IT MONITORING
DIGITAL SECURITY

Инструкция по настройке АРМ для работы с электронной подписью на базе macOS

г. Краснодар 2020 г.

IT MONITORING

ПРОСТЫЕ И МОЩНЫЕ РЕШЕНИЯ ДЛЯ КОМПЛЕКСНОГО УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ
ЭЛЕКТРОННАЯ ПОДПИСЬ | SOCSHELL 4.0 | ЦЕНТР МОНИТОРИНГА

Рассматриваемая конфигурация:

- macOS 10.15.2 (в других поддерживаемых версиях macOS настройки аналогичны);

- КриптоПро CSP 5.0 R2;

- КриптоПро ЭЦП Browser plug-in 2.0;

- Chromium GOST.

1) Установка КриптоПро CSP 5.0:

Скачайте дистрибутив КриптоПро CSP 5.0 R2 с сайта КриптоПро (загрузка доступна после предварительной регистрации на сайте).

Откройте папку «Загрузки» и распакуйте скачанный архив macos-uni.tgz (рисунок 1).

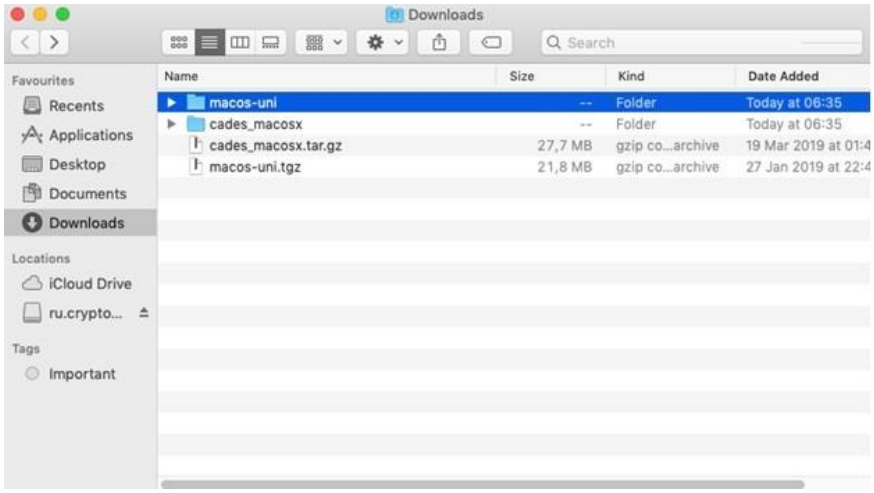

Рисунок 1 – Распакованный архив с КриптоПро CSP

Далее необходимо открыть распакованную папку macos-uni (рисунок 2).

