Установка ключа электронной подписи и сертификатов

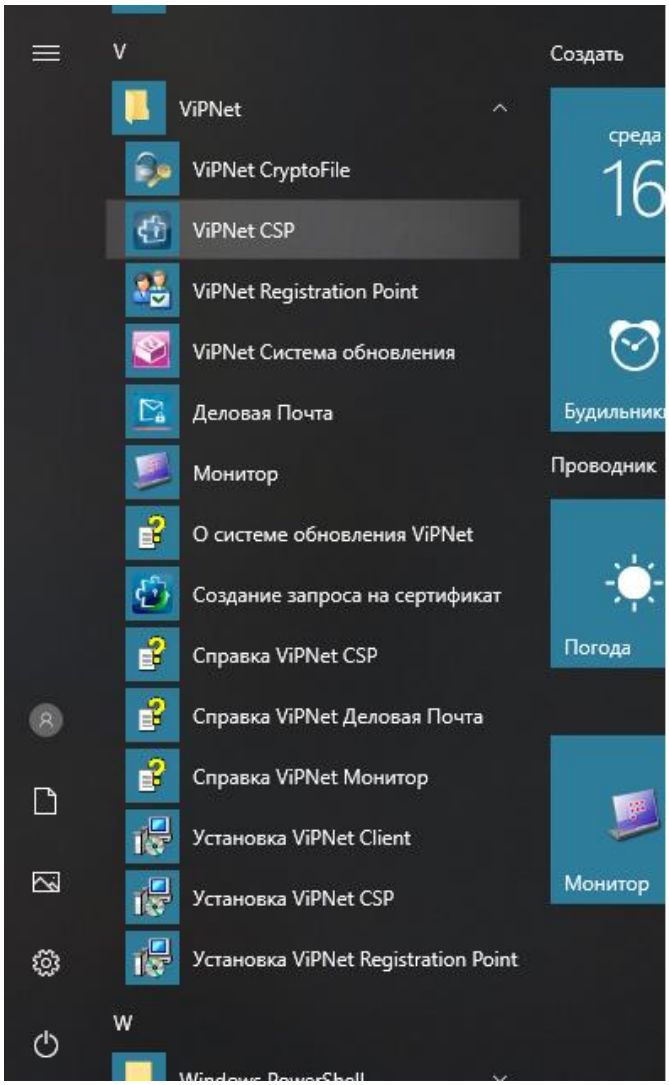
Чтобы начать работу с электронной подписью, необходимо установить в операционную систему контейнер ключа подписи, сертификат пользователя, корневой сертификат Удостоверяющего центра и список отозванных сертификатов (далее - СОС).

Контейнер ключа подписи защищен для сертифицированных носителей ключей ЭП PIN-кодом, в других случаях – паролем, известным только пользователю (лицу, формировавшему запрос на сертификат).

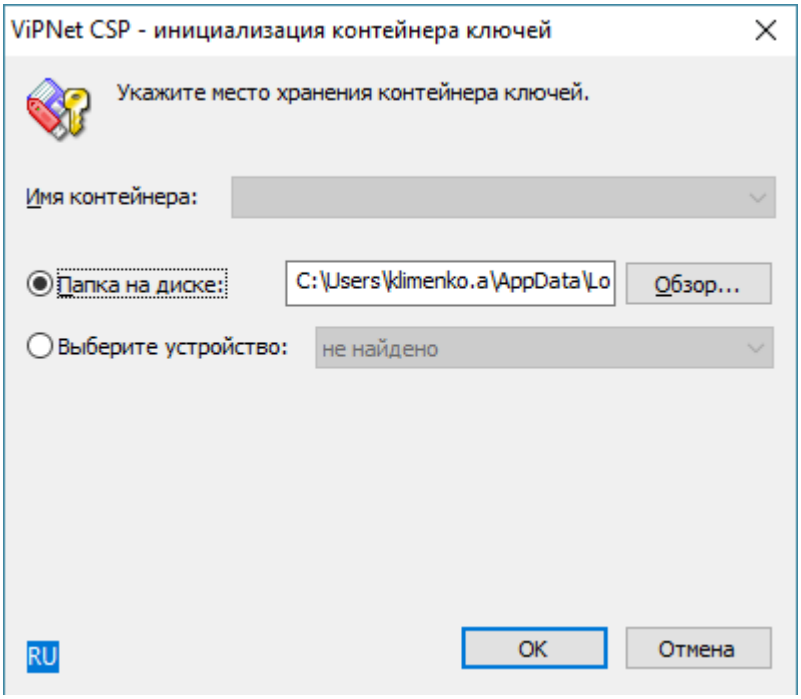
Сертификат с открытым ключом (для проверки подлинности вашей подписи), сертификат уполномоченного лица Удостоверяющего центра и СОС выдаются Удостоверяющим центром при получении сертификата ключа подписи.

Установка ключа электронной подписи и личного сертификата пользователя.

