

**Перенос и настройка программы TrustTax
(СКЗИ ViPNet CSP)**

Листов 15

Оглавление

I. Введение.....	3
II. Копирование данных со старого рабочего места	4
III. Получение и установка ViPNet CSP.....	6
IV. Настройка ViPNet CSP для работы с электронной цифровой подписью	9
А. Установка личного сертификата с ключевого носителя.....	9
Б. Установка личного сертификата с дискового носителя/флеш карты.....	13
V. Установка и настройка TrustTax.....	14
А. Загрузка и установка TrustTax	14
Б. Настройка подключения.	14
В. Выбор сертификата для входа в TrustTax	15

I. Введение

- ✓ Документ предназначен для пользователей, осуществляющих самостоятельный перенос данных программы TrustTax на другой компьютер и её настройку.
- ✓ **С 1 января 2022 года получить квалифицированный сертификат электронной подписи руководителя юридического лица или индивидуального предпринимателя можно только в государственных удостоверяющих центрах (ФНС России, Федерального казначейства, Центрального банка РФ)¹. В УЦ ИИТ можно получить сертификат на физическое лицо, сотрудника ЮЛ или доверенное лицо ИП.**
- ✓ В удостоверяющем центре «Инфотекс Интернет Траст» (далее — УЦ ИИТ) срок действия ключей и сертификата ЭП установлен равным 1 году.
- ✓ При необходимости произвести плановую (скорое истечение срока действия ЭП) или внеплановую (изменение учетных данных владельца ЭП, потеря доступа к ключевому носителю, потеря ключевого носителя и т.д.) смену ЭП необходимо повторно посетить УЦ ИИТ по согласованию с менеджером «Инфотекс Интернет Траст».
- ✓ Для правильной работы СКЗИ ViPNet CSP необходимо выполнить все пункты данного руководства в указанной последовательности.
- ✓ Для аутентификации пользователя и заверения документов электронной подписью в программе TrustTax используются ключи электронной подписи, работу с которыми обеспечивает криптопровайдер. Гарантирована поддержка работы с криптопровайдером ViPNet CSP (версия 4.4 или выше).
- ✓ **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 Согласно изменениям в № 63-ФЗ «Об электронной подписи».

II. Копирование данных со старого рабочего места

➔ **Внимание!** Если контейнер сохраняли на ключевом носителе, то достаточно вставить его на другом компьютере в USB-порт компьютера. Перейдите к следующему пункту инструкции.

Перед установкой программного обеспечения на новом рабочем месте необходимо скопировать контейнер закрытого ключа.

Запустите криптопровайдер ViPNet CSP из панели **Пуск** -> **Все программы** -> **ViPNet** -> **ViPNet CSP** либо ярлык на рабочем столе **ViPNet CSP**.

Перейдите на вкладку «**Контейнеры ключей**», найдите нужный контейнер и посмотрите путь к контейнеру. Нажмите на кнопку «**Копировать в...**» (Рисунок 1).

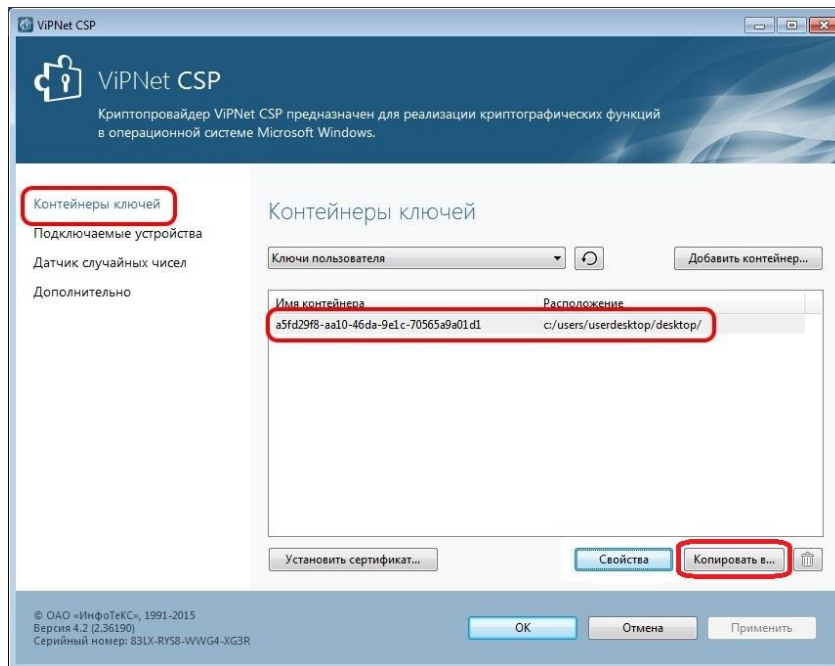


Рисунок 1

Укажите имя для контейнера, затем нажмите на кнопку «**Обзор**» и выберите путь, по которому необходимо скопировать контейнер, например, на ваш защищенный носитель (Рисунок 2).

