

**Инструкция по переносу контейнера закрытого ключа на носители
(JaCarta LT и флеш-накопитель) и на ПК с использованием СКЗИ
ViPNet CSP**

Листов 11

Оглавление

I.	ВВЕДЕНИЕ	3
II.	ДОБАВЛЕНИЕ КОНТЕЙНЕРОВ ЗАКРЫТЫХ КЛЮЧЕЙ С CD ДИСКА ИЛИ USB-ФЛЭШ-НАКОПИТЕЛЯ.....	4
III.	ПЕРЕНОС КОНТЕЙНЕРА ЗАКРЫТОГО КЛЮЧА НА ФЛЭШ-НАКОПИТЕЛЬ.....	5
IV.	ДОБАВЛЕНИЕ СЕРТИФИКАТА В КОНТЕЙНЕР КЛЮЧЕЙ В VIPNET CSP	7
V.	УСТАНОВКА ДРАЙВЕРА И ПЕРЕНОС КОНТЕЙНЕРА НА JACARTA LT	9

I. Введение

- ✓ Документ предназначен для пользователей, осуществляющих перенос контейнера закрытого ключа на ключевой носитель JaCarta LT, либо на флэш-накопитель с использованием средства криптографической защиты информации (СКЗИ) ViPNet CSP, а также установку сертификата в контейнер. Выберите необходимый раздел инструкции в зависимости от действия, которое хотите выполнить.
- ✓ Данный документ предполагает, что перед переносом контейнеров закрытых ключей на вашем автоматизированном рабочем месте (АРМ) уже установлено, зарегистрировано и настроено средство криптографической защиты информации (СКЗИ) ViPNet CSP.
- ✓ С 1 января 2022 года получить квалифицированный сертификат электронной подписи руководителя юридического лица или индивидуального предпринимателя можно только в государственных удостоверяющих центрах (ФНС, Федеральное казначейство, Центральный банк РФ)¹. В УЦ ИИТ можно получить сертификат на физическое лицо.
- ✓ Необходимо обращать особое внимание на примечания помеченные знаком ➡.

➡ **Внимание!** Вид окон может отличаться в зависимости от используемой операционной системы. В примерах использовалась операционная система Windows 10.

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

¹ Согласно изменениям в 63-ФЗ «Об электронной подписи».

II. Добавление контейнеров закрытых ключей с CD диска или usb-флэш-накопителя

Полученные контейнеры с диска желательно перенести в папку хранения контейнеров ключей по умолчанию: **C:\Users\%username%\AppData\Local\Infotecs\Containers** (скопируйте путь до папки в поисковую строку) (Рисунок 1).

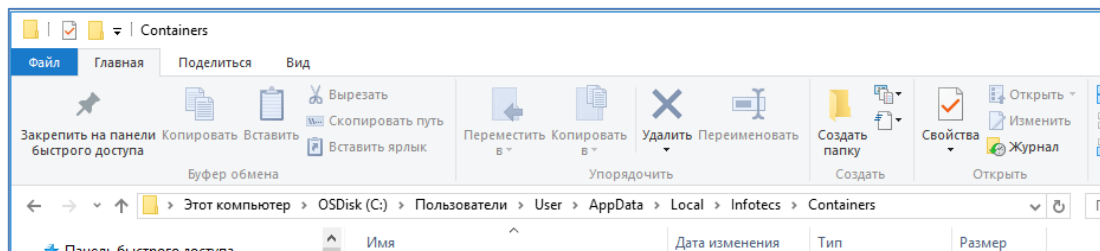



Рисунок 1

Откройте программу VipNet CSP и нажмите на кнопку . В списке контейнеров ключей отобразится ваш контейнер (если контейнер расположен не в папке по умолчанию, добавьте его через кнопку «Добавить контейнер...», указав до него путь). В списке контейнеров ключей найдите актуальный контейнер и дважды кликните по нему левой кнопкой мыши, затем нажмите кнопки «Открыть» => «Установить сертификат...» => «Далее» => «Далее» => «Готово» (Рисунок 2).

