

Рутокен ЭЦП в операционных системах macOS

- [Общая информация](#)
- [Определение названия модели USB-токена](#)
- [Проверка корректности подключения считывателя для смарт-карт к компьютеру](#)
- [Определение названия модели смарт-карты](#)
- [Проверка работы Рутокен ЭЦП в системе](#)
- [Проверка наличия RSA сертификатов и ключевых пар RSA на Рутокен ЭЦП](#)
 - [Начиная с версии 10.15](#)
 - [До версии 10.15](#)
- [Проверка наличия ГОСТ сертификатов и ключевых пар ГОСТ на Рутокен ЭЦП](#)
- [Изменение PIN-кода Рутокен ЭЦП](#)
- [Решение проблем с Рутокен ЭЦП в системе](#)

Общая информация

Устройства семейства Рутокен ЭЦП используются для безопасного хранения и предъявления персональной информации: ключей шифрования, сертификатов, лицензий, удостоверений и других данных.

Для работы с USB-токеном подключите его к USB-порту компьютера.

Для работы со смарт-картой вставьте ее в считыватель для смарт-карт и подключите считыватель к USB-порту компьютера.

Чтобы проверить корректность работы Рутокен ЭЦП в операционных системах macOS необходимо выполнить действия, указанные в данной инструкции.

Если вы используете для устройства стандартный PIN-код (12345678), то рекомендуется его изменить на более сложный.

Определение названия модели USB-токена

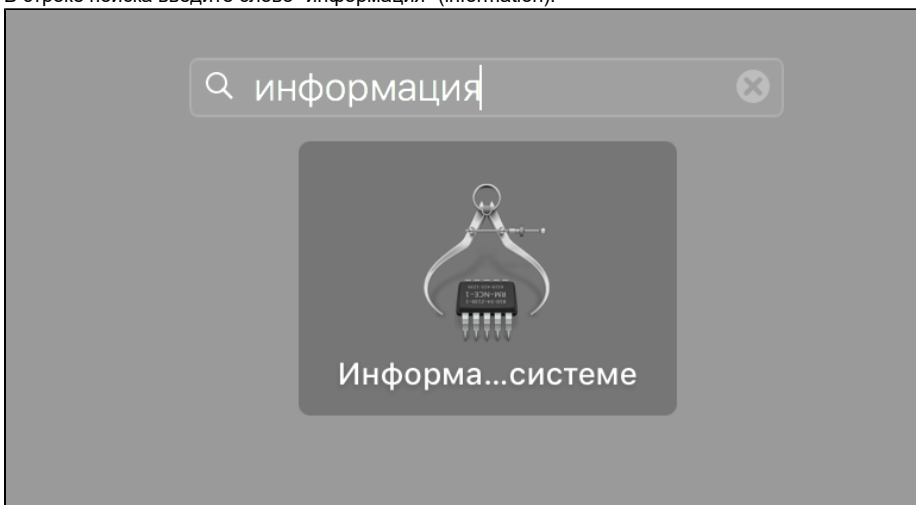
Если вы работаете со смарт-картой, то выполнять процедуру, описанную в этом разделе, не надо.

Для определения названия модели USB-токена:

1. Подключите USB-токен к компьютеру
2. Откройте программу **Launchpad**.



3. В строке поиска введите слово "информация" (information).

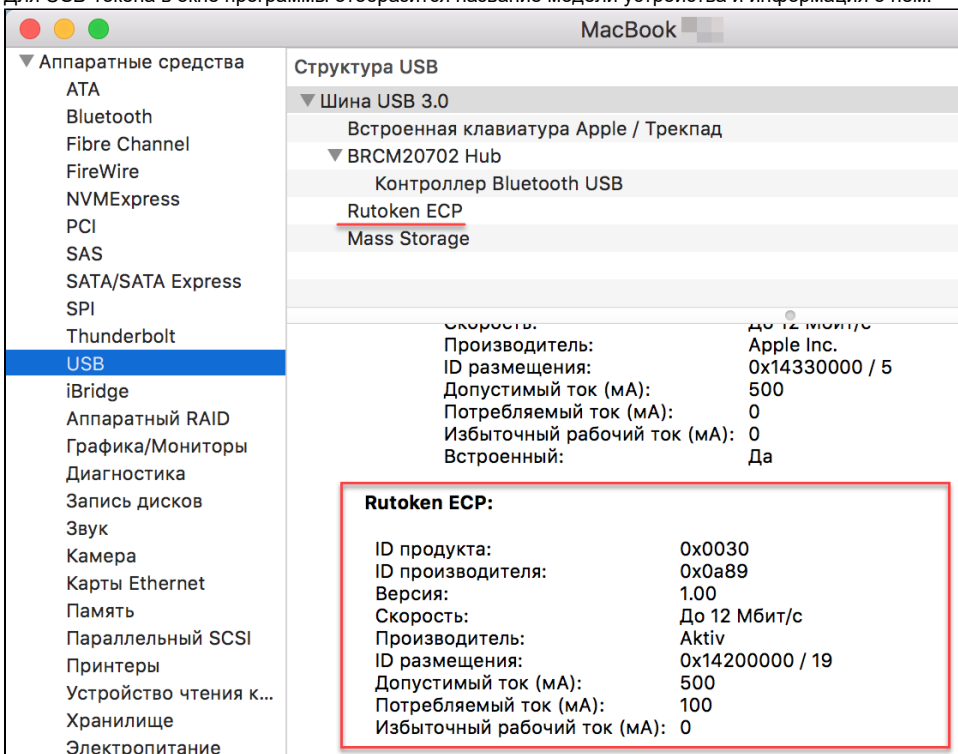


4. Откройте программу **Информация о системе (System Information)**.



5. На боковой панели окна программы выберите пункт **USB**.

6. Для USB-токена в окне программы отобразится название модели устройства и информация о нем:



Проверка корректности подключения считывателя для смарт-карт к компьютеру

Если вы работаете с USB-токеном, то выполнять процедуру, описанную в этом разделе, не надо.

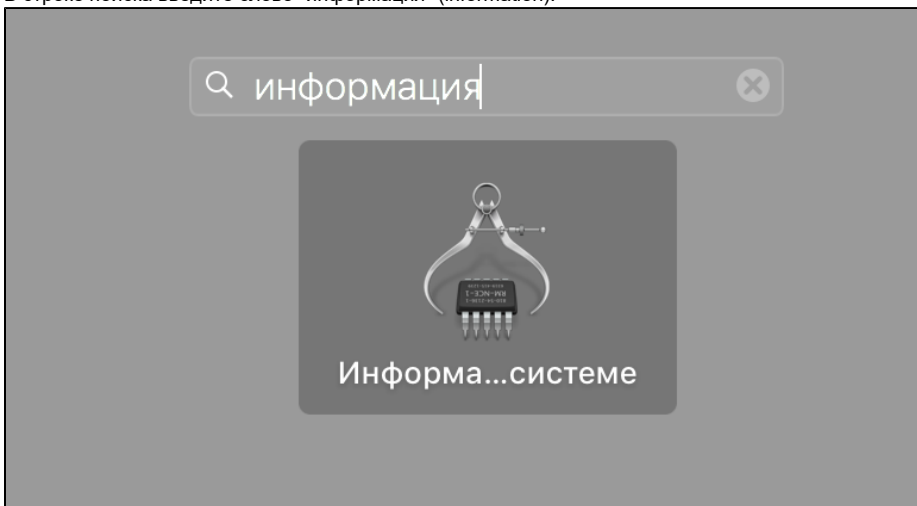
Для проверки корректности подключения считывателя для смарт-карт к компьютеру:

1. Подключите считыватель для смарт-карт к компьютеру и вставьте в него смарт-карту

2. Откройте программу **Launchpad**.



3. В строке поиска введите слово "информация" (information).

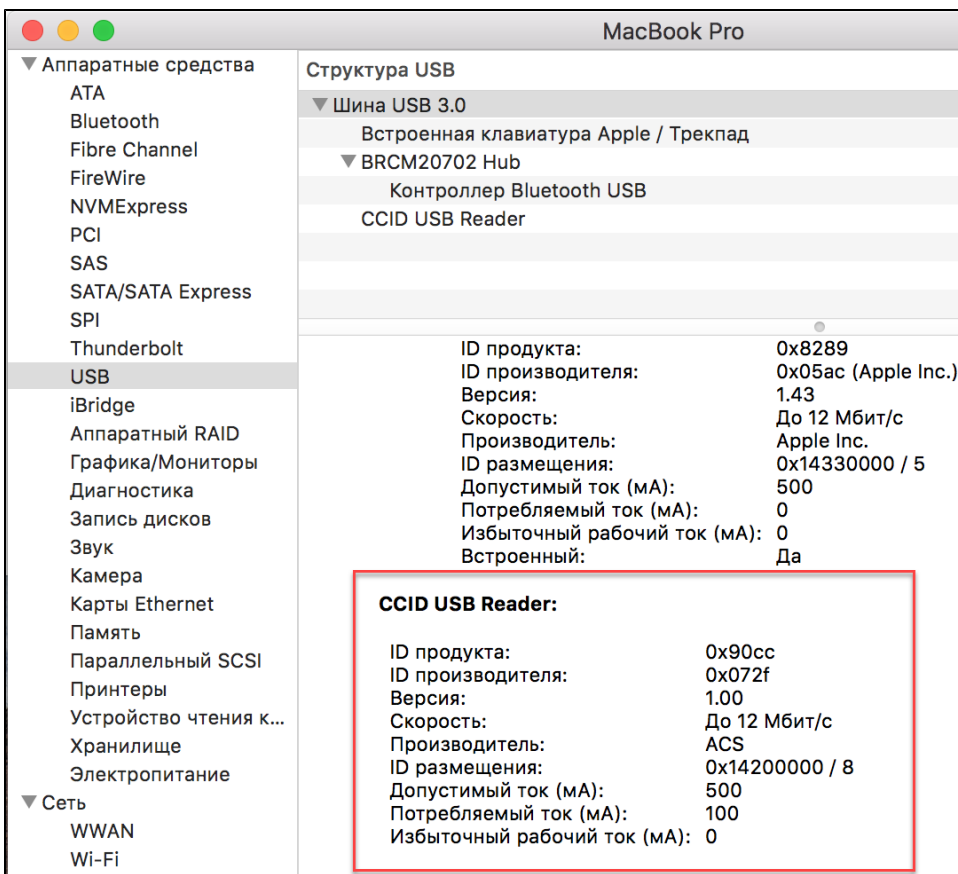


4. Откройте программу **Информация о системе (System Information)**.



