# Получение сертификатов для работы TSP/OCSP-сервера 1 1



# Получение сертификатов для работы TSP/OCSP-сервера

Для обработки TSP/OCSP-запросов и подписи формируемых ответов на TSP/OCSP-сервере должны быть установлены два

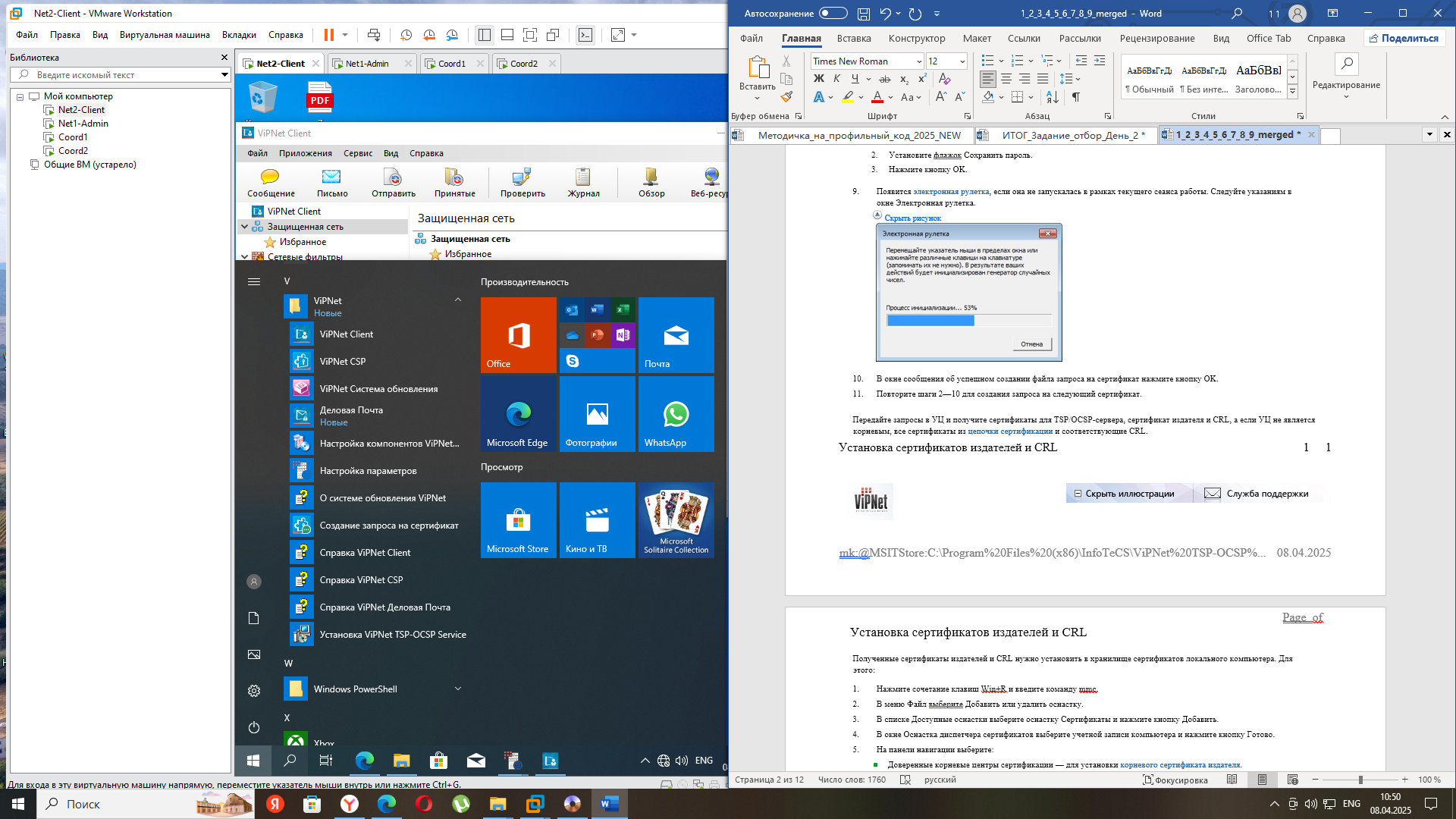
Чтобы получить сертификаты:

1. Создайте запрос с помощью криптопровайдера ViPNet CSP.
2. Передайте запросы в УЦ — администратору программы ViPNet УКЦ и получите сертификаты для TSP/OCSP-сервера, а также сертификат издателя и CRL, а если УЦ не является корневым, все сертификаты из цепочки сертификации и соответствующие CRL.
3. Установите сертификаты издателей и CRL в хранилище сертификатов Windows локального компьютера.
4. Установите сертификаты TSP/OCSP-сервера в контейнеры ключей и хранилище сертификатов Windows локального компьютера.

# Создание запроса на сертификат

Чтобы создать запрос на сертификат:

1. Запустите программу «Создание запроса на сертификат», входящую в комплект поставки программы ViPNet CSP.



1. В окне Служба сертификации выберите Запросить новый сертификат.
2. В разделе Параметры сертификата:

 В списке Криптопровайдер выберите криптопровайдер, с помощью которого вы хотите создать ключ ЭП и ключ проверки ЭП. При этом ниже отобразится используемый алгоритм хэширования.

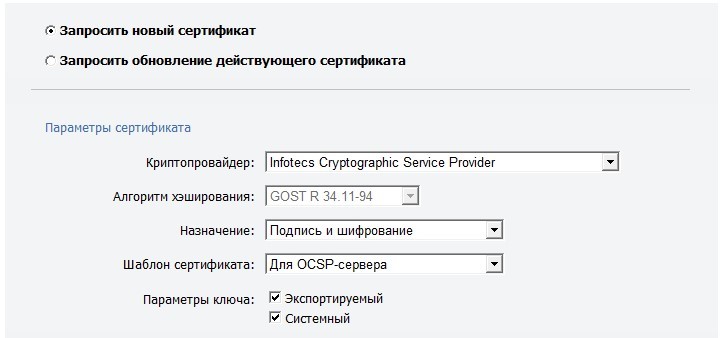
 В списке Назначение выберите Подпись и шифрование.

 В списке Шаблон сертификата выберите один из шаблонов.

 Чтобы в дальнейшем экспортировать вместе с полученным сертификатом ключ ЭП в файл формата PKCS#12, установите флажок Экспортируемый.

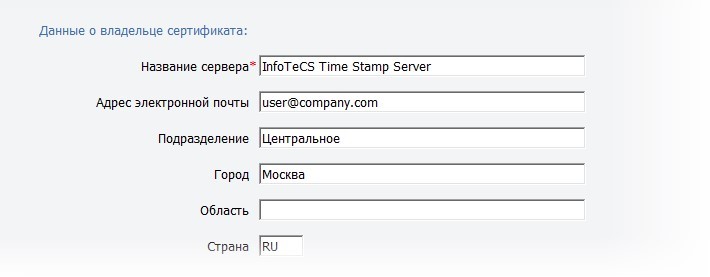
 Установите флажок Системный.

 Скрыть рисунок



1. В разделе Данные о владельце сертификата укажите информацию о сервере.

 Скрыть рисунок

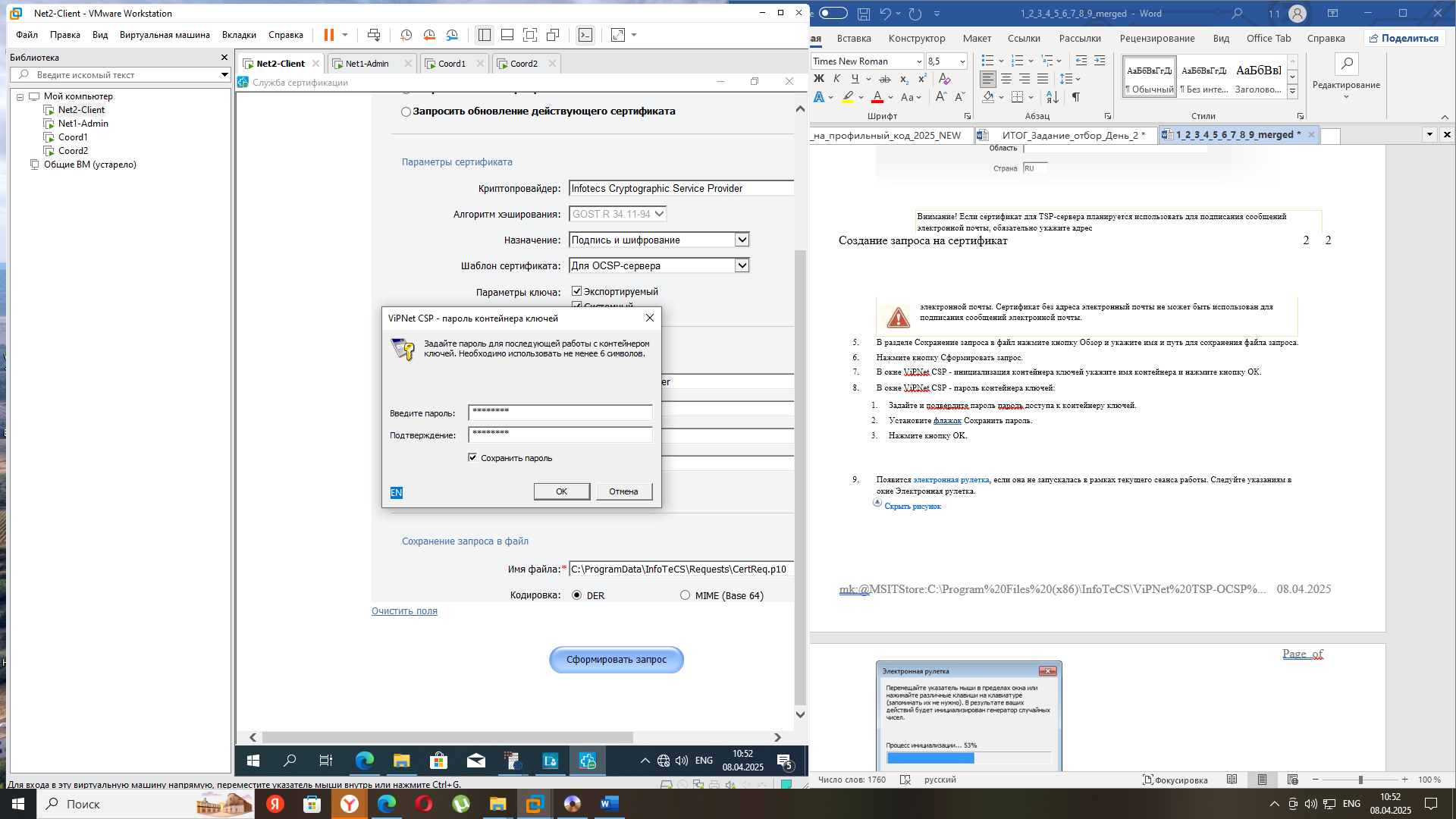


Внимание! Если сертификат для TSP-сервера планируется использовать для подписания сообщений электронной почты, обязательно укажите адрес