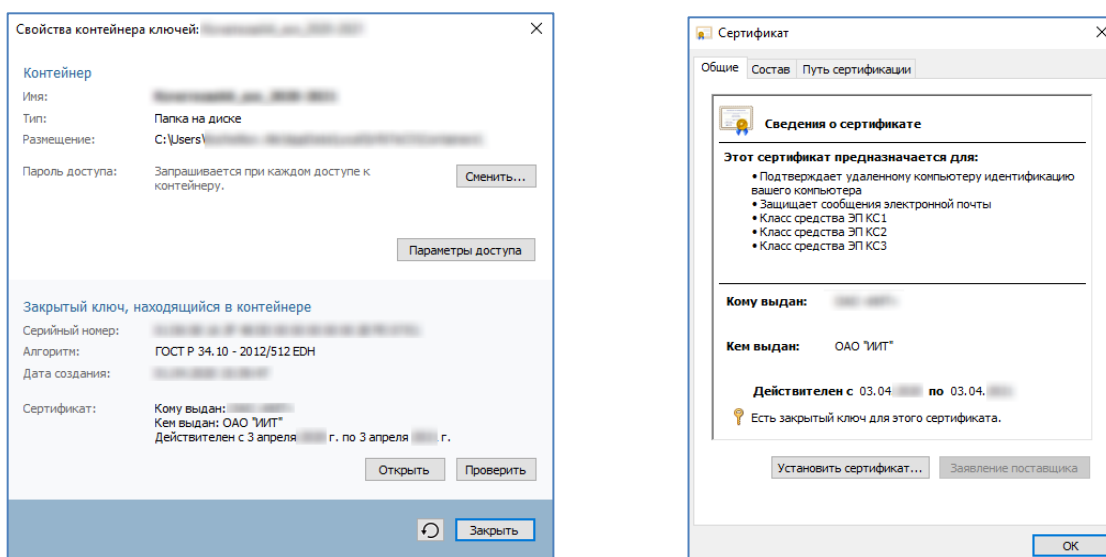


Рисунок 2

III. Перенос контейнера закрытого ключа на флэш-накопитель

► **Возможен перенос контейнера ключей на флэш-накопитель, например, для переноса и последующей настройки на другом рабочем месте. По умолчанию контейнер ключей сохраняется на жестком диске в папке:**

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

Если при генерации ключей Вы указывали другой путь для сохранения контейнера ключей и его нет в списке, необходимо перенести папки, которую вы указывали ранее, либо воспользоваться стандартным способом, описанным ниже.

1. Создайте на носителе каталог Infotecs\Containers
2. Запустите криптопровайдер **ViPNet CSP** с ярлыка на рабочем столе или из кнопки меню **«Пуск»** -> **«Все приложения»** -> **«ViPNet»** -> **«ViPNet CSP»**.
3. Перейдите в раздел **«Контейнеры ключей»**. Выберите сформированный ранее контейнер закрытого ключа и нажмите кнопку **«Копировать в...»** (Рисунок 3).

