**Содержание**

[Алгоритм использованию ПО в организации 4](#__RefHeading__10_1981230353)

Инструкция по [загрузке созданного запроса в ПО АРМ Администратора ЦР 1](#__RefHeading__12_1981230353)3

[I. Запрос на регистрацию пользователя 1](#__RefHeading__14_1981230353)3

[II. Запрос на сертификат 1](#__RefHeading__16_1981230353)6

**Системные требования**

**Системные требования:**

* Windows XP и выше, а так же Net Framework 2;
* Для генерации запросов для центра сертификации(УЦ) - Криптопровайдер КриптоПро CSP;
* Любая программа для просмотра pdf;
* Для работы из командной строки - MS Office 2007 и выше;

# Алгоритмы использования ПО в организации

1. Отправить сотрудникам или разместить на сетевом ресурсе ПО RequestGen(файл программы и settings.xml) с заранее сохраненными сведениями об организации (кнопка сохранить Шаг 3). Попросить их заполнить сведения на Шаге 2 и 4, после чего сохранить xml, а затем передать файл xml оператору.

После чего пригласить сотрудника, для проверки переданных сведений в формате XML, на соответствие имеющимся у сотрудника документам. При положительном решении распечатать заявление и согласие. а также сформировать файл запроса к центру сертификации файл \*.req. Сформированные документы попросить подписать сотрудника и потом заявление передать на подпись руководителю организации. Далее оператор после получения подписанных руководителем организации документов, сформированный ранее req файл загружает в УЦ, а также сканирует полученные документы и размещает их для проверки Администратором в ЦА.

2.Аналогично 1-му способу только пользователи сами генерируют закрытые ключи, печатают и отдают на утверждение выходные документы. В этом случае есть вероятность, что они сделают что-то не так, например, сократят названия или укажут ошибочные данные. Данный способ удобен для удаленных от УЦ площадок, но требует подготовки со стороны сотрудников организации или помощи со стороны тех.специалистов.

3. Оператор собирает все требуемые документы и самостоятельно вносит сведения в программу, после чего формирует запрос для центра сертификации (файл \*.req) и отправляет документы для подписания руководителем и работником, которому изготавливается ЭП. Далее оператор после получения документов подписанных руководителем организации, сформированный ранее req файл загружает в УЦ, а также сканирует полученные документы и размещает их для проверки Администратором в ЦА.

4. Через командную строку.

Подготовить сведения согласно файлу shablon\_gen\_key.xls(x)(или подготовить массив xml файлов и сохранить в одну папку), например, выгрузить с 1С. Далее передать сформированный файл/папку в качестве параметра программе. После чего произойдет формирование выходных документов и закрытых ключей.

*Печатные формы и файл запроса(\*.req) сохраняются в папку с программой.ИСПОЛЬЗОВАНИЕ:*

requestgen.exe /mode [pdf|key|both] | /path [Полный путь к файлу|Путь к папке]

*Пример использования:*

*RequestGen.exe /mode both /path C:\Temp\123.xlsx*

*RequestGen.exe /mode both /path C:\Temp\123.xml*

*RequestGen.exe /mode pdf /path C:\Temp\ReqestGenKad\test*

Первый способ являет наиболее предпочтительным, поскольку ввод сведений проверяют как минимум 2 лица (сотрудник заполняющий и оператор УЦ).

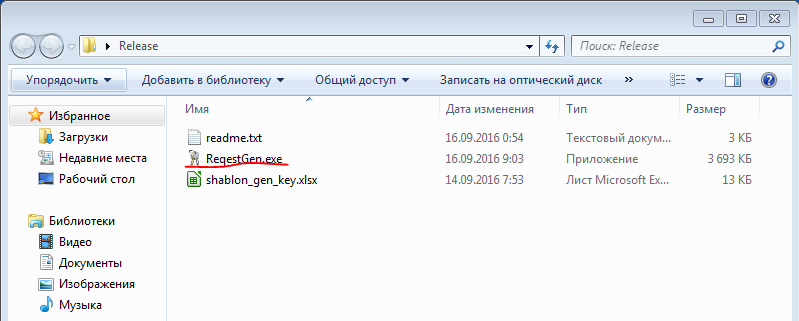
Вместе с тем следует обратить внимание, что способ 2 является наиболее правильным для удаленных площадок (например, регистраторы УРР сидящие в других городах). Дело в том, что если не делать этим способом, то единственным верным является последующая отправка сформированных ключей ЭП почтой (по требованиям обращения с документами ДСП), либо курьером. Особо следует обратить на этом внимание. Поскольку этот вопрос может в последующем интересовать контролирующие органы (ФСБ РФ). Поэтому закрытые ключи следует формировать удаленно.