## Создание запроса на сертификат 2 2

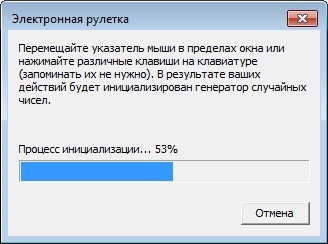
|  |
| --- |
| электронной почты. Сертификат без адреса электронный почты не может быть использован для подписания сообщений электронной почты. |

1. В разделе Сохранение запроса в файл нажмите кнопку Обзор и укажите имя и путь для сохранения файла запроса.
2. Нажмите кнопку Сформировать запрос.
3. В окне ViPNet CSP - инициализация контейнера ключей укажите имя контейнера и нажмите кнопку ОК.
4. В окне ViPNet CSP - пароль контейнера ключей:
   1. Задайте и подвердите пароль пароль доступа к контейнеру ключей.
   2. Установите флажок Сохранить пароль.
   3. Нажмите кнопку OK.

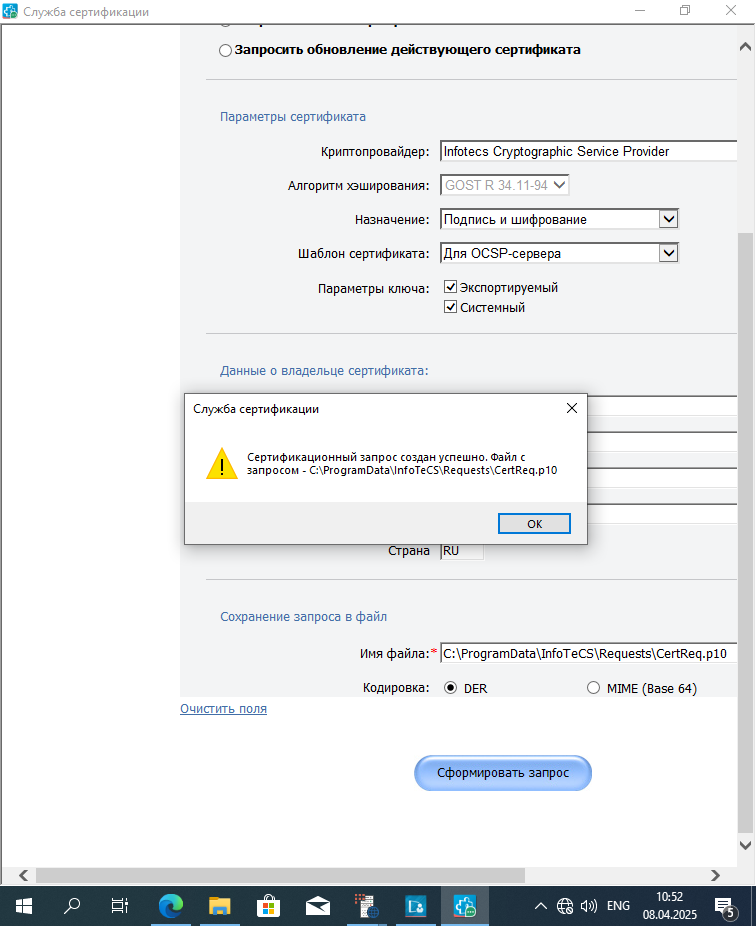


1. Появится электронная рулетка, если она не запускалась в рамках текущего сеанса работы. Следуйте указаниям в окне Электронная рулетка.

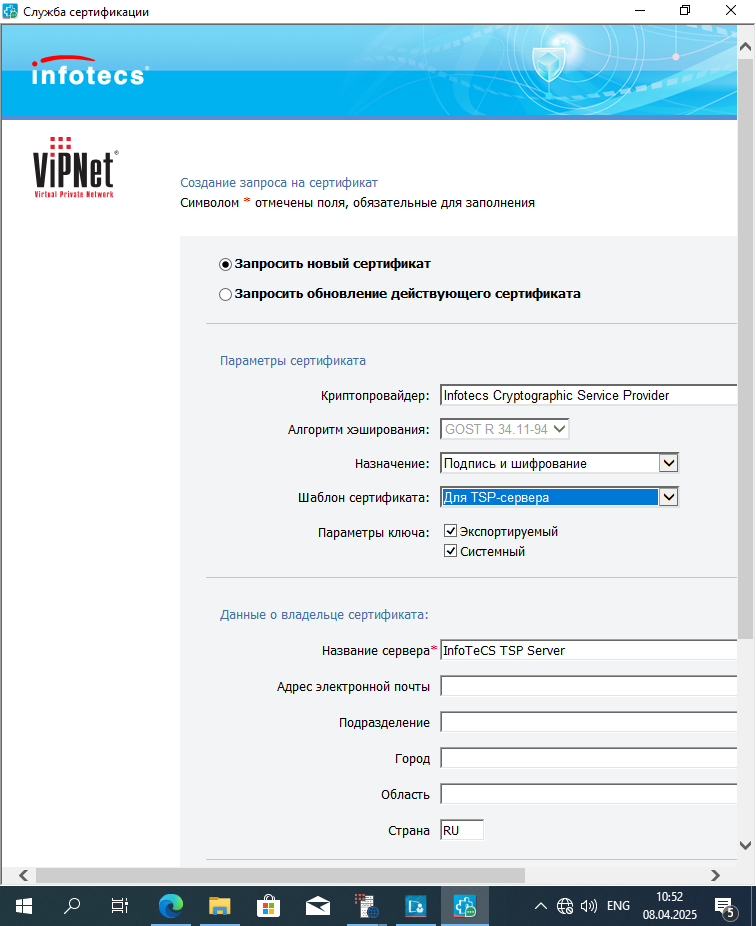
 Скрыть рисунок



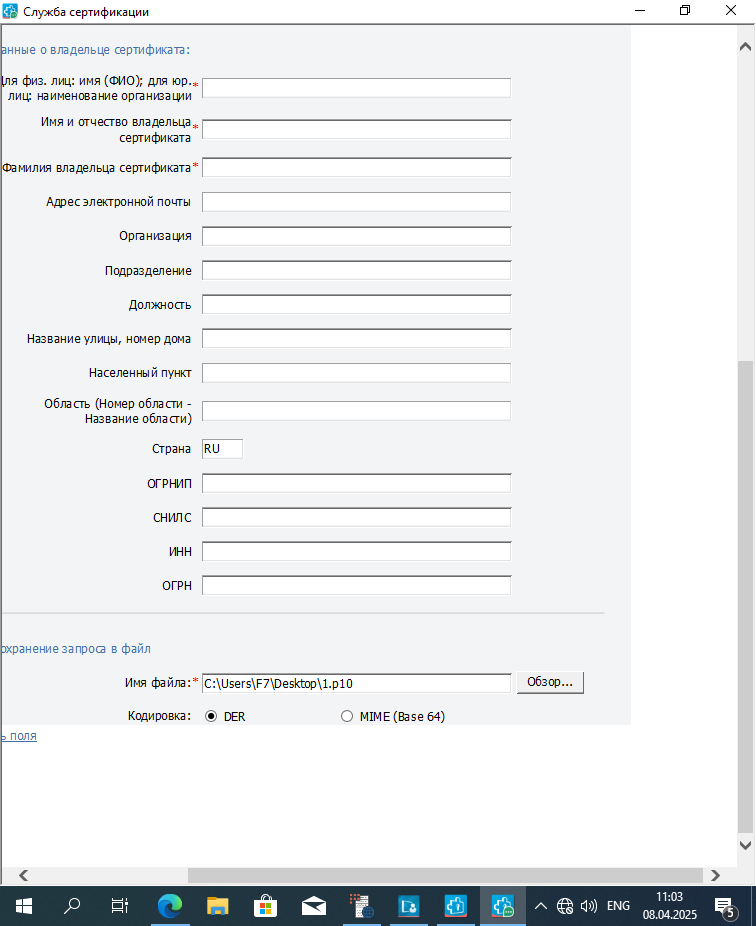
1. В окне сообщения об успешном создании файла запроса на сертификат нажмите кнопку OK.



1. Повторите шаги 2—10 для создания запроса на следующий сертификат.

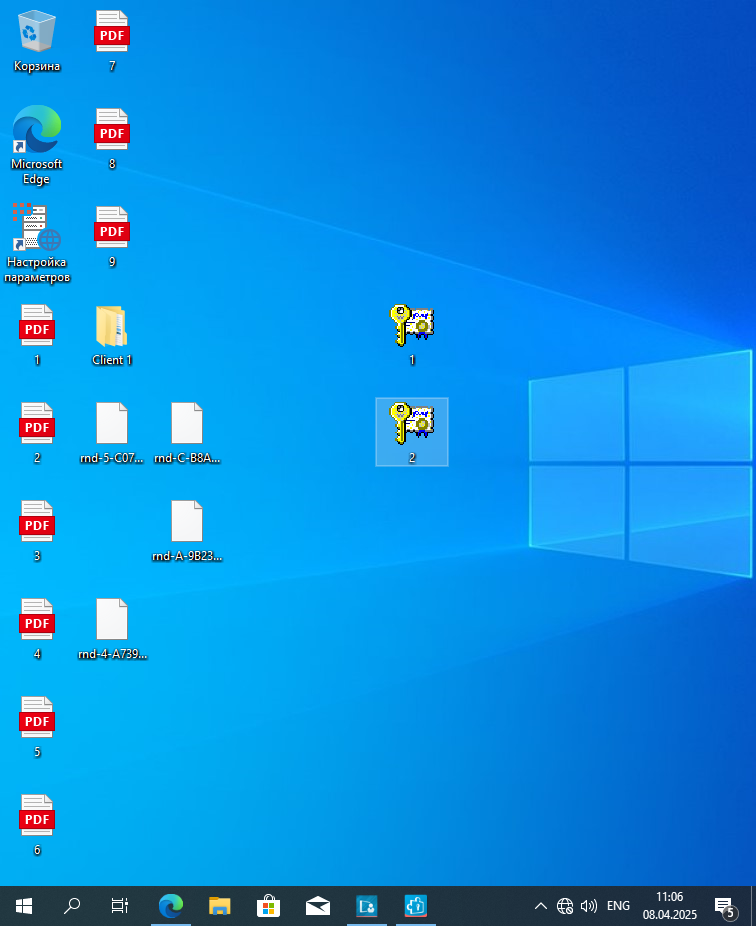


При сохранение запроса на сертификат обязательно меняем название файла!!!

