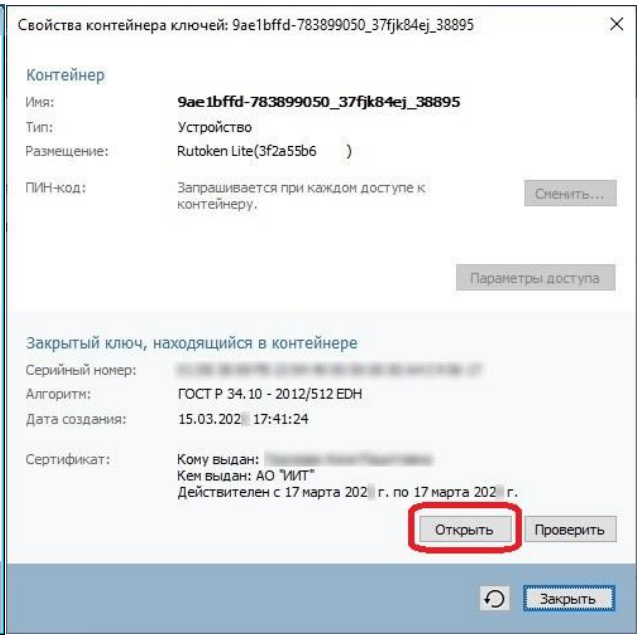

Рисунок 11

4. Убедитесь, что выбран именно тот сертификат, который необходимо использовать, и нажмите кнопку ***«Установить сертификат»*** (Рисунок 12).

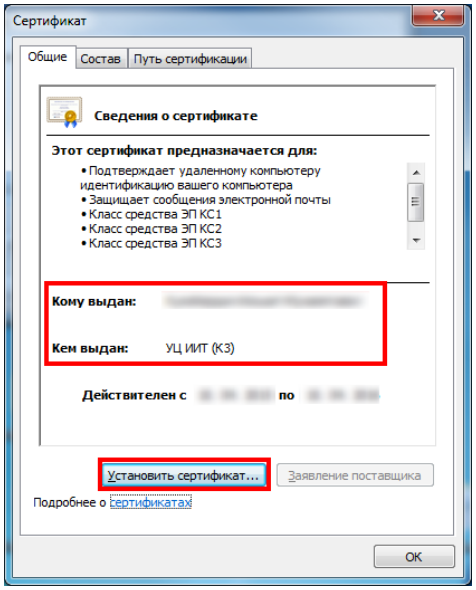

Рисунок 12

5. Далее следуйте указаниям **Мастера установки сертификатов**. В ходе установки сертификата обращайте внимание на выбранные опции, которые должны соответствовать рисункам 13-15.