**Инструкция по работе с программным обеспечением ReqeustGen.exe**

1. Для начала работы с программным обеспечением (далее — ПО) для формирования запроса на сертификат, его следует **загрузить** с портала технического и методологического обеспечения ФГБУ «ФКП Росреестра» по адресу <http://support.kadastr.ru/dashboard_fap>

2. **Разархивировать** ПО архиватором в удобное для Вас место.

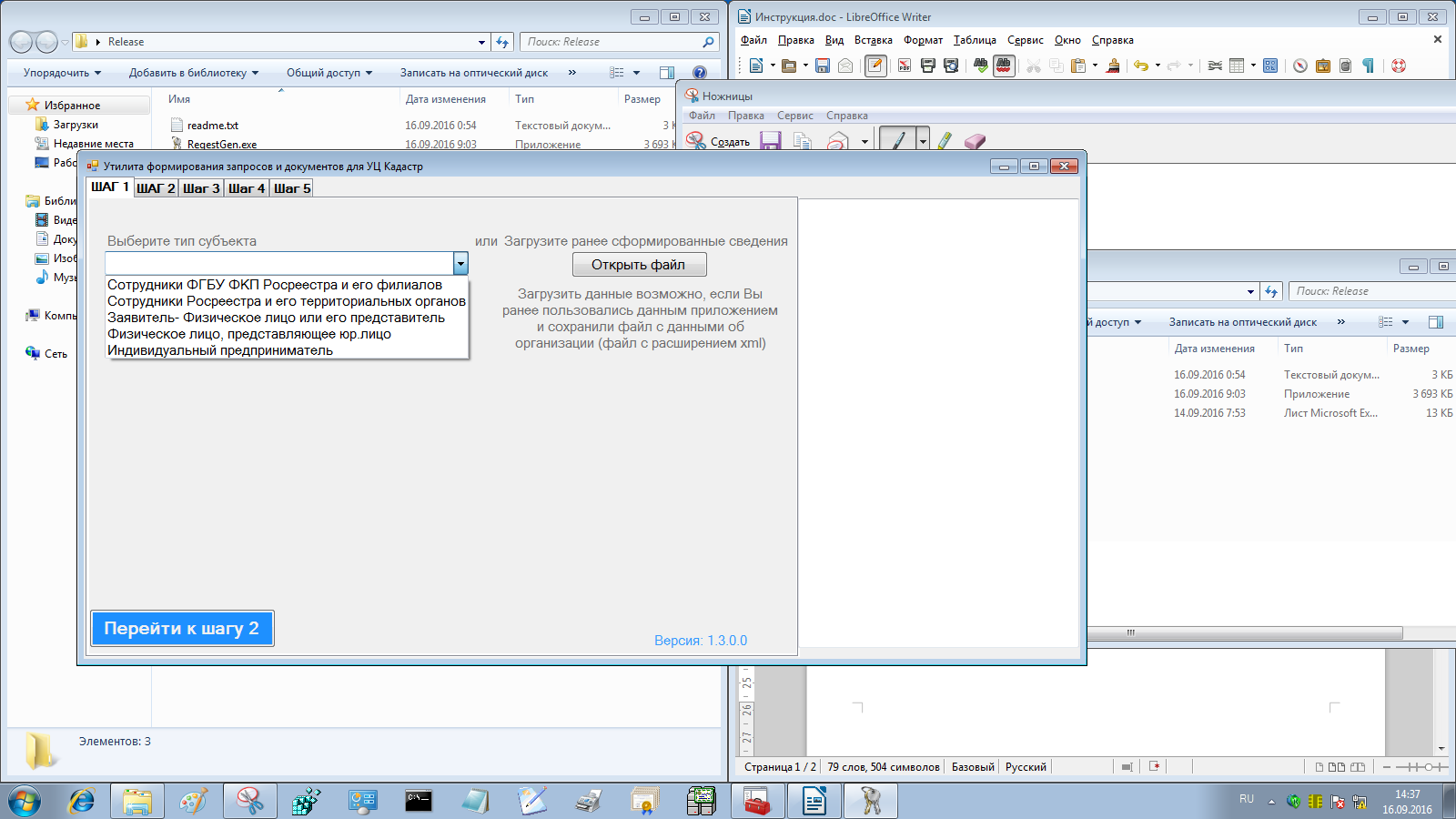
3. Открыть двойным щелчком мыши или ПКМ (правая кнопка мыши) и выбрать Открыть → **RequestGen.exe**.

