Инструкция по подаче запроса на квалифицированный сертификат ключа проверки электронной подписи с использованием Единой биометрической системы (ЕБС)

(посещение ТОФК не требуется)

Содержание

Перечень сокращений 3
Системные требования к рабочему месту пользователя 4
Подготовка к работе 5
Формирование запроса на сертификат 6
Скачивание полученного сертификата 23

Перечень сокращений

Сокращение	Полное наименование
АРМ	Автоматизированное рабочее место
ВРС	Подсистема ведения реестра сертификатов, обеспечивающая ввод, проверку, централизованное хранение сведений, представленных заявителями, информирование владельцев сертификатов и публикацию списка аннулированных сертификатов
ЕБС	Единая биометрическая система
ИНН	Идентификационный номер налогоплательщика
ОГРН	Основной государственный регистрационный номер
ПО	Программное обеспечение
Портал заявителя	Онлайн сервис подачи документов для получения сертификатов (https://fzs.roskazna.ru/)
Сертификат	Квалифицированный сертификат ключа проверки электронной подписи
СМЭВ	Система межведомственного электронного взаимодействия
СКЗИ	Средство криптографической защиты информации
СНИЛС	Страховой номер индивидуального лицевого счета
ТОФК	Территориальный орган Федерального казначейства
УЦ ФК	Удостоверяющий центр Федерального казначейства

Системные требования к рабочему месту пользователя

Системные требования к АРМ пользователя приведены в таблицах (см. Таблица 1, Таблица 2, Таблица 3).

Таблица 1. Общие системные требования к рабочему месту пользователя

Минимальные аппаратные требования	
Процессор	Тактовая частота не менее 2,3 ГГЦ
Оперативная память	Не менее 1 024 МБ
Пропускная способность канала	Не менее 1 024 Кбит/сек

Таблица 2. Дополнительные требования к АРМ пользователя при использовании СКЗИ КриптоПро CSP

Требования к ПО	
Операционная система (семейство Microsoft)	Microsoft Windows 7 и выше
Интернет-браузер для ОС семейства Microsoft	Яндекс.Браузер версии 18.9.1.954 и выше, Chromium-gost версии 83.0.4103.61 и выше.
Операционная система (семейство Linux)	Альт Линукс, Astra Linux, РЕД ОС, GosLinux
Интернет-браузер для ОС семейства Linux	Chromium-gost версии 83.0.4103.61 и выше.
Плагин (дополнение) к браузеру	КриптоПро ЭЦП Browser Plug-In версии 2.0 и выше
Средство криптографической защиты информации	СКЗИ «КриптоПро CSP 4.0» и выше

Таблица 3. Дополнительные требования к АРМ пользователя при использовании СКЗИ VipNet CSP

Требования к ПО	
Операционная система (семейство Microsoft)	Microsoft Windows 7 и выше
Интернет-браузер для ОС семейства Microsoft	Яндекс.Браузер версии 18.9.1.954 и выше, Chromium-gost версии 83.0.4103.61 и выше, Google Chrome версии 94 и выше.

Операционная система (семейство Linux)	Альт Линукс, Astra Linux, РЕД ОС, GosLinux
Интернет-браузер для ОС семейства Linux	Chromium-gost версии 83.0.4103.61 и выше, Mozilla Firefox версии 63 и выше
Средство криптографической защиты информации	ViPNet PKI Client версии 1.6 и выше

Подготовка к работе

- Обеспечить на АРМ наличие поддерживаемой ОС, согласно разделу «Системные требования к рабочему месту пользователя»
- Обеспечить на АРМ наличие одного из поддеживаемых Web-браузеров, согласно разделу «Системные требования к рабочему месту пользователя»
- Установить сертифицированную версию СКЗИ КриптоПро CSP 4.0 и выше либо ViPNet PKI Client (Инструкция по установке ViPNet PKI Client)
- Установить «КриптоПро ЭЦП Browser Plugin» версии 2.0 и выше (инструкция по настройке для Яндекс.Браузера).

  Примечание: в случае использования ViPNet PKI Client не требуется
- Установить сертификаты Минцифры России (ГУЦ) и УЦ ФК согласно инструкции
- Проверить настройку АРМ (проверить).

ВНИМАНИЕ! В случае использования ViPNet PKI Client необходимо осуществить настройку АРМ согласно инструкции.

Формирование запроса на сертификат

Для первичного получения сертификата необходимо выполнить следующие действия:

1. Перейти на главную страницу открытой части Портала Заявителя, расположенной по адресу https://fzs.roskazna.ru/ (Рисунок 1).

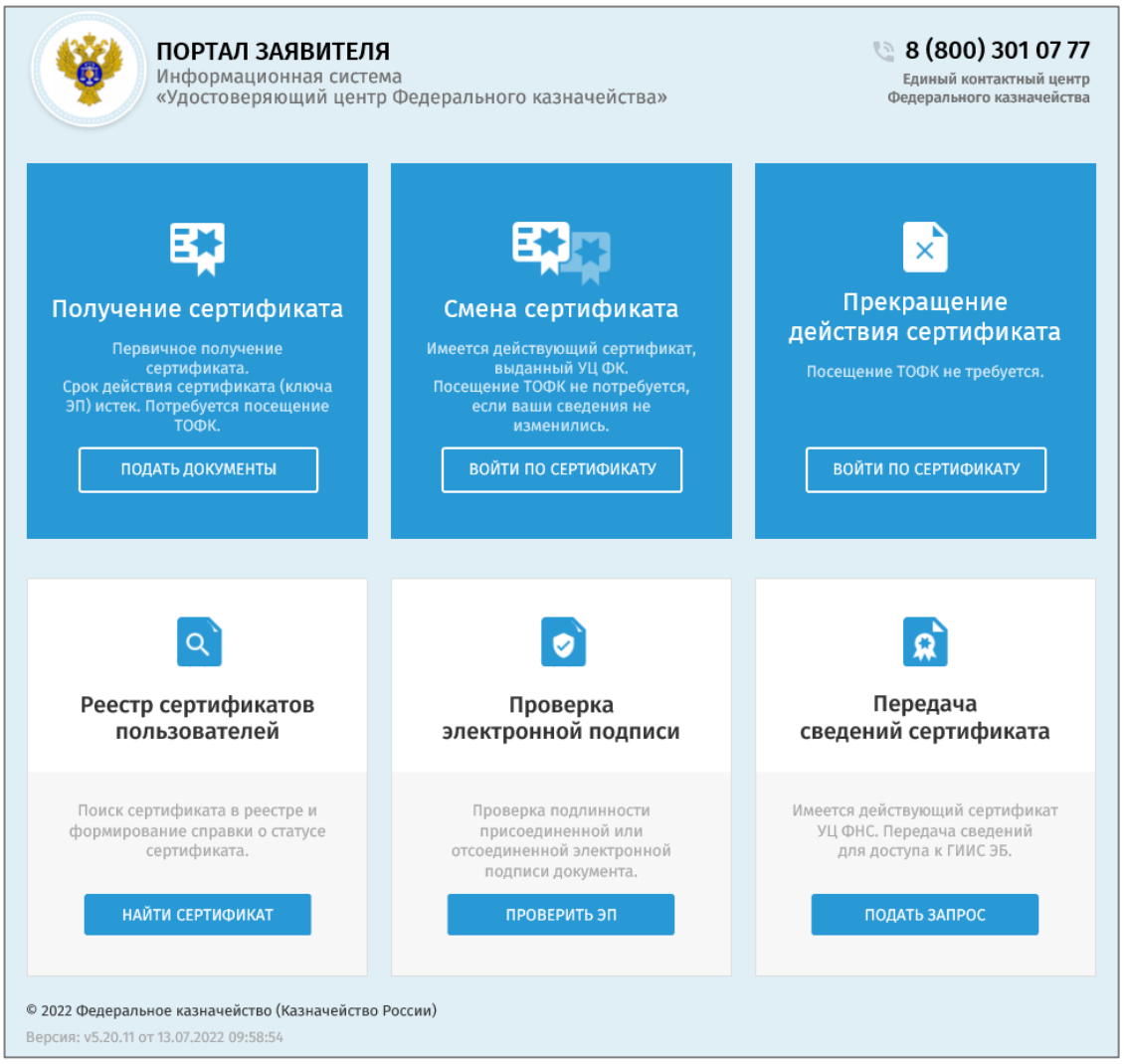


Рисунок 1. Главная страница открытой части Портала Заявителя

2. Нажать на кнопку «Подать документы» в блоке «Получение сертификата» (Рисунок 2).

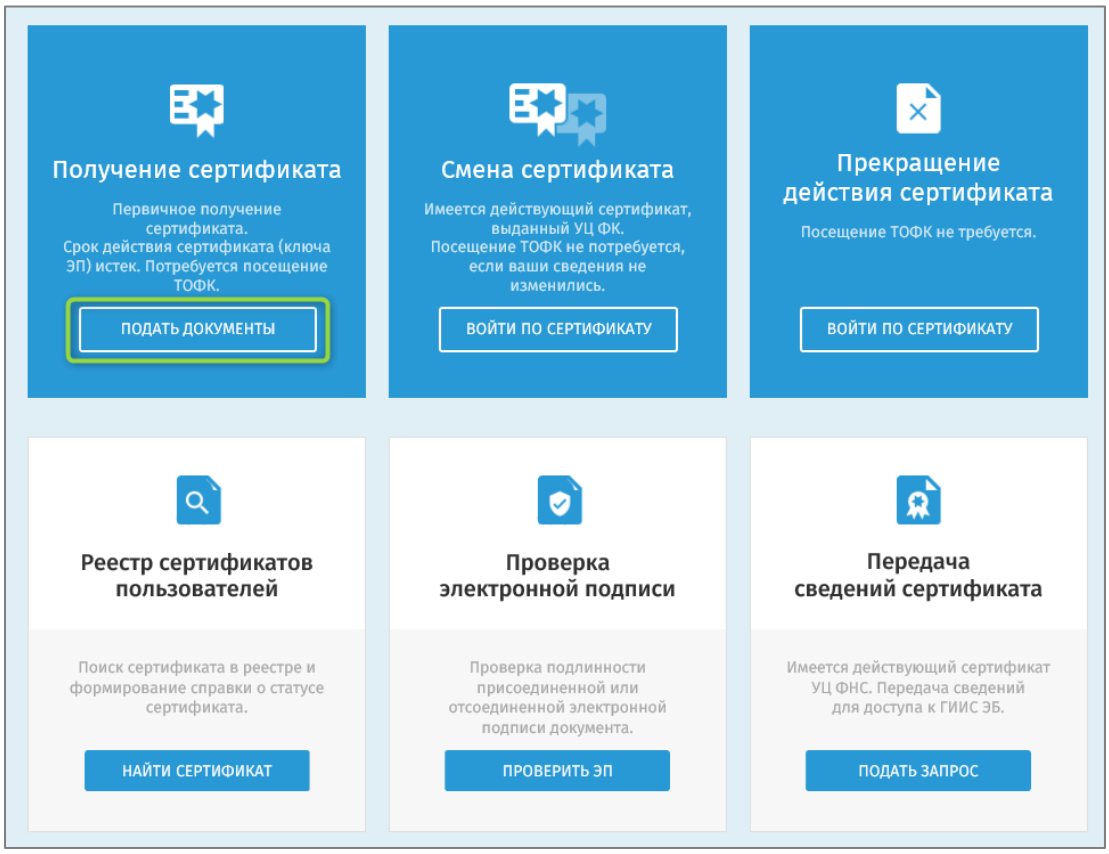


Рисунок 2. Блок «Получение сертификата». Кнопка «Подать документы»

