**Технологическая инструкция**

**по ПОДКЛЮЧЕНИЮ пользователей К Государственной информационной системе обязательного медицинского страхования (ГИС ОМС) С ИСПОЛЬЗОВАНИЕМ КВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСИ**

Редакция 1.4.

МОСКВА, 2020

**Аннотация**

Настоящий документ является инструкцией по защищенному удаленному подключению пользователей к подсистеме «Документы ОМС» государственной информационной системы обязательного медицинского страхования (ГИС ОМС) (далее – Система) с использованием квалифицированного сертификата ключа проверки электронной подписи (далее – сертификат).

Настоящая инструкция не заменяет Руководство пользователя к Системе. Комплект руководств пользователя размещается в разделе «Методические материалы», доступном после входа в Систему.

**Содержание**

[1. Проверка настроек АРМ перед Подключением к ГИС оМС 4](#_Toc58582262)

[1.1. Проверка наличия КриптоПро 4](#_Toc58582263)

[1.2. Проверка установленных сертификатов 5](#_Toc58582264)

[2. Требования к аппаратно-техническим и программным средствам 8](#_Toc58582265)

[2.1. Требования к техническому обеспечению 8](#_Toc58582266)

[2.2. Требования к программному обеспечению 8](#_Toc58582267)

[2.3. Требования к сертификату электронной подписи 8](#_Toc58582268)

[2.4. Что делать, если у Вас нет действующего сертификата электронной подписи 9](#_Toc58582269)

[2.5. Настройка программного обеспечения 10](#_Toc58582270)

[2.5.1. Установка криптопровайдера «КриптоПро CSP» 10](#_Toc58582271)

[2.5.2. Установка и настройка КриптоПро ЭЦП Browser plug-in 11](#_Toc58582272)

[2.5.3. Установка драйвера используемого носителя ключевой информации сертификата пользователя 12](#_Toc58582273)

[2.5.4. Установка личного сертификата и сертификата доверенного корневого центра сертификации 18](#_Toc58582274)

[2.5.5. Установка сертификатов промежуточных центров сертификации 29](#_Toc58582275)

[2.5.6. Проверка установки личного сертификата электронной подписи 41](#_Toc58582276)

[2.5.7. Настройка «Яндекс.Браузер» 42](#_Toc58582277)

[3. Работа с подсистемой «Документы ОМС» ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОБЯЗАТЕЛЬНОГО МЕДИЦИНСКОГО СТРАХОВАНИЯ 44](#_Toc58582278)

[3.1. Вход в подсистему «Документы ОМС» государственной информационной системы обязательного медицинского страхования 44](#_Toc58582279)

[3.2. Работа в подразделе «Реестр заявок» 45](#_Toc58582280)

[3.2.1. Формирование заявки на регистрацию уполномоченных лиц участника системы 47](#_Toc58582281)

[3.2.2. Формирование заявки на изменение сведений и полномочий уполномоченных лиц участника системы 51](#_Toc58582282)

[3.2.3. Формирование заявки на прекращение доступа уполномоченных лиц участника системы 54](#_Toc58582283)

[3.2.4. Согласование заявок 56](#_Toc58582284)

[4. ПРОБЛЕМЫ при подключении к системе и их устранение 64](#_Toc58582285)

[4.1. Окно входа в Систему 64](#_Toc58582286)

[4.2. Иные ошибки 64](#_Toc58582287)

Проверка настроек АРМ перед Подключением к ГИС оМС

Перед началом подключения нужно выполнить проверку текущих настроек АРМ, так как если ранее с этого АРМа был настроен доступ к Подсистемам Электронного Бюджета или аналогичным системам использующем для авторизации и аутентификации протокол TLS (англ. transport layer security — Протокол защиты транспортного уровня), то в этом случае дополнительных действия по настройке подключения к ГИС ОМС не требуется.

## Проверка наличия КриптоПро

Для проверки наличия установленной программы КриптоПро откройте «Панель управления», Нажмите «Пуск – Служебные-Windows – Панель Управления.

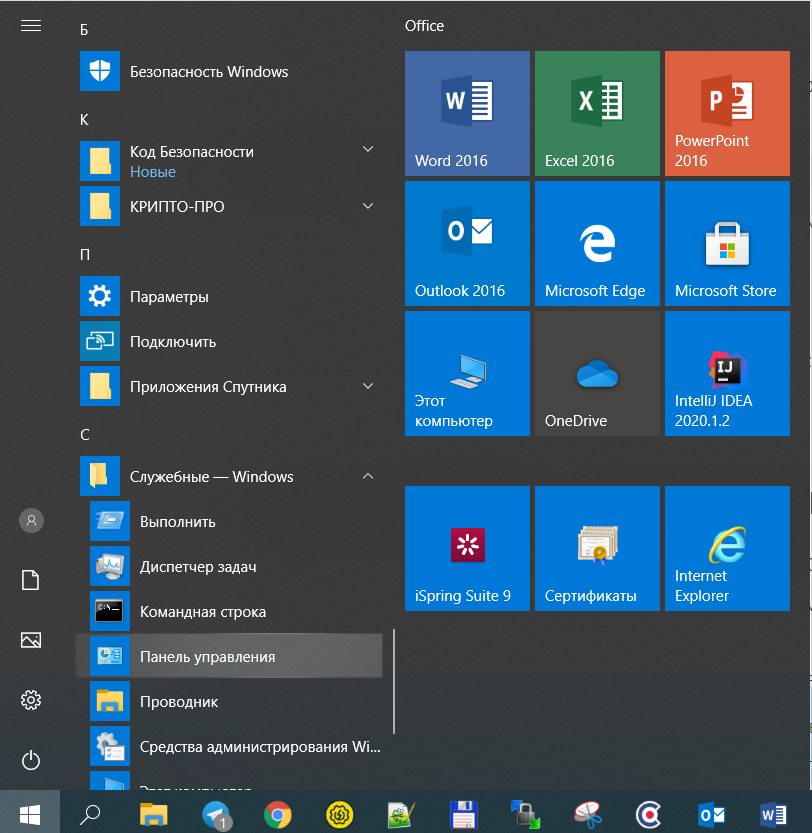


Рисунок 1 Вход в панель управления

После открытия Панели управления убедитесь, что на ней присутствует значок программы КриптоПро.

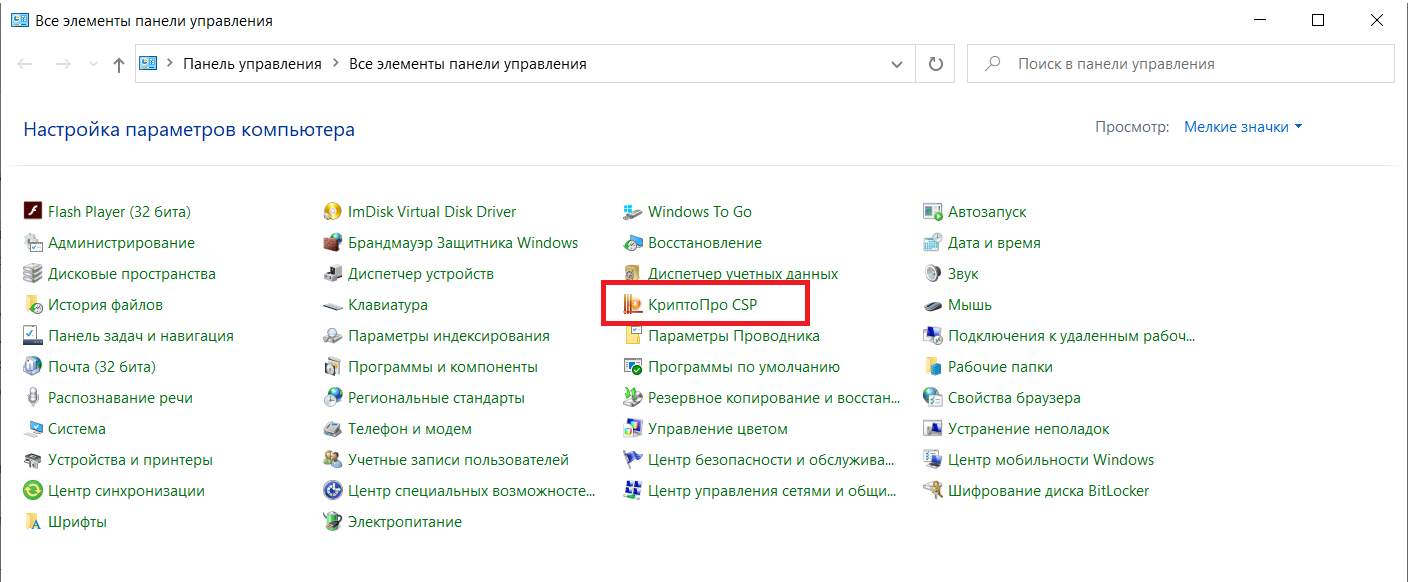


Рисунок 2 Панель управления

Двойным нажатием левой кнопки мыши откройте программу КриптоПро, убедитесь, что она имеет версию не ниже 4й и срок действия лицензии не истек.

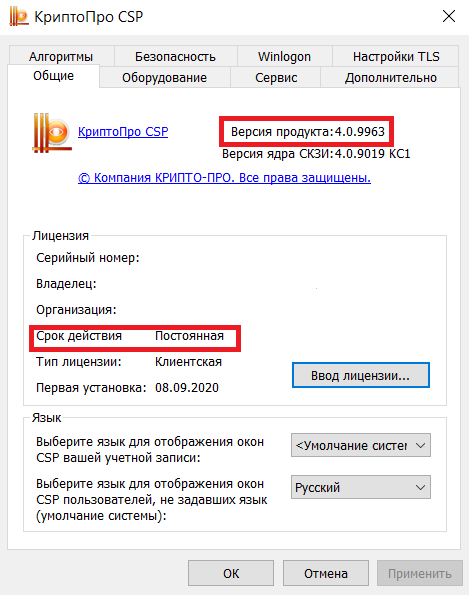


Рисунок 3 КриптоПро

## Проверка установленных сертификатов

В открытой программе КриптоПро перейдите на вкладку «Сервис» и нажмите кнопку «Посмотреть сертификаты в контейнере».

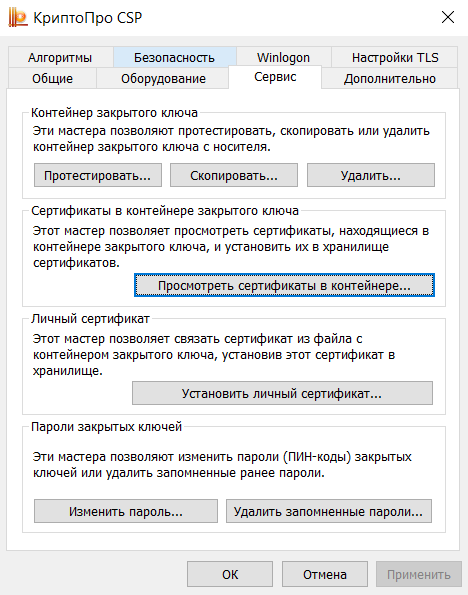


Рисунок 4 Сервисы

В открывшемся окне нажмите кнопку «По сертификату»

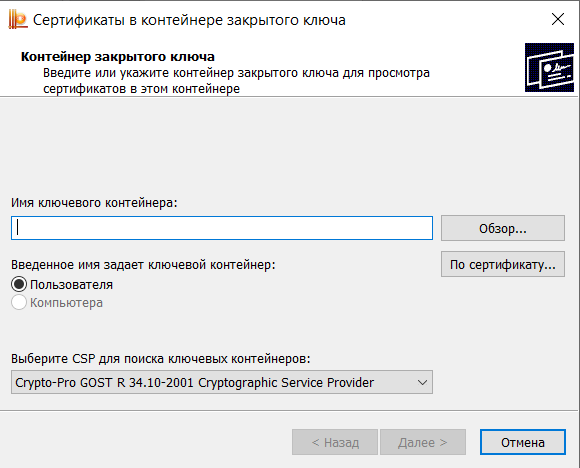


Рисунок 5 Просмотр сертификатов

В открывшемся окне убедится что в списке сертификатов есть ваш личный сертификат и если есть, то выбрать его и нажать кнопку «Посмотреть свойства сертификата».

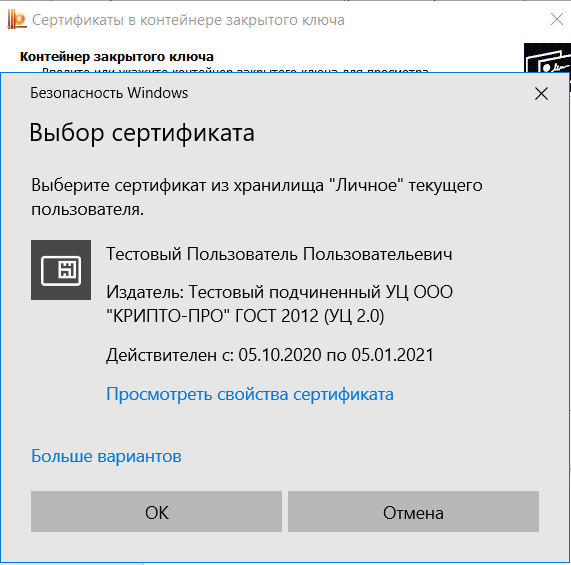


Рисунок 6 выбор сертификата

После вы нажатия кнопки откроется окно сертификата, в котором нужно убедится что сертификат Действителен (т.е. нет сообщений о том, что сертификат не действителен или к нему нет доверия), что у него не истек срок действия и что он умеет правильную цепочку корневых промежуточных сертификатов как показано на рисунке ниже.