5. На боковой панели окна программы выберите пункт **USB**.

6. Для считывателя в окне программы отобразится название модели считывателя и информация о нем.



Это означает, что считыватель для смарт-карт подключен корректно.

Определение названия модели смарт-карты

Если вы работаете с USB-токеном, то выполнять процедуру, описанную в этом разделе, не надо.

Перед запуском процесса определения названия модели смарт-карты:

- загрузите и установите пакет **OpenSC**;
- загрузите и установите библиотеку **PKCS#11**;
- определите путь до библиотеки **libtpkcs11ecp.dylib**.

Актуальная версия установочного пакета OpenSC доступна по ссылке:

<https://github.com/OpenSC/OpenSC/wiki>

Download

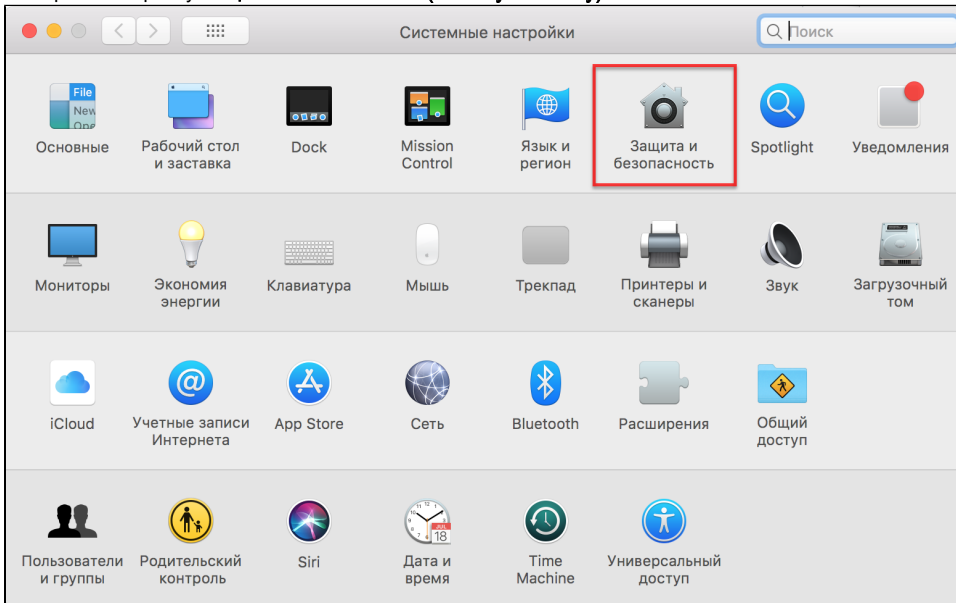
OpenSC 0.22.0 is the latest stable version released on 10.08.2021. It is available as

- Windows installer
 - [OpenSC-0.22.0_win64.msi](#) for 64 bit programs
 - [OpenSC-0.22.0_win32.msi](#) for 32 bit programs
- [OpenSC-0.22.0.dmg](#): macOS installer
- [opensc-0.22.0.tar.gz](#): Source code distribution

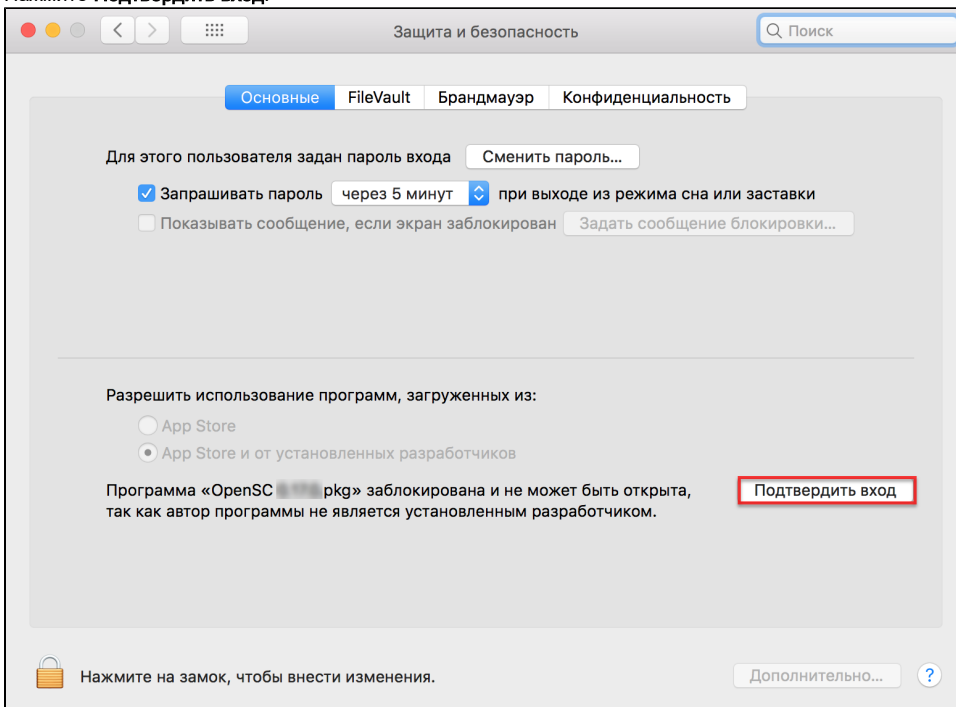
Для установки пакета OpenSC:

1. Запустите программу установки пакета OpenSC.
2. В окне с уведомлением о том, что автор программы является неустановленным разработчиком нажмите **ОК**.

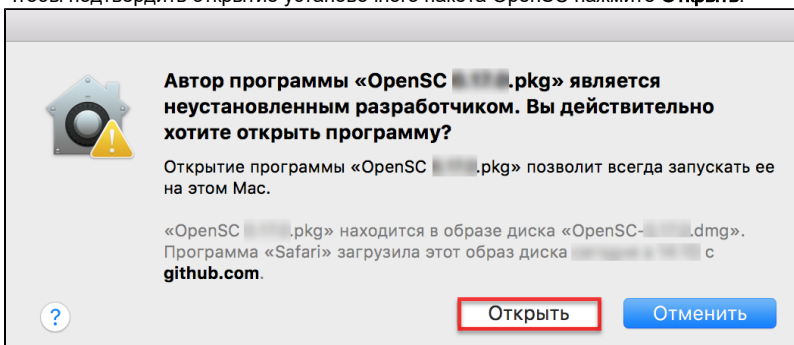
3. Выберите в меню Apple (🍏) пункт **Системные настройки (System Preferences)**.
4. Выберите настройку **Защита и безопасность (Security & Privacy)**.



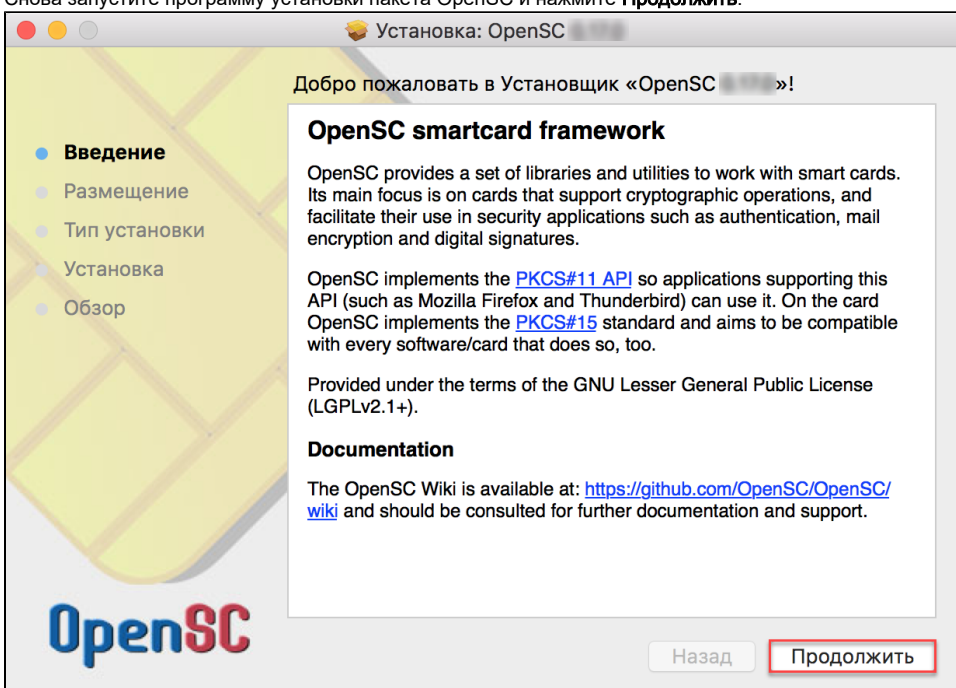
5. Нажмите **Подтвердить вход**.



