Инструкция по использованию сертификатов, выпущенных государственными АУЦ, в рамках услуги «Информационная безопасность»

Листов 11

Инфотекс Интернет Траст
2024 г.

Оглавление

I. Введение

✓ Документ предназначен для пользователей услуги информационной безопасности Удостоверяющего Центра АО «Инфотекс Интернет Траст» (***УЦ ИИТ***), осуществляющих самостоятельную установку средства криптографической защиты информации (СКЗИ) КриптоПро CSP и настройку автоматизированного рабочего места для работы с квалифицированной электронной подписью аккредитованных удостоверяющих центров (КЭП АУЦ). С перечнем аккредитованных удостоверяющих центров можно ознакомиться на официальном сайте Минцифры в разделе «Аккредитация». В данном документе приведен пример использования сертификатов, полученных в Удостоверяющем центре Федеральной налоговой службы (***УЦ ФНС***), в Удостоверяющем центре Федерального Казначейства (***УЦ ФК***) и в Удостоверяющем центре Банка России (***УЦ Банка России***)[1], для передачи данных по защищённым каналам между подразделениями компании и контрагентами через ViPNet Client.

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 соответствующий АУЦ.

✓ Для правильной работы СКЗИ КриптоПро CSP необходимо выполнить все пункты данного руководства в указанной последовательности.

✓ ***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] Аккредитованные удостоверяющие центры в соответствии с ч. 1 ст. 15 Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи».

II. Получение и установка КриптоПро CSP

Внимание! В программе ViPNet CSP выберите пункт Дополнительно и убедитесь, что снят флажок Поддержка работы ViPNet CSP через Microsoft CryptoAPI.

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, 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»***[2] (серийный номер, полученный у организации-разработчика или организации, имеющей права на распространение продукта)[3] и нажмите кнопку ***«ОК»*** (Рисунок 1).