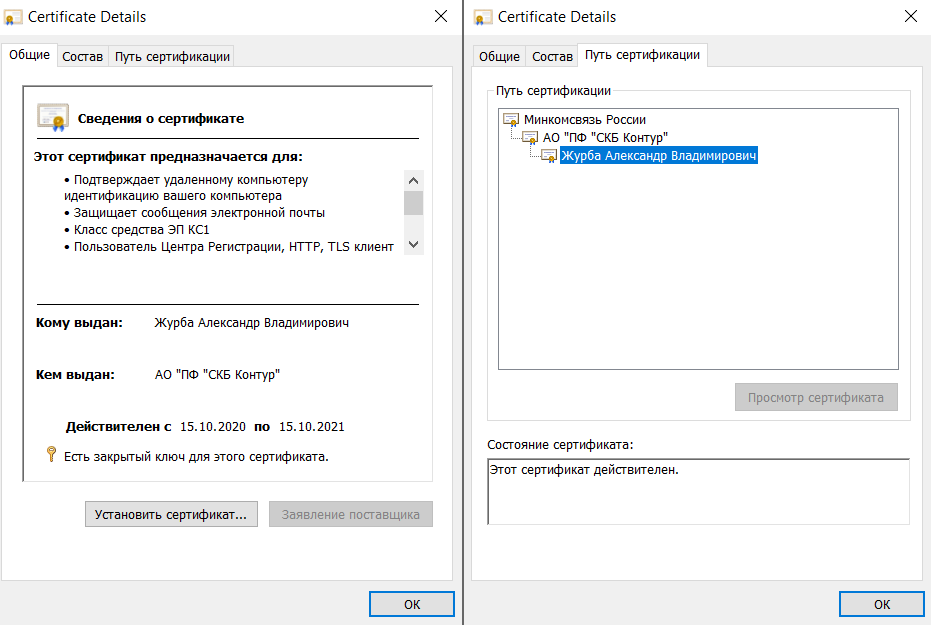


Рисунок 7 Действительный сертификат

Если выполнены все условия пунктов 1.1 и 1.2 то дальнейших настроек по подключению к ГИС ОМС не требуется.

Требования к аппаратно-техническим и программным средствам

## Требования к техническому обеспечению

Для автоматизированных рабочих мест пользователей Системы устанавливаются следующие минимальные технические требования:

1. Процессор с тактовой частотой не менее 1,2 МГц, не менее 2 ядер.
2. Объем оперативной памяти, не менее 2048 Мб;
3. Объем жесткого диска, не менее 50 Гб;
4. Клавиатура, манипулятор типа мышь;
5. Монитор SVGA (графический режим должен иметь разрешение не менее 1024x768);
6. USB-порт;
7. Квалифицированный сертификат ключа проверки электронной подписи.

На рабочем месте должен быть предоставлен доступ к сети Интернет со скоростью не менее 10 Мбит/сек.

## Требования к программному обеспечению

Программные средства, требуемые для обеспечения работы в Системе и возможности подписания документов электронной подписью:

1. Интернет-браузер «Яндекс.Браузер» или «Google Chromium GOST Версия 86.0.4240.111 и выше» с поддержкой отечественной криптографии;
2. Операционная система: Windows 7 и выше;
3. Cертифицированная версия «КриптоПро CSP» версия 4.0 и выше (в связи с переходом на ГОСТ Р 34.10‑2012)
4. КриптоПро ЭЦП Browser plug-in версия 2.0 и выше

## Требования к сертификату электронной подписи

Для утверждения (подписания) документов в Системе подходит любой, выданный аккредитованным удостоверяющим центром, действующий сертификат электронной подписи юридического лица с указанием физического лица (владельца сертификата), действующего от имени юридического лица на основании учредительных документов или доверенности.

Сертификат, в первую очередь, требуется для регистрации в подсистеме Документы ОМС и входа в подсистемы Документы ОМС, ЕТД и Портал Методические материалы Системы, а также, если пользователь наделен правами, для юридически значимых действий в подсистеме Документы ОМС.

В соответствии с Приказом ФСБ России от 27 декабря 2011 г. № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи» сертификат юридического лица должен содержать:

* уникальный номер квалифицированного сертификата;
* даты начала и окончания действия квалифицированного сертификата;
* наименование и место юридического лица, а также в случаях, предусмотренных Федеральным законом, фамилия, имя и отчество (если имеется) физического лица, действующего от имени владельца квалифицированного сертификата - юридического лица на основании учредительных документов юридического лица или доверенности;
* основной государственный регистрационный номер (далее - ОГРН) юридического лица - владельца квалифицированного сертификата;
* идентификационный номер налогоплательщика (далее - ИНН) юридического лица - владельца квалифицированного сертификата;
* ключ проверки ЭП;
* наименование используемого средства ЭП и (или) стандарты, требованиям которых соответствует ключ ЭП и ключ проверки ЭП;
* наименования средств ЭП и средств аккредитованного УЦ, которые использованы для создания ключа ЭП, ключа проверки ЭП, квалифицированного сертификата, а также реквизиты документа, подтверждающего соответствие указанных средств требованиям, установленным в соответствии с Федеральным законом;
* наименование и место нахождения аккредитованного УЦ, который выдал квалифицированный сертификат;
* номер квалифицированного сертификата аккредитованного УЦ;
* ограничения использования квалифицированного сертификата (если такие ограничения установлены).

Кроме того, для работы в подсистеме «Документы ОМС» сертификат должен иметь дополнительное поле СНИЛС (snils), с указанием номера СНИЛС уполномоченного лица – владельца сертификата.

## Что делать, если у Вас нет действующего сертификата электронной подписи

Для утверждения (подписания) документов в Системе необходимо получить в аккредитованном УЦ, действующий сертификат электронной подписи юридического лица с указанием физического лица (владельца сертификата), действующего от имени юридического лица на основании учредительных документов или доверенности.

## Настройка программного обеспечения

### Установка криптопровайдера «КриптоПро CSP»

1. Для установки криптопровайдера «КриптоПро CSP» на рабочем месте Пользователя необходимо выполнить следующие действия:

* Загрузите и запустите установочный файл сертифицированной версии «КриптоПро CSP», доступный для скачивания по адресу https://www.cryptopro.ru/products/csp/downloads. Окно приветствия установщика «КриптоПро CSP» представлено на рисунке (Рисунок 1).

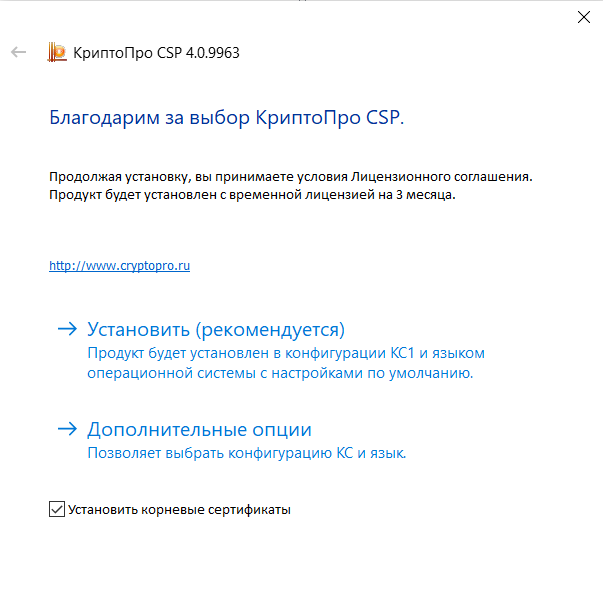


Рисунок 8. Окно приветствия «КриптоПРО CSP»

* Нажмите кнопку «Установить». После завершения процесса установки и настройки «КриптоПРО CSP» появится сообщение об успешной установке (Рисунок 2).

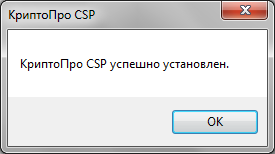


Рисунок 9. Установка «КриптоПро CSP»

При установке программы «КриптоПро CSP» может быть запрошен лицензионный ключ, который поставляется с установочным пакетом «КриптоПро CSP».

**Замечание:** Возможны проблемы при входе в Систему, в случае, если программа «КриптоПро CSP» не активирована и (или) истек пробный период.

* Далее, если в качестве носителя ключевой информации сертификата пользователя используется flash-накопитель или дискета, запустите «КриптоПро CSP» (Пуск/Все программы/КриптоПро/КриптоПро CSP).
* Откройте вкладку «Оборудование», нажмите кнопку «Настроить считыватели». В появившемся окне, выберите пункт «Все съемные диски» (Рисунок 3).

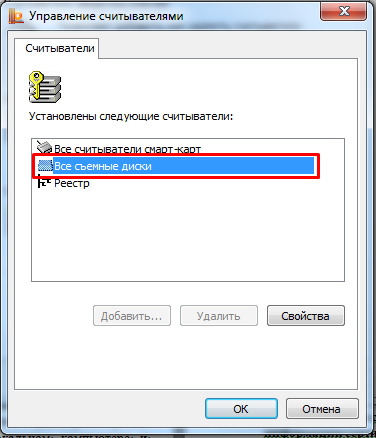


Рисунок 10. Настройка считывателей

* Нажмите кнопку «Добавить». Если кнопка добавить неактивна, перейдите во вкладку «Общие» и нажмите кнопку «Запустить с правами администратора».
* В окне «Мастера установки считывателя нажмите кнопку «Далее».
* В появившемся окне выберите считыватель, соответствующий usb‑порту, ключевому носителю на flash –накопителе или дисководу гибких дисков (дискет).
* В окне «Мастера установки считывателя нажмите кнопку «Далее» и «Готово».

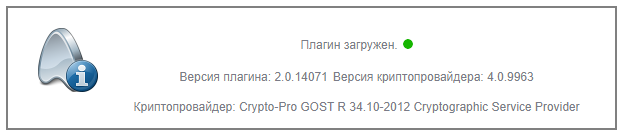
### Установка и настройка КриптоПро ЭЦП Browser plug-in

Для того, чтобы установить и настроить КриптоПро ЭЦП Browser plug-in на рабочем месте Пользователя перейдите по ссылке для скачивания: https://www.cryptopro.ru/products/cades/plugin.

В случае использования интернет-браузеров «Спутник» или «Яндекс.Браузер» с поддержкой отечественной криптографии **дополнительно** необходимо в указанных интернет-браузерах установить расширение «CryptoPro Extension for CAdES Browser Plug-in», доступное в «Интернет-магазине chrome» по адресу <https://chrome.google.com/webstore/detail/cryptopro-extension-for-c/iifchhfnnmpdbibifmljnfjhpififfog>

1. Для проверки корректности установки «КриптоПро ЭЦП Browser plug-in» необходимо пройти по указанному адресу <https://www.cryptopro.ru/sites/default/files/products/cades/demopage/cades_bes_sample.html>.

Если установка КриптоПро ЭЦП Browser plug-in прошла успешно, появится окно с надписью «Плагин загружен», указанием его версии и используемой Вами версии КриптоПро CSP (Рисунок 4).



**Рисунок 11. Проверка загрузи плагина**

### Установка драйвера используемого носителя ключевой информации сертификата пользователя

Если в качестве носителя ключевой информации сертификата пользователя используется носитель типа eToken (JaCarta) или Rutoken, необходимо выполнить установку драйвера соответствующего накопителя в ОС (если ранее не был установлен).

Если необходимый драйвер не установлен, необходимо:

1. **Драйвер носителя типа Rutoken**
2. Загрузите и запустите установочный файл, доступный на странице <http://www.rutoken.ru/support/download/drivers-for-windows/>. Окно приветствия установщика драйверов Rutoken представлено на рисунке (Рисунок 5).

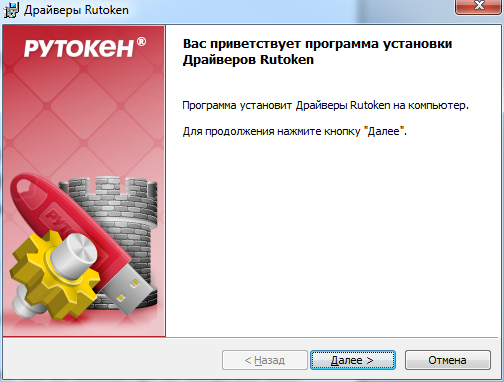


Рисунок 12. Экранная форма приветствия установщика драйвера Rutoken

1. Нажмите кнопку «Далее». На экране отобразится диалог о готовности к выполнению установки драйверов (Рисунок 6).

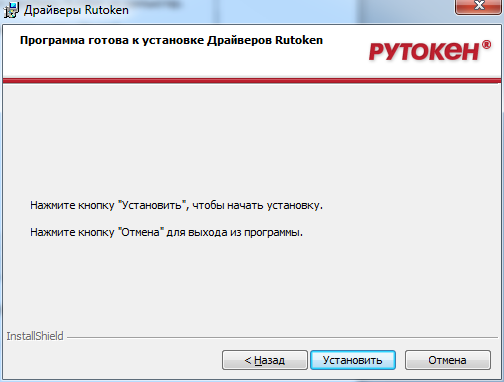


Рисунок 13. Сообщение о готовности к выполнению установки драйверов

1. Нажмите кнопку «Установить». Начнется установка драйверов Rutoken на АРМ пользователя. Установка может занять несколько минут, информация о прогрессе установки выводится в окне, представленном на рисунке (Рисунок 7).

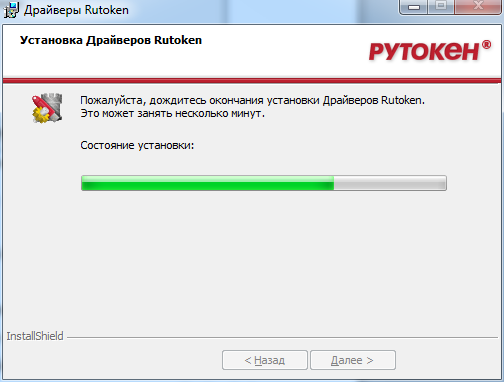


Рисунок 14. Окно, информирующее о прогрессе установки драйверов Rutoken

После завершения установки пользователю будет выведено сообщение об успешной установке драйверов, представленное на рисунке (Рисунок 8).

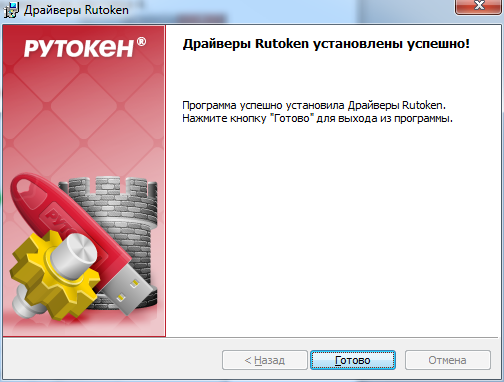


Рисунок 15. Сообщение об успешной установке драйверов Rutoken.

1. Нажмите кнопку «Готово». Окно установщика драйверов Rutoken будет закрыто.
2. В случае появления диалога о необходимости перезагрузки автоматизированного рабочего места Пользователя, ответить отрицательно.
3. **Драйвер носителя типа eToken (JaCarta)**
4. Загрузите и запустите установочный файл, доступный на странице  [https://www.aladdin-rd.ru/support/downloads/jacarta/](http://www.aladdin-rd.ru/support/downloads/). Окно приветствия установщика драйвера eToken представлено на рисунке (Рисунок 9).