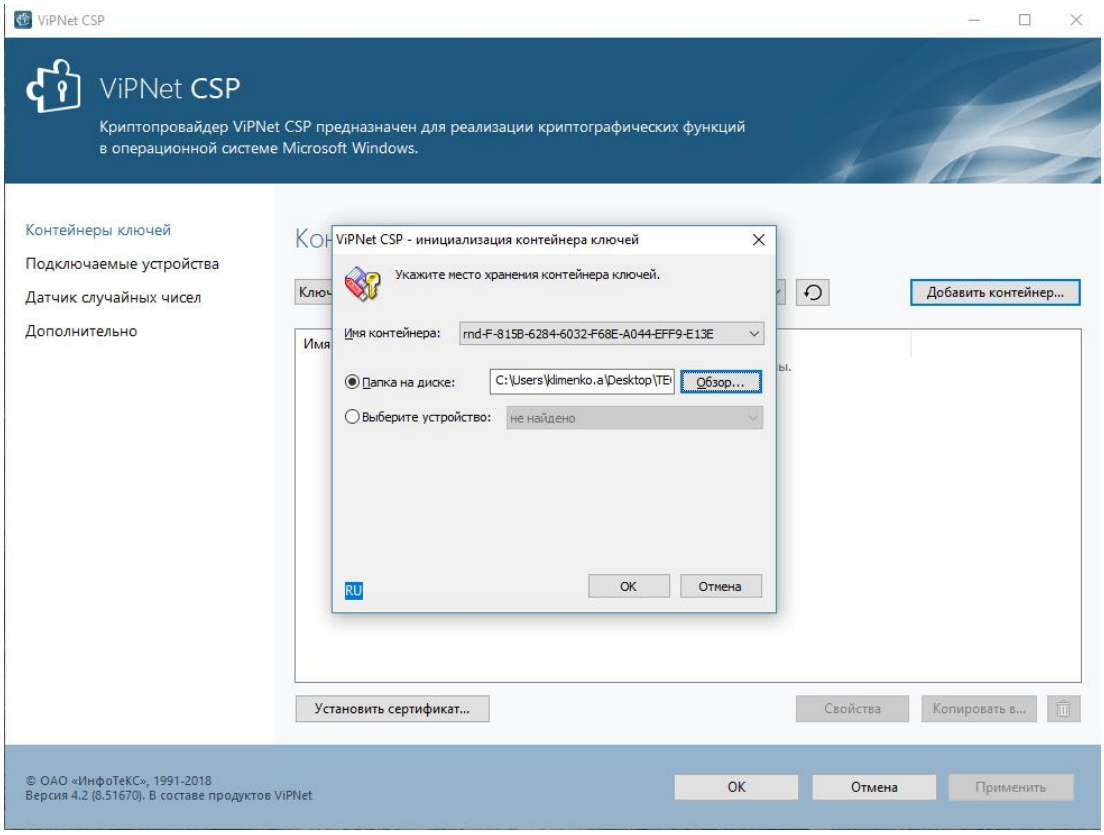
1. Перенесите с флеш-носителя ключи электронной подписи на рабочий стол компьютера.
2. Запустите программу VipNet CSP.



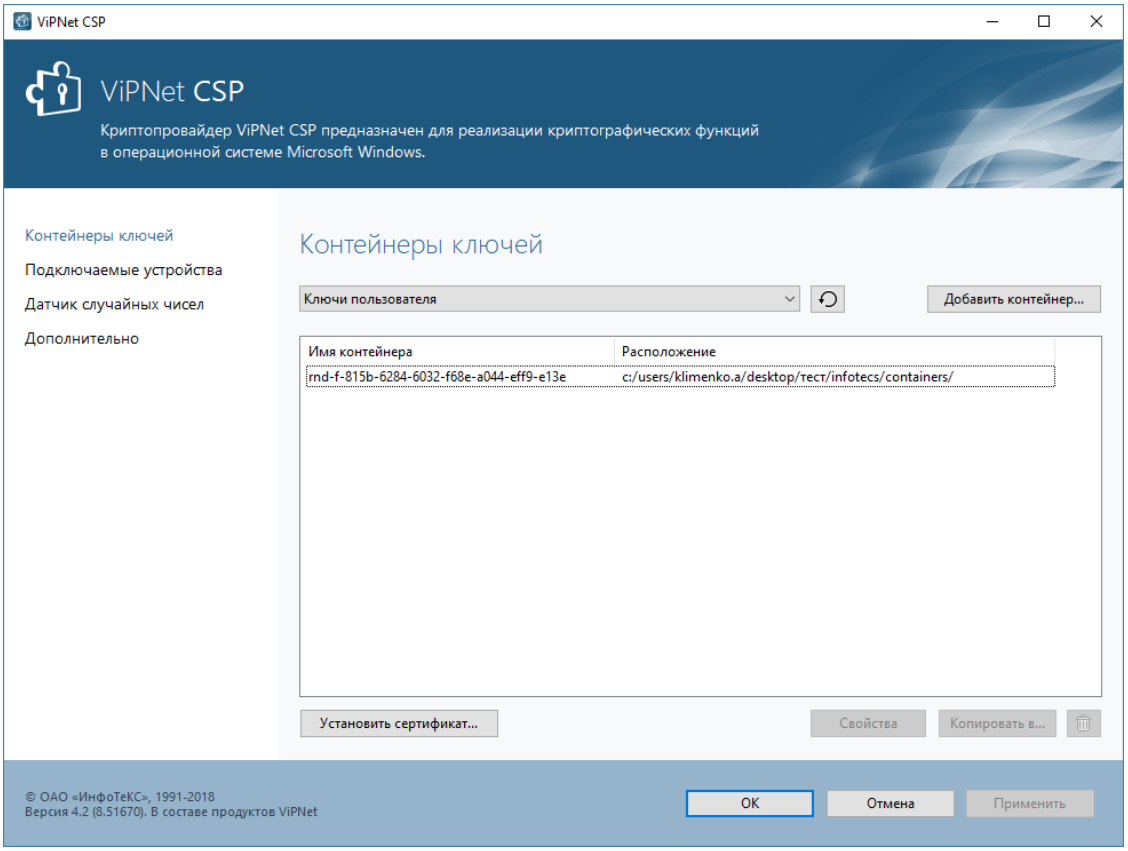
3. В окне программы ViPNet CSP нажмите на Добавить контейнер. Выйдет окно инициализации контейнера ключей.



