Инструкция по настройке автоматизированного рабочего места для работы с электронной подписью (УЦ ФНС России, УЦ ФК, КриптоПро CSP)

Листов 10

Инфотекс Интернет Траст
2024 г.

Оглавление

I. Введение 3

II. Получение и установка КриптоПро CSP.....4

III. Установка программного обеспечения для ключевых носителей 5

А. Установка программного обеспечения для ключевых носителей JaCarta 5

Б. Установка программного обеспечения для ключевых носителей Рутокен..... 6

В. Установка программного обеспечения для ключевых носителей ESMART Token 6

IV. Установка личного сертификата 7

V. Построение цепочки сертификатов до головного удостоверяющего центра Министерства цифрового развития, связи и массовых коммуникаций.....9

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), выпущенной в УЦ ФНС России, УЦ ФК (Федеральное Казначейство).

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.

✓ 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 обратиться в ФНС/Федеральное Казначейство.

✓ 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 PKI Client, выберите соответствующую инструкцию из представленных в разделе «Пользовательская документация».

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[2]. Запустите КриптоПро CSP. Откройте вкладку ***«Общие»*** и нажмите на кнопку ***«Ввод лицензии…»***. Затем заполните поля ***«Пользователь»***, ***«Организация»***, введите ***«Серийный номер»***[3] (серийный номер, полученный у организации-разработчика или организации, имеющей права на распространение продукта)[4] и нажмите кнопку ***«ОК»*** (Рисунок 1).

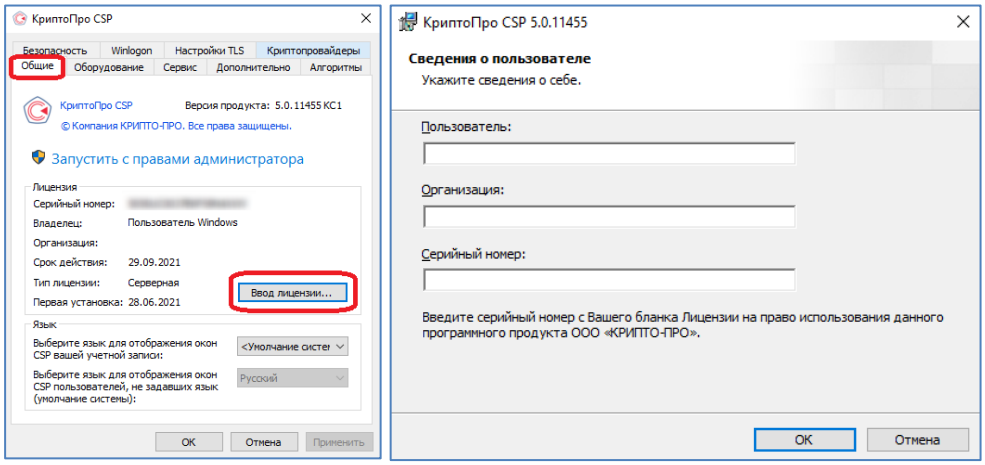

Рисунок 1

[2] С 12.04.2022г. по 20.03.2023г. УЦ ФНС в рамках Эксперимента по безвозмездному предоставлению пользователям Удостоверяющего центра ФНС России программного обеспечения для работы с электронной подписью осуществлял выдачу квалифицированных сертификатов со встроенной лицензией на КриптоПро CSP. Владельцу квалифицированного сертификата со встроенной ограниченной лицензией предоставляется право на использование КриптоПро CSP на условиях простой неисключительной лицензии без ввода серийного номера. Срок действия такой лицензии ограничивается сроком действия квалифицированного сертификата.

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

[4] 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;

В. Если ЭП выпущена на носителях ESMART Token, ESMART Token ГОСТ, произведите установку программного обеспечения для ключевых носителей ESMART Token

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).

