**Настройка пользователя СЭД «Электронное ДЕЛО» и его рабочего места для подписания документов ЭЦП**

***для «толстого» клиента версии 12.2.1 – 22.2:***

1. Для подписания документов в «толстом» клиенте на компьютере пользователя должна быть установлена и запущена Криптография и КАРМа версии 56.0.219 (*как приложение*).
2. В настройках КАРМА во вкладке «ТРАНСПОРТ» обязательно должен быть выставлен флаг «Включить HTTP».
3. В настройках пользователя в СЭД во вкладке «ЭП» (*Рисунок 1*) в строке инициализации для «Объект поддержки ЭП и шифрование» прописана строка **FORCE\_CERTINCLUDE=1;ADD\_CARMA\_SIGNED\_ATTR="False";**



Рисунок 1

***для WEB-клиента версии 16.2 – 22.2:***

**ВАЖНО!** Корректное формирование ЭЦП при подписании документов в ДЕЛО-WEB возможно только в версии СЭД 16.2 и выше.

1. Для подписания документов в браузере на сервере с ДЕЛО-WEB должна быть установлена и запущена Криптография и КАРМа версии 56.0.219 (*как служба*).
2. На компьютере пользователя должна быть установлена и запущена Криптография и КАРМа 56.0.219 (*как приложение*).
3. В настройках КАРМА во вкладке «ТРАНСПОРТ» обязательно должен быть выставлен флаг «Включить HTTP».
4. В настройках пользователя в СЭД во вкладке «ЭП» (*Рисунок 2*) при настройке из модуля «Пользователи» (во вкладке «Электронная подпись» (*Рисунок 3*) при настройке из браузера) в строке инициализации для «Объект поддержки ЭП и шифрование» прописана строка

**SERVER="http://localhost:8080";FORCE\_CERTINCLUDE=1;ADD\_CARMA\_SIGNED\_ATTR="False";**

а в строке инициализации для «Объект поддержки работы с инфраструктурой открытых ключей» **–** строка **SERVER="http://localhost:8080";**



Рисунок 2



Рисунок 3

***для версии 24.3 и выше:***

1. Для подписания документов в СЭД на Backend сервере должна быть установлена Криптография и КАРМа версии 56.2.487 и выше (*как служба*).
2. На компьютере пользователя должна быть установлена и запущена Криптография и КАРМа 56.2.487 и выше (*как приложение*).
3. В настройках КАРМА во вкладке «ТРАНСПОРТ» обязательно должен быть выставлен флаг «Включить HTTP».
4. В параметрах системы СЭД на вкладке «Криптография» (*Рисунок 4*) должен быть добавлен «Общий профиль», в котором в строке инициализации прописано

**SERVER="http://127.0.0.1:8080";SERVER\_KP="http://127.0.0.1:8084";**

1. В настройках пользователя в СЭД во вкладке «Электронная цифровая подпись» (*Рисунок 5*) в строке инициализации для «Объект поддержки ЭП и шифрование» прописана строка

**ADD\_CARMA\_SIGNED\_ATTR="False";FORCE\_CERTINCLUDE=1;ADD\_SCV2\_ATTR="False";**

1. В случае, если при подписании документов ЭЦП используется USB-носитель AvPass или AvBign основного СОК с атрибутным сертификатом (АС) **ИЛИ** id-карта (независимо от наличия АС), то дополнительно:
	1. На Backend сервере должна быть установлена клиентская программа NTClientSoftware (КП, [предоставляется НЦЭУ](https://nces.by/service/po/)), т.е. загружены библиотеки.
	2. На компьютере пользователя должна быть установлена и запущена КП.
	3. В настройках КП необходимо выбрать тип носителя, который используется для формирования ЭЦП.
	4. В настройках КАРМА во вкладке «Общие» в поле «Модуль по умолчанию» должно быть прописано «**kp**» (англ.), после чего КАРМА должна быть перезагружена.
	5. В настройках пользователя в СЭД во вкладке «Электронная цифровая подпись» (*Рисунок 6*) в строке инициализации для «Объект поддержки ЭП и шифрование» прописана строка

**ADD\_CARMA\_SIGNED\_ATTR="False";FORCE\_CERTINCLUDE=1;ADD\_SCV2\_ATTR="False";DESCRIPTIONFORMAT="<SN> <OID.2.5.4.41> <G>";** **SERVER\_KP="http://127.0.0.1:8084";**

а в строке инициализации для «Объект поддержки работы с инфраструктурой открытых ключей» – строка **SERVER="http://localhost:8080";**

* 1. В настройках пользователя в СЭД во вкладке «Атрибутные сертификаты» должен быть загружен АС к основному СОК пользователя (для id-карты при его наличии).



Рисунок 4



Рисунок 5



Рисунок 6