

Средство криптографической защиты информации «Рутокен ЭЦП 2.0»

Руководство пользователя

Версия 1.2

Содержание

Предисловие	3
Общие сведения	4
Подготовка «Рутокен ЭЦП» к работе	7
Настройка для Windows	7
Настройка для Linux и macOS	9
Проверка работоспособности	13
Работа с «Рутокен ЭЦП» в системе «iBank для Бизнеса»	16
Эксплуатация и хранение	16
Использование при регистрации в системе	16
Использование при входе в систему	18
Администрирование ключей ЭП	20
Администрирование «Рутокен ЭЦП»	23
Обновление драйверов «Рутокен ЭЦП» для Windows	29
Устранение неисправностей	31
USB-токен недоступен	31
BIFIT Signer не определяет USB-токен	34
Ошибка в ходе установки библиотеки rtPKCS11ECP	36
Нестабильная работа USB-токена	37

Предисловие

Настоящий документ является руководством по использованию в системе электронного банкинга «iBank для Бизнеса» средств криптографической защиты информации:

- «Рутокен ЭЦП 2.0»;
- «Рутокен ЭЦП 2.0 2100»;
- «Рутокен ЭЦП 2.0 3000».

«Рутокен ЭЦП» — это линейка устройств для практически любых приложений электронной подписи и строгой двухфакторной аутентификации.

Это полнофункциональные СКЗИ и средства электронной подписи с аппаратной реализацией ГОСТ Р 34.10-2012 с длиной ключа 256/512 бит и ГОСТ Р 34.11-2012. Операции выполняются без извлечения ключа в память компьютера. Срок действия неизвлекаемых ключей электронной подписи — до 3 лет.

Работа с «Рутокен ЭЦП» поддерживается в ОС Windows, Linux и macOS.

В разделе [Общие сведения](#) рассмотрено назначение «Рутокен ЭЦП» и представлена информация о его совместимости с различными операционными системами.

В разделе [Подготовка «Рутокен ЭЦП» к работе](#) представлена информация о действиях необходимых для обеспечения корректной работы устройства.

В разделе [Требования к эксплуатации](#) описаны меры по обеспечению сохранности и надежности устройства.

В разделе [Обновление драйверов «Рутокен ЭЦП» для Windows](#) описан порядок обновления драйверов устройства для Windows.

В разделе [Устранение неисправностей](#) описаны типовые неисправности, которые могут возникнуть при эксплуатации «Рутокен ЭЦП», и способы их устранения.

Применение «Рутокен ЭЦП» при работе с системой «iBank для Бизнеса» рассмотрено в разделах:

- [Использование «Рутокен ЭЦП» при регистрации в системе «iBank для Бизнеса»;](#)
- [Использование «Рутокен ЭЦП» при входе в систему «iBank для Бизнеса»;](#)
- [Администрирование ключей ЭП;](#)
- [Администрирование «Рутокен ЭЦП».](#)

Общие сведения

«Рутокен ЭЦП» представляет собой компактное USB-устройство с аппаратной реализацией российских стандартов электронной подписи (ЭП), шифрования и хеширования.



Рис. 1. Рутокен ЭЦП

«Рутокен ЭЦП» предназначен для безопасной двухфакторной аутентификации пользователей, генерации и защищенного хранения ключей шифрования и ключей электронной подписи, выполнения шифрования и электронной подписи в самом устройстве, хранения цифровых сертификатов и иных данных.

«Рутокен ЭЦП 2.0», «Рутокен ЭЦП 2.0 2100» и «Рутокен ЭЦП 2.0 3000» поддерживают:

- Интерфейс USB 1.1 и выше;
- USB CCID: работа без установки драйверов устройства в современных версиях ОС.

Аппаратная реализация криптографических алгоритмов (электронной подписи, хеш-функции и шифрования) внутри устройства обеспечивает:

- конфиденциальность обрабатываемой информации при передаче и хранении;
- целостность обрабатываемой информации;
- подтверждение авторства посредством электронной подписи.

Формирование ЭП в соответствии с ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012 происходит непосредственно внутри устройства: на вход «Рутокен ЭЦП» принимает электронный документ, на выходе выдает ЭП под данным документом.

Ключ ЭП генерируется самим «Рутокен ЭЦП», хранится в защищенной памяти «Рутокен ЭЦП» и никогда, никем и ни при каких условиях не может быть считан из «Рутокен ЭЦП».

«Рутокен ЭЦП» имеет защищенную область памяти, позволяющую хранить до 84-и ключей ЭП ответственных сотрудников одного или нескольких клиентов.

Поддержка устройств в системе «iBank для Бизнеса» обеспечена:

- «Рутокен ЭЦП 2.0» начиная с версии 2.0.24 №96;
- «Рутокен ЭЦП 2.0 2100» начиная с версии 2019.8;
- «Рутокен ЭЦП 2.0 3000» начиная с версии 2021.7.

Использование «Рутокен ЭЦП» возможно в следующих АРМ корпоративных клиентов системы «iBank для Бизнеса»:

- Интернет-Банк;
- ЦФК;
- Офлайн-Банк;
- Автоклиент.

Возможна одновременная работа сразу с несколькими подключенными к компьютеру устройствами (актуально при работе с ЦФК).

Для работы в АРМах системы «iBank для Бизнеса» с ключами ЭП, находящимся в памяти «Рутокен ЭЦП», необходим BIFIT Signer. Его установка и дистрибутив для скачивания предлагаются при обращении к АРМ.

Для использования «Рутокен ЭЦП 2.0 3000» необходим BIFIT Signer версии 8.18 и выше. Использование «Рутокен ЭЦП 2.0 3000» в ОС Windows XP не предусмотрено в связи с прекращением поддержки BIFIT Signer выше версии 8.15 в ОС Windows XP.

«Рутокен ЭЦП» обеспечивает двухфакторную аутентификацию в компьютерных системах. Для успешной аутентификации требуется выполнение двух условий: знания пользователем PIN-кода и физическое наличие самого устройства. Это обеспечивает гораздо более высокий уровень безопасности по сравнению с традиционным доступом только по паролю.

В «Рутокен ЭЦП» реализованы следующие криптографические алгоритмы:

- Поддержка ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012: генерация ключевых пар с проверкой качества, импорт ключевых пар, формирование и проверка электронной подписи. Срок действия закрытых ключей до 3-х лет.
- Поддержка ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012: вычисление значения хэш-функции данных, в том числе с возможностью последующего формирования ЭП.
- Поддержка ГОСТ Р 28147-89: генерация и импорт ключей шифрования, шифрование данных в режимах простой замены, гаммирования и гаммирования с обратной связью, вычисление и проверка криптографической контрольной суммы данных (имитовставки ГОСТ).
- Выработка сессионных ключей (ключей парной связи): по схеме VKO GOST R 34.10-2001 (RFC 4357) и VKO GOST R 34.10-2012 (RFC 7836), расшифрование по схеме EC El-Gamal.
- Поддержка RSA: поддержка ключей размером до 2048 бит, генерация ключевых пар с настраиваемой проверкой качества, импорт ключевых пар, формирование электронной подписи.
- Генерация последовательности случайных чисел требуемой длины.

Основу «Рутокен ЭЦП» составляет современный защищенный микроконтроллер и встроенная защищенная память, в которой безопасно хранятся данные пользователя: пароли, ключи шифрования и подписи, сертификаты и т.д.

Все модели «Рутокен ЭЦП» имеют сертификаты соответствия ФСБ РФ:

- № СФ/124-3673 от 10.04.19г. – действителен до 10.04.2022 г.
- № СФ/124-4077 от 17.06.21г. – действителен до 01.06.2024 г.
- № СФ/124-3994 от 11.12.20г. – действителен до 11.12.23 г.

Примечание:

В системе «iBank для Бизнеса» поддерживается работа USB-токенов «Рутокен ЭЦП» в специальной конфигурации, предназначенной для использования исключительно в системе «iBank для Бизнеса».

Компания «БИФИТ» согласовала данную конфигурацию с производителем USB-токенов «Рутокен ЭЦП» АО «Актив-софт», встроила поддержку конфигурации в систему «iBank для Бизнеса», протестировала систему «iBank для Бизнеса» на предмет совместимости с USB-токенами «Рутокен ЭЦП» в данной конфигурации и осуществляет поддержку в системе «iBank для Бизнеса» USB-токенов «Рутокен ЭЦП» только в специальной конфигурации.

В настоящее время в системе «iBank для Бизнеса» реализована поддержка USB-токенов «Рутокен ЭЦП» со специальной конфигурацией, приобретенных через авторизованных поставщиков ООО «БИФИТ Дата Секьюрити» и/или ООО «БИФИТ ЭДО» с ограничением области применения данных USB-токенов только в составе системы «iBank для Бизнеса».

Использование USB-токенов «Рутокен ЭЦП» с иными конфигурациями и/или приобретенных через не авторизованных поставщиков невозможно ввиду отсутствия поддержки работы таких устройств в системе «iBank для Бизнеса».

Подготовка «Рутокен ЭЦП» к работе

Настройка для Windows

Для полноценной работы «Рутокен ЭЦП 2.0», «Рутокен ЭЦП 2.0 2100» и «Рутокен ЭЦП 2.0 3000» необходимо установить драйвер и панель управления устройства, с помощью которой осуществляется:

- задание PIN-кода доступа к устройству;
- управление политиками качества PIN-кодов;
- форматирование устройства.

Внимание!

Перед началом установки драйверов рекомендуется отсоединить «Рутокен ЭЦП» от USB-порта компьютера.

Для установки драйвера необходимо загрузить установочный файл, запустить его и следовать указаниям мастера установки. После завершения процесса установки необходимо подключить «Рутокен ЭЦП» к свободному USB-порту.

Установочный файл можно получить с сайта разработчика «Рутокен ЭЦП» компании АО «Актив-софт»:

[Драйверы Рутокен для Windows](#)

Поддерживаемые ОС: 32- и 64-разрядные Microsoft Windows 10/8.1/2012R2/8/2012/7/2008R2/Vista/2008

Запустите программу установки драйвера «Рутокен ЭЦП» и следуйте ее указаниям. Далее представлены основные этапы работы мастера установки (см. [рис. 2](#) – [рис. 4](#)). По умолчанию мастер установки предлагает создать ярлык для запуска панели управления на рабочем столе.