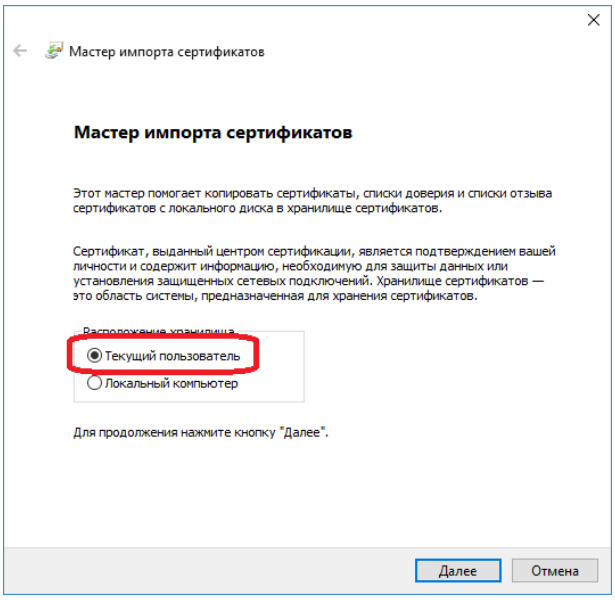

Рисунок 13

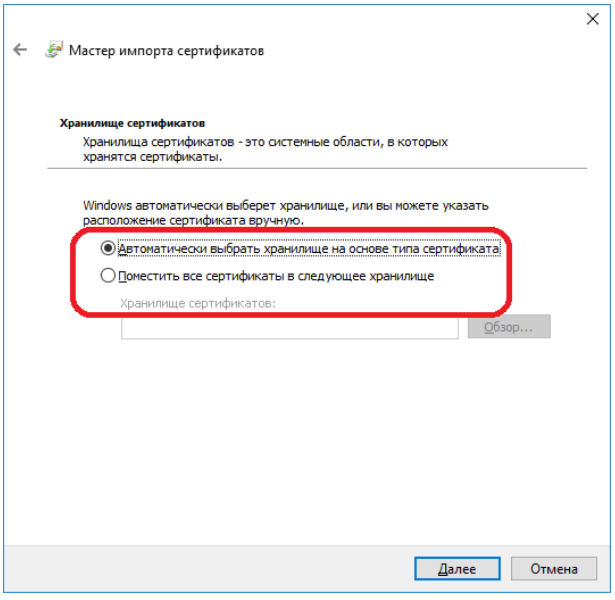

Рисунок 14

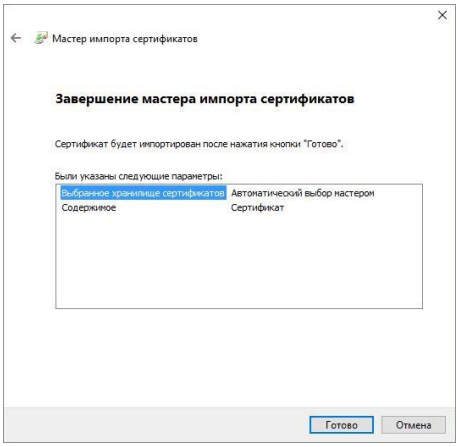

Рисунок 15

6. В появившемся на очередном шаге окне (Рисунок 16) введите PIN-код к устройству.
7. На этом работа Мастера установки сертификата завершается (Рисунок 17) нажмите кнопку ***«Готово»*** и переходите к следующему пункту инструкции.

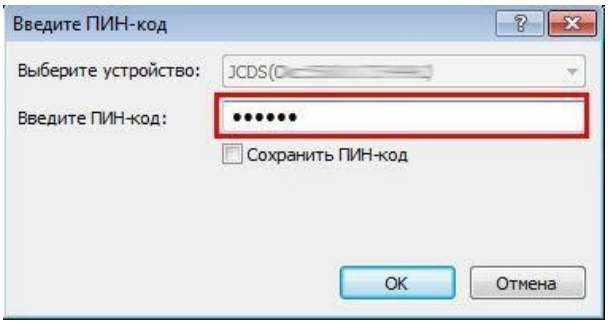

Рисунок 16

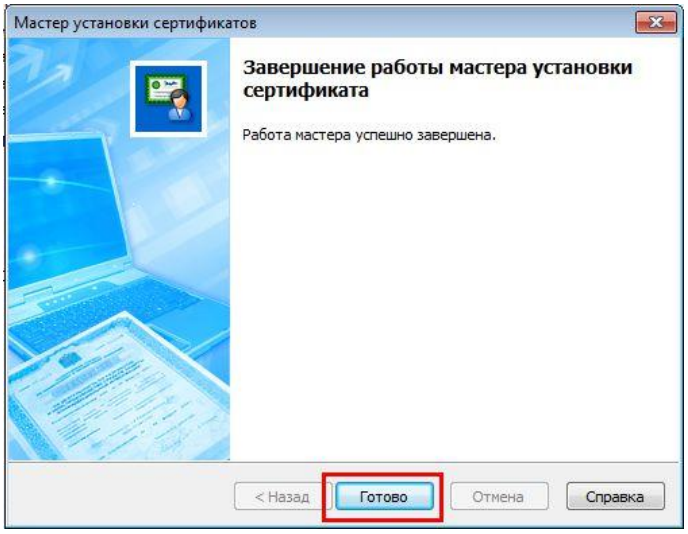

Рисунок 17

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.

11. 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. 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 18).

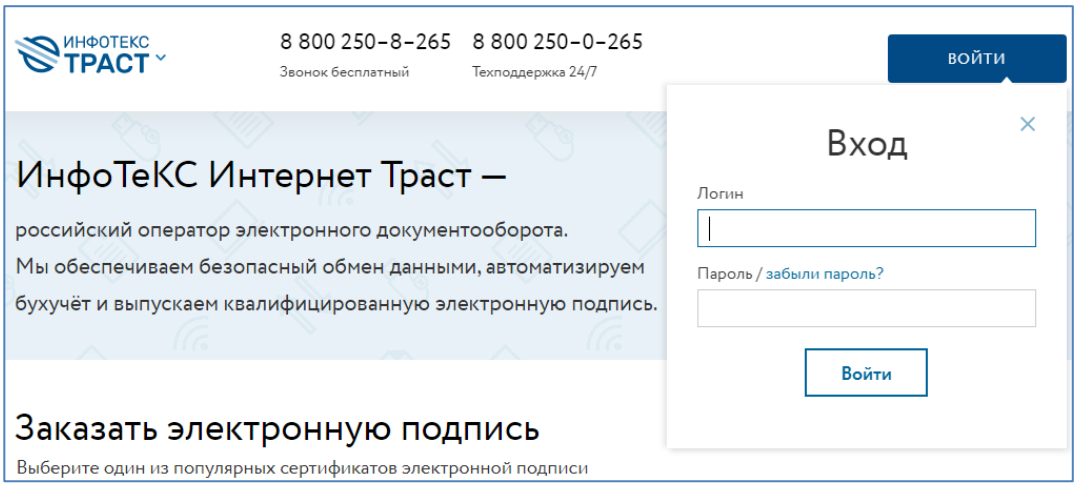

Рисунок 18

В списке заявок выберите заявку в статусе ***«Завершена»***, в которой выпускался сертификат, и нажмите на ее номер/строчку (Рисунок 19).