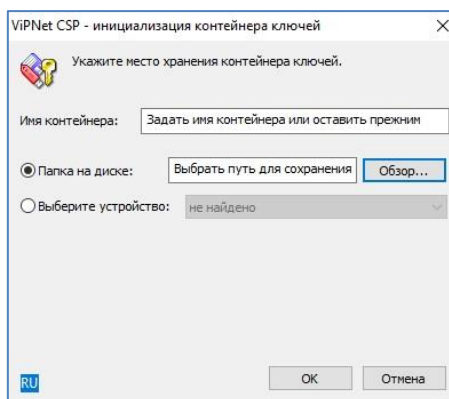


Рисунок 2

Если контейнер ключа был сохранен по стандартному пути, то можете скопировать всё содержимое каталога с контейнером(-ами) закрытого ключа на флеш-карту в отдельный каталог.

► **Внимание!** По умолчанию сгенерированные контейнеры ключей сохраняются на жёстком диске в папке:

`C:\Users\[имя учетной записи]\AppData\Local\InfoTeCS\Containers\`

► Если при генерации ключей вы указывали другой путь для сохранения контейнера, то копируйте соответствующую папку.

Для того чтобы отображались все папки по путям, приведённым в сноске, необходимо включить отображение скрытых папок, для этого нажмите **Пуск -> Панель управления -> Свойства папки/Параметры проводника -> Вид -> Показать скрытые файлы, папки и диски** (Рисунок 3).

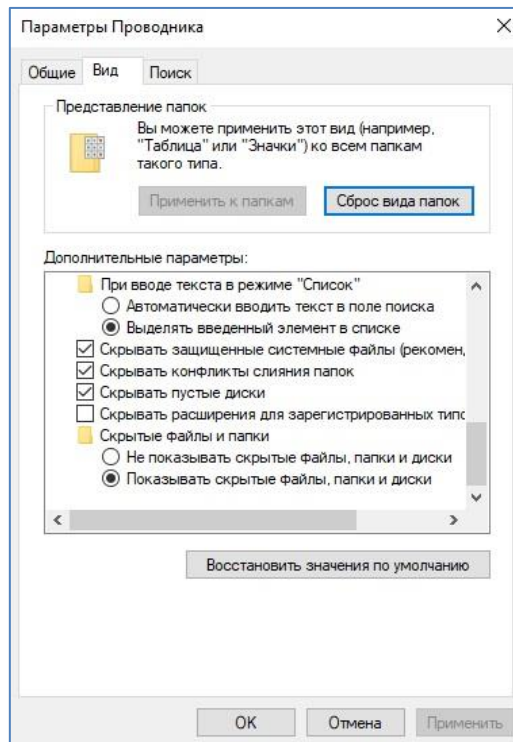


Рисунок 3

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

III. Получение и установка ViPNet CSP

1. Для получения ViPNet CSP необходимо перейти на официальный сайт разработчика:
 - a. Если вы работаете на операционных системах **Windows 10/11²**, вам необходимо перейти по адресу https://infotecs.ru/downloads/latest/?product=vipnet_csp&type=beta для загрузки и регистрации ViPNet CSP поддерживаемой данными ОС.
 - b. Если вы работаете на операционной системе **Windows: 8.1/Server 2008/Server 2008 R2/Server 2012/Server 2012R2/2016/2019**, вам необходимо перейти по адресу https://infotecs.ru/downloads/latest/?product=vipnet_csp&type=full для загрузки и регистрации ViPNet CSP поддерживаемой данными ОС.
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 своём 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».
6. Выберите пункт «*Зарегистрировать ViPNet CSP*» и нажмите кнопку «*Далее*» (Рисунок 4)³.

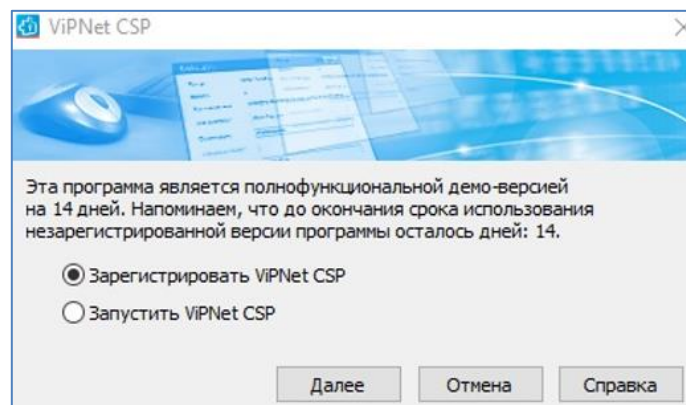


Рисунок 4

- ✓ Выберите пункт «*Запрос на регистрацию (получить код регистрации)*» и нажмите кнопку «*Далее*» (Рисунок 5).

