

**СИСТЕМА ЭЛЕКТРОННОЙ  
ПОДАЧИ ЗАЯВОК  
НА  
ИЗОБРЕТЕНИЯ И ПОЛЕЗНЫЕ  
МОДЕЛИ**

**Краткое руководство пользователя**



## **Оглавление**

Введение.....	3
Настройка рабочего места пользователя.....	3
Установка сертификатов электронной подписи.....	5
Начало работы .....	6



## Введение

Система электронной подачи заявок на изобретения и полезные модели (<https://patdoc.fips.ru>) (далее - сервис подачи) предназначена для формирования электронных заявок, подписывания их квалифицированной электронной подписью и подачи заявок в патентное ведомство. Дальнейшая переписка по поданным заявкам может вестись в электронном виде через отдельный сервис на сайте ФИПС «Личный кабинет для переписки по заявкам» (см. <http://new.fips.ru/office/>) (далее - сервис переписки).

Пользователем сервиса подачи может быть любое физическое лицо, выступающее от своего имени или от имени группы лиц, или организации и обладающее сертификатом квалифицированной электронной подписи, выданным одним из аккредитованных при Минкомсвязи удостоверяющих центров. Чтобы стать пользователем сервиса подачи, надо выполнить несколько простых шагов, перечисленных на сайте ФИПС в разделе «ПОДАЧА ЗАЯВКИ НА ИЗОБРЕТЕНИЕ/ПОЛЕЗНУЮ МОДЕЛЬ» - «[КАК СТАТЬ ПОЛЬЗОВАТЕЛЕМ СИСТЕМЫ](#)».

**Важно!** После регистрации Вас в качестве пользователя системы Вы получите идентификатор пользователя, который Вы обязаны указывать при обращении в службу технической поддержки (см. ниже).

Функционально система подачи заявок состоит из личного кабинета подачи, доступного в Интернет по адресу <https://patdoc.fips.ru> и программного обеспечения PatDoc.

Личный кабинет подачи (не путать с сервисом переписки, см. выше) позволяет

- скачать и установить на рабочем месте пользователя программное обеспечение PatDoc;
- открыть электронную форму новой заявки для заполнения;
- отслеживать состояние поданной заявки;
- перейти в сервис переписки;
- получать уведомления сервиса подачи о регистрации заявок, выходе новой версии PatDoc и т.п.;
- получать доступ к пользовательской документации, часто задаваемым вопросам и другим документам, относящимся к сервису подачи.

Подробно кабинет подачи описан в документе «[Руководство пользователя \(заявителя\)](#)».

**Важно!** Текущая версия сервиса подачи работает только с PatDoc версии 4.1.0.1 и новее. Все более ранние версии PatDoc работать с сервисом подачи не будут!

## Настройка рабочего места пользователя

Для успешной работы с сервисом подачи подходит любой компьютер (или ноутбук), работающий под управлением ОС Windows и подключенный к сети Интернет. Компьютер должен быть оборудован портом USB не ниже 2.0 для установки ключа электронной подписи.

На компьютере должно быть установлено следующее программное обеспечение:

**Операционная система:**



- Windows XP\*/Vista\*/7/8/8.1/10;

**Браузер:**

- IE 8.0 и выше (предпочтительно), Edge, Google Chrome + IE tab, Chromium GOST, Safari for Windows;

***Важно!** В настройках Интернет-браузера должна быть включена поддержка всех протоколов TLS. Узел <https://patdoc.fips.ru/> должен быть включен в список надежных узлов. При этом опция «Для всех узлов этой зоны требуется проверка серверов (https)» должна быть отключена.*

*Если подключение к интернету осуществляется через прокси-сервер, то в параметрах прокси сервера должно быть*

*- добавлен адрес <https://patdoc.fips.ru/> в список исключений;*

*- обеспечен сетевой доступ к адресу <https://patdoc.fips.ru/> по протоколу TCP на порты 443 (для чтения/записи).*

**Криптопровайдер:**

-Крипто-Про CSP 4.0 или выше (предпочтительно), ViPNet CSP 4.2

***Важно!** Выбирать версию криптопровайдера следует исходя из операционной системы, поддержки требуемых криптографических алгоритмов и наличия сертификата ФСБ. При определении требуемой версии, например, КриптоПро CSP удобно пользоваться таблицами на сайте разработчика: <http://www.cryptopro.ru/products/csp/compare>. В любом случае проконсультируйтесь в Удостоверяющем центре, который выдает Вам сертификат электронной подписи о соответствии Вашей версии Windows версии приобретаемого Вами криптопровайдера.*

*Недопустимо устанавливать на одно рабочее место два криптопровайдера - не будет работать ни один из них!*

**Драйвер носителя сертификата электронной подписи («электронный ключ»):**

- RuToken (драйверы для RuToken находятся в свободном доступе по адресу <http://www.rutoken.ru/hotline/download/>);

***Важно!** Если Вы планируете использовать другой тип носителя – eToken, JaCarta или иной, Вам может потребоваться другой криптопровайдер. Обязательно проконсультируйтесь с сотрудниками удостоверяющего центра, в котором Вы получаете сертификат электронной подписи, о совместимости носителя сертификата ЭП и криптопровайдера.*

**Сертификаты электронной подписи (см. ниже)**

**Текстовый редактор:**

- MS Word 2003-2013

**Антивирус:**

---

\* Не рекомендуется к использованию, поскольку эти версии Windows могут не обеспечивать корректную работу нужных криптопровайдеров.



Специально устанавливать антивирус не требуется, но если он есть, в нем необходимо произвести настройки:

- отключить проверку защищенных соединений (протокола https через порт 443);
- дать все разрешения для программы patdoc.exe (это нужно будет сделать после успешного входа в кабинет подачи и установки PatDoc (см. «Руководство пользователя (заявителя)»)).