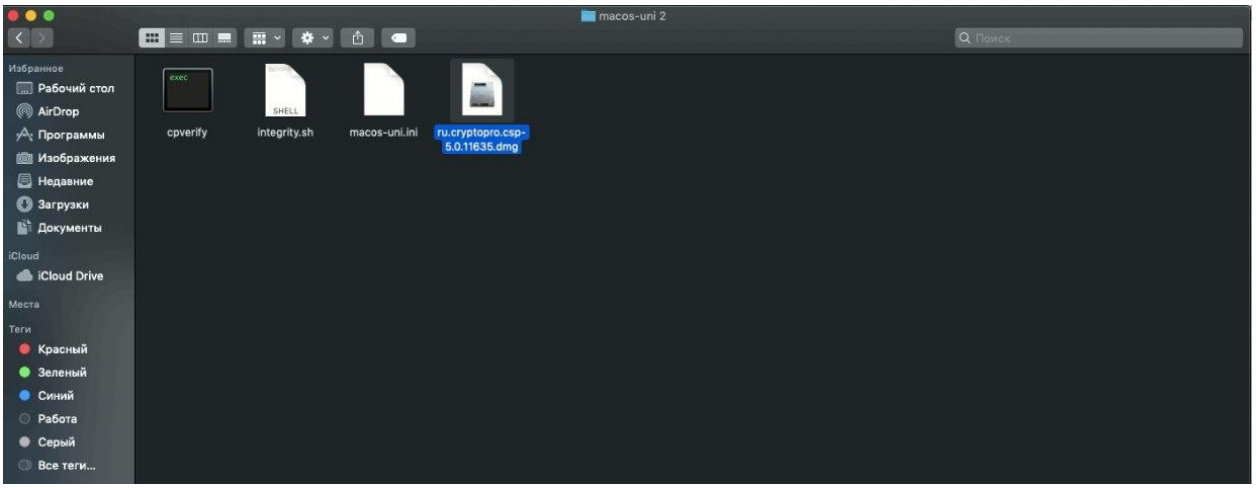

Рисунок 2 - Распакованная папка macos-uni

В контекстном меню файла ru.cryptopro.csp-5.0.11635.dmg выберите «Открыть». В открывшемся окне правой кнопкой мыши нажмите на ярлык ru.cryptopro.csp-5.0.11635.mpkg и выберите «Открыть» (рисунок 3).

Рисунок 3 – Файл ru.cryptopro.csp-5.0.11635.mpkg

В появившемся предупреждающем окне нажмите кнопку «Открыть» и щелкните по ярлыку установщика в Dock (рисунок 4).

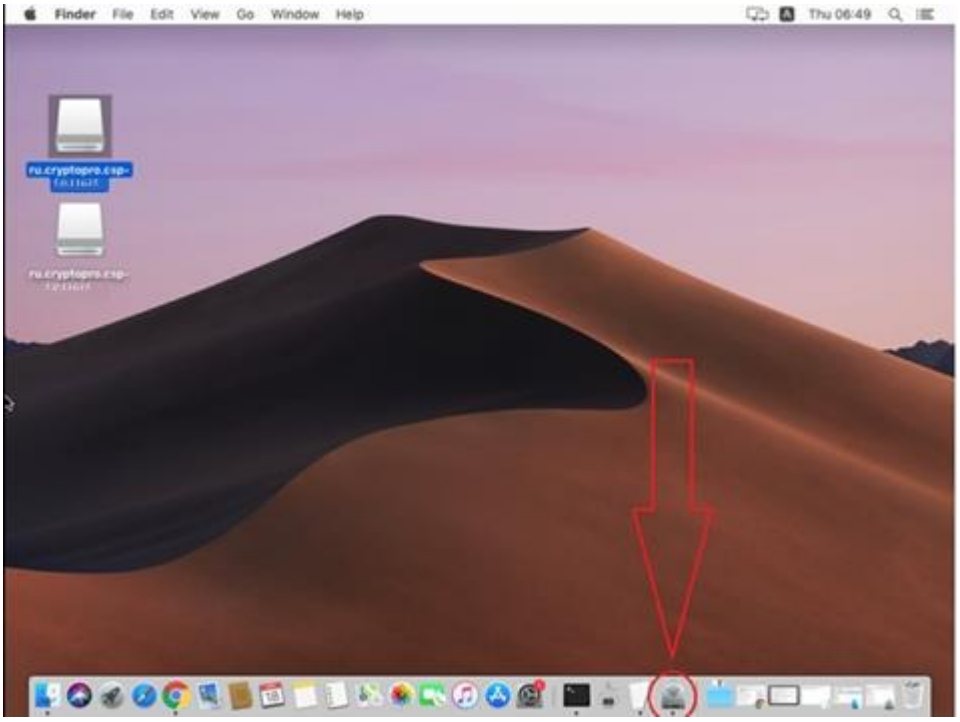

Рисунок 4 – Установщик Dock

Затем необходимо нажать «Продолжить» в предупреждающем окне (рисунок 5).

Рисунок 5 - Установщик Dock

Следуйте инструкциям установщика.

2) Установите КриптоПро ЭЦП Browser Plug-in 2.0 (аналогично КриптоПро CSP):

Скачайте КриптоПро ЭЦП Browser plug-in 2.0 с официального сайта КриптоПро. Откройте папку «Загрузки» и распакуйте скачанный архив cades_macosx.tar.gz. Затем необходимо открыть папку «cades_macosx» (рисунок 6).