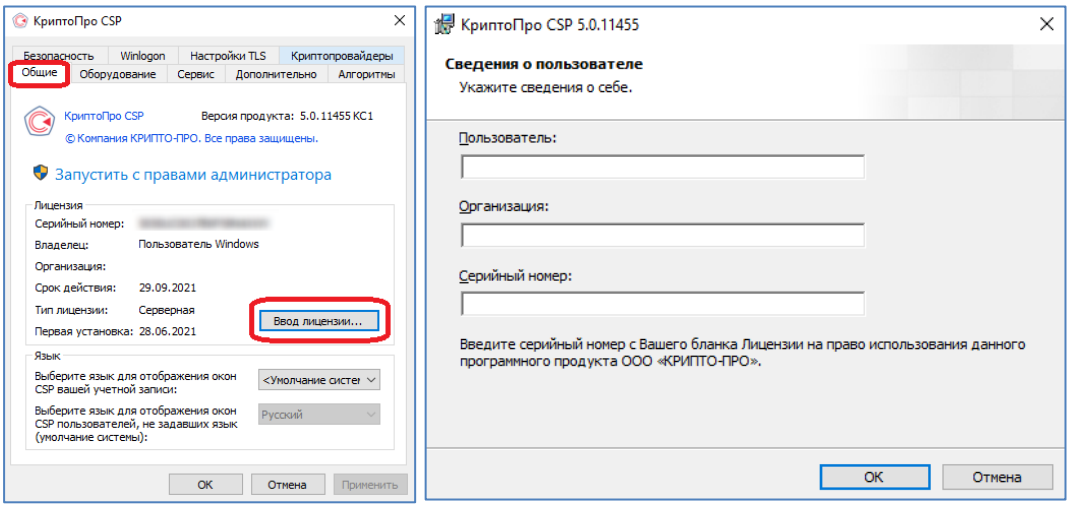

Рисунок 1

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

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

III. 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 2, позиция А).

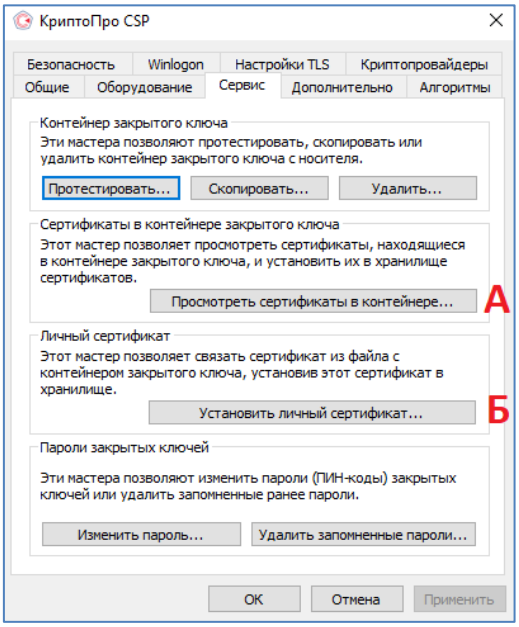

Рисунок 2

2. В открывшемся окне нажмите кнопку ***«Обзор»***, чтобы выбрать контейнер для просмотра. После выбора нужного контейнера нажмите кнопку ***«Ок»*** (Рисунок 3).

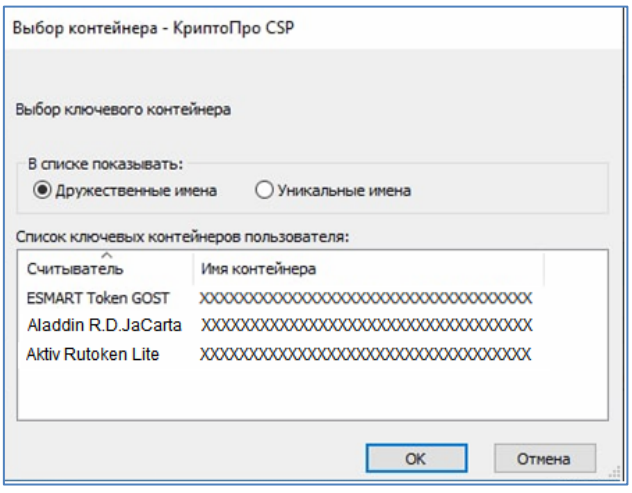

Рисунок 3

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 4).

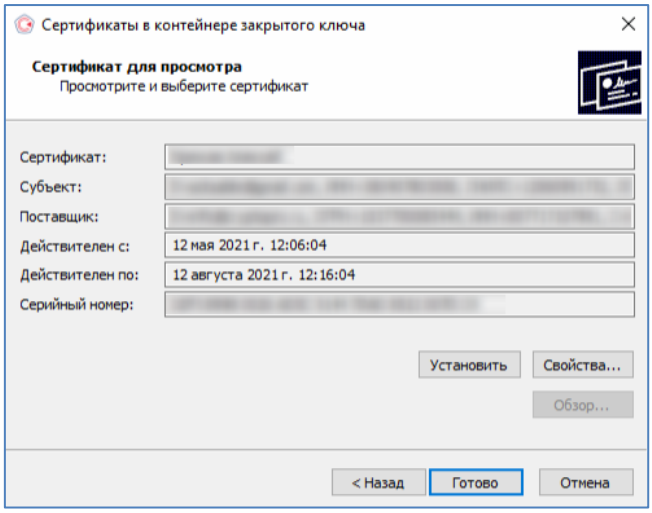

Рисунок 4

5. Если сертификат ранее уже был установлен, появится следующее информационное окно, нажмите кнопку ***«Да»*** (Рисунок5).