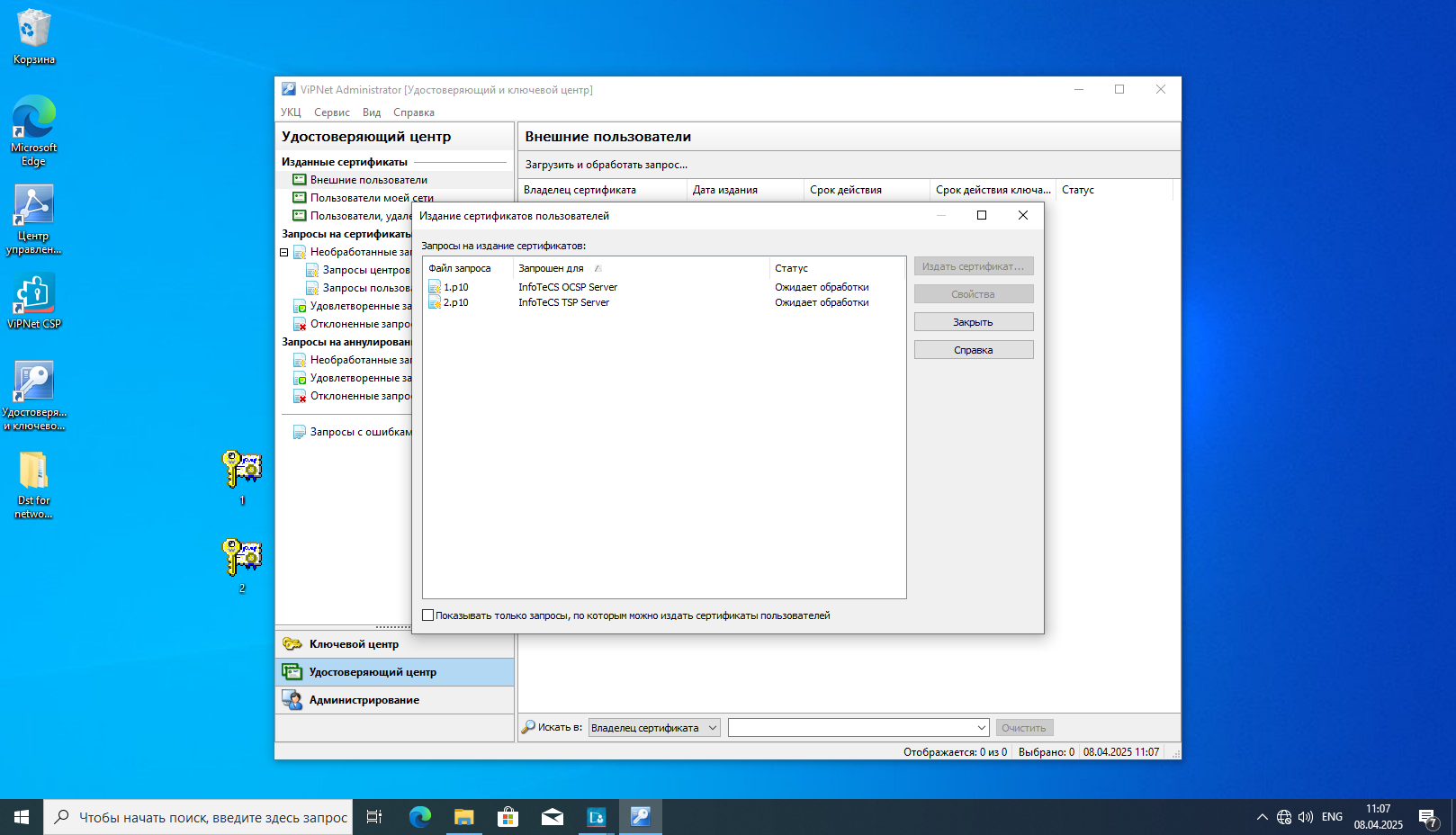


Передайте запросы в УЦ и получите сертификаты для TSP/OCSP-сервера, сертификат издателя и CRL, а если УЦ не является корневым, все сертификаты из цепочки сертификации и соответствующие CRL.