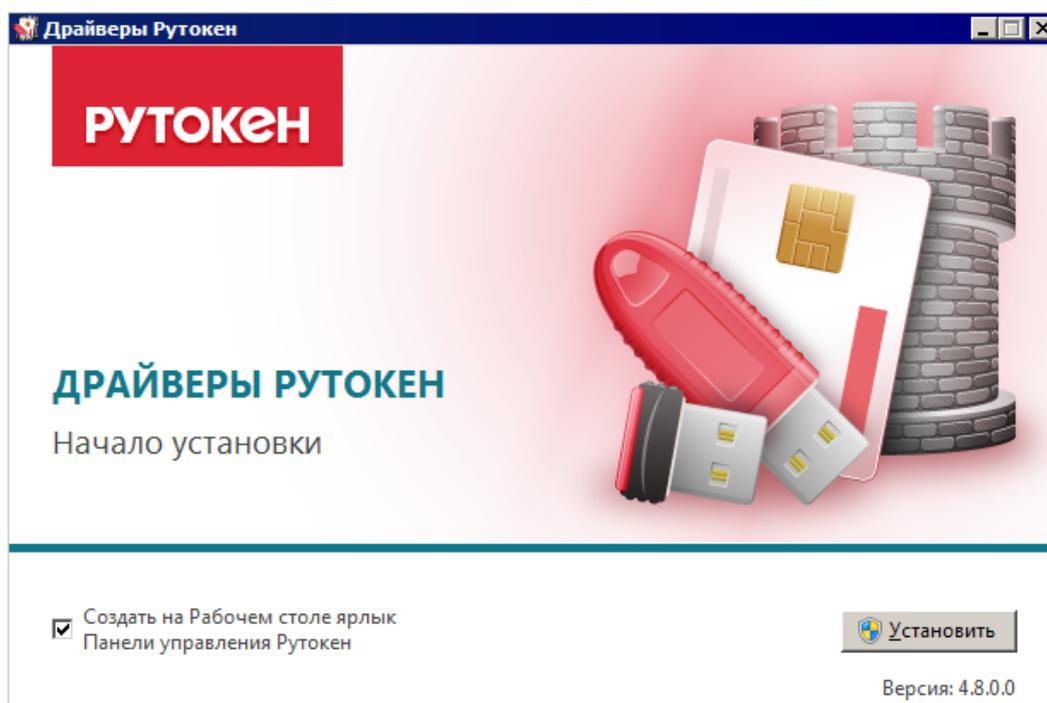


Рис. 2. Мастер установки драйвера

Для продолжения установки драйвера нажмите кнопку **Установить**. Начнется процесс установки драйвера и панели управления устройством (см. [рис. 2](#)).

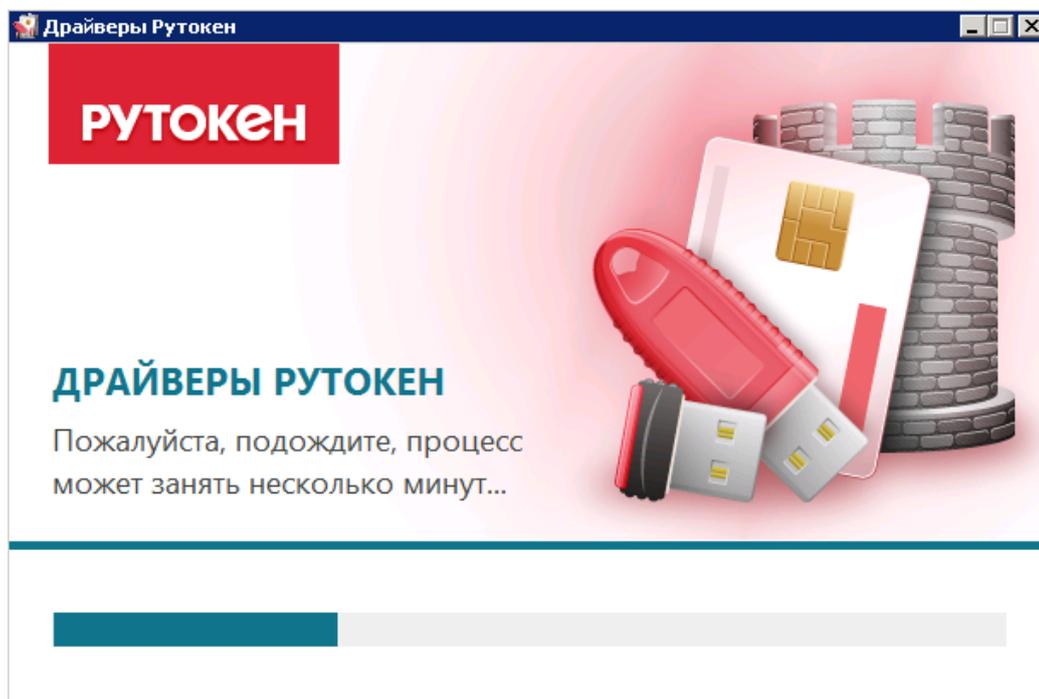


Рис. 3. Мастер установки драйвера

Далее необходимо дождаться окончания установки драйвера (см. [рис. 3](#)) и нажать кнопку **Зак-
рыть** (см. [рис. 4](#)).

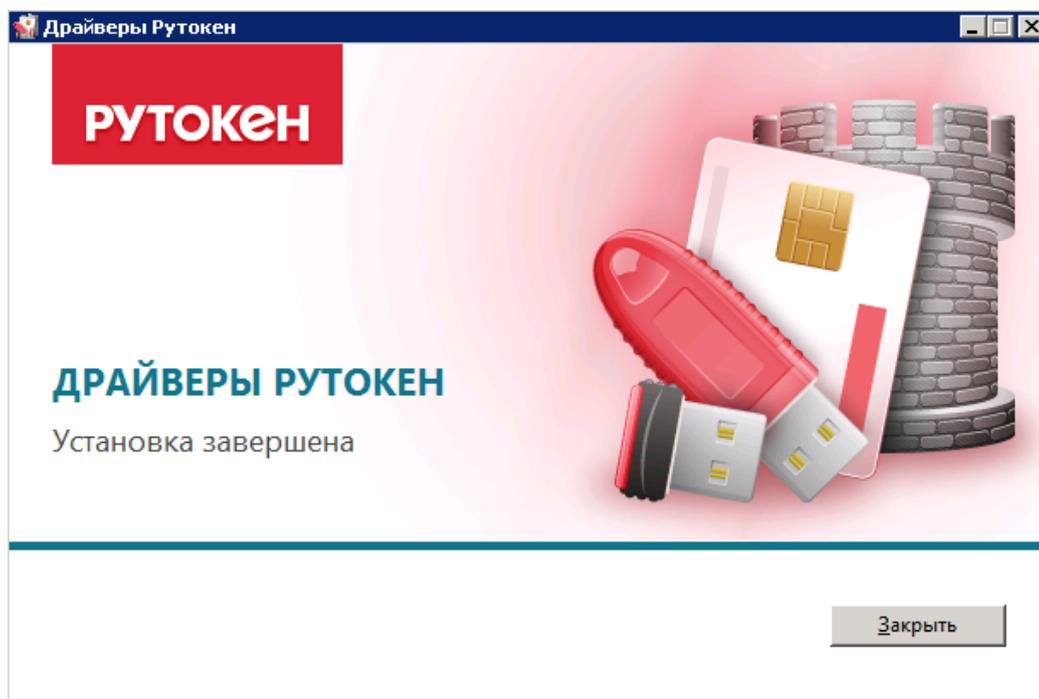


Рис. 4. Мастер установки драйвера

После окончания установки драйвера подключите «Рутокен ЭЦП» к USB-порту компьютера. В области уведомлений панели задач появится сообщение, свидетельствующее об обнаружении системой подключенного устройства и готовности его к использованию (см. [рис. 5](#)).

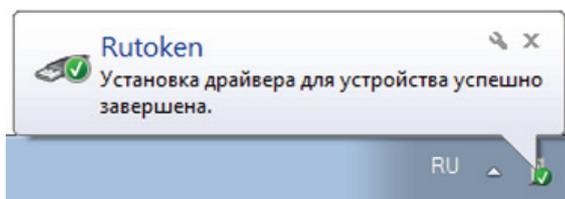


Рис. 5. Панель задач. Сообщение об успешной установке

Настройка для Linux и macOS

Установка драйвера для «Рутокен ЭЦП» в современных операционных системах GNU/Linux (версия libccid не ниже 1.4.2) и macOS (версия 10.7 и выше) не требуется.

«Рутокен ЭЦП» – это устройство поддерживающее стандарт CCID

В операционных системах GNU/Linux и macOS X за поддержку стандарта CCID в psc-lite отвечает модуль libccid

У libccid существует конфигурационный файл, содержащий описание идентификаторов устройств, которые проверены автором libccid на совместимость.

Внести запись о «Рутокен ЭЦП» в конфигурационный файл может потребоваться:

- пользователям устаревших дистрибутивов GNU/Linux;
- пользователям macOS 10.6 Snow Leopard и предыдущих версий.

В GNU/Linux конфигурационный файл обычно находится в `/usr/lib/pcsc/drivers/ifd-bundle/Contents/Info.plist`

В macOS X конфигурационный файл находится в `/usr/libexec/SmartCardServices/drivers/ifd-ccid.bundle/Contents/Info.plist`

Это обычный текстовый файл, который можно открыть любым доступным текстовым редактором и в который необходимо внести изменения:

- в массив `<key>ifdVendorID</key>` добавить `<string>0x0A89</string>` (см. рис. 6).

```
<key>ifdVendorID</key>
<array>
  <string>0x0A89</string>
  <string>0x08E6</string>
  <string>0x08E6</string>
  <string>0x08E6</string>
```

Рис. 6. Массив `<key>ifdVendorID</key>`

- в массив `<key>ifdProductID</key>` добавить `<string>0x0030</string>` (см. рис. 7).

```
<key>ifdProductID</key>
<array>
  <string>0x0030</string>
  <string>0x2202</string>
  <string>0x3437</string>
  <string>0x3438</string>
```

Рис. 7. Массив `<key>ifdProductID</key>`

– в массив `<key>ifdFriendlyName</key>` добавить `<string>Aktiv Rutoken ECP</string>` (см. [рис. 8](#)).

```
<key>ifdFriendlyName</key>
<array>
  <string>Aktiv Rutoken ECP</string>
  <string>Gemalto Gem e-Seal Pro</string>
```

Рис. 8. Массив `<key>ifdFriendlyName</key>`

Установка библиотеки `rtPKCS11ECP` на macOS X

Для работы «Рутокен ЭЦП» в системе «iBank для Бизнеса» на macOS X необходимо установить кроссплатформенную библиотеку `rtPKCS11ECP`, работающую с RSA и ГОСТ-алгоритмами.

Для установки библиотеки скачайте установочный файл с сайта разработчика «Рутокен ЭЦП» компании АО «Актив-софт»: [Установщик библиотеки `rtPKCS11ECP` для macOS X](#).

Запустите инсталлятор библиотеки. На экране отобразится стартовое окно инсталлятора (см. [рис. 9](#)).

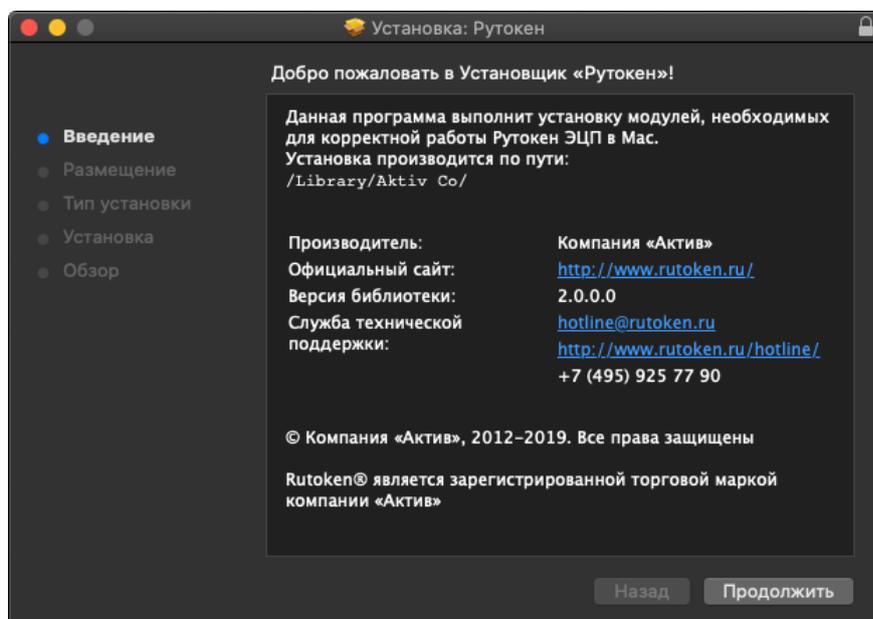


Рис. 9. Установка Рутокен. Введение

Для продолжения и перехода к шагу выбора места установки библиотеки (см. [рис. 10](#)) нажмите кнопку **Продолжить**.