3. В качестве выбора способа заполнения сведений для включения в запрос на сертификат выбрать вход через Госуслуги путем нажатия кнопки «Войти через Госуслуги (ЕСИА)» (Рисунок 3. Выбор способа заполнения сведений для включения в запрос на сертификат).

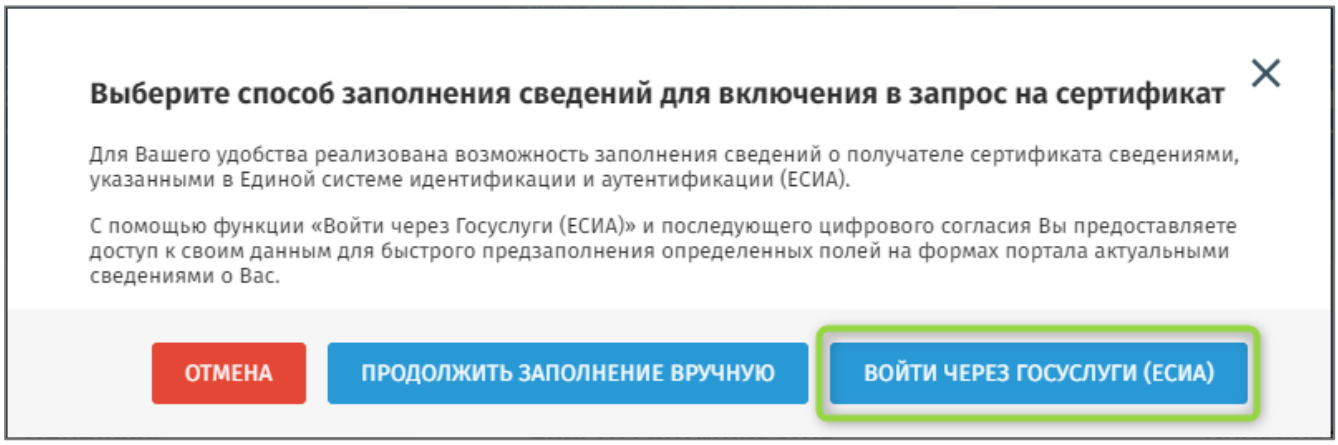


Рисунок 3. Выбор способа заполнения сведений для включения в запрос на сертификат

4. В открывшемся окне указать необходимые для авторизации на Госуслугах сведения и нажать «Войти» (Рисунок 4).

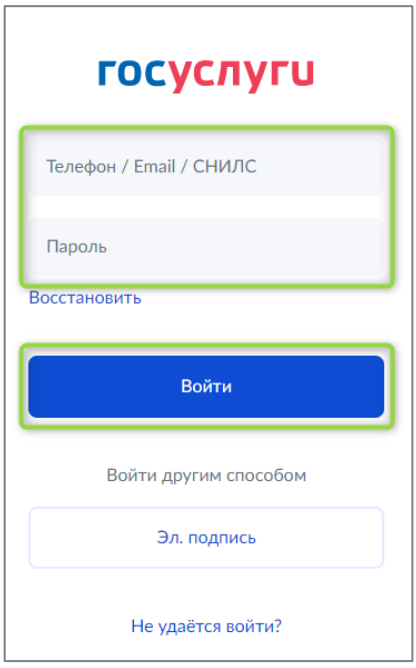


Рисунок 4. Авторизация на Госуслугах

5. В отобразившейся форме «Формирование запроса на сертификат» выберите место хранения ключа электронной подписи и сертификата (Рисунок 5) и затем заполните все необходимые сведения, указанные в пунктах 6-11.

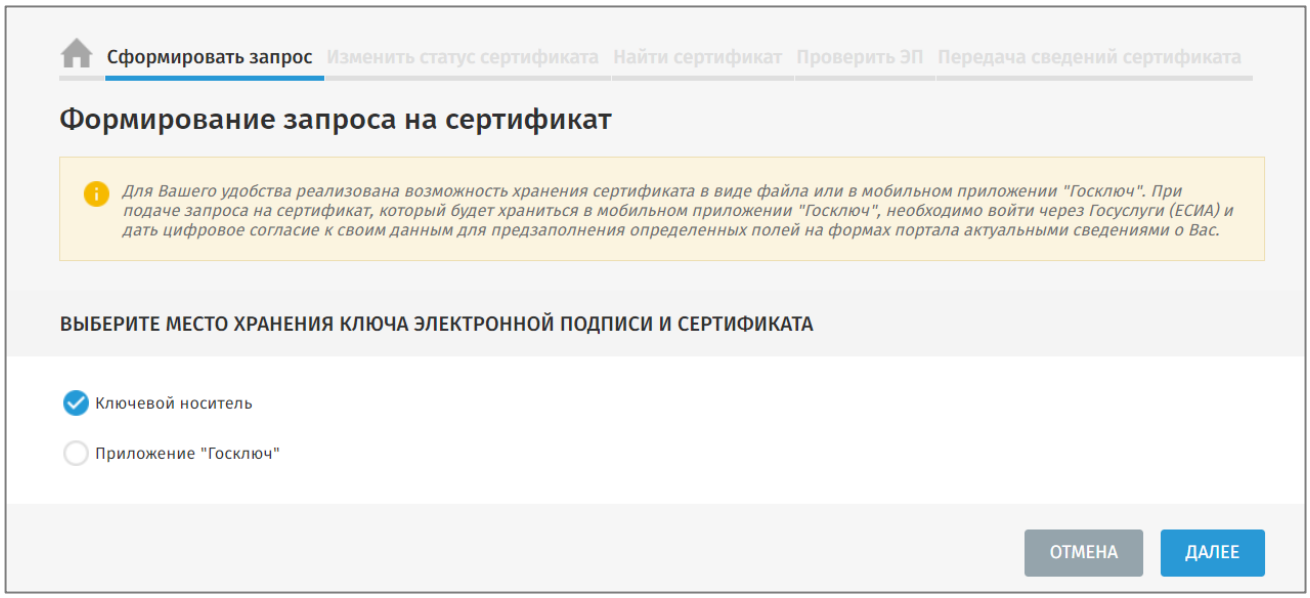


Рисунок 5. Выбор места хранения ключа электронной подписи и сертификата

6. В разделе «Выбор субъекта Российской Федерации» в поле «Субъект РФ» выберите из раскрывающегося списка регион, в котором будет осуществляться подача документов на получение сертификата (Рисунок 6).

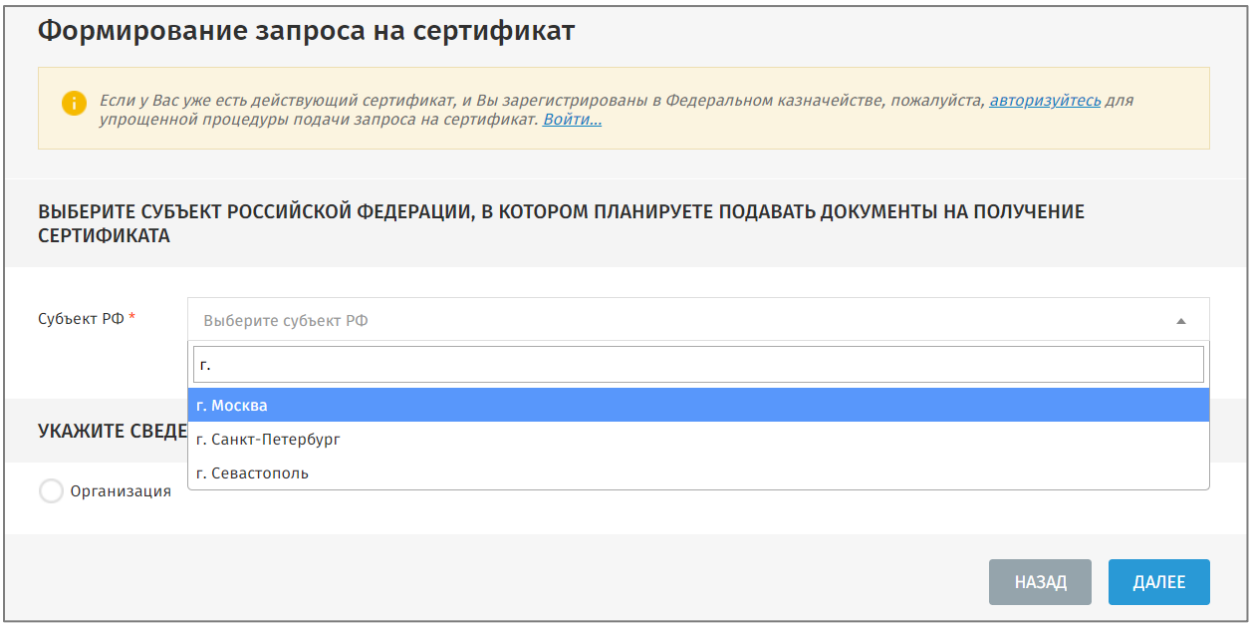


Рисунок 6. Формирование запроса на сертификат. Выбор «Субъекта РФ»

7. В разделе «Укажите сведения о Заявителе» выберите «Организация» (Рисунок 7).