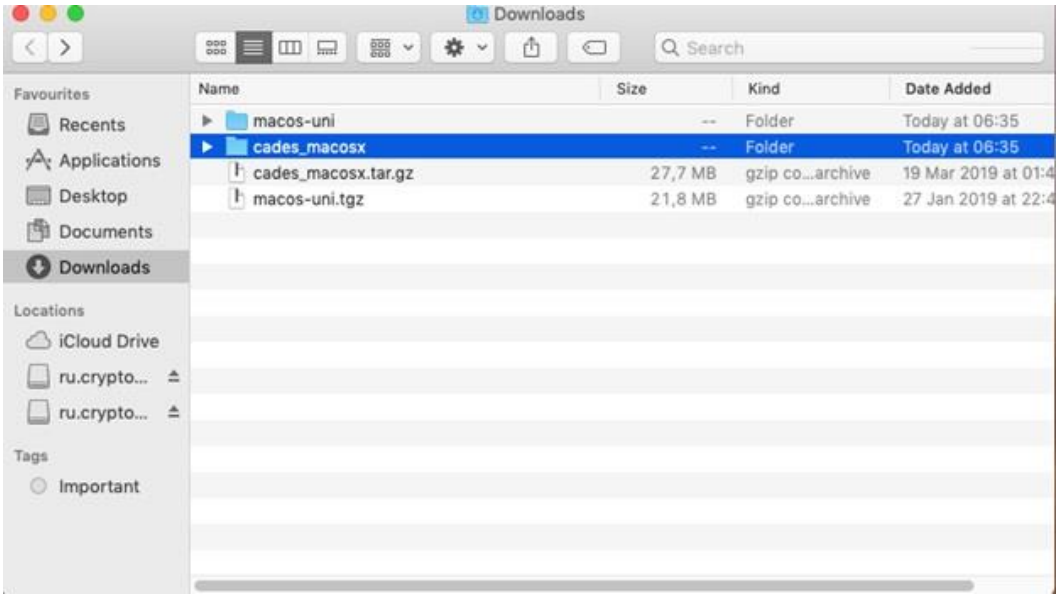

Рисунок 6 – Папка cades_macosx

Нажав правой кнопкой на файл cprocsp-pki-2.0.0.dmg выберите «Открыть» (рисунок 7).

Рисунок 7 – файл cprocsp-pki-2.0.0.dmg

В открывшемся окне необходимо нажать правой кнопкой мыши на ярлык cprocsp-pki-2.0.0.mpkg и выбрать «Открыть». В появившемся предупреждающем окне нажмите кнопку «Открыть».

Щелкните по ярлыку установщика в нижнем меню (аналогично рисунку 6) и нажмите «Продолжить» в предупреждающем окне. Следуйте инструкциям установщика.

Дальнейшая настройка осуществляется через стандартное приложение macOS Терминал (Terminal) - Finder> пункт меню «Переход»> Утилиты> Терминал

3) Установка личного сертификата (при вставленном ключевом носителе) команда в терминале:

Обращаем ваше внимание на то, что Облачная подпись работает только с КриптоПро версии 5.0 сборки R2.

Установка осуществляется следующим образом:

1) скачать приложение myDSS на Ваш мобильный телефон (Android/iOS);

2) запускаем приложение myDSS> три полоски (☰) > Сканировать QR-код;

3) на ПК запускаем приложение «Инструменты КриптоПро» и переходим на вкладку «Облачный провайдер»:

в поле Сервер авторизации указываем ссылку: https://dss.e-signature.pro/STS/oauth

в после Сервер DSS указываем ссылку: https://dss.e-signature.pro/SignServer/rest

нажимаем на кнопку «Установить сертификаты» появится окно подтверждения действий, где необходимо нажать «ОК».

После чего откроется окно авторизации, где необходимо:

4) ввести логин в формате XXX-XXX-XXX-XX (Ваш СНИЛС, указывается с дефисами) (рисунок 8).