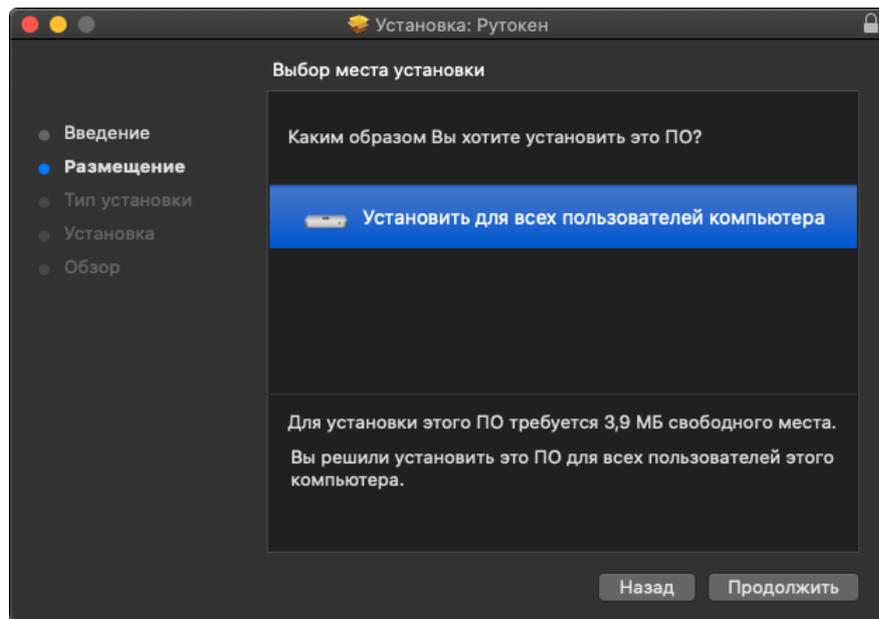


Рис. 10. Установка Рутокен. Размещение

Для определения списка пользователей, для которых необходимо установить библиотеку, нажмите на соответствующую строку окна.

Для продолжения и перехода к шагу выбора типа установки драйвера (см. [рис. 11](#)) нажмите кнопку **Продолжить**.

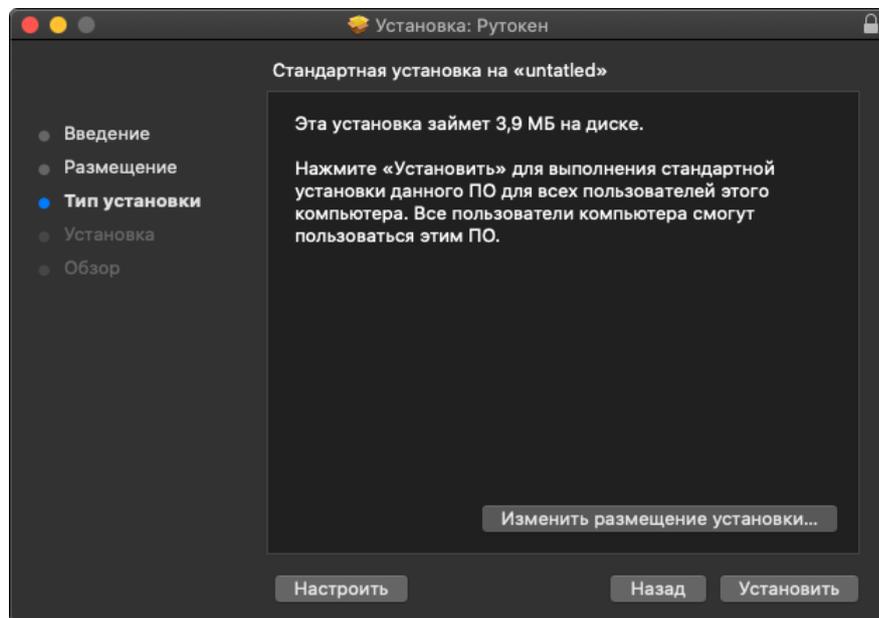


Рис. 11. Установка Рутокен. Тип установки

Для изменения параметров установки нажмите кнопку **Настройка** (см. [рис. 12](#)).

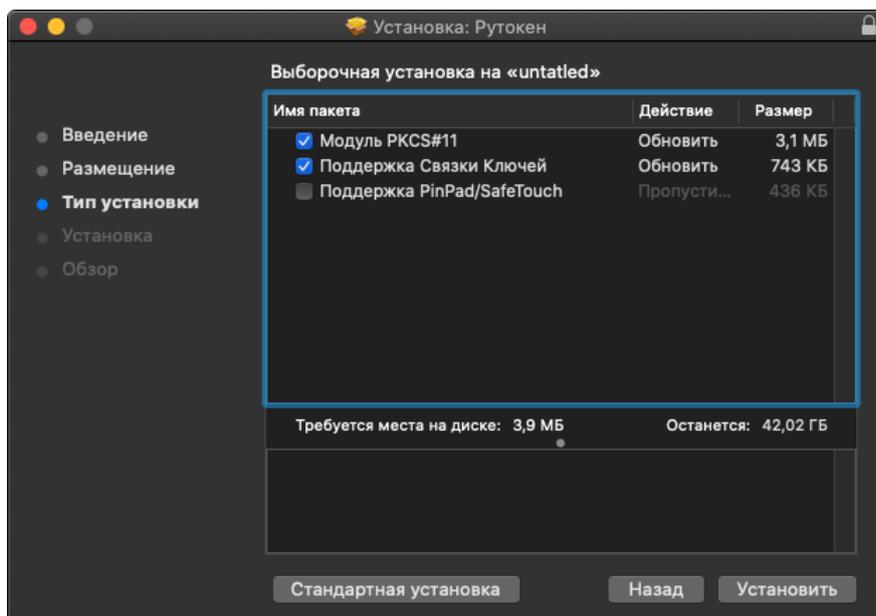


Рис. 12. Установка Рутокен. Настройка

Установите библиотеку `rtPKCS11ECP`. Для этого отметьте компонент **Модуль PKCS#11** и нажмите кнопку **Установить**.

На экране отобразится информация о ходе процесса установки (см. [рис. 13](#)), после завершения которой необходимо перезагрузить компьютер для обновления системных файлов. Для этого нажмите кнопку **Перезагрузить** (см. [рис. 14](#)).

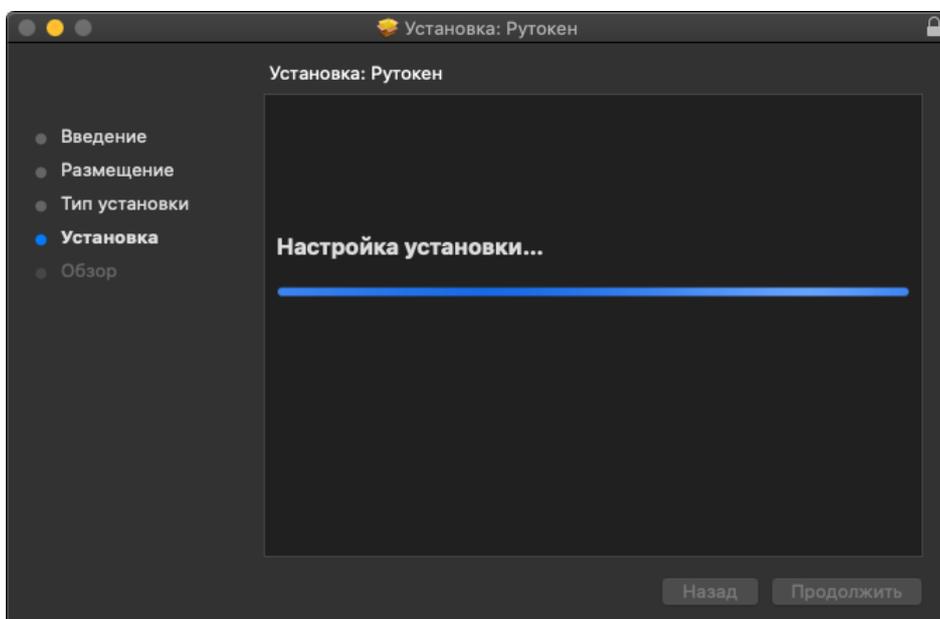


Рис. 13. Установка Рутокен. Установка

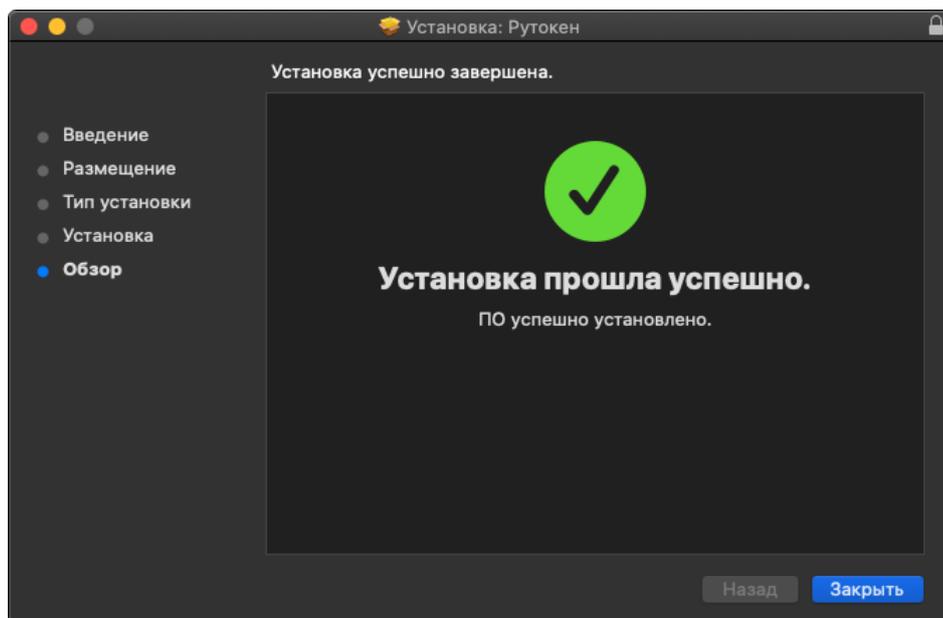


Рис. 14. Установка Рутокен. Обзор

Для корректной работы «Рутокен ЭЦП» в Офлайн-Банке необходимо установить библиотеку `rtPKCS11ECP` вручную. Для этого:

1. Получите библиотеку с сайта разработчика «Рутокен ЭЦП» компании АО «Актив-софт»: [Библиотека `rtPKCS11ECP` для macOS X](#).
2. Поместите файл `librtpkcs11ecp.dylib` в каталог `/Users/bifit/Library/Java/Extensions/` (если его нет, необходимо создать каталог `/Java/Extensions/`).

