



# Руководство по настройке рабочего места пользователя Сервиса АРМ Регистратор









#### Оглавление

1	ПРОГ	РАММНО-АППАРАТНЫЕ ТРЕБОВАНИЯ	3
2	ПОРЯ	ЯДОК НАСТРОЙКИ РАБОЧЕГО МЕСТА ПОЛЬЗОВАТЕЛЯ	4
	2.1 HA	АСТРОЙКА КОМПЬЮТЕРА ДЛЯ РАБОТЫ С ЭЛЕКТРОННОЙ ПОДПИСЬЮ ПО ИНСТРУКЦИЯМ УЦ	4
	2.2 Ус	становка ПО "КриптоПро ЭЦП Browser plug-in"	4
	2.3 По	ОДКЛЮЧЕНИЕ ПЛАГИНА В БРАУЗЕРЕ	4
	2.3.1	Браузер Google Chrome	4
	2.3.2	Браузер Internet Explorer 11	5
	2.3.3	Яндекс.Браузер	7
3	ПРОІ	ВЕРКА РАБОТЫ ПЛАГИНА	7
Γл	оссарий		13



# Введение

Настоящий документ содержит описание действий по настройке рабочего места Сервиса «APM Регистратор» для подачи и ведения переписки по заявкам на товарный знак, наименование места происхождения товара и/или предоставление исключительного права на ранее зарегистрированное наименование места происхождения товара, изобретение и полезную модель (далее - Сервис), включающих в себя установку и настройку необходимого программного обеспечения.

Для выполнения установки и настройки ПО в соответствии с настоящим руководством пользователь должен обладать навыками по работе с компьютером и иметь права локального администратора на своем компьютере.

## 1 Программно-аппаратные требования

Программно-аппаратные требования для работы в Сервисе:

- клавиатура, мышь или совместимое указывающее устройство;
- разрешение экрана не менее чем 1024х768 точек;
- доступ к веб-серверу через Интернет по адресу <u>https://kpsrtz.fips.ru</u>;
- операционная система: Windows 7, Windows 8.1, Windows 10;
- браузер: Internet Explorer 11, Google Chrome (версия 49.0 и выше), Яндекс.Браузер;
- ключ электронной подписи с квалифицированным сертификатом, предназначенный для работы на интернет-порталах, работающий с использованием ПО "КриптоПро ЭЦП Browser plug-in" версия 2.0;
- текстовый редактор Microsoft Office Word 2010-2016;
- средство просмотра pdf-документов (Adobe Reader).



## 2 Порядок настройки рабочего места пользователя

Для работы в Сервисе необходимо приобрести квалицированный сертификат ЭП для работы на интернет-порталах в одном из аккредитованных удостоверяющих центров (далее – УЦ). Перечень всех аккредитованных УЦ опубликован на портале уполномоченного федерального органа в области использования электронной подписи (<u>http://e-trust.gosuslugi.ru/CA</u>).

## 2.1 Настройка компьютера для работы с электронной подписью по инструкциям УЦ

Настройку компьютера для работы с электронной подписью выполните по инструкциям УЦ, в котором был приобретён сертификат. Эта настройка включает в себя следующее:

- Установка средства электронной подписи (криптопровайдер), предназначенного для работы с вашим ключом ЭП;
- Установка драйвера ключевого носителя (например, Рутокен S), при необходимости;
- Установка личного сертификата;
- Установка цепочки сертификатов для личного сертификата.

### 2.2 Установка ПО "КриптоПро ЭЦП Browser plug-in"

Для создания электронной подписи в Сервисе используется ПО «КриптоПро ЭЦП Browser plug-in» (далее - Плагин). Для установки Плагина скачайте установочный файл **cadesplugin.exe** по ссылке <u>https://www.cryptopro.ru/products/cades/plugin/get\_2\_0</u>, запустите его, дождитесь завершения установки.

### 2.3 Подключение Плагина в браузере

Для входа в Сервис и подписания подготовленных документов электронной подписью необходимо в используемом Вами браузере подключить Плагин, установленный в соответствии с п.2.2.

### 2.3.1 Браузер Google Chrome.

Откройте меню браузера -> «Дополнительные настройки» -> «Расширения», включите расширение "CryptoPro Extension for CAdES Browser Plug-in" (см. Рис. 1).



Рис. 1 Подключение Плагина для браузера Google Chrome.