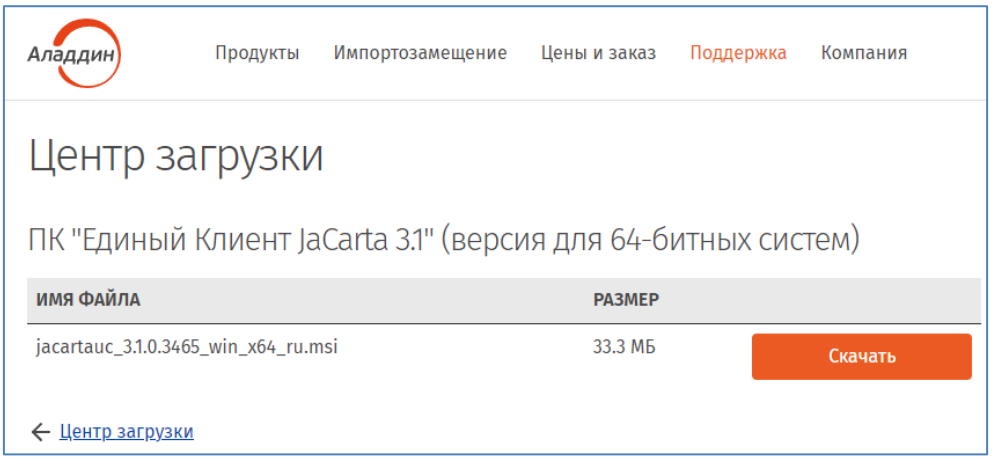

Рисунок 2

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, позиция А).