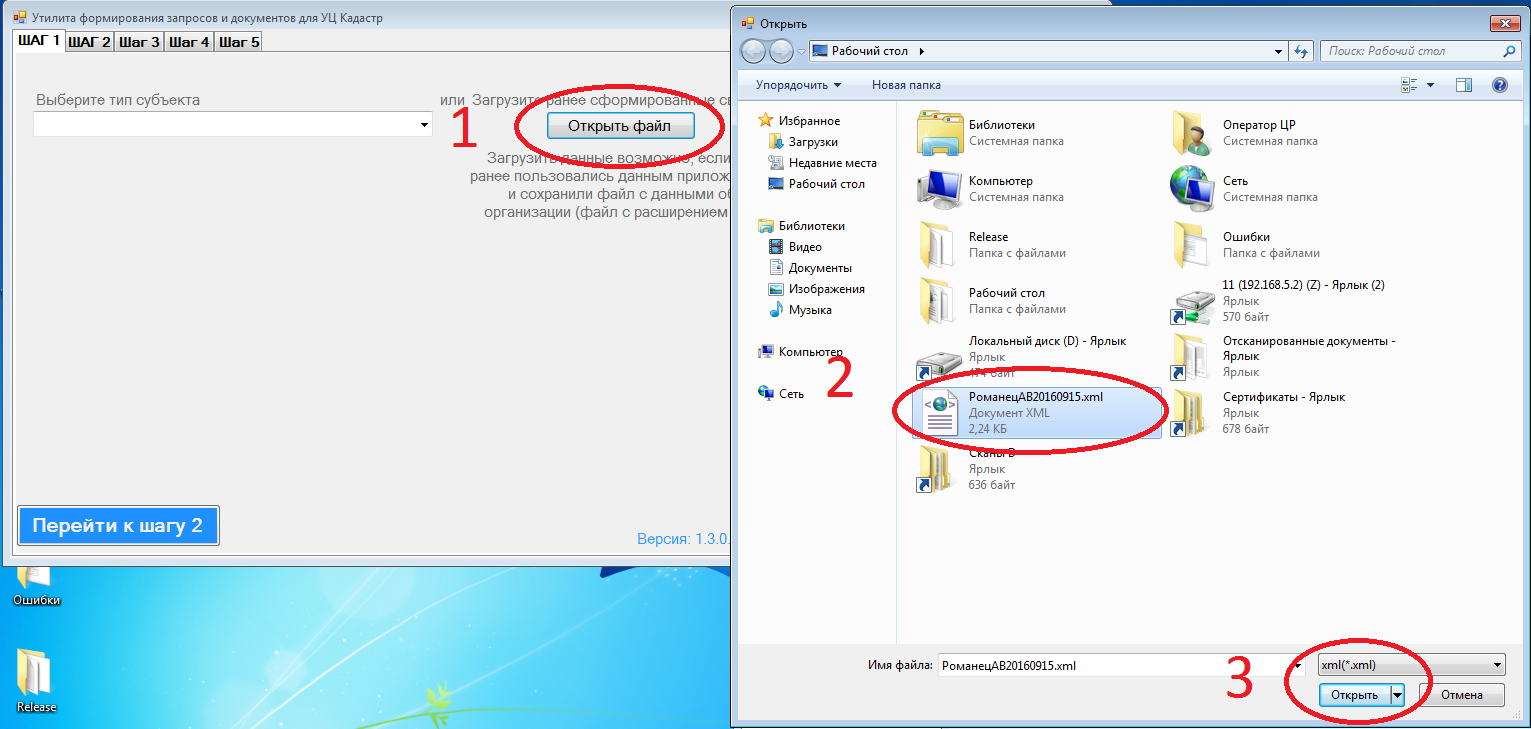
Рисунок 1 - Файл ReqestGen.exe

4. Шаг 1.

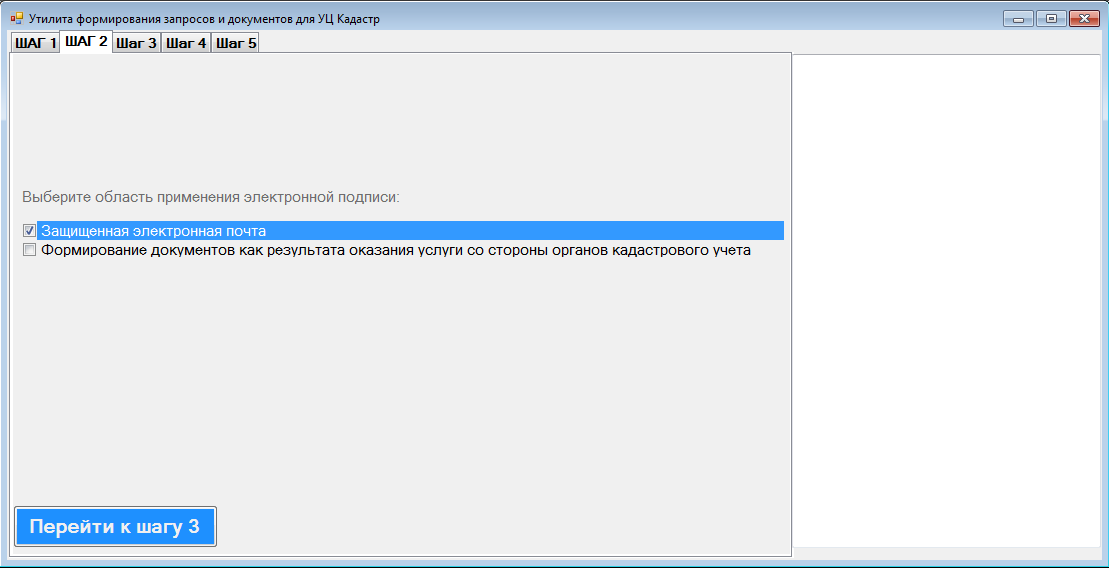
4.1. В форме на Шаге 1 следует выбрать соответствующий **Тип субъекта из выпадающего списка** (Рисунок 2) и нажать кнопку Перейти к Шагу 2.

4.2. Также на Шаге 1 возможно **загрузить информацию из раннее созданного** в данном ПО файла с расширением **.xml** (Рисунок 3). Надо нажать кнопку *Открыть файл*, найти его в соответствующей директории, затем выбрать соответствующий файл и нажать кнопку *Открыть*. Данные загрузятся. Далее на Шаге 5 можно сформировать запрос и закрытый ключ и/или распечатать сформированные документы (Смотреть пункт 8).

Рисунок 2 - Шаг 1

Рисунок 3 - Загрузка ранее созданного xml

5. На Шаге 2 следует выбрать **Ограничение использования квалифицированного сертификата ключа проверки электронной подписи** (Рисунок 4). Для этого нужно слева от соответствующей формулировки поставить *галочку*. Далее следует нажать кнопку Перейти к Шагу 3.

Рисунок 4 - Шаг 2

6. На Шаге 3 следует внести **Данные об организации** (Рисунок 5):

1. **Наименование организации** в именительном падеже (есть: Кто? Что?). С такими кавычками ",".

2. **Должность руководителя** в именительном падеже.

3. **Фамилия, имя, отчество** в именительном падеже.