² **Внимание! Обновление Microsoft Windows 10 KB5009543 (версии 20H2, 21H1, 21H2) от 11.01.2022 г. несовместимо с ViPNet CSP 4.4.2 и может привести к нарушению работы операционной системы. [Рекомендуем использовать бета-версию для данных сборок Windows 10.](#)**

³ Без регистрации ViPNet CSP будет функционировать в течение 14 дней и не сможет обеспечить юридической значимости электронной подписи.

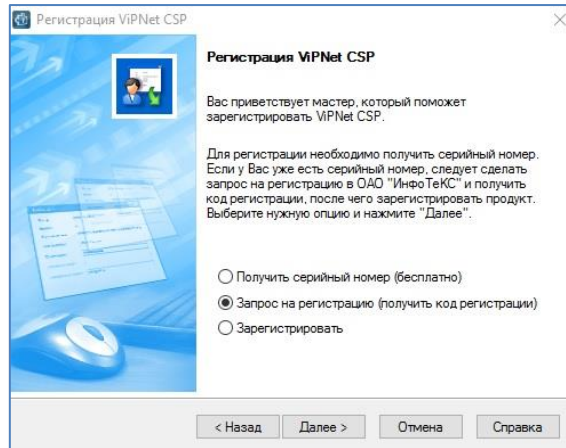


Рисунок 5

- ✓ Выберите пункт «*Через Интернет (online)*» и нажмите кнопку «*Далее*» (Рисунок 6).

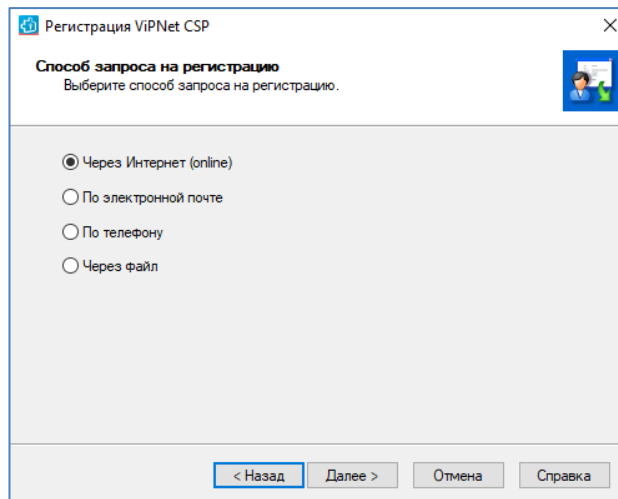


Рисунок 6

- ✓ Заполните форму своими регистрационными данными, включая «*Серийный номер*» ViPNet CSP, полученный при регистрации на Ваш E-mail и нажмите кнопку «*Далее*» (Рисунок 7).

Рисунок 7

- ✓ После завершения процесса регистрации нажмите кнопку «Готово» (Рисунок 8).

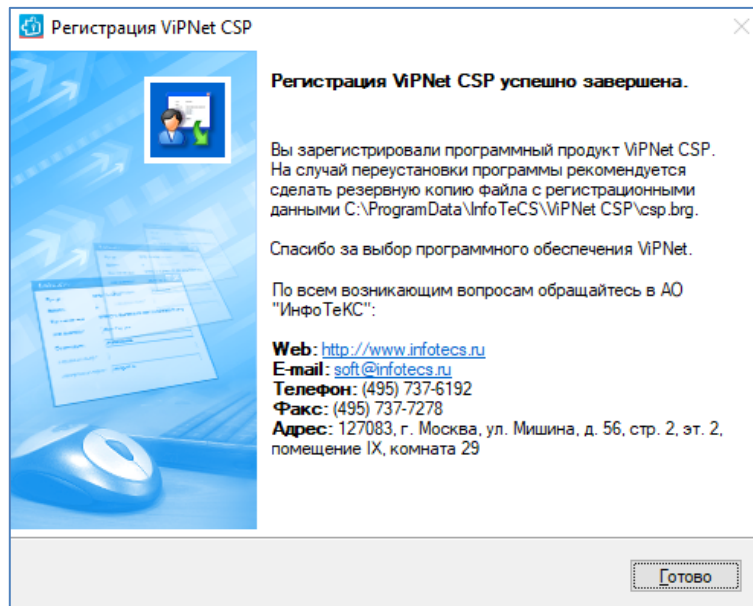


Рисунок 8

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

IV. Настройка ViPNet CSP для работы с электронной цифровой подписью

Установку личного сертификата возможно выполнить двумя способами:

- А. Установка личного сертификата с ключевого носителя.
- Б. Установка личного сертификата с дискового носителя/флеш карты.