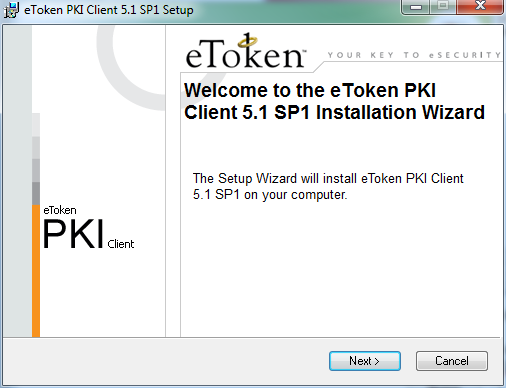


Рисунок 16. Экранная форма приветствия установщика драйверов eToken

1. Нажмите кнопку «Next». На экране появится диалог выбора языка, который будет использован в устанавливаемом ПО (Рисунок 10).

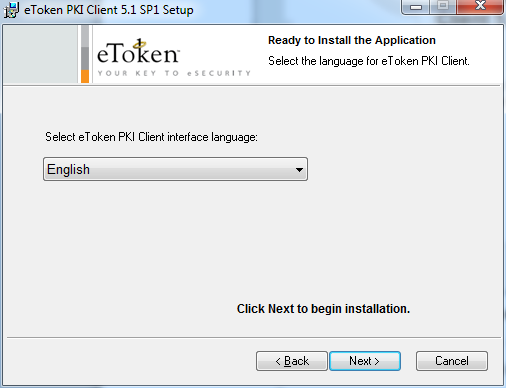


Рисунок 17. Окно выбора языка программы, управляющей ключевыми носителями eToken

1. В поле выберите язык «Русский» и нажмите «Next». На экране появится диалог лицензионного соглашения (Рисунок 11).

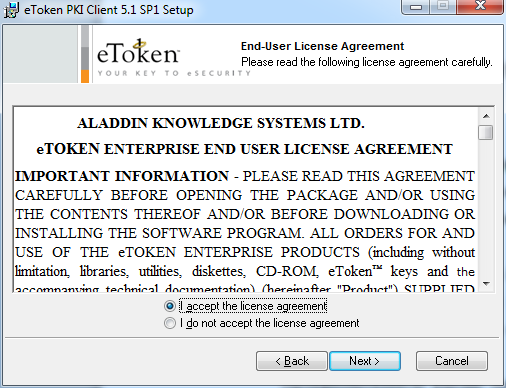


Рисунок 18. Окно просмотра лицензионного соглашения

1. Выберете пункт «I accept the license agreement» и нажмите кнопку «Next». На экране появится диалог выбора пути установки компонентов устанавливаемого ПО (Рисунок 12).

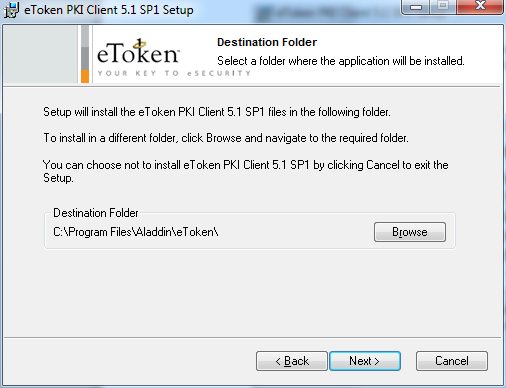


Рисунок 19. Окно выбора пути для установки программы

1. Оставьте путь установки по умолчанию либо измените на необходимый. Нажмите кнопку «Next».

Начнется установка программы и драйверов. Диалог процесса установки представлено на рисунке (Рисунок 13).

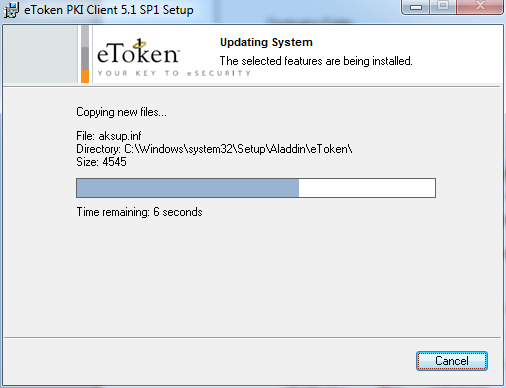


Рисунок 20. Прогресс установки драйверов eToken

После завершения установки пользователю будет выведено сообщение об успешной установке драйверов, представленное на рисунке (Рисунок 14).

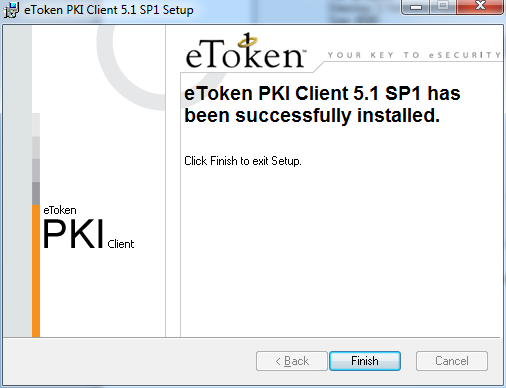


Рисунок 14. Сообщение об успешной установке драйверов Rutoken

1. Нажмите кнопку «Finish». Окно установщика драйверов будет закрыто.
2. В случае появления диалога о необходимости перезагрузки автоматизированного рабочего места пользователя, ответить отрицательно или осуществить перезагрузку.

### Установка личного сертификата и сертификата доверенного корневого центра сертификации

Установка личного сертификата электронной подписи пользователя и сертификата доверенного корневого центра сертификации выполняется под учетной записью пользователя, которая будет использоваться в процессе входа в личный кабинет Системы.

Инструкция по установке личного сертификата электронной подписи и сертификата доверенного корневого центра сертификации обычно предоставляется удостоверяющим центром при выдаче сертификата электронной подписи.

#### Установка личного сертификата электронной подписи

Для установки сертификатов на рабочем месте Пользователя необходимо выполнить следующие действия:

1. Запустите на своем рабочем компьютере «КриптоПро CSP» (Пуск/Все программы/КриптоПро/ КриптоПро CSP). В открывшемся окне на вкладке «Сервис» необходимо нажать на кнопку «Просмотреть сертификаты в контейнере» (Рисунок 15).

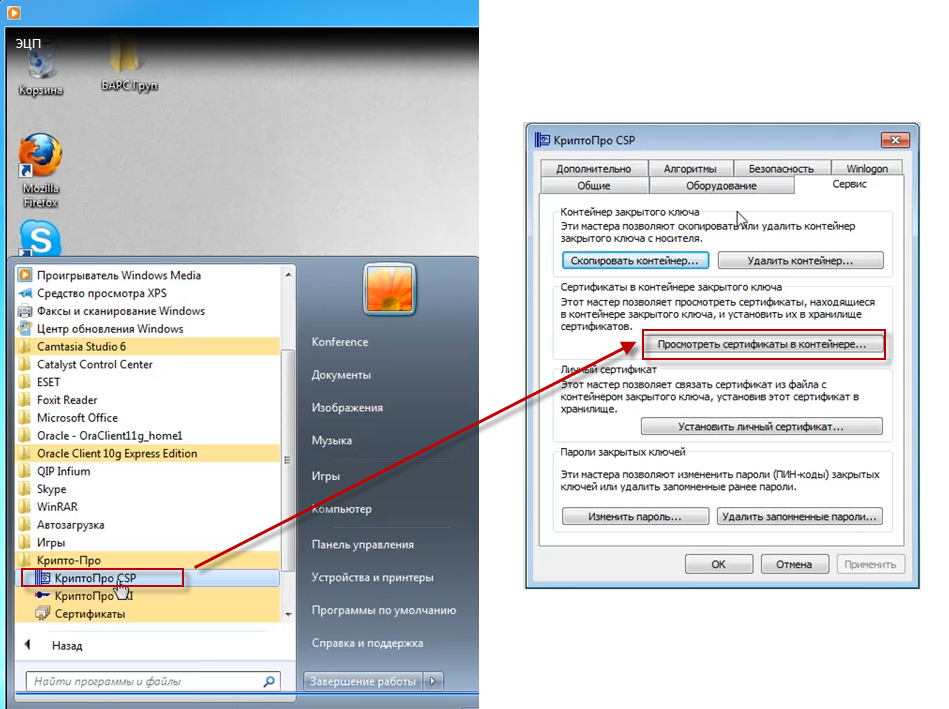


Рисунок 15. Добавление ключа в хранилище

1. В открывшемся диалоговом окне «Сертификаты в контейнере закрытого ключа» нажмите на кнопку «Обзор…» и выберите используемый ключ (предварительно установленный в USB-порт или дисковод ключ, предоставленный на носителе ruToken/eToken/JaCarta, помещённый в реестр) (Рисунок 16). После этого нажмите на кнопку «ОК».

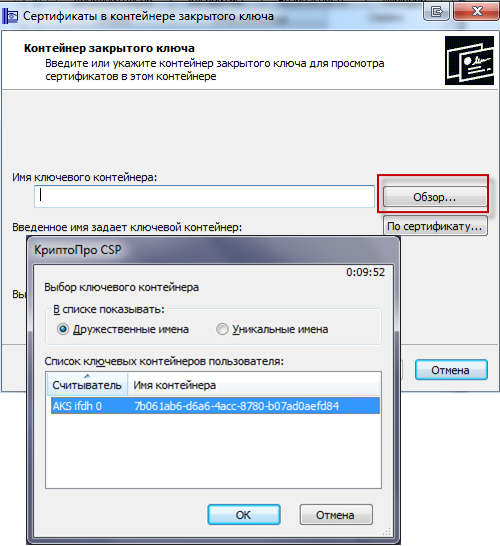


Рисунок 16. Выбор ключевого контейнера

1. Для завершения выбора контейнера закрытого ключа нажмите кнопку «Далее» (Рисунок 17)



Рисунок 17. Выбор контейнера закрытого ключа

1. В открывшемся диалоговом окне нажмите на кнопку «Установить» (Рисунок 18):

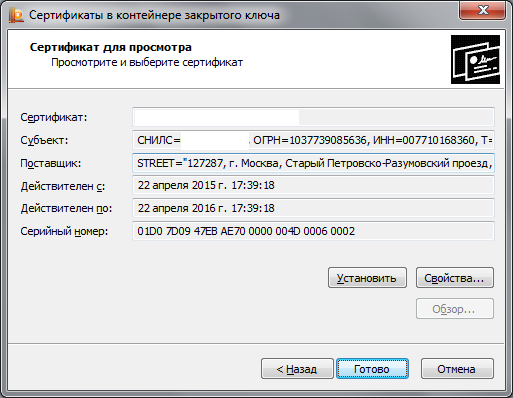


Рисунок 218. Выбор сертификата

1. После установки появится уведомление об успешной установке сертификата. Для подтверждения нажмите кнопку «ОК» (Рисунок 19).

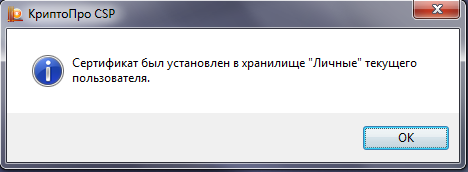


Рисунок 19. Уведомление об успешной установке сертификата

Если в процессе выполнения действий появится сообщение «A new certificate was added to the certificate store» (Рисунок 20), необходимо нажать кнопку «Cancel».

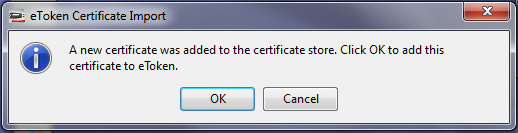


Рисунок 20. Сообщение драйвера eToken

#### Установка сертификата Минкомсвязи России в качестве доверенного корневого центра сертификации

Чтобы проверить установлен ли уже на компьютере сертификат Минкомсвязи России в качестве доверенного корневого центра сертификации, необходимо:

1. Открыть программу Крипто Про CSP в меню «Пуск». Перейти на вкладку «Сервис», нажать кнопку «Просмотреть сертификаты в контейнере…», нажать кнопку «По сертификату…», из списка выбрать электронную подпись пользователя (Рисунок 21) и нажать кнопку «Просмотреть свойства сертификата».

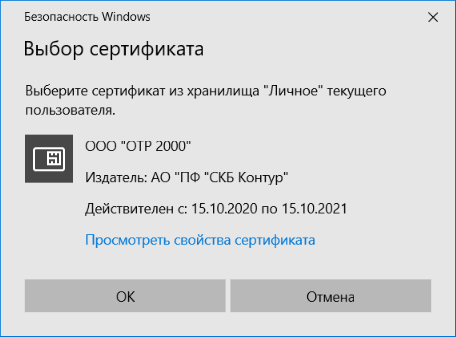


Рисунок 21. Окно просмотра сертификатов

1. В открывшемся окне перейдите на вкладку «Путь сертификации» (Рисунок 22), может отображаться две ситуации, когда сертификат Минкомсвязи России уже установлен и когда отсутствует.

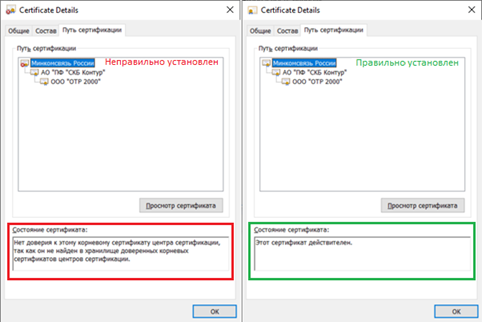


Рисунок 22. Окно просмотра электронной подписи пользователя

1. Проверьте, установлен ли сертификат Минкомсвязи России (сертификат доверенного корневого центра сертификации).

Знак (1)  свидетельствует о том, что сертификат не установлен.

Знак (2)  свидетельствует о том, что сертификат установлен.

Если у первого в списке сертификата стоит знак 1, то сертификат Минкомсвязи России не установлен в качестве доверенного корневого сертификата, необходимо добавить его в доверенные корневые центры сертификации (пункт 6 данного подраздела).

Если у первого в списке сертификата стоит знак 2, то сертификат Минкомсвязи России установлен. Необходимо проверить его идентификатор ключа субъекта (пункт 4 данного подраздела).

1. Для проверки идентификатора ключа субъекта у сертификата Минкомсвязи России необходимо открыть информацию о нём. Для этого в просмотре информации личного сертификата электронной подписи перейти на вкладку «Пусть сертификации» (Рисунок 23) и выбрать сертификат Минкомсвязи России в списке левой кнопкой мыши, затем нажать кнопку «Просмотр сертификата».