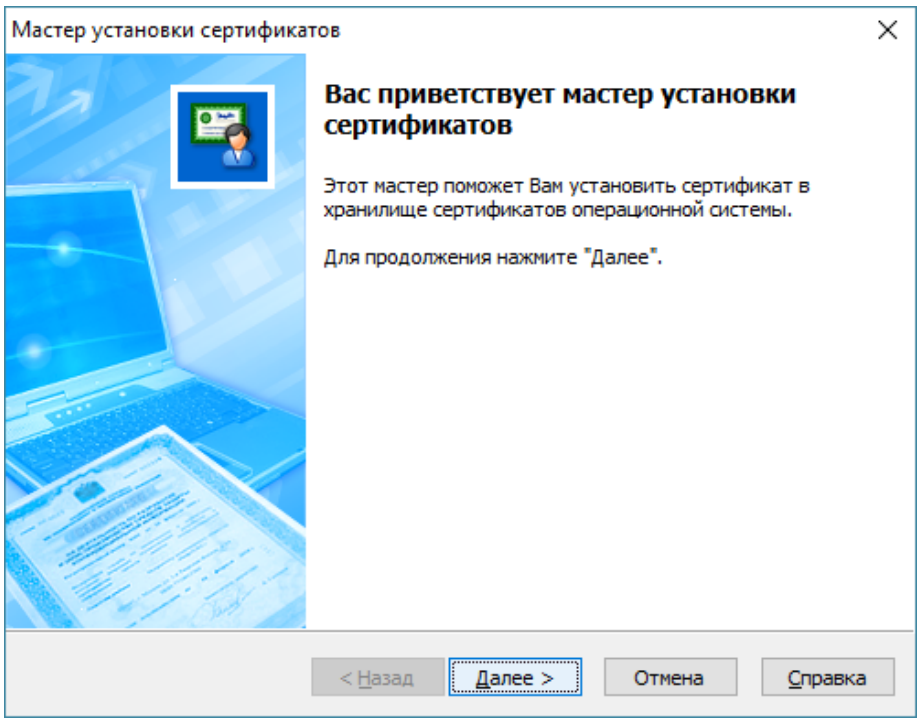
4. Выберите контейнер закрытого ключа электронной подписи, в зависимости, где он расположен. В данном примере, закрытый контейнер расположен на рабочем столе, в папке Тест – Infotecs – Containers.
5. После выбора закрытого контейнера в Имени контейнера будет отображен контейнер закрытого ключа электронной подписи. Нажимаем **Ок**.



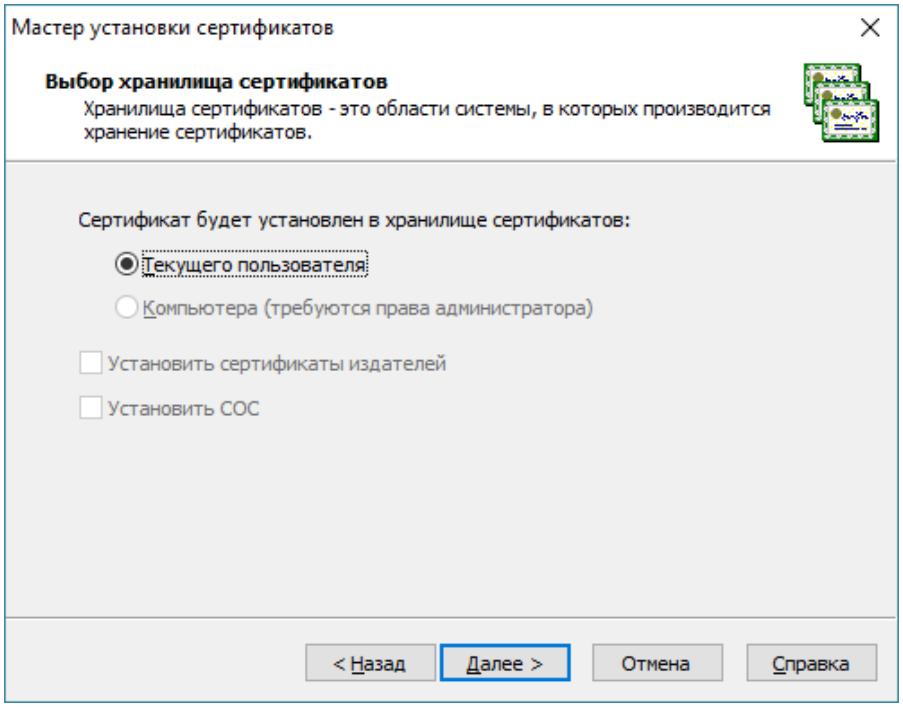
6. После этого контейнер закрытого ключа отобразится в программе ViPNet CSP как показано на рисунке.