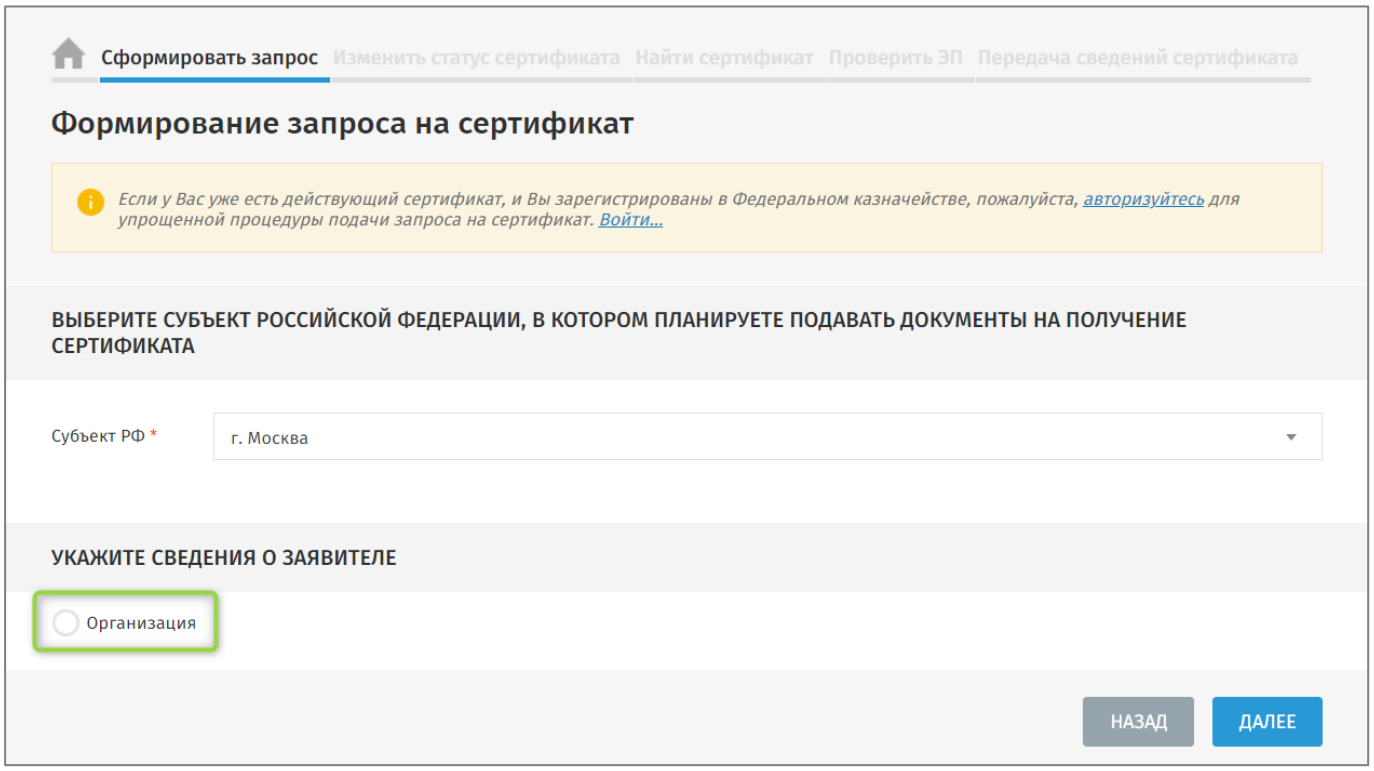


Рисунок 7. Формирование запроса на сертификат. Блок выбора заявителя

8. Отображается поле для ввода ОГРН (Рисунок 8).

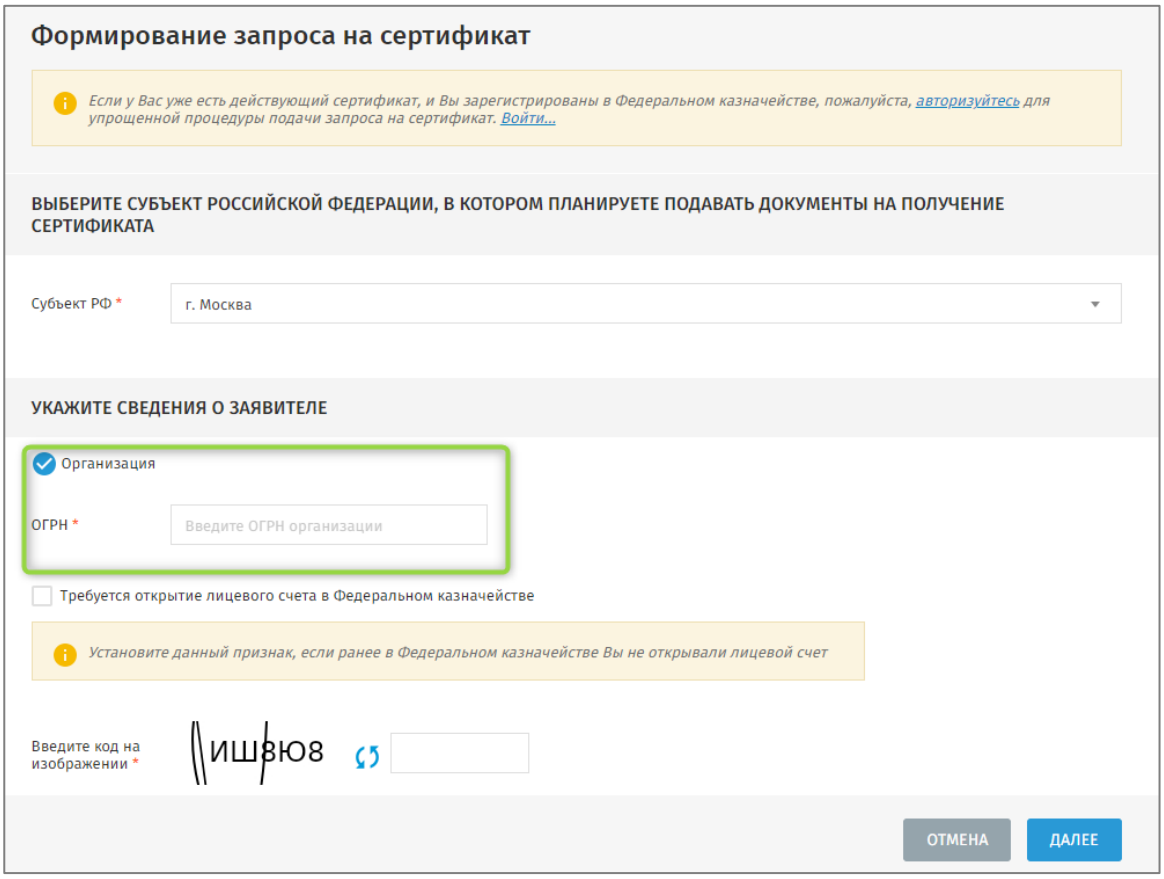


Рисунок 8. Формирование запроса на сертификат. Поле «ОГРН»

9. В разделе «Укажите сведения о Заявителе» заполните обязательное поле «ОГРН».

10. Введите код с изображения капчи и нажмите на кнопку «Далее».

11. Выберите подачу в ТОФК и в поле «ТОФК» нажмите на пиктограмму «» для выбора ТОФК, в который будет подан запрос на получение сертификата (Рисунок 9) и нажмите кнопку «Далее».

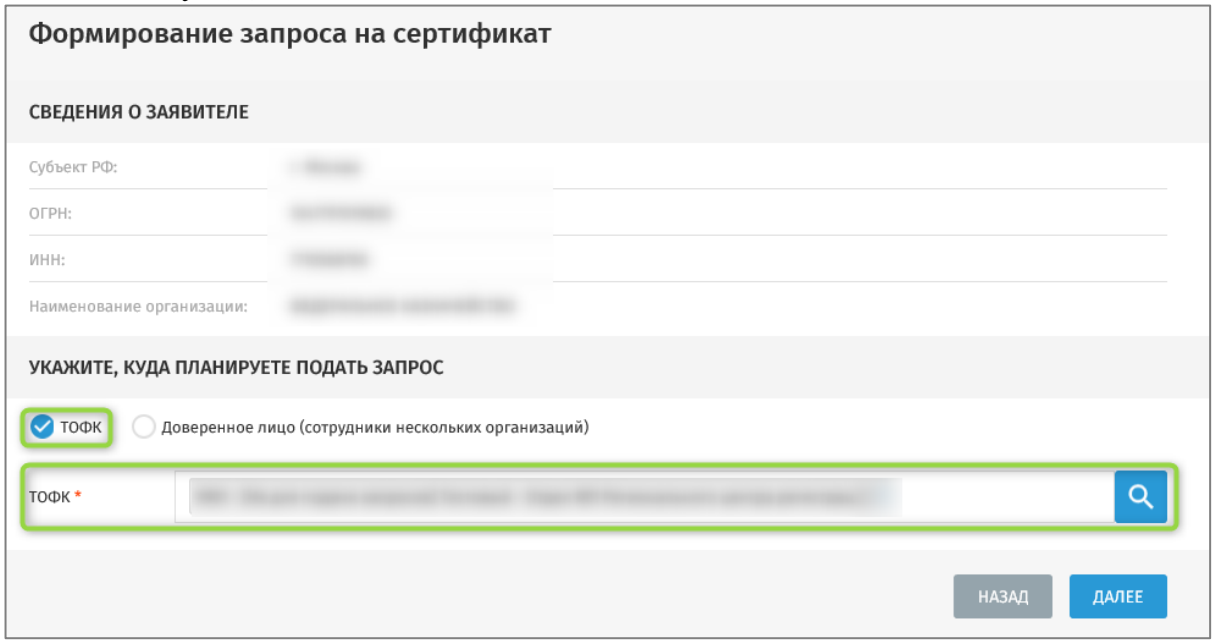


Рисунок 9. Формирование запроса на сертификат. Выбор ТОФК

12. В отобразившимся блоке «Формирование сведений для подачи запроса на сертификат» заполните все необходимые сведения, указанные в пунктах 0-25.