**Важно!** *Некоторые антивирусы, например Avast или AVG, могут вызывать проблемы в работе с системой, которые нельзя исправить настройками антивируса. Если нет возможности заменить такой антивирус на антивирус другого производителя, необходимо отключать его во время работы с сервисом подачи.*

## Установка сертификатов электронной подписи

Сервис подачи работает с сертификатами электронной подписи, выданными аккредитованными удостоверяющими центрами (см. «Перечень аккредитованных удостоверяющих центров» <http://e-trust.gosuslugi.ru/CA>) по ГОСТ Р 34.11/34.10-2001 и ГОСТ Р 34.11-2012/34.10-2012 256 бит.

**Важно!** *Начиная с 01.01.2019 удостоверяющие центры выдают только сертификаты ГОСТ Р 34.11-2012/34.10-2012. Сертификаты по ГОСТ Р 34.11/34.10-2001, выданные до 01.01.2019 будут действовать до конца срока своего действия, но не позже 31.12.2019.*

На Вашем рабочем месте должны быть установлены две цепочки следующие сертификатов - для серверного сертификата и для Вашего личного. Как проводить процедуру установки подробно написано в документе «Руководство по установке сертификата «ЭП». Ниже написано, где взять эти сертификаты и куда устанавливать.

### Устанавливаем цепочку серверного сертификата

1. Скачиваем по ссылке

<http://e-trust.gosuslugi.ru/Shared/DownloadCert?thumbprint=8CAE88BBFD404A7A53630864F9033606E1DC45E2>

корневой сертификат «Головной удостоверяющий центр» и устанавливаем его в раздел «Доверенные корневые центры сертификации».

2. Скачиваем по ссылке

<http://e-trust.gosuslugi.ru/Shared/DownloadCert?thumbprint=40896752A02F920DEB542A5F0D87B225FDF3F63B>

промежуточный сертификат «Федеральный институт промышленной собственности» и устанавливаем его в раздел «Промежуточные центры сертификации».

### Устанавливаем цепочку личного сертификата

Далее следуйте инструкции в зависимости от того, какому ГОСТ соответствует Ваш личный сертификат.

Если Ваш сертификат выдан по ГОСТ Р 34.11/34.10-2001:

1. Скачиваем по ссылке



<http://e-trust.gosuslugi.ru/Shared/DownloadCert?thumbprint=8CAE88BBFD404A7A53630864F9033606E1DC45E2>

корневой сертификат «Головной удостоверяющий центр» и устанавливаем его в раздел «Доверенные корневые центры сертификации».

2. На портале аккредитованных удостоверяющих центров находим (см. «Перечень аккредитованных удостоверяющих центров» <http://e-trust.gosuslugi.ru/CA>) ссылку для скачивания нужного Вам одного или нескольких промежуточных сертификатов. Скачиваем и устанавливаем в раздел «Промежуточные центры сертификации».

**Важно!** Как найти, скачать и установить нужный кросс-сертификат подробно описано в документе «Руководство по установке сертификата ЭП». Вы так же можете обратиться к сотрудникам аккредитованного удостоверяющего центра, выдавшего Вам личный сертификат за консультацией по установке цепочки личного сертификата.

3. Устанавливаем Ваш личный сертификат в раздел «Личные». Порядок и правила установки личного сертификата с закрытым ключом приводятся в пользовательской документации Вашего криптопровайдера.

Если Ваш сертификат выдан по ГОСТ Р 34.11-2012/34.10-2012:

1. Скачиваем по ссылке

<http://e-trust.gosuslugi.ru/Shared/DownloadCert?thumbprint=4BC6DC14D97010C41A26E058AD851F81C842415A>

корневой сертификат «Минкомсвязь России» и устанавливаем его в раздел «Доверенные корневые центры сертификации».

2. На портале аккредитованных удостоверяющих центров находим (см. «Перечень аккредитованных удостоверяющих центров» <http://e-trust.gosuslugi.ru/CA>) ссылку для скачивания нужного Вам одного или нескольких промежуточных сертификатов. Скачиваем и устанавливаем в раздел «Промежуточные центры сертификации».

**Важно!** Как найти, скачать и установить нужный кросс-сертификат подробно описано в документе «Руководство по установке сертификата ЭП». Вы так же можете обратиться к сотрудникам аккредитованного удостоверяющего центра, выдавшего Вам личный сертификат за консультацией по установке цепочки личного сертификата.

3. Устанавливаем Ваш личный сертификат в раздел «Личные». Порядок и правила установки личного сертификата с закрытым ключом приводятся в пользовательской документации Вашего криптопровайдера.

## Начало работы

После выполнения всех предыдущих настроек можно приступить к работе с сервисом подачи.

- Войдите в Интернет по адресу <https://patdoc.fips.ru>.

- В открывшемся личном кабинете подачи откройте закладку «Установка», скачайте и установите PatDoc.



- Перейдите на закладку «Заявки», откройте ссылку «Новая заявка» и приступайте к ее заполнению.

***Важно!*** Детальное описание личного кабинета подачи и работы с PatDoc приводится в документе «Руководство пользователя (заявителя)».

Если возникнут вопросы, или что-то пойдет не так, вначале ознакомьтесь с документами «Аварийные ситуации» и «Часто задаваемые вопросы». Если ответ на Ваш вопрос там не обнаружится, обращайтесь по электронной почте в службу поддержки по адресу [helpdesk@rupto.ru](mailto:helpdesk@rupto.ru). В письме обязательно указывайте Ваш идентификатор пользователя (см. выше).