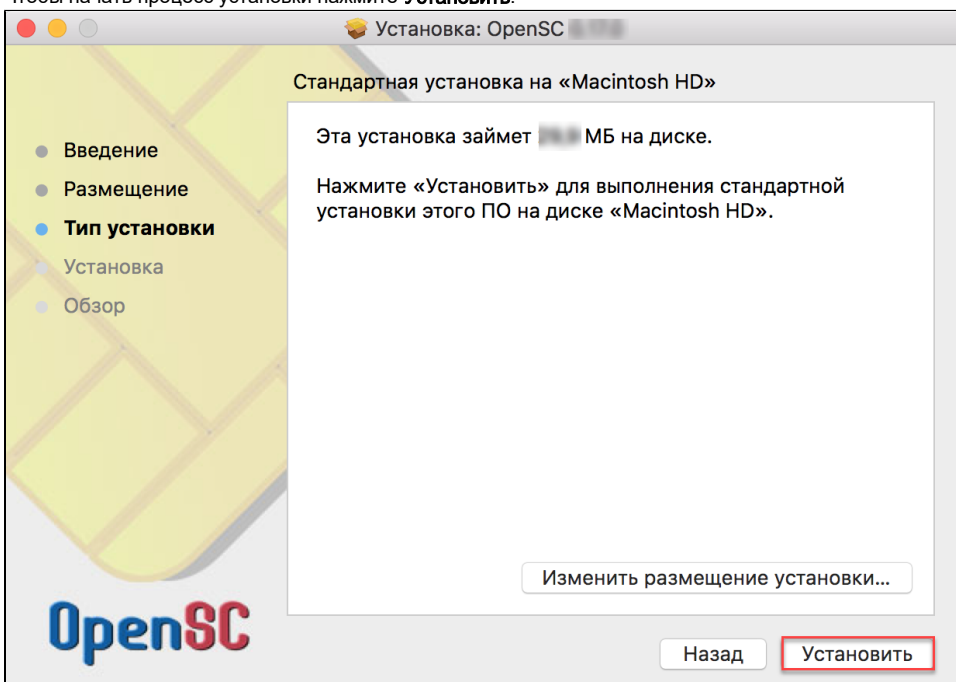
6. Чтобы подтвердить открытие установочного пакета OpenSC нажмите **Открыть**.



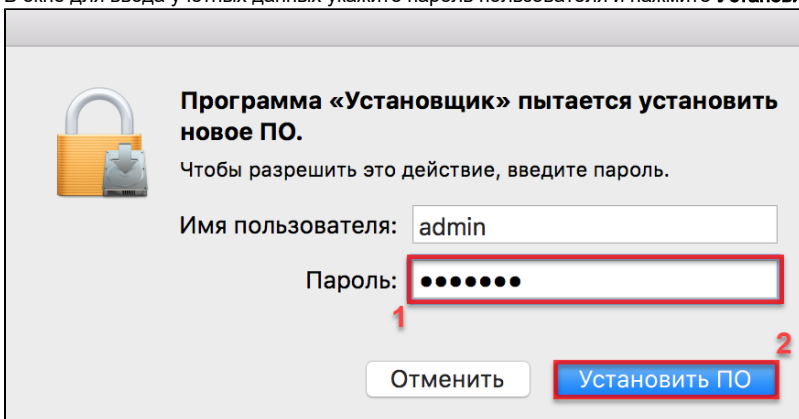
7. Снова запустите программу установки пакета OpenSC и нажмите **Продолжить**.



8. Чтобы начать процесс установки нажмите **Установить**.

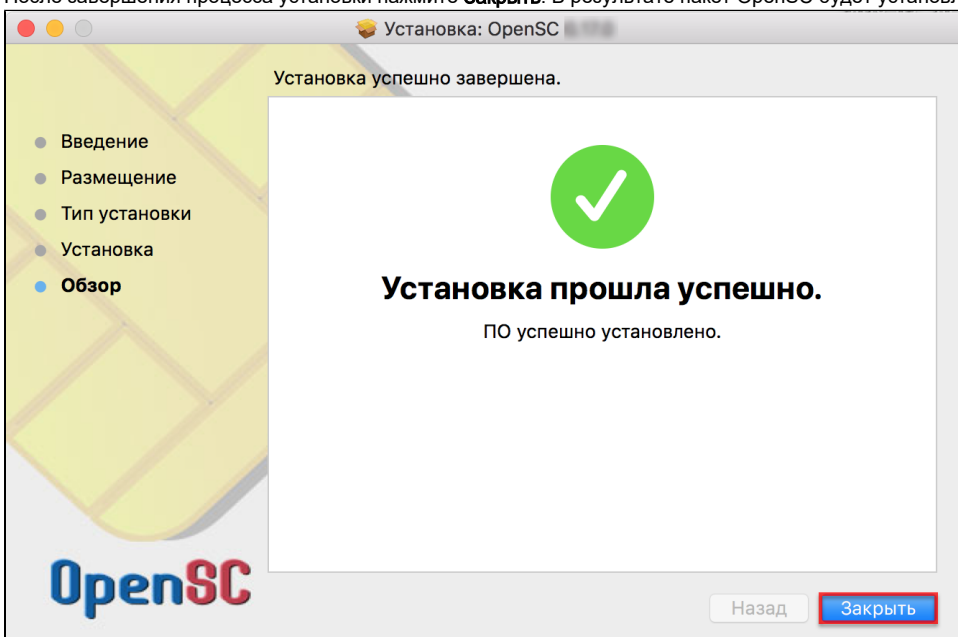


9. В окне для ввода учетных данных укажите пароль пользователя и нажмите **Установить ПО**.



The screenshot shows a window titled "Программа «Установщик» пытается установить новое ПО." (The program "Installer" is trying to install new software). It contains a lock icon and the text "Чтобы разрешить это действие, введите пароль." (To allow this action, enter the password). Below this, there are two input fields: "Имя пользователя:" (Username) with the value "admin" and "Пароль:" (Password) with masked characters. A red box highlights the password field with a red "1" next to it. At the bottom, there are two buttons: "Отменить" (Cancel) and "Установить ПО" (Install software), with a red "2" next to the latter.

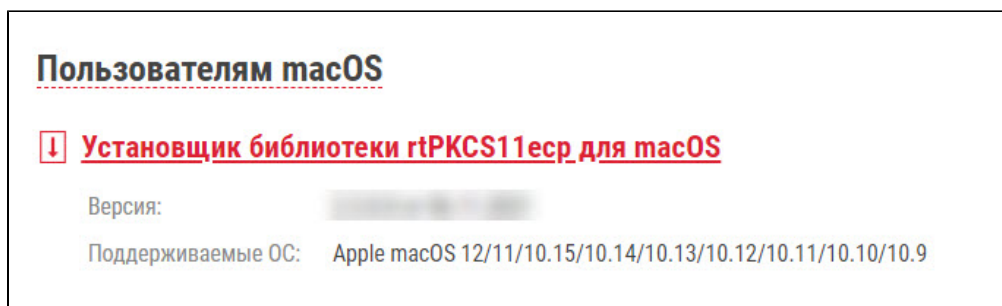
10. После завершения процесса установки нажмите **Заккрыть**. В результате пакет OpenSC будет установлен.



The screenshot shows a window titled "Установка: OpenSC" (Installation: OpenSC). It displays a large green checkmark and the text "Установка прошла успешно." (Installation completed successfully.) and "ПО успешно установлено." (Software successfully installed.). On the left side, there is a list of steps: "Введение" (Introduction), "Размещение" (Placement), "Тип установки" (Installation type), "Установка" (Installation), and "Обзор" (Review), with "Обзор" being the active step. At the bottom right, there are two buttons: "Назад" (Back) and "Заккрыть" (Close), with a red box highlighting the latter.

11. Если после установки пакета необходимо остановить установщик, то нажмите **Остановить**.

Для того чтобы загрузить библиотеку PKCS#11 перейдите по указанной ссылке и выберите необходимую версию:
<https://www.rutoken.ru/support/download/pkcs/>

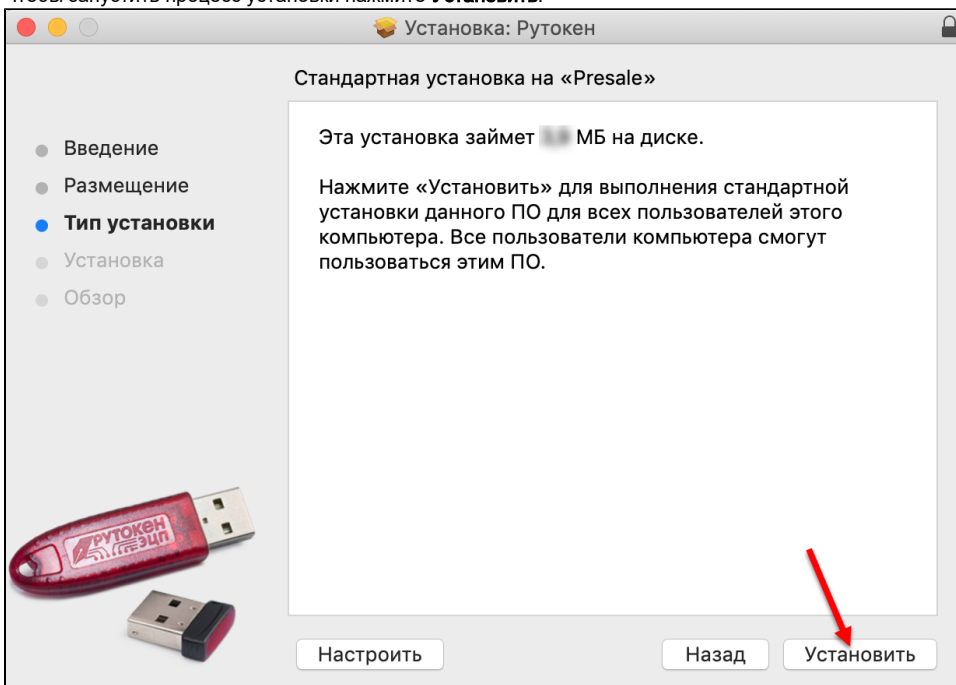


The screenshot shows a page titled "Пользователям macOS" (For macOS users). It features a red download icon and the text "Установщик библиотеки rtPKCS11еср для macOS" (Installer for rtPKCS11еср library for macOS). Below this, there are two fields: "Версия:" (Version) and "Поддерживаемые ОС:" (Supported OS), with the latter containing the text "Apple macOS 12/11/10.15/10.14/10.13/10.12/10.11/10.10/10.9".