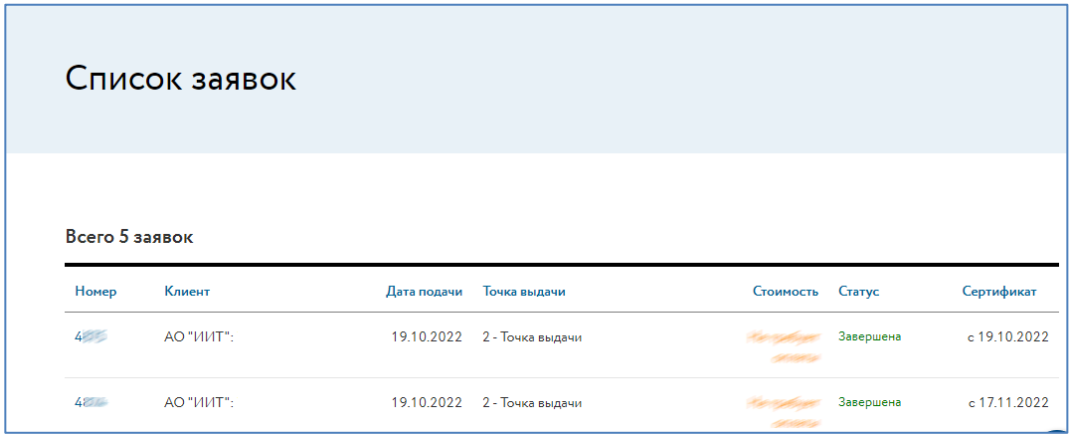

Рисунок 19

На странице нажмите кнопку ***«Установить»***[5] (Рисунок 20). Сертификат будет успешно установлен в контейнер (Рисунок 21).

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

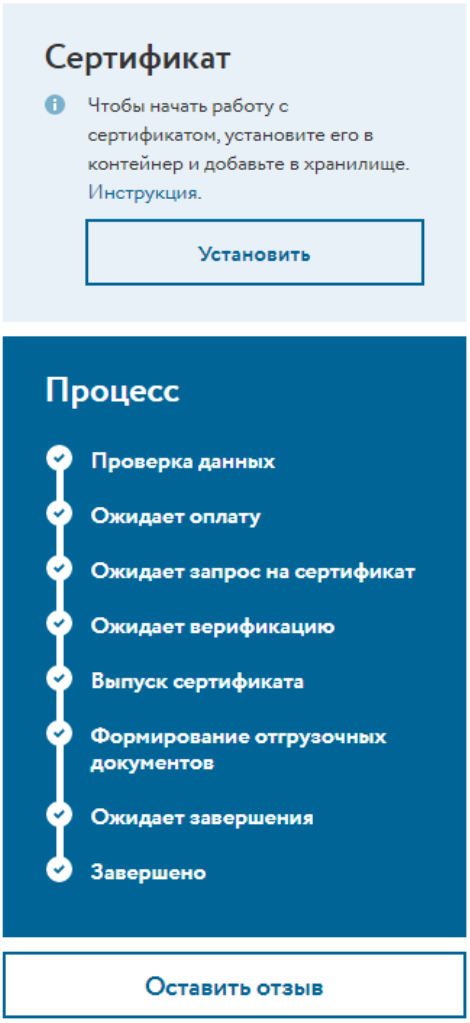

Рисунок 20

Рисунок 21

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, пункты 5-8**.

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 22).