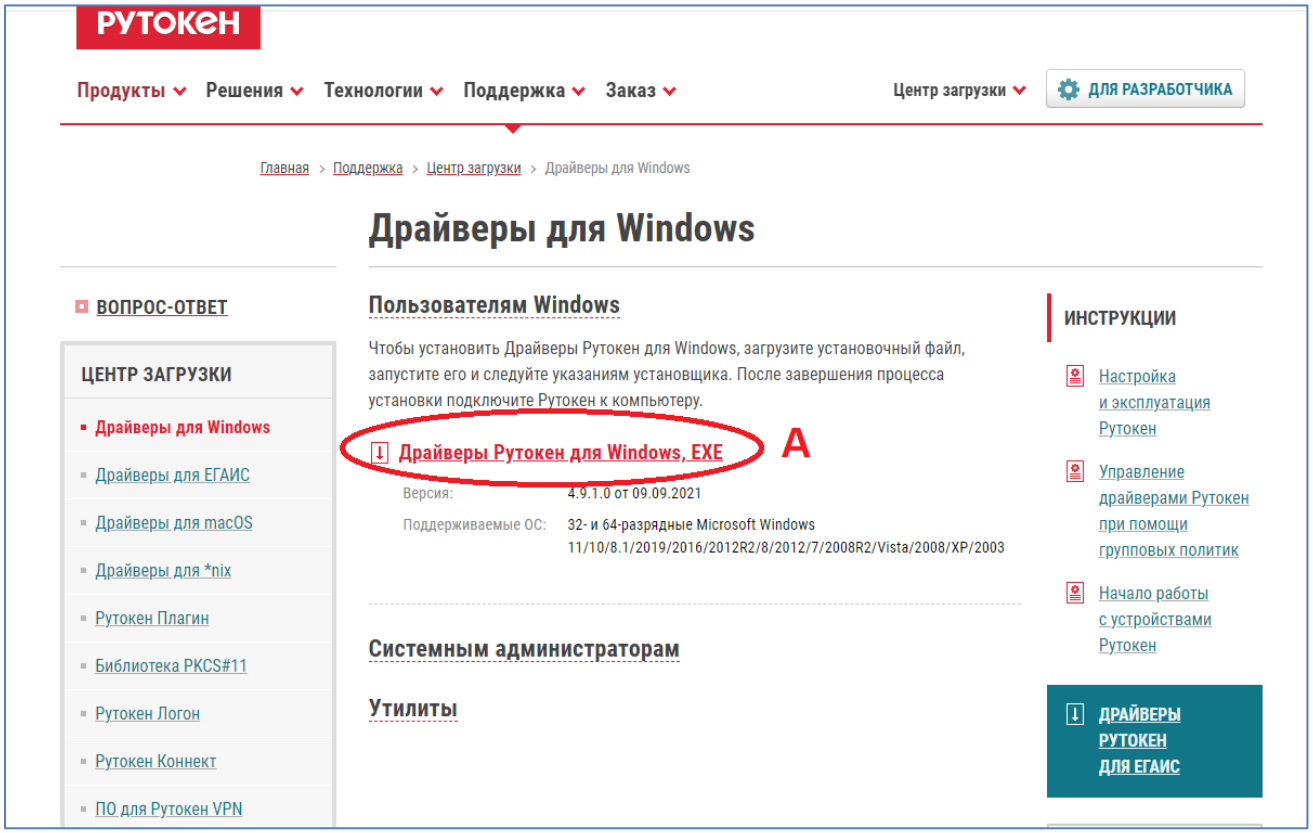

Рисунок 3

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

В. Установка программного обеспечения для ключевых носителей ESMART Token

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

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

Для получения программного обеспечения актуальной версии необходимо перейти на сайт разработчика ESMART в раздел «Загрузки» (Рисунок 4, позиция А) по данной ссылке:

https://esmart.ru/download/ Нажмите кнопку «ESMART PKI Client 4.X для Windows (рекомендуется)» (Рисунок 4, позиция Б).

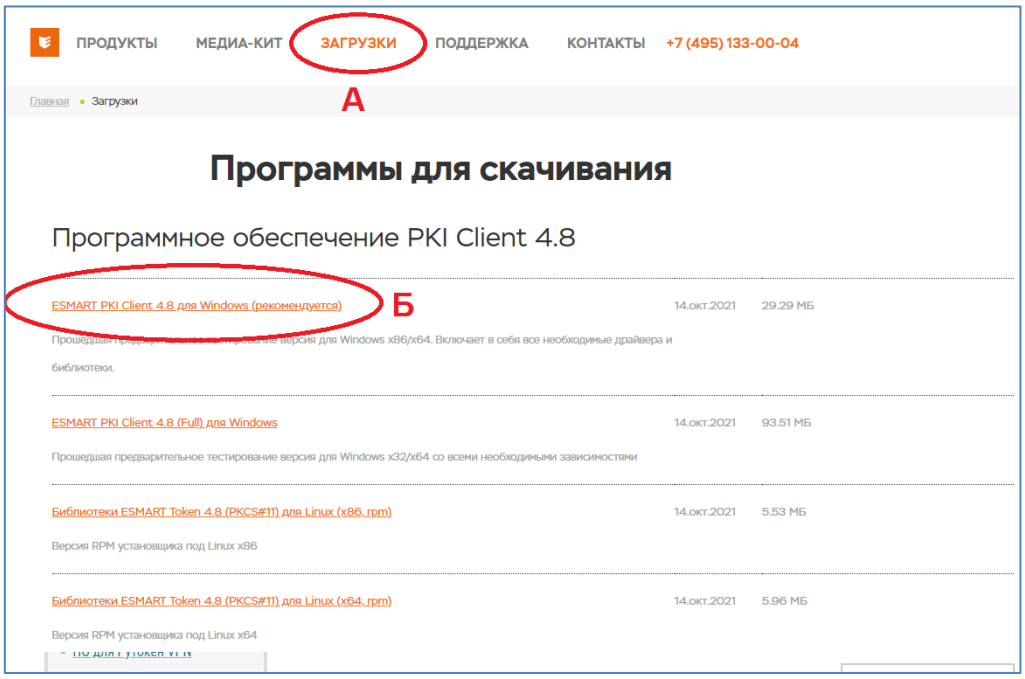

Рисунок 4

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

Внимание! Убедитесь, что ключевой носитель находится в USB-порте Вашего компьютера

1. Запустите приложение КриптоПро CSP, перейдите на вкладку ***«Сервис»*** и нажмите кнопку ***«Просмотреть сертификаты в контейнере»*** (Рисунок 5, позиция А).