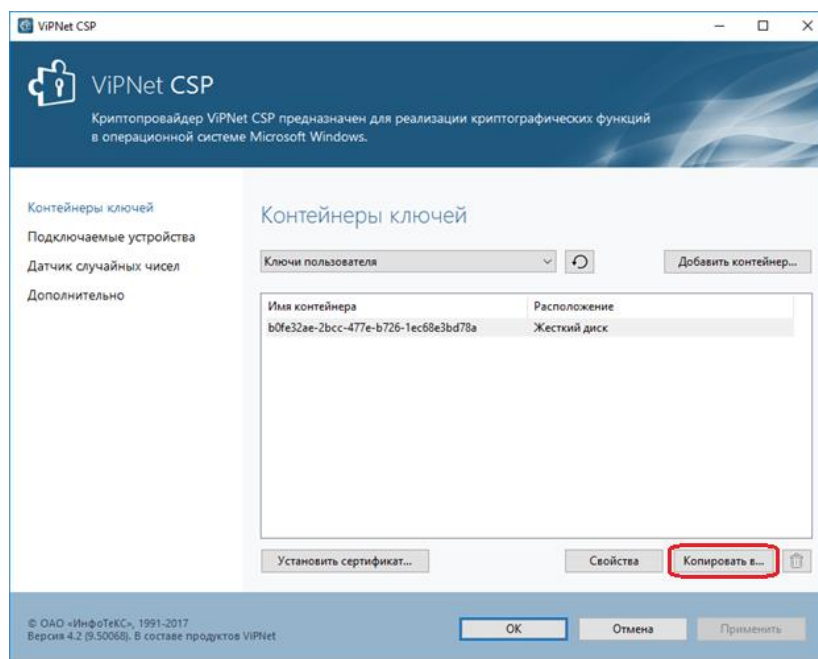


Рисунок 3

4. Необходимо нажать кнопку **«Обзор...»** и выбрать папку по пути **infotecs/containers** на флэш-накопителе и нажать **ОК** (Рисунок 4).

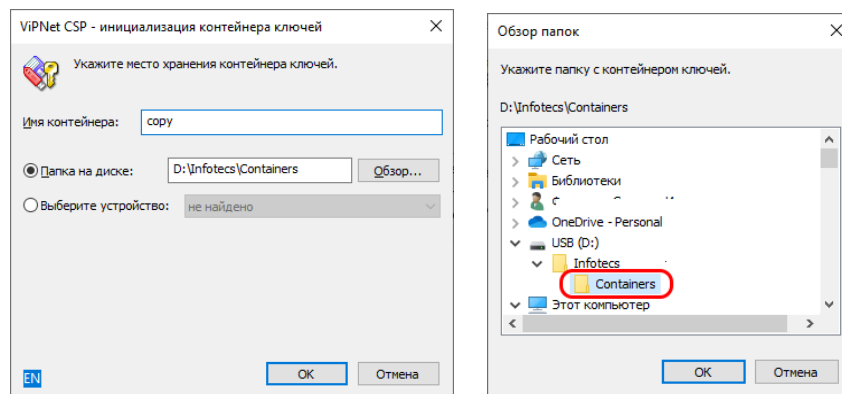


Рисунок 4

5. При необходимости введите пароль² к контейнеру закрытого ключа, заданный Вами при генерации ключа (Рисунок 5).

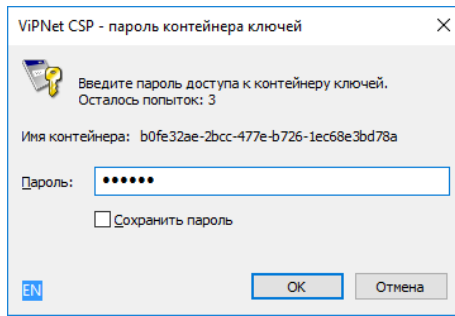


Рисунок 5

6. После этого необходимо задать пароль для нового контейнера на флэш-накопителе (Рисунок 6).

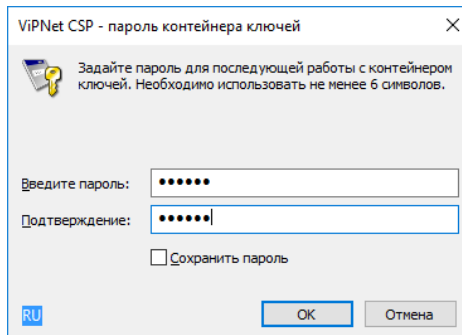


Рисунок 6

Внимание! Обязательно запомните введенный пароль. В случае если пароль будет утерян (забыт), доступ к ключевой информации будет невозможен.

7. В результате на флэш-накопителе в папке **InfoTeCS**, в подкаталоге **Containers** будет находиться контейнер ключа (Рисунок 7).