Проверка работоспособности

Проверка работоспособности «Рутокен ЭЦП» в ОС Windows

1. Подключите «Рутокен ЭЦП» к компьютеру и запустите **Панель управления Рутокен**.
2. На вкладке **Администрирование** в раскрывающемся списке **Подключенные Рутокен** должно отображаться название подключенного «Рутокен ЭЦП».
3. Если название устройства отобразилось, значит оно работает корректно.

Если название устройства не отображается, то попробуйте подключить его еще раз.

Проверка работоспособности «Рутокен ЭЦП» в ОС GNU/Linux

1. Установите утилиту `pcsc_scan` (обычно содержится в пакете `pcsc-tools`) и запустите её. Если утилита выдает длинный лог, в котором есть упоминание нужного устройства, значит оно работает корректно (см. [рис. 15](#)).

```
ubuser@ubuntu:~$ sudo pcsd -afddddd
[sudo] password for ubuser:
00000000 debuglog.c:277:DebugLogSetLevel() debug level=debug
00001545 debuglog.c:277:DebugLogSetLevel() debug level=debug
00000112 debuglog.c:277:DebugLogSetLevel() debug level=debug
00000015 debuglog.c:277:DebugLogSetLevel() debug level=debug
00000012 debuglog.c:277:DebugLogSetLevel() debug level=debug
00000182 configfile.l:245:DBGetReaderListDir() Parsing conf directory: /etc/read
er.conf.d
00000400 configfile.l:287:DBGetReaderList() Parsing conf file: /etc/reader.conf.
d/libccidtwi
00000224 pcscdaemon.c:550:main() pcsc-lite 1.7.2 daemon ready.
00001670 hotplug_libudev.c:258:get_driver() Looking for a driver for VID: 0x1D6B
, PID: 0x0001, path: /dev/bus/usb/002/001
00000280 hotplug_libudev.c:258:get_driver() Looking for a driver for VID: 0x1D6B
, PID: 0x0001, path: /dev/bus/usb/002/001
00000263 hotplug_libudev.c:258:get_driver() Looking for a driver for VID: 0x0E0F
, PID: 0x0003, path: /dev/bus/usb/002/002
00000257 hotplug_libudev.c:258:get_driver() Looking for a driver for VID: 0x0E0F
, PID: 0x0003, path: /dev/bus/usb/002/002
00000283 hotplug_libudev.c:258:get_driver() Looking for a driver for VID: 0x1D6B
, PID: 0x0001, path: /dev/bus/usb/002/001
00000268 hotplug_libudev.c:258:get_driver() Looking for a driver for VID: 0x0E0F
, PID: 0x0002, path: /dev/bus/usb/002/003
00000266 hotplug_libudev.c:258:get_driver() Looking for a driver for VID: 0x0A89
, PID: 0x0030, path: /dev/bus/usb/002/013
00000120 hotplug_libudev.c:258:get_driver() Looking for a driver for VID: 0x0A89
, PID: 0x0030, path: /dev/bus/usb/002/013
00000080 hotplug_libudev.c:309:HPAddDevice() Adding USB device: Aktiv Rutoken EC
P
00000110 readerfactory.c:934:RFInitializeReader() Attempting startup of Aktiv Ru
token ECP 00 00 using /usr/lib/pcsc/drivers/ifd-ccid.bundle/Contents/Linux/libcc
id.so
```

Рис. 15. Отладочный лог для GNU/Linux

2. Остановите сервис `pcscd`, если он запущен.

Для получения расширенной информации запустите `pcscd` вручную в отладочном режиме: `# /usr/sbin/pcscd -afddddd`, если устройство работает, то при подключении/отключении вы заметите его упоминание в отладочном логге.

Проверка работоспособности «Рутокен ЭЦП» в Apple Mac OS

1. Подключите «Рутокен ЭЦП» к компьютеру и откройте терминал.
2. Для запуска тестирования устройств введите команду `pcscstest`.
3. В строку `Enter the reader number` введите значение "1".
4. Повторите Шаг 3.
5. В окне терминала должно отобразиться сообщение о том, что тестирование работы устройства успешно завершено (см. рис. 16).

```
tester — -bash — 93x43
Last login: Tue Apr 18 09:35:08 on console
Mac-mini-Tester:~ tester$ 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 !
Mac-mini-Tester:~ testers$
```

Рис. 16. Терминал Mac OS

Работа с «Рутокен ЭЦП» в системе «iBank для Бизнеса»

Эксплуатация и хранение

«Рутокен ЭЦП» является чувствительным электронным устройством. При хранении и эксплуатации пользователю необходимо соблюдать ряд правил и требований, при нарушении которых указанное устройство может выйти из строя.

Следующие правила эксплуатации и хранения обеспечат длительный срок службы устройства, а также сохранность конфиденциальной информации пользователя:

- Оберегайте устройство от механических воздействий (ударов, падения, сотрясения, вибрации и т. п.), от воздействия высоких и низких температур, агрессивных сред, высокого напряжения.
- Не прилагайте излишних усилий при подсоединении устройства к порту компьютера.
- Не допускайте попадания на устройство (особенно на его разъем) пыли, грязи, влаги и т. п. При засорении разъема примите меры для его очистки. Для очистки корпуса и разъема устройства используйте сухую безворсовую ткань. Использование растворителей и моющих средств недопустимо.
- Не разбирайте устройство! Такие действия могут привести к поломке корпуса, а также к порче или поломке элементов печатного монтажа и, как следствие — к ненадежной работе или выходу из строя самого устройства. Кроме того, при этом будет утрачена гарантия на устройство
- Разрешается подключать «Рутокен ЭЦП» только к исправному оборудованию. Параметры USB-порта должны соответствовать спецификации для USB.
- Не рекомендуется использовать длинные переходники или USB-хабы без дополнительного питания, поскольку из-за этого на вход, предназначенный для устройства, может подаваться несоответствующее напряжение.
- Запрещается извлекать «Рутокен ЭЦП» из порта компьютера, если на устройстве мигает индикатор, поскольку это обозначает работу с данными, и прерывание работы может негативно сказаться как на данных, так и на работоспособности устройства.
- Запрещается оставлять подключенным к компьютеру «Рутокен ЭЦП» во время включения, выключения, перезагрузки, ухода в режимы sleep или hibernate, поскольку в это время возможны перепады напряжения на USB-порте и, как следствие, выход устройства из строя.
- Не рекомендуется оставлять «Рутокен ЭЦП» подключенным к компьютеру, когда он не используется.
- В случае неисправности или неправильного функционирования «Рутокен ЭЦП» обращайтесь в ваш банк.

Внимание!

- Не передавайте «Рутокен ЭЦП» третьим лицам! Не сообщайте третьим лицам пароли от ключей электронной подписи!
- Подключайте «Рутокен ЭЦП» к компьютеру только на время работы с системой «iBank для Бизнеса».
- В случае утери (хищения) или повреждения «Рутокен ЭЦП» немедленно обратитесь в ваш банк.

Использование при регистрации в системе

Процесс предварительной регистрации корпоративных клиентов осуществляется в АРМ «Регистратор для корпоративных клиентов»:

1. Подключите «Рутокен ЭЦП» к USB-порту компьютера.
2. Для регистрации подключитесь к интернету, запустите web-браузер и перейдите на страницу для клиентов банка системы «iBank для Бизнеса» вашего банка.

3. На странице входа клиентов выберите пункт: **Регистрация и создание ЭП** → **Подключение к системе**.

В результате загрузится соответствующий АРМ.

Если на компьютере еще не установлен BIFIT Signer, появится соответствующее предупреждение со ссылкой на скачивание дистрибутива.

4. Пройдите все этапы регистрации. На восьмом шаге в качестве хранилища ключей выберите из списка пункт **Аппаратное устройство** (см. [рис. 17](#)). В поле ниже отобразится серийный номер подключенного к компьютеру устройства.

iBank для Бизнеса

Подключение к системе

Шаг 8 из 12

Новый ключ ЭП должен быть добавлен в хранилище ключей.
В одном хранилище может содержаться несколько ключей ЭП.

Укажите полный путь к файлу или серийный номер аппаратного устройства,
которое будет использоваться для генерации ключей ЭП.

Если хранилище не существует, будет создано новое.

Аппаратное устройство

Рутокен ЭЦП 2.0 (0923216834) **Выбрать...**

Назад **Вперед**

Рис. 17. Интернет-Банк. Предварительная регистрация. Шаг 8 из 12

5. Если к «Рутокен ЭЦП» задан PIN-код, то появится окно для ввода PIN-кода (см. [рис. 18](#)). Укажите значение PIN-кода пользователя.

Внимание!

Неправильно ввести PIN-код доступа к «Рутокен ЭЦП» можно не более 10 раз подряд, после чего «Рутокен ЭЦП» блокируется для использования (подробнее см. в разделе [Администрирование «Рутокен ЭЦП»](#)).

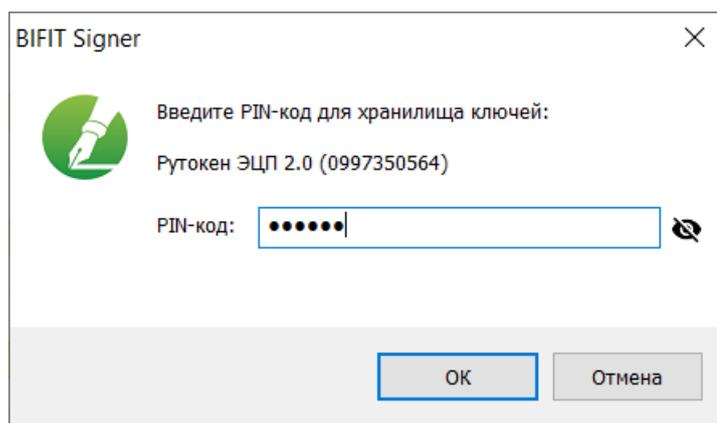


Рис. 18. Ввод PIN-кода пользователя

6. На следующих шагах регистрации вам необходимо указать наименование и пароль к создаваемому ключу ЭП. Для повышения уровня безопасности пароля воспользуйтесь следующими рекомендациями:
- пароль не должен состоять из одних цифр;
 - пароль не должен быть слишком коротким и состоять из символов, находящихся на одной линии на клавиатуре;
 - пароль должен содержать в себе как заглавные, так и строчные буквы, цифры и знаки препинания;
 - пароль не должен быть значимым словом (ваше имя, дата рождения, девичья фамилия жены и т.д.), которое можно легко подобрать или угадать.

Примечание:

В одном «Рутокен ЭЦП» может содержаться до 84-и ключей ЭП ответственных сотрудников разных корпоративных клиентов, обслуживаемых в разных банках с разными экземплярами системы «iBank для Бизнеса».

Внимание!

Неправильно указать пароль к ключу ЭП, который находится в памяти «Рутокен ЭЦП», можно не более 15 раз подряд. После этого ключ ЭП блокируется навсегда.

Использование при входе в систему

1. Подключитесь к интернету, запустите web-браузер и перейдите на страницу для клиентов банка системы «iBank для Бизнеса» вашего банка.
2. Подключите «Рутокен ЭЦП» к USB-порту компьютера.
3. На странице входа корпоративных клиентов банка выберите необходимый пункт:
 - Вход в Интернет-Банк → Выбрать электронную подпись;
 - Вход в Центр Финансового Контроля;
 - Запустите приложение Офлайн-Банк и выполните синхронизацию.
4. Выберите в списке «Рутокен ЭЦП» (см.рис. 19), если к устройству задан PIN-код, то появится окно для его ввода. Укажите значение PIN-кода.