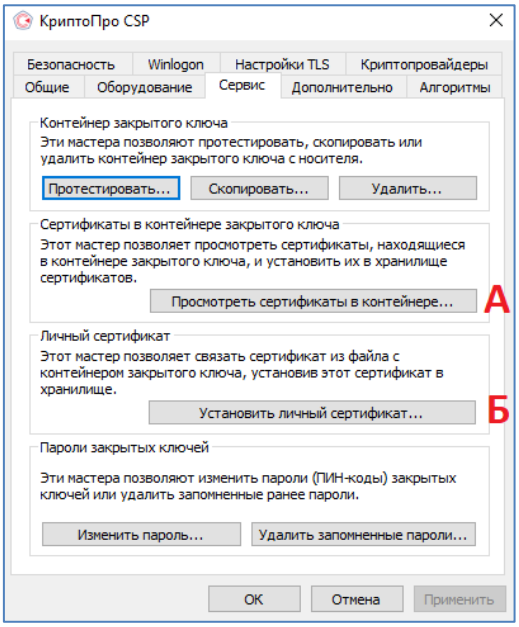

Рисунок 5

2. В открывшемся окне нажмите кнопку ***«Обзор»***, чтобы выбрать контейнер для просмотра. После выбора нужного контейнера нажмите кнопку ***«Ок»*** (Рисунок 6).

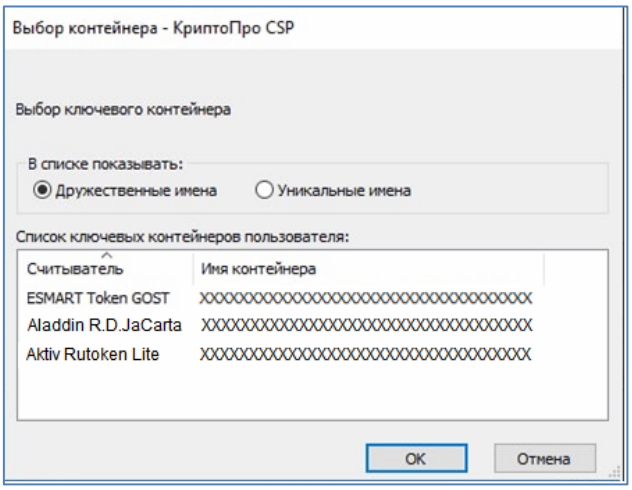

Рисунок 6

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 7).

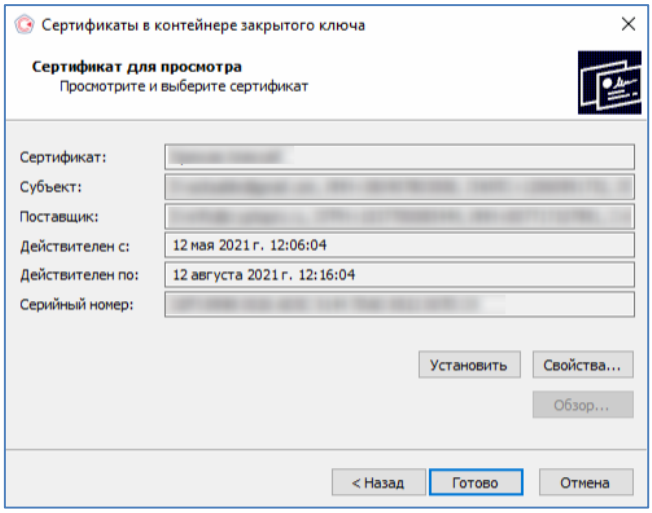

Рисунок 7

5. Если сертификат ранее уже был установлен, появится следующее информационное окно, нажмите кнопку ***«Да»*** (Рисунок8).

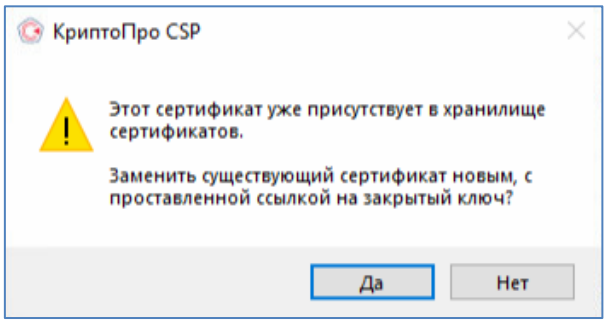

Рисунок 8

6. Если ранее сертификат не был установлен, то появится информационное окно, что сертификат был успешно установлен в хранилище «Личное» текущего пользователя (Рисунок 9).