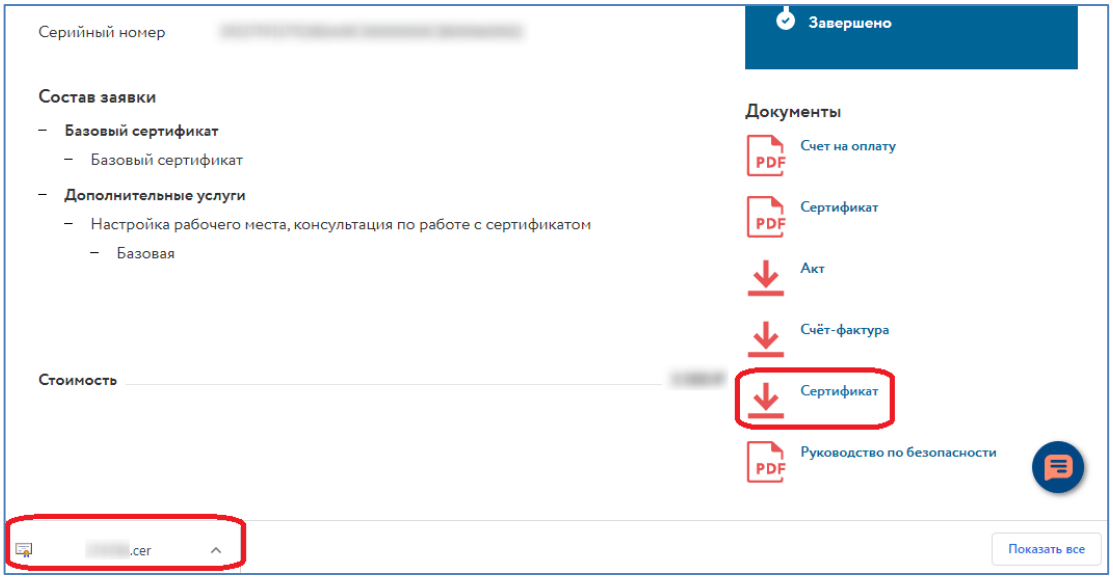

Рисунок 22

По умолчанию контейнер ключей сохраняется на жестком диске в папке:

- C:\Users\%username%\AppData\Local\Infotecs\Containers\

Для установки сертификата в контейнер ключей выполните следующие действия:

1. Запустите криптопровайдер ***ViPNet CSP*** с ярлыка на рабочем столе или из кнопки меню ***«Пуск» -> «Все приложения» -> «ViPNet» -> «ViPNet CSP».***

2. В разделе ***«Контейнеры ключей»*** проверьте, отображается ли контейнер, который ранее был сформирован**.** Если в списке контейнера нет, то необходимо его добавить, нажав на кнопку ***«Добавить контейнер…»*** и указав путь до контейнера ключей, указанного при генерации запроса. Затем нажмите кнопку ***«Установить сертификат…»*** (Рисунок 23).

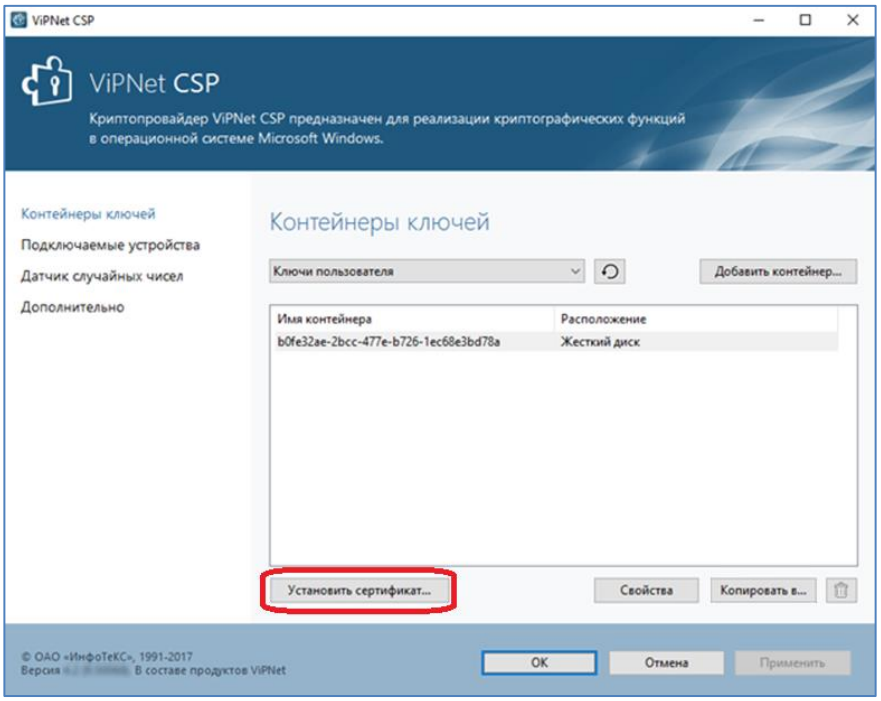

Рисунок 23

3. Укажите файл с сертификатом, загруженный из ЛК ИИТ в формате ***«имя файла».cer*** и нажмите кнопку ***«Открыть»*** (Рисунок 24).