Выберите тип запрашиваемого сертификата – «Сертификат должностного лица» либо «Сертификат юридического лица». (Рисунок 10).

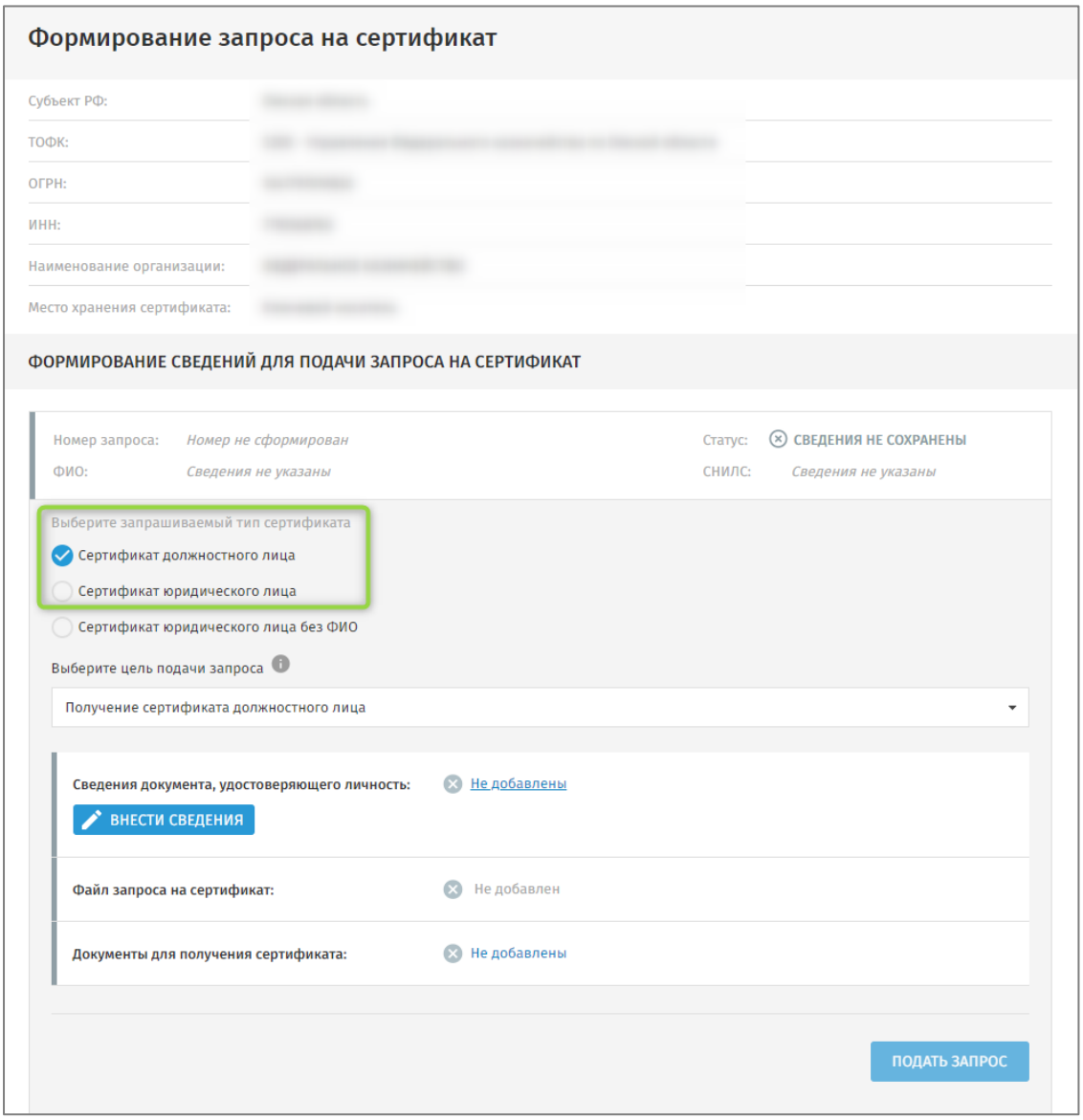


Рисунок 10. Формирование сведений для подачи запроса на сертификат. Выбор типа запрашиваемого сертификата

13. В разделе «Сведения документа, удостоверяющего личность», нажмите на кнопку «Внести сведения» (Рисунок 11).

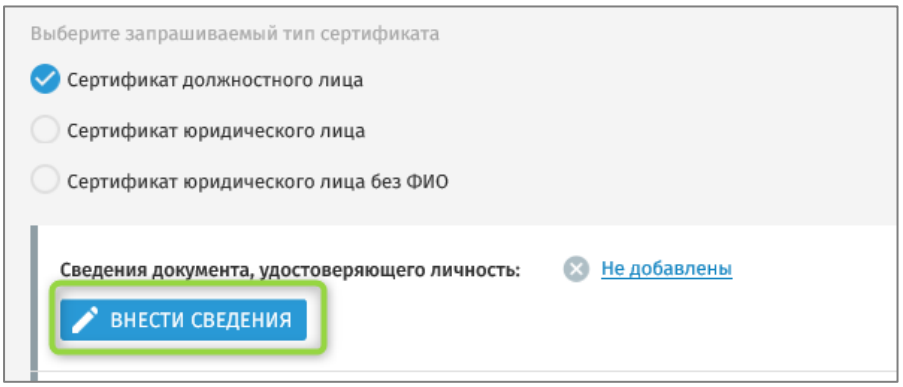


Рисунок 11. Блок «Сведения документа, удостоверяющего личность». Кнопка «Внести сведения»

14. В отобразившемся модальном окне нажмите на кнопку «Да» (Рисунок 12) и пройдите удаленную идентификацию по инструкции на портале Госуслуги (Рисунок 13)

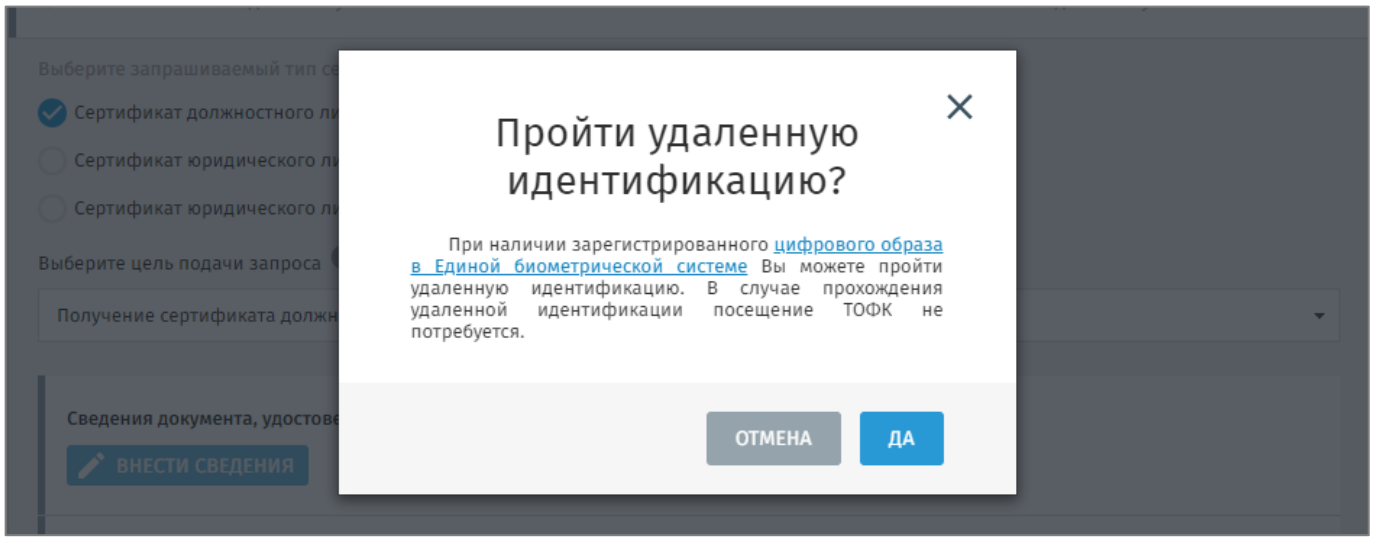


Рисунок 12. Модальное окно «Пройти удаленную идентификацию?»

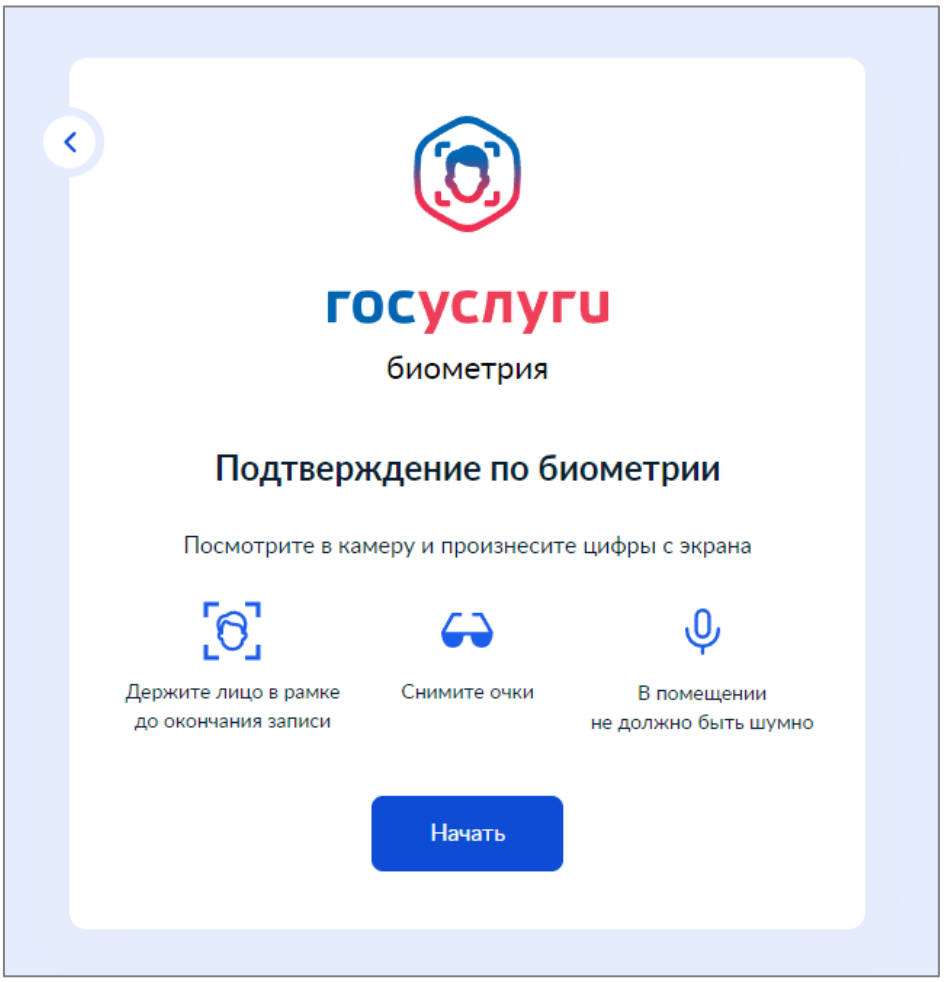


Рисунок 13. Портал Госуслуги. Подтверждение по биометрии

15. После успешного прохождения Удаленной идентификации, осуществляется переход на портал ФЗС. Отображается модальное окно подтверждающее успешное прохождение удаленной идентификации (Рисунок 14).