Опишем каждый из них подробнее, необходимо выполнить подходящий.

А. Установка личного сертификата с ключевого носителя

➔ **Внимание! Данный пункт инструкции следует использовать, ТОЛЬКО если контейнер ключей находится на защищённом ключевом носителе (токене). Если у вас ключевой дистрибутив на диске/флеш-карте, то вам следует перейти к пункту Б текущей инструкции.**

1. Для корректной работы ключевого носителя под управлением операционной системы Microsoft Windows необходимо установить программное обеспечение, позволяющее выполнять базовые операции. Установку программного обеспечения необходимо выполнить в зависимости от типа используемого ключевого носителя:

- для устройств JaCarta LT, JaCarta-2 SE, JaCarta-2 ГОСТ, JaCarta-2 PKI/ГОСТ, JaCarta PKI произведите установку [программного обеспечения для ключевых носителей JaCarta](#);
- для устройств Рутокен S, Рутокен Lite, Рутокен ЭЦП 2.0, произведите установку [программного обеспечения для ключевых носителей Рутокен](#);
- для устройств ESMART Token, ESMART Token ГОСТ, произведите установку [программного обеспечения для ключевых носителей ESMART Token](#).

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

➔ **Внимание! Убедитесь, что ключевой носитель находится в USB-порте вашего компьютера**

4. Запустите ViPNet CSP и убедитесь, что в разделе «Дополнительно» включена опция «Поддержка работы ViPNet CSP через Microsoft CryptoAPI» (Рисунок 9).

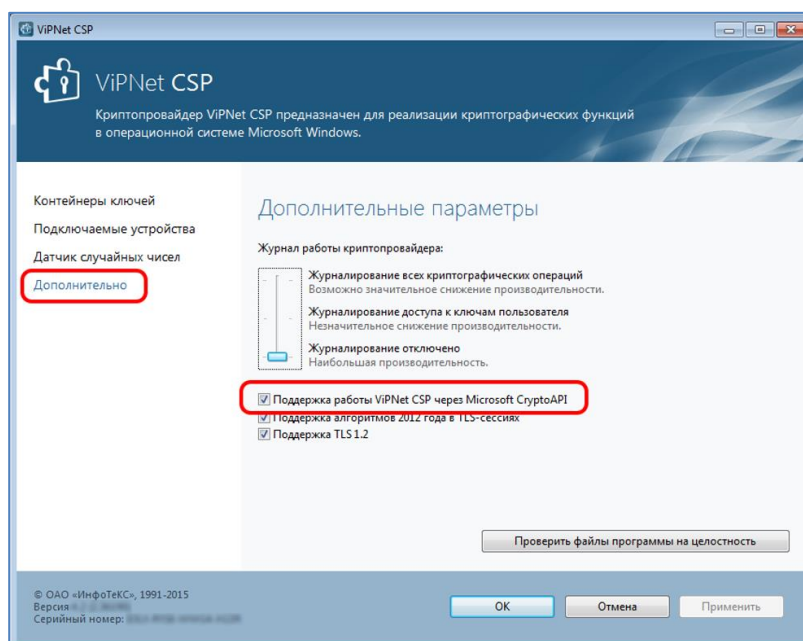


Рисунок 9

5. Перейдите в раздел «Контейнеры ключей». В выпадающем списке выберите подключенный защищенный носитель⁴, а в разделе «Имя контейнера» — контейнер ключей «XXX-XXXX-XXXX-XXXX-XXXX». Затем нажмите кнопку «Свойства» (Рисунок 10).