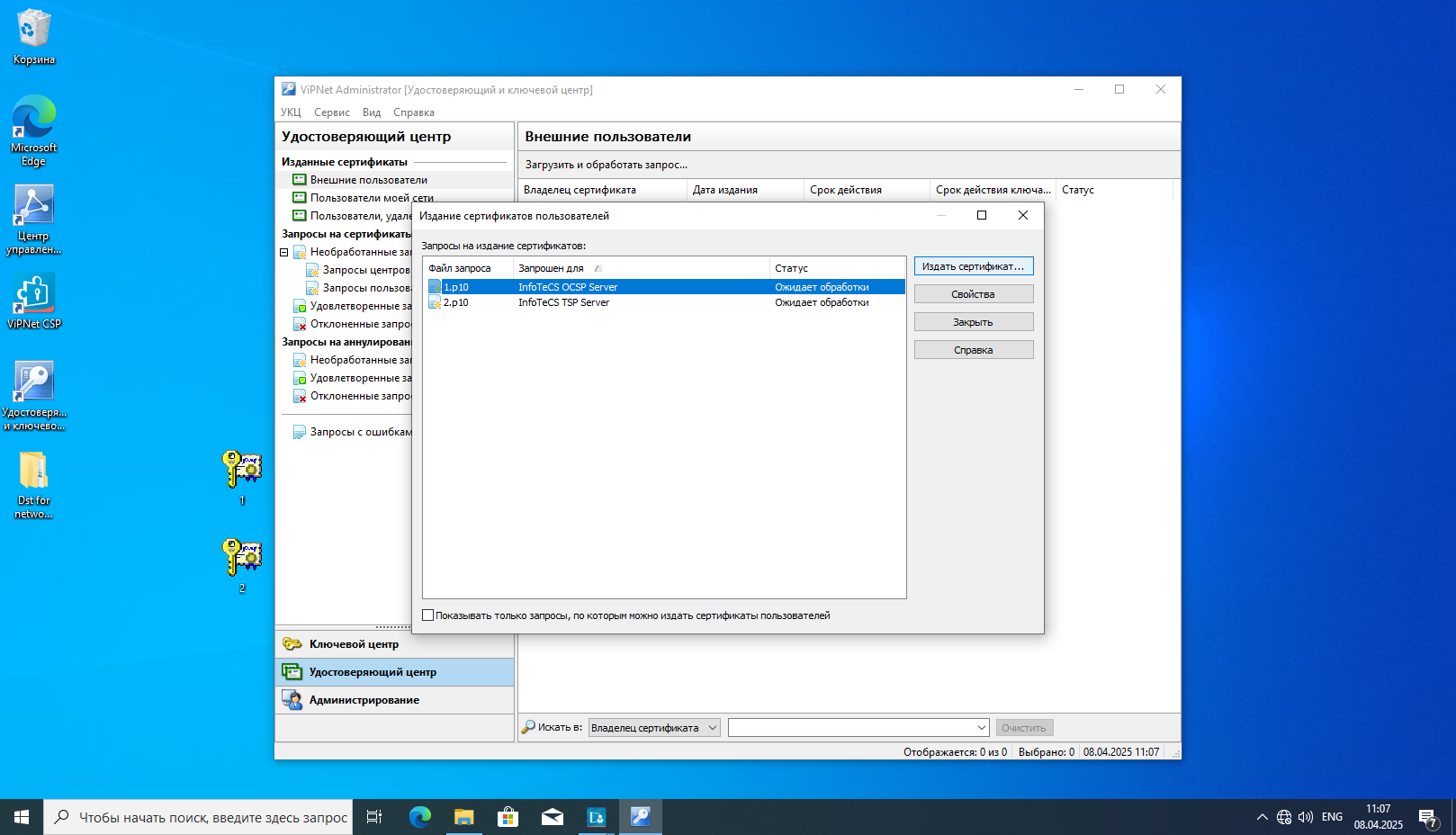
Появятся вот такие запросы



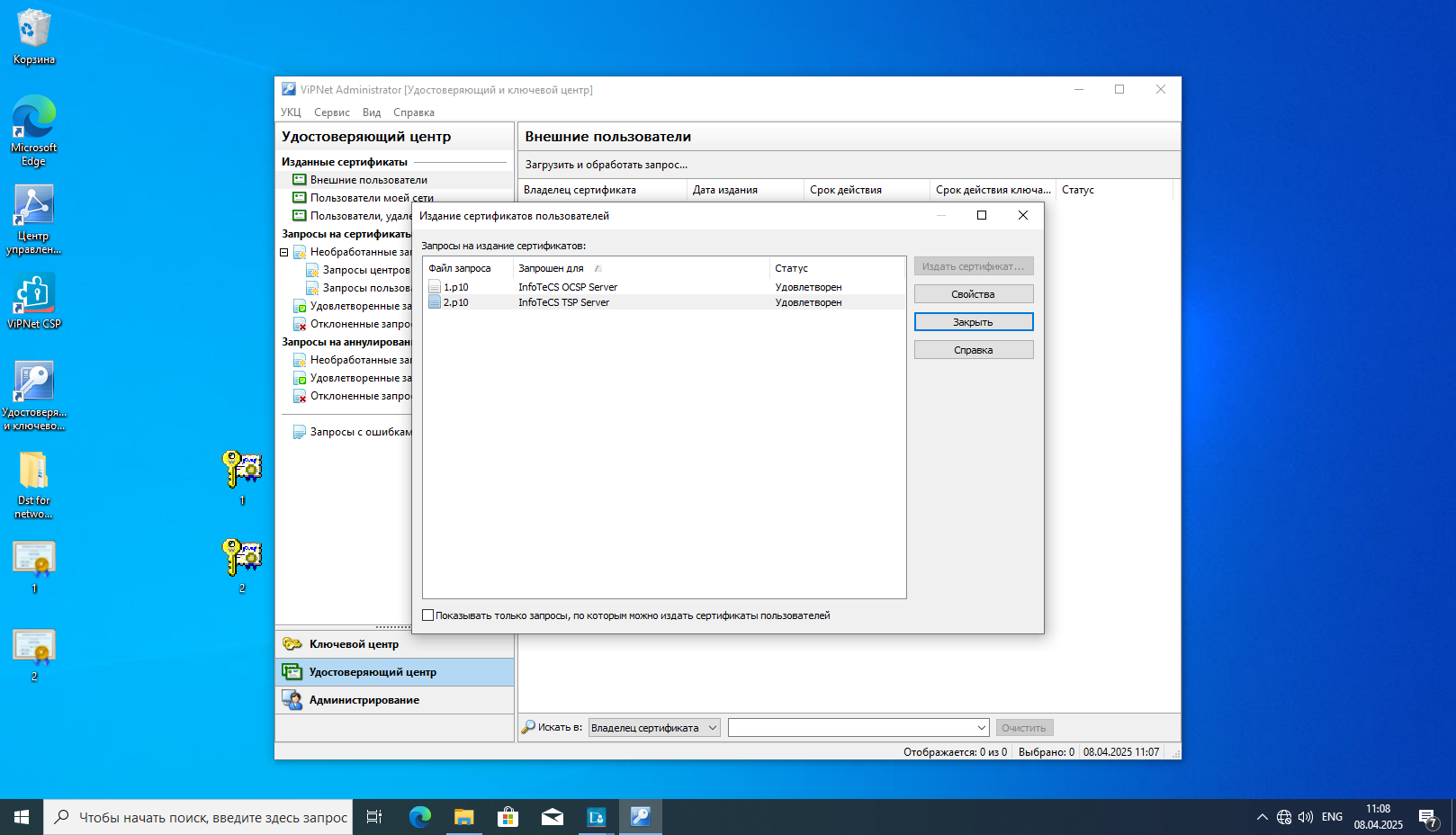
## Копируем эти файлы на Администратора и заходим в УЦ. На вкладке Удостоверяющий центр нажимаем Загрузить и обработать запрос и выбираем наши файлы.