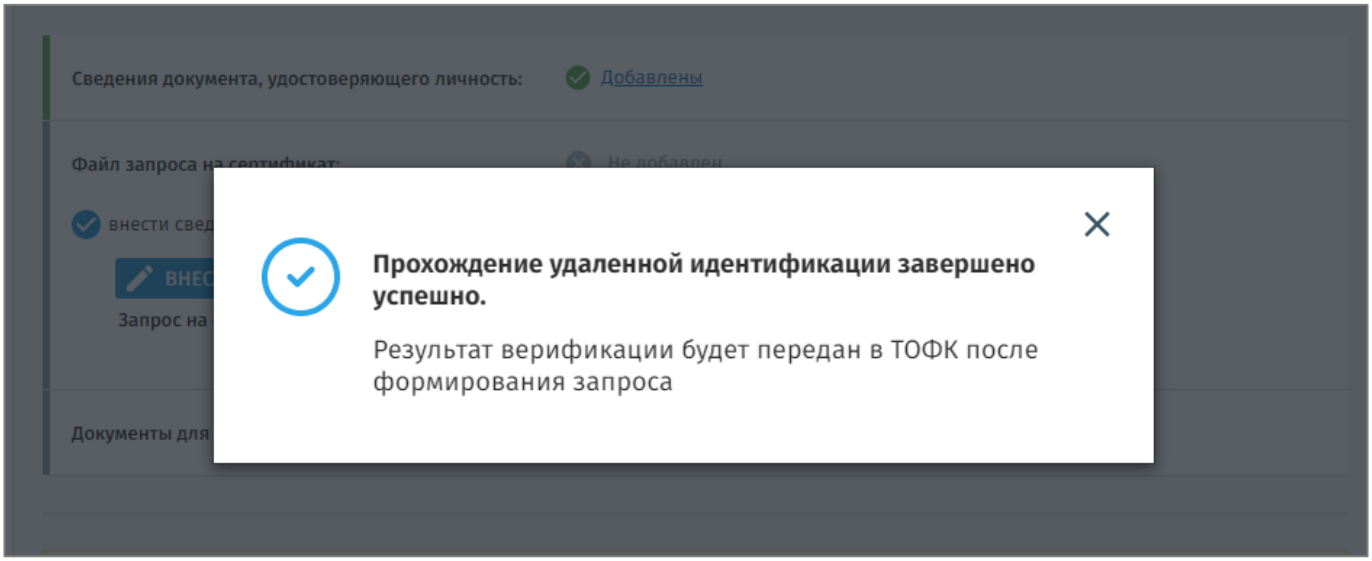


Рисунок 14. Портал ФЗС. Модальное окно «Прохождение удаленной идентификации завершено успешно»

16. В блоке «Сведения документа, удостоверяющего личность» добавлены сведения получателя сертификата из учетной записи Госуслуг. Сведения не доступны редактирования (Рисунок 15).

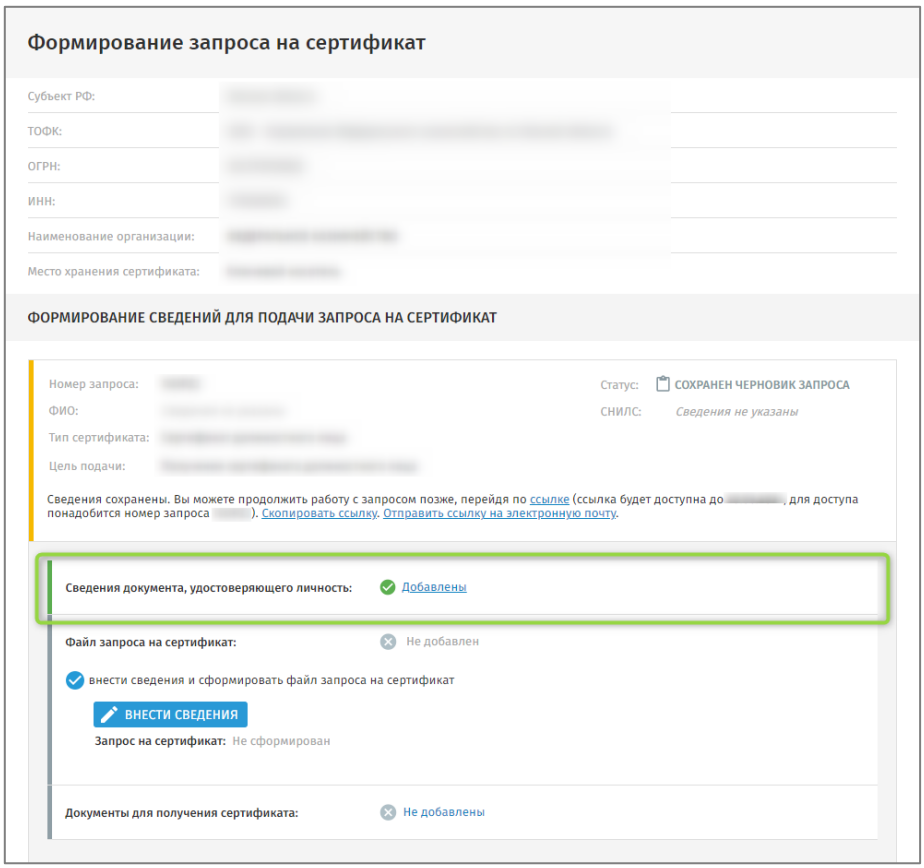


Рисунок 15. Блок «Сведения документа, удостоверяющего личность»

17. В блоке «Формирование сведений для подачи запроса» в разделе «Файл запроса на сертификат» нажмите кнопку «Внести сведения». (Рисунок 16).

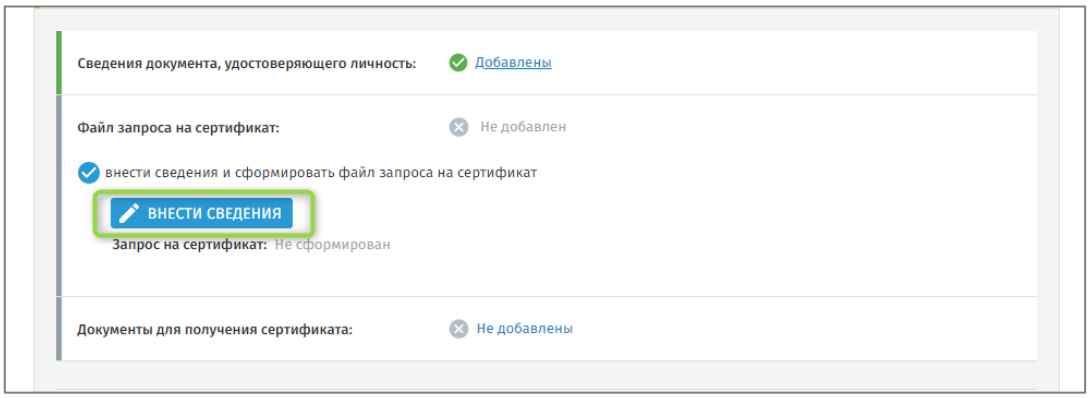


Рисунок 16. Блок «Файл запроса на сертификат».
Кнопка «Внести сведения»

18. Вставьте носитель ключа электронной подписи в системный блок АРМ.

19. В отобразившейся форме «Формирование запроса на сертификат» укажите полномочия, необходимые для работы в информационных системах Федерального казначейства и заполните обязательные поля. Обязательные поля отмечены * (Рисунок 17).