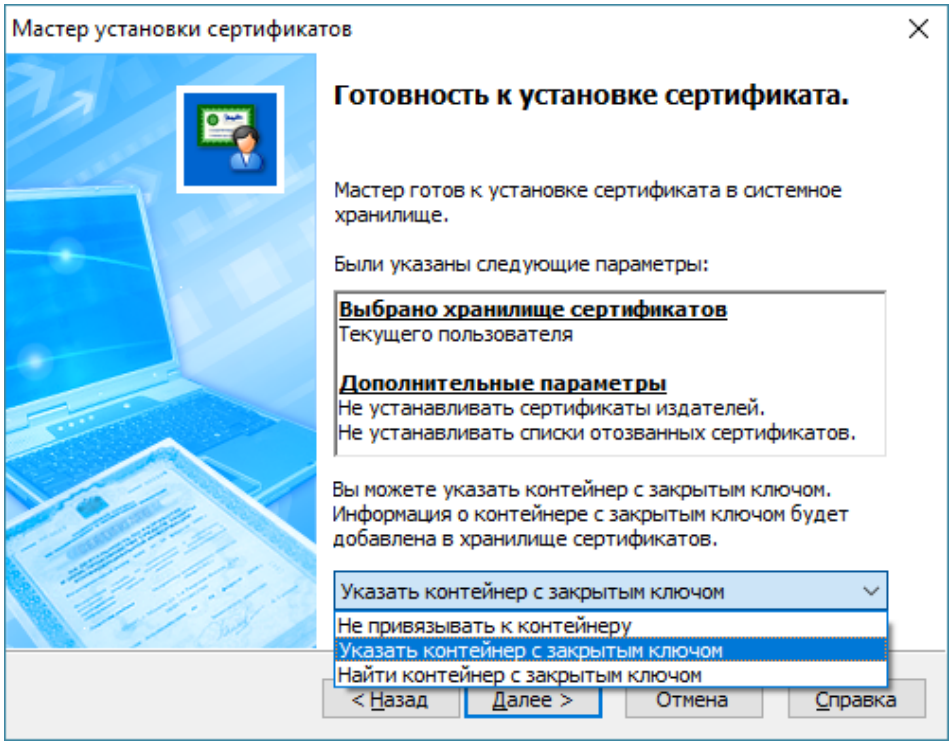
7. Далее выбираем контейнер и нажимаем Установить сертификат. Выбираем сертификат открытого ключа, который находится в архивной папке cert, переданной удостоверяющим центром. Перед тем как установить сертификат, необходимо извлечь сертификат из архивной папки.
8. В открывшемся окне мастера установки сертификатов нажмите Далее.



9. В открывшемся окне мастера установки сертификатов нажмите Далее.



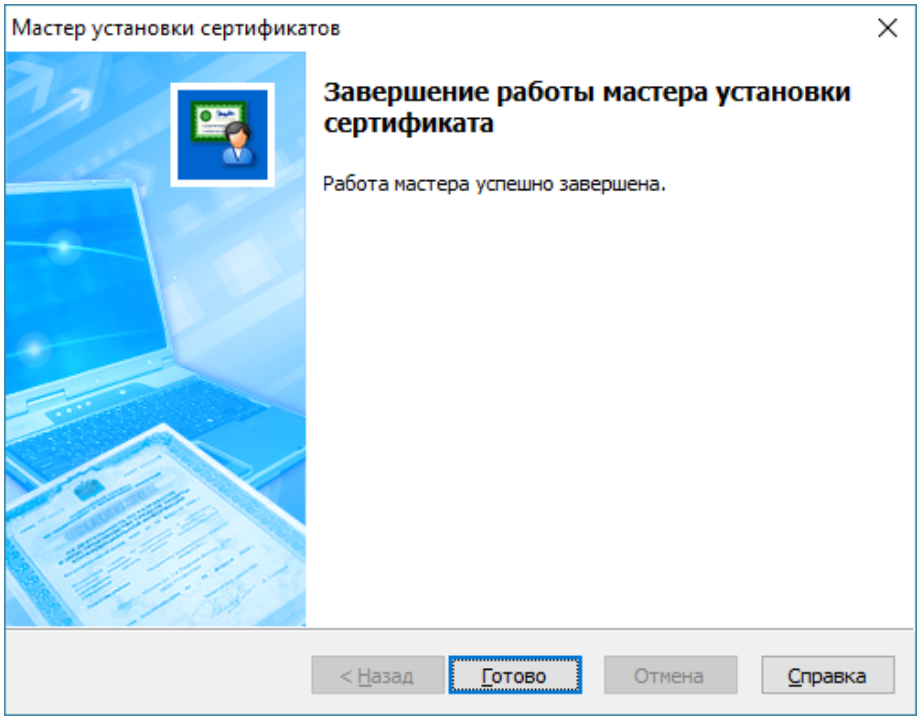
10. В открывшемся окне мастера установки отметьте Указать контейнер с закрытым ключом, затем нажмите Далее.