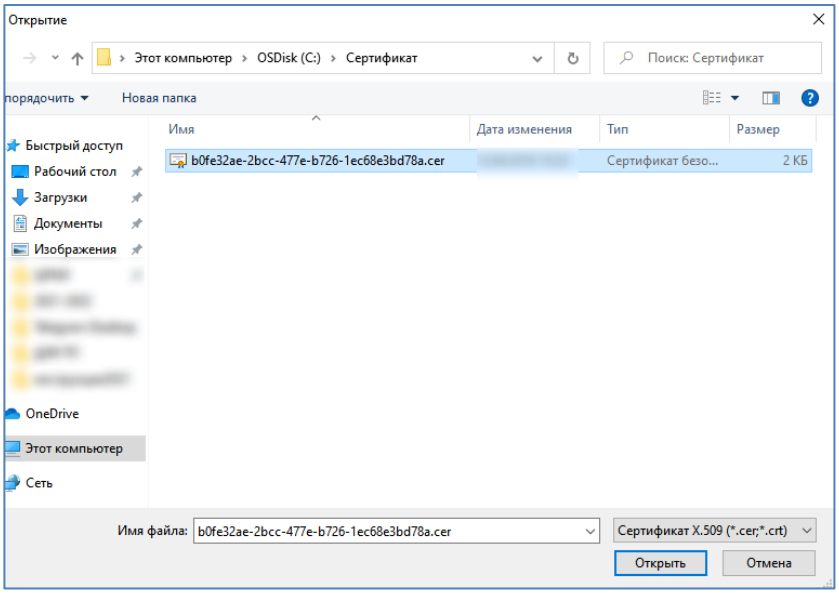

Рисунок 24

4. Нажмите кнопку ***«Далее»*** и затем выберите установить в хранилище сертификатов **текущего пользователя** (Рисунок 25).

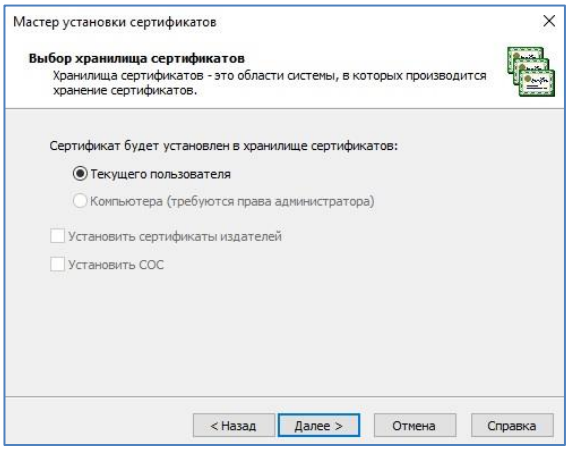

Рисунок 25

5. Откроется мастер установки сертификатов. Укажите ***«Найти контейнер с закрытым ключом»*** (Рисунок 26).

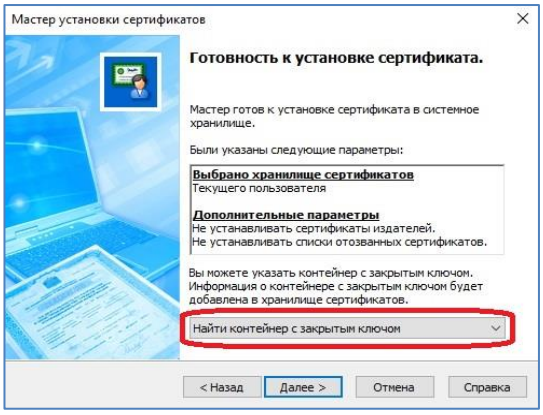

Рисунок 26

6. ViPNet CSP автоматически определит расположение контейнера на ПК, затем нажмите ***«ОК»*** и ***«Готово»*** (Рисунки 27-28).