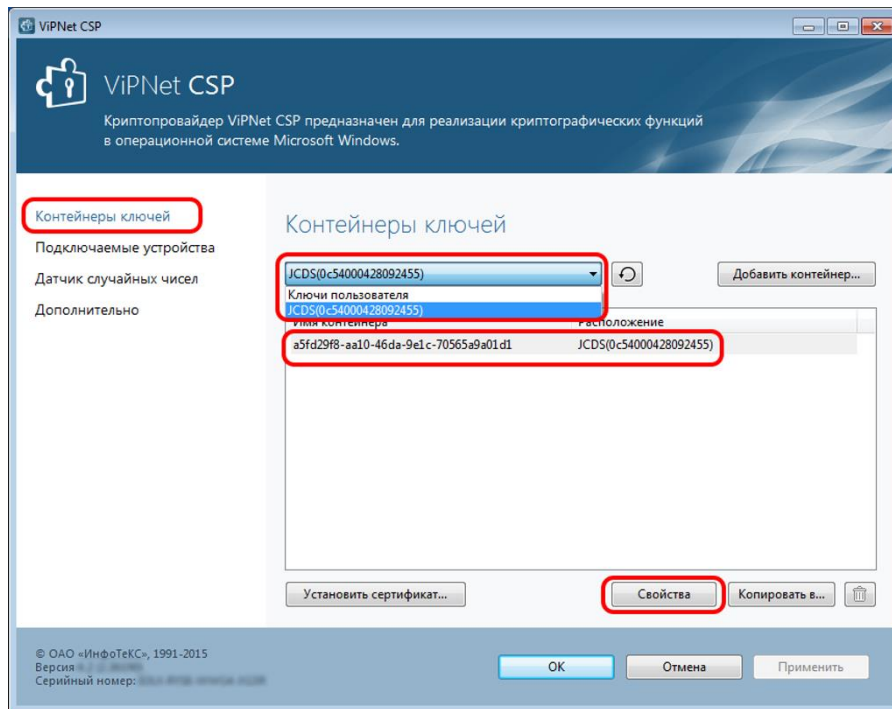


Рисунок 10

6. В окне свойств контейнера ключей (Рисунок 11) в разделе «Закрытый ключ, находящийся в контейнере» нажмите кнопку «Открыть».

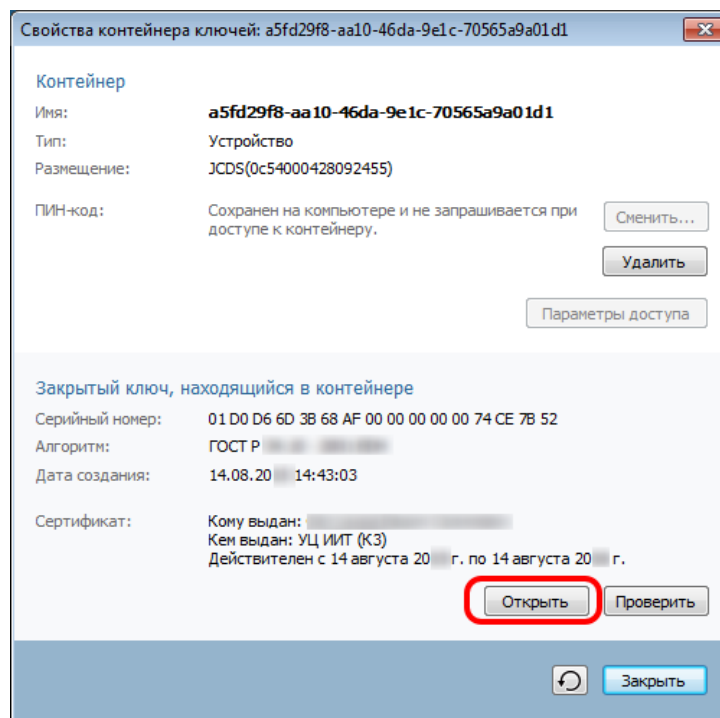


Рисунок 11

⁴ В примерах использовался носитель JaCarta LT.

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

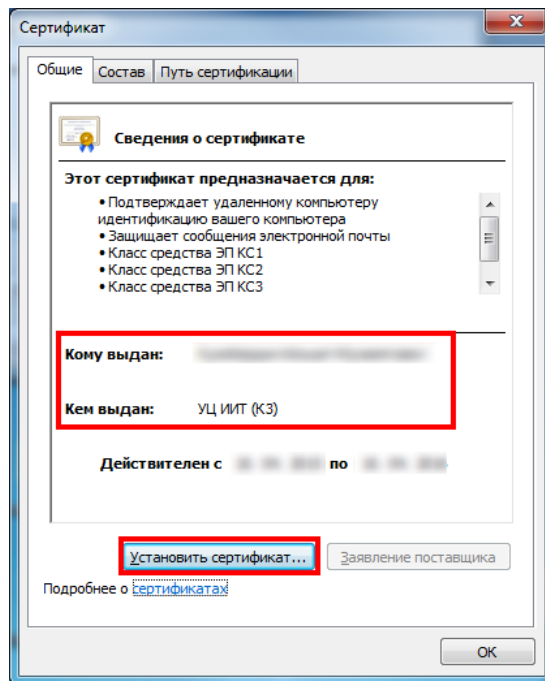


Рисунок 12

8. Далее следуйте указаниям Мастера установки сертификатов. В ходе установки сертификата обращайте внимание на выбранные опции (Рисунок 13).

