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). Для органов государственной власти и местного самоуправления обязательно использование сертифицированных носителей ключей.
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. Вставьте сертифицированный носитель ключей подписи, в примерах используется Rutoken, работа с eToken принципиально не отличается.
2. Запустите программу **ViPNet CSP**.

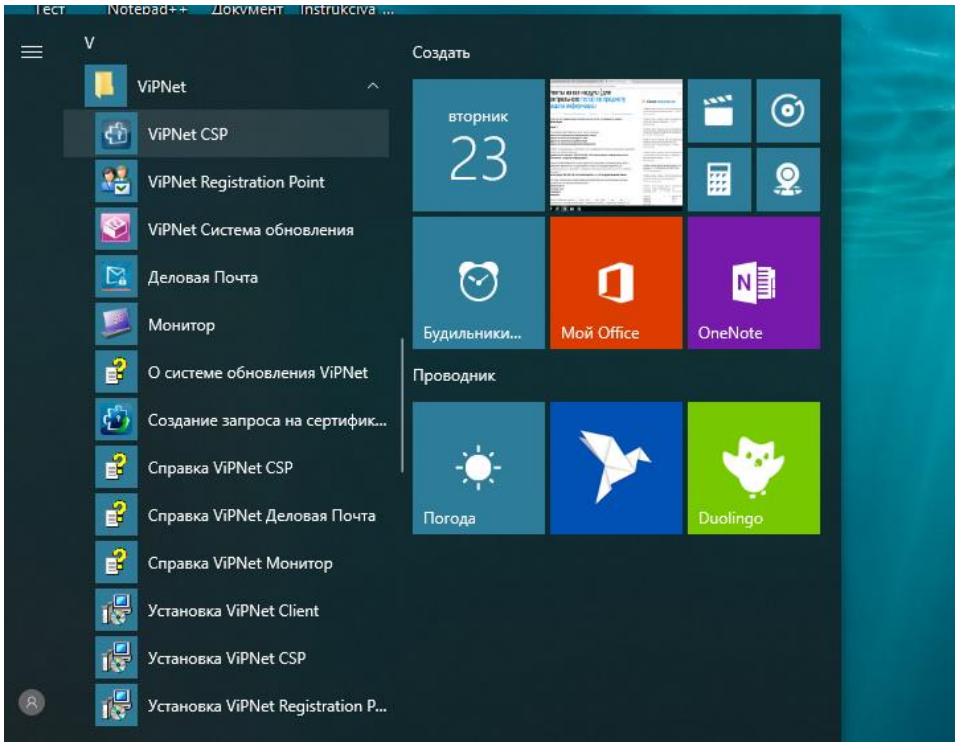

Рисунок 1 – Запуск программы ViPNet CSP

3. В окне программы **ViPNet CSP** выберите контейнер ключей**, в зависимости где он располагается,** затем нажмите кнопку **Установить сертификат.**

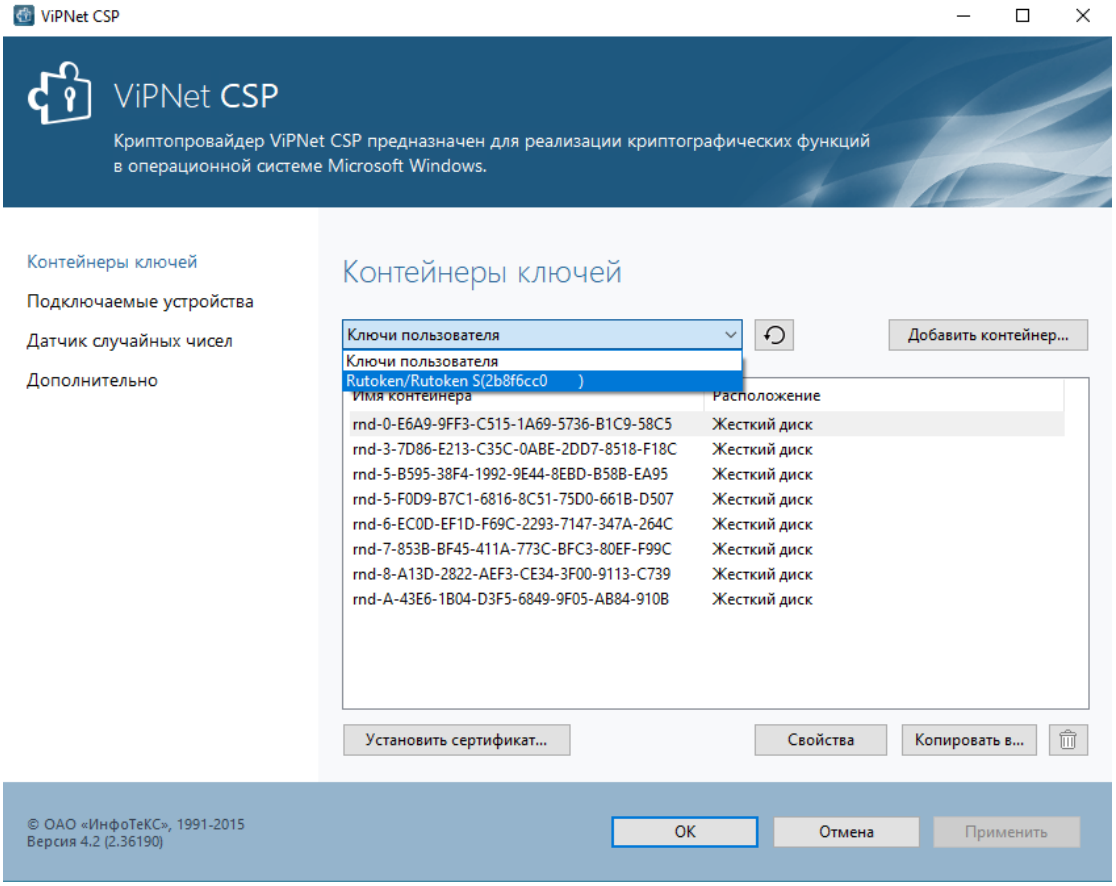

Рисунок 2 - Панель контейнеров ключей

4. В открывшемся окне укажите путь к сертификату и выберите сертификат пользователя.