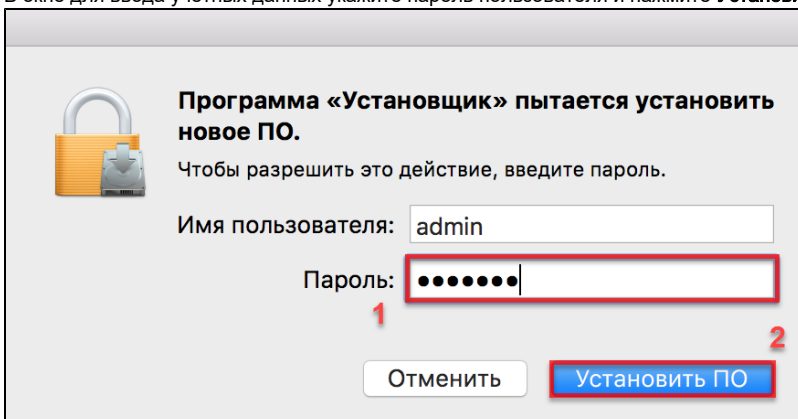
Для установки библиотеки PKCS#11:

1. Запустите программу установки библиотеки PKCS#11 и нажмите **Продолжить**.

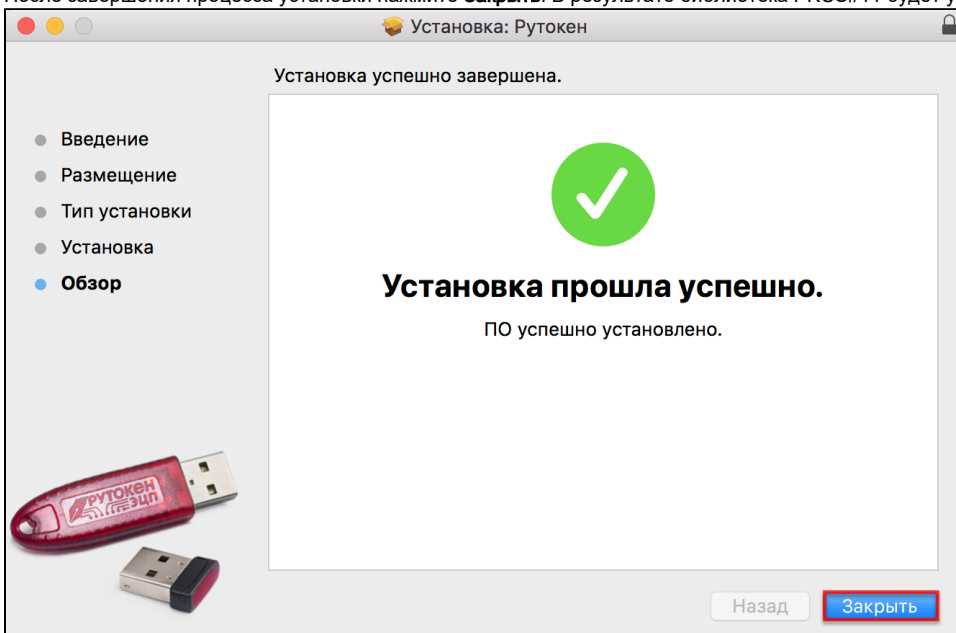
2. Чтобы запустить процесс установки нажмите **Установить**.



3. В окне для ввода учетных данных укажите пароль пользователя и нажмите **Установить ПО**.



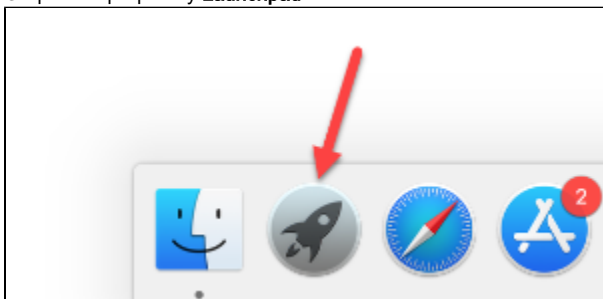
4. После завершения процесса установки нажмите **Заккрыть**. В результате библиотека PKCS#11 будет установлена.



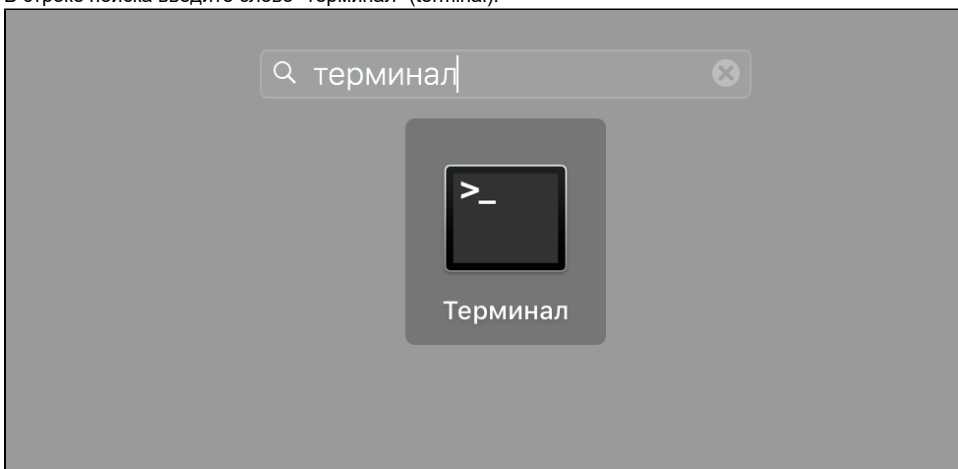
5. Если после установки библиотеки необходимо остановить установщик, то нажмите **Остановить**.

Для того чтобы определить путь до библиотеки librtpkcs11ecp.dylib:

1. Откройте программу **Launchpad**.



2. В строке поиска введите слово "терминал" (terminal).



3. Откройте **Терминал (Terminal)**.



4. Введите команду:

```
sudo find /usr -name librtpkcs11ecp.dylib
```

5. Нажмите **Enter**. В результате в окне Терминала отобразится путь до библиотеки librtpkcs11ecp.dylib.

```
android-cb449385bb8d1615:~ admin$ sudo find /usr -name librtpkcs11ecp.dylib
Password:
/usr/local/lib/pkcs11/librtpkcs11ecp.dylib
/usr/local/lib/librtpkcs11ecp.dylib
```

Чтобы **определить название модели смарт-карты** введите команду:

```
pkcs11-tool --module {A} -T
```

A — путь до библиотеки librtpkcs11ecp.dylib.

В разделе **token model** отобразится название модели смарт-карты.

```
android-cb449385bb8d1615:~ admin$ pkcs11-tool --module /usr/local/lib/librtpkcs11ecp.dylib -T
Available slots:
Slot 0 (0x0): ACS ACR 38U-CCID
token label      : Rutoken ECP <no label>
token manufacturer : Aktiv Co.
token model      : Rutoken ECP SC
token flags      : login required, rng, SO PIN to be changed, token initialized, PIN initialized, user PIN to be changed
hardware version : 54.2
firmware version : 18.0
serial num       : 332882eb
pin min/max      : 6/32
```

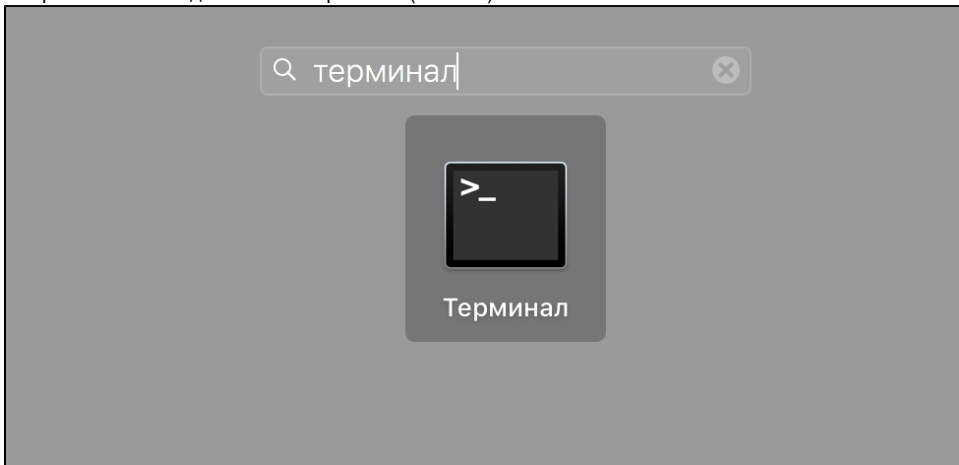
Проверка работы Рутокен ЭЦП в системе

Для проверки работы Рутокен ЭЦП:

1. Подключите устройство к компьютеру.
2. Откройте программу **Launchpad**.