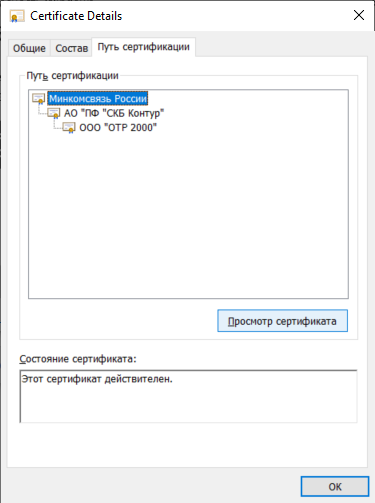


Рисунок 23. Вкладка «Путь сертификации»

1. В открывшемся окне сертификата Минкомсвязи России перейти на вкладку «Состав» и найти строку «Идентификатор ключа субъекта» (Рисунок 24), он должен быть равен c254f1b46bd44cb7e06d36b42390f1fec33c9b06  
   Если значение не совпадает, необходимо загрузить его с сайта ФОМС и установить (пункт 6 данного подраздела).

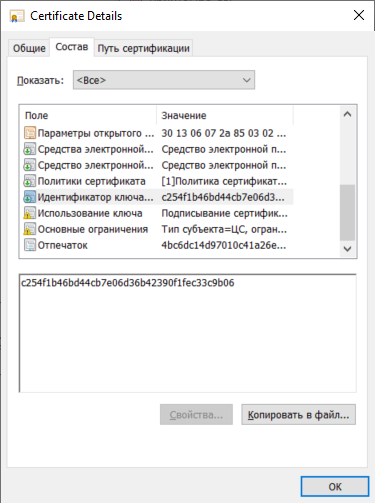


Рисунок 24. Просмотр Идентификатора ключа субъекта сертификата Минкомсвязи Россиии

1. Установка корневого сертификата Минкомсвязи России в доверенные корневые центры сертификации

Для установки корневого сертификата Минкомсвязи России его необходимо скачать с сайта ФОМС по ссылке: <http://www.ffoms.ru/system-oms/Certification/certification-doc/%D0%A3%D0%A6%20%D0%9C%D0%98%D0%9D%D0%9A%D0%9E%D0%9C%D0%A1%D0%92%D0%AF%D0%97%D0%AC%2034.10.2012.cer> имя файла «УЦ МИНКОМСВЯЗЬ 34.10.2012.cer». Запустить двойным кликом левой кнопки мыши файл «УЦ МИНКОМСВЯЗЬ 34.10.2012.cer» (Рисунок 25) после скачивания.

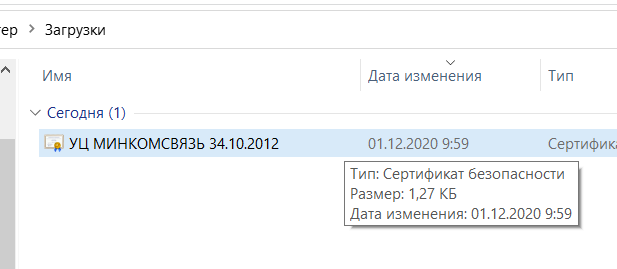


Рисунок25. Скаченный файл сертификата Минкомсвязи России

В открывшемся окне просмотра сертификата Минкомсвязи Россиии нажать кнопку «Установить сертификат…» (Рисунок 26).

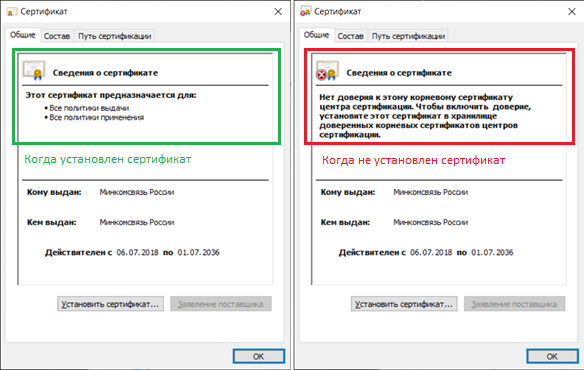


Рисунок 26. Окно просмотра сертификата Минкомсвязи России

Выбрать пункт «Поместить все сертификаты в следующее хранилище» (Рисунок 27) и нажать «Обзор…»

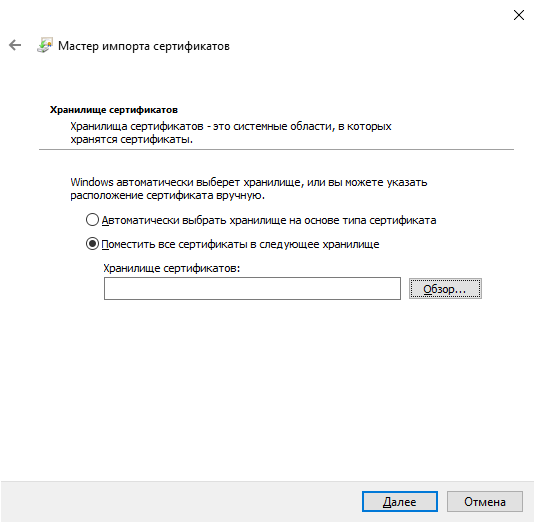


Рисунок 27. Мастер импорта сертификатов

Выбрать пункт «Доверенные корневые центры сертификации» (Рисунок 28). Нажмите кнопку «Ок».

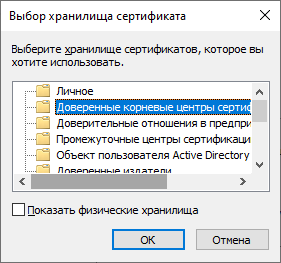


Рисунок 28. Выбор хранилища сертификатов

1. В окне «Мастер импорта сертификатов» нажмите кнопку «Далее» затем кнопку «Готово». В случае успешного импорта сертификата отобразится диалог «Импорт успешно выполнен.», где необходимо нажать кнопку «ОК». Если появится окно «Предупреждение безопасности» нажмите кнопку «Да».
2. Чтобы проверить корректную установку корневого сертификата Минкомсвязи России необходимо в просмотре информации (шаги 1 и 2 данного подраздела) об электронной подписи пользователя перейти на вкладку «Пусть сертификации». При корректной установке должен отображаться знак 2 слева от сертификата Минкомсвязи (рисунок 29)

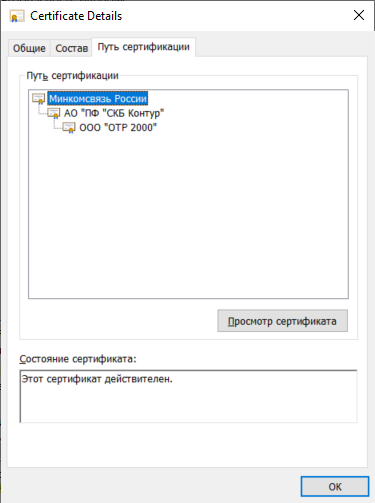


Рисунок 29. Вкладка «Путь сертификации» сертификата пользователя

### Установка сертификатов промежуточных центров сертификации

Для корректной работы необходимо установить сертификаты промежуточных центров сертификации:

* сертификат промежуточного удостоверяющего центра ФОМС для корректного соединения браузера к сайту <https://gisoms.ffoms.gov.ru/>
* сертификат удостоверяющего центра, выдавшего сертификат ЭП пользователя, для корректной аутентификации пользователя и наложения ЭП.

#### Установка сертификата промежуточного удостоверяющего центра ФОМС

1. Пользователю необходимо убедиться, что на рабочем компьютере установлен сертификат Минкомсвязи России в доверенные корневые центры сертификации. Для этого необходимо открыть программу Крипто Про CSP в меню «Пуск». Перейти на вкладку «Сервис», нажать кнопку «Просмотреть сертификаты в контейнере…», из списка выбрать нужную электронную подпись и нажать кнопку «Просмотреть свойства сертификата». Перейти на вкладку «Путь сертификации». При корректной установке должен отображаться знак  слева от сертификата Минкомсвязи России (Рисунок 30).

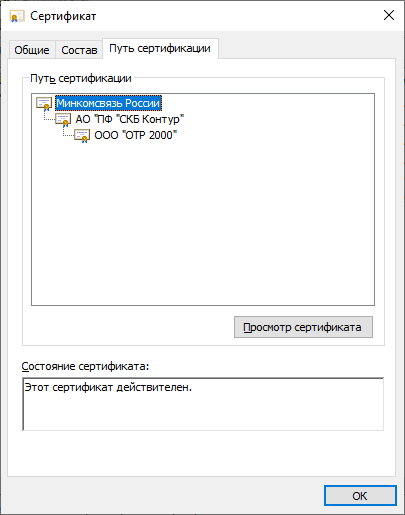


Рисунок 30. Вкладка «Путь сертификации» сертификата пользователя

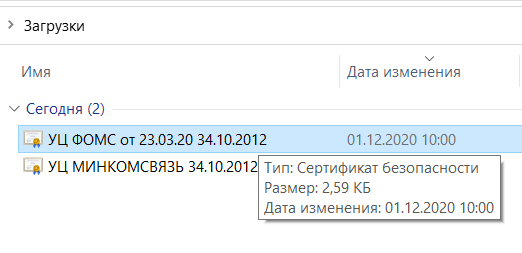
1. Загрузите файл сертификата УЦ ФОМС с сайта ФОМС, расположенного по адресу <http://www.ffoms.ru/system-oms/Certification/certification-doc/%D0%A3%D0%A6%20%D0%A4%D0%9E%D0%9C%D0%A1%20%D0%BE%D1%82%2023.03.20%2034.10.2012.cer> имя файла «УЦ ФОМС от 23.03.20 34.10.2012.cer».
2. Откройте загруженный файл «УЦ ФОМС от 23.03.20 34.10.2012.cer» (Рисунок 31) двойным кликом левой кнопки мыши. 

Рисунок 31. Загруженный файл сертификат УЦ ФОМС

1. В появившемся окне нажмите на кнопку «Установить сертификат…» (Рисунок 32). На экране отобразится мастер импорта сертификатов, где необходимо нажать кнопку «Далее»

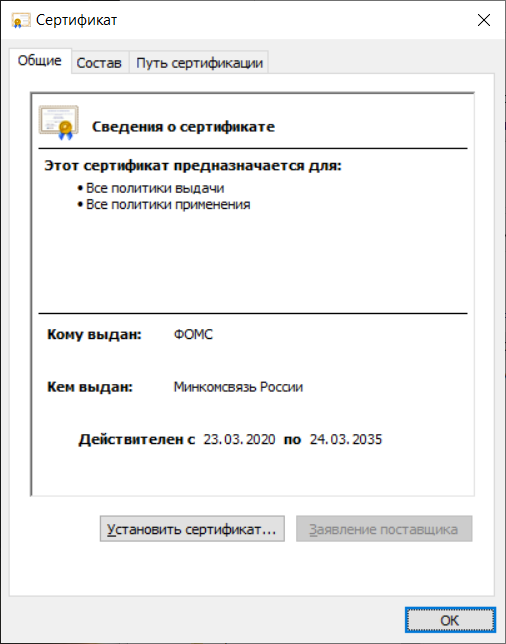


Рисунок 32. Окно просмотра сертификата УЦ ФОМС

1. В окне «Хранилище сертификата» (Рисунок 33) выбрать размещение сертификата вручную, указав поле «Поместить все сертификаты в следующее хранилище». Нажать кнопку «Обзор…».

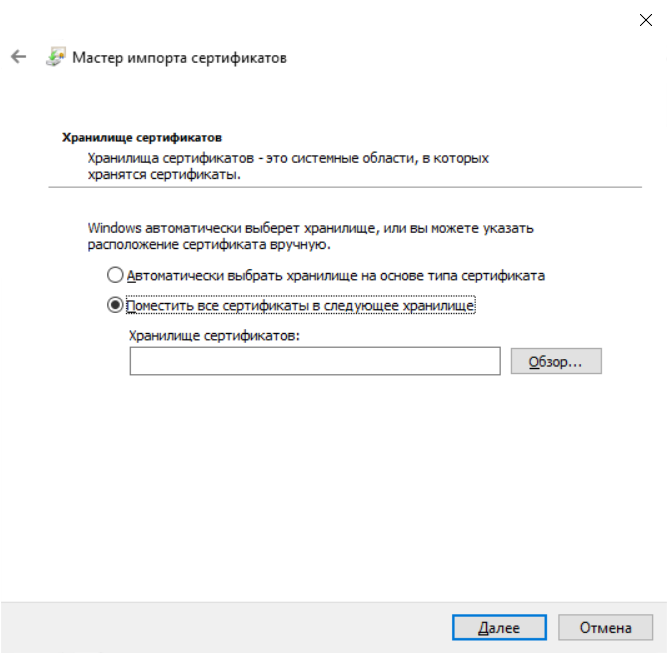


Рисунок 33. Мастер импорта сертификатов

1. В открывшемся окне выбор хранилища сертификатов выберите контейнер «Промежуточные центры сертификации». Нажмите кнопку «Ок». (Рисунок 34)

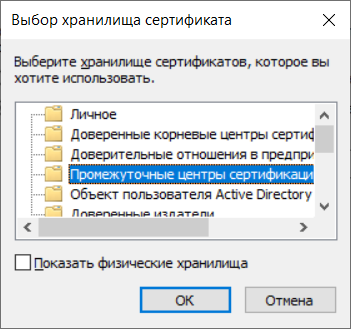


Рисунок 34. Промежуточные центры сертификации

1. В окне «Мастер импорта сертификатов» нажмите кнопку «Далее» затем кнопку «Готово». В случае успешного импорта сертификата отобразится диалог «Импорт успешно выполнен», где необходимо нажать кнопку «ОК». Если появится окно «Предупреждение безопасности» нажмите кнопку «Да».

#### Установка сертификата удостоверяющего центра, выдавшего сертификат ЭП пользователя

1. Обычно сертификат удостоверяющего центра, выдавшего сертификат ЭП пользователя, необходимо установить в качестве сертификата промежуточного центра сертификации. Для этого необходимо открыть программу Крипто Про CSP в меню «Пуск». Перейти на вкладку «Сервис», нажать кнопку «Просмотреть сертификаты в контейнере…», из списка выбрать нужную электронную подпись и нажать кнопку «Просмотреть свойства сертификата». Перейти на вкладку «Путь сертификации» (Рисунок 35), выбрать вторую строку с наименованием удостоверяющего центра, выдавшего электронную подпись, и нажать «Просмотр сертификата»

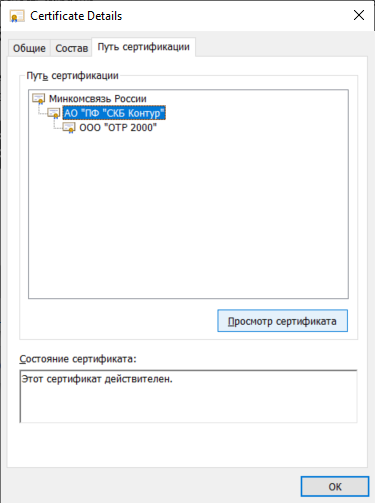


Рисунок 35. Вкладка «Путь сертификации»

1. Затем перейти во вкладку «Состав» и нажать кнопку «Копировать в файл» (Рисунок 36).