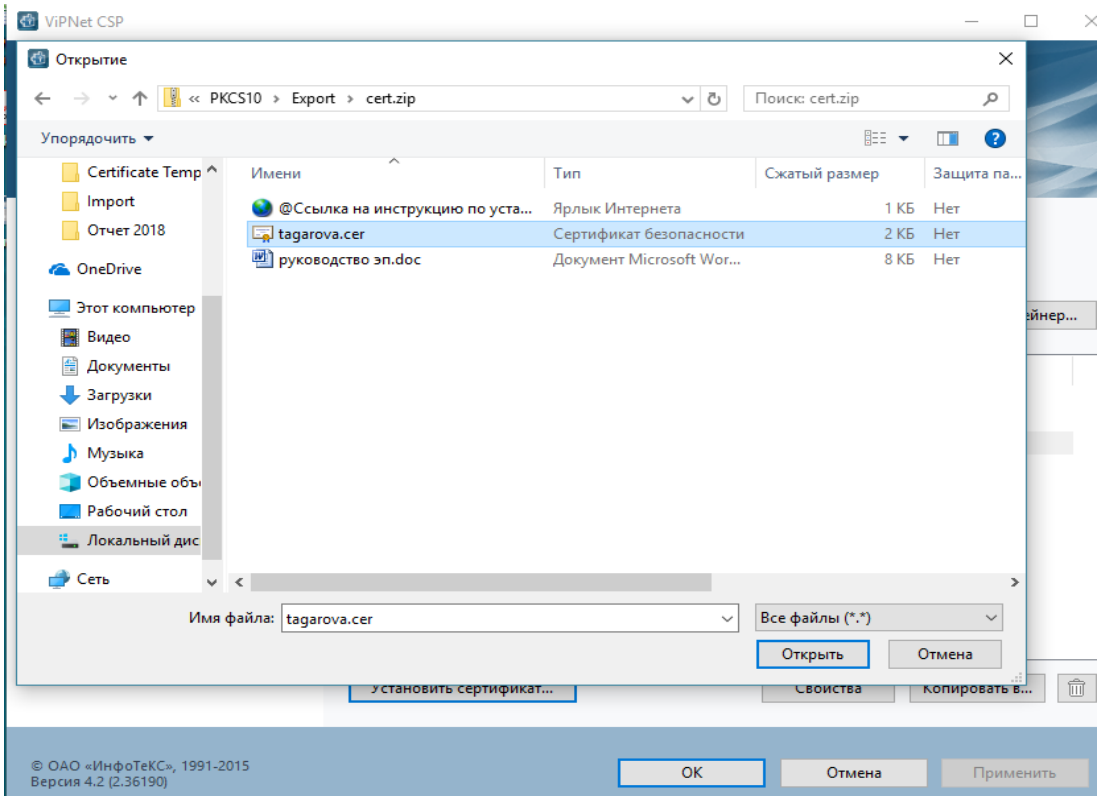

Рисунок 3 - Выбор сертификата пользователя

5. В открывшемся окне мастера установки сертификатов нажмите **Далее.**

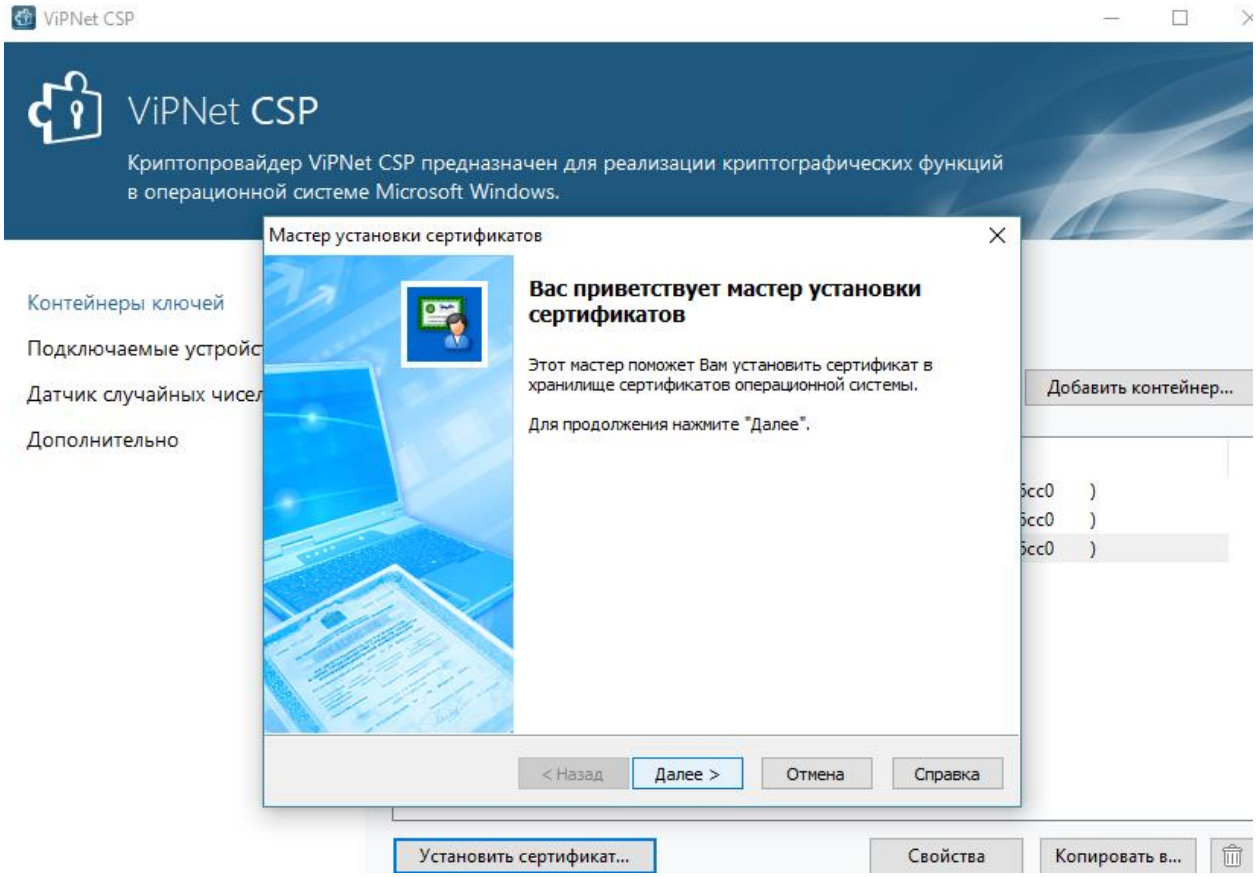

Рисунок 4 - Окно приветствия мастера установки сертификата

6. В открывшемся окне мастера установки сертификатов нажмите **Далее.**

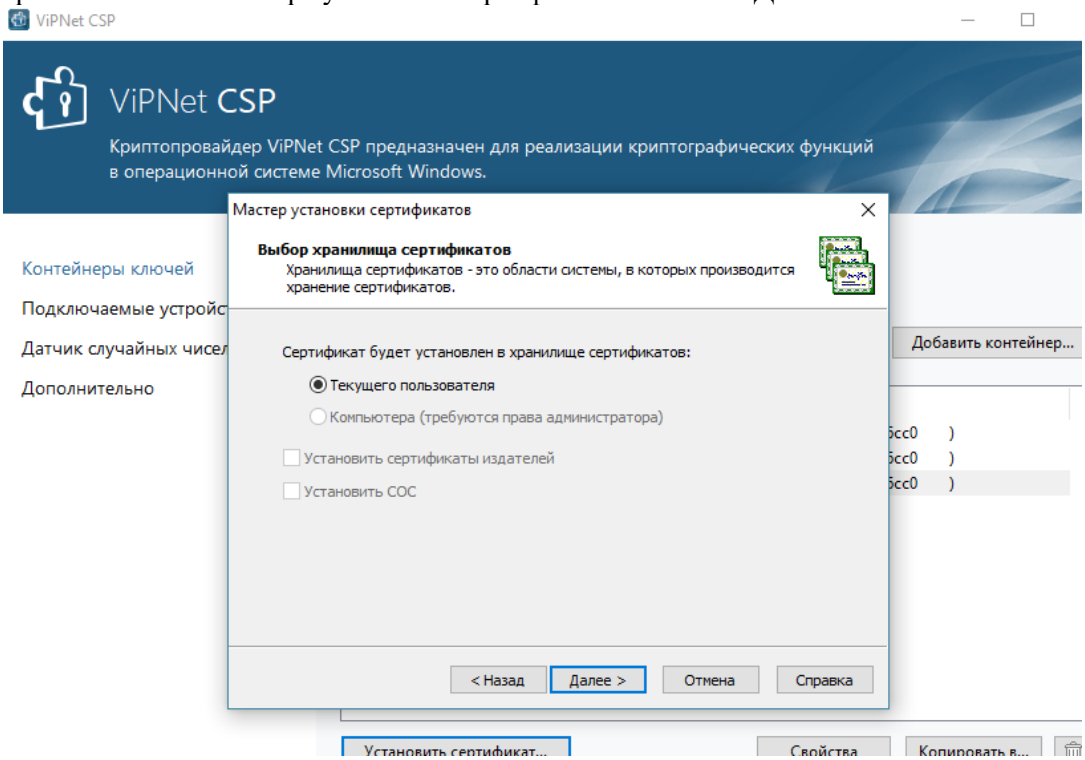