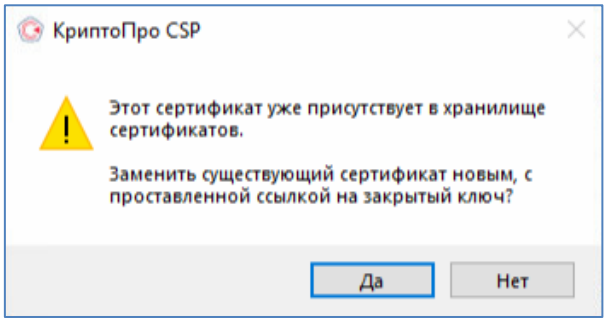

Рисунок 5

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

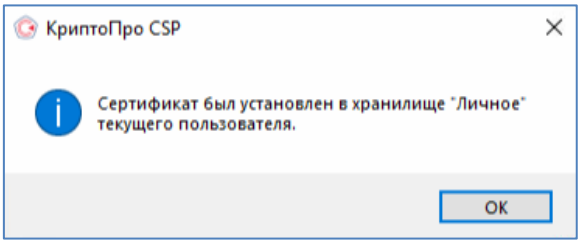

Рисунок 6

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

1. Необходимо загрузить головные сертификаты удостоверяющего центра Министерства связи и массовых коммуникаций (далее по тексту - ***Головной УЦ***) можно самостоятельно с официального сайта[4], либо по ссылкам:

- **http://reestr-pki.ru/cdp/guc_gost12.crt**
- **http://reestr-pki.ru/cdp/guc2021.crt**
- **http://reestr-pki.ru/cdp/guc2022.crt**

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

2. Откройте загруженный сертификат и нажмите ***«Установить сертификат»*** (Рисунок 7).

3. Запустится мастер импорта сертификатов, нажмите ***«Далее»***.

4. При установке корневого сертификата Головного УЦ в окне выбора хранилища, необходимо хранилище указать вручную, для этого выбрать ***«Поместить все сертификаты в следующее хранилище»*** (Рисунок 8, позиция А), нажать ***«Обзор»*** (Рисунок 8, позиция Б), выбрать ***«Доверенные корневые центры сертификации»*** (Рисунок 8, позиция В), нажать ***«Далее»*** (Рисунок 8, позиция Г).

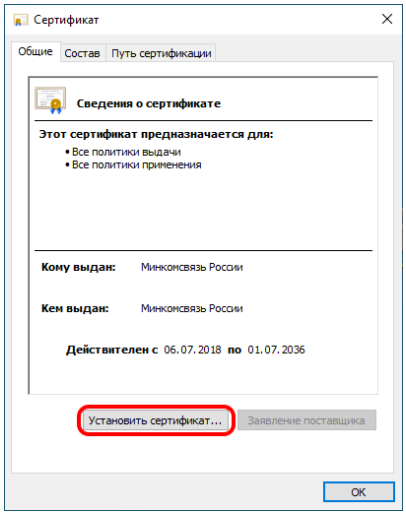

Рисунок 7

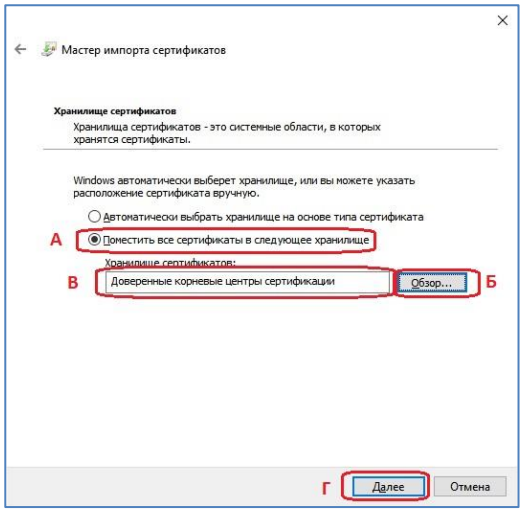

Рисунок 8

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

6. Установите оба сертификата.