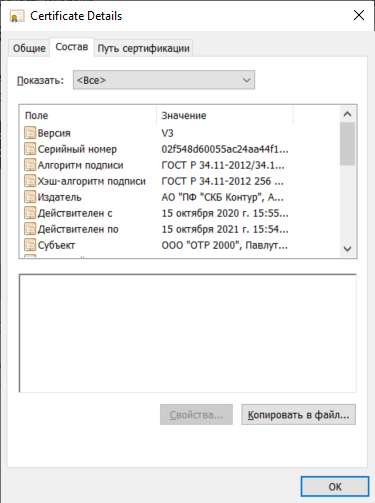


Рисунок 3622. Копирование сертификата в файл

1. В открывшемся Мастере экспорта сертификатов (Рисунок 37) нажмите на кнопку «Далее». Затем «Нет, не экспортировать закрытый ключ» и «Далее»

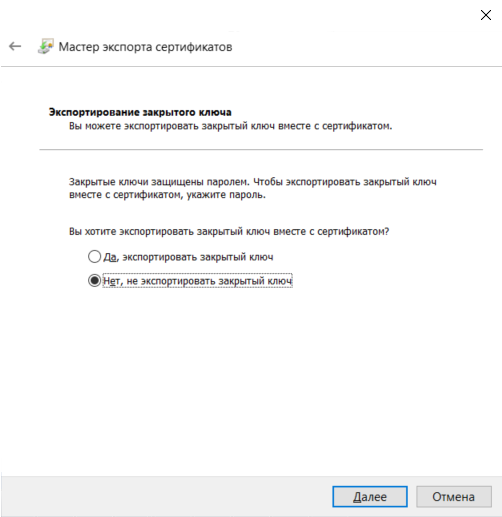


Рисунок 37. Мастер экспорта сертификатов

1. Убедитесь, что в открывшемся окне выбора формата экспортируемого сертификата выбран только вариант «Файлы Х.509 (.CER) в кодировке DER (Рисунок 38), затем нажмите кнопку «Далее».

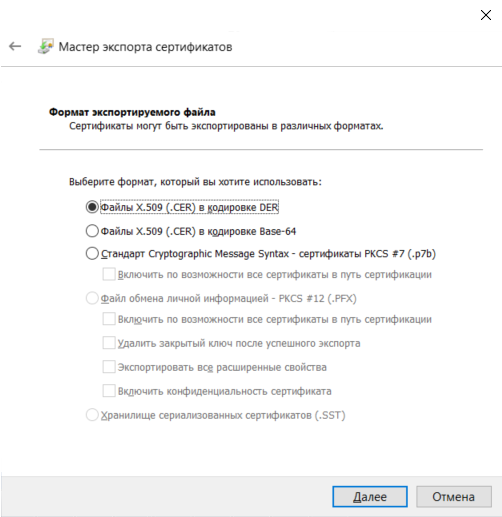


Рисунок 38. Мастер экспорта сертификатов, выбор формата экспортируемого файла.

1. В окне «Имя экспортируемого файла» нажмите кнопку «Обзор…».
2. В диалоговом окне «Сохранить как» перейдите в папку «Рабочий стол», в поле «Имя файла» укажите «ПромежуточныйУЦ», нажмите кнопку «Сохранить».
3. Убедитесь, что в окне «Имя экспортируемого файла» в поле «Имя файла» (Рисунок 39) верно отобразился путь сохранения сертификата (например, C:\Users\Users\Desktop\ ПромежуточныйУЦ.cer). Нажмите кнопку «Далее».

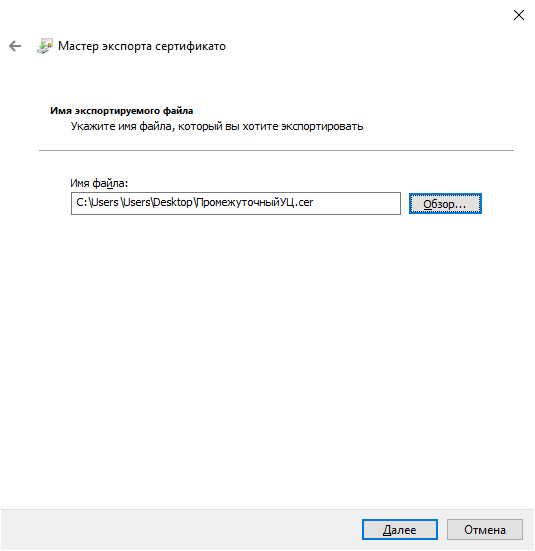


Рисунок 39. Мастер экспорта сертификатов. Имя сохраняемого файла.

1. Подтвердите успешный экспорт сертификата, нажав кнопку «ОК».
2. В окне «Завершение работы мастера экспорта сертификатов» нажмите кнопку «Готово»
3. Перейдите в папку «Рабочий стол», найдите и откройте файл «ПромежуточныйУЦ.cer».
4. В появившемся окне нажмите на кнопку «Установить сертификат…» (Рисунок 40). На экране отобразится мастер импорта сертификатов, где необходимо нажать кнопку «Далее».

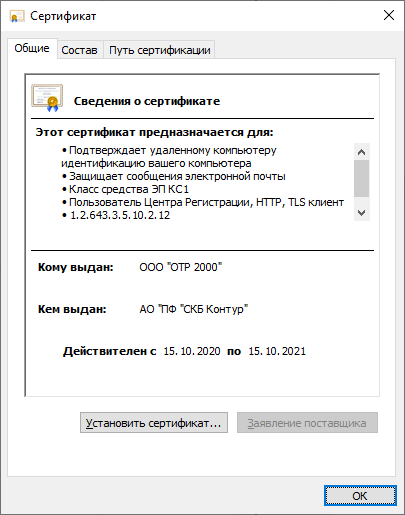


Рисунок 40. Установка корневого сертификата центра сертификации

1. В окне «Хранилище сертификата» (Рисунок 41) выбрать размещение сертификата вручную, указав поле «Поместить сертификаты в следующее хранилище». Нажать кнопку «Обзор…».

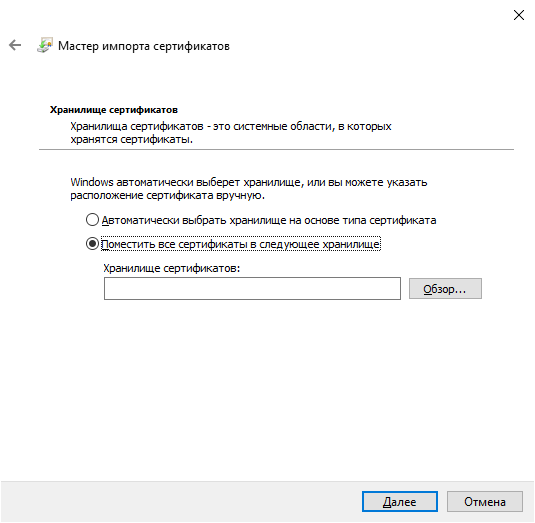


Рисунок 41. Выбор хранилища сертификата

1. В окне выбора хранилища сертификатов выберите контейнер «Промежуточные центры сертификации». Нажмите кнопку «Ок» (Рисунок 42).

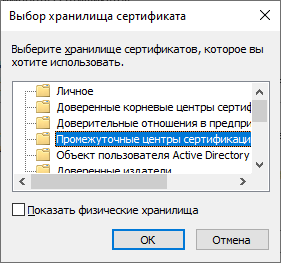


Рисунок 42. Выбор хранилища сертификата

1. В окне «Мастер импорта сертификатов» нажмите кнопку «Далее» затем кнопку «Готово». В случае успешного импорта сертификата отобразится диалог «Импорт успешно выполнен», где необходимо нажать кнопку «ОК». Если появится окно «Предупреждение безопасности» нажмите кнопку «Да».

### Проверка установки личного сертификата электронной подписи

Убедитесь, что личный сертификат электронной подписи успешно установлен в директории «Сертификаты – текущий пользователь – Личное – Сертификаты». Для этого:

* + - 1. Запустите утилиту «Сертификаты» расположенную в меню «Пуск: выберите «Выполнить» введите текст «Сертификаты», нажмите «ОК» и в открывшемся окне найдите данный сертификат в директории «Сертификаты–текущий пользователь – Личное – Сертификаты» (Рисунок 43).

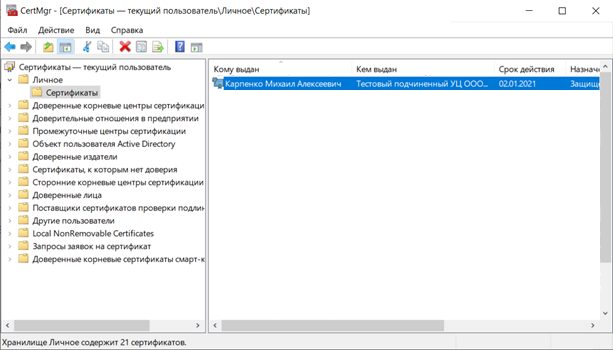


Рисунок 43. Утилита «Сертификаты»

* + - 1. Если сертификат электронной подписи отсутствует, вернитесь к разделу 1.5.4.1 «Установка личного сертификата электронной подписи» и провести установку личного сертификата пользователя на рабочее место.
      2. Если сертификат присутствует, откройте его. Перейдите на вкладку «Путь сертификации» и проверьте, установлен ли сертификат доверенного корневого центра сертификации в соответствии с разделом 1.5.4.2. Если сертификат установлен, то автоматизированное рабочее место пользователя успешно настроено для работы с Системой.

### Настройка «Яндекс.Браузер»

Для настройки корректной работы барузера «Яндекс.Браузер» выполните следующие действия:

1. Откройте настройки интернет-браузера посредством нажатия кнопки

  → Настройки.



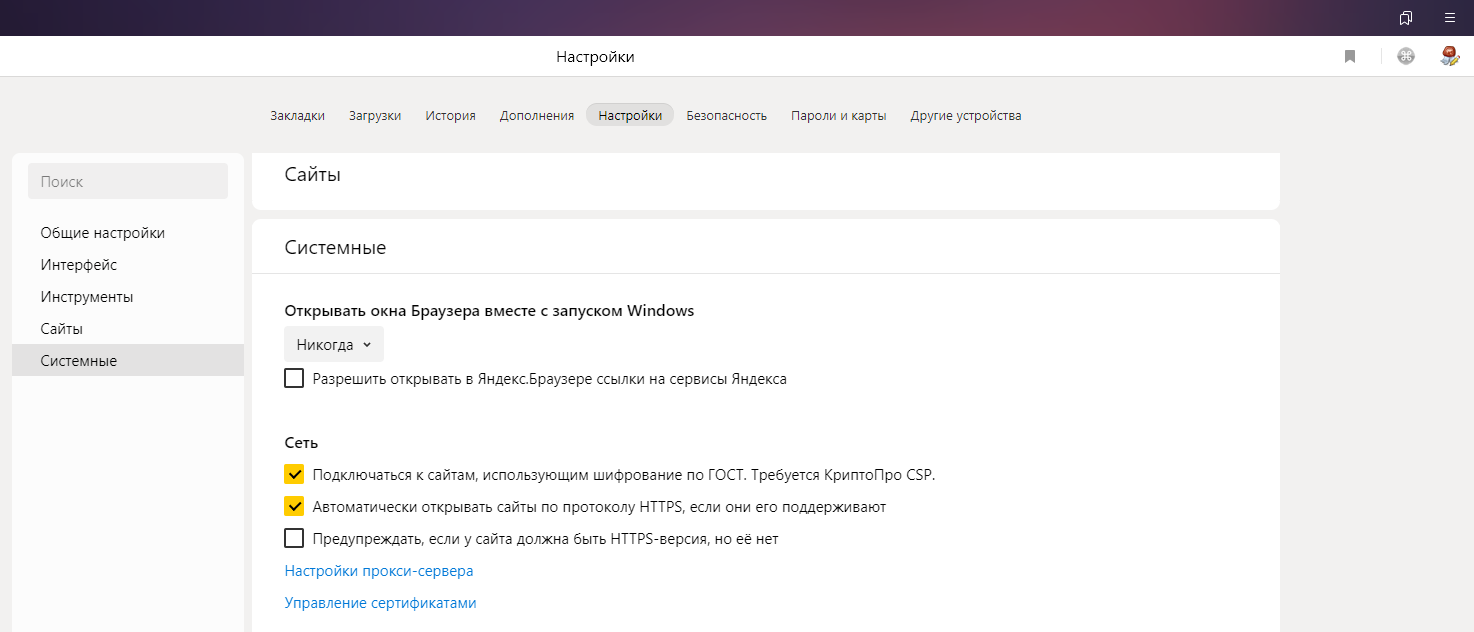
1. Перейдите в раздел Системные.
2. Убедитесь, что в разделе Сеть включена опция «Подключаться к сайтам, использующих шифрование по ГОСТ» (рисунок 44). 

Рисунок 44. Настройка Яндекс.Браузера

В случае отсутствия указанной опции установите актуальную версию интернет-браузера.

Работа с подсистемой «Документы ОМС» ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОБЯЗАТЕЛЬНОГО МЕДИЦИНСКОГО СТРАХОВАНИЯ

## Вход в подсистему «Документы ОМС» государственной информационной системы обязательного медицинского страхования

Для начала работы с системой необходимо выполнить следующую последовательность действий:

- запустить совместимый браузер двойным нажатием левой кнопки мыши на его ярлыке на рабочем столе или нажать на кнопку «Пуск» и в открывшемся меню выбрать пункт, соответствующий используемому интернет-браузеру;

- в браузере в адресной строке ввести адрес: <https://gisoms.ffoms.gov.ru/> [[1]](#footnote-1);

- в окне идентификации выбрать сертификат для входа в компонент и нажать на кнопку «Войти» (Рисунок 45).