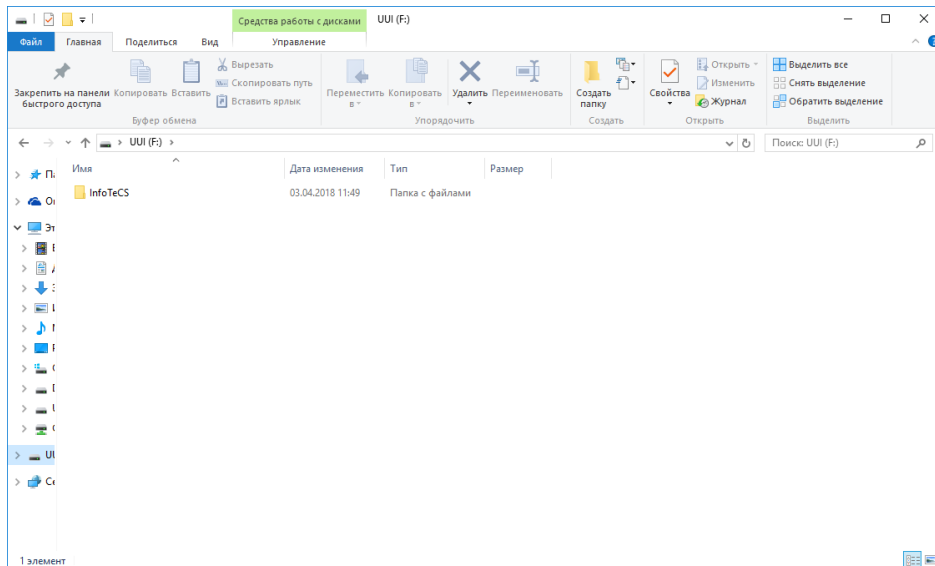


Рисунок 7

² По умолчанию пароль на контейнер: **123456**

IV. Добавление сертификата в контейнер ключей в ViPNet CSP

После того как УЦ ИИТ предоставил изготовленный сертификат в формате *«имя файла».cer*, вам необходимо добавить полученный сертификат в контейнер ключей.

Для добавления сертификата в контейнер ключей:

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»** нажмите кнопку **«Установить сертификат...»** (Рисунок 8).

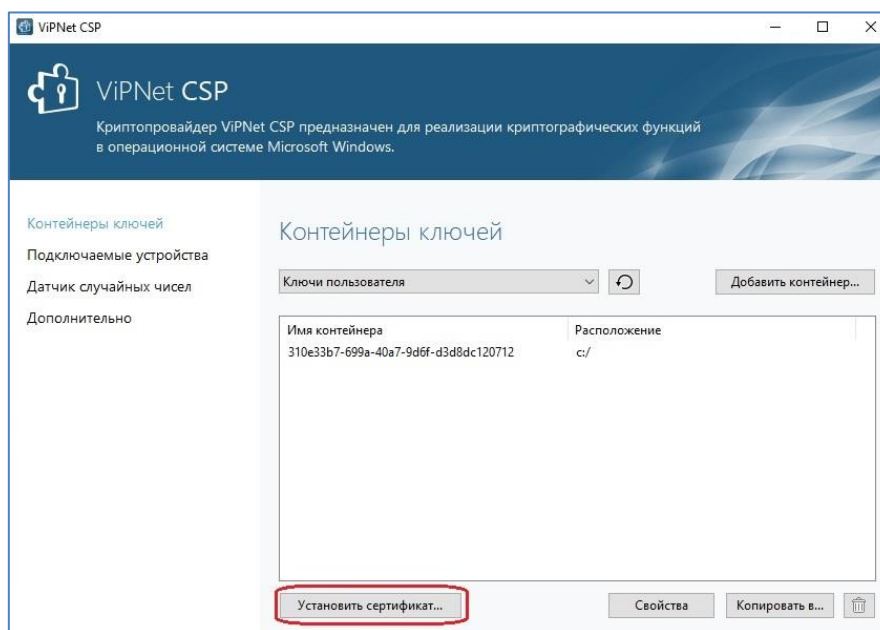


Рисунок 8

➔ По умолчанию контейнер ключей сохраняется на жестком диске в папке:

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

Если при генерации ключей Вы указывали другой путь для сохранения контейнера и его нет в списке – нажмите «Добавить» и укажите место хранения вашего контейнера.

3. Укажите файл с сертификатом, полученным в УЦ ИИТ в формате *«имя файла».cer* и нажмите кнопку **«Открыть»** (Рисунок 9).