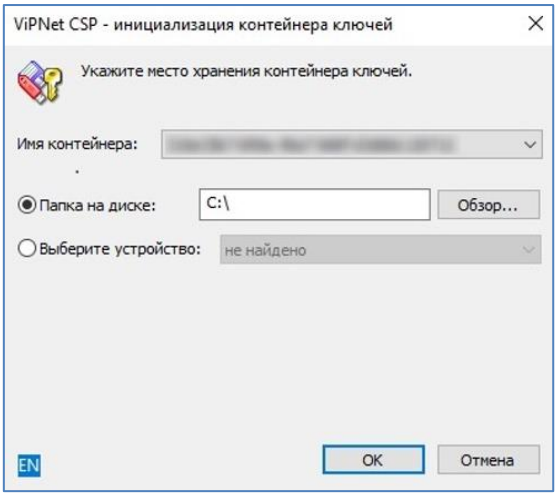

Рисунок 27

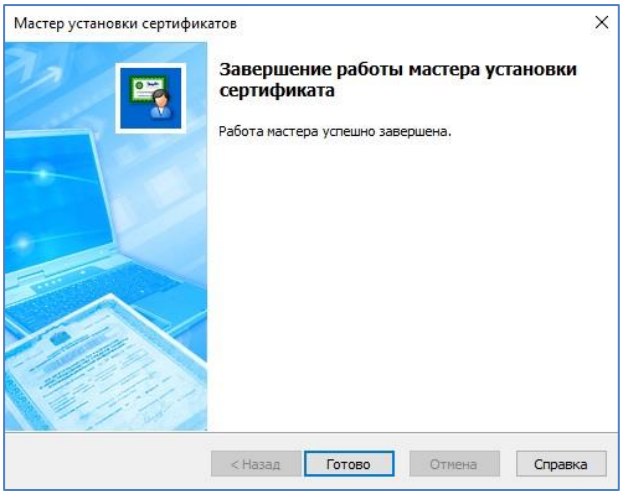

Рисунок 28

- ✓ Для того чтобы скопировать контейнер ключей на ключевой носитель JaCarta/Рутокен необходимо установить драйвер ***«Единый клиент JaCarta»/ «Панель управления Рутокен»***, описание установки приведено в разделе III. Если вы не приобретали JaCarta/Рутокен, контейнер должен располагаться на жестком диске, в разделе ключи пользователя.
- ✓ Запустите криптопровайдер ***ViPNet CSP*** с ярлыка на рабочем столе или из **кнопки** меню ***«Пуск» -> «Все приложения» -> «ViPNet» -> «ViPNet CSP».***
- ✓ Перейдите в раздел ***«Контейнеры ключей»***. Выберите сформированный ранее контейнер закрытого ключа и нажмите кнопку ***«Копировать в…»*** (Рисунок 29).

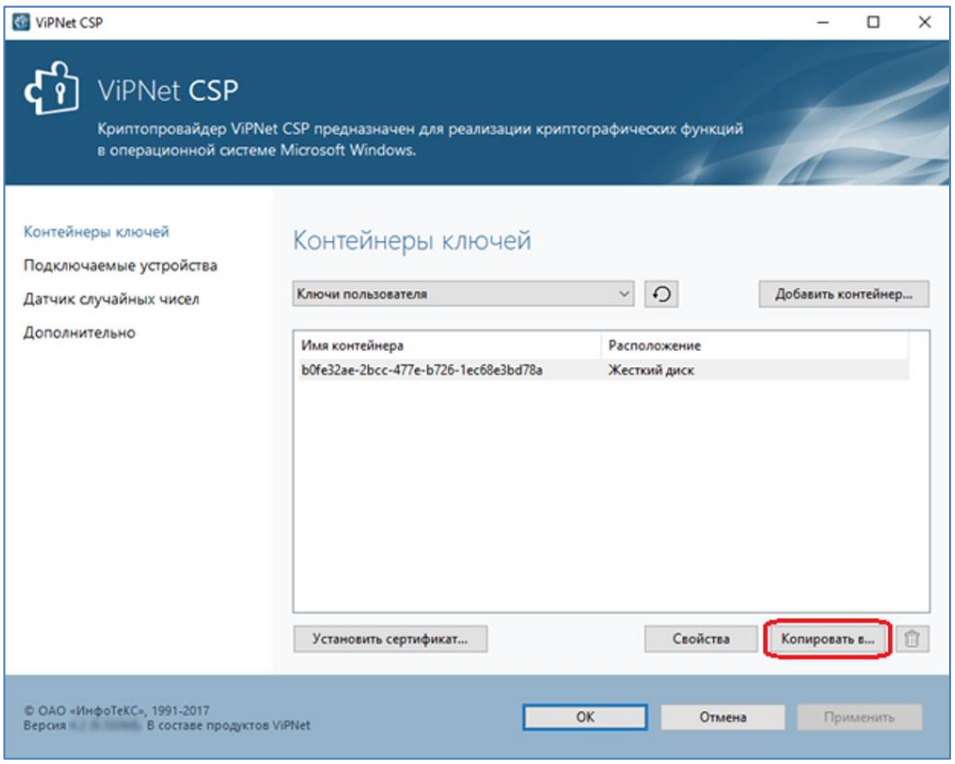

Рисунок 29

- ✓ Укажите новое место хранения ключа - устройство JaCarta LT/Rutoken и введите пин-код[6] (Рисунок 30).

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

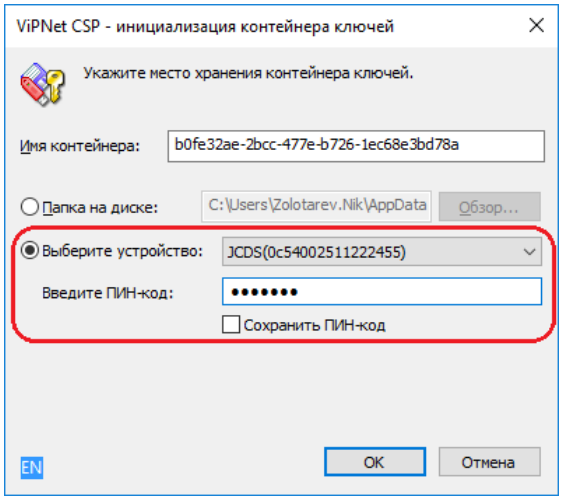

Рисунок 30

✓ При необходимости введите пароль к контейнеру закрытого ключа, **заданный вами при генерации ключа** (Рисунок 31).