3. В строке поиска введите слово "терминал" (terminal).



4. Откройте **Терминал (Terminal)**.



5. Введите команду:

```
pcsc test
```

6. Нажмите **Enter** и введите цифру "1".
7. Нажмите **Enter** и введите цифру "1".
8. Нажмите **Enter**.
9. Если отобразилось следующее сообщение:
Для USB-токена:

```
admin — -bash — 80x43
Last login: Mon Dec 25 16:05:22 on ttys000
MBP-~ admin$ pcsctest

MUSCLE PC/SC Lite Test Program

Testing SCardEstablishContext : Command successful.
Testing SCardGetStatusChange
Please insert a working reader : Command successful.
Testing SCardListReaders : Command successful.
Reader 01: Aktiv Rutoken ECP
Enter the reader number : 1
Waiting for card insertion
Testing SCardConnect : Command successful.
Testing SCardStatus : Command successful.
Current Reader Name : Aktiv Rutoken ECP
Current Reader State : 0x54
Current Reader Protocol : 0x1
Current Reader ATR Size : 15 (0xf)
Current Reader ATR Value : 3B 8B 01 52 75 74 6F 6B 65 6E 20 44 53 20 C1
Testing SCardDisconnect : Command successful.
Testing SCardReleaseContext : Command successful.
Testing SCardEstablishContext : Command successful.
Testing SCardGetStatusChange
Please insert a working reader : Command successful.
Testing SCardListReaders : Command successful.
Reader 01: Aktiv Rutoken ECP
Enter the reader number : 1
Waiting for card insertion
Testing SCardConnect : Command successful.
Testing SCardStatus : Command successful.
Current Reader Name : Aktiv Rutoken ECP
Current Reader State : 0x54
Current Reader Protocol : 0x1
Current Reader ATR Size : 15 (0xf)
Current Reader ATR Value : 3B 8B 01 52 75 74 6F 6B 65 6E 20 44 53 20 C1
Testing SCardDisconnect : Command successful.
Testing SCardReleaseContext : Command successful.

PC/SC Test Completed Successfully !
MBP-~ admin$
```

Значит USB-токен работает.

Для смарт-карты:

```
admin — -bash — 94x39

MUSCLE PC/SC Lite Test Program

Testing SCardEstablishContext : Command successful.
Testing SCardGetStatusChange
Please insert a working reader : Command successful.
Testing SCardListReaders : Command successful.
Reader 01: ACS ACR 38U-CCID
Enter the reader number : 1
Waiting for card insertion

Testing SCardConnect : Command successful.
Testing SCardStatus : Command successful.
Current Reader Name : ACS ACR 38U-CCID
Current Reader State : 0x54
Current Reader Protocol : 0x0
Current Reader ATR Size : 16 (0x10)
Current Reader ATR Value : 3B 9C 96 00 52 75 74 6F 6B 65 6E 45 43 50 73 63
Testing SCardDisconnect : Command successful.
Testing SCardReleaseContext : Command successful.
Testing SCardEstablishContext : Command successful.
Testing SCardGetStatusChange
Please insert a working reader : Command successful.
Testing SCardListReaders : Command successful.
Reader 01: ACS ACR 38U-CCID
Enter the reader number : 1
Waiting for card insertion

Testing SCardConnect : Command successful.
Testing SCardStatus : Command successful.
Current Reader Name : ACS ACR 38U-CCID
Current Reader State : 0x54
Current Reader Protocol : 0x0
Current Reader ATR Size : 16 (0x10)
Current Reader ATR Value : 3B 9C 96 00 52 75 74 6F 6B 65 6E 45 43 50 73 63
Testing SCardDisconnect : Command successful.
Testing SCardReleaseContext : Command successful.

PC/SC Test Completed Successfully !
```

Значит смарт-карта работает.

10. Если отобразилось сообщение:

```
admin — pcsctest — 80x11

Last login: Mon Dec 25 16:04:48 on ttys000
MBP- ~ admin$ pcsctest

MUSCLE PC/SC Lite Test Program

Testing SCardEstablishContext : Command successful.
Testing SCardGetStatusChange
Please insert a working reader :
```

Значит Рутокен ЭЦП не работает. Для решения данной проблемы перейдите в раздел [Решение проблем с Рутокен ЭЦП в системе](#).

Проверка наличия RSA сертификатов и ключевых пар RSA на Рутокен ЭЦП

Процесс проверки наличия RSA сертификатов изменился в операционной системе с версии 10.15.

В первом подразделе описан текущий процесс проверки, а во втором — тот, что был раньше.

Начиная с версии 10.15

Перед проверкой наличия RSA сертификатов с ключевыми парами на Рутокен ЭЦП загрузите и установите на компьютер специальное приложение для работы с RSA-сертификатами.

Для того чтобы загрузить это приложение перейдите по указанной ссылке:

<https://www.rutoken.ru/support/download/drivers-for-mac/>

↓ **Рутокен для macOS**

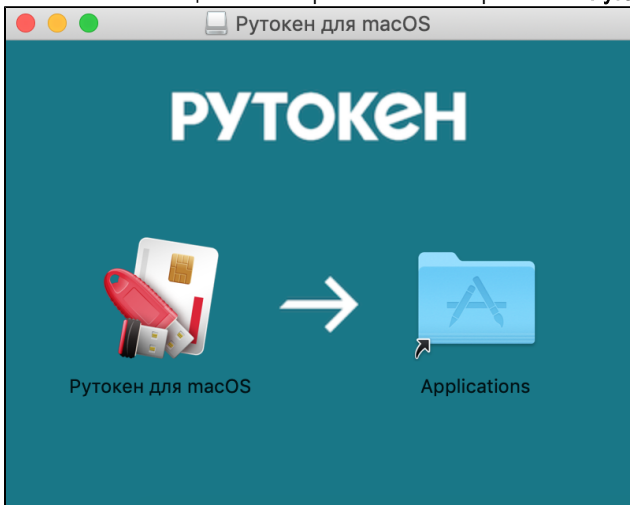
Версия:

Поддерживаемые ОС:

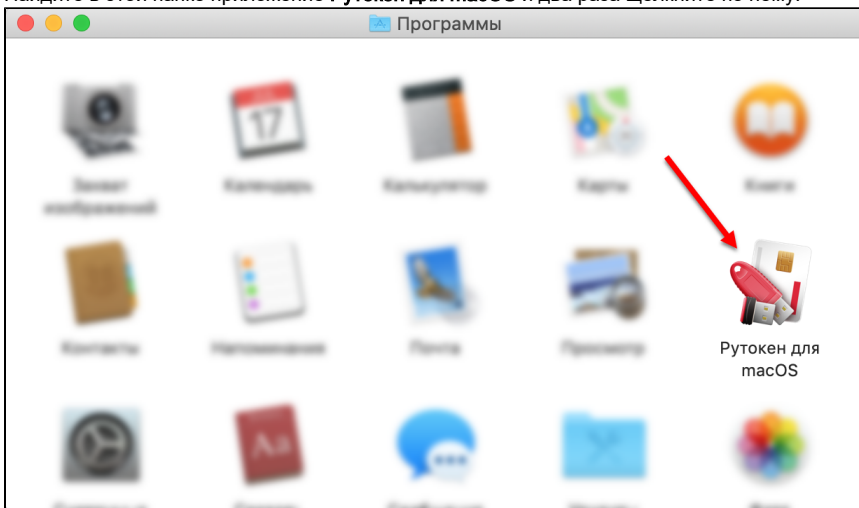
Специальное приложение для работы RSA-сертификатов на устройствах семейства Рутокен ЭЦП с использованием инструментов macOS.

Для установки приложения:

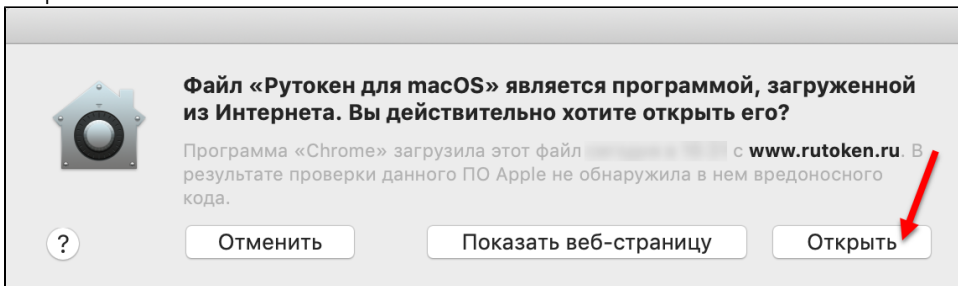
1. Запустите программу установки. На экране отобразится окно **Рутокен для macOS**.
2. В этом окне с помощью мыши перенесите значок приложения **Рутокен для macOS** в папку **Applications**.