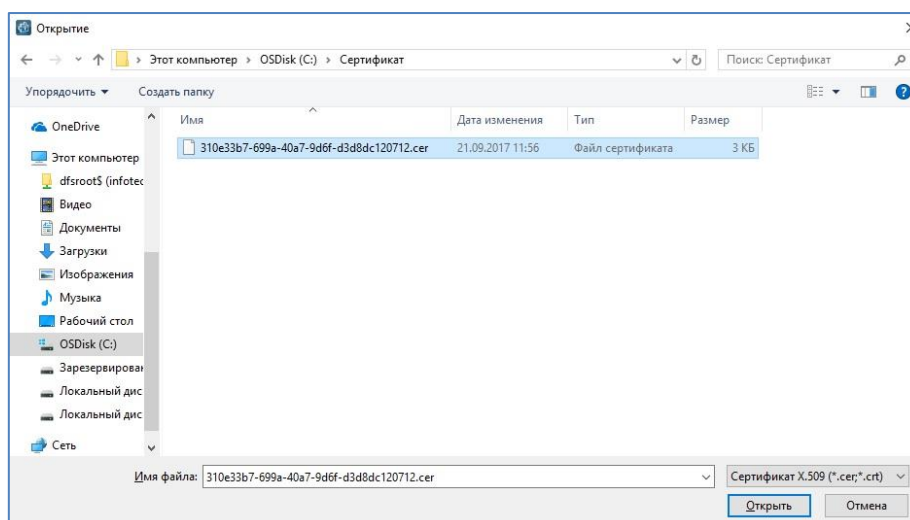


Рисунок 9

4. Нажмите кнопку **«Далее»** и затем выберите установить в хранилище сертификатов **текущего пользователя** (Рисунок 10).

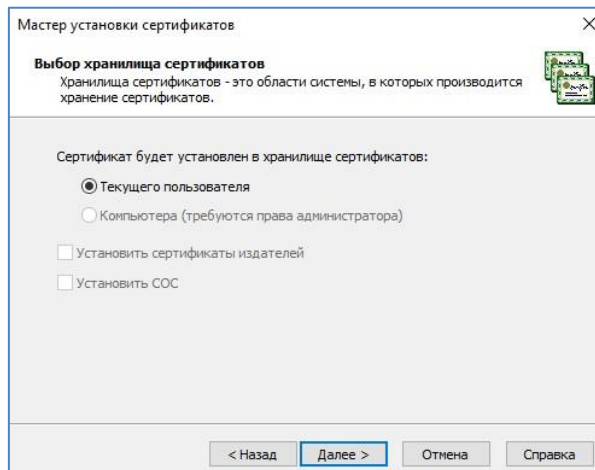


Рисунок 10

5. Откроется мастер установки сертификатов. Укажите **«Найти контейнер с закрытым ключом»** (Рисунок 11).