Внимание!

Неправильно ввести PIN-код доступа к «Рутокен ЭЦП» можно не более 10 раз подряд, после чего «Рутокен ЭЦП» блокируется для использования (подробнее см. в разделе [Администрирование «Рутокен ЭЦП»](#)).

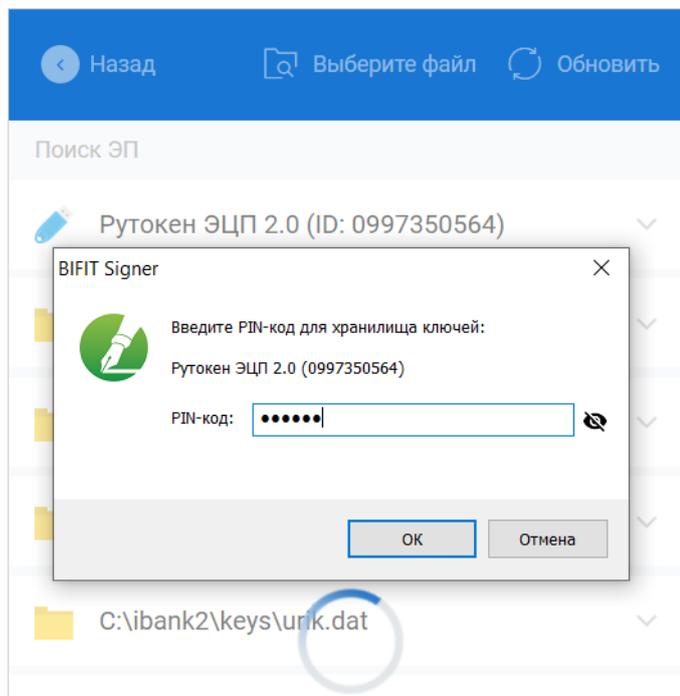


Рис. 19. Вход в Интернет-Банк. Ввод PIN-кода

Если ввод PIN-кода не требуется выберите ключ ЭП (см. [рис. 20](#)) и укажите пароль к нему.

При вводе пароля учитываются язык (русский/английский) и регистр (заглавные/прописные буквы).

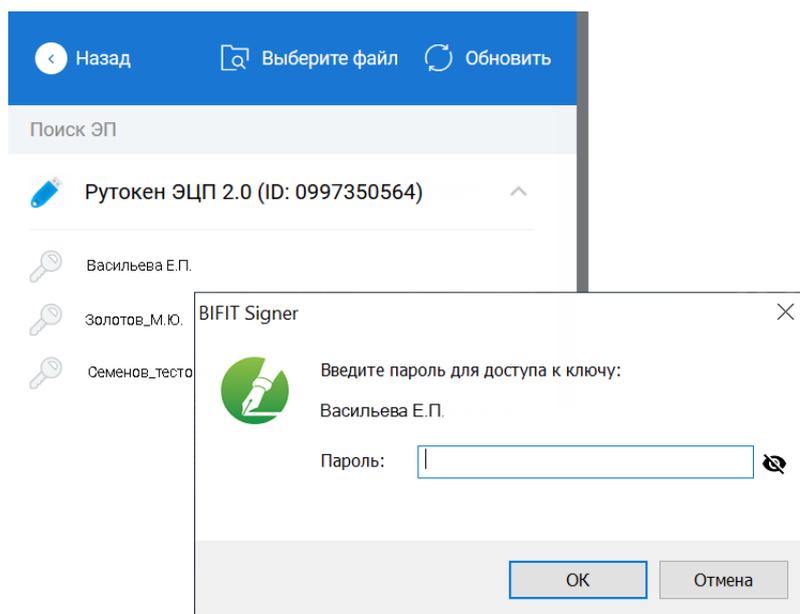


Рис. 20. Список ключей ЭП

5. Окно **Вход в систему** для ЦФК представлено на [рис. 21](#).

Рис. 21. Вход в ЦФК

Выполните следующие действия:

- В поле **Тип хранилища** выберите **Аппаратное устройство**. В поле **Токен** отобразится серийный номер выбранного USB-токена.
- При использовании устройства, к которому задан PIN-код, отобразится окно для его ввода (см. рис. 22). Укажите значение PIN-кода.

Внимание!

Неправильно ввести PIN-код доступа к «Рутокен ЭЦП» можно не более 10 раз подряд, после чего «Рутокен ЭЦП» блокируется для использования (подробнее см. в разделе [Администрирование «Рутокен ЭЦП»](#)).

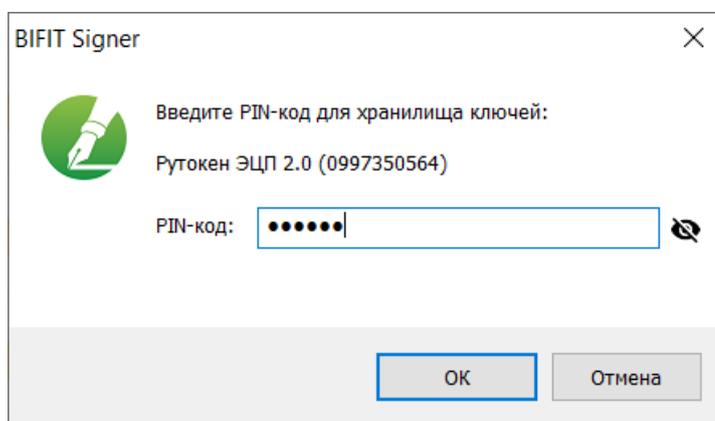


Рис. 22. Ввод PIN-кода

- Из списка поля **Ключ** выберите наименование ключа ЭП и нажмите кнопку **Войти**.
- Укажите **Пароль** для доступа к выбранному ключу (см. рис. 23). При вводе пароля учитываются язык (русский/английский) и регистр (заглавные/прописные буквы).

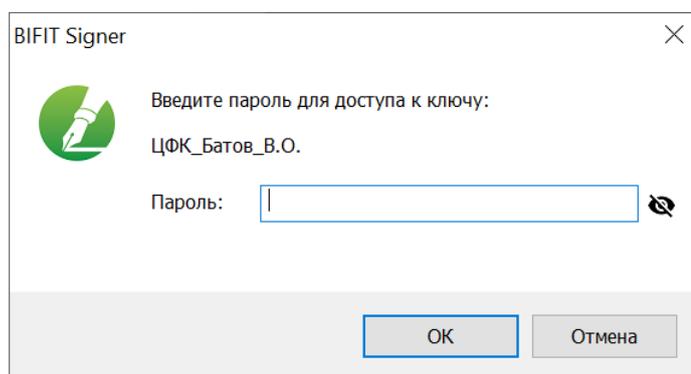


Рис. 23. Ввод пароля для доступа к ключу ЭП

Администрирование ключей ЭП

Для ключей ЭП хранящихся в памяти «Рутокен ЭЦП» доступны следующие действия:
Возможны следующие действия с ключами ЭП:

- [Печать сертификата ключа проверки ЭП](#)
- [Смена пароля доступа к ключу ЭП](#)

- Смена наименования ключа ЭП
- Удаление ключа ЭП

Внимание!

Задание PIN-кода устройства осуществляется через **Панель управления Рутокен**, которая устанавливается вместе с драйвером устройства (подробнее см. в разделе [Администрирование «Рутокен ЭЦП»](#)). Смена PIN-кода устройства доступна в Интернет-Банке и через **Панель управления Рутокен**.

Администрирование ключей ЭП, хранящихся в памяти «Рутокен ЭЦП», выполняется:

- корпоративными клиентами и сотрудниками центра финансового контроля в АРМ **«Регистратор для корпоративных клиентов»**. Для перехода в АРМ выполните:
 - Интернет-Банк — на странице входа клиентов банка перейдите: **Регистрация** → **Администрирование ключей ЭП**;
 - Офлайн-Банк — перейдите в раздел **Электронные подписи** → **Администрирование ключей ЭП**;
 - ЦФК — на странице входа клиентов банка перейдите: **Вход в Центр Финансового Контроля** → **Управление ключами ЭП**.

Выполните следующие действия:

1. Запустите соответствующий АРМ.
2. Укажите тип хранилища ключей ЭП — **Аппаратное устройство**.
3. В поле ниже отобразится серийный номер подключенного к компьютеру устройства. Под серийным номером отобразится список ключей ЭП (см. [рис. 24](#)).

iBank для Бизнеса

Администрирование ключей ЭП

Укажите тип хранилища ключей ЭП

Ключ на диске

Аппаратное устройство

Рутокен ЭЦП 2.0 (0923216834) Выбрать

Наименование ключа
Золотов М.Ю.(Крокус)

Количество ключей на аппаратном устройстве: 1

Сменить PIN Печать Сменить пароль Переименовать Удалить

Рис. 24. АРМ «Регистратор». Администрирование ключей ЭП

4. Выберите ключ ЭП и нажмите кнопку, соответствующую операции, которую необходимо выполнить.

Печать сертификата ключа проверки ЭП

Выберите в списке требуемый ключ ЭП и нажмите кнопку **Печать**. Укажите пароль для доступа к ключу ЭП. Нажмите кнопку **Принять**. Далее откроется стандартное окно вывода документа на печать.

Смена пароля доступа к ключу ЭП

Выберите в списке требуемый ключ ЭП и нажмите кнопку **Сменить пароль**. Укажите текущий пароль ключа ЭП и дважды новый пароль. Нажмите кнопку **Принять**. Новый пароль к ключу ЭП будет установлен.

Смена наименования ключа ЭП

Выберите в списке требуемый ключ ЭП и нажмите кнопку **Переименовать**. Укажите пароль для доступа к ключу ЭП и новое наименование ключа ЭП. Нажмите кнопку **Принять**. Новое наименование ключа ЭП будет установлено.

Удаление ключа ЭП

Внимание!

Если ключ ЭП удалить из хранилища ключей, восстановить его будет невозможно. Поэтому удалять можно ключи, которые в дальнейшем не будут использоваться при работе с системой (ключи с истекшим сроком действия, скомпрометированные ключи и т.д.).

Выберите в списке требуемый ключ ЭП и нажмите кнопку **Удалить**. Укажите пароль для доступа к ключу ЭП. После нажатия кнопки **Принять** ключ будет безвозвратно удален из хранилища ключей.

Администрирование «Рутокен ЭЦП»

Администрирование «Рутокен ЭЦП» осуществляется через **Панель управления «Рутокен ЭЦП»**, которая устанавливается вместе с драйвером устройства.

Возможны следующие действия с «Рутокен ЭЦП»:

- [Задание PIN-кода доступа \[23\]](#)
- [Настройки политик безопасности PIN-кодов \[25\]](#)
- [Разблокировка PIN-кода \[26\]](#)
- [Форматирование «Рутокен ЭЦП» \[26\]](#)

Все действия с устройством доступны только после ввода корректного PIN-кода.

По умолчанию для «Рутокен ЭЦП» установлены следующие значения PIN-кодов:

Пользователь: 12345678

Администратор: 87654321

Задание PIN-кода доступа к «Рутокен ЭЦП»

Для обеспечения дополнительной защиты от несанкционированного доступа к ключам ЭП, хранящимся на «Рутокен ЭЦП», реализована возможность задавать PIN-код доступа к «Рутокен ЭЦП».