4. **Должность руководителя** в родительном падеже.

5. **Фамилия, имя, отчество** в родительном падеже.

6. **Документ, определяющий полномочия руководителя организации** в родительном падеже. Дата и номер обязательны!

7. **Регион**. Выбрать из выпадающего списка.

8. **Город** (населенный пункт).

9. **Улица, дом.** Ввести данные согласно положению об организации.

10. Внести **ИНН организации**.

11. Ввести **ОГРН организации**.

12. Кнопка *Сохранить* необходима для того чтобы в следующий раз не вводить повторно не вводить информацию на этом шаге. Нажимать на свое усмотрение.

На Рисунке 5 представлен пример заполненной формы на Шаге 3.

Перейти на Шаг 4, нажав соответствующую кнопку на форме.

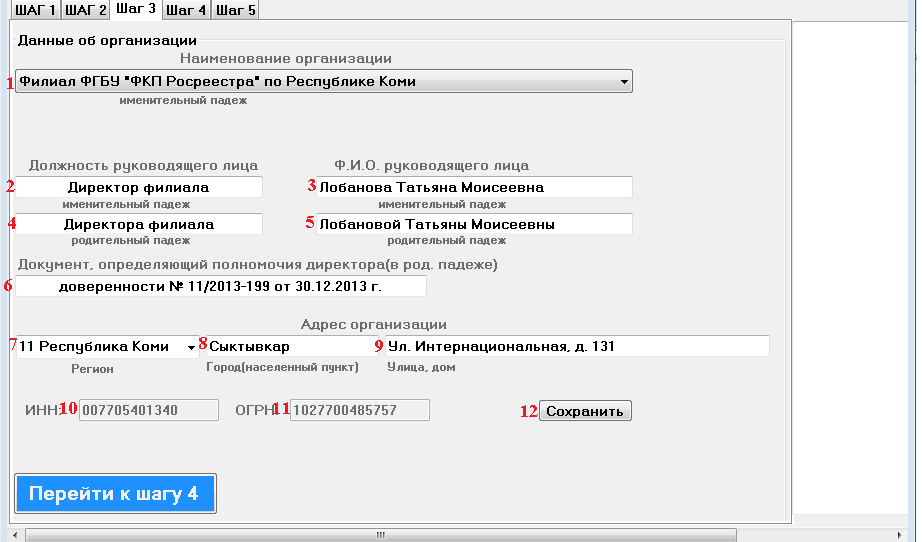


Рисунок 5- Заполненная форма на Шаге 3

7. Ввести **данные о заявителе** (Рисунок 6):

1. **Фамилия, имя, отчество** в именительном падеже.

2. **Персональный адрес электронной почты.** Настоятельно рекомендуется указывать персональный корпоративный адрес электропочты. Например [IvanovSK@uXX.rosreestr.ru](mailto:IvanovSK@uXX.rosreestr.ru) .

3. **Кодовая фраза**, необходимая при обращении в Удостоверяющий центр.

4. **Серия и номер паспорта**.

5. **Дата выдачи паспорта**.

6. **Кем выдан паспорт**. Заполнять строго в соответствии с записью в паспорте с запятыми, пробелами, регистром символов.

7. **Адрес регистрации**. Заполнять строго в соответствии с записью в паспорте с запятыми и пробелами. Если нет региона и населенного пункта, то необходимо их ввести в соответствии со штампом над данными регистрации.

8. Номер **СНИЛС**. Если указана ошибка, что «Неверно введен СНИЛС», то необходимо проверить введенные данные.