В случае отсутствия указанного расширения, можно перейти в Интернет-магазин Chrome, найти и установить расширение.

## 2.3.2 Браузер Internet Explorer 11

Добавьте адрес <u>https://kpsrtz.fips.ru</u> в зону «Надёжные сайты». Если параметры безопасности зоны «Надежные сайты» установлены по умолчанию, то будет обеспечено автоматическое подключение Плагина.

Откройте браузер Internet Explorer 11, откройте меню «Сервис» -> «Свойства браузера» (см.Рис. 2)



Рис. 2 Свойства браузера Internet Explorer 11





ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ФЕДЕРАЛЬНЫЙ ИНСТИТУТ ПРОМЫШЛЕННОЙ СОБСТВЕННОСТИ

В открывшемся окне перейдите на вкладку «Безопасность», выберите зону «Надежные сайты», нажмите кнопку «Сайты» (см.Рис. 3):

Общие	1 Безопасность	- iporporinior	House		
coupie		KOHO	биленциальность		
			Prideridianonocio		
ыберите зону д	ля настройки ее паран	етров безопасност	ги.		
	2				
Интернет	Местная Над	ежные Опасн	ые		
	интрасеть	йты сайты	bl		
Надеж	ные сайты	3	Colima		
Зона дл	я надежных сайтов, к	оторые не	Санты		
причиня	т вреда вашему комп	ьютеру или			
данным В этой з	оне есть веб-сайты.				
Vacanue 6coor					
Уровень безопасности для этой зоны					
Газрешенные	уровни. люове				
сред	HNN		WKIMOTO		
- н	еподписанные элемен	гы ActiveX не скачи	ваются		
Включить	защищенный режим (	потребуется переза	апуск		
Internet Ex	plorer)				
	Дру	ой По ум	іолчани <u>ю</u>		
Выбрать уровень безопасности по умолчанию для всех зон					

Рис. 3 Надежные сайты

Укажите адрес <u>https://kpsrtz.fips.ru</u>, нажмите кнопку «Добавить» (см. Рис. 4):

адежные саиты Вы можете добавлять в эту зону ве из нее. Заданные для зоны парамет использоваться для всех ее сайтов.	б-сайты и удалять их ры безопасности будут
Добавить в зону следующий узел:	
nttps://kpsrtz.tips.ru	<u>До</u> оавить
<u>В</u> еб-сайты:	Vлалить
	240/110
для в <u>с</u> ех сайтов этой зоны требуется про	верка серверов (пцрз:
	Закрыть
	Закрыть

Рис. 4 Добавление адреса в «Надежные сайты»

### 2.3.3 Яндекс.Браузер

Откройте «Настройки Яндекс.Браузера» -> «Дополнения», включите расширение "CryptoPro Extension for CAdES Browser Plug-in" (см. Рис. 5).



Рис. 5 Подключение Плагина для Яндекс.Браузера

В случае отсутствия указанного расширения, можно перейти по кнопке «Каталог расширений для Яндекс.Браузера», найти и установить расширение.

## 3 Проверка работы Плагина.

В случае возникновения проблем при входе в Сервис проверьте работу плагина на тестовой странице КриптоПро:

https://www.cryptopro.ru/sites/default/files/products/cades/demopage/simple.html или

https://www.cryptopro.ru/sites/default/files/products/cades/demopage/cades\_bes\_sample.html

В случае успешного завершения проверки, после нажатия на кнопку «Подписать» появится электронная подпись в виде блока текстовых символов (см. Рис. 6).