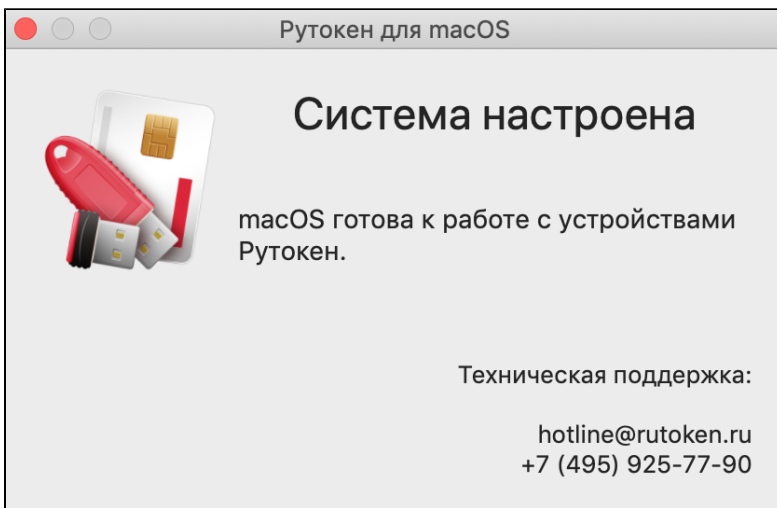


3. В окне **Рутокен для macOS** два раза щелкните по папке **Applications**. Откроется папка **Программы**.
4. Найдите в этой папке приложение **Рутокен для macOS** и два раза щелкните по нему.



5. Чтобы подтвердить открытие приложения, нажмите **Открыть**. В результате на экране отобразится уведомление о том, что система настроена.





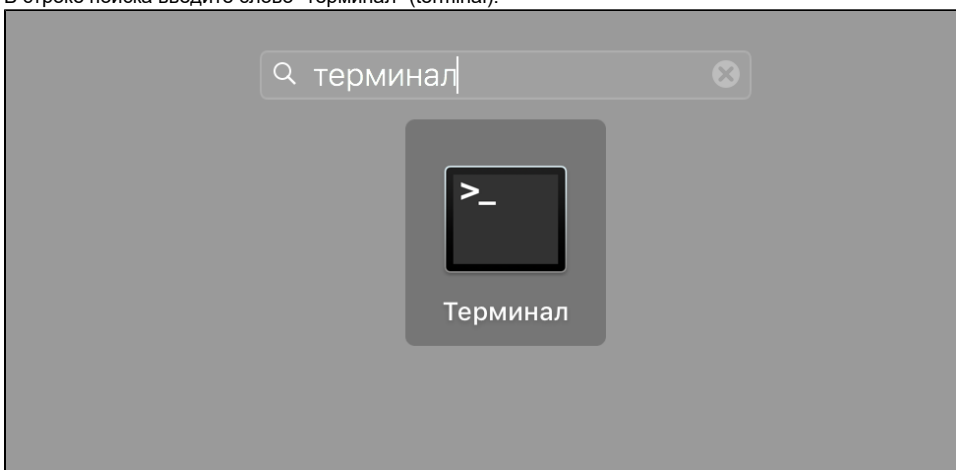
6. Закройте окно с этим уведомлением и окно Рутокен для macOS.

Для проверки наличия RSA сертификатов с ключевыми парами RSA на Рутокен ЭЦП:

1. Подключите устройство к компьютеру.
2. Откройте программу **Launchpad**.



3. В строке поиска введите слово "терминал" (terminal).



4. Откройте **Терминал (Terminal)**.



5. Введите команду:

```
sc_auth identities
```

В результате в окне Терминала отобразится информация обо всех RSA-сертификатах с ключевыми парами RSA, хранящихся на устройстве Рутокен ЭЦП.

```
user — -bash — 80x24
Last login: Mon Nov 18 17:34:14 on ttys000
android-93312e4947dbd71c:~ user$ sc_auth identities
objc[1245]: Class TKTokenRefImpl is implemented in both /System/Library/Frameworks/Security.framework/Versions/A/Security (0x7fff8afc0098) and /System/Library/Frameworks/CryptoTokenKit.framework/ctkbind.bundle/Contents/MacOS/ctkbind (0x10ec3cd40). One of the two will be used. Which one is undefined.
objc[1245]: Class TKTokenRefCtkd is implemented in both /System/Library/Frameworks/Security.framework/Versions/A/Security (0x7fff8afc00c0) and /System/Library/Frameworks/CryptoTokenKit.framework/ctkbind.bundle/Contents/MacOS/ctkbind (0x10ec3cd68). One of the two will be used. Which one is undefined.
SmartCard: ru.rutoken.RutokenApp.Rutoken:Евгений Белов(864778457)
Unpaired identities:
D4E2D7E06C852703361B81E7991095194482CEBC      Евгений Белов, Users
android-93312e4947dbd71c:~ user$
```

До версии 10.15

Перед запуском процесса проверки наличия RSA сертификатов и ключевых пар RSA на РутOKEN ЭЦП загрузите и установите на компьютер модуль поддержки Связка Ключей (KeyChain).

Для того чтобы загрузить данный модуль поддержки перейдите по указанной ссылке и выберите необходимую версию модуля:

<https://www.rutoken.ru/support/download/drivers-for-mac/>

 **Модуль поддержки Связки Ключей (KeyChain)**

Версия: 

Поддерживаемые ОС: macOS 10.14/10.13/10.12/10.11/10.10/10.9

Модуль поддержки Связки Ключей добавляет поддержку РутOKEN ЭЦП при работе с сертификатами RSA. Сертификаты и ключи ГОСТ, хранящиеся на РутOKEN ЭЦП в Связке Ключей (KeyChain), видны не будут.

Для установки модуля поддержки Связки Ключей (KeyChain) запустите программу установки модуля и следуйте инструкциям, отображающимся на экране.

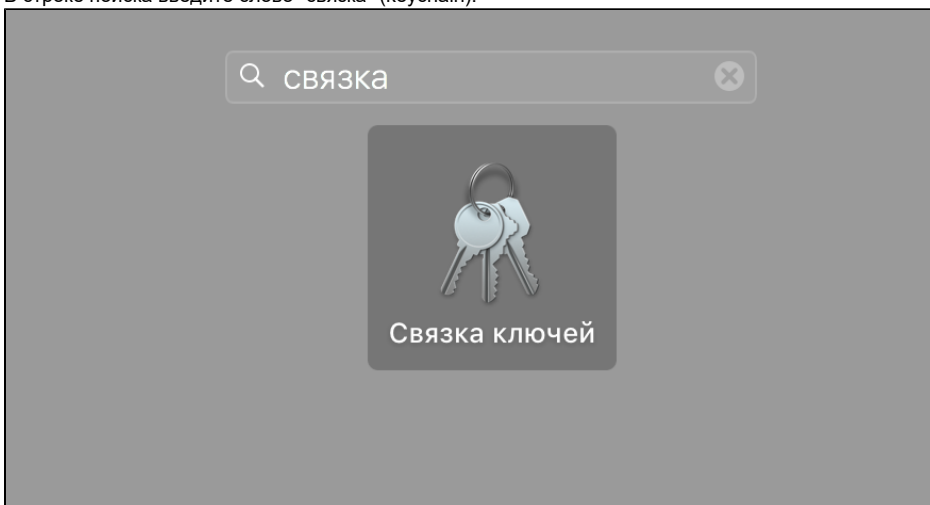
После установки модуля перезагрузите систему.

Для проверки наличия RSA сертификатов и ключевых пар RSA на РутOKEN ЭЦП:

1. Подключите устройство к компьютеру.
2. Откройте программу **Launchpad**.



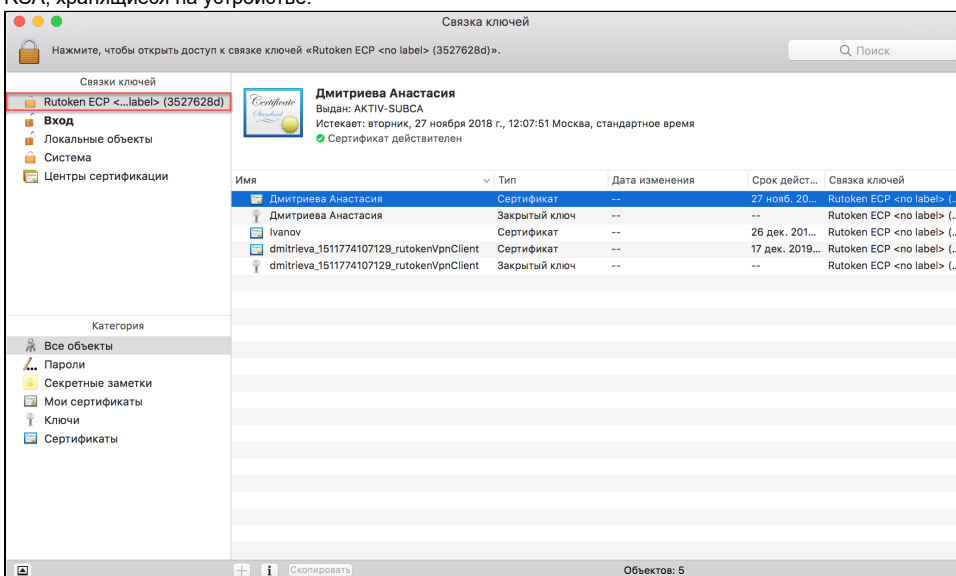
3. В строке поиска введите слово "связка" (keychain).



4. Откройте программу **Связка ключей (Keychain Access)**.

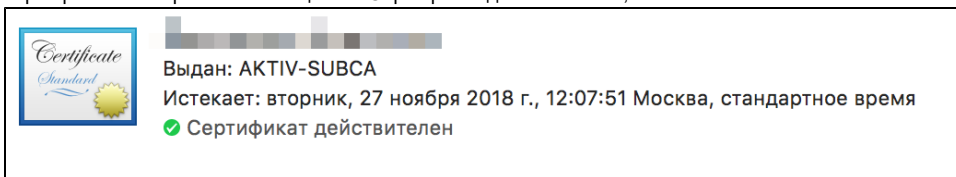


5. В боковой панели окна программы выберите название устройства. В окне программы отобразятся RSA сертификаты и ключевые пары RSA, хранящиеся на устройстве.