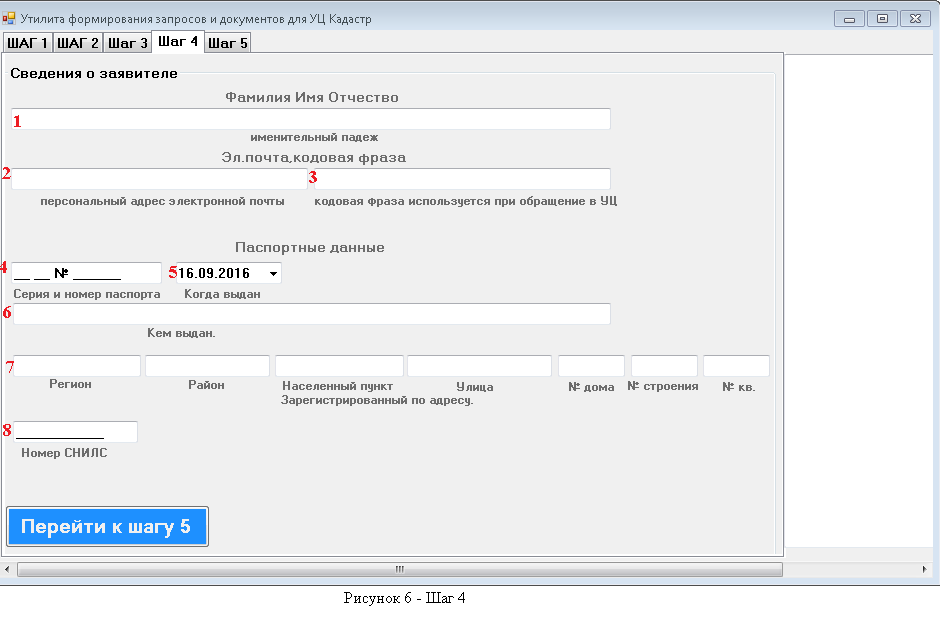


Рисунок 6 - Шаг 4

8. На Шаге 5 Можно выполнить следующие действия (Рисунок 7):

Рисунок 7 - Шаг 5

1. **Сохранить сведения в XML**. Необходимо, чтобы в следующий раз, при необходимости, не вводить заново данные, а загрузить их из специального созданного файла.

2. **Печать выходных документов**. Документы формируются в формате .pdf. *Если при нажатии кнопки печати в открывшемся ПО для просмотра pdf, не происходит печать документов, то ПРОБЛЕМА в настройках печати или принтера, а не в данном ПО.*

3. **Сформировать запрос и закрытый ключ**.

Необходимо вставить носитель в usb-разъем ПК. Нажать кнопку *Сформировать запрос.*

Появится окно перехода для выбора носителя (Рисунки 8,9) нажать *Просмотреть сообщение*. При появлении окна для выбора носителя следует выбрать нужный носитель(Рисунок 10) и ввести pin-код токкена (Рисунок 11) .



Рисунок 8 - Предупреждение о выборе носителя

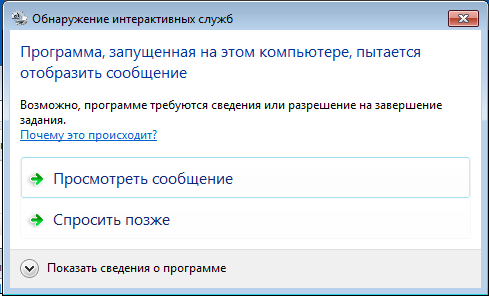


Рисунок 9 - Окно перехода

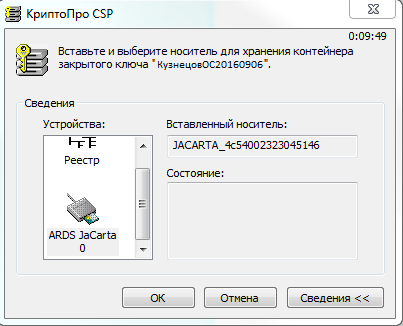
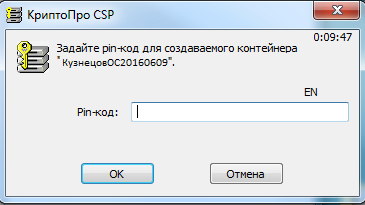


Рисунок 10- Выбор носителя

Рисунок 11 - Ввести пин-код от токкена

Далее выбрать директорию, где будет сохранен файл и нажать кнопку Сохранить. Сформированный файл, который должен иметь расширение .req необходимо использовать в АРМ Администратора ЦР при подаче запроса на регистрацию пользователя и при подаче заявки на сертификат.