Рисунок 5 - Окно мастера установки сертификата

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

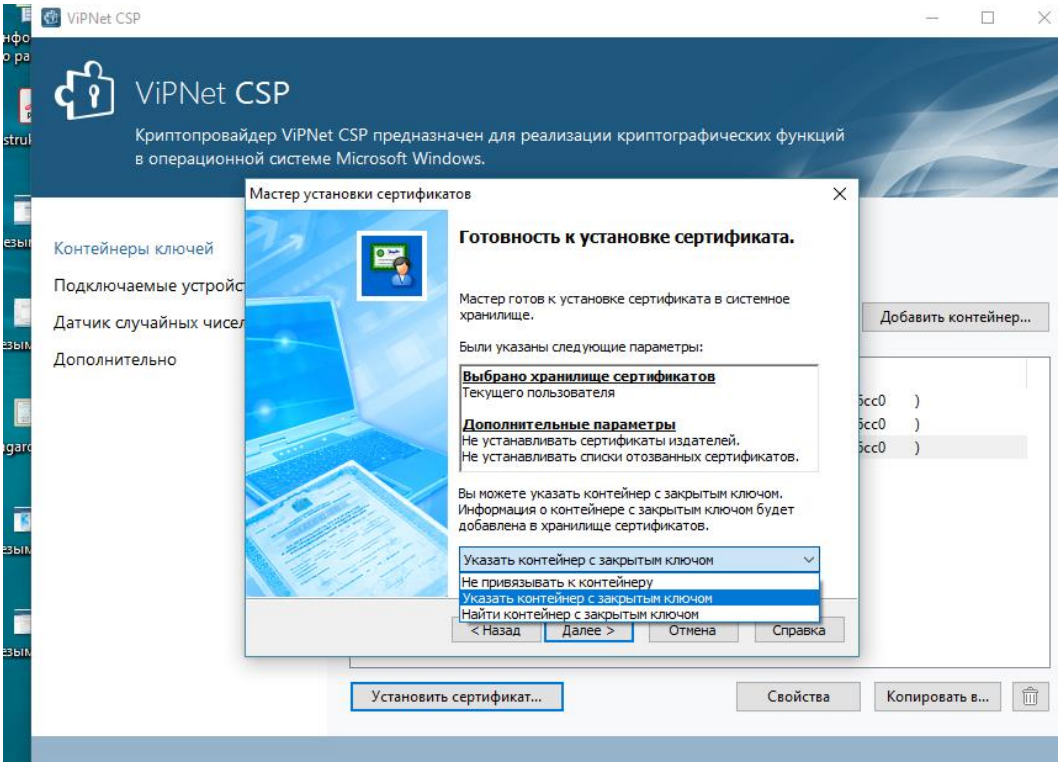

Рисунок 6 - Окно мастера установки сертификата

8. В открывшемся окне выбора контейнера установите переключатель **Выберите устройство –** для сертифицированных носителей или **Папка на диске –** во всех