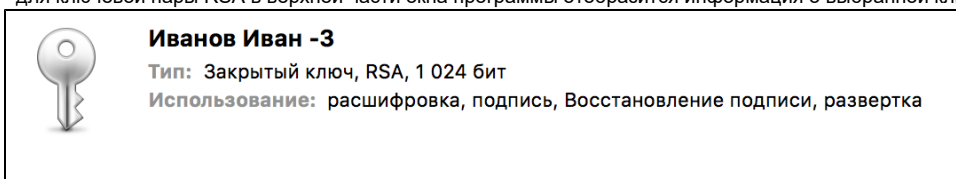


6. Щелкните левой кнопкой мыши в строке с необходимым RSA сертификатом или ключевой парой RSA.

- для RSA сертификата в верхней части окна программы отобразится информация о выбранном сертификате. У действительного сертификата отобразится сообщение "Сертификат действителен";



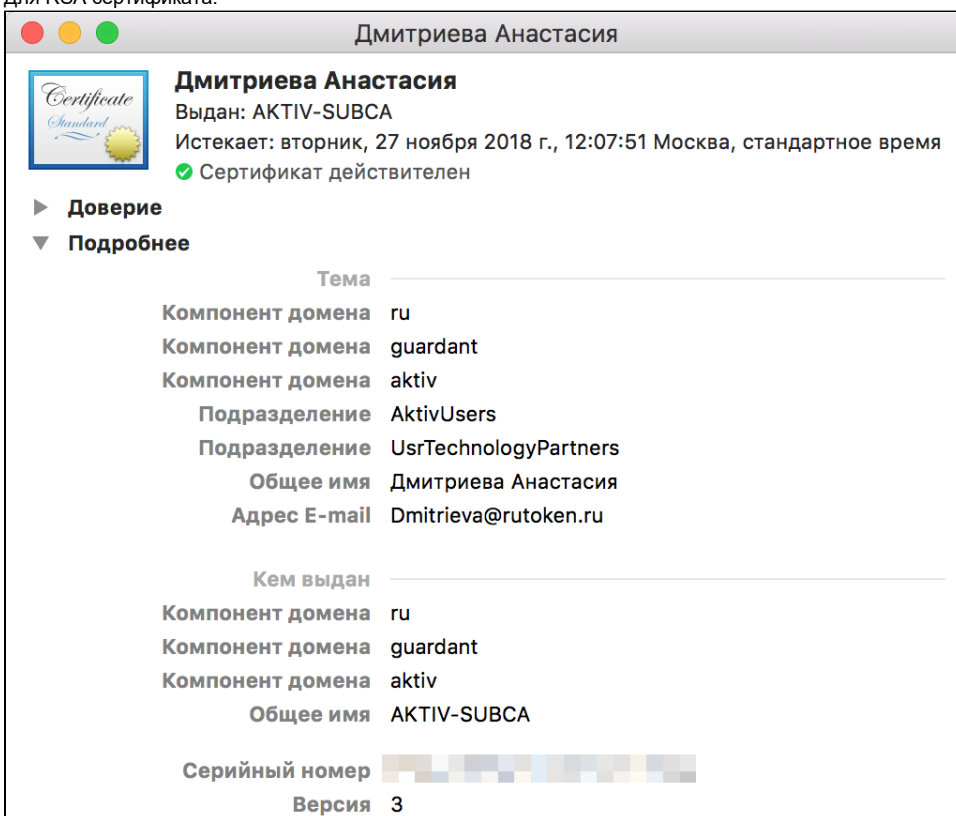
- для ключевой пары RSA в верхней части окна программы отобразится информация о выбранной ключевой паре.



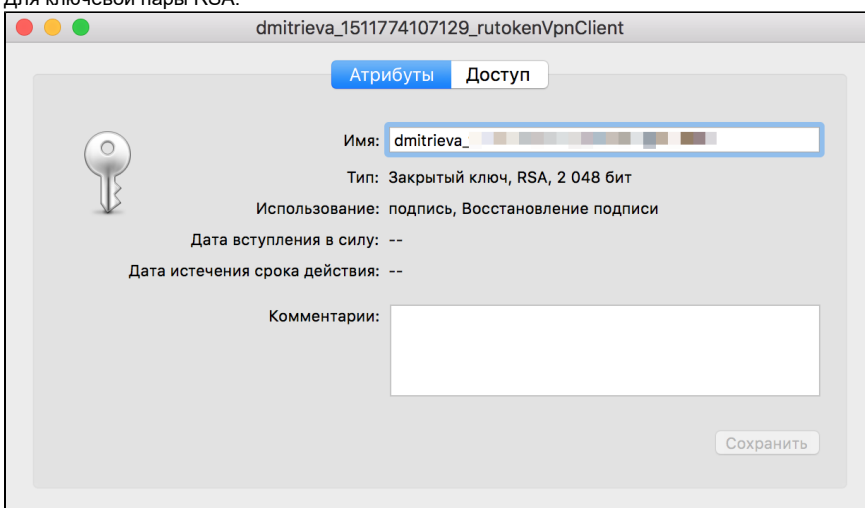
Чтобы открыть RSA сертификат или ключевую пару RSA щелкните два раза по строке с именем необходимого объекта. В результате

откроется окно с полной информацией о нем.

Для RSA сертификата:



Для ключевой пары RSA:



Если для Рутокен ЭЦП вы используете стандартный PIN-код (12345678), то следует его изменить на более сложный.

Проверка наличия ГОСТ сертификатов и ключевых пар ГОСТ на Рутокен ЭЦП

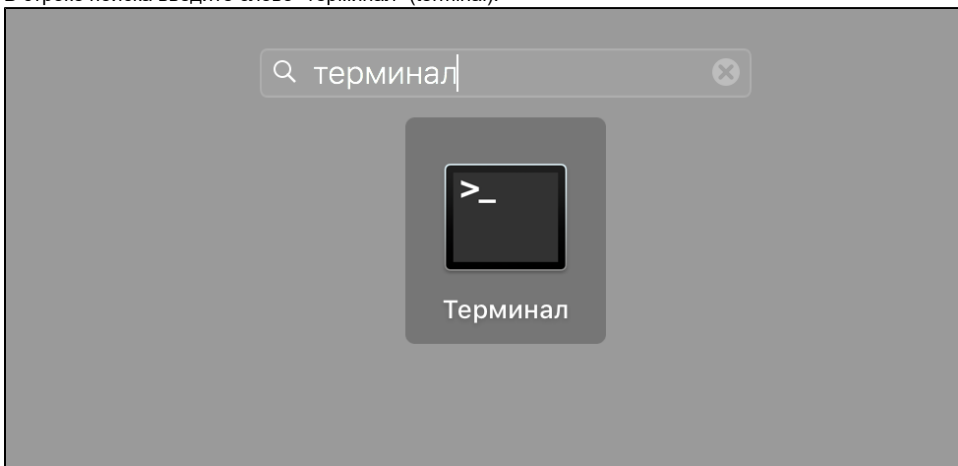
Для проверки наличия ГОСТ сертификатов и ключевых пар ГОСТ на Рутокен ЭЦП:

1. Подключите устройство к компьютеру.

2. Откройте программу **Launchpad**.



3. В строке поиска введите слово "терминал" (terminal).



4. Откройте **Терминал (Terminal)**.

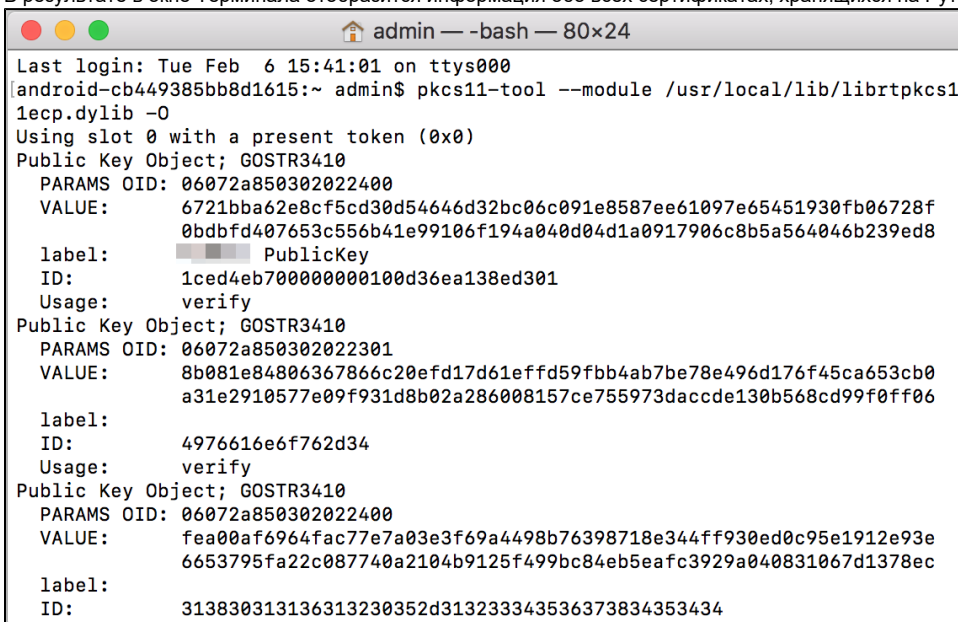


5. Введите команду:

```
pkcs11-tool --module {A} -0
```

A — путь до библиотеки librtpkcs11esp.dylib.