При обращении к «Рутокен ЭЦП» с заданным PIN-кодом отсутствует возможность получения списка ключей «Рутокен ЭЦП» и каких-либо действий с ними, до момента ввода корректного PIN-кода.

PIN-код к «Рутокен ЭЦП», если он установлен, запрашивается у пользователя при выполнении следующих действий:

- аутентификация в Интернет-Банке;
- обращение к «Рутокен ЭЦП» в случае его отключения и последующего подключения;
- обращение к «Рутокен ЭЦП» в ходе администрирования ключей ЭП;
- подпись документов и синхронизация данных с банком во время работы в Офлайн-Банке.

Задание PIN-кода устройства осуществляется через **Панель управления Рутокен**, которая устанавливается вместе с драйвером устройства.

Запуск панели управления можно осуществить, например, через **Пуск/Программы/Рутокен/Панель управления Рутокен**. Откроется главное окно программы (см. [рис. 25](#)).

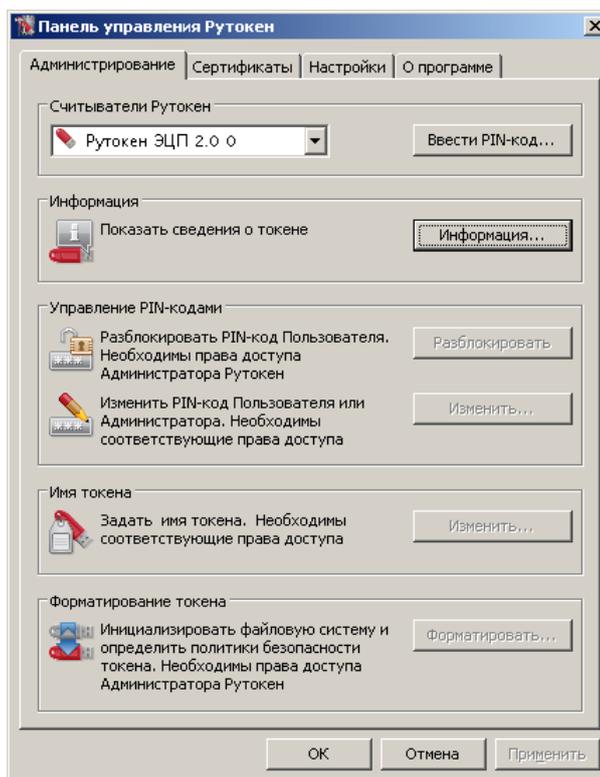


Рис. 25. Панель управления Рутокен. Закладка Администрирование

Для аутентификации в программе нажмите кнопку **Ввести PIN-код...** В открывшемся окне (см. рис. 26) выберите тип пользователя, под которым необходимо работать, укажите значение PIN-кода и нажмите кнопку **ОК**.

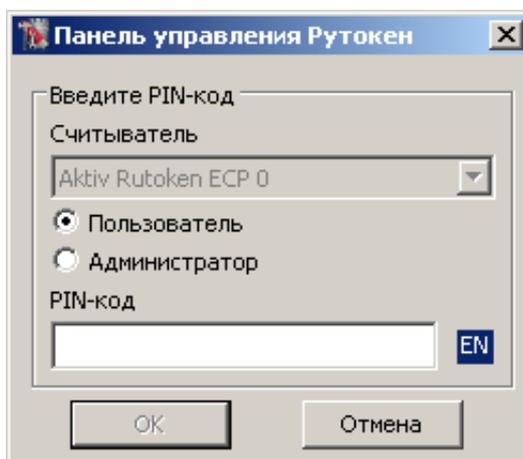


Рис. 26. Панель управления Рутокен. Ввод PIN-кода

Для смены PIN-кода в блоке **Управление PIN-кодами** нажмите кнопку **Изменить...** В открывшемся окне дважды укажите новое значение PIN-кода (см. рис. 27).

Значение PIN-кода должно соответствовать политикам безопасности.

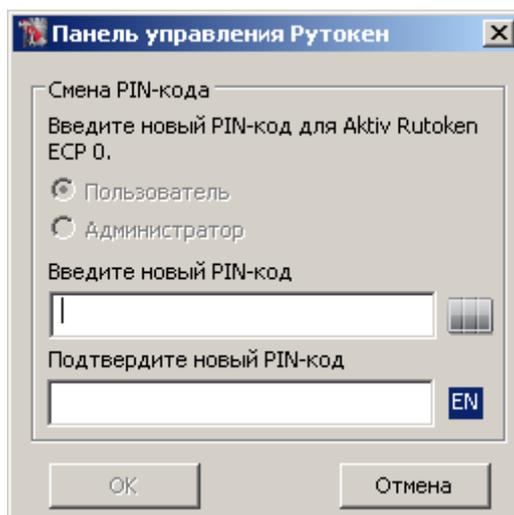


Рис. 27. Панель управления Рутокен. Смена PIN-кода

Назначенный PIN-код удалить нельзя, его можно лишь сменить.

Внимание!

Неправильно ввести PIN-код доступа к «Рутокен ЭЦП» можно не более 10 раз подряд, после чего «Рутокен ЭЦП» блокируется для использования:

- Устройство, заблокированное неверным вводом PIN-кода Пользователя — разблокируется Администратором;
- Устройство, заблокированное неверным вводом PIN-кода Администратора — разблокировать невозможно.

Настройки политик безопасности PIN-кодов

Политики контроля качества PIN-кодов «Рутокен ЭЦП» используются для повышения уровня информационной безопасности.

По уровню надежности все PIN-коды «Рутокен ЭЦП» делятся на три категории: "слабые", "средние" и "надежные". Критерием такого деления являются весовые коэффициенты используемых политик и общая (интегральная) оценка PIN-кода. Пользователь «Рутокен ЭЦП» может задать необходимость появления на экране предупреждающего сообщения при попытке сменить PIN-код на "слабый" или "средний". Кроме того, есть возможность запретить использование "слабого" PIN-кода на токене.

Для контроля качества PIN-кодов «Рутокен ЭЦП» используются следующие политики:

- Минимальная длина PIN-кода.
- Длина PIN-кода.
- Политика использования PIN-кода, заданного по умолчанию.
- Политика использования PIN-кода, состоящего из одного повторяющегося символа.
- Политика использования PIN-кода, состоящего только из цифр.
- Политика использования PIN-кода, состоящего только из букв.
- Политика использования PIN-кода, совпадающего с предыдущим PIN-кодом.

При установке драйверов «Рутокен ЭЦП» значения параметров политик контроля качества PIN-кодов установлены по умолчанию.

Политики контроля качества PIN-кода могут быть изменены пользователем с правами администратора через **Панель управления Рутокен**.

Для изменения политик контроля качества перейдите на закладку **Настройки** панели управления Рутокен. В блоке **Политики качества PIN-кодов** нажмите кнопку **Настройка...** Откроется окно как на [рис. 28](#).

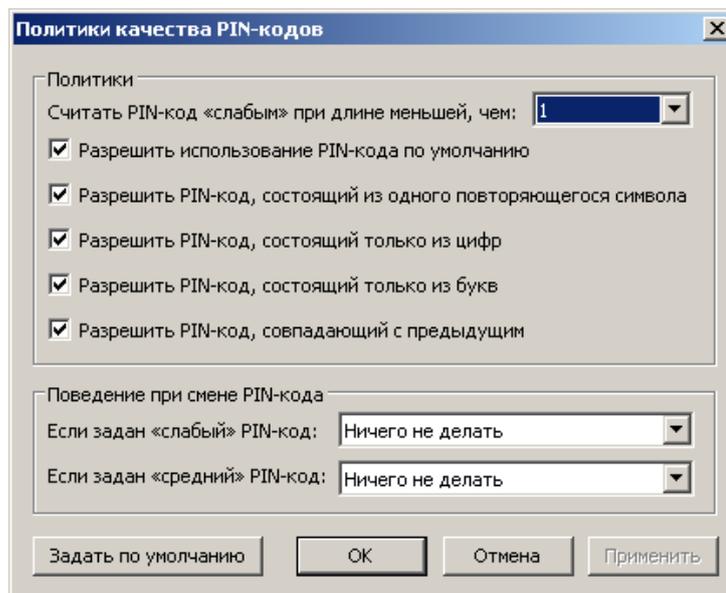


Рис. 28. Политики качества PIN-кодов

Для изменения настроек в блоках **Политики** и **Поведение при смене PIN-кодов** установите флаги в соответствующих чекбоксах, выберите необходимые значения из выпадающих списков и нажмите кнопку **Ок**. Чтобы задать настройки по умолчанию нажмите кнопку **Задать по умолчанию**.

Разблокировка PIN-кода

Разблокирование PIN-кода пользователя «Рутокен ЭЦП» выполняется в тех случаях, когда он был заблокирован после определенного числа последовательных неудачных попыток ввода PIN-кода.

Разблокировку должен осуществлять пользователь с правами администратора.

Внимание!

При выполнении разблокировки счетчик попыток ввода PIN-кода восстанавливается в свое исходное значение, заданное при инициализации токена. Сбрасывается именно счетчик попыток, а не сам PIN-код!

Для разблокировки запустите **Панель управления Рутокена**. На закладке **Администрирование** нажмите кнопку **Ввести PIN-код...** В открывшемся окне (см. [рис. 25](#)) выберите тип пользователя **"Администратор"**, укажите его значение PIN-кода и нажмите кнопку **ОК** Затем нажмите кнопку **Разблокировать**.

Далее необходимо аутентифицироваться с правами **"Пользователя"** и продолжить попытки восстановления значения PIN-кода. Если сделать это не удастся, то можно лишь отформатировать «Рутокен ЭЦП» с потерей всей информации на нем.

Форматирование «Рутокен ЭЦП»

Внимание!

Форматирование «Рутокен ЭЦП» приводит к потере всей информации на нем!

Удаленная информация восстановлению не подлежит!

Для форматирования устройства запустите **Панель управления Рутокена**. На закладке **Администрирование** (см. [рис. 27](#)) нажмите кнопку **Ввести PIN-код...** В открывшемся окне выберите тип пользователя "**Администратор**", укажите его значение PIN-кода и нажмите кнопку **ОК** Нажмите ставшей активной кнопку **Форматировать...** В открывшемся окне, если не требуется дополнительных настроек, нажмите кнопку **Начать** (см. [рис. 29](#)).

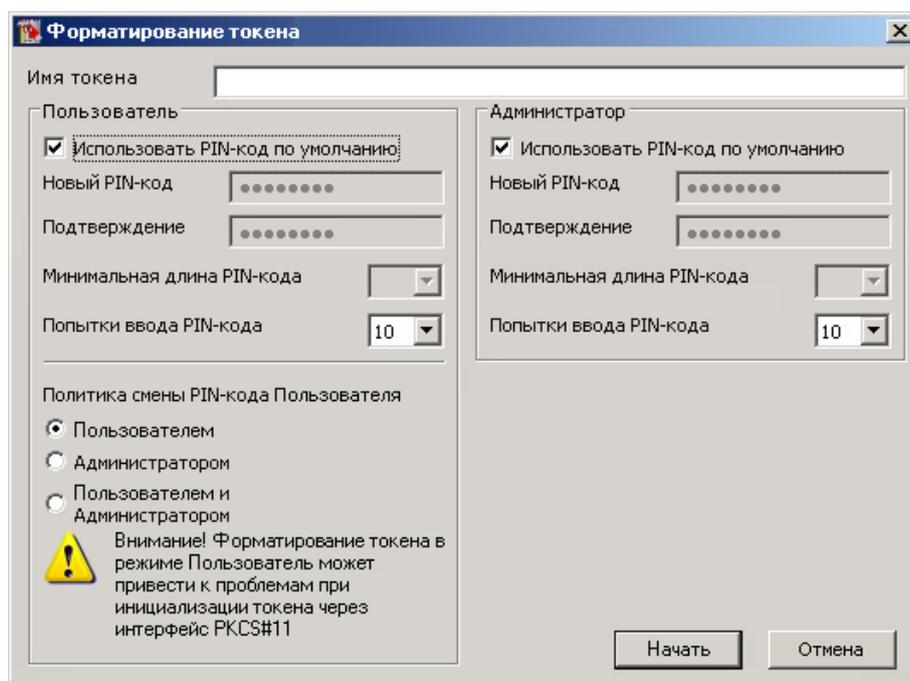


Рис. 29. Форматирование токена

Для продолжения подтвердите свои намерения (см. [рис. 30](#)).