# Инструкция по загрузке созданного запроса в ПО АРМ Администратора ЦР

## I. Запрос на регистрацию пользователя

Зайти в ПО **АРМ Администратора ЦР** и перейти по пути:

*КриптоПроУЦ → АРМ администратора Центра Регистрации → Центр регистрации... → Пользователи → Создать → Нового пользователя.*

Далее выбрать *Чтение запроса на сертификат из файла → Обзор*. Найти файл в соответствующей директории, затем выбрать соответствующий файл и нажать кнопку *Открыть (Рисунок 12)*.

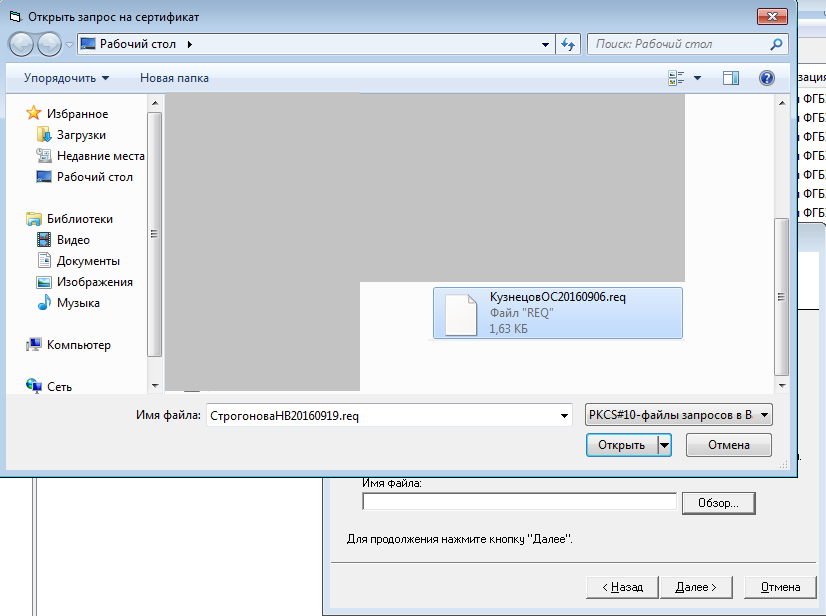


Рисунок 12 - Выбор файла запроса на сертификат

Данные из запроса загрузятся в специальную Форму для заполнения (Рисунок 13). Следует ПРОВЕРИТЬ загруженные данные.

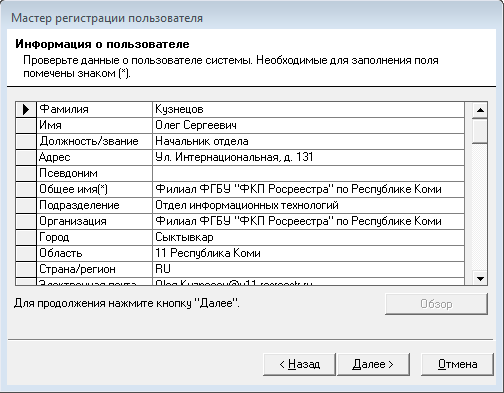


Рисунок 13 - Загруженные из запроса данные

Далее необходимо **ввести ключевую фразу**, придуманную заявителем (Рисунок 14).

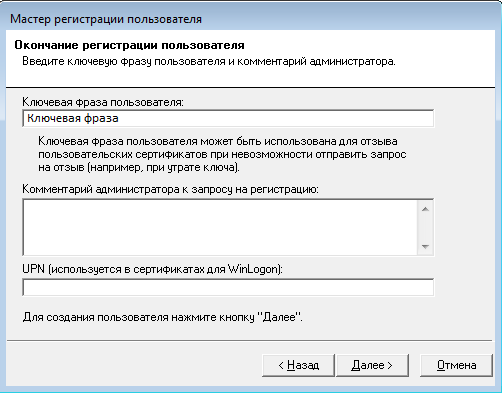
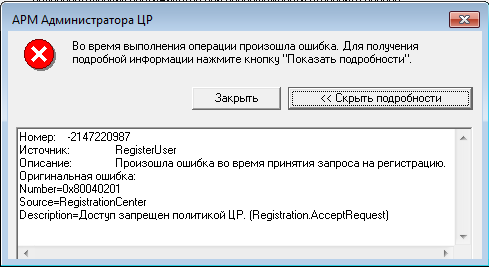