11. В открывшемся окне выбора контейнера выберете, Папка на диске, нажмите Обзор и выберете папку нахождения закрытого контейнера, затем нажмите кнопку ОК.

В данном примере, контейнер находится на рабочем столе, в папке Тест – Infotecs – Containers. Далее появится окно с запрашиваемым пин-кодом от закрытого контейнера, он находится в файле пароль, переданный Удостоверяющим центром.

12. Если появится запрос о сохранение сертификатов в контейнере, ответьте **Да**. Дождитесь завершения работы мастера, после чего программу VipNet CSP можно закрыть.



Установка корневого сертификата Удостоверяющего центра и СОС

Имена файлов сертификатов и СОС:
ChitaCA_20xx.crt – корневой сертификат Удостоверяющего центра.
revokedCerts.crl - СОС;

Эти файлы пользователь получает из Удостоверяющего центра в папках вида, где XX – год выпуска корневого сертификата и соответствующего ему списка отозванных сертификатов, поскольку срок действия ключа подписи составляет 1 год, то достаточно иметь папки за текущий и предыдущий год.

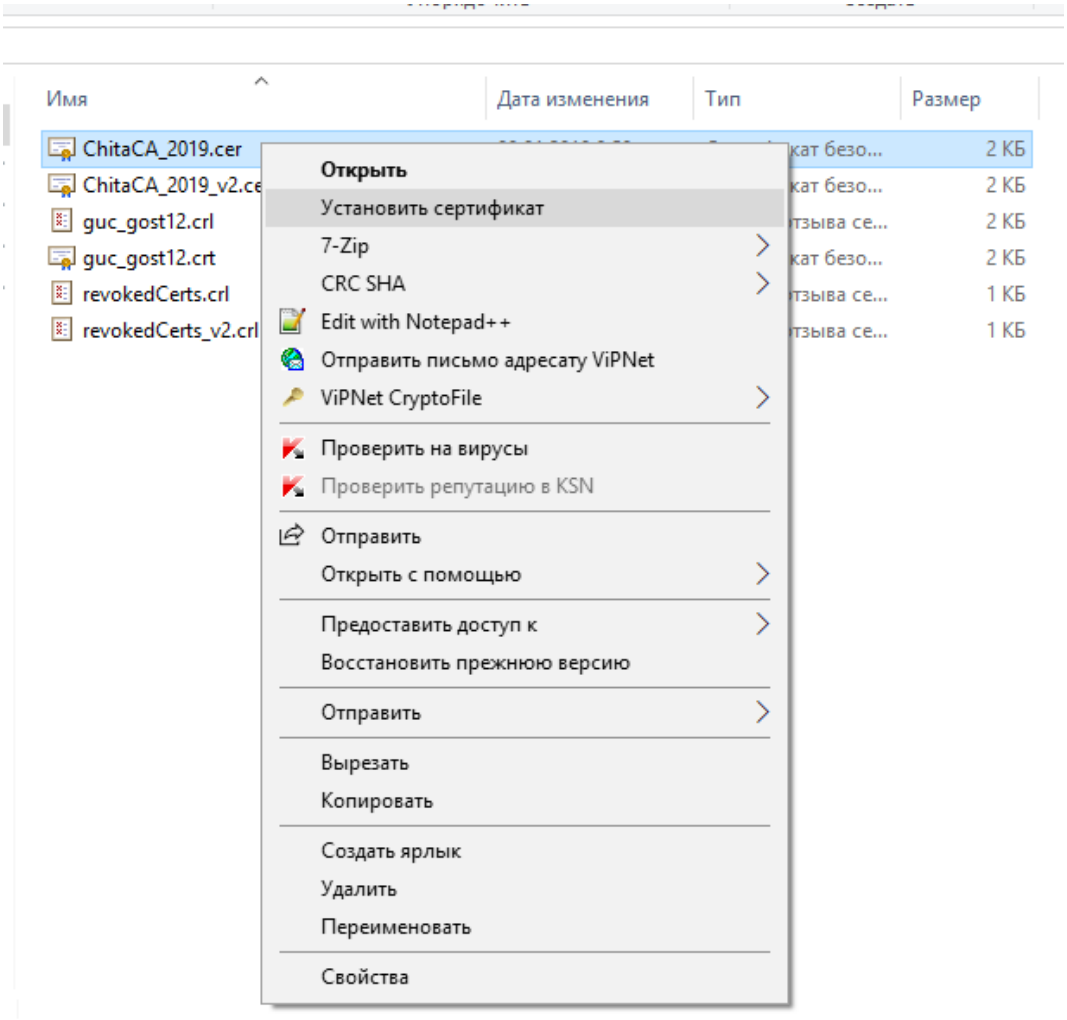
Установка сертификатов и СОС выполняется средствами операционной системы Windows.