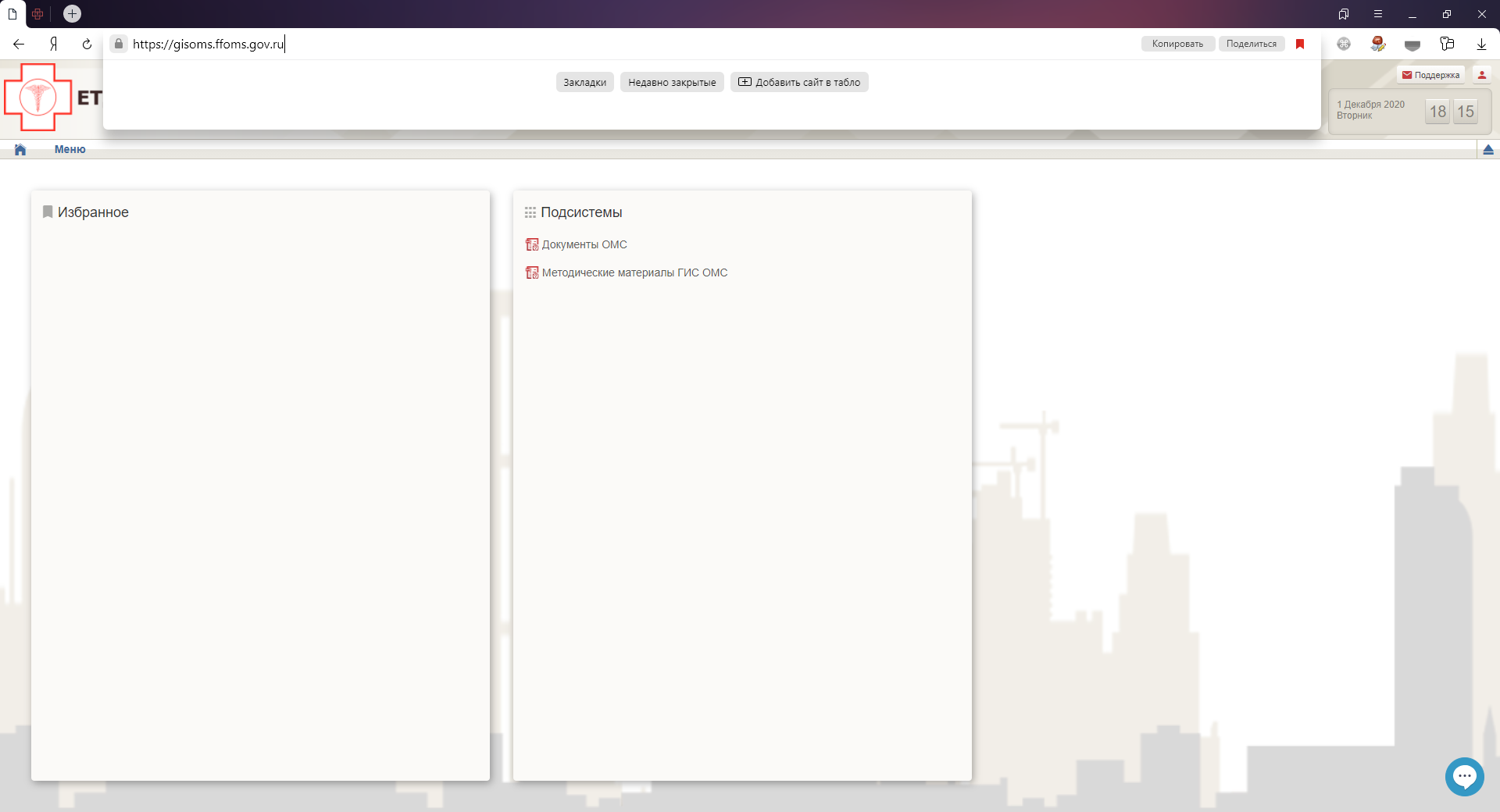


Рисунок 45. Окно ввода адреса ЕТД

1. После этого откроется рабочий стол единой точки доступа Системы (Рисунок 46). Необходимо нажать кнопку «Меню» в левом верхнем углу, далее выбрать подсистему «Документы ОМС». В открывшемся списке нажать на строку «Документы и справочники». В отобразившемся справа окне нажать на строку «Реестр заявок».

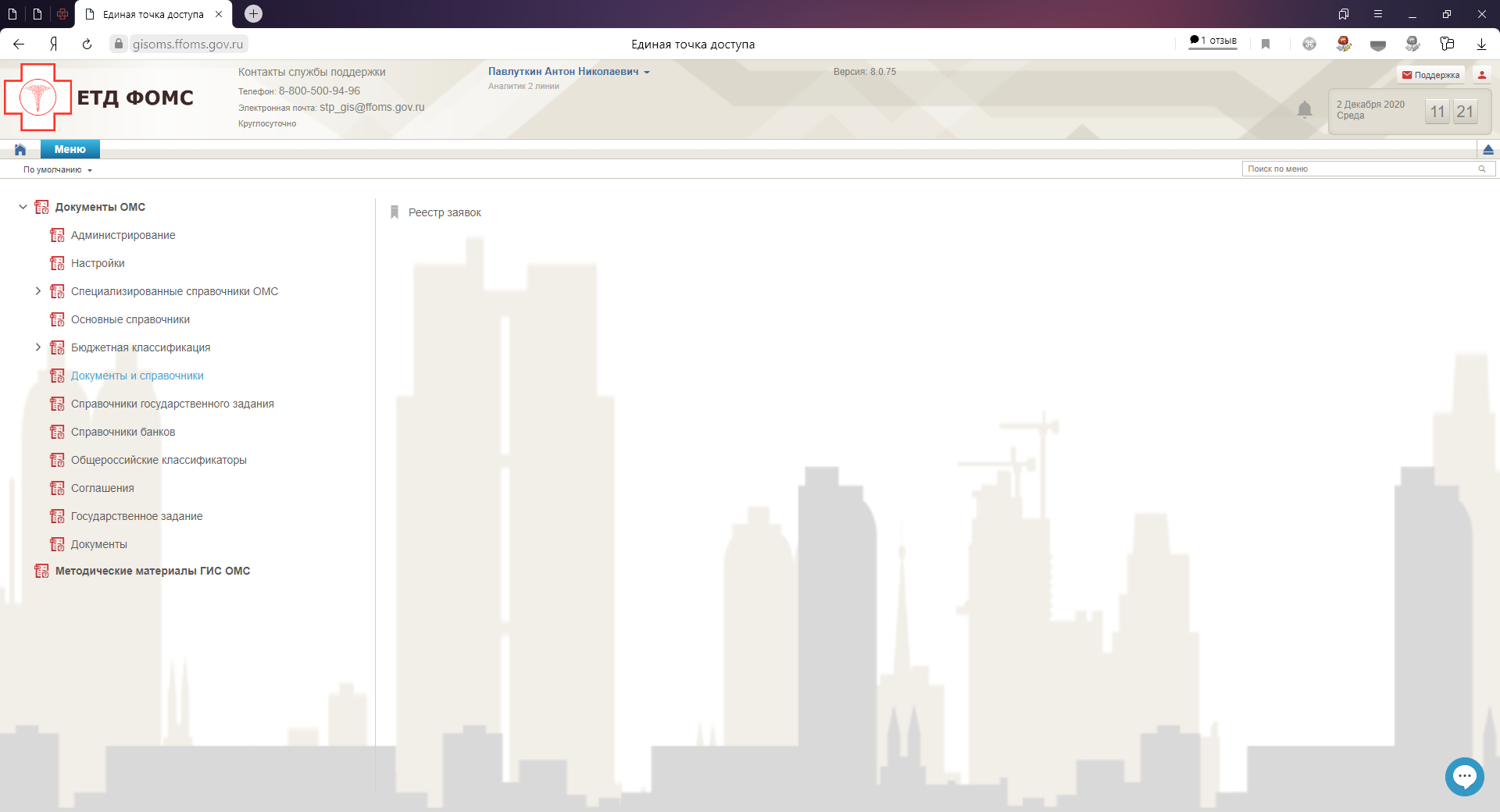


Рисунок 46. Главное меню (Рабочий стол)

## Работа в подразделе «Реестр заявок»

Формирование заявок на регистрацию новых пользователей в системе, изменение сведений и полномочий пользователя, прекращение доступа пользователя к системе осуществляется в разделе пункта меню «Документы и справочники» в реестре: «Реестр заявок» (Рисунок 47).

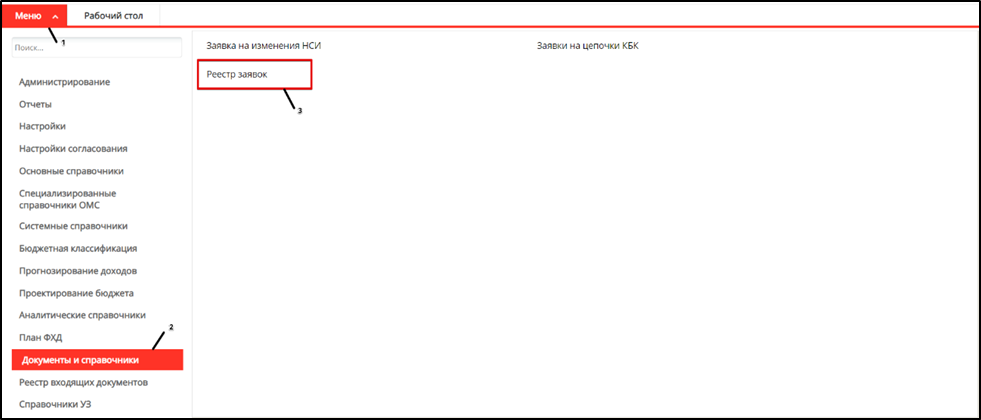


Рисунок 47. Пункт «Меню»

В результате откроется окно «Реестр заявок», в котором будет осуществляться работа (Рисунок 48).

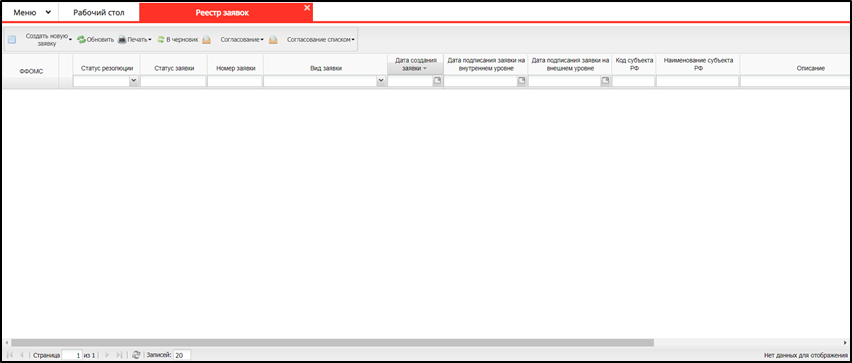


Рисунок 48. Реестр заявок

Описание функциональных кнопок реестра (Рисунок 49):

1. Кнопка «Создать новую заявку» - формирование новой заявки «на регистрацию уполномоченных лиц участника системы», «на изменение сведений и полномочий уполномоченных лиц участника системы», «на прекращение доступа уполномоченных лиц участника системы», «на регистрацию организаций», «на изменение платежных реквизитов».
2. Кнопка «Обновить» - обновление отображения реестра.
3. Кнопка «Печать» - печать выделенного документа.
4. Кнопка «В черновик» - Сброс Статуса заявки=Черновик.
5. Кнопка «Согласование» - Выбор раздела для открытия:

- Внутреннее согласование – Лист согласования заявки

- Внешнее согласование – Резолюция, История резолюций, Уведомление об отклонении

- Подписи документа – информация об электронно-цифровых подписей заявки

1. Кнопка «Согласование списком» - Выбор раздела для открытия:

- Создание резолюции - создание резолюции одновременно для неограниченного количества заявок

- Создание листа согласования - создание одного листа согласования сразу для неограниченного количества заявок

- Согласование - согласование/не согласование неограниченного количества заявок

- Утверждение - утверждение/не утверждение неограниченного количества заявок

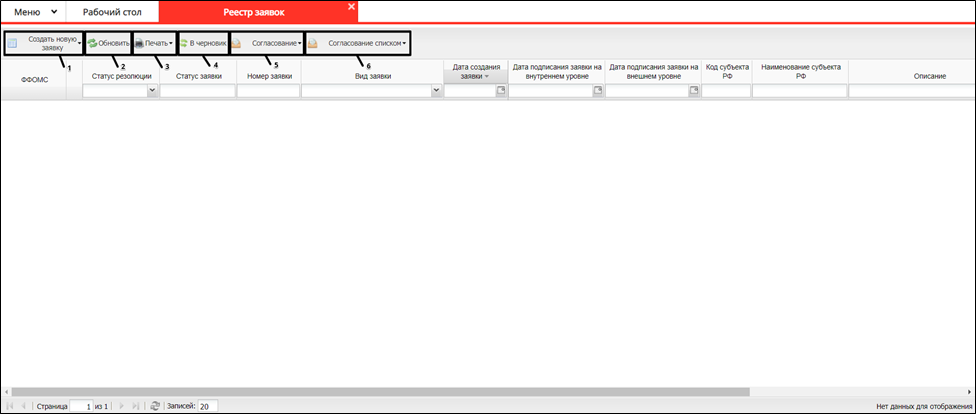


Рисунок 49. Панель инструментов

### Формирование заявки на регистрацию уполномоченных лиц участника системы[[2]](#footnote-2)

Для регистрации нового пользователя в системе необходимо нажать на кнопку «Создать новую заявку» - «На регистрацию уполномоченных лиц участника системы» (Рисунок 50).

