Создание запроса на сертификат и формирование закрытого ключа

Для создания запроса на сертификат необходимо обновить VipNet CSP до актуальной версии:

1. В меню **Пуск** выберите пункт **Все программы** затем группу **ViPNet** в ней **ViPNet CSP** и щелкните значок **Создание запроса на сертификат**.

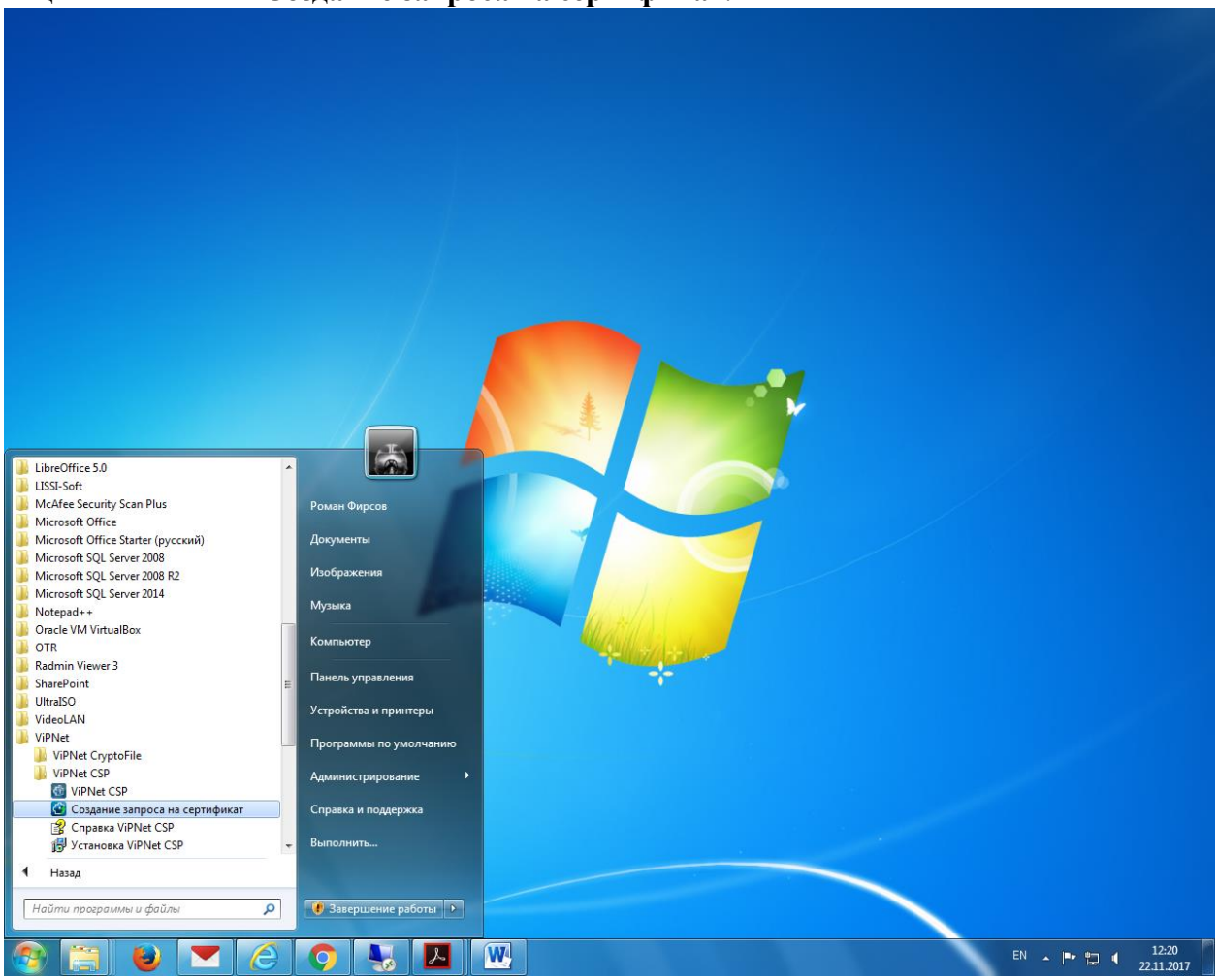


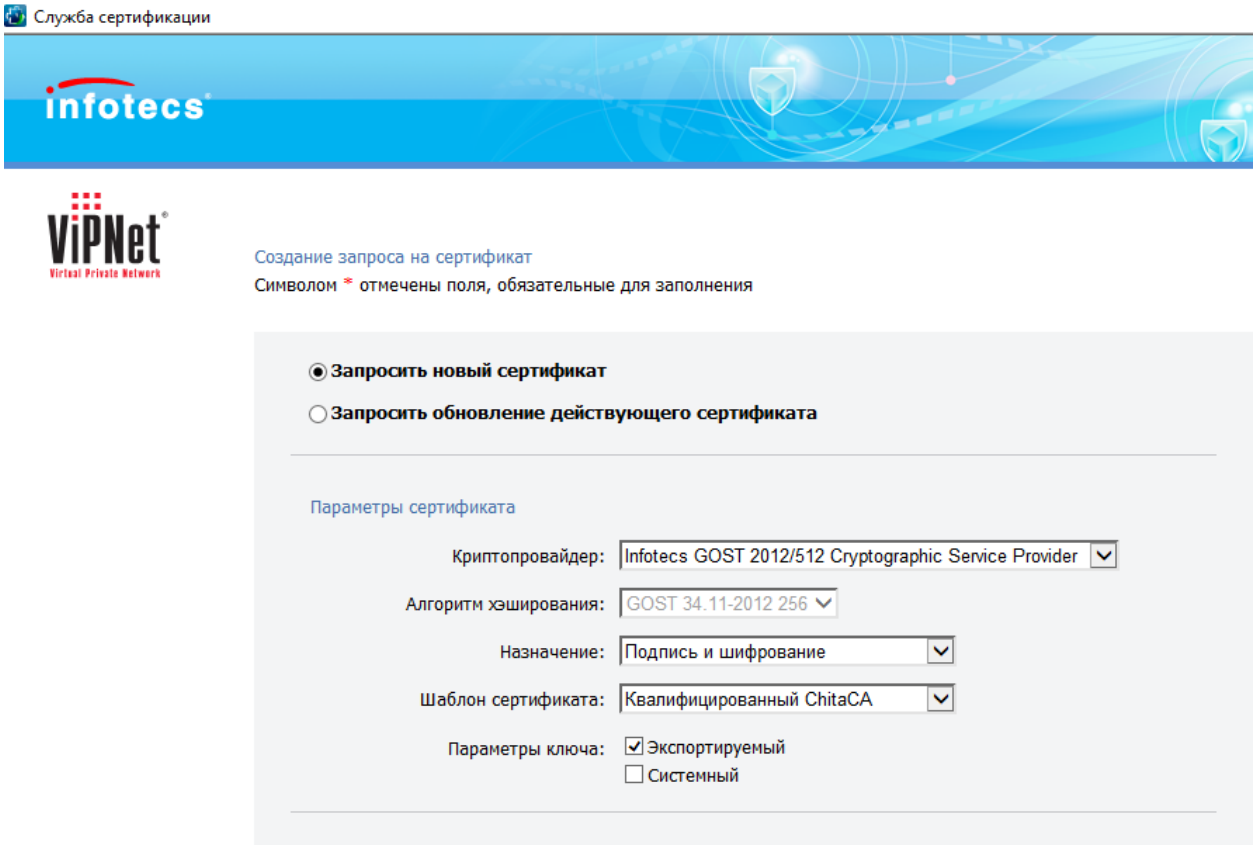
Рисунок: Вызов программы создания запроса на сертификат

2. На открывшейся странице выберите действие **Запросить новый сертификат** – для создания запроса на новый сертификат.

В разделе **Параметры сертификата** укажите следующие параметры:

В списке **Криптопровайдер** необходимо выбрать Infotecs GOST 2012/512 , как показано на рисунке.

В **Назначение** выберите **Подпись и шифрование**, как показано на рисунке.



В списке **Шаблон сертификата** выберите в зависимости от назначения сертификата:
СМЭВ – для всех сотрудников без права формирования запросов в Росреестр;
СМЭВ ИОГВ РОСРЕЕСТР – для сотрудников ИОГВ и подведомственным им учреждений с правом формирования запросов в Росреестр;
СМЭВ ОМСУ РОСРЕЕСТР – для сотрудников ОМСУ и подведомственным им учреждений с правом формирования запросов в Росреестр;
СМЭВ АИС – для автоматизированных систем – формируется только по отдельному указанию.
Квалифицированный ChitaCA – квалифицированный сертификат для различных областей применения;
Квалифицированный ChitaCA ФЛ – квалифицированный сертификат различных областей применения для физического лица;
ГИС ГМП – для работы в государственной информационной системе о государственных и муниципальных платежах**;**
Квалифицированный ChitaCA ФНС – квалифицированный сертификат различных областей применения, в том числе для портала ФНС;
Квалифицированный ChitaCA Росреестр – квалифицированный сертификат различных областей применения, в том числе для портала Росреестра.