Установка корневого сертификата Удостоверяющего центра:

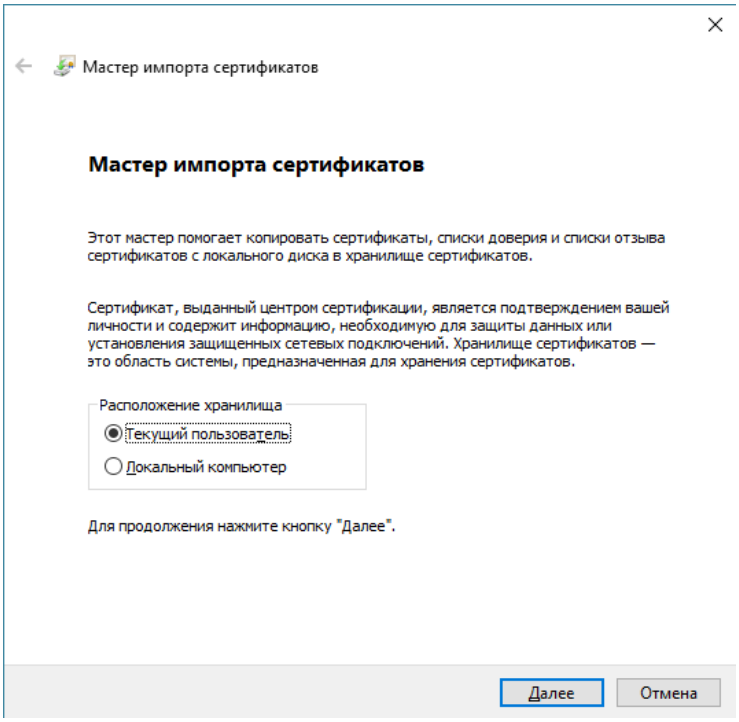
1. Откройте папку с файлом сертификата и щелкните правой кнопкой мыши по значку сертификата.
2. В контекстном меню выберите пункт **Установить сертификат.**

Примечание: отсутствие вкладки **Установить сертификат** свидетельствует о том, что вы используете несертифицированную копию операционной системы Windows,

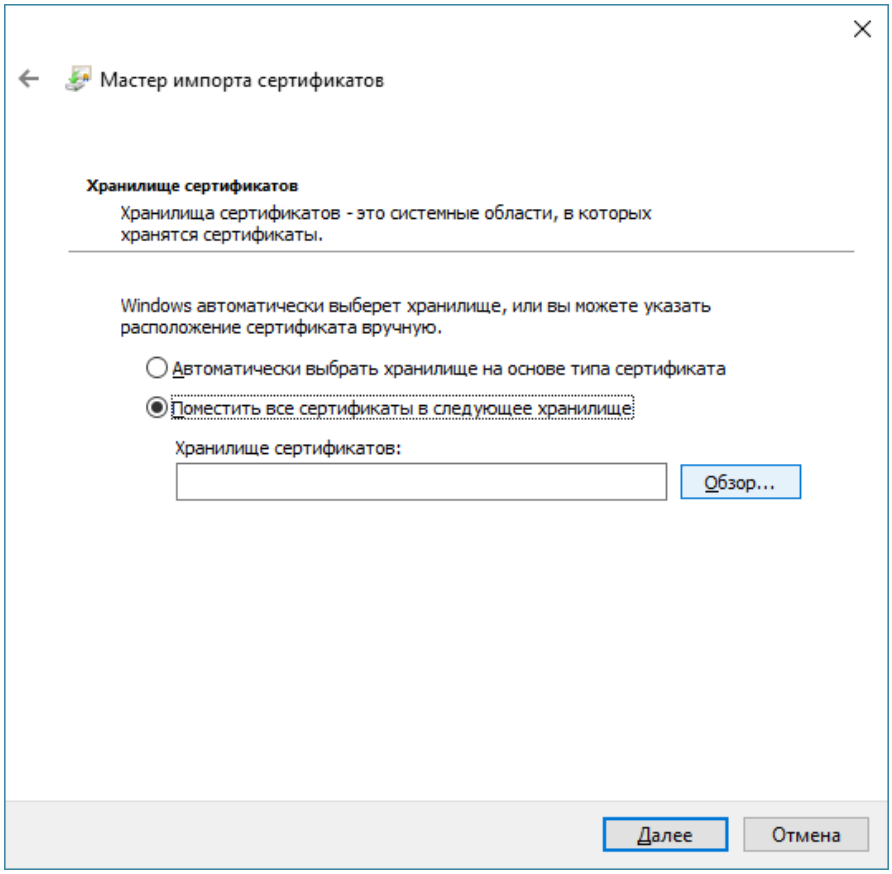
из которой вырезаны средства работы с сертификатами, в этом случае следует установить сертифицированную версию Windows.