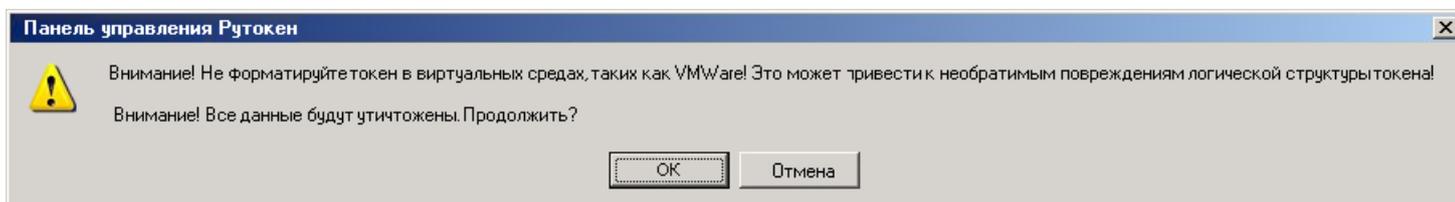


Рис. 30. Предупреждение

Дождитесь окончания форматирования (см. [рис. 31 - 30](#)).

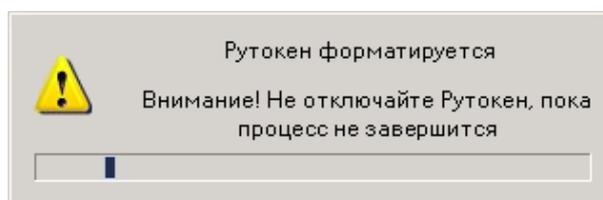


Рис. 31. Предупреждение

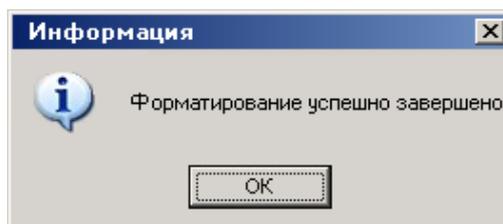


Рис. 32. Предупреждение

Внимание!

Если операция форматирования «Рутокен ЭЦП» не будет завершена («Рутокен ЭЦП» будет отключен, программа будет принудительно закрыта, питание компьютера будет выключено...), то это приведет к неработоспособности устройства.

Если неизвестен (заблокирован) PIN-код администратора, то в большинстве случаев вы все равно можете отформатировать «Рутокен ЭЦП» самостоятельно. После исчерпания попыток ввода корректного PIN-кода администратора кнопка **Форматировать** становится доступной.

Обновление драйверов «Рутокен ЭЦП» для Windows

Перед началом обновления драйверов рекомендуется отключить «Рутокен ЭЦП» от USB-порта компьютера.

Загрузите новую версию пакета драйверов с сайта разработчика <http://www.rutoken.ru/support/download/get/rtDrivers-exe.html>

Поддерживаемые ОС: MS Windows 10/8.1/2012R2/8/2012/7/2008R2/ Vista/2008

Запустите загруженный файл и следуйте указаниям мастера установки (см. [рис. 33 – 33](#)).

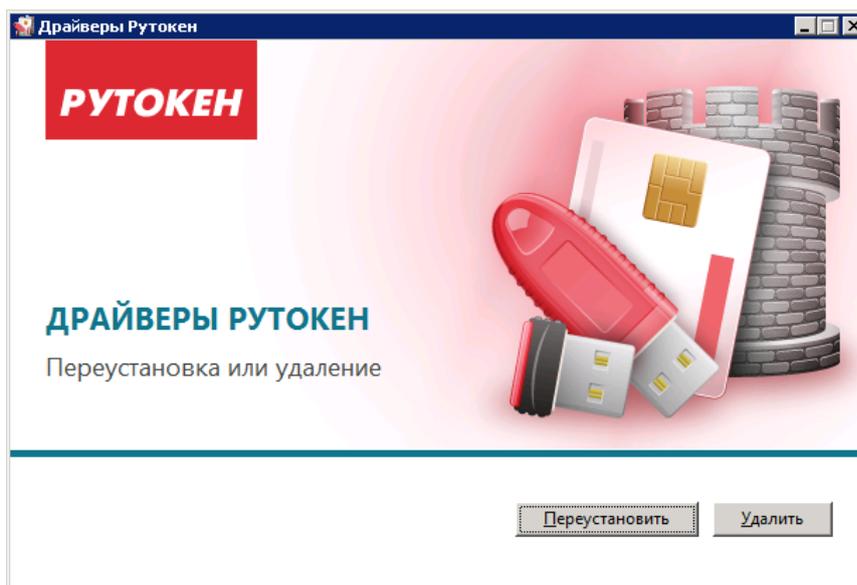


Рис. 33. Мастер установки драйвера

Для переустановки драйвера нажмите кнопку **Переустановить**, для удаления драйвера с компьютера кнопку **Удалить**.

Далее необходимо дождаться окончания процесса (см. [рис. 34](#)) и нажать кнопку **Заккрыть**.

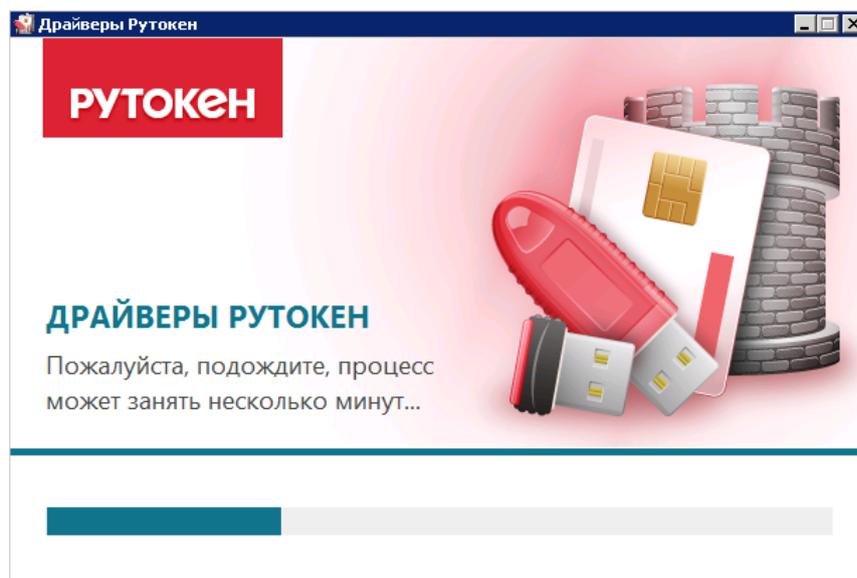


Рис. 34. Мастер установки драйвера

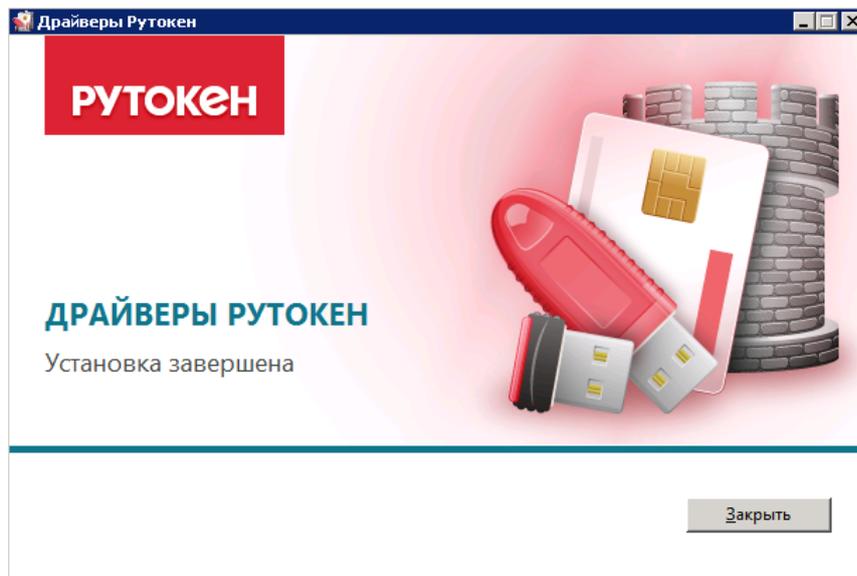


Рис. 35. Мастер установки драйвера

Устранение неисправностей

Наиболее часто встречающиеся неисправности:

- USB-токен недоступен для выбора
- Плагин BIFIT Signer не определяет USB-токен
- Ошибка в ходе установки библиотеки rtPKCS11ECP
- Нестабильная работа USB-токена

USB-токен недоступен

Причиной неисправности может быть установленное в современных версиях ОС семейства Windows ограничение на общее количество устройств чтения смарт-карт в Диспетчере устройств — **не более 10 устройств**.

В случае превышения установленного ограничения при запуске **Панели управления Рутокен** отобразится предупреждение о достижении максимального значения подключенных считывателей смарт-карт (см. [рис. 36](#)).

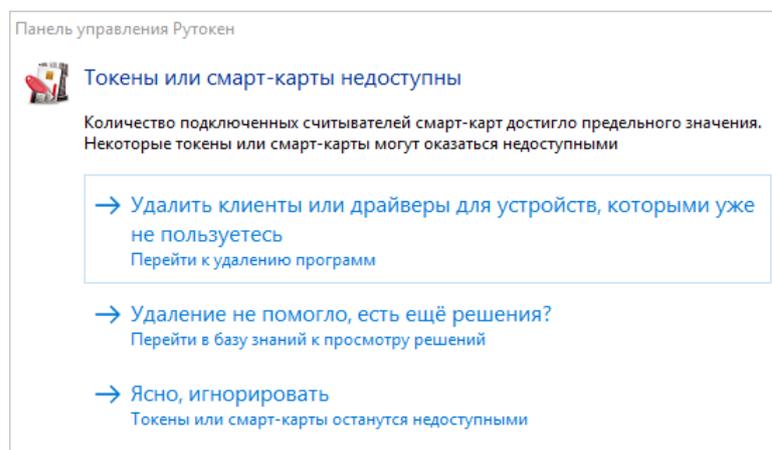


Рис. 36. Предупреждение при запуске Панели управления Рутокен

Решение неисправности заключается в сокращении до допустимого количества подключенных считывателей в **Диспетчере устройств**.

Для устранения неисправности выполните действия:

1. Проверьте текущее количество устройств в системе: **Диспетчер устройств** → список **Устройства чтения смарт-карт** (см. [рис. 37](#)).