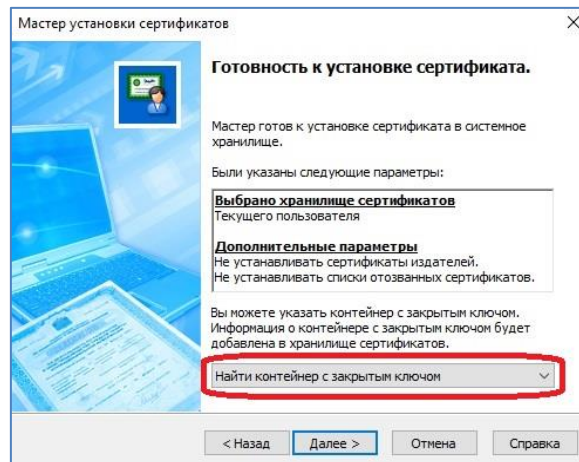


Рисунок 11

6. ViPNet CSP автоматически определит расположение контейнера на ПК, затем нажмите **«OK»** и **«Готово»** (Рисунок 12).

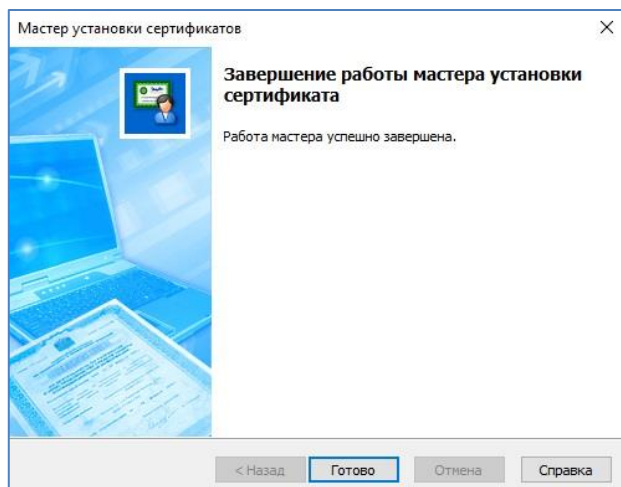
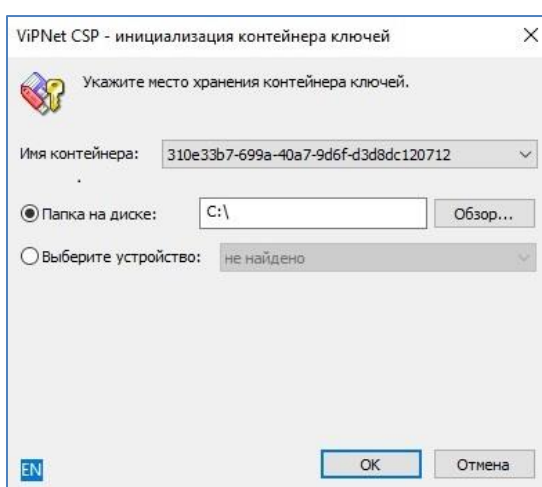


Рисунок 12

V. Установка драйвера и перенос контейнера на JaCarta LT³

► **Внимание!** Данный пункт инструкции следует использовать, **ТОЛЬКО** если Вам выдали ключевой носитель JaCarta LT.

1. Для корректной работы ключевого носителя JaCarta LT 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 13).

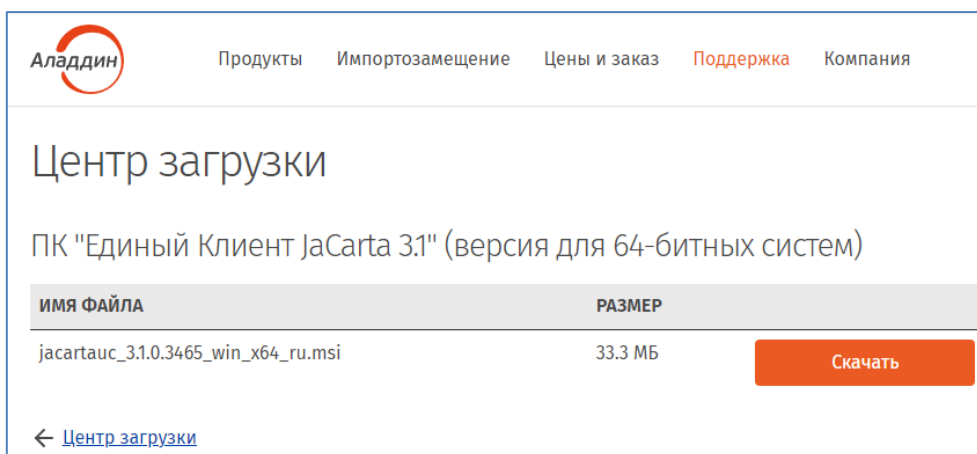


Рисунок 13

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-порте Вашего компьютера

4. Запустите криптопровайдер **VipNet CSP** с ярлыка на рабочем столе или из кнопки меню **«Пуск»** -> **«Все приложения»** -> **«VipNet»** -> **«VipNet CSP»**.
5. Перейдите в раздел **«Контейнеры ключей»**. Выберите сформированный ранее контейнер закрытого ключа и нажмите кнопку **«Копировать в...»** (Рисунок 14).

³ 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 Алaddin РД **«eToken PKI Client»** по ссылкам:

- [для 64-разрядной системы;](#)
- [для 32-разрядной системы.](#)