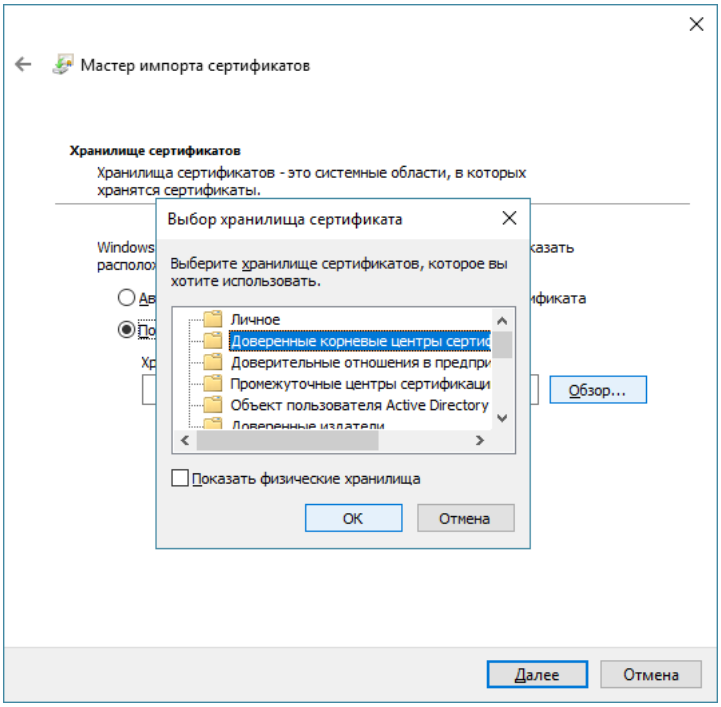
3. В окне приветствия мастера импорта сертификатов нажмите **Далее.**



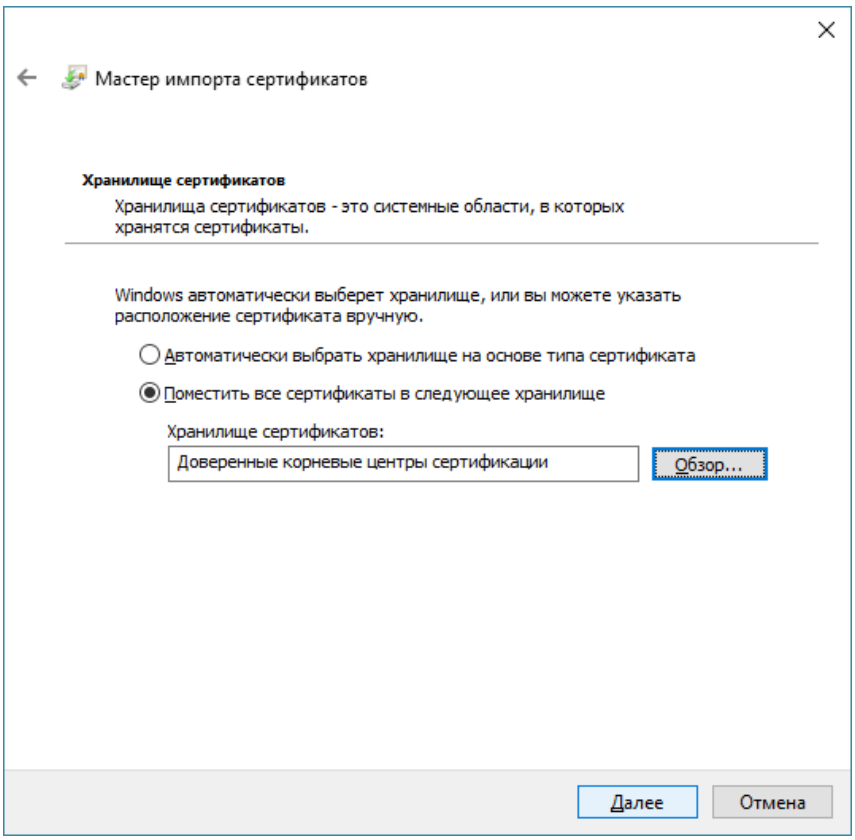
4. На странице Хранилище сертификатов выберите Поместить все сертификаты следующее хранилище и нажмите **Далее.**