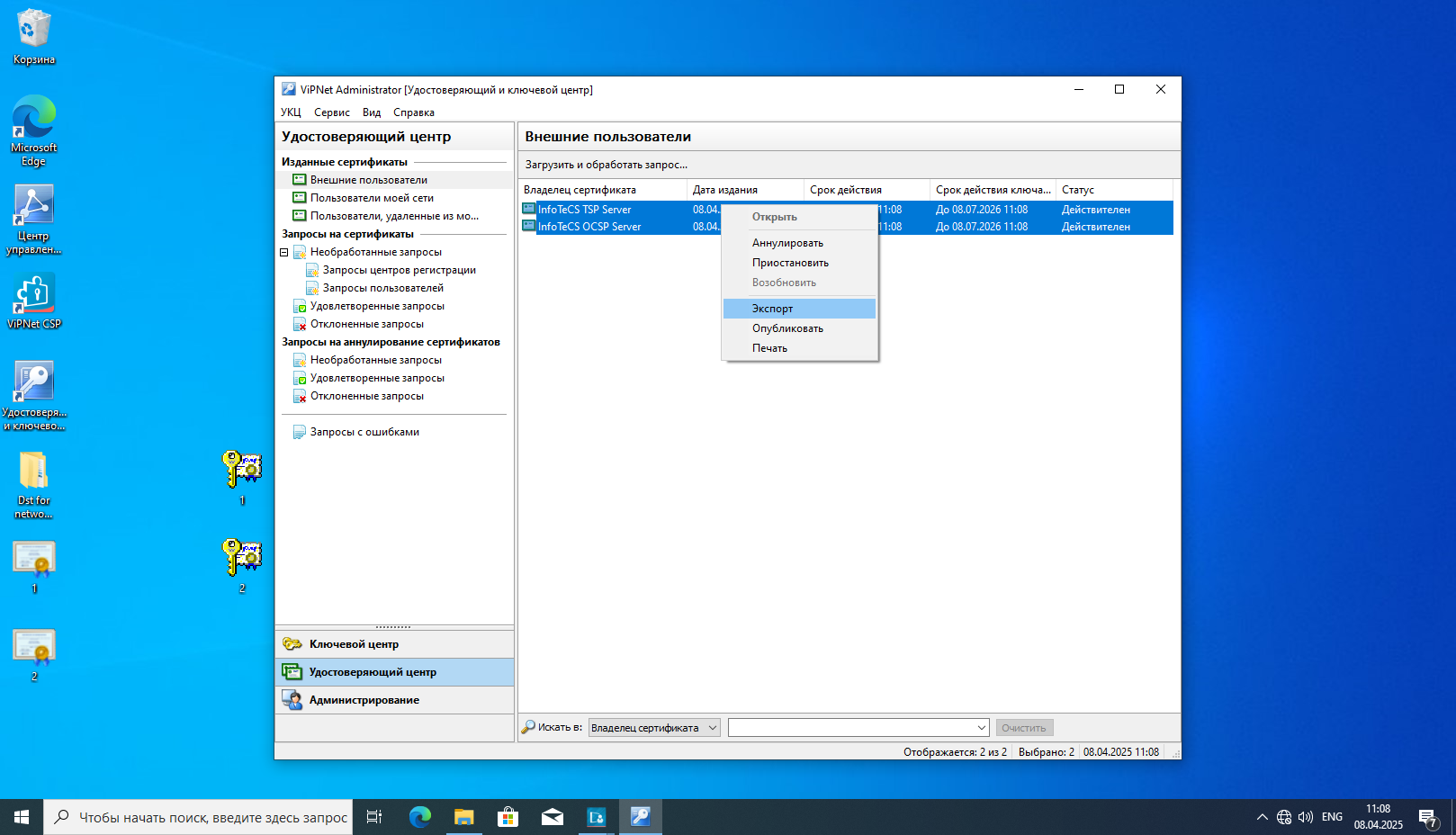
По очереди издаем сертификаты



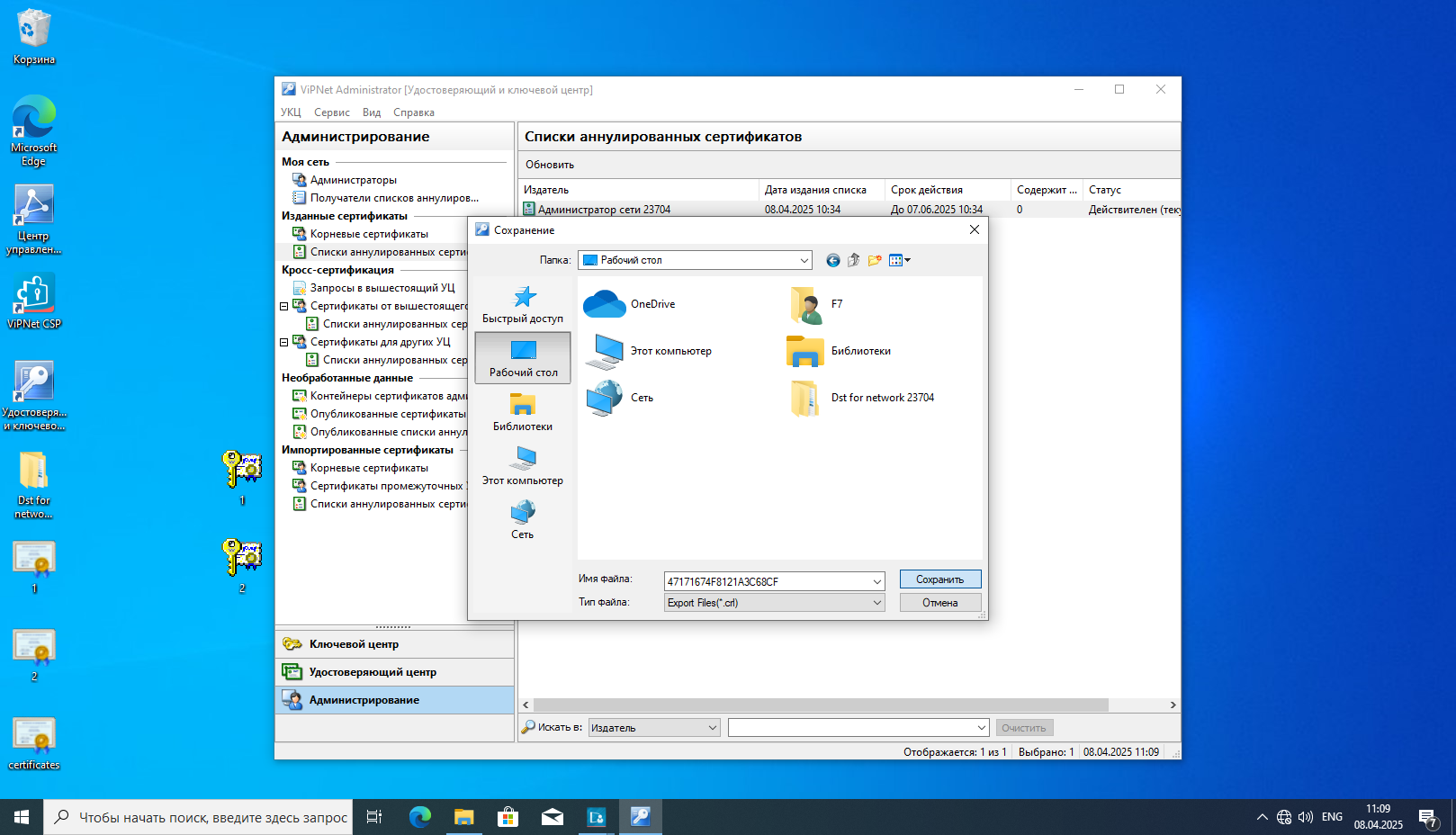
## 



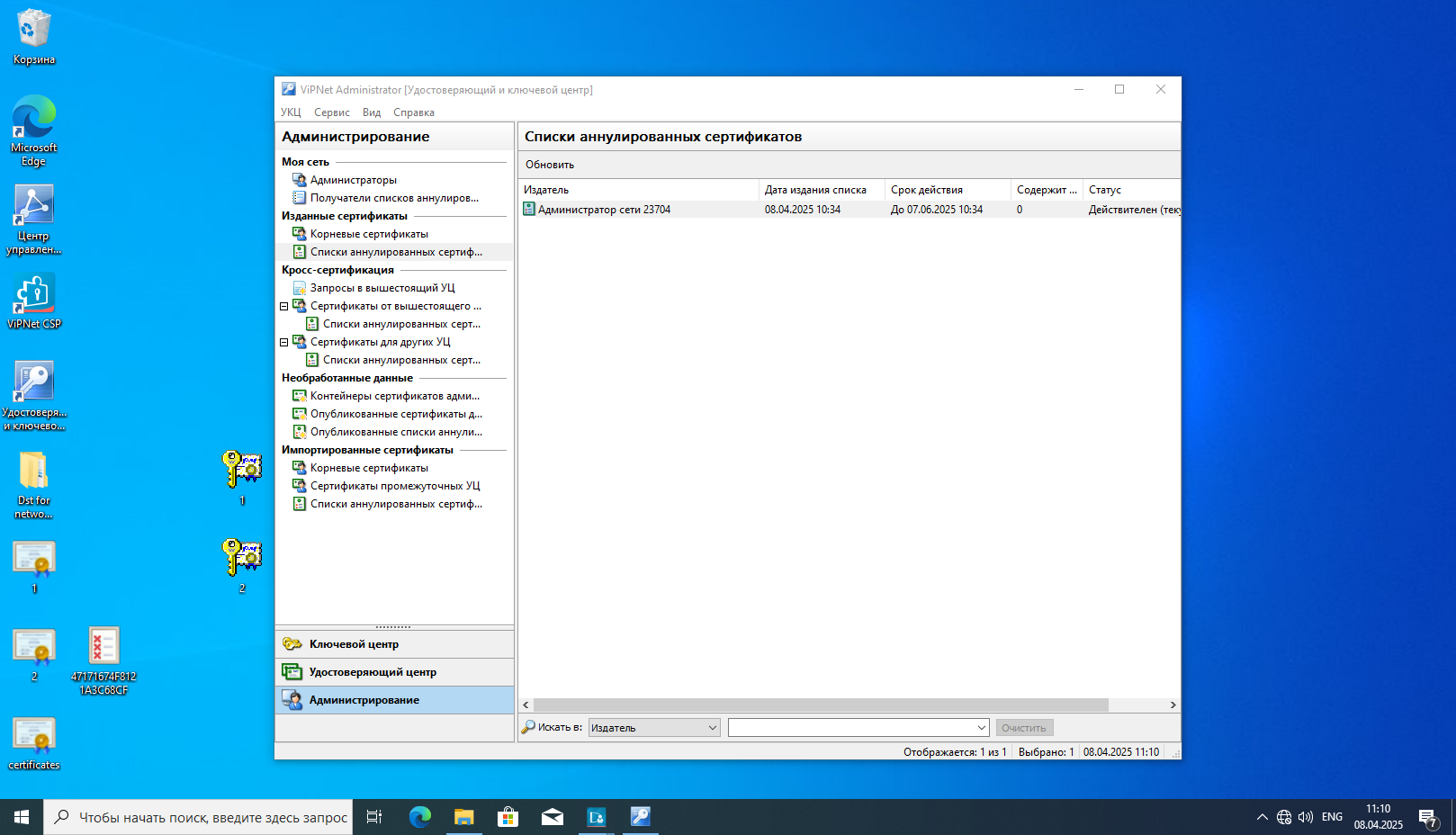
Нажимаем закрыть и экспортируем серификаты



На вкладке Администрирование – Изданные сертификаты – списки аннулированных сертификатов экспортируем сертификат админа



В итоге должно получиться 4 файла



## Теперь переходим на VM клиента и сначала устанавливаем сертификат админа и CRL

## Установка сертификатов издателей и CRL 1 1

# Установка сертификатов издателей и CRL

Полученные сертификаты издателей и CRL нужно установить в хранилище сертификатов локального компьютера. Для этого:

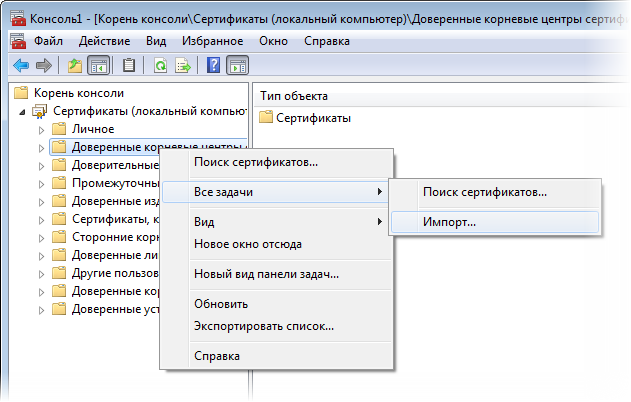
1. Нажмите сочетание клавиш Win+R и введите команду mmc.
2. В меню Файл выберите Добавить или удалить оснастку.
3. В списке Доступные оснастки выберите оснастку Сертификаты и нажмите кнопку Добавить.
4. В окне Оснастка диспетчера сертификатов выберите учетной записи компьютера и нажмите кнопку Готово.
5. На панели навигации выберите:

 Доверенные корневые центры сертификации — для установки корневого сертификата издателя.

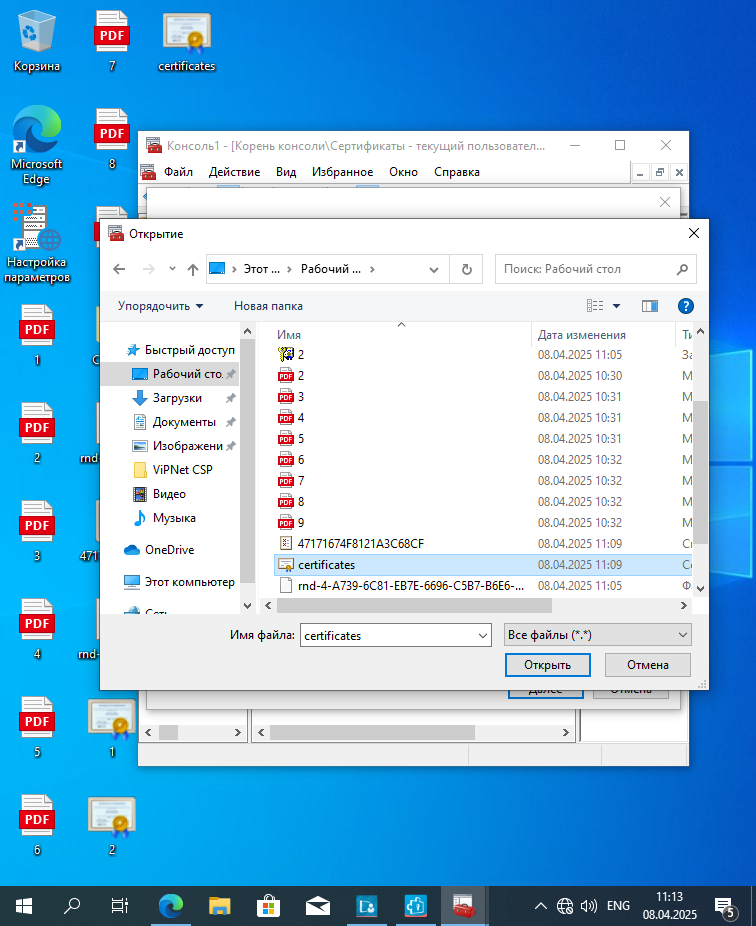
 Промежуточные центры сертификации — для установки промежуточного сертификата или CRL.

1. В контекстном меню выберите Все задачи > Импорт.

 Скрыть рисунок



1. На первой странице мастера нажмите кнопку Далее.
2. На странице Мастер импорта сертификатов выберите файл с сертификатом издателя или CRL.



1. На странице Хранилище сертификатов отобразится выбранное ранее хранилище сертификатов.
2. На странице Завершение мастера импорта сертификатов нажмите кнопку Готово.
3. Повторите шаги 5-10 для всех сертификатов издателей и CRL.

## Установка сертификатов TSP/OCSP-сервера 2

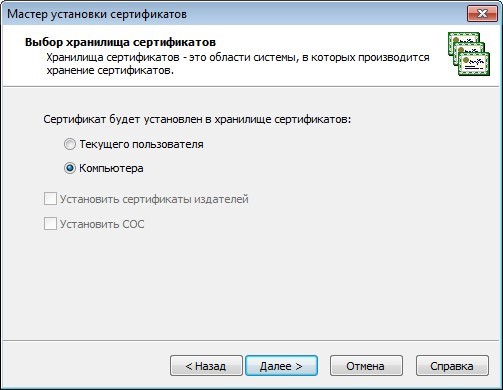


# Установка сертификатов TSP/OCSP-сервера

Полученные сертификаты TSP/OCSP-сервера нужно установить в контейнеры ключей и хранилище сертификатов локального компьютера. Для этого:

1. Запустите криптопровайдер ViPNet CSP от имени администратора.
2. Установите сертификаты в контейнер ключей:
   1. В окне ViPNet CSP в разделе Контейнеры ключей в списке выберите Ключи компьютера.
   2. В списке ниже выберите контейнер ключей и нажмите кнопку Добавить сертификат из файла.
   3. Выберите сертификат и нажмите кнопку Открыть.
   4. Введите пароль контейнера ключей и нажмите кнопку ОК.
   5. Повторите шаги 2.2–2.4 для другого сертификата.
3. Установите сертификаты в хранилище сертификатов локального компьютера:
   1. В окне ViPNet CSP в разделе Контейнеры ключей нажмите кнопку Установить сертификат и укажите путь к файлу сертификата.
   2. На странице Выбор хранилища сертификатов установите переключатель в положение Компьютера.