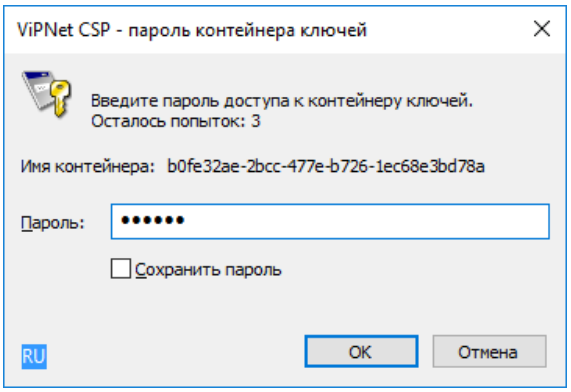

Рисунок 31

Убедитесь, что в списке контейнеров отображаются контейнеры на локальном диске компьютера и на ключевом носителе. Если вы хотите оставить контейнер только на ключевом носителе, то удалите контейнер, находящийся на локальном диске компьютера.

Затем **обязательно установите сертификат в системное хранилище**, процесс установки личного сертификата приведен в **разделе А, пункты 5-8**.

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

По умолчания PIN-код пользователя на устройство Рутокен: **12345678**

V.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[7], либо по ссылкам:
  - http://reestr-pki.ru/cdp/guc_gost12.crt[8]
  - http://reestr-pki.ru/cdp/guc2021.crt[9]
  - http://reestr-pki.ru/cdp/guc2022.crt[10]
- ✓ Откройте загруженный сертификат и нажмите ***«Установить сертификат»*** (Рисунок 32).
- ✓ 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 33, позиция А), нажать ***«Обзор»*** (Рисунок 33, позиция Б), выбрать ***«Доверенные корневые центры сертификации»*** (Рисунок 33, позиция В), нажать ***«Далее»*** (Рисунок 33, позиция Г).

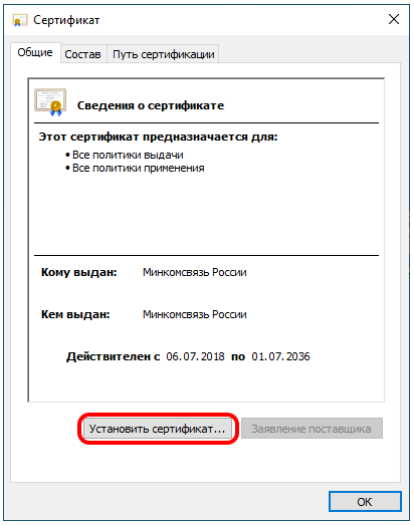

Рисунок 32

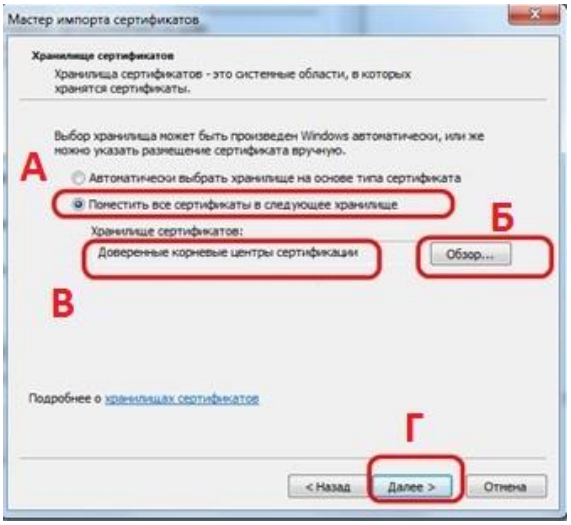

Рисунок 33

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

---

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

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

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

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

VI. 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 34).
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 35).
7. Нажмите кнопку ***«Выполнить»***. При успешной установке нового PIN-кода пользователя появится соответствующее сообщение (Рисунок 36).