В результате в окне Терминала отобразится информация обо всех сертификатах, хранящихся на Рутокен ЭЦП.



Чтобы открыть сертификат или ключевую пару скопируйте ID необходимого объекта и введите команду:

```
pkcs11-tool --module {A} -r -y cert --id {B} | openssl x509 -inform der -text
```

A — путь до библиотеки libtpkcs11esp.dylib.

B — ID сертификата.

В результате в окне Терминала отобразится полная информация об указанном объекте.



Чтобы скопировать сертификат в файл введите команду:

```
pkcs11-tool --module {A} -r -y cert --id {B} > ./{C}
```

A — путь до библиотеки libtpkcs11esp.dylib.

B — ID сертификата.

C — имя файла.

Изменение PIN-кода РутOKEN ЭЦП

Перед запуском процесса смены PIN-кода устройства:

- загрузите и установите пакет OpenSC;
- загрузите и установите библиотеку PKCS#11;
- определите путь до библиотеки libtpkcs11esp.dylib.

Для того чтобы загрузить установочный пакет OpenSC перейдите по указанной ссылке и выберите необходимую версию:

Download

OpenSC 0.22.0 is the latest stable version released on 10.08.2021. It is available as

- Windows installer
 - [OpenSC-0.22.0_win64.msi](#) for 64 bit programs
 - [OpenSC-0.22.0_win32.msi](#) for 32 bit programs
- [OpenSC-0.22.0.dmg](#): macOS installer
- [opensc-0.22.0.tar.gz](#): Source code distribution

Для установки пакета OpenSC запустите программу установки пакета и следуйте инструкциям, отображающимся на экране.

Для того чтобы загрузить библиотеку PKCS#11 перейдите по указанной ссылке и выберите необходимую версию:

<https://www.rutoken.ru/support/download/pkcs/>

Пользователям macOS

↓ Установщик библиотеки **rtPKCS11esp** для macOS

Версия:

Поддерживаемые ОС: Apple macOS 12/11/10.15/10.14/10.13/10.12/10.11/10.10/10.9

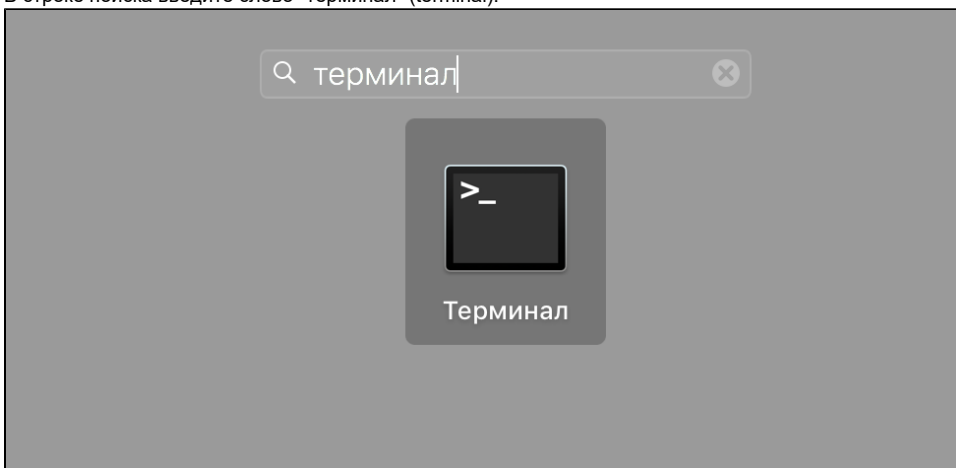
Для установки библиотеки PKCS#11 запустите программу установки библиотеки и следуйте инструкциям, отображающимся на экране.

Для того чтобы определить путь до библиотеки `librtpkcs11esp.dylib`:

1. Откройте программу **Launchpad**.



2. В строке поиска введите слово "терминал" (terminal).



3. Откройте **Терминал** (Terminal).



4. Введите команду:

```
sudo find /usr -name librtpkcs11ecp.dylib
```

5. Нажмите **Enter**. В результате в окне Терминала отобразится путь до библиотеки librtpkcs11ecp.dylib.

```
android-cb449385bb8d1615:~ admin$ sudo find /usr -name librtpkcs11ecp.dylib
Password:
/usr/local/lib/pkcs11/librtpkcs11ecp.dylib
/usr/local/lib/librtpkcs11ecp.dylib
```

Для изменения PIN-кода введите команду:

```
pkcs11-tool --module {A} --login --pin {B} --change-pin --new-pin {C}
```

A — путь до библиотеки librtpkcs11ecp.dylib.

B — текущий PIN-код устройства.

C — новый PIN-код устройства.

```
android-cb449385bb8d1615:~ admin$ pkcs11-tool --module /usr/local/lib/librtpkcs11ecp.dylib --login --pin 12345678 --change-pin --new-pin 123456
Using slot 0 with a present token (0x0)
PIN successfully changed
```

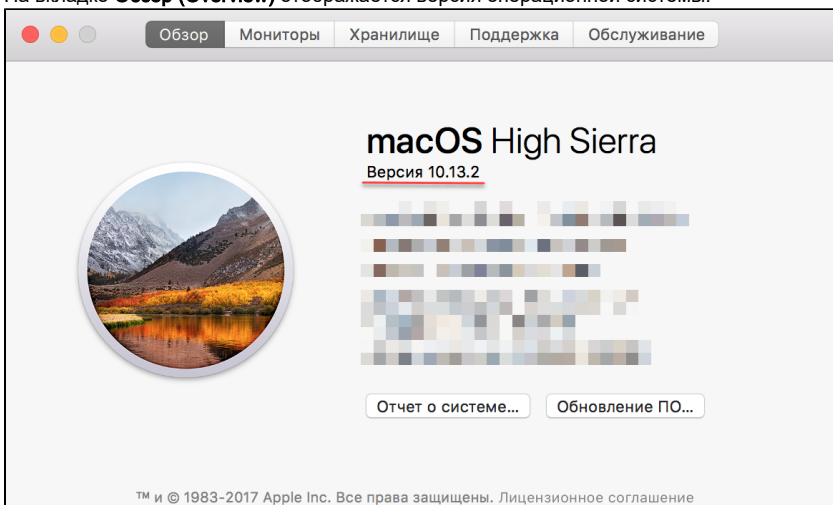
В результате PIN-код устройства будет изменен.

Решение проблем с Рутокен ЭЦП в системе

Для начала определите версию операционной системы, которую вы используете. Для этого:

1. Выберите в меню «Apple» () пункт «Об этом Mac» (About This Mac).

2. На вкладке **Обзор (Overview)** отображается версия операционной системы.



Если вы используете версию 10.7 и выше, то устройство семейства РутOKEN ЭЦП должно определяться системой автоматически. В таком случае проверьте корректно ли подключено устройство к компьютеру и снова повторите процедуру [Проверка работы РутOKEN ЭЦП в системе](#).

Если вы используете версию ниже чем 10.7, то необходимо изменить конфигурационный файл и перезагрузить систему.

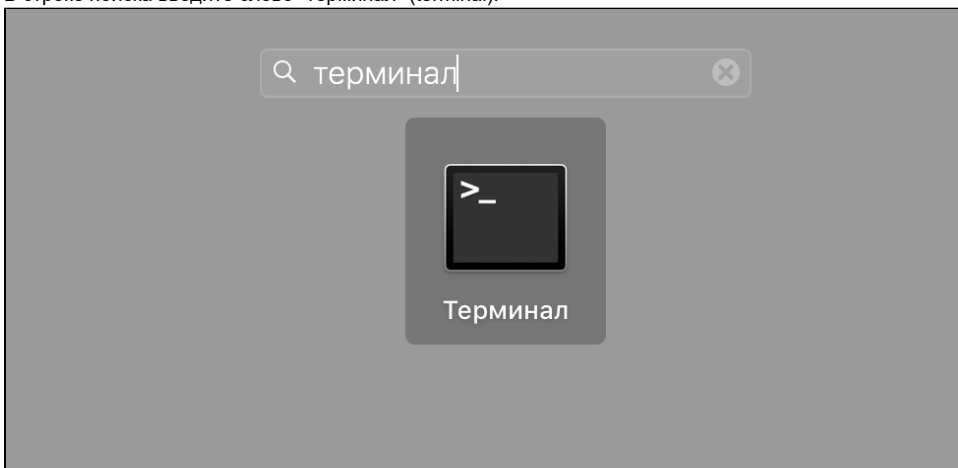
Будьте очень внимательны при работе с конфигурационным файлом info.plist

Для изменения конфигурационного файла:

1. Откройте программу **Launchpad**.



2. В строке поиска введите слово "терминал" (terminal).



3. Откройте **Терминал (Terminal)**.

4. Откройте конфигурационный файл. Для этого введите команду:

```
sudo nano /usr/libexec/SmartCardServices/drivers/ifd-ccid.bundle  
/Contents/Info.plist
```

5. В конфигурационный файл добавьте следующие строки:

- a. в массив <key>ifdVendorID</key> строку <string>0x0A89</string>;
 - b. в массив <key>ifdProductID</key> строку <string>0x0030</string>.
 - c. в массив <key>ifdFriendlyName</key> строку <string>Aktiv Rutoken ECP</string>.
6. Перезагрузите систему.

После этого снова проверьте работу устройства в системе, а именно повторите процедуру [Проверка работы РутOKEN ЭЦП в системе](#).