остальных случаях, как показано на рисунке и введите PIN-код носителя, затем нажмите кнопку **ОК.**

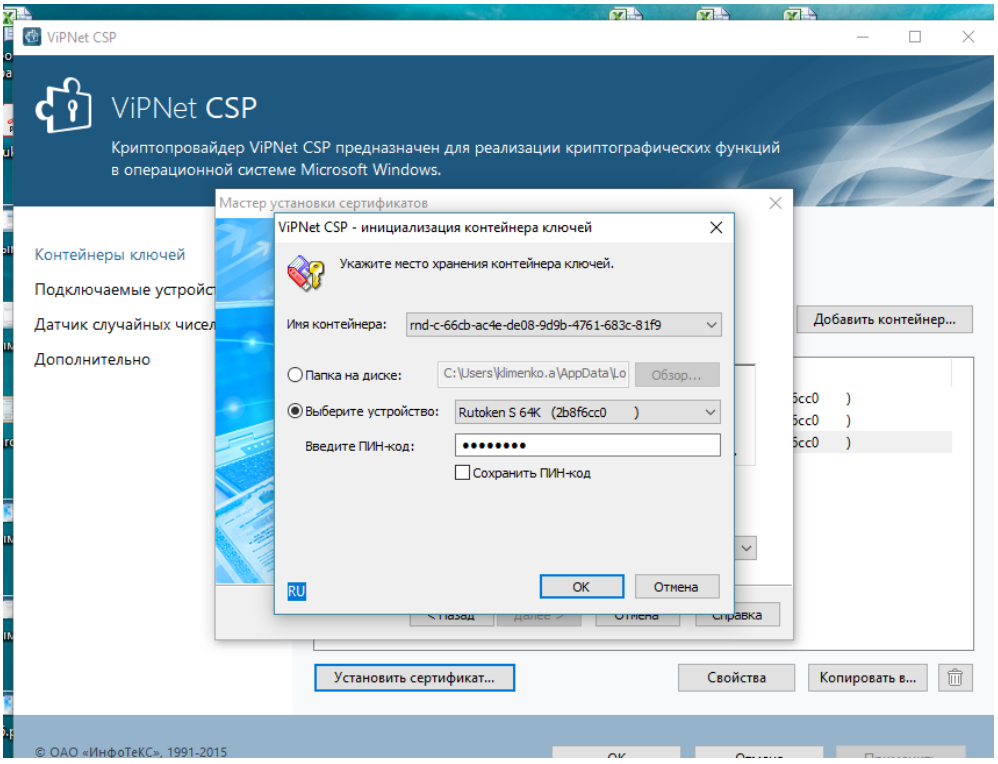

Рисунок 7 - Окно выбора контейнера закрытого ключа

9. Если появится запрос о сохранении сертификата в контейнере, ответьте **Да.**
Дождитесь завершения работы мастера, после чего программу ViPNet CSP можно завершить.