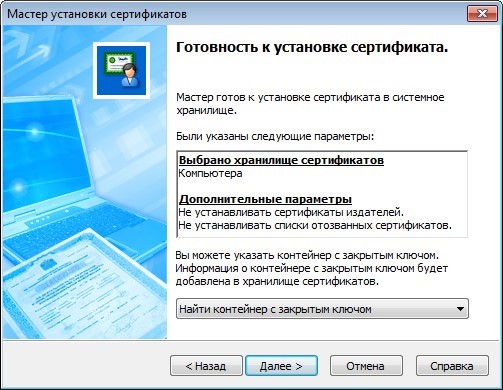
 Скрыть рисунок



* 1. На странице Готовность к установке сертификата выберите пункт Найти контейнер с закрытым ключом.

 Скрыть рисунок

## Установка сертификатов TSP/OCSP-сервера 2 2



1. На последней странице мастера нажмите кнопку Готово.
2. Повторите шаги 3.1—3.4 для другого сертификата.

## Настройка подключения к TSP/OCSP-серверу 1

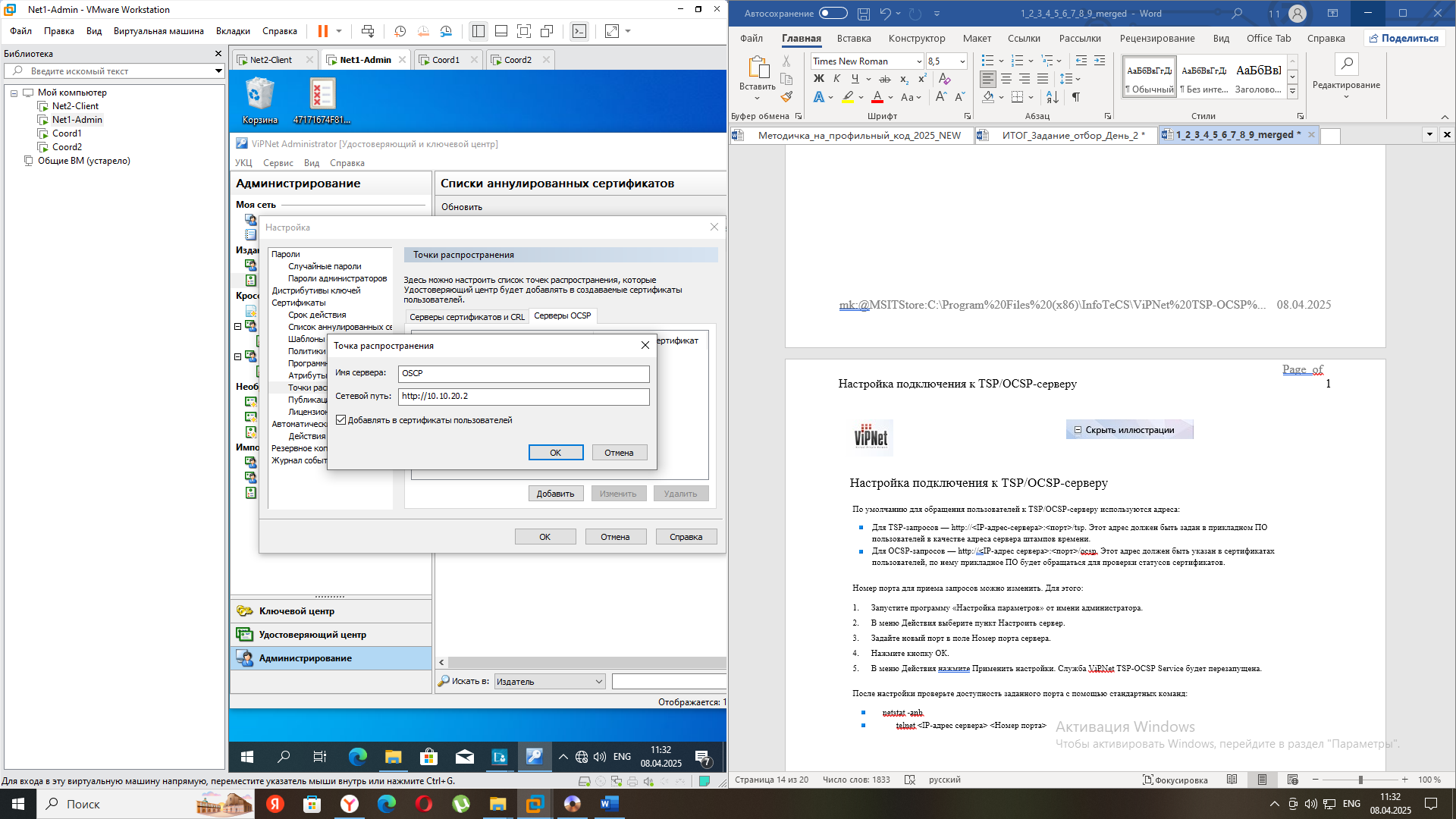


# Настройка подключения к TSP/OCSP-серверу

По умолчанию для обращения пользователей к TSP/OCSP-серверу используются адреса:

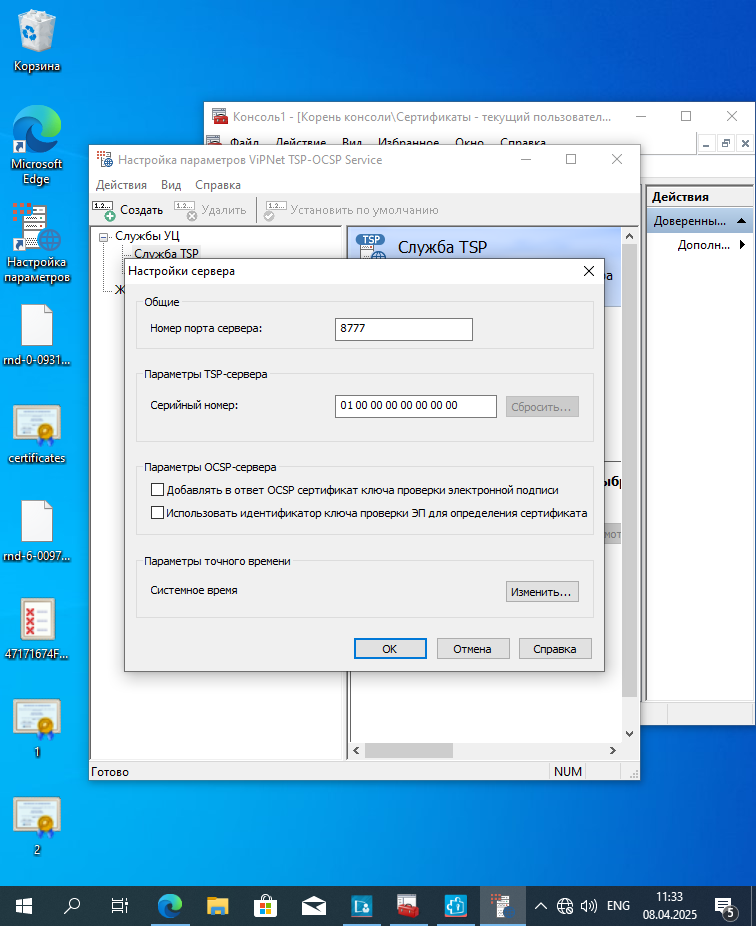
 Для TSP-запросов — http://<IP-адрес-сервера>:<порт>/tsp. Этот адрес должен быть задан в прикладном ПО пользователей в качестве адреса сервера штампов времени.

* Для OCSP-запросов — http://<IP-адрес сервера>:<порт>/ocsp. Этот адрес должен быть указан в сертификатах пользователей, по нему прикладное ПО будет обращаться для проверки статусов сертификатов.



Номер порта для приема запросов можно изменить. Для этого:

1. Запустите программу «Настройка параметров» от имени администратора.
2. В меню Действия выберите пункт Настроить сервер.
3. Задайте новый порт в поле Номер порта сервера.



1. Нажмите кнопку ОК.
2. В меню Действия нажмите Применить настройки. Служба ViPNet TSP-OCSP Service будет перезапущена.

После настройки проверьте доступность заданного порта с помощью стандартных команд:

 netstat -anb

 telnet <IP-адрес сервера> <Номер порта>

## Настройка OCSP-сервера 1



# Настройка OCSP-сервера

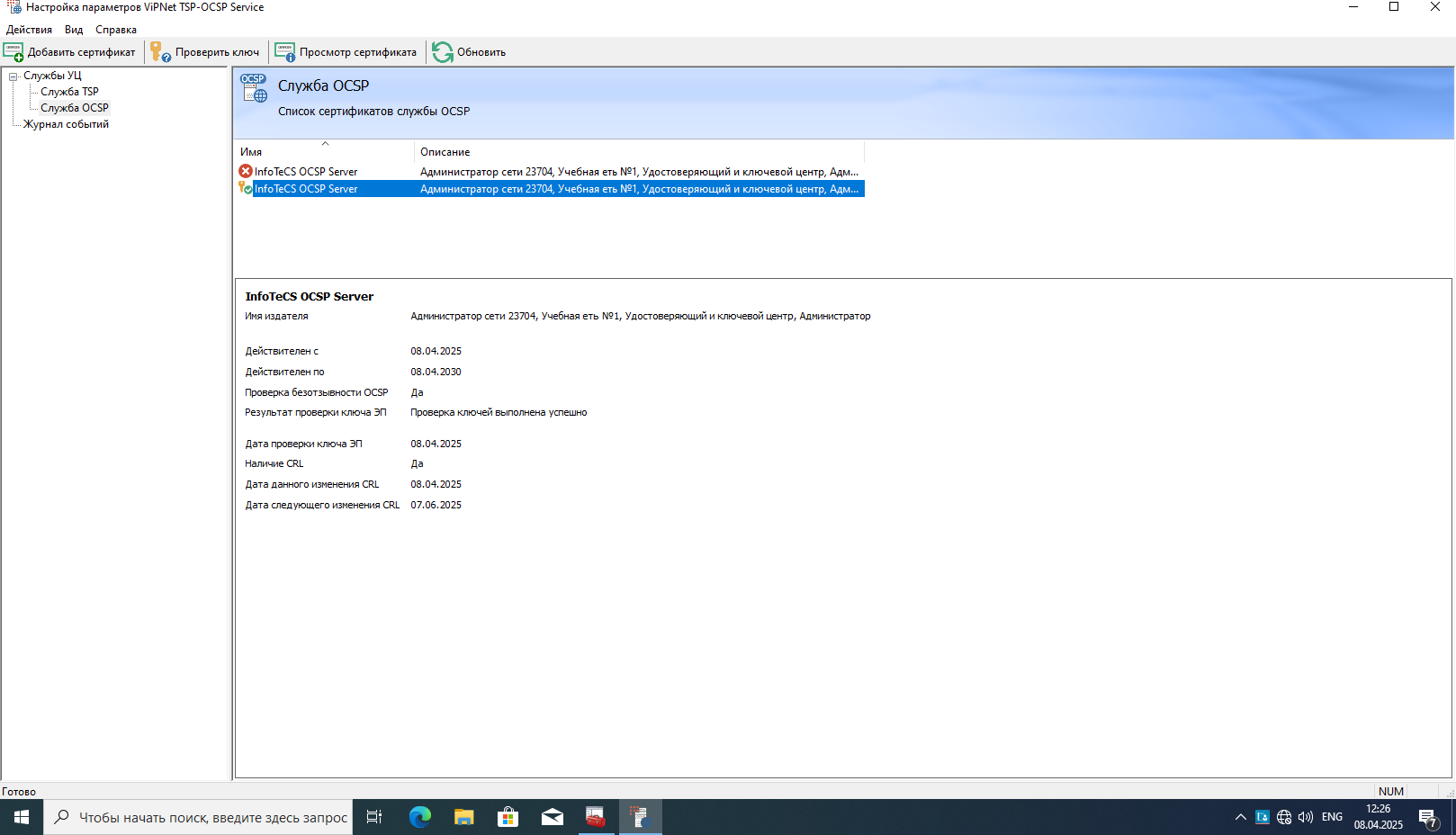
Чтобы настроитьOCSP-сервер:

1. Запустите программу «Настройка параметров» от имени администратора.
2. В меню Действия выберите пункт Настроить сервер.
3. В группе Параметры OCSP-сервера:

 Чтобы сертификат OCSP-сервера добавлялся в ответы на OCSP-запросы, установите флажок Добавлять в ответ OCSP сертификат. Это позволит проверять OCSP-ответы на стороне пользователей.

 Чтобы при получении OCSP-запросов политики их обработки автоматически определялись на основе расширений запросов и политик, содержащихся в сертификате OCSP-сервера, установите флажок Использовать идентификатор ключа проверки ЭП для определения сертификата, .

1. По окончании настройки нажмите кнопку ОК.
2. В меню Действия нажмите кнопку Применить настройки. Служба ViPNet TSP-OCSP Service будет перезапущена.



## Настройка параметров обработки TSP-запросов 2

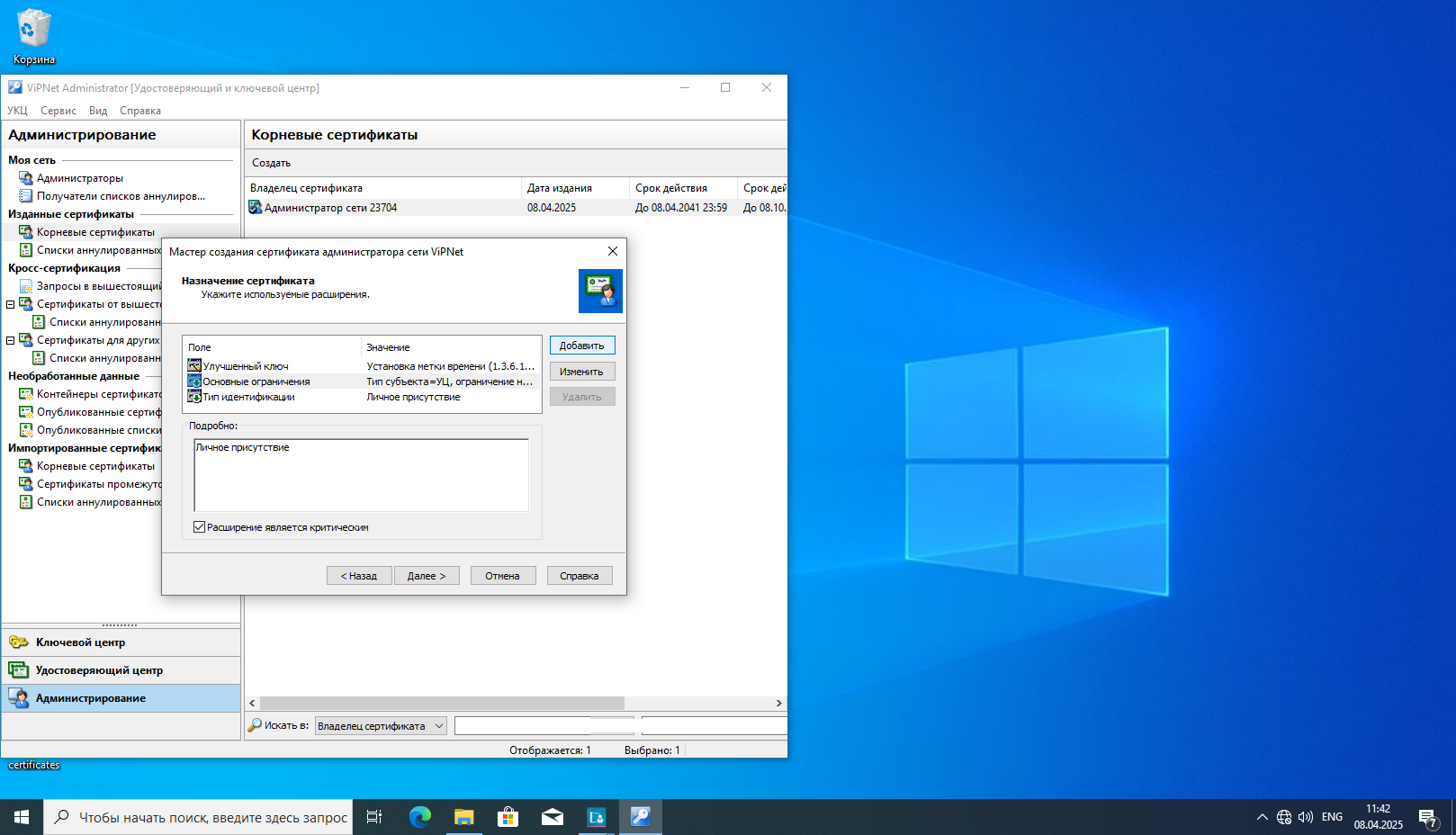


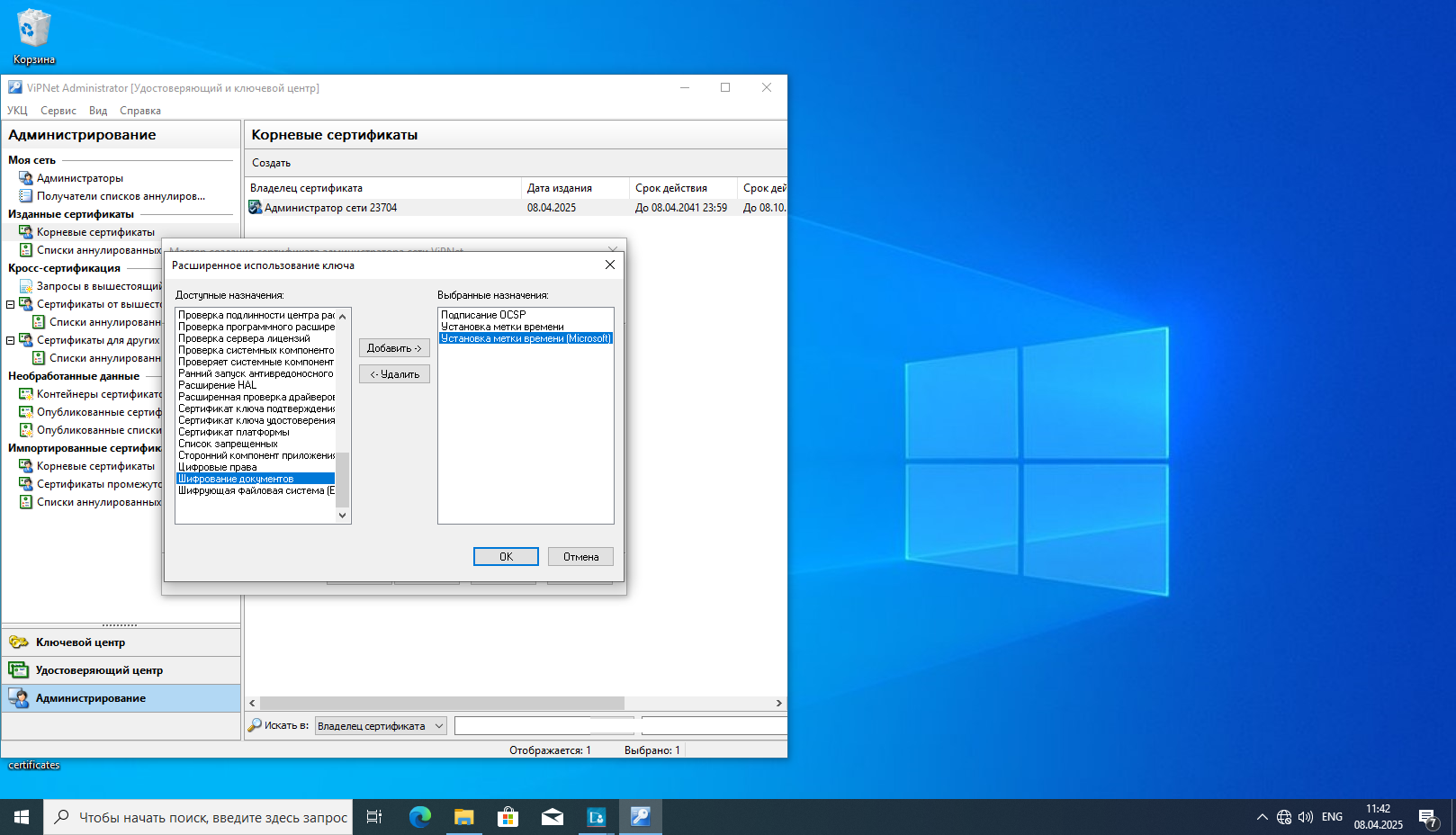
## Настройка параметров обработки TSP-запросов

Обработка TSP-запросов (выдача штампов времени пользователям) производится в соответствии с определенной политикой штампов времени. Политика обработки TSP-запроса может быть указана в самом запросе в виде идентификатора. Если поступивший запрос не содержит идентификатора политики, то ViPNet TSP/OCSP-сервер использует для его обработки свою политику, выбранную по умолчанию. Подробнее см. раздел Процесс обработки TSP-запросов.