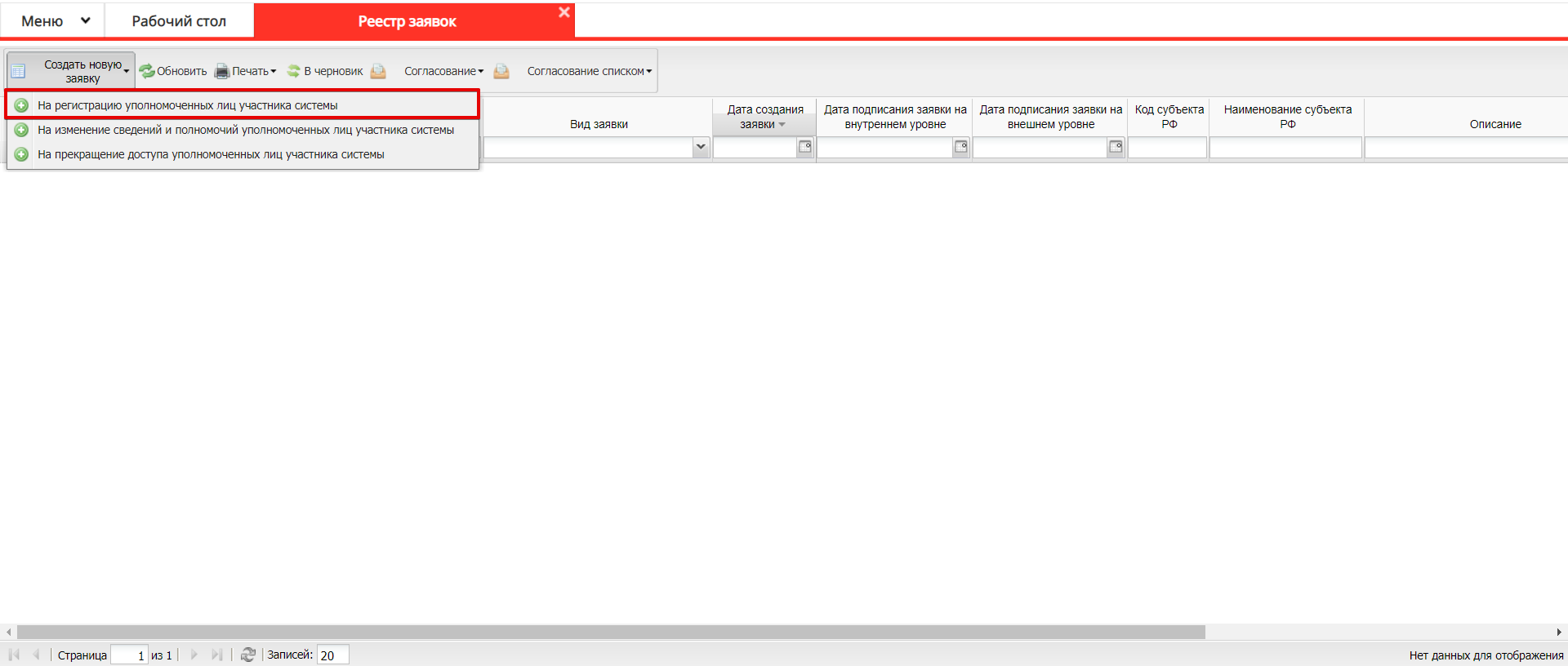


Рисунок 50. Создание заявки на регистрацию пользователей

В открывшемся окне поля «Вид заявки», «Номер заявки», «Дата создания заявки», «Автор», «Контактный телефон» заполняются автоматически. Пользователю необходимо заполнить поля «Организация» (выбрать организацию из списка), «Должность», «Фамилия», «Имя», «Отчество» (поле необязательно для ввода при условии включенного чекбокса «Отсутствует отчество»), «СНИЛС» (в формате NNN-NNN-NNN KK), «Телефон» (Это поле должно содержать номер телефона, начинающийся с 8. Номер телефона должен иметь 11 знаков), «Адрес электронной почты» (в формате <логин(имя почты)@.домен>), «Документ» (загрузка документа-основания на регистрацию) и «Сертификат» (загрузка сертификата для подписания электронно-цифровой подписью).

После введения необходимых для регистрации нового пользователя данных необходимо нажать на кнопку «Сохранить» (Рисунок 51).

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 51. Сохранение данных

В разделе «Полномочия» необходимо по кнопке «Добавить» назначить полномочия для регистрируемого пользователя (Рисунок 52).

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 52. Добавление полномочий

В выпадающем окне представлен перечень полномочий и соответствующих им ролей. Необходимо отметить галочкой необходимые роли, после нажать на кнопку «Заполнить» (Рисунок 53)

Изображение выглядит как стол

Автоматически созданное описание

Рисунок 53. Заполнение полномочий

По кнопке  полномочие удаляется из списка (Рисунок 54).

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 54. Удаление полномочий

Чтобы сохранить заполненные данные в заявке необходимо нажать «Сохранить», закрытие окна создание заявки без сохранения по кнопке «Закрыть» (Рисунок 55).

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 55. Сохранение и закрытие окна

### Формирование заявки на изменение сведений и полномочий уполномоченных лиц участника системы

Для изменения данных о пользователе или добавление/исключение полномочий необходимо нажать на кнопку «Создать новую заявку» - «На изменение сведений и полномочий уполномоченных лиц участника системы» (Рисунок 56).

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 56. Создание заявки на изменение сведений и полномочий

В открывшемся окне поля «Вид заявки», «Номер заявки», «Дата создания заявки», «Автор», «Контактный телефон» заполняются автоматически. Необходимо в поле «Пользователь» выбрать пользователя для изменения сведений или добавление/исключение полномочий. После выбора пользователя автоматически заполняются имеющиеся о нем данные. Поля редактируемые, данные о пользователе можно поменять (Рисунок 57).

Изображение выглядит как текст

Автоматически созданное описание

**Рисунок 57. Создание заявки на изменение сведений и полномочий**

Для сохранения измененных данных необходимо нажать на кнопку «Сохранить».

В разделе полномочия есть возможность добавить пользователю новые полномочия по кнопке «Добавить», либо по кнопке  удалить (Рисунок 58).

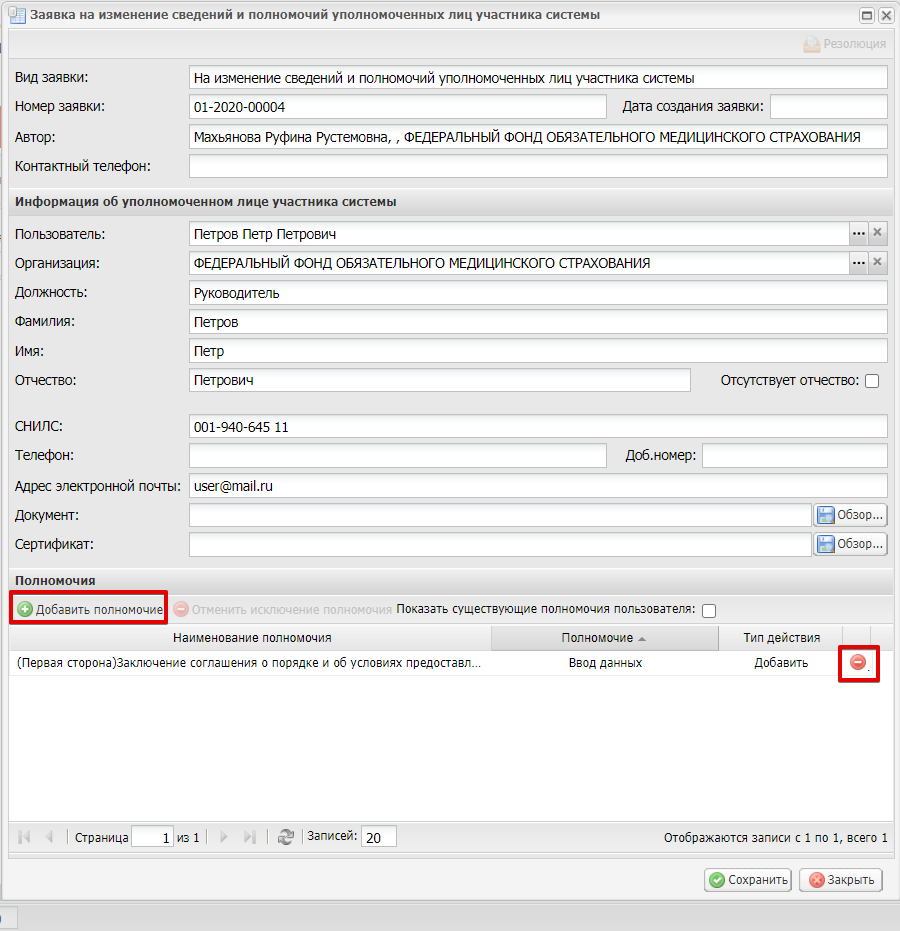


Рисунок 58. Добавление полномочий

Чтобы сохранить измененные данные в заявке необходимо нажать «Сохранить», закрытие окна создание заявки без сохранения по кнопке «Закрыть» (Рисунок 59).

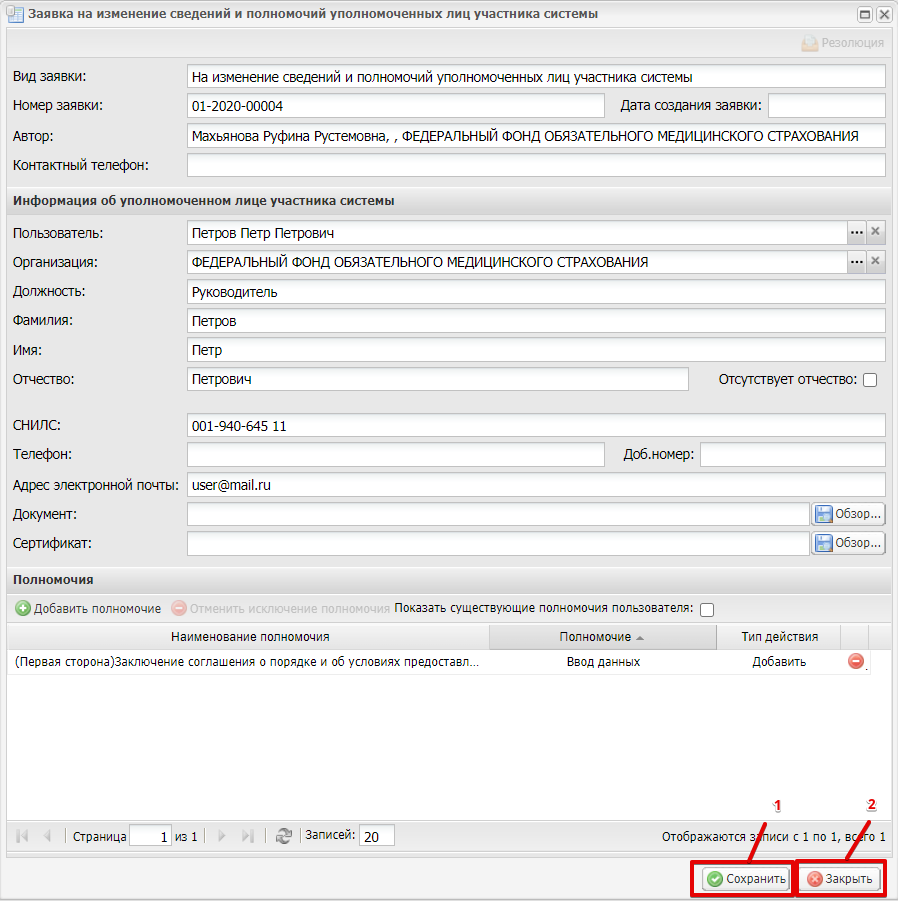


Рисунок 59. Сохранение и закрытие окна

### Формирование заявки на прекращение доступа уполномоченных лиц участника системы

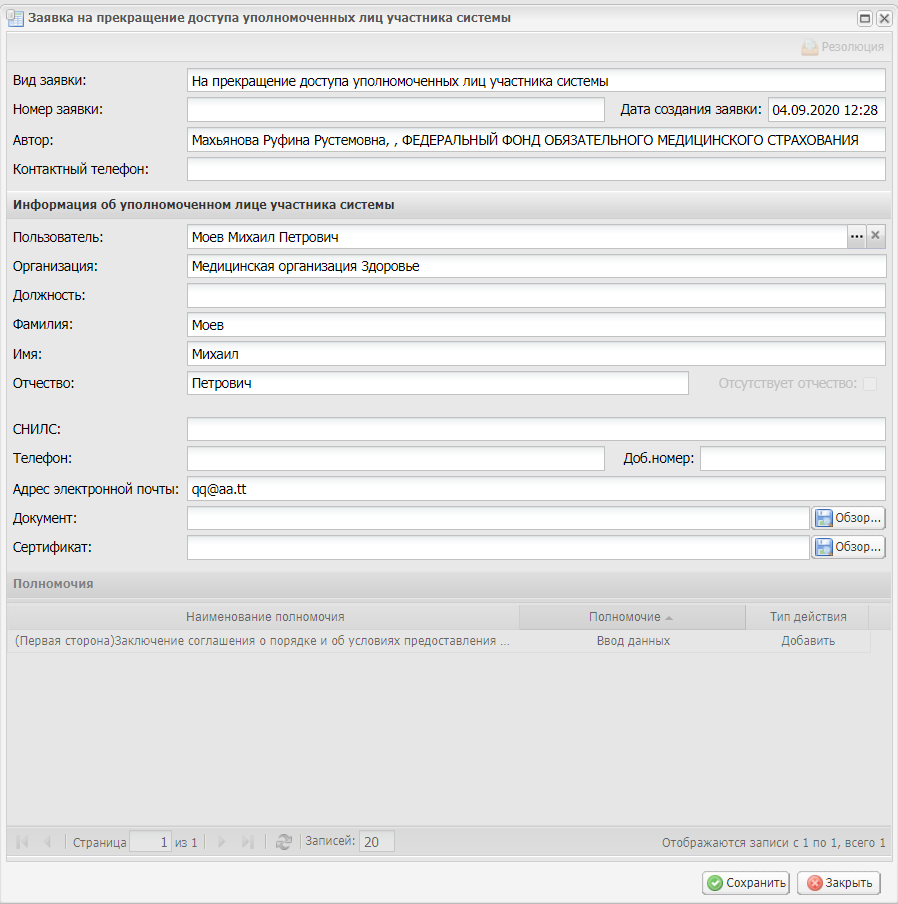
Для прекращения доступа пользователя к системе необходимо нажать на кнопку «Создать новую заявку» - «На прекращение доступа уполномоченных лица участника системы» (Рисунок 60).

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 60. Создание заявки на прекращение действия полномочий пользователя

В открывшемся окне поля «Вид заявки», «Номер заявки», «Дата создания заявки», «Автор», «Контактный телефон» заполняются автоматически. Необходимо в поле «Пользователь» выбрать пользователя для прекращения доступа к системе (Рисунок 61).



**Рисунок 61. Заявка на прекращение действия полномочий пользователя**

Чтобы сохранить данные в заявке необходимо нажать «Сохранить», закрытие окна создание заявки без сохранения по кнопке «Закрыть» (Рисунок 62).