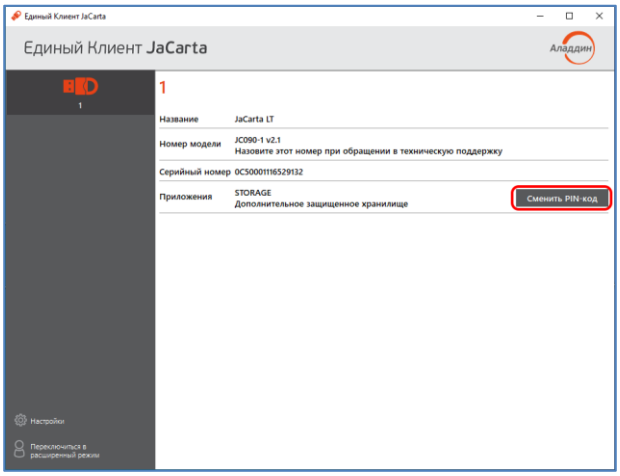

Рисунок 34

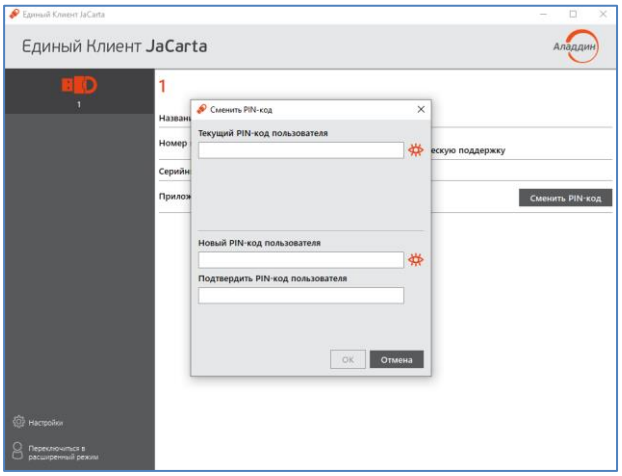

Рисунок 35

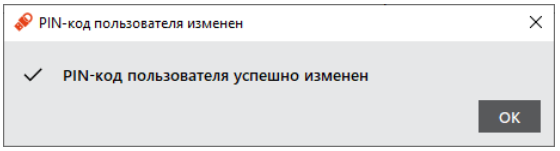

Рисунок 36

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.

VII. 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 37).

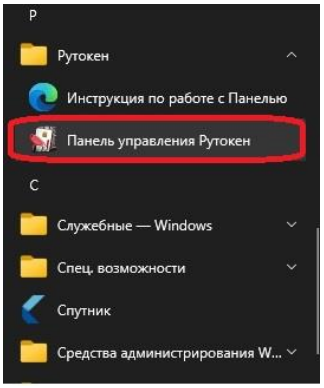

Рисунок 37

3. Если к компьютеру подсоединено несколько электронных ключей, во вкладке ***«Администрирование»*** в выпадающем списке ***«Подключенные Рутокены»*** выберите нужный электронный ключ (Рисунок 38).

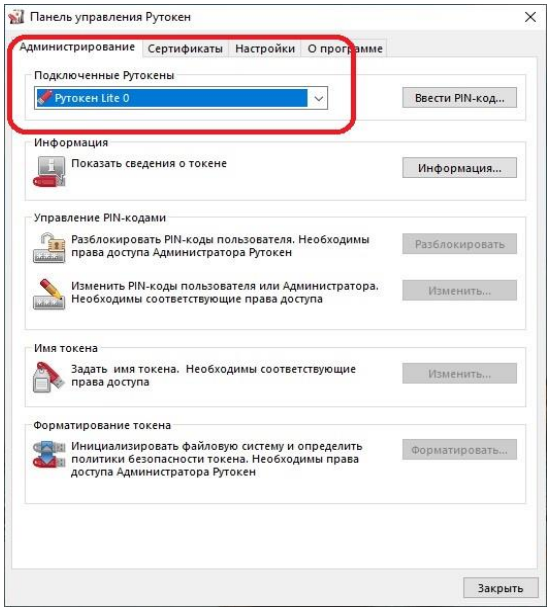

Рисунок 38

4. Во вкладке ***«Администрирование»*** нажмите кнопку ***«Ввести PIN-код…»***. Для смены Pin-кода пользователя необходимо ввести PIN-код пользователя[11] (Рисунок 39).

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

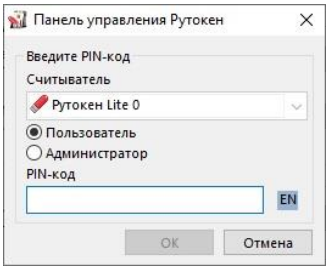

Рисунок 39

8. В полях ***«Введите новый PIN-код»*** и ***«Подтвердите новый PIN-код»*** введите новый PIN-код пользователя (Рисунок 40).

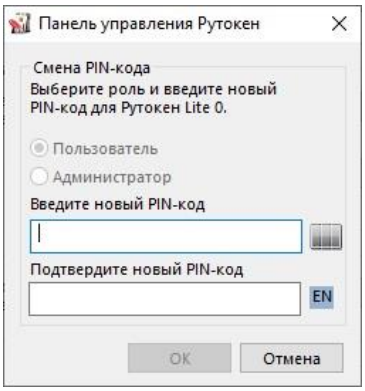

Рисунок 40

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.***