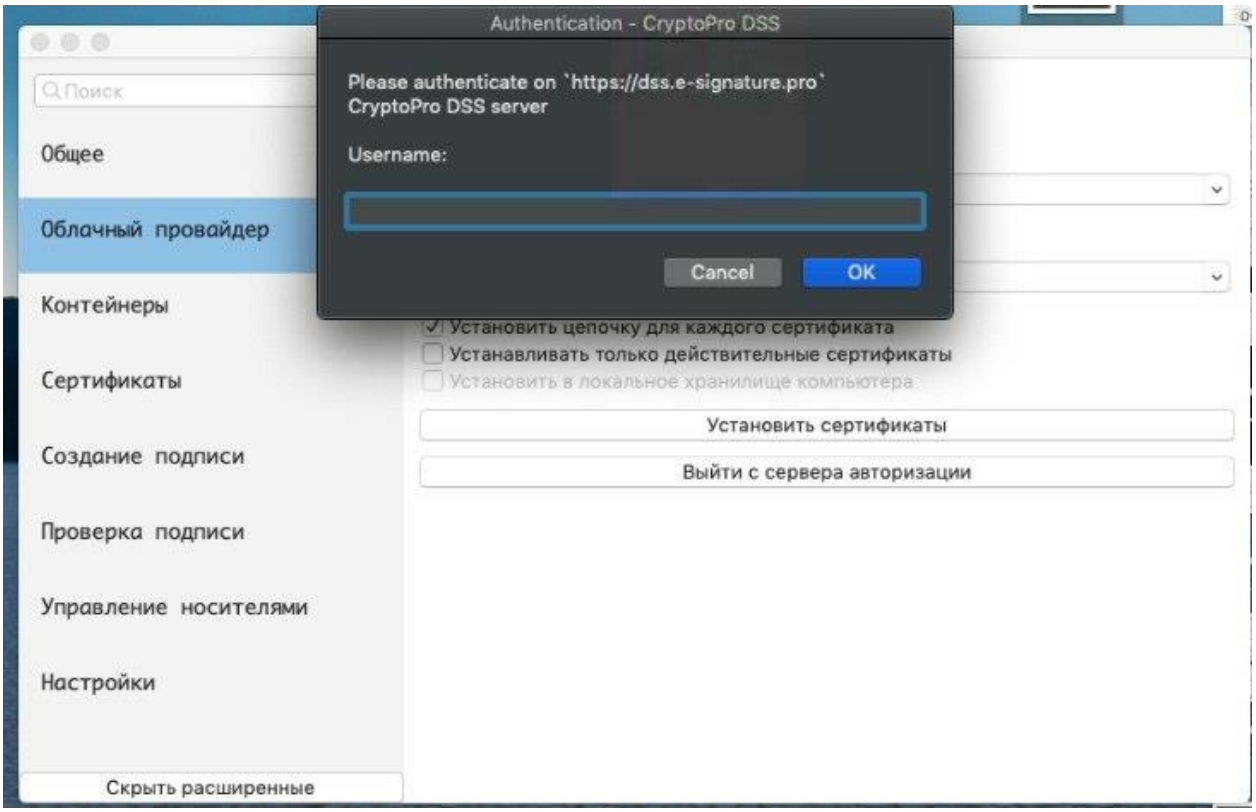

Рисунок 8 – Ввод СНИЛС

5) ввести пароль, высылаемый вместе с QR-кодом (рисунок 9);