Действителен до: 08.02.2027 14:34:03	
Криптопровайдер: Crypto-Pro GOST R 34.10-2001 Cryptographic Provider	Service
Алгоритм ключа: ГОСТ Р 34.10-2001	
Статус: Действителен	
Hello World	
Подписать	
Подпись сформирована успешно:	
MIIaEgYJKoZIhvcNAQcCoIIaAzCCGf8CAQExDDAKBgYqhQMCAgkFADAaBgkqhkiG9w08BwGgDQQL SGVsbGgV29ybGSgghT/MIIFGTCCBMigAwIBAgIQMGgeQMtB7zOpoLfIdpKaKTAIBgYqhQMCAgMw ggFKMRAwHAYJKoZIhvcNAQkBFg9kaXRAbHluc3Z5YXoucnUxCzAJBgINBAYTAIJVMRwwGgTVQQI DBM3hyQ5yAg032qvct6BuLrOstCwLLDRg9C7LiDQotCy0LXRgMGB0LrOstLCDQtC4gHzEsMCoG AlUECgwJ0J2QulC90LrOstCwLCDRg9C7LiDQotCy0LXRgMGB0LrOstCDQtC4gHzEsMCoG AlUECgwJ0J2QulC90LrOvtC8DVG5C4PoLFG1CDQtC4QH2RgC40LgxGDAWBgUqhQNKARINH7A NzcwMJAyNjcwMTEaMBg6CqFAwOBAvEBgswMDc3MTA0HzQ1zUzUxQTA/BgNVBAMMOLTOUTQJQ9C+ 0LQUdc40Lkg0YPQtNC+09HRgtC-0LLQtdGA0YJRjtG30LjQuSDRhtC10L3BKGAMBAXDTEyMDcy MDEyMzEXNFoXDTI3MDcxNzEyMzExHFowggFKMR4wHAY3Ko2ThvcNAQkBFg9kaXRAbWluc3Z5YXou csNscrMJAXTAIJMRACGATVINDIBM3UnDcurdad3DxtsGBuLostC4M2LkaAbWluc3Z5YXou	Å

Рис. 6 Успешное завершение проверки на тестовой странице КриптоПро





9





# Глоссарий

Сервис – сервис АРМ Регистратор.

- ОС операционная система.
- ПО программное обеспечение.

заявка на ТЗ - заявка на регистрацию заявляемого обозначения в качестве товарного знака.

**заявка на НМПТ/ПНМПТ** – Заявка на регистрацию заявляемого обозначения в качестве наименование места происхождения товара и/или предоставление исключительного права на ранее зарегистрированное наименование места происхождения товара.

заявка на ИЗ/ПМ – Заявка о выдаче патента на изобретение/полезную модель.

ФЗ-63 – Федеральный закон № 63-ФЗ «Об электронной подписи» от 06.04.2011.

ЭП - электронная подпись.

файл ЭП – файл, содержащий ЭП. Содержимое файла соответствует стандарту РКСЅ#7.

квалифицированный сертификат – электронный документ, выданный в соответствии с ФЗ-63 аккредитованным удостоверяющим центром, подтверждающий принадлежность открытого ключа ЭП определённому лицу, которое является владельцем ключа ЭП.

аккредитованный удостоверяющий центр (УЦ) – удостоверяющий центр, прошедший процедуру аккредитации в соответствии с ФЗ-63.

**средства** электронной подписи (криптопровайдер) – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

ключевой носитель - устройство, используемое для хранения ключа ЭП.

#### Некоторые термины криптографии, имеющие отношение к электронной подписи:

электронная подпись – это информация, полученная в результате криптографического преобразования другой информации (подписываемой информации) с использованием ключа ЭП и позволяющая проверить отсутствие искажения подписанной информации с момента формирования подписи (целостность), принадлежность подписи владельцу сертификата ключа ЭП (авторство), а в случае успешной проверки подтвердить факт подписания электронного документа (неотказуемость).

ключ — это информация, необходимая для выполнения криптографических операций (зашифровывание/расшифровывание сообщений, создание/проверка ЭП) с помощью





определённого криптографического алгоритма. В ассиметричных криптографических алгоритмах используется ключевая пара – открытый ключ и закрытый ключ.

закрытый ключ (private key, ключ ЭП) - закрытая (секретная) часть пары криптографических ключей. Служит для создания ЭП, которые потом можно проверять с помощью соответствующего открытого ключа, или для расшифровки сообщений, которые были зашифрованы соответствующим открытым ключом. Закрытый ключ конфиденциален (доступен только его владельцу), передача его кому-либо запрещена. Похищение закрытого ключа означает возможность получения злоумышленником любой информации, зашифрованной для владельца ключа ЭП, а также возможность подделки ЭП владельца ключа ЭП. Поэтому закрытый ключ должен сохраняться в тайне особо тщательно.

открытый ключ (public key, ключ проверки ЭП) — открытая (несекретная) часть пары криптографических ключей. Служит для проверки электронных подписей, созданных с помощью соответствующего ему закрытого ключа, или для шифрования сообщений, которые будут потом расшифрованы соответствующим ему закрытым ключом. Удостоверяющий центр подтверждает принадлежность открытых ключей конкретным лицам по запросу любого обратившегося лица.