В связи с этим перед началом обработки TSP-запросов сервером требуется указать идентификаторы объектов (OID) подходящих политик штампов времени и одну из них назначить политикой по умолчанию.

Вы можете указать идентификаторы нескольких политик с разным назначением, например:





 Политика для тестовых штампов. Штампы по этой политике выдаются всем пользователям, но могут использоваться только для тестовых целей (то есть для реальной системы документооборота такие штампы будут непригодны).

 Основная политика штампов. Штампы по этой политике выдаются всем пользователям, при этом в системе документооборота такие штампы могут быть использованы для документов, не являющихся важными.

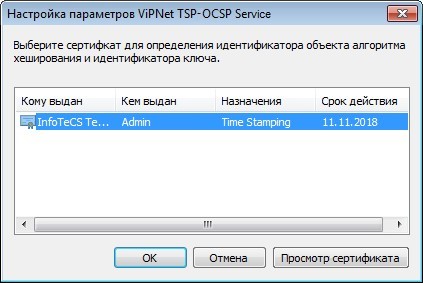
 Точная политика штампов. Штампы по этой политике выдаются пользователям, допущенным к работе с важными документами. Системой документооборота такие штампы будут приниматься для любых документов.

Для указания подходящих идентификаторов политик необходимо наличие на сервере установленных сертификатов, в которых содержатся эти политики (см. Получение сертификатов для работы ViPNet TSP/OCSP-сервера).

Чтобы настроить параметры обработки TSP-запросов:

1. В программе «Настройка параметров» укажите сертификат TSP-сервера:
   1. Перейдите в раздел Служба TSP.
   2. На панели свойств нажмите кнопку Выбрать сертификат.
   3. Выберите сертификат и нажмите кнопку OK.

 Скрыть рисунок

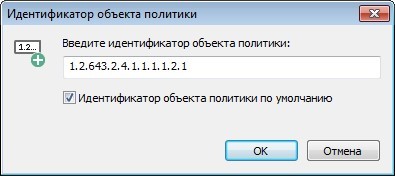


На панели свойств отобразится информация о выбранном сертификате.

1. Укажите идентификаторы объектов (OID) политик, в соответствии с которыми будут обрабатываться TSP-запросы:
   1. На панели инструментов нажмите кнопку  Создать.
   2. Введите идентификатор политики.
   3. Чтобы политика с заданным идентификатором использовалась по умолчанию, установите флажок Идентификатор объекта политики по умолчанию.
   4. Нажмите кнопку OK.

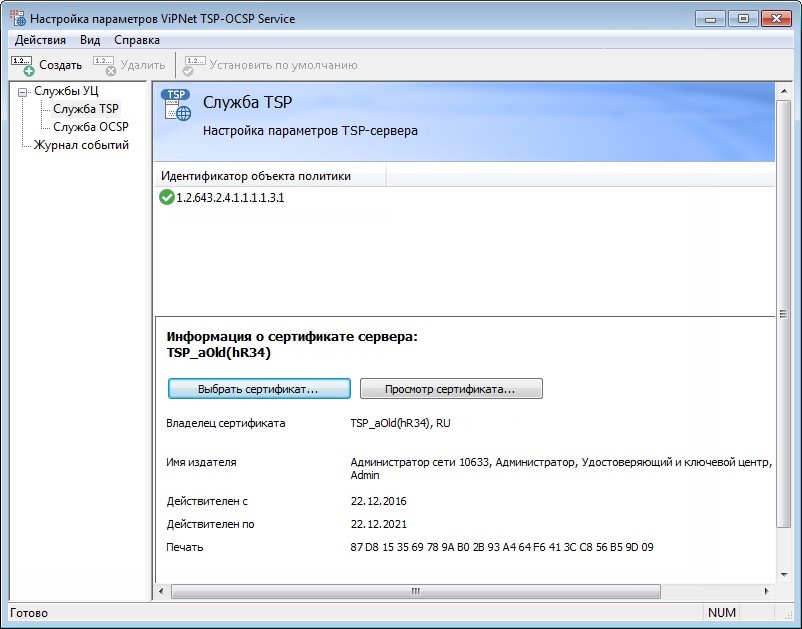
### Настройка параметров обработки TSP-запросов 2 2

 Скрыть рисунок



Аналогичным образом добавьте идентификаторы объектов всех нужных политик.

 Скрыть рисунок



Чтобы переназначить политику по умолчанию, в контекстном меню политики выберите пункт По умолчанию либо на панели инструментов нажмите кнопку Установить по умолчанию. Идентификатор политики, выбранной по умолчанию, будет отмечен знаком .



|  |
| --- |
| Внимание! Всегда назначайте идентификатор политики по умолчанию, иначе запросы, не содержащие идентификатор политики, обрабатываться не будут. |

Чтобы удалить идентификатор объекта политики, выберите его в списке и нажмите кнопку  Удалить.

### Настройка OCSP-сервера 1



# Настройка OCSP-сервера

Чтобы настроитьOCSP-сервер:

1. Запустите программу «Настройка параметров» от имени администратора.
2. В меню Действия выберите пункт Настроить сервер.
3. В группе Параметры OCSP-сервера:

 Чтобы сертификат OCSP-сервера добавлялся в ответы на OCSP-запросы, установите флажок Добавлять в ответ OCSP сертификат. Это позволит проверять OCSP-ответы на стороне пользователей.

 Чтобы при получении OCSP-запросов политики их обработки автоматически определялись на основе расширений запросов и политик, содержащихся в сертификате OCSP-сервера, установите флажок Использовать идентификатор ключа проверки ЭП для определения сертификата, .

1. По окончании настройки нажмите кнопку ОК.
2. В меню Действия нажмите кнопку Применить настройки. Служба ViPNet TSP-OCSP Service будет перезапущена.

## Проверка работоспособности ViPNet TSP/OCSP-сервера 1 2



# Проверка работоспособности ViPNet TSP/OCSP-сервера

После настройки TSP/OCSP-сервера проверьте его работоспособность.

## Проверка TSP-сервера

Для проверки можно использовать любое прикладное ПО для подписи файлов и поддержкой штампов времени, например, ViPNet PKI Client. Для этого в программе ViPNet PKI Client настройте подключение к службе штампов времени (TSP-серверу) и подпишите файл (см. документ «ViPNet PKI Client File Unit. Руководство пользователя»). Если настройка параметров TSP была выполнена корректно, к подписанному в программе ViPNet PKI Client файлу будет добавлен штамп точного времени.

## Проверка OCSP-сервера

|  |
| --- |
| Внимание! Для проверки работоспособности OCSP-сервера потребуется изменить настройки программы ViPNet Удостоверяющий и ключевой центр, чтобы получить сертификат, содержащий адрес вашего OCSP-сервера. Поэтому издавайте сертификат в тестовом контуре или приостановите издание сертификатов на время проверки. |

Для проверки потребуется сертификат пользователя, в котором содержится адрес OCSP-сервера (поле Доступ к информации о центрах сертификации). Чтобы издать такой сертификат:

1. В программе ViPNet Удостоверяющий и ключевой центр (далее — УКЦ) настройте добавление адреса вашего OCSP-сервера в издаваемые сертификаты. Подробнее см. документ «ViPNet Удостоверяющий и ключевой центр. Руководство администратора».
2. С помощью криптопровайдера ViPNet CSP создайте запрос и издайте сертификат в УКЦ.
3. Получите изданный сертификат пользователя и сертификат издателя, а если УЦ не является корневым, все сертификаты из цепочки сертификации.



Внимание

!

Сертификат пользователя должен иметь кодировку

DER (

\*.cer

).

Подготовьте рабочее место пользователя:

1. Установите криптопровайдер ViPNet CSP.
2. Установите полученные сертификаты издателей в хранилище сертификатов локального компьютера.
3. Скопируйте сертификат пользователя у любую папку.

Для проверки OCSP-сервера:

1. На рабочем месте пользователя запустите утилиту СertUtil со следующими параметрами:

certutil -url <путь к файлу сертификата пользователя>

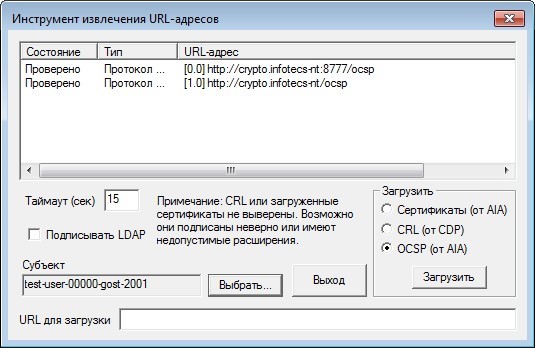
1. В открывшемся окне утилиты СertUtil установите флажок OCSP (от AIA) и нажмите кнопку Загрузить.

|  |
| --- |
| Внимание! Не вводите адрес OCSP-сервера в поле URL для загрузки. Утилита СertUtil некорректно обрабатывает такие запросы. Для проверки могут использоваться только адреса, указанные в сертификате в поле Доступ к информации о центрах сертификации. |

При успешном выполнении OCSP-запроса в столбце Состояние появится запись Проверено, а в журнале событий ViPNet TSP/OCSP-сервера появится запись с кодом события 500.

 Скрыть рисунок

## Проверка работоспособности ViPNet TSP/OCSP-сервера 2 2



Если при обработке запроса возникла ошибка, в столбце Состояние появится запись Неудачно, а в журнале событий ViPNet TSP/OCSP-сервера появится запись с кодом ошибки. Устраните причины появления ошибки и повторно выполните OCSP-запрос.