В списке могут отображаться следующие типы устройств:

- **Реальные считыватели** — смарт-карты и токены, подключенные к компьютеру в текущий момент;
- **Виртуальные считыватели** — предназначены для определенных моделей токенов и создаются в системе при установке драйверов на устройства различных производителей. Виртуальный считыватель отображается всегда, вне зависимости от наличия подключенного устройства.

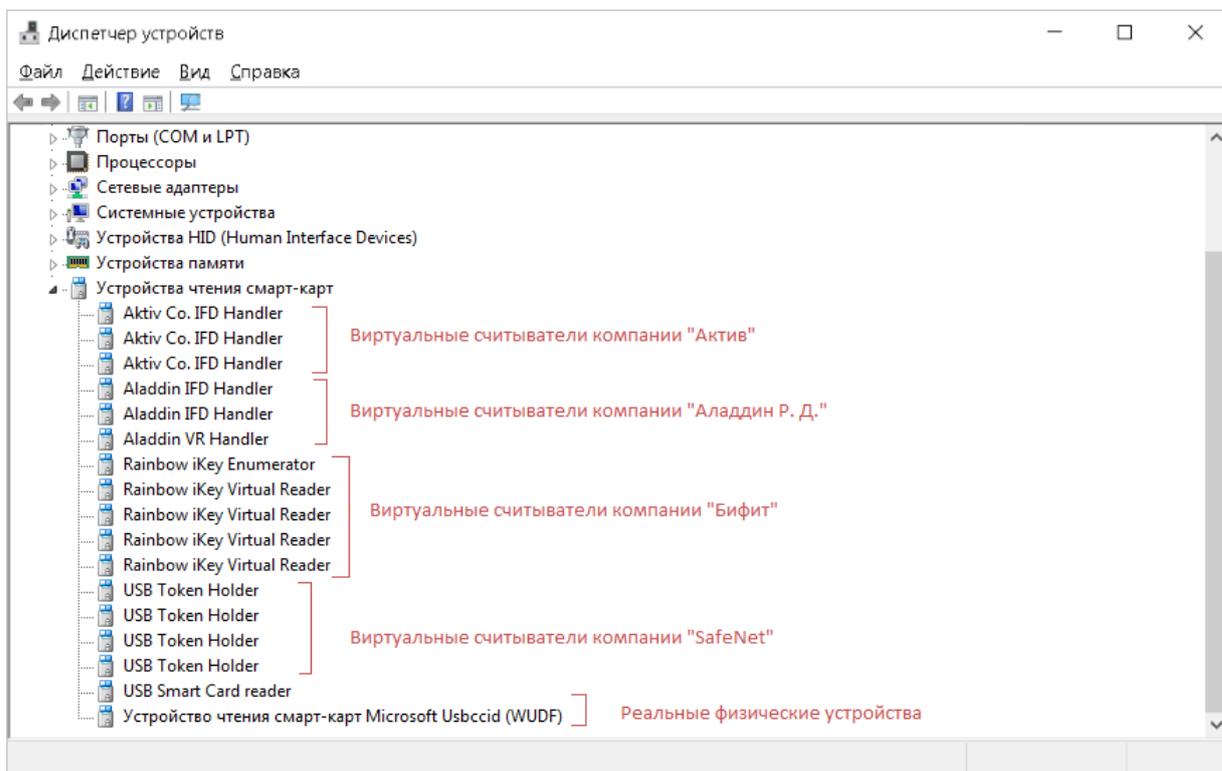


Рис. 37. Диспетчер устройств. Устройства чтения смарт-карт

В списке устройств могут быть следующие виртуальные считыватели:

- **USB Token Holder** — предназначен для работы ключевого идентификатора iBank 2 Key производства компании "Бифит";
- **Aladdin IFD Handler** или **Aladdin VR Handler** — предназначен для работы ключевого идентификатора Etoken производства компании "Аладдин Р. Д.";
- **Rainbow iKey Virtual Reader** — предназначен для работы ключевого идентификатора iKey производства компании "SafeNet";
- **Aktiv Co. IFD Handler** — предназначен только для работы с ключом модели Рутокен S.

Для работоспособности данного ключа количество устройств **Aktiv Co. IFD Handler** в **Диспетчере устройств** должно быть равно количеству ключевых идентификаторов Рутокен S, которые необходимо одновременно подключить к компьютеру — не более 5.

Вы можете уменьшить количество считывателей Рутокен S до фактического числа используемых вами устройств. Если ключи Рутокен S не используются — наличие виртуальных считывателей **Aktiv Co. IFD Handler** не требуется.

Уменьшить количество считывателей **Aktiv Co. IFD Handler** можно через **Панель управления Рутокен** → вкладка **Настройки** (см. [рис. 38](#))

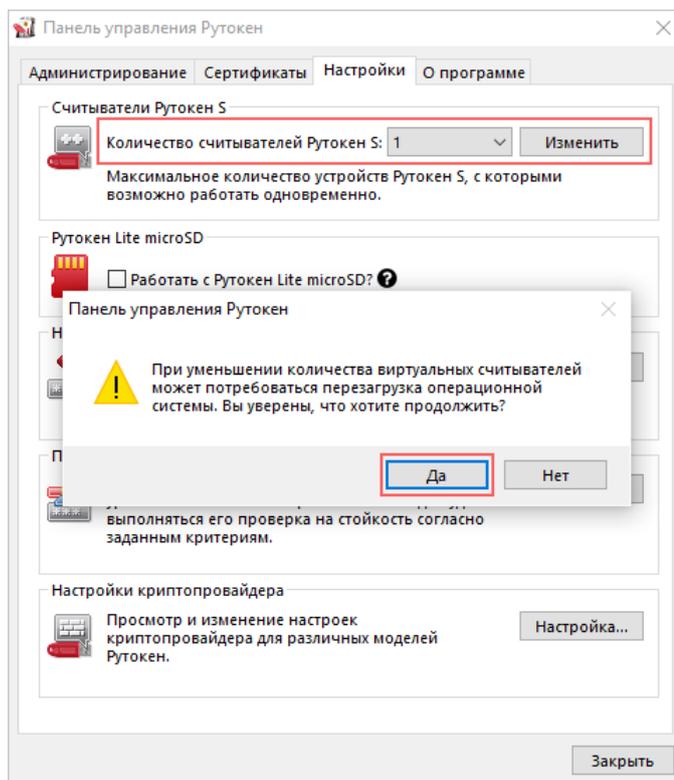


Рис. 38. Панель управления Рутокен. Настройки

2. Определите устройства по производителю и модели подключенных токенов и смарт-карт, которые можно удалить.
3. Удалите считыватели из списка **Устройства чтения смарт-карт**:
 - **Реальные считыватели** — отключите устройство от компьютера;
 - **Виртуальные считыватели** — используйте контекстное меню в **Диспетчере устройств** (см. рис. 39) или выполните деинсталляцию установленного для устройства ПО.

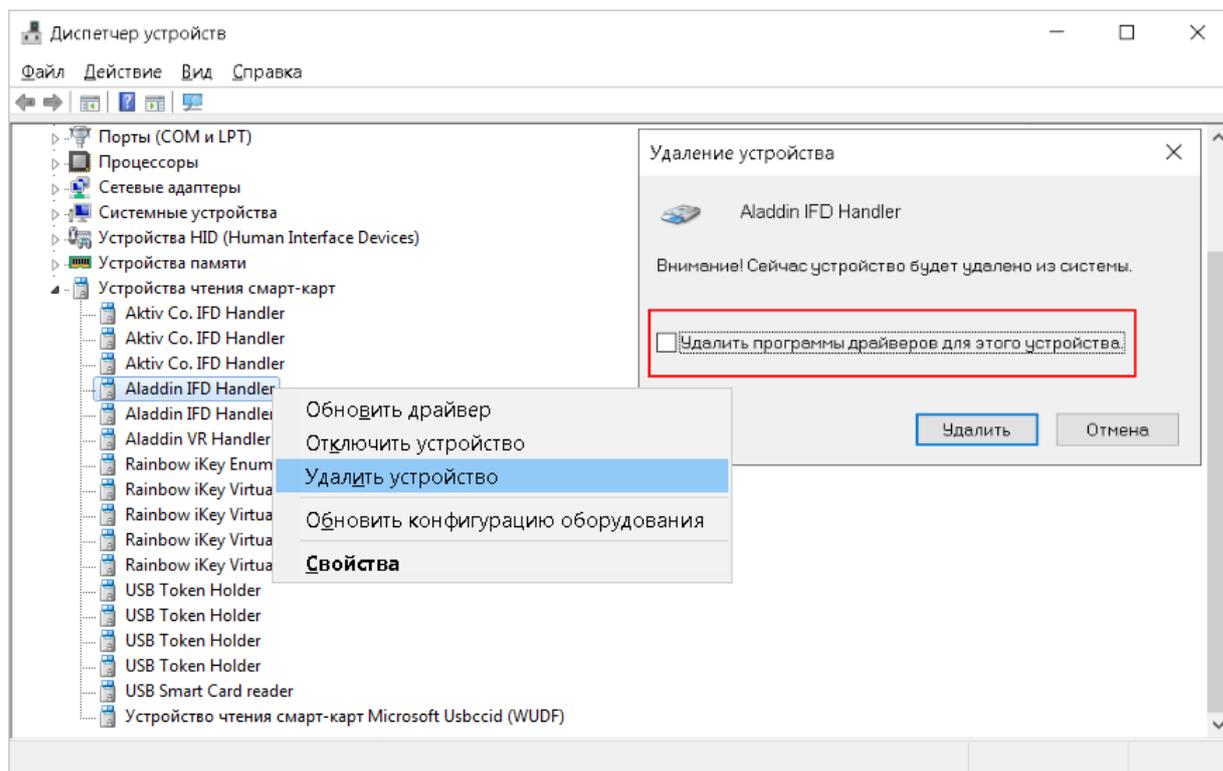


Рис. 39. Диспетчер Устройств. Удаление виртуального считывателя

BIFIT Signer не определяет USB-токен

Решение неисправности приведено отдельно для каждой операционной системы:

- [ОС семейства Windows](#)
- [ОС семейства Linux](#)
- [ОС Apple OS X](#)

Неисправность может проявляться следующим образом:

- USB-токен не отображается:
 - при входе в систему в списке ключей ЭП;
 - при входе в систему для ЦФК, сотрудников банка и оператора сервиса «Чат»;
 - при администрировании ключей ЭП;
 - при выборе аппаратного устройства для генерации ключа ЭП;
 - в иных случаях.
- Отображается сообщение об ошибке – *Не установлены драйвера или не запущена служба 'Smart Card'*:
 - при входе в систему для ЦФК и сотрудников банка;
 - при выборе аппаратного устройства для генерации ключа ЭП;
 - при переходе в раздел **Электронные подписи** в Интернет-Банке для корпоративных клиентов;
 - при подписании документов в ЦФК;
 - в иных случаях.

Решение для операционных систем семейства Windows

USB-токен может отображаться в диспетчере устройств, но не определяться BIFIT Signer.

Варианты устранения неисправности:

- Перезапустите службу **Смарт-карта**, например, указанным способом:
 1. Откройте окно настроек служб Windows: **Панель управления** → **Система и безопасность** → **Администрирование** → **Службы**
 2. Выберите пункт контекстного меню **Перезапустить** для службы **Смарт-карта** (см. [рис. 40](#)).