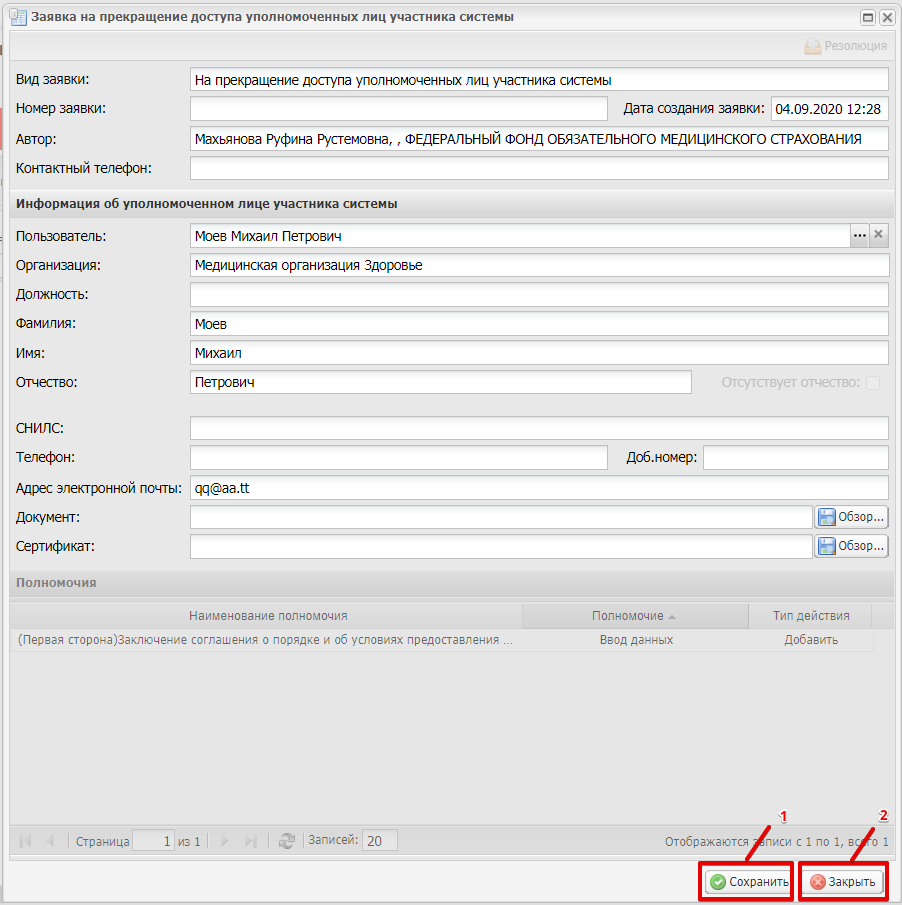


Рисунок 62. Сохранение и закрытие окна

### Согласование заявок

Процесс согласования заявки начинается после создания листа согласования для заявки. Для формирования листа согласования необходимо нажать на кнопку «Согласование»-«Внутреннее согласование» (Рисунок 63).

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 63. Создание листа согласования

В открывшемся окне поля «Дата, время», «ФИО, Организация», «Продолжительность согласования», «Документ утвержден», «Комментарий» заполняются автоматически. Пользователю необходимо по кнопке «Добавить» выбрать перечень согласующих (их может быть 2 и более) и перечень утверждающих (утверждающий всегда 1) (Рисунок 64).

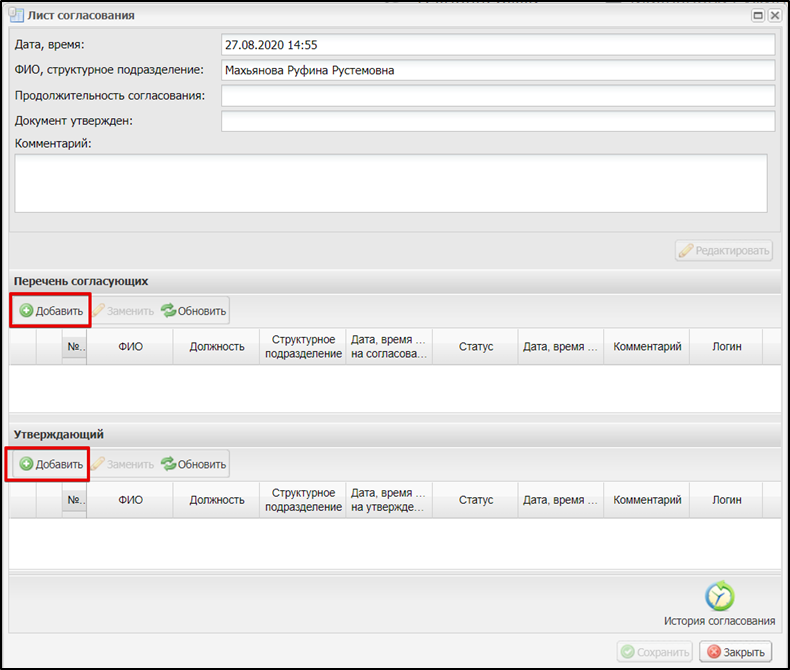


Рисунок 64. Лист согласования

По кнопке «Сохранить» запускается процесс согласования заявки. Заявка переходит из статуса «Черновик» в статус «На согласовании» (Рисунок 65).

Изображение выглядит как текст

Автоматически созданное описание

**Рисунок 65. Сохранение листа согласования**

Далее пользователи, указанные в перечне согласующих, согласовывают заявку. Для этого необходимо зайти в «Документы и справочники»-«Реестр заявок»-«Согласование»-«Внутреннее согласование». В листе согласования для согласующих пользователей появится кнопка «Согласовано» или «Не согласовано» (Рисунок 66).

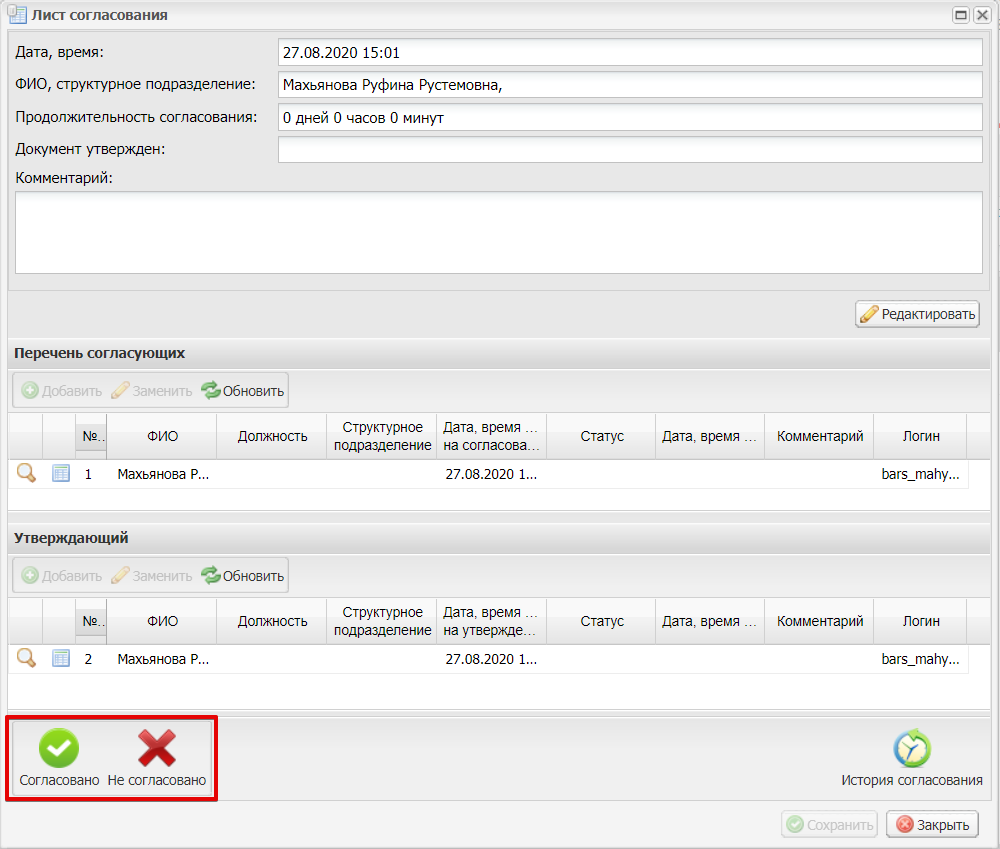


Рисунок 66. Согласование заявок

Далее пользователь, указанный в перечне утверждающих, утверждает заявку. Для этого необходимо зайти в «Документы и справочники»-«Реестр заявок»-«Согласование»-«Внутреннее согласование»-«Лист согласования». В листе согласования для утверждающего пользователя появится кнопка «Утверждено» или «Не утверждено» (Рисунок 67).

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 67 Утверждение заявок

После утверждения выходит окно «Подпись» для выбора сертификата. (Рисунок 68).

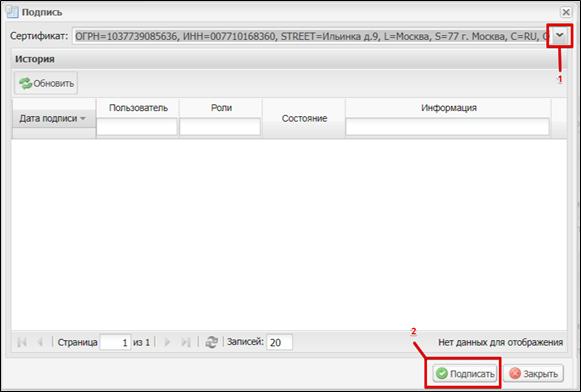


Рисунок 68. Окно «Подпись»

После появляется печатная форма заявки для наложения электронной подписи (Рисунок 69).

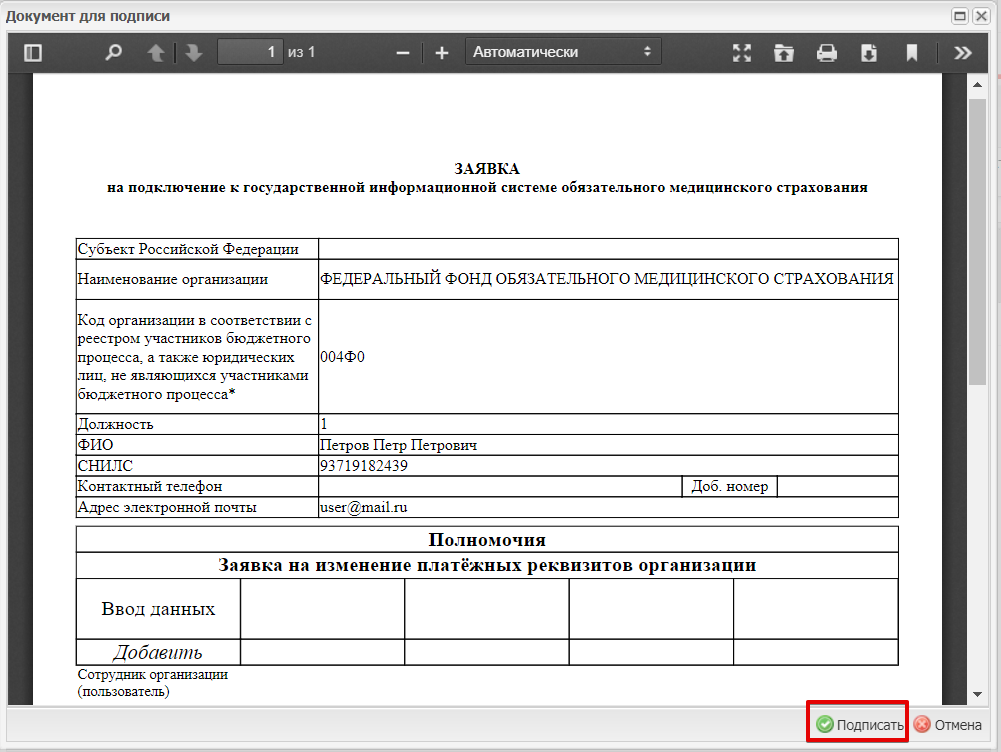


Рисунок 69. Подписание электронной подписью

После успешного согласования и утверждения заявки внутри организации заявка переходит на согласование ФОМС. Индикатор «ФОМС» в «Реестре заявок» показывает статус резолюции наложенной пользователем ФОМС. Если индикатор серый, то резолюция еще не создана, и заявка еще не перешла на согласование ФОМС. Если индикатор желтый, то заявка находится на согласовании. Если индикатор зеленый, значит резолюция положительна (Резолюция=Подписано). Если индикатор красный, значит резолюция отрицательна (Резолюция=Отклонено) (Рисунок 70).

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 70. Индикаторы заявки

Для того чтобы создать резолюцию необходимо нажать на кнопку «Согласование» - «Внешнее согласование» - «Резолюция» (Рисунок 71).

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 71. Создание резолюции

Откроется окно выбора резолюции. Резолюция может быть положительная – “Зарегистрировать” (Рисунок 72).

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 72. Резолюция

Может быть отрицательной – «Не зарегистрировать». При отрицательной резолюции обязательно для заполнения поле «Комментарий» (Рисунок 73).

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 73. Отрицательная резолюция

После наложения резолюции необходимо нажать на кнопку «Сохранить».

После создания резолюции необходимо ее согласовать. Для этого необходимо сформировать лист согласования по кнопке «Согласование» - «Согласование резолюции» (Рисунок 74).

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 74. Согласование резолюции

Создание листа согласование для внешнего согласования происходит аналогично внутреннему согласованию. Необходимо выбрать перечень согласующих и утверждающих (Рисунок 75).

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 75. Лист согласования резолюции

После успешного согласования и утверждения выбранными пользователями в списке согласующих и утверждающих на внешнем уровне согласования ФОМС (аналогично согласованию и утверждению на внутреннем уровне согласования) создается пользователь.

# ПРОБЛЕМЫ при подключении к системе и их устранение

## Окно входа в Систему

В случае отказа во входе в Систему, необходимо:

* + - 1. Убедиться в том, что уполномоченному лицу подтверждено разрешение работы в Системе (высылается на адрес уполномоченного лица после утверждения заявки в Федеральном фонде обязательного медицинского страхования).
      2. Убедиться в том, что в автоматизированном рабочем месте установлен сертификат лица, которому подтверждено участие.
      3. Убедиться в том, что СНИЛС владельца сертификата (указан в поле субъект сертификата) соответствует значению СНИЛС в Системе.
      4. Проверить свой интернет-браузер на список совместимых браузеров в разделе 1 данной инструкции.

В случае, если проблемы сохраняются, за разъяснением порядка регистрации пользователей обращайтесь в службу поддержки Системы по телефону 8-800-500-94-96.

## Иные ошибки

В случае возникновения ошибок в процессе подключения и настройки программного обеспечения, не описанных в данной инструкции, необходимо:

1. сделать снимок экрана (скриншот) ошибки;
2. в соответствии с шагами 1 - 9 раздела 1.5.5.2 инструкции сохранить сертификат корневого центра сертификации;
3. заархивировать **(обязательно!)** сертификат и скриншот;
4. отправить архив на адрес электронной почты **stp\_gis@ffoms.gov.ru** с указанием наименования организации, ИНН организации, наименования вышестоящего федерального органа исполнительной власти (при наличии), СНИЛС пользователя.

При возникновении вопросов, связанных с функционированием Системы необходимо обращаться по телефону 8-800-500-94-96 или оставить обращение в электронной форме с использованием раздела Системы «Техническая поддержка» доступного с использованием в меню Системы.

1. В следующих редакциях Инструкции адрес соединения может измениться. [↑](#footnote-ref-1)
2. Раздел предназначен для привилегированных пользователей Системы [↑](#footnote-ref-2)