Внимание! Необходимо установить следующие сертификаты в хранилище сертификатов:

А. Если ЭП получена в УЦ ФНС, то необходимо загрузить сертификат УЦ ФНС самостоятельно с официального сайта[5], либо по ссылкам:

- **http://uc.nalog.ru/crt/CA_FNS_Russia_2022.crt**
- **http://cdp.tax.gov.ru/crt/CA_FNS_Russia_2023_01.crt**

Б. Если ЭП получена в УЦ ФК, то необходимо загрузить сертификат УЦ ФК самостоятельно с официального сайта[6], либо по ссылке:

- **http://crl.roskazna.ru/crl/ucfk_2022.crt**
- **http://crl.roskazna.ru/crl/ucfk_2023.crt**

В. Если ЭП получены в УЦ Банка России, то необходимо загрузить сертификат УЦ Банка России самостоятельно с официального сайта[7], либо по ссылке:

- **http://crl1.ca.cbr.ru/aucbr-D944F67B23B815C9803690ECFE34B2C5F09652A2.cer**

7. Откройте загруженный сертификат и нажмите ***«Установить сертификат»*** (Рисунок 9).

8. Запустится мастер импорта сертификатов, нажмите ***«Далее»***.

9. При установке подчиненного сертификата в окне выбора хранилища, необходимо хранилище указать вручную, для этого выбрать ***«Поместить все сертификаты в следующее хранилище»*** (Рисунок 10, позиция А), нажать ***«Обзор»*** (Рисунок 10, позиция Б), выбрать ***«Промежуточные корневые центры сертификации»*** (Рисунок 10, позиция В), нажать ***«Далее»*** (Рисунок 10, позиция Г).

[5] URL: https://www.nalog.gov.ru/rn77/related_activities/ucfns/ccenter_res/
[6] URL: https://roskazna.gov.ru/gis/udostoveryayushhij-centr/kornevye-sertifikaty/?year=2021
[7] URL: https://www.cbr.ru/certification_center_br/resursy_udostoveryayuschego_centra/

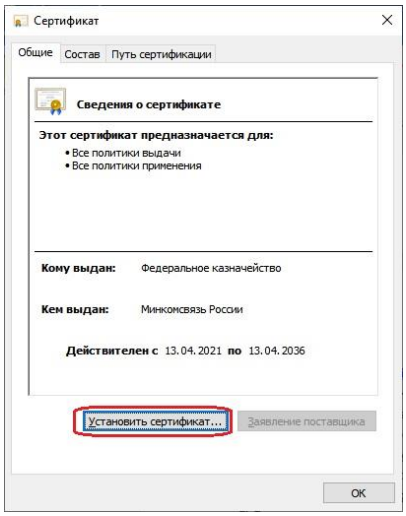

Рисунок 9

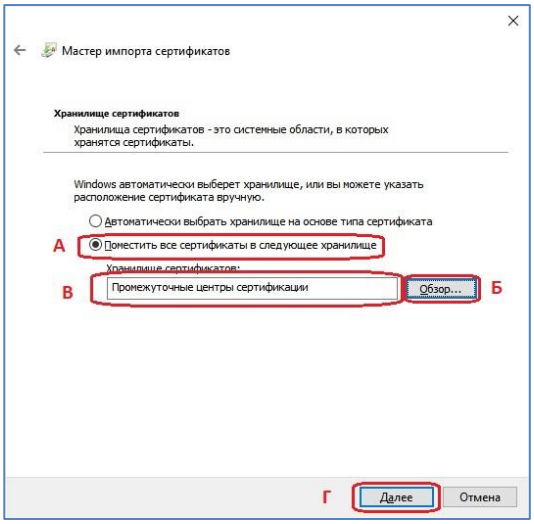

Рисунок 10

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

V. Добавление КЭП АУЦ в ViPNet Client

Внимание!. Версия ViPNet Client должна быть выше 4.5.1.

1. Запустить ***ViPNet Client*** (Рисунок 11, позиция А) или ***ViPNet Деловая почта*** (Рисунок 11, позиция В).