Рисунок 14 - Ввод ключевой фразы

Нажать кнопку *Далее*. Выйдет окно ошибки (Рисунок 15). Не беспокойтесь и данная ошибка является штатной. Удостоверьтесь о выполнении подачи запроса на регистрацию, зайдя в:

*КриптоПроУЦ → АРМ администратора Центра Регистрации → Центр регистрации... → Запросы на регистрацию.*

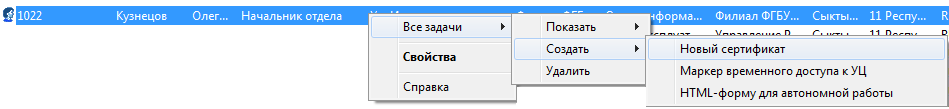
Рисунок 15 - Ошибка доступ запрещен политикой ЦР

Созданный Вами запрос должен появиться в списке. Далее следует ждать одобрения запроса на регистрацию, после которого следует подавать запрос на сертификат.

**II. Запрос на сертификат**

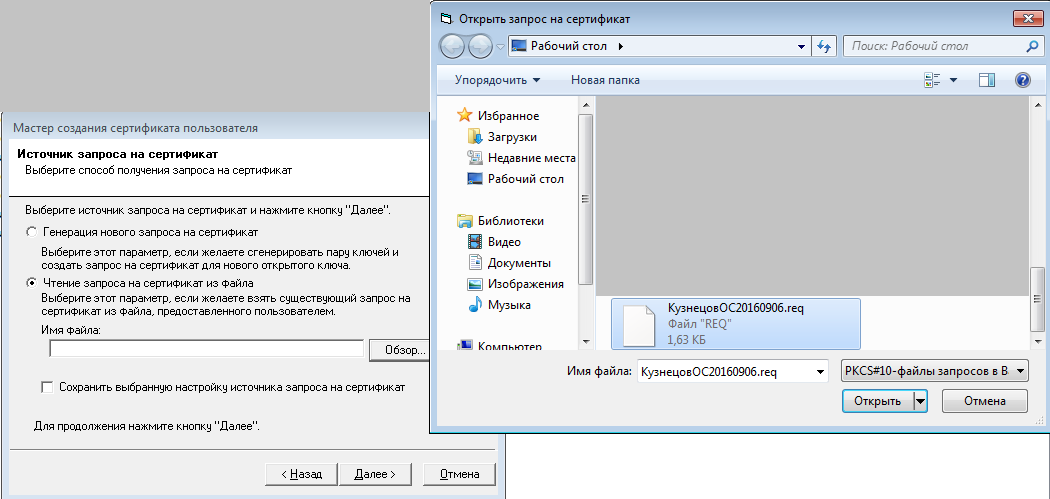
Выбрать созданного пользователя и перейти по пути (Рисунок 16):

*«Пользователь» → Все задачи → Создать → Новый сертификат.*

Рисунок 16 - Создание сертификата

Далее появится форма ввода информации о пользователе. Выбрать *Чтение запроса на сертификат из файла → Обзор.* Найти файл в соответствующей директории, затем выбрать соответствующий файл и нажать кнопку *Открыть*. Нажать кнопку *Далее* (Рисунок 17).

Откроется форма, на которой в случае необходимости можно посмотреть данные о подаваемом запросе на сертификат, с помощью кнопки *Просмотр*.

Рисунок 17 - Выбор файла запроса на сертификат

После нажатия на кнопку Далее запрос на сертификат будет подан на согласование (Если не убрать галочку с пункта Принять запрос на сертификат после отправки на Центр Регистрации, то выйдет ошибка типа «Ошибка доступ запрещен политикой ЦР»).

После одобрения сертификат следует искать по пути:

*КриптоПроУЦ → АРМ администратора Центра Регистрации → Центр регистрации... → Сертификаты.*