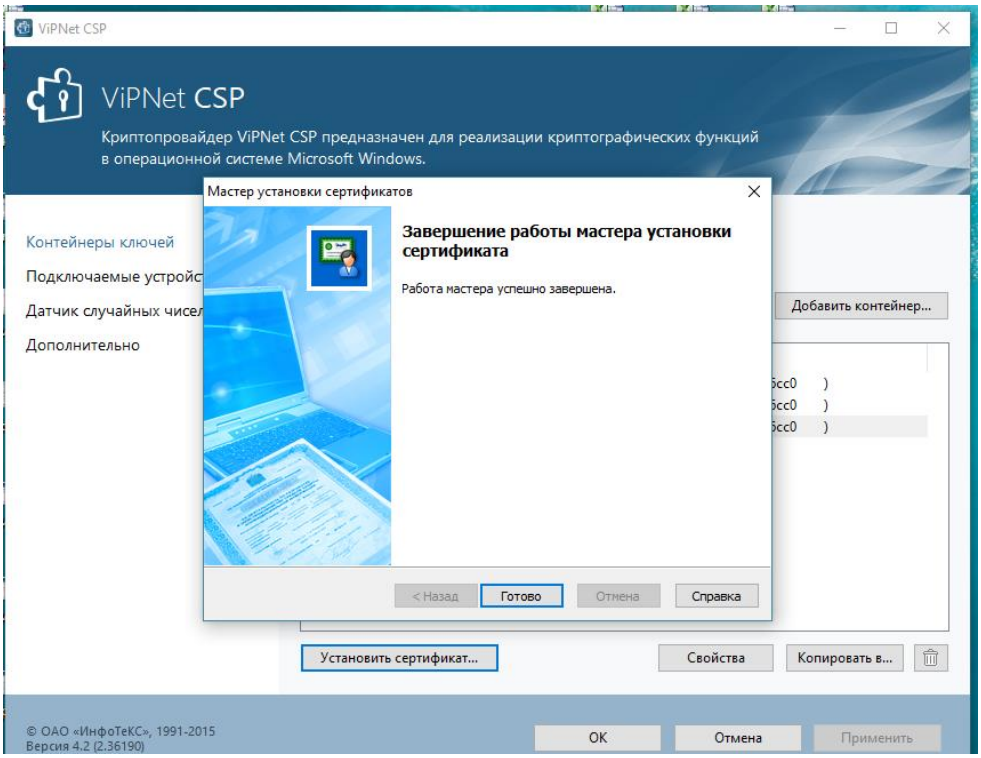

Рисунок 8 – Завершение работы мастера установки сертификата

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.