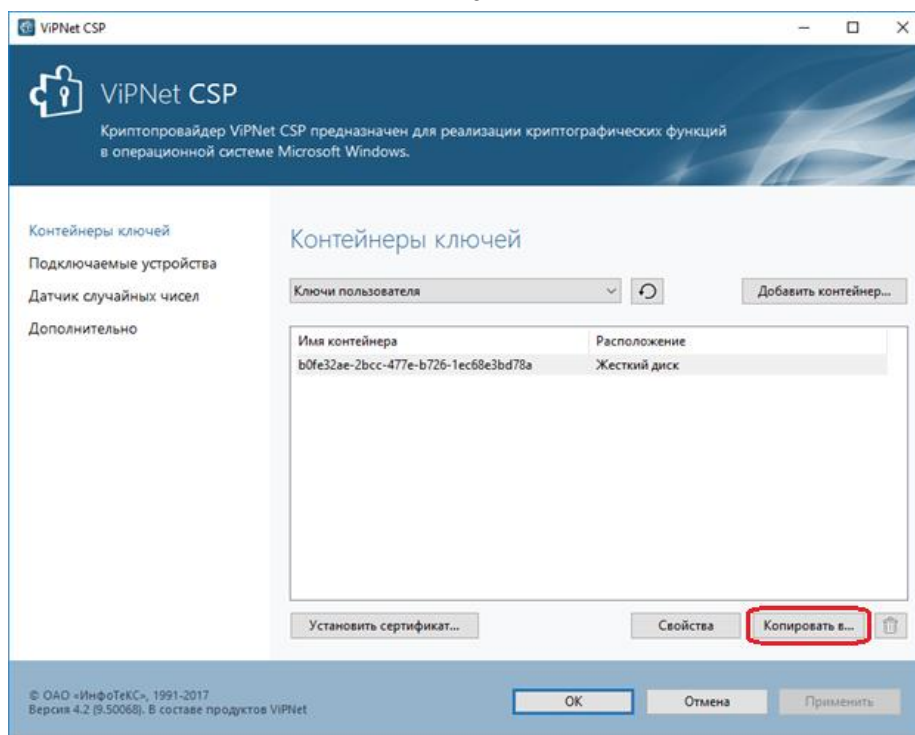


Рисунок 14

6. Укажите новое место хранения ключа - устройство JaCarta LT и введите пин-код⁴ (Рисунок 15).

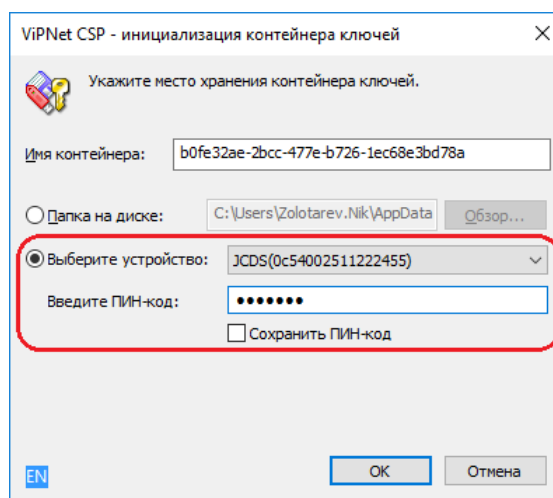


Рисунок 15

При необходимости введите пароль к контейнеру закрытого ключа⁵, заданный вами при генерации ключа (Рисунок 16).

⁴ 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**

⁵ Пароль от контейнера по умолчанию: **123456**

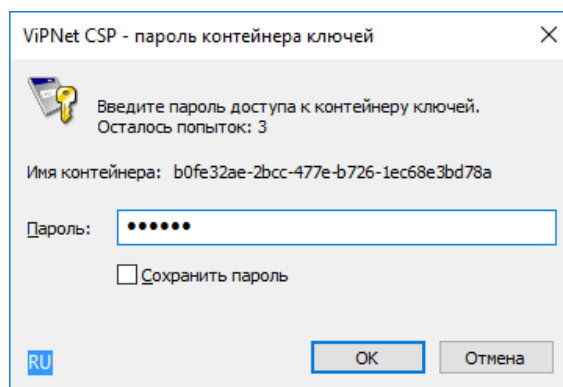


Рисунок 16

7. Убедитесь, что в списке контейнеров отображаются контейнеры на локальном диске компьютера и на ключевом носителе JaCarta LT. Если вы хотите оставить контейнер только на ключевом носителе, то удалите контейнер, находящийся на локальном диске компьютера⁶.



На этом процедура по добавлению сертификата в контейнер, а также по общему переносу контейнера на съемный носитель завершена.

⁶ Внимание! Контейнер удаляется безвозвратно.