9. В появившемся на очередном шаге окне (Рисунок 14) введите PIN-код к устройству⁵.

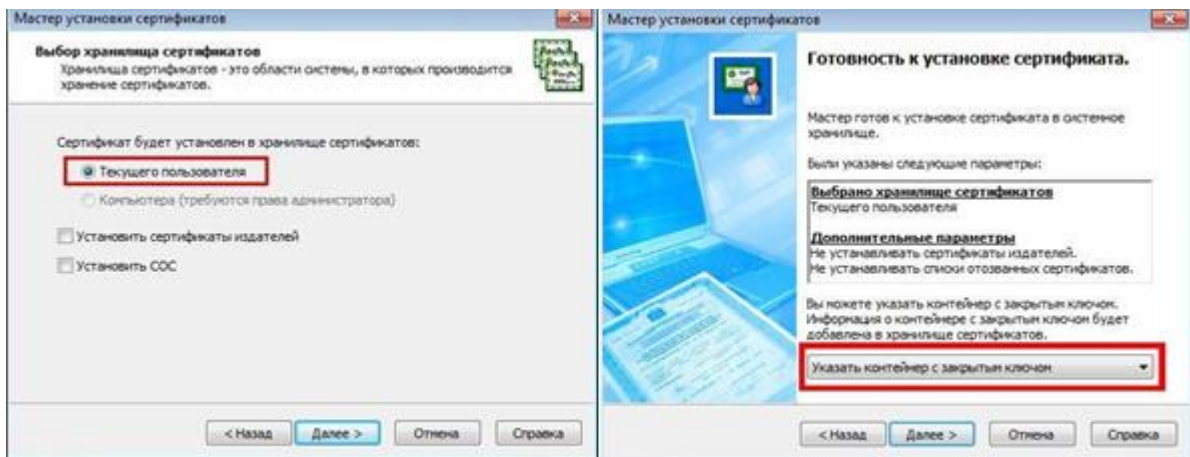


Рисунок 13

⁵ 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**.

на устройство Рутокен: **12345678**

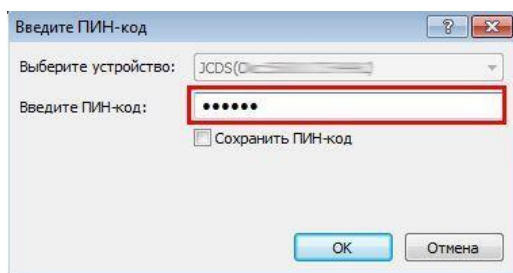


Рисунок 14

10. На этом работа Мастера установки сертификата завершается (Рисунок 15) нажмите кнопку «Готово» и переходите к следующему пункту инструкции.

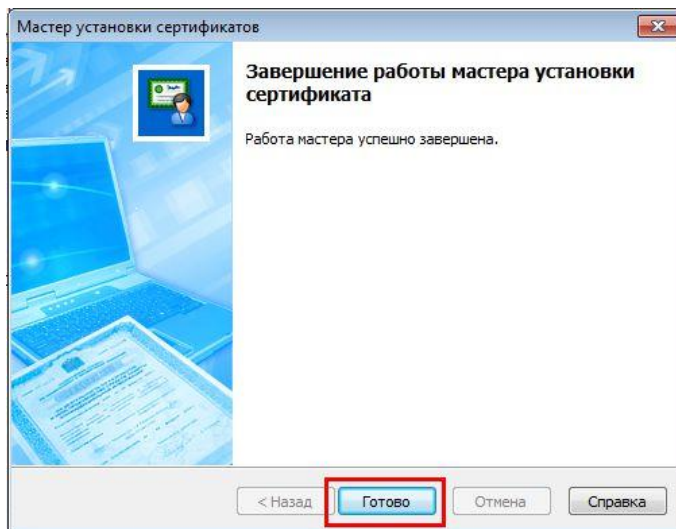


Рисунок 15

Б. Установка личного сертификата с дискового носителя/флеш-карты

➔ **Внимание!** Данный пункт инструкции следует использовать, **ТОЛЬКО** если ключевой дистрибутив сохранён на диске или флэш карте.

1. Скопируйте ключевой контейнер (папку с компакт-диска) в любое место жёсткого диска компьютера.