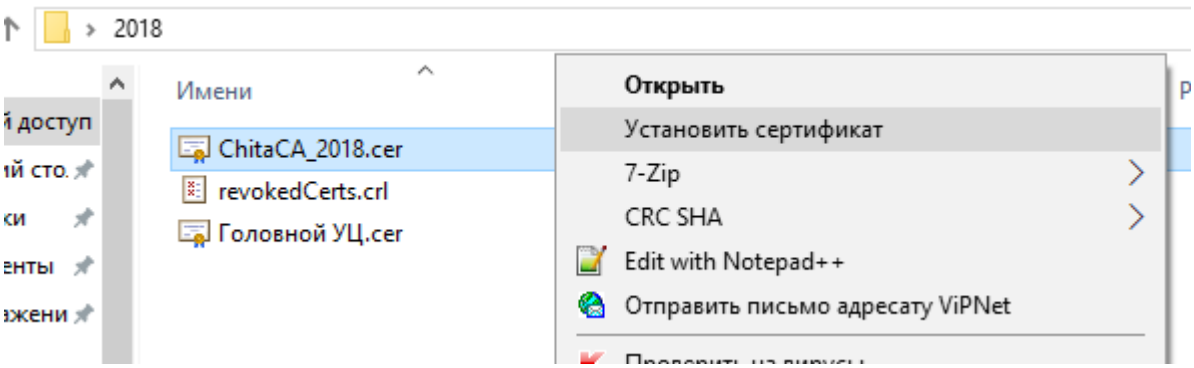

Рисунок 9 - Установка сертификата

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

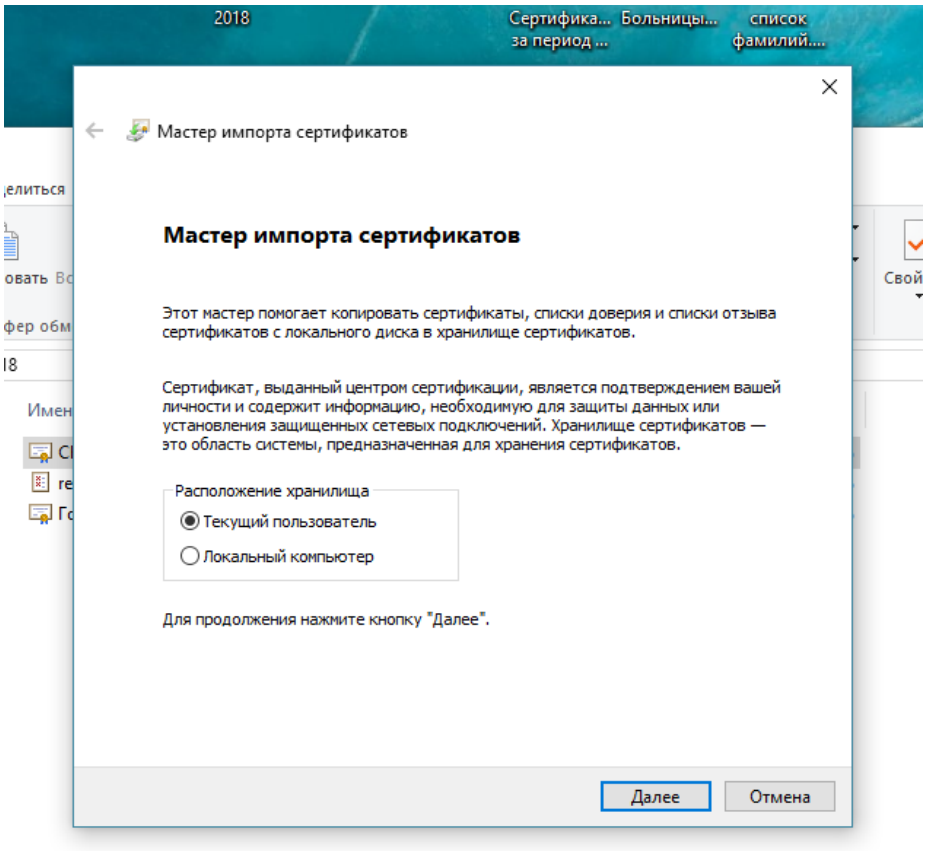

Рисунок 10 – Окно приветствия мастера импорта сертификатов

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

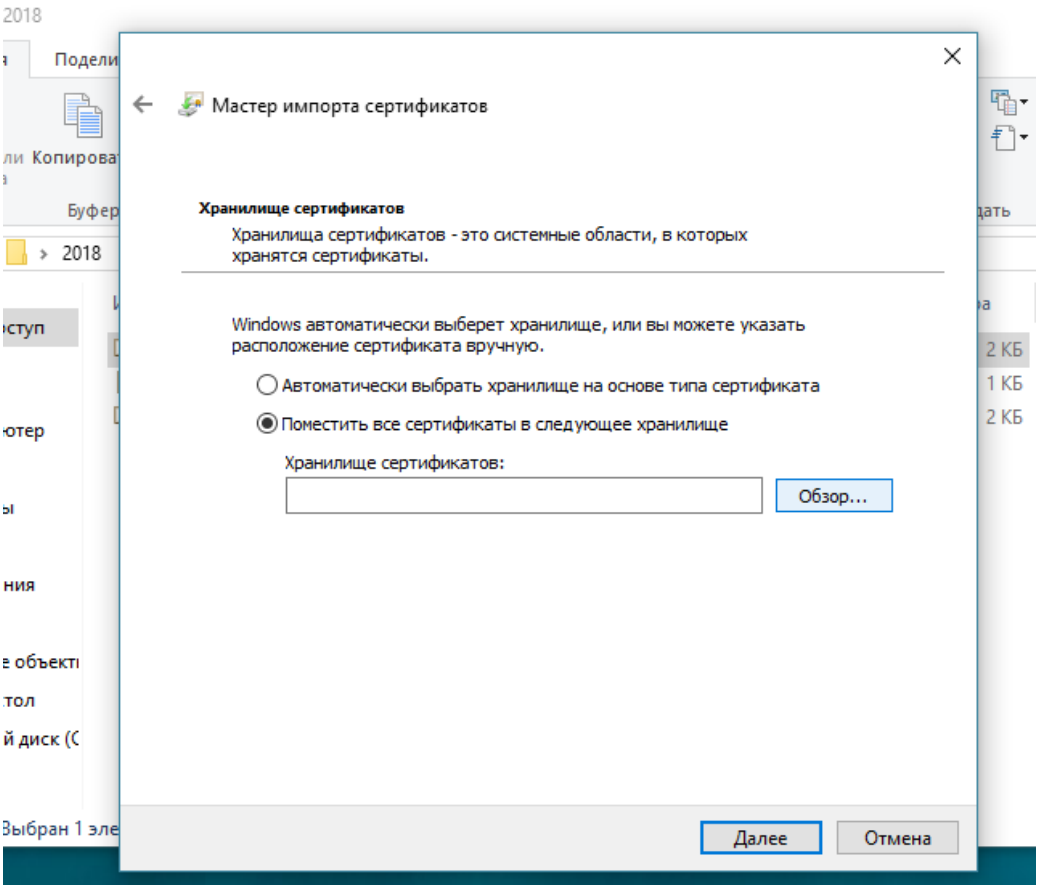

Рисунок 11 - Выбор хранилища для сертификата Удостоверяющего центра

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

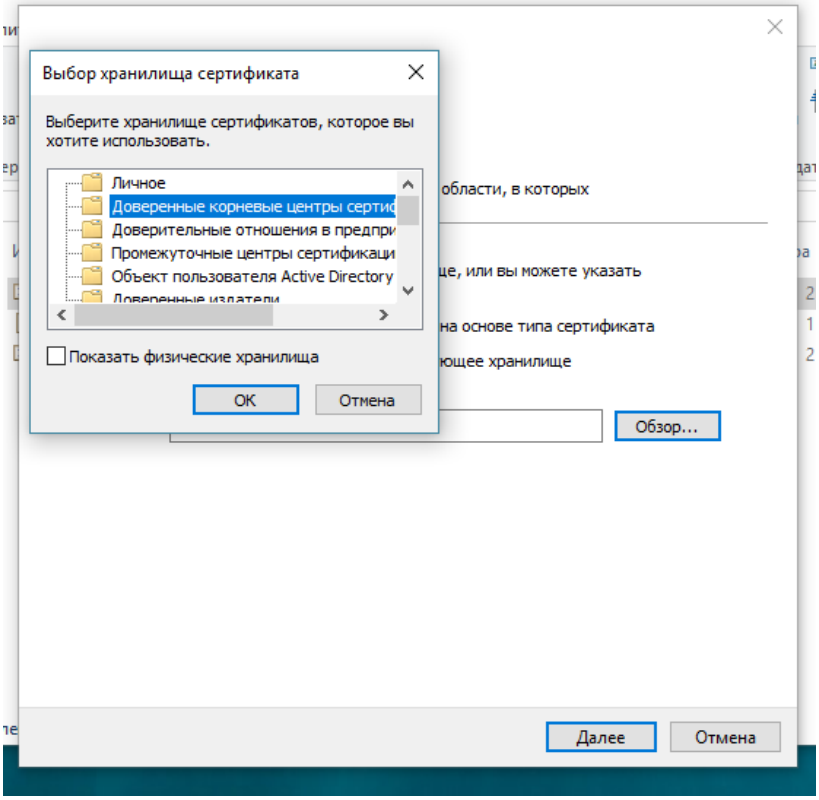

Рисунок 12 - Выбор хранилища для сертификата Удостоверяющего центра