Примечание: **В форме «Формирование запроса на сертификат» часть обязательных полей заполняется сведениями из учетной записи Госуслуг. Сведения не доступны для изменения.**

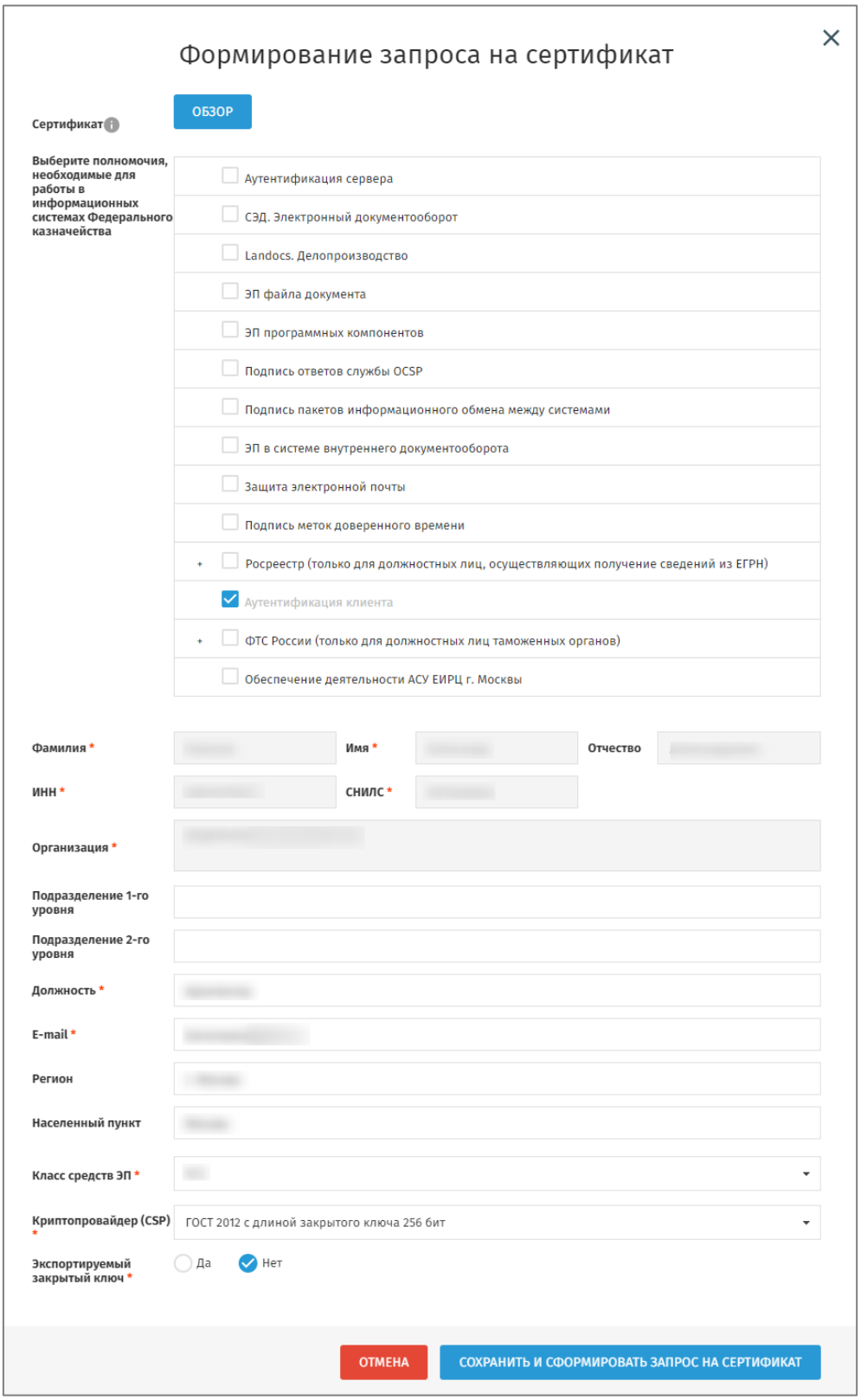


Рисунок 17. Отображение формы «Формирование запроса на сертификат»

20. После внесения сведений нажмите на кнопку «Сохранить и сформировать запрос на сертификат».

21. На форме создания запроса на сертификата со сформированными данными нажать «Сформировать».

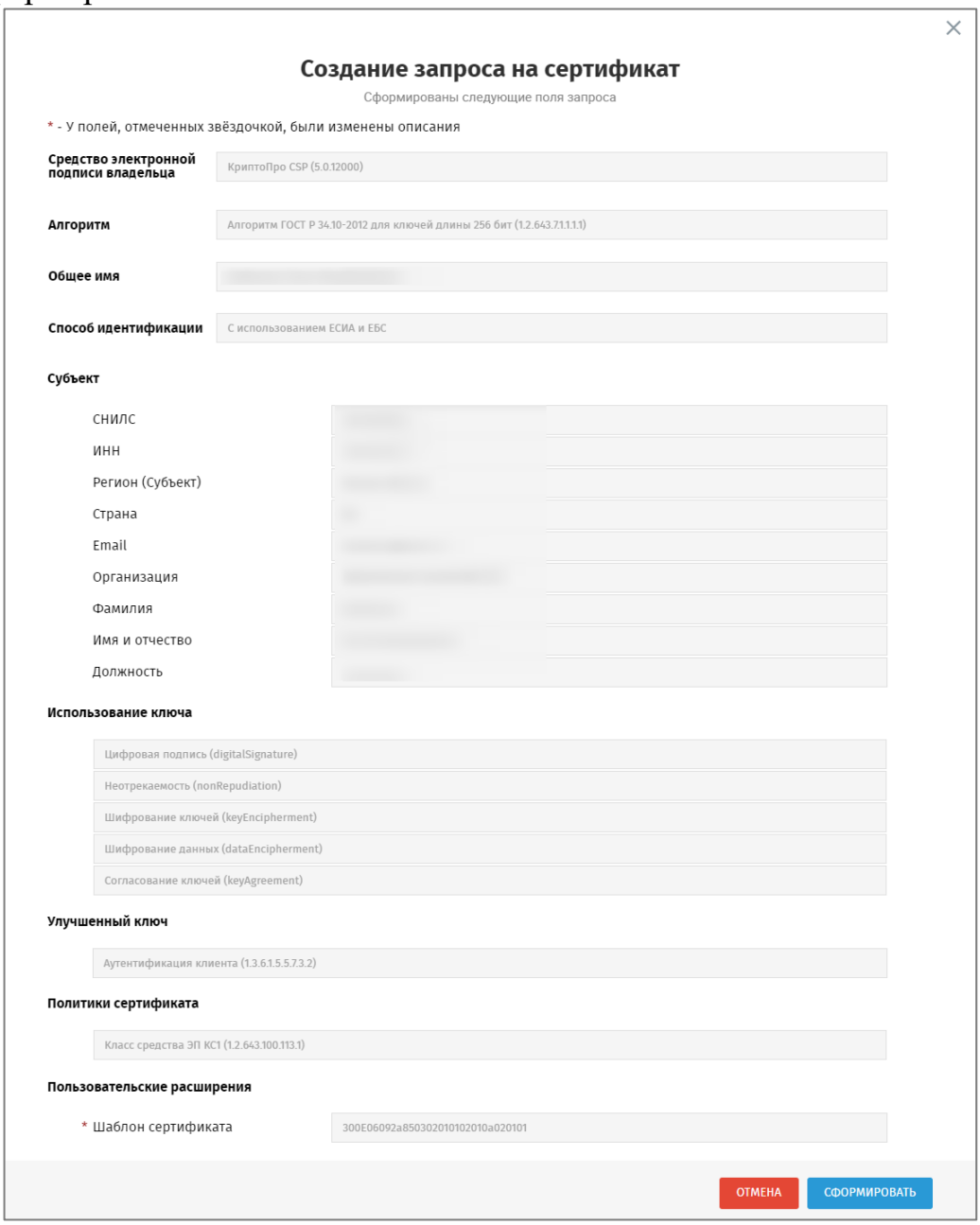


Рисунок 18. Форма создания запроса на сертификат со сформированными полями запроса

Важно! Формирование запроса осуществляется с помощью СКЗИ «КриптоПро CSP 4.0» и ПО «КриптоПро ЭЦП Browser Plug-In» версии 2.0. Для формирования запроса необходимо подключить отформатированный ключевой носитель (Рутокен, флеш-накопитель и т.п.) к системному блоку АРМ. После выбора носителя необходимо ввести пароль и подтвердить его.

ВНИМАНИЕ! Введенный пароль необходимо запомнить, в случае утери, его восстановление невозможно. После генерации запроса на сертификат владелец должен обеспечивать хранение носителя ключевой информации с ключом электронной подписи в соответствии с установленными требованиями (приказ ФАПСИ от 13.06.2001 № 152).

22. На отобразившемся блоке «Формирование сведений для подачи запроса на сертификат» в разделе «Документы для получения сертификата» признак Получателя сертификата (Рисунок **19**):

a. В случае, если Получатель сертификата является лицом, имеющим право действовать без доверенности от имени Заявителя, необходимо установить признак «Получатель сертификата является лицом, имеющим право действовать без доверенности от имени Заявителя»;
b. Если владелец сертификата не является лицом, имеющим право действовать без доверенности от имени получателя сертификата, необходимо заполнить данные в разделе «Документ или сведения, подтверждающие полномочия получателя сертификата» - указать название, дату и номер документа, а также посредством нажатия кнопки «Обзор» прикрепить сканированный образ документа.

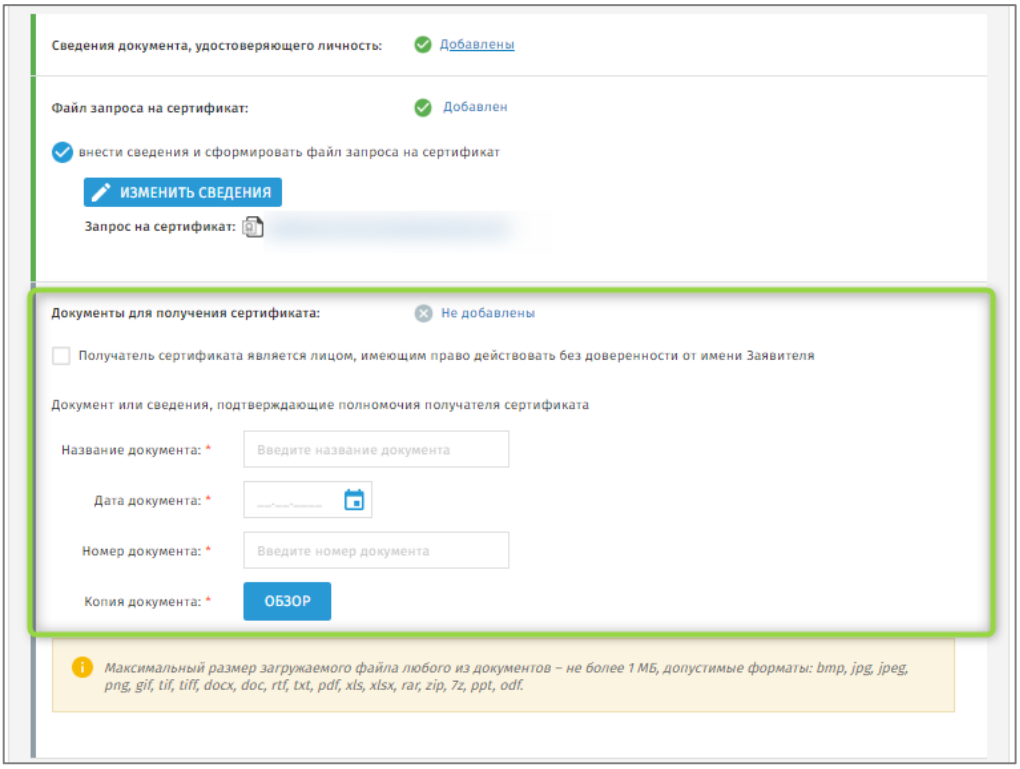


Рисунок 19 Блок «Документы для получения сертификата»

23. Введите номер контактного телефона (Рисунок 20).