➔ **Внимание!** Настоятельно рекомендуем сохранить выданный вам компакт-диск или отдельно сохранить записанные на диске файлы. Утеря файлов с учётными данными ведёт к внеплановой смене электронной подписи, что в свою очередь является платной услугой с обязательным личным посещением УЦ ИИТ.

Запустите ViPNet CSP и перейдите в раздел «Контейнеры ключей» (Рисунок 16).

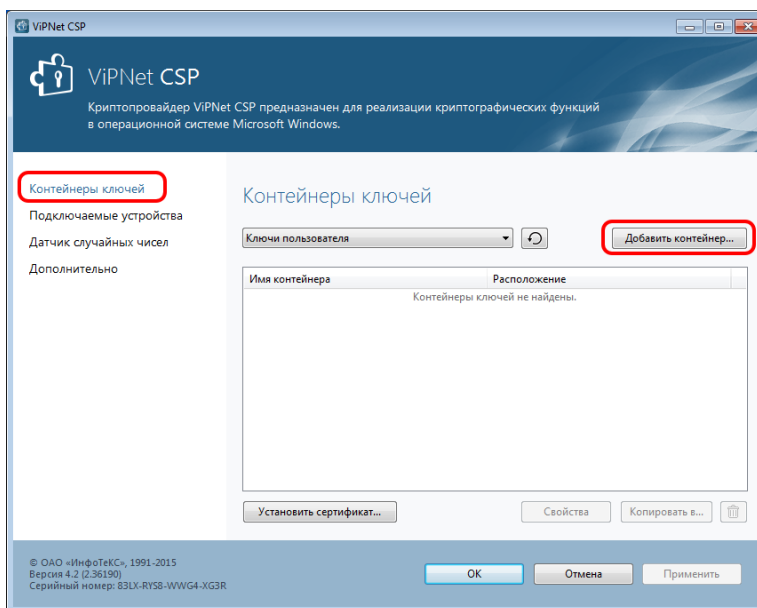


Рисунок 16

2. Нажмите кнопку «Добавить контейнер» (Рисунок 16), укажите местоположение ключей, нажав на кнопку «Обзор», выберите «Имя контейнера» вида «XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX» (единственный файл в выпадающем списке без расширения) и нажмите кнопку «OK» (Рисунок 17).

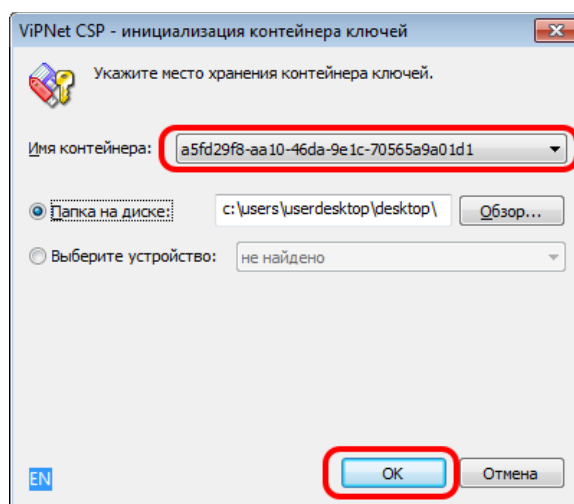


Рисунок 17

3. ViPNet CSP выдаст уведомление «*Контейнер успешно добавлен*» и задаст вопрос об установке найденных в контейнере сертификатов в системное хранилище. Нажмите кнопку «*Да*» и перейдите к следующему пункту инструкции (Рисунок 18).

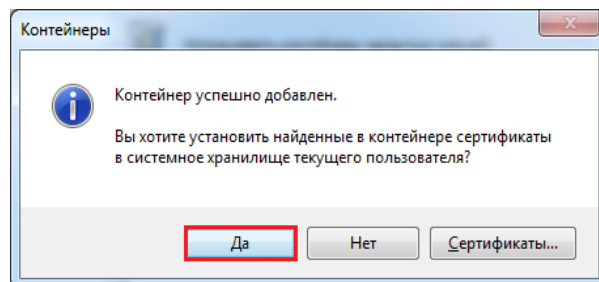


Рисунок 18

V. Установка и настройка TrustTax

Установка и настройка TrustTax делится на 3 этапа:

- A. Загрузка и установка TrustTax.
- Б. Настройка подключения.
- В. Выбор сертификата для входа в TrustTax.

A. Загрузка и установка TrustTax:

1. Для получения TrustTax необходимо загрузить установочный файл по данной [ссылке](#).
2. Запустите загруженный файл.
3. Следуйте указаниям «*Мастера Установки TrustTax*». Везде нажимайте **Да/Далее**.
4. По завершении установки нажмите кнопку «*Готово*».

Б. Настройка подключения.