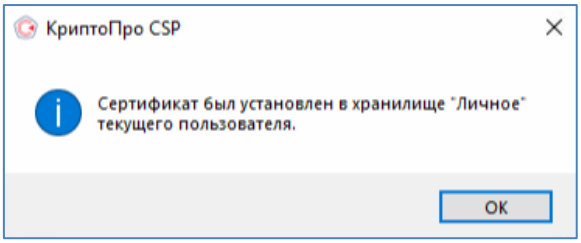

Рисунок 9

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

- ✓ Загрузить головные сертификаты удостоверяющего центра Министерства связи и массовых коммуникаций (далее по тексту - ***Головной УЦ***) можно самостоятельно с официального сайта[5], либо по ссылкам:
  - **http://reestr-pki.ru/cdp/guc_gost12.crt**[6]
  - **http://reestr-pki.ru/cdp/guc2021.crt**[7]
  - **http://reestr-pki.ru/cdp/guc2022.crt**[8]
- ✓ Откройте загруженный сертификат и нажмите ***«Установить сертификат»*** (Рисунок 10).
- ✓ 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 11, позиция А), нажать ***«Обзор»*** (Рисунок 11, позиция Б), выбрать ***«Доверенные корневые центры сертификации»*** (Рисунок 11, позиция В), нажать ***«Далее»*** (Рисунок 11, позиция Г).

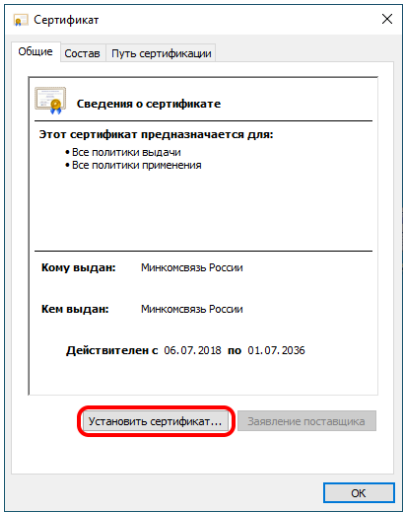

Рисунок 10

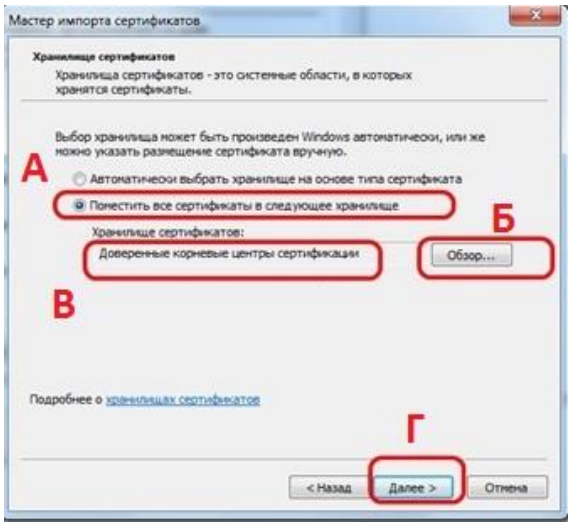

Рисунок 11

- ✓ Далее на все запросы мастера импорта сертификатов об установке сертификата

---

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

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

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

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

«Далее»/«Да»/«ОК» - соглашаетесь.

- ✓ Установите оба сертификата.
- ✓ Для сертификатов, выпущенных в УЦ ФНС после 05.05.2022 года, установите подчиненный сертификат УЦ ФНС России[9] в хранилище «Промежуточные центры сертификации».
- ✓ Для сертификатов, выпущенных в УЦ ФНС после 18.03.2023 года, установите подчиненный сертификат УЦ ФНС России[10] в хранилище «Промежуточные центры сертификации».
- ✓ Для сертификатов, выпущенных в УЦ ФНС после 11.11.2023 года, установите подчиненный сертификат УЦ ФНС России[11] в хранилище «Промежуточные центры сертификации».

[9] URL: https://e-trust.gosuslugi.ru/app/scc/portal/api/v1/portal/ca/download/021B60DA90EDB6DCE479528359057BE69D4D4884
[10] URL: https://e-trust.gosuslugi.ru/app/scc/portal/api/v1/portal/ca/download/08A4C134FFE120D8572DF0CB8465E6C3A77E7727
[11] URL: https://e-trust.gosuslugi.ru/app/scc/portal/api/v1/portal/ca/download/08A4C134FFE120D8572DF0CB8465E6C3A77E7727