Рисунок 20. Поле ввода контактного телефона

24. При необходимости измените адрес электронной почты для уведомлений, обновив данные в поле «Дополнительный адрес электронной почты для уведомлений» и нажав на кнопку «Сохранить адрес» (Рисунок 21).

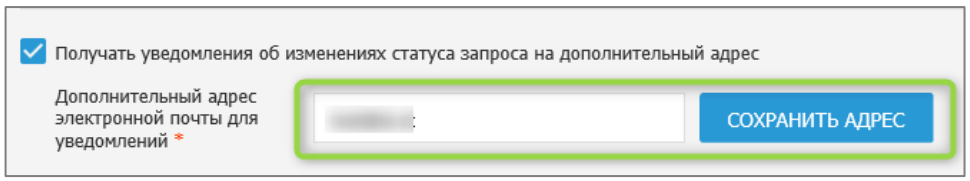


Рисунок 21. Сохранение дополнительного адреса электронной почты для уведомлений

Нажмите на кнопку «Подписать заявление и подать запрос» (Рисунок 22)

Важно! Для доступа к карточке запроса необходимо будет авторизоваться на Портале заявителя с помощью ЕСИА.

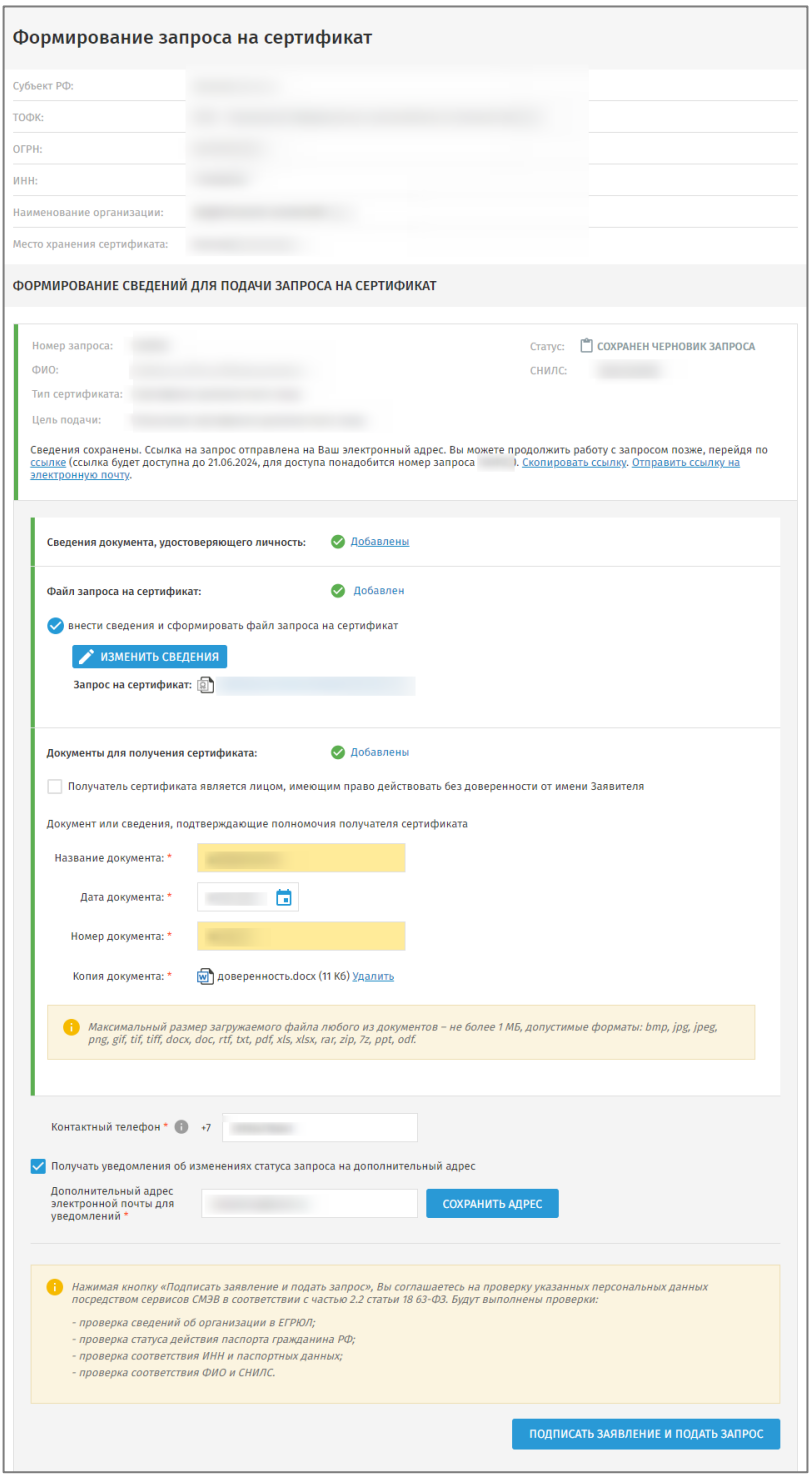


Рисунок 22. Подача запроса на странице «Формирование сведений для подачи запроса на сертификат»

25. В отобразившейся печатной форме заявления на выдачу квалифицированного сертификата проверьте внесенные сведения и нажмите на кнопку «Подписать» (Рисунок 23).

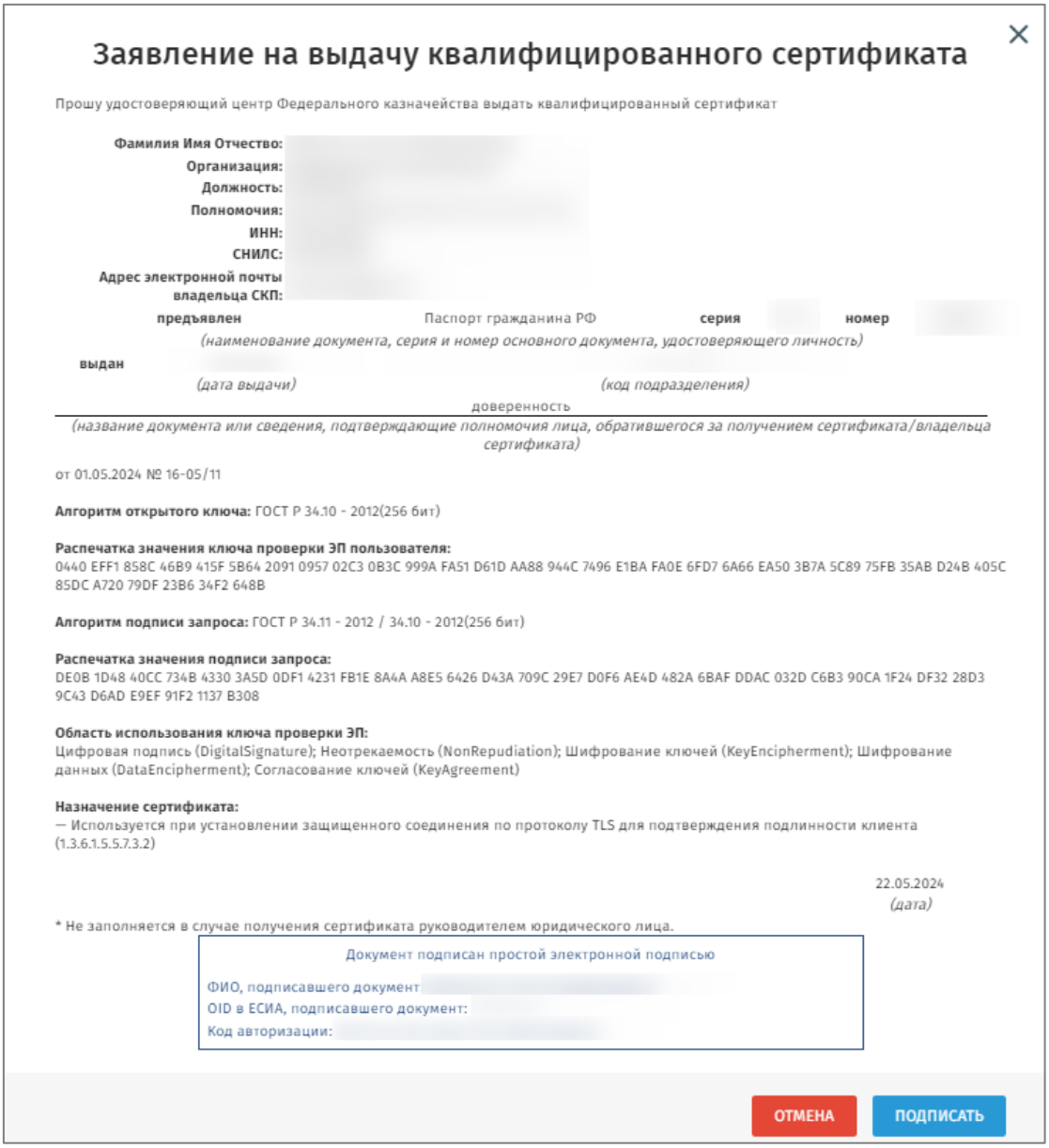


Рисунок 23. Заявление на выдачу квалифицированного сертификата

26. В отобразившейся форме «Передать сведения запроса в УЦ ФК?» ознакомьтесь с информацией и нажмите на кнопку «Передать» (Рисунок 24).