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

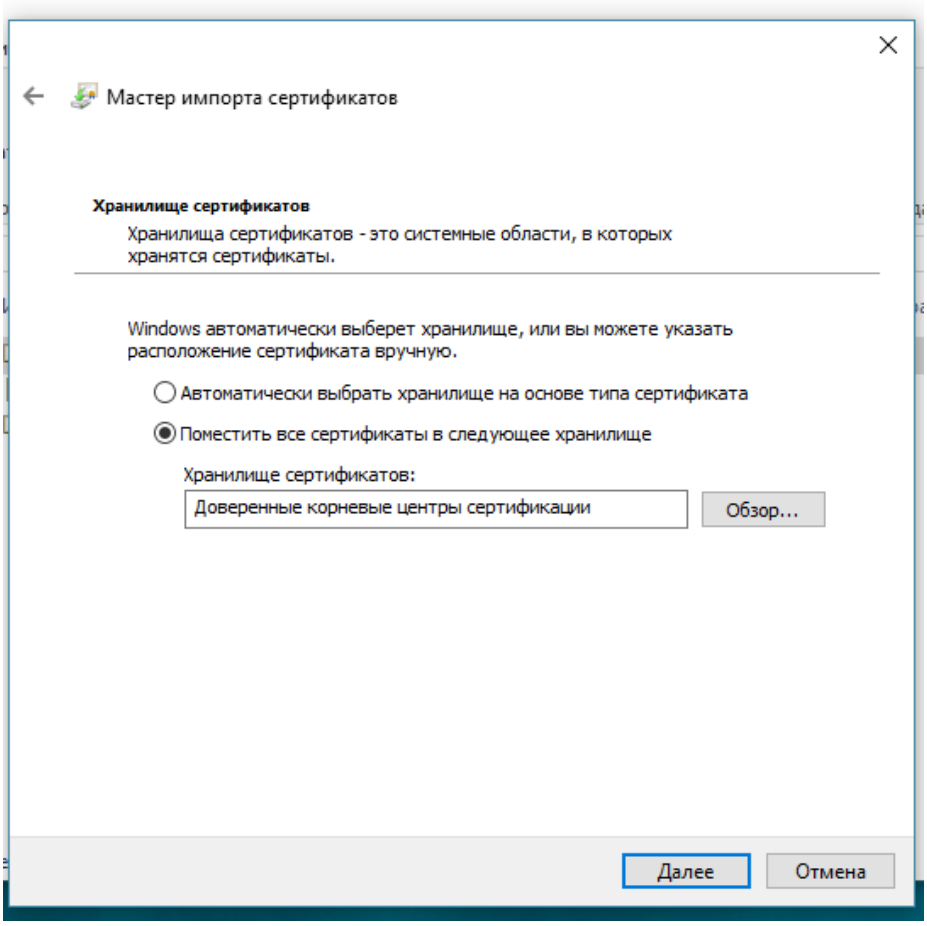

Рисунок 13 - Окно мастера импорта сертификатов

7. На следующей странице нажмите **Готово**.

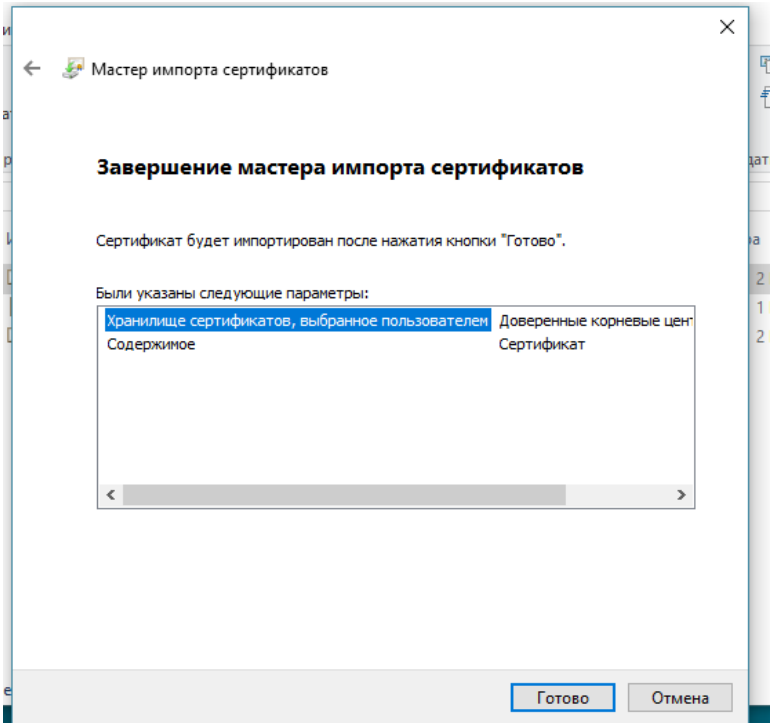

Рисунок 14 - Окно завершения работы мастера импорта сертификатов

9. В окне **Мастер импорта сертификатов** появится сообщение об успешном импорте сертификата. Нажмите **ОК**, установка завершена.

Установка СОС:

1. Откройте папку с файлом СОС 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 с сертификатами, в этом случае следует установить сертифицированную версию Windows.