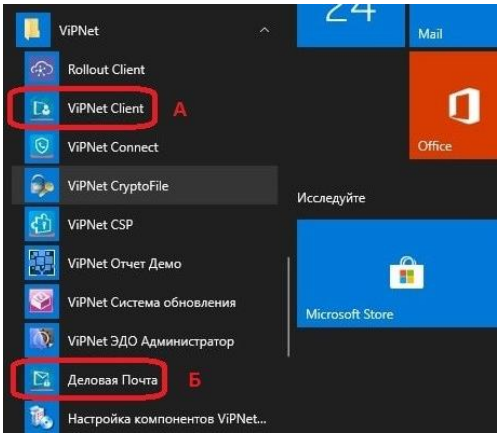

Рисунок 11

2. Если запускается ***ViPNet Client***, то необходимо нажать на кнопку ***«Сервис»*** и выбрать ***«Настройка параметров безопасности»*** (Рисунок 12). Если запускается ***ViPNet Деловая Почта***, то необходимо нажать на кнопку ***«Инструменты»*** и выбрать ***«Настройка параметров безопасности»*** (Рисунок 13).

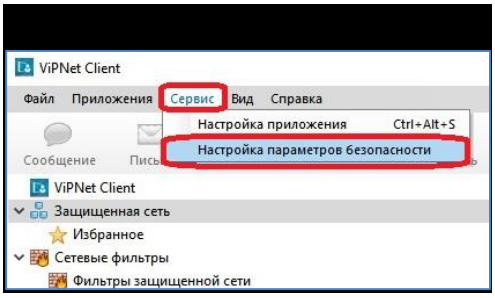

Рисунок 12

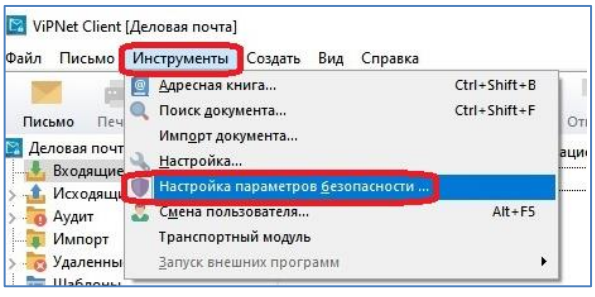

Рисунок 13

3. Убедитесь, что установлена галочка на пункте ***«Разрешить использование сертификатов из хранилища ОС»*** (Рисунок 14).

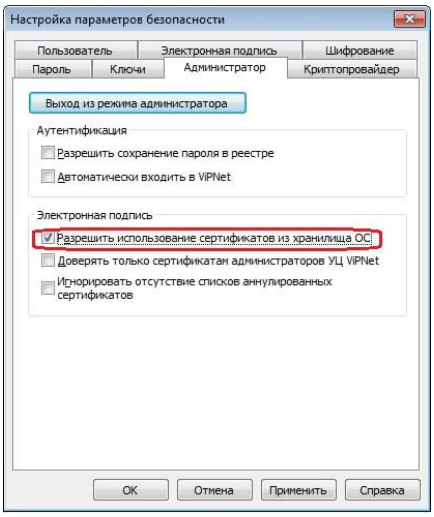

Рисунок 14

4. Если галочка не установлена, в появившемся окне на вкладке ***«Администратор»*** нажать кнопку ***«Вход в режим администратора»*** (Рисунок 15). Далее необходимо ввести индивидуальный пароль администратора сетевого узла.

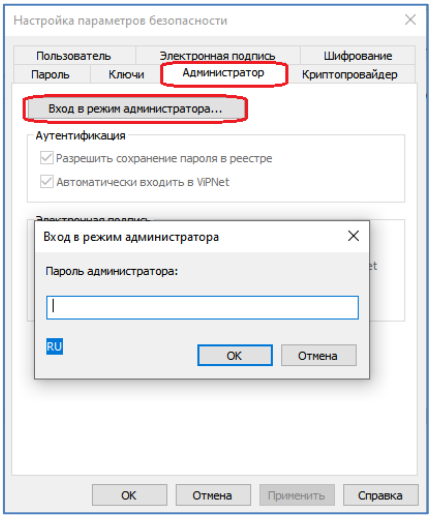

Рисунок 15

Внимание! Индивидуальный пароль сетевого узла должен быть получен в точке выдачи УЦ ИИТ на бумажном носителе. Если данный бумажный носитель утерян, или не был получен в УЦ ИИТ, необходимо обратиться в службу технической поддержки УЦ ИИТ по номеру телефона: 8-800-250-0-265.