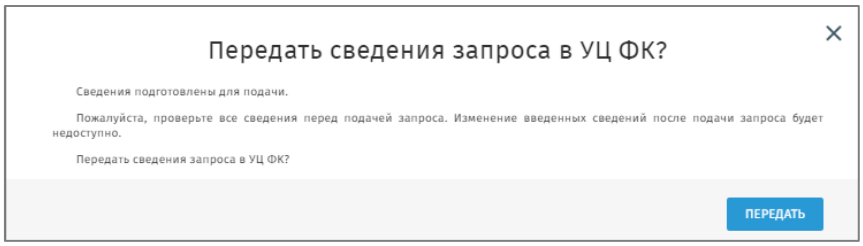


Рисунок 24. Отображение формы «Передать сведения запроса в УЦ ФК?»

27. Запрос будет сформирован и отправлен на проверку сервисами СМЭВ. Отобразится памятка по предоставлению комплекта документов и сведений в Удостоверяющий центр Федерального казначейства, которую можно распечатать, нажав на кнопку «Печать» (Рисунок 25).

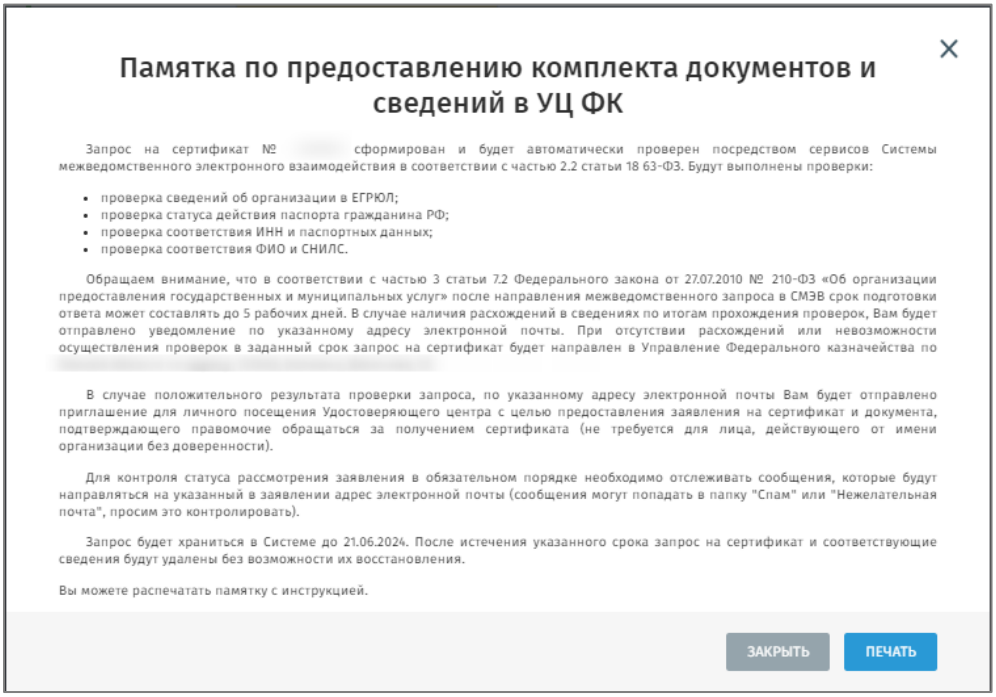


Рисунок 25. Памятка по предоставлению комплекта документов и сведений в УЦ ФК

28. После успешных проверок сведений запроса на создание сертификата с помощью сервисов СМЭВ, запрос автоматически передается в подсистему ВРС для рассмотрения оператором УЦ. В случае нахождения расхождений сведений запроса и сведений, полученных из СМЭВ, запрос отклоняется, и получатель сертификата получает соответствующее уведомление.

29. Оператор УЦ осуществляет проверку пакета электронных документов на создание сертификата. В случае положительного результата проверки, Оператор УЦ согласовывает запрос в подсистеме ВРС и осуществляется изготовление сертификата.

30. Если Оператор УЦ отклоняет запрос в подсистеме ВРС, запрос переходит в статус «Отклонен», о чем получателю сертификата отправляется соответствующее уведомление.

Скачивание полученного сертификата

1. После того, как сертификат был изготовлен, перейдите на карточку запроса на получение сертификата на Портале заявителя с помощью одного из способов:

   a. По ссылке из уведомления об изготовлении сертификата;

b. На Портале заявителя при переходе на вкладку «Мои запросы»;

Важно! *Для доступа к карточке запроса необходимо авторизоваться на Портале заявителя с помощью ЕСИА.*

2. На карточке запроса на получение сертификата нажмите на кнопку «Скачать сертификат» (Рисунок 26).

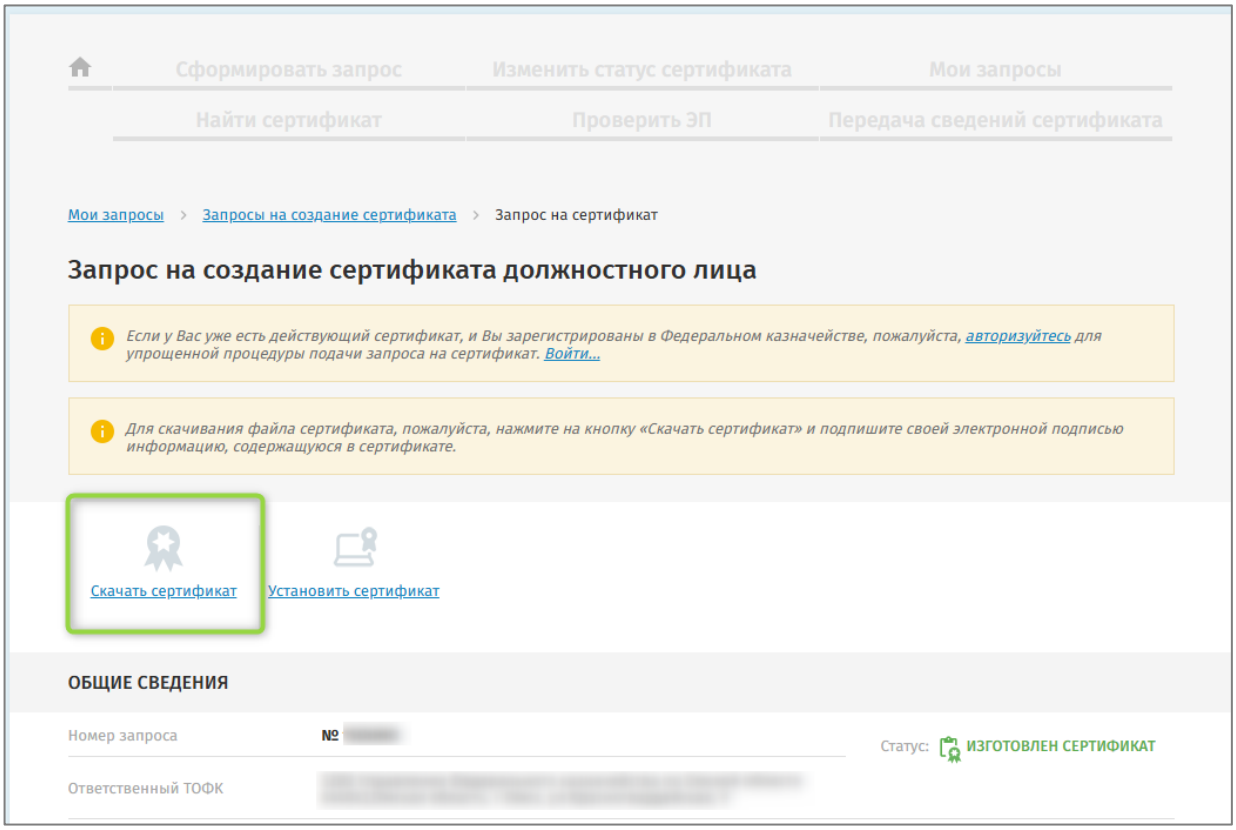


Рисунок 26. Карточка запроса – кнопка «Скачать сертификат»

3. На открывшейся форме «Расписка в ознакомлении с информацией, содержащейся в квалифицированном сертификате» ознакомьтесь с Руководством по обеспечению безопасности использования квалифицированной электронной подписи и средства квалифицированной электронной подписи и подтвердите ознакомление и подтвердите ознакомление (Рисунок 27).

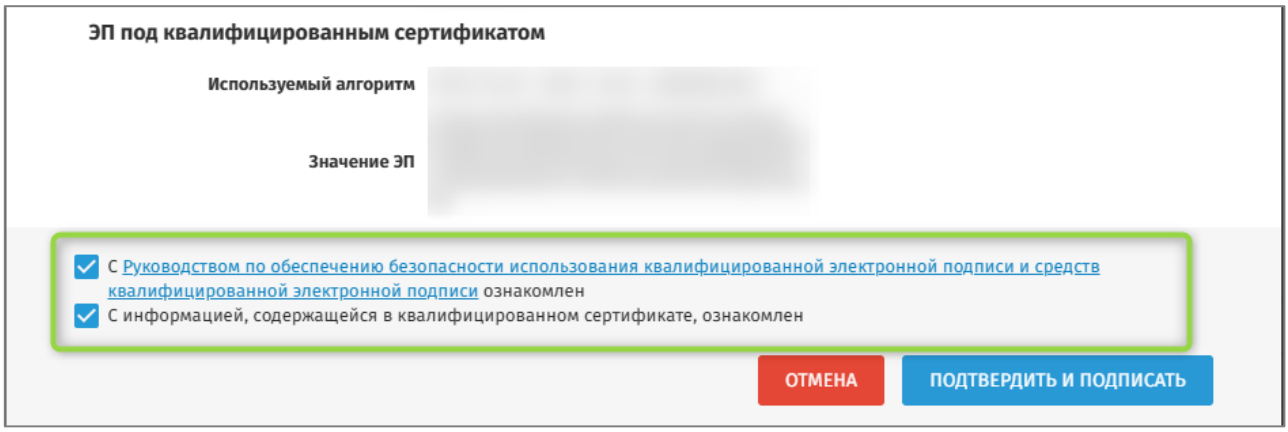


Рисунок 27. Предпечатная форма «Расписка в ознакомлении с информацией, содержащейся в квалифицированном сертификате» - блок элементов для подтверждения

4. Нажмите на кнопку «Подтвердить и подписать» и подпишите сведения .
5. После подтверждения ознакомления с информацией, содержащейся в квалифицированном сертификате файл сертификата автоматически начнет скачиваться на АРМ.