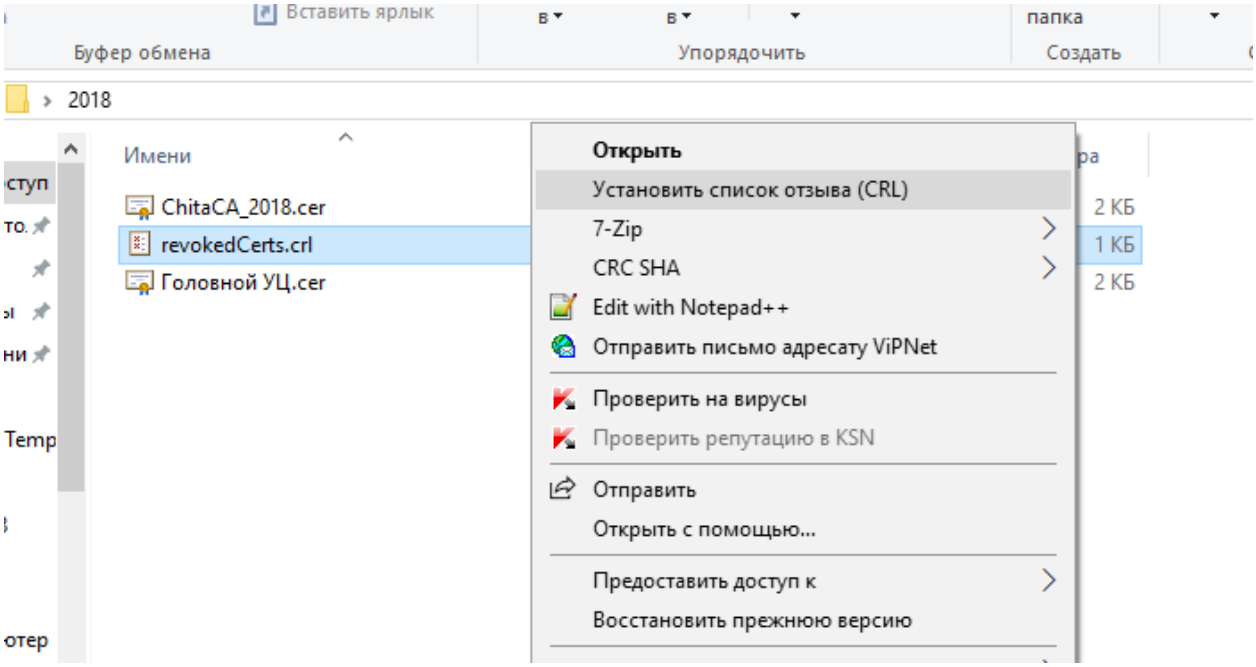

Рисунок 15 - Установка СОС

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.

Установка Головного УЦ:

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

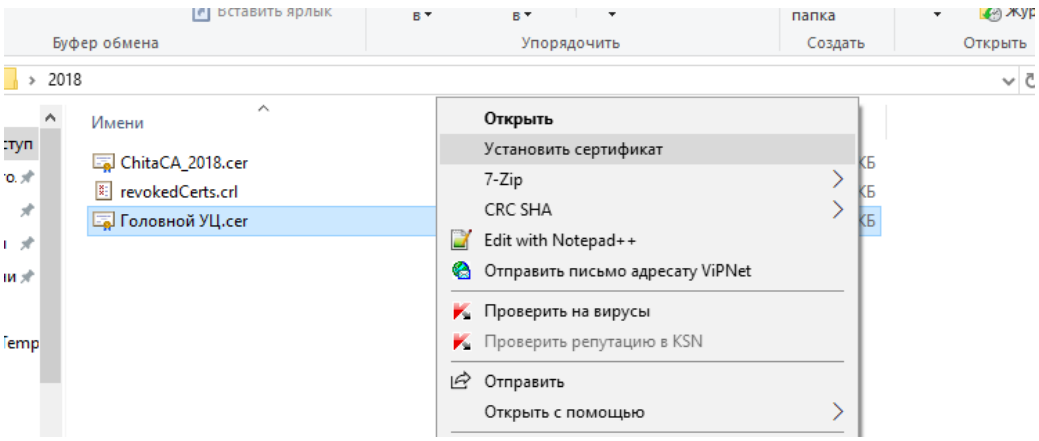

Рисунок 16 - Установка Головного УЦ

3. Установить сертификат Головной УЦ по тому же принципу, что и корневой сертификат Удостоверяющего центра.

Установка СОС Головного УЦ:

1. Откройте папку с файлом Список отзывы ГУЦ 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 с сертификатами, в этом случае следует установить сертифицированную версию Windows.

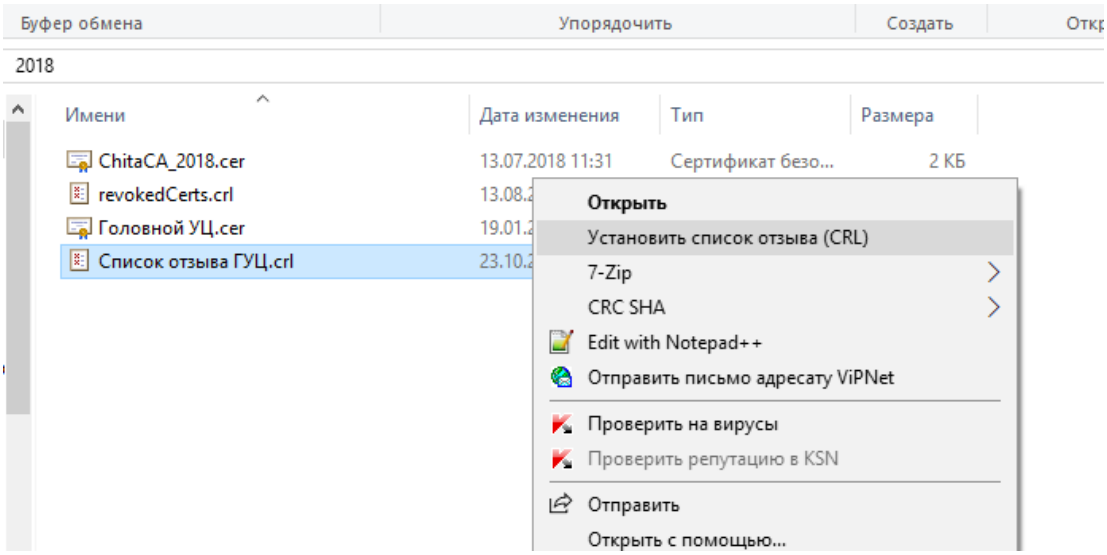

Рисунок 17 - Установка СОС Головного УЦ

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.