Запустите через программу через TrustTax через **Пуск -> Все программы -> ИTrust -> TrustTax** либо щелкните на **ярлык** на рабочем столе. Откроется окно входа в программу.

Для доступа к серверу оператора электронного документооборота в окне входа в программу кликните ссылку «*Настройка подключения*» и настройте параметры подключения (Рисунок 19).

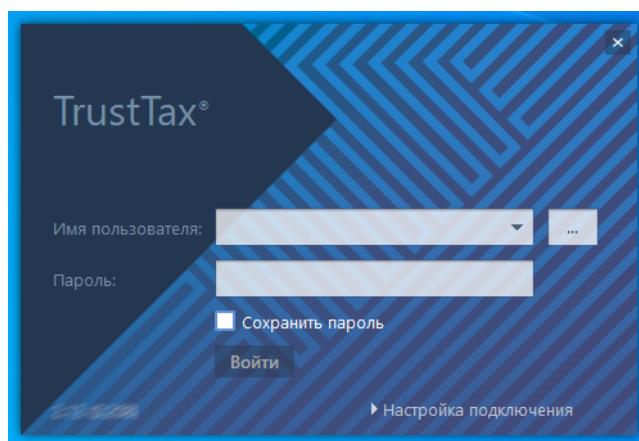


Рисунок 19

Настройки подключения будут установлены автоматически. Если в вашей организации используется прокси-сервер, установите флажок «*Прокси-сервер*» и в соответствующих полях введите адрес и номер порта прокси-сервера. При необходимости укажите параметры аутентификации пользователя (Рисунок 20).

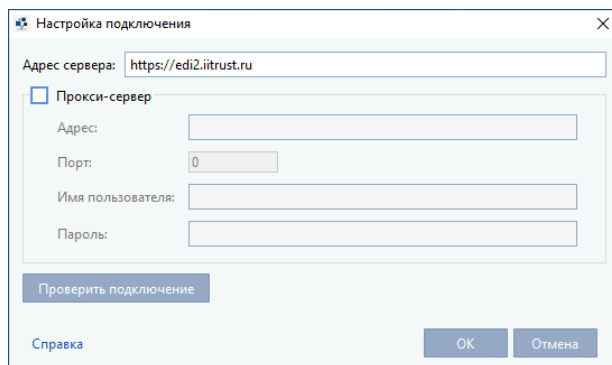


Рисунок 20

➔ **Внимание!** Если настроить автоматически подключение не удалось, обратитесь к системному администратору.

В. Выбор сертификата для входа в TrustTax

Зайдите в «Управление учетными записями», нажав на «...» (Рисунок 21).

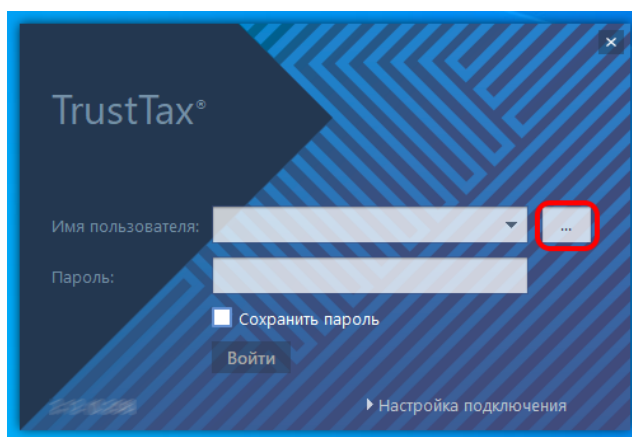


Рисунок 21

Выберите нужный сертификат (Рисунок 22).

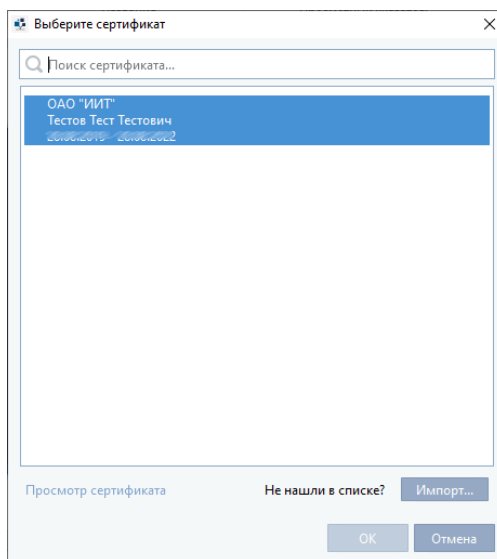


Рисунок 22

Чтобы вернуться к окну входа в программу, нажмите кнопку «OK».