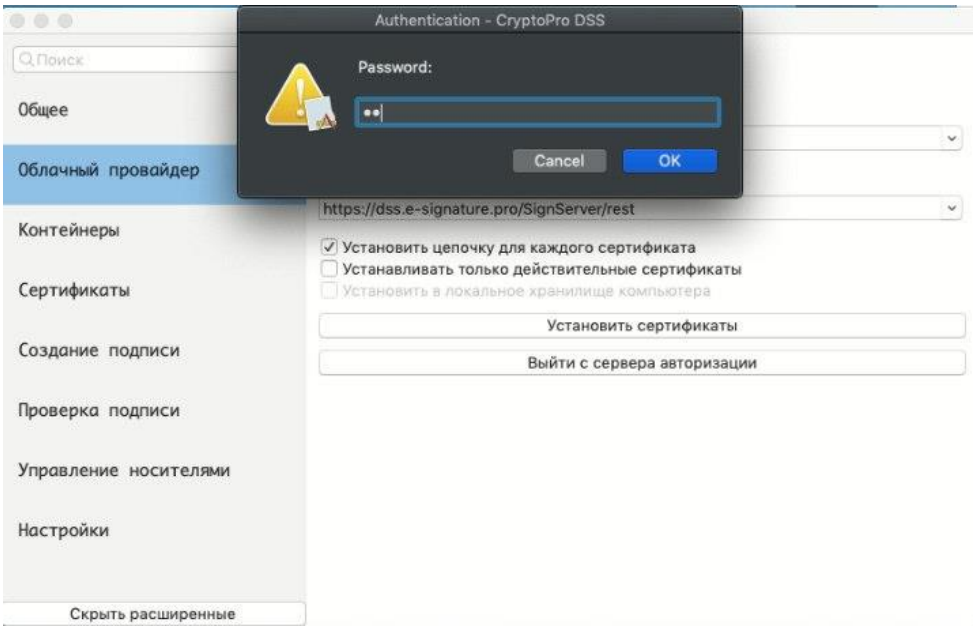

Рисунок 9 – Ввод пароля

6) на телефоне в приложении myDSS подтвердить операцию и после подтверждения на телефоне нажать «ОК» на компьютере (рисунок 10).

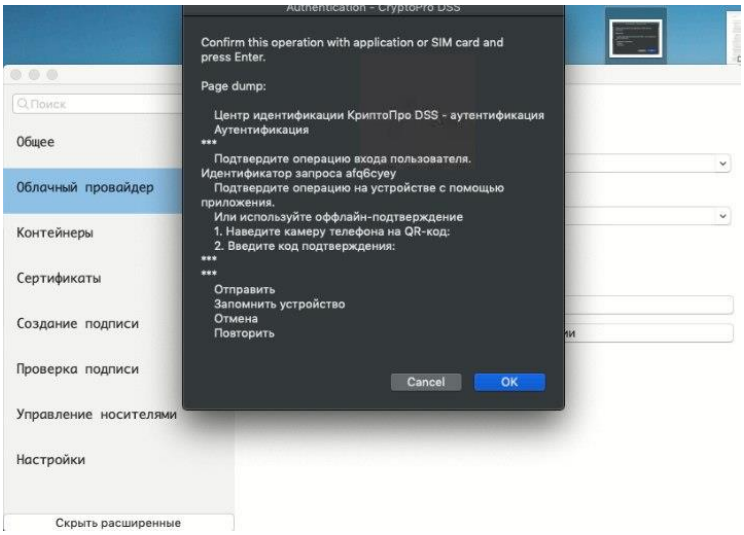

Рисунок 10 – окно подтверждения действий

После чего в окне программы Вы увидите надпись «Сертификат успешно установлен».

*Если подпись на **физическом носителе (USB, JaCarta, RuToken и т.д.)**, необходимо в терминале ввести команду:*

/opt/cprocsp/bin/csptestf -absorb -certs -autoprov

4) При использовании личного сертификата, необходима установка корневого сертификата удостоверяющего центра.

Осуществляется это путем прописывания команды в терминале:

/opt/cprocsp/bin/certmgr -list

1. скопировать адрес строки URL сертификата УЦ (CA cert URL) в блоке информации о сертификате из вывода предыдущей команды;

2. скачать сертификат удостоверяющего центра, вставив скопированный ранее адрес в адресную строку браузера или команда в терминале:

curl http://ra.docshell.ru/aia/llc_it_monitoring_2012.cer -o ~/Downloads/root.cer

либо

curl http://krasnodar.pro/cdp/llc_it_monitoring_2012.cer -o ~/Downloads/root.cer

либо

curl http://rosreport.ru/cdp/llc_it_monitoring_2012.cer -o ~/Downloads/root.cer

команда в терминале:

/opt/cprocsp/bin/certmgr -inst -store root -f ~/Downloads/root.cer

(при условии, что сертификат удостоверяющего центра сохранен в директорию Загрузки под именем root.cer).

5) Проверить правильность настройки можно на тестовой странице проверки плагина (только Chromium GOST).

Если настройка произведена корректно, то в поле Сертификат появится строка, соответствующая сертификату.

После выбора сертификата и нажатия кнопки «Подписать» появится надпись «Подпись сформирована успешно».