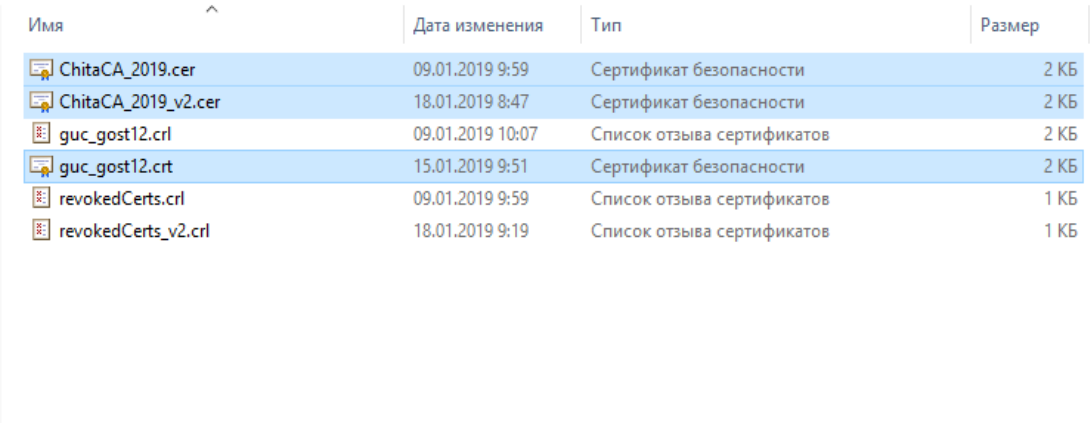
5. На странице Выбора хранилища сертификатов выберите Доверенные корневые центры сертификации и нажмите **ОК.**



6. В окне Мастер импорта сертификатов нажмите **Далее.**



7. На следующей странице нажмите **Готово.**
8. В окне Мастер импорта сертификатов появится сообщение об успешном импорте сертификата. Нажмите Ок, установка завершена.
9. Для каждого сертификата безопасности указанных на рисунке, сделайте тоже самое.

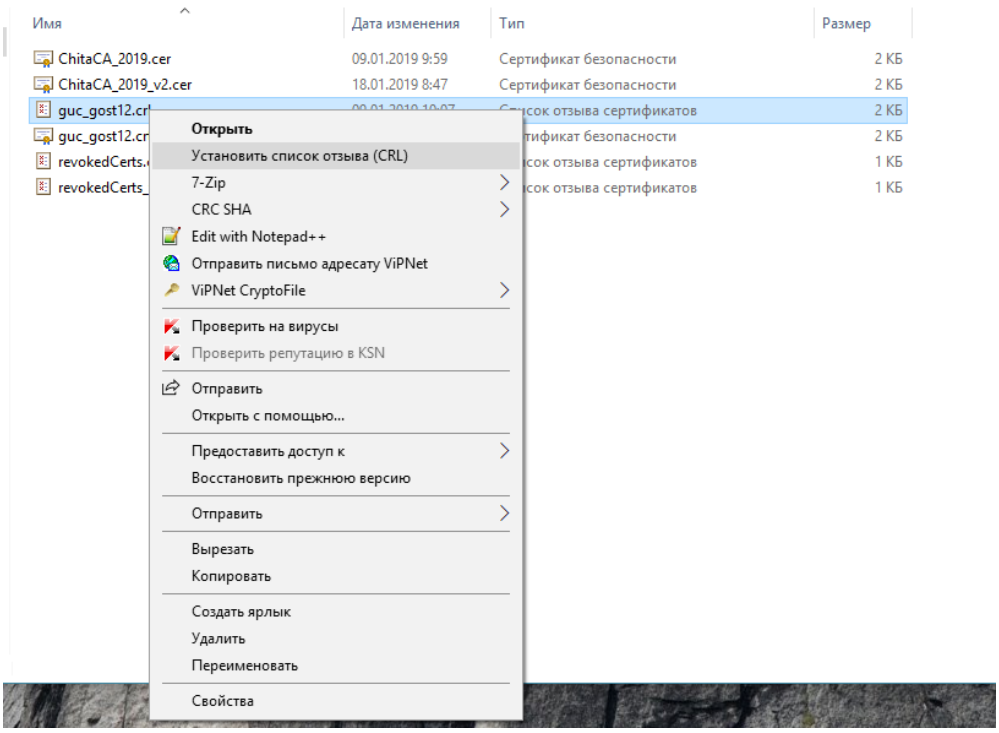


Имя	Дата изменения	Тип	Размер
ChitaCA_2019.cer	09.01.2019 9:59	Сертификат безопасности	2 КБ
ChitaCA_2019_v2.cer	18.01.2019 8:47	Сертификат безопасности	2 КБ
guc_gost12.crl	09.01.2019 10:07	Список отзыва сертификатов	2 КБ
guc_gost12.crt	15.01.2019 9:51	Сертификат безопасности	2 КБ
revokedCerts.crl	09.01.2019 9:59	Список отзыва сертификатов	1 КБ
revokedCerts_v2.crl	18.01.2019 9:19	Список отзыва сертификатов	1 КБ

Установка списка отозванных сертификатов (COC)

1. Откройте папку с файлом COC и щелкните правой кнопкой мыши по значку списка.
2. В контекстном меню выберите пункт **Установить список отзыва (CRL).**

Примечание: отсутствие вкладки **Установить список отзыва (CRL)** свидетельствует о том, что вы используете несертифицированную копию операционной системы Windows, из которой вырезаны средства работы



3. Дальше на все предложения мастера установки нажимайте кнопку **Далее**, в конце работы нажмите кнопку **Готово**, дождитесь окончания работы мастера и сообщения об успешном завершении работы.
4. Для каждого списка отозванного сертификата, указанных на рисунке, сделайте тоже самое.