

СИСТЕМА ЭЛЕКТРОННОЙ ПОДАЧИ ЗАЯВОК НА ИЗОБРЕТЕНИЯ (ПОЛЕЗНЫЕ МОДЕЛИ)

**Требования к программно-аппаратному уровню персонального
компьютера**

МОСКВА 2018



Оглавление

Требования к оборудованию	3
Требования к программному обеспечению	4
Требования к Интернет-браузеру	4
Если подключение к интернет осуществляется через прокси-сервер	4
Требования к антивирусным программам	4
Требования к криптопровайдеру	4
Требования к текстовому редактору	5
Требования к сертификатам электронной подписи.....	5



Требования к оборудованию

Pentium совместимый процессор с частотой не менее 500 МГц;

Рекомендуется не менее 256 Мб оперативной памяти;

Клавиатура, мышь Microsoft Mouse или совместимое указывающее устройство;

Видеокарта и монитор, поддерживающие режим Super VGA с разрешением не менее чем 1024x768 пх.

Порт USB2;

Устройство считывания УЭК (в случае, если в качестве носителя сертификата ЭП используется УЭК) ,



Требования к программному обеспечению

Операционная система: MS Windows XP SP3,2000, Windows Vista, Windows 7 SP1 (32x, 64x), Windows 8.1, Windows 10;

Требования к Интернет-браузеру

Интернет-браузер: MS Internet Explorer версии 8.0 и выше, Edge (Windows 10), Safari for Windows;

В настройках Интернет-браузера должна быть включена поддержка всех протоколов TLS и SSL

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.

Доступ к веб-серверу через Интернет по адресу <https://patdoc.fips.ru/>

Если подключение к интернет осуществляется через прокси-сервер

- В список исключений (см. «Параметры прокси-сервера») должны быть добавлены адрес <https://patdoc.fips.ru/>;

- Обеспечить сетевой доступ к адресу <https://patdoc.fips.ru/> по протоколу TCP на порты 443;

Требования к антивирусным программам

Адрес портала подачи <https://patdoc.fips.ru/> должен быть внесен в список исключений.

Антивирус не должен проверять протокол https через порт 443 (в разных антивирусах эта настройка называется по разному, например «Проверка защищенных соединений», «Контроль портов» и т.п.).

Антивирус Avast может вызывать проблемы в работе с системой. Если нет возможности заменить антивирус Avast на антивирус другого производителя, желательно отключать его во время работы с системой.

Требования к криптопровайдеру

Рекомендуемый криптопровайдер - программное обеспечение СКЗИ CryptoPro CSP версии 3.6 R2 (для версий Windows XP, Vista и Windows 7) и выше (для версий Windows 8.1, 10); Возможно использование программного обеспечения криптопровайдера VipNet CSP версии 4.0 и выше.

Соответствие версии криптопровайдера версии Windows имеет важное значение. Проконсультируйтесь о нем у поставщика Вашего криптопровайдера.

Носитель сертификата электронной подписи («электронный ключ») RuToken (драйверы для RuToken находятся в свободном доступе по адресу <http://www.rutoken.ru/hotline/download/>);



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

Требования к текстовому редактору

Текстовый редактор: MS Office 2003 - 2013 (в соответствии с версией Windows);

Требования к сертификатам электронной подписи

На компьютере должны быть установлены следующие сертификаты (выделенные жирным шрифтом устанавливаются обязательно, остальные – по обстоятельствам, смотри ниже):

1. **Корневой сертификат «Головной удостоверяющий центр»** в раздел «Доверенные корневые центры сертификации». скачать здесь <http://e-trust.gosuslugi.ru/Shared/DownloadCert?thumbprint=8CAE88BBFD404A7A53630864F9033606E1DC45E2>
2. **Кросс-сертификат (один или несколько) «УЦ 1 ИС ГУЦ»** в раздел «Промежуточные центры сертификации» скачать здесь <http://e-trust.gosuslugi.ru/Shared/DownloadCert?thumbprint=9E78A331020E528C046FFD57704A21B7D2241CB3>
<http://e-trust.gosuslugi.ru/Shared/DownloadCert?thumbprint=9D05A704C8C1E565ACDE5878FE0BB96EC53C2A40>
<http://e-trust.gosuslugi.ru/Shared/DownloadCert?thumbprint=0408435EB90E5C8796A160E69E4BFAC453435D1D>
<http://e-trust.gosuslugi.ru/Shared/DownloadCert?thumbprint=0932E483C4420E668F64D360006D0BEB0BFACCA7>
3. **Кросс-сертификат «УЦ 2 ИС ГУЦ»** в раздел «Промежуточные центры сертификации» <http://e-trust.gosuslugi.ru/Shared/DownloadCert?thumbprint=B11108FFDCAD99D7A845023AB552CB1ABE845A1B>
4. **Кросс-сертификат «Федеральный институт промышленной собственности»** в раздел «Промежуточные центры сертификации». скачать здесь <http://e-trust.gosuslugi.ru/Shared/DownloadCert?thumbprint=40896752A02F920DEB542A5F0D87B225FDF3F63B>
5. **Кросс-сертификат удостоверяющего центра, выдавшего личный сертификат** в раздел «Промежуточные центры сертификации». (найти и скачать с портала <http://e-trust.gosuslugi.ru/CA>);
6. **Личный сертификат пользователя** в раздел «Личные».

Внимание! Сертификаты 1, 4, 5, 6 устанавливаются обязательно! Сертификаты 2 или 3 устанавливаются, если кросс-сертификат 5 выдан УЦ 1 ИС ГУЦ или УЦ 2 ИС ГУЦ.

Обратите внимание, что значение параметра «Идентификатор ключа центра сертификации» личного сертификата 6 должно быть равно значению «Идентификатор ключа субъекта» кросс-сертификата 5.

Так же, значение параметра «Идентификатор ключа центра сертификации» кросс-сертификата 5 должно быть равно значению «Идентификатор ключа субъекта» кросс-сертификата 2 или 3.

Как найти, скачать и установить нужный кросс-сертификат детально описано в документе «Руководство по установке сертификата ЭП»