5. После входа в режим администратора необходимо установить галку на пункте ***«Разрешить использование сертификатов из хранилища ОС»*** (Рисунок 14).

6. В том же окне настроек параметров безопасности во вкладке ***«Электронная подпись»*** необходимо выбрать сертификат для использования (Рисунок 16).

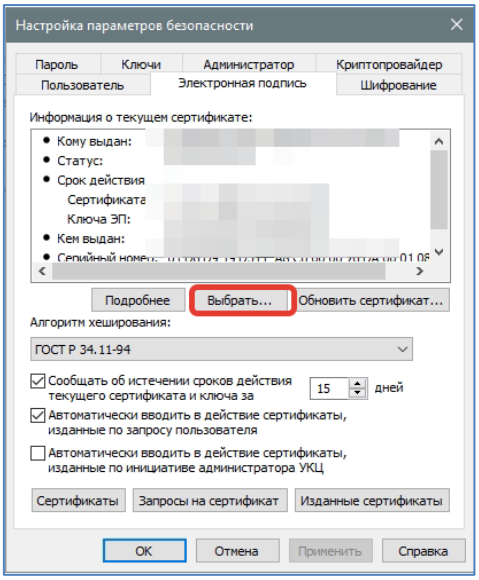

Рисунок 16

7. Далее выбрать новый сертификат и нажать кнопку ***«ОК»*** (Рисунок 17).

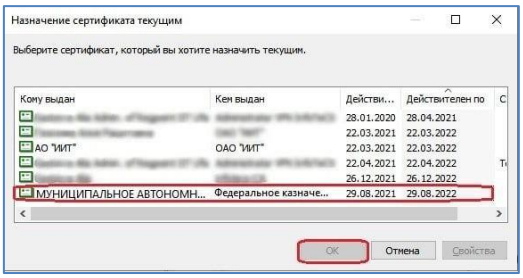

Рисунок 17

8. Информация о текущем сертификате изменится на актуальную. Убедитесь в том, что сертификат действителен (Рисунок 18).

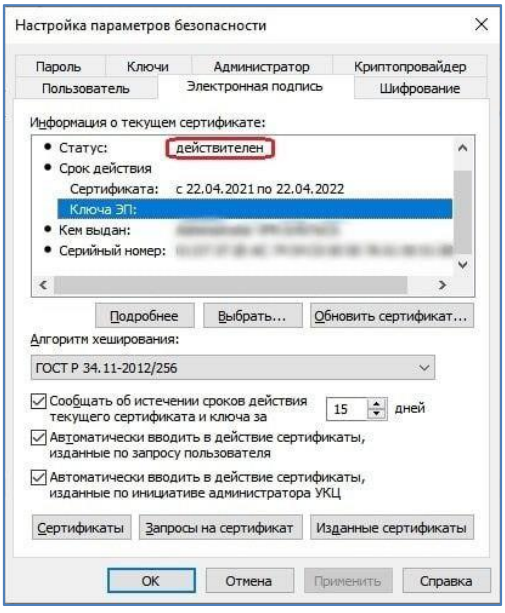

Рисунок 18

9. После выполнения вышеуказанных шагов и при отправке письма в Деловой почте появится окно с предложением ввести пароль от контейнера ключей (Рисунок 19). На усмотрение пользователя можно сохранить пароль. При использовании автопроцессинга для автоматизации процесса рекомендуется

сохранять пароль. Если сохранение пароля недопустимо, то пароль от контейнера ключей необходимо будет вводить каждый раз после перезапуска Деловой почты.

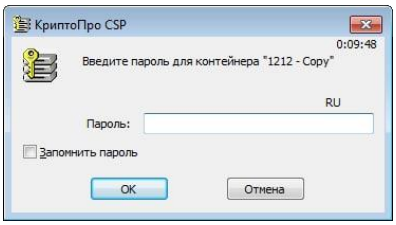

Рисунок 19