6) Проверить статус лицензии КриптоПро CSP можно командой:

/opt/cprocsp/sbin/cpconfig -license -view

7) Активировать лицензию КриптоПро CSP можно командой:

sudo /opt/cprocsp/sbin/cpconfig -license -set серийный_номер_лицензии

При появлении строки Password: нужно ввести пароль пользователя в операционной системе macOS и нажать клавишу Enter.

Поддерживаемые ключевые носители:

- флеш-накопитель;
- жесткий диск компьютера;
- Рутокен (для Рутокен S необходима установка драйвера) и перезагрузка компьютера;

- ESMART Token;
- иное.

<u>Внимание:</u> в КриптоПро CSP 4.0 ключевые носители eToken и JaCarta не поддерживаются (JaCarta поддерживается в КриптоПро CSP 5.0)

Возможность работы на macOS с ЭЦП на порталах нужно уточнять в технической поддержке порталов.

Если в требованиях к рабочему месту при работе на портале с ЭЦП только наличие КриптоПро CSP и КриптоПро ЭЦП Browser plug-in, то, вероятнее всего, на этом портале есть возможность работы на macOS.

Настройка браузера Chromium GOST для операционной системы MacOS для входа на gosuslugi.ru и nalog.ru

Рассматриваемая конфигурация:

— macOS 10.15.2 (в других поддерживаемых версиях macOS настройки аналогичны);

— КриптоПро CSP 5.0 R2;

— плагин для работы с порталом государственных услуг (IFCPlugin) - поддерживаются версии macOS 10.9 - 10.15;

— ключевой контейнер с соответствующим квалифицированным сертификатом внутри;

— Chromium GOST.

Порядок настройки:

1) Установить КриптоПро CSP 5.0 R2 (или новее) (если он не установлен!) - список устанавливаемых пакетов оставить по умолчанию.

2) Установить плагин для работы с порталом государственных услуг (IFCPlugin) (если он не установлен!).

3) Скачать файл конфигурации для IFCPlugin в директорию Загрузки.

4) Выполнить в терминале команды (при появлении строки Password: нужно ввести пароль пользователя в операционной системе macOS и нажать клавишу Enter):

sudo cp ~/Downloads/ifc.cfg /Library/Internet/Plug-Ins/IFCPlugin.plugin/Contents

/opt/cprocsp/bin/csptestf -absorb -certs -autoprov

5) Для Chromium GOST также выполнить в терминале команду (все 3 строки – это одна команда):

sudo cp

/Library/Google/Chrome/NativeMessagingHosts/ru.rtlabs.ifcplugin.json/Library/Application/Support/Chromium/NativeMessagingHosts

6) Проверить в используемом браузере (Chromium GOST), что включено расширение - Расширение для плагина Госуслуг.

Расширение для Chromium GOST.

8) На странице входа на портал Госуслуг:

1. нажать на ссылку Вход с помощью электронной подписи;
2. нажать на кнопку «Готово»;
3. выбрать нужный сертификат электронной подписи;

4. в окне «Ввод» пин-кода нажать кнопку «Продолжить»;

5. при возникновении окна CryptoPro CSP ввести пин-код для ключевого контейнера в поле Password и нажать кнопку «OK».

7) Для работы на портале nalog.ru необходимо:

выполнить команды:

sudo /opt/cprocsp/sbin/cpconfig -ini '\cryptography\OID\1.2.643.7.1.1.1.1!3' -add string 'Name' 'GOST R 34.10-2012 256 bit'

sudo /opt/cprocsp/sbin/cpconfig -ini '\cryptography\OID\1.2.643.7.1.1.1.2!3' -add string 'Name' 'GOST R 34.10-2012 512 bit'

При появлении строки Password: нужно ввести пароль пользователя в операционной системе macOS и нажать клавишу Enter.

- использовать браузер с поддержкой TLS сертификатов по ГОСТ Р 34.10-2012 (Chromium GOST),

- входить в личный кабинет по прямой ссылке:

https://lkul.nalog.ru - для юридических лиц,

https://lkipgost.nalog.ru/lk - для индивидуальных предпринимателей.

Чтобы удалить выбранный ранее сертификат электронной подписи из кеша Chromium GOST перезапустите браузер.