3. В разделе **Данные о владельце сертификата** укажите необходимую информацию для формирования запроса на сертификат.

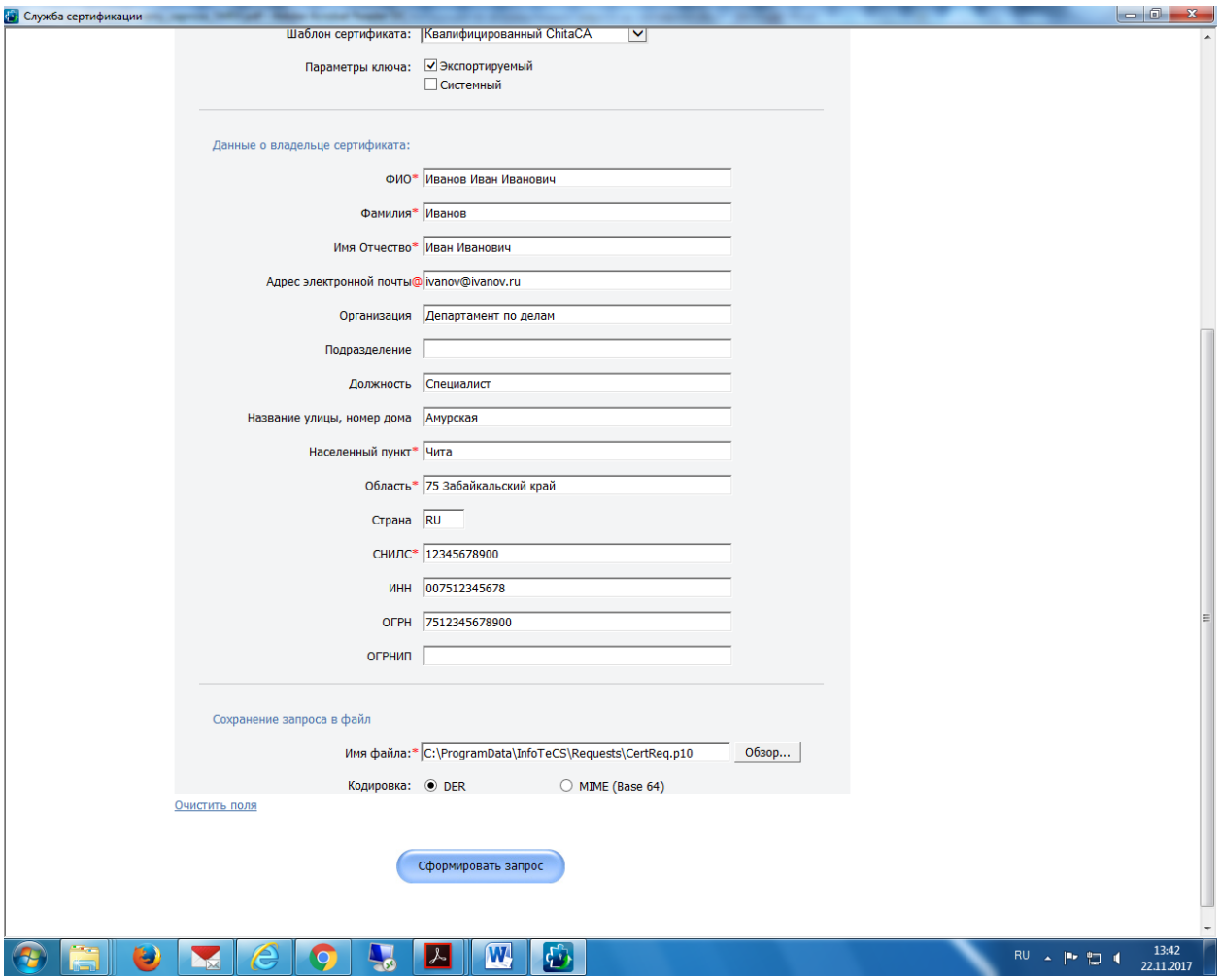


Рисунок: Заполнение данных для запроса на сертификат

Примечание: Если при выборе соответствующего шаблона не отображаются поля **СНИЛС**, **ИНН и ОГРН,** это означает, что необходимо обновить программное обеспечение ViPNet CSP до новой версии, указанной в инструкции.
При этом следует соблюдать следующие правила:
В связи с ограничением на длину полей запроса в 64 символа, следует использовать принятые в официальной деловой переписке сокращения наименований организаций, должностей сотрудников, подразделений, а также названий городов, районов и муниципальных образований с целью уложиться в ограничение длины 64 символа.
СНИЛС – указываются только 11 цифр, без разделяющих знаков.

Важно: Ответственность за полноту и достоверность сведений, указанных в запросе, несет лицо, формирующее запрос на сертификат.

Указания по заполнению полей:
1. **ФИО сотрудника.**

ФИО должно быть указано полностью так, как оно указано в документе, удостоверяющем личность владельца (например, паспорт). Формат:
а. первое слово – Фамилия;

б. 1 пробел;

в. второе слово – Имя;

г. 1 пробел;

д. третье слово – Отчество (если имеется);

Если в фамилии, имени или отчестве в написании присутствует «дефис», то в сертификат так и вносится с дефисом без пробелов (например: Салтыков-Щедрин).

Если фамилия, имя или отчество состоит из нескольких слов разделенных пробелом, то в сертификат вносится одним словом, части которого соединены «подчеркиванием» без пробелов (например: фамилия «Ван чо» будет записана Ван_чо).

Фамилия, имя и отчество (если имеется) должны разделяться 1 пробелом.

Не разрешается использовать пробел в начале и в конце текста.

2. **Организация.**

Каждое слово в тексте должно быть отделено 1 пробелом.

Не разрешается использовать пробел в начале и в конце текста.

Следующие символы разрешается использовать только в том случае, если они встречаются внутри официального названия организации:

3. **Поля Подразделение и Название улицы, номер дома** не являются обязательными к заполнению, но если в организации есть подразделения, то необходимо их указывать.

4. **Населенный пункт.**

Каждое слово в тексте должно быть отделено 1 пробелом.

Не разрешается использовать пробел в начале и в конце текста.

В название населенного пункта также входит название муниципального района (кроме названий областных, краевых и районных центров).

5. Поля **Область** и **Страна** остаются без изменений.

6. В поле **СНИЛС** указывается СНИЛС сотрудника без дефисов и пробелов – 11 цифр.

7. В поле **ИНН организации** указывается 10-значный ИНН организации с приписанными слева 00 – всего должно быть 12 цифр.

8. В поле **ОГРН** указывается ОГРН организации – 13 цифр.

4. Либо в разделе **Данные о владельце сертификата** укажите необходимую информацию об информационной системе, для которой формируется запрос на сертификат.

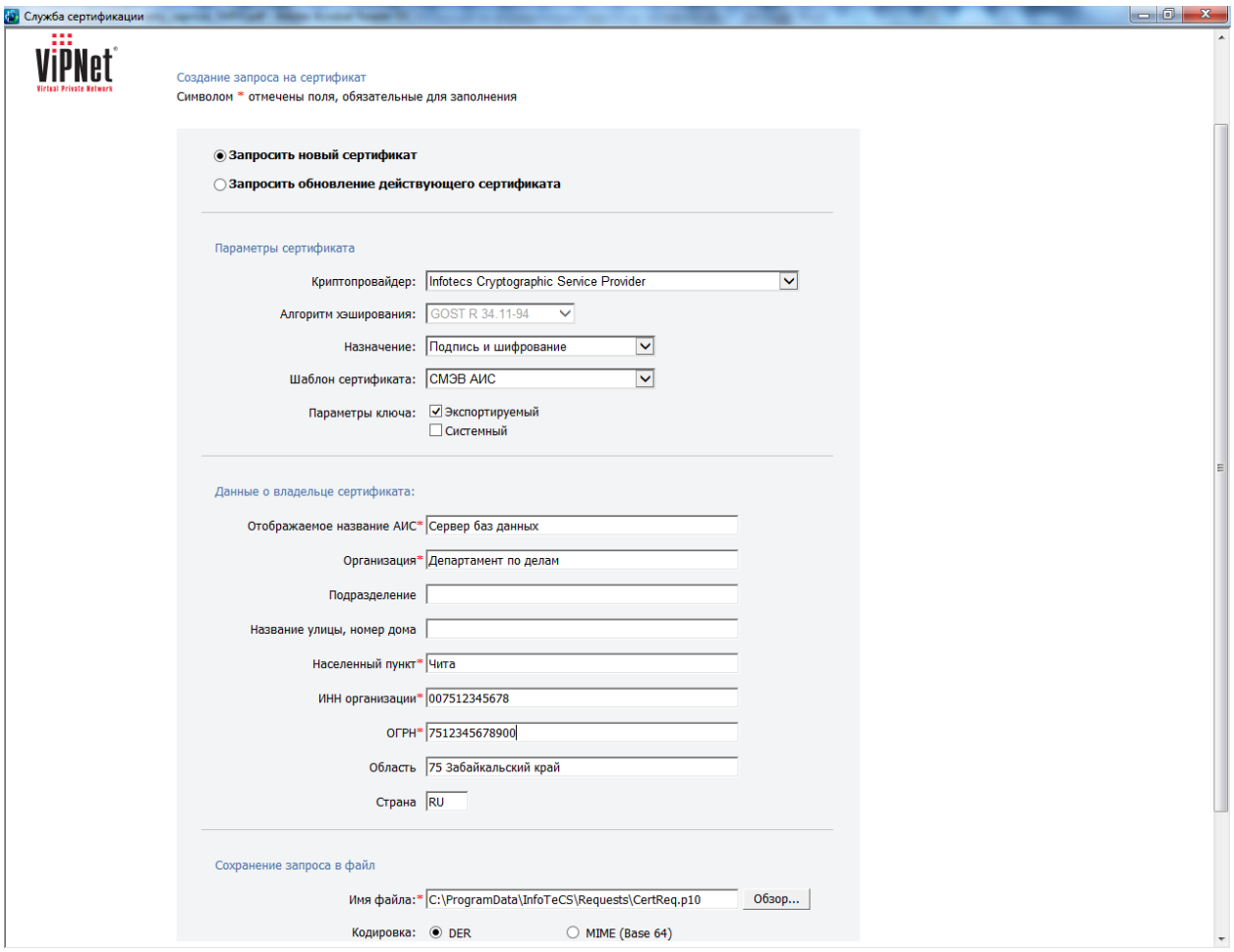
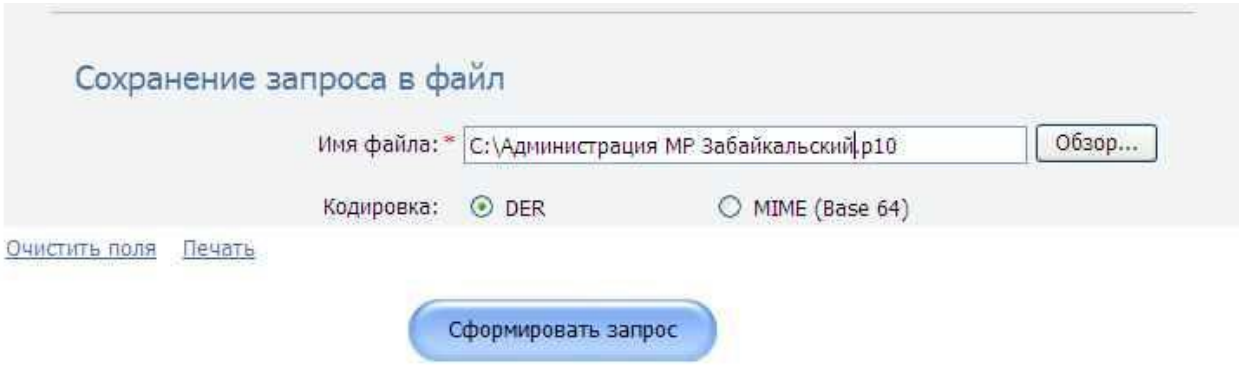


Рисунок: Заполнение данных об информационной системе

При этом следует соблюдать правила заполнения полей, приведенные выше.
В разделе **Сохранение запроса в файл** нажмите **Обзор** и укажите место на диске или съемном носителе, а также имя файла для сохранения файла запроса, имя файла следует выбирать так, чтобы можно было однозначно связать файл запроса и на кого этот запрос формировался.



5. Присоедините сертифицированный носитель ключа электронной подписи. Нажмите кнопку **Сформировать запрос**. Эта кнопка появляется после того, как будут заполнены все поля, обязательные для заполнения (отмечены *). Появится окно инициализации контейнера закрытого ключа, в качестве примера используется eToken, работа с Rutoken принципиально не отличается.

Примечание: до присоединения носителя, на компьютере должны быть установлены драйвера для Вашего типа носителя, которые можно скачать на сайте производителя. Введите PIN-код носителя.
Обычно заводские установки PIN-кодов:
eToken – 1234567890
Rutoken - 12345678

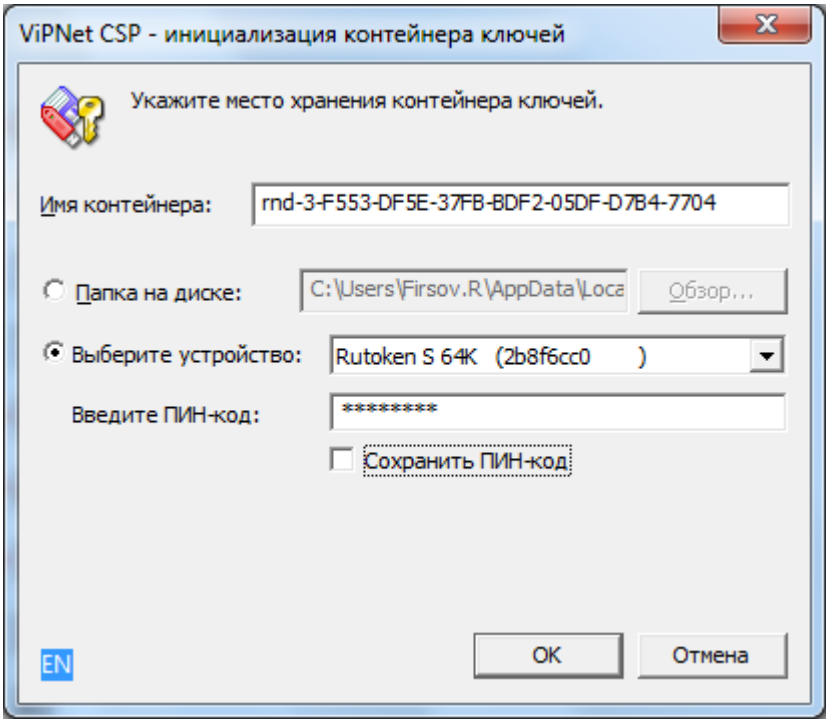
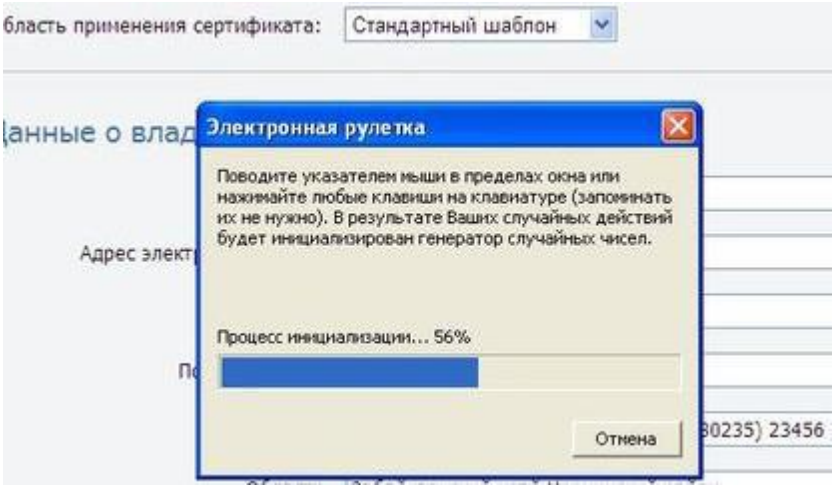


Рисунок: Окно инициализации контейнера закрытого ключа

6. Следуйте указаниям, приведенным в окне **Электронная рулетка.**



7. В окне сообщения об успешном создании файла запроса на сертификат нажмите **ОК**, извлеките носитель из компьютера и храните его в надежном месте, исключающем доступ к нему посторонних лиц.
8. При необходимости создайте следующий запрос на сертификат.
9. После создания файла запроса страницу браузера **Служба сертификации** можно закрыть.

После создания запроса на сертификат, необходимо переслать файл запроса с расширением .p10 (и никаких других файлов) в Удостоверяющий центр на электронный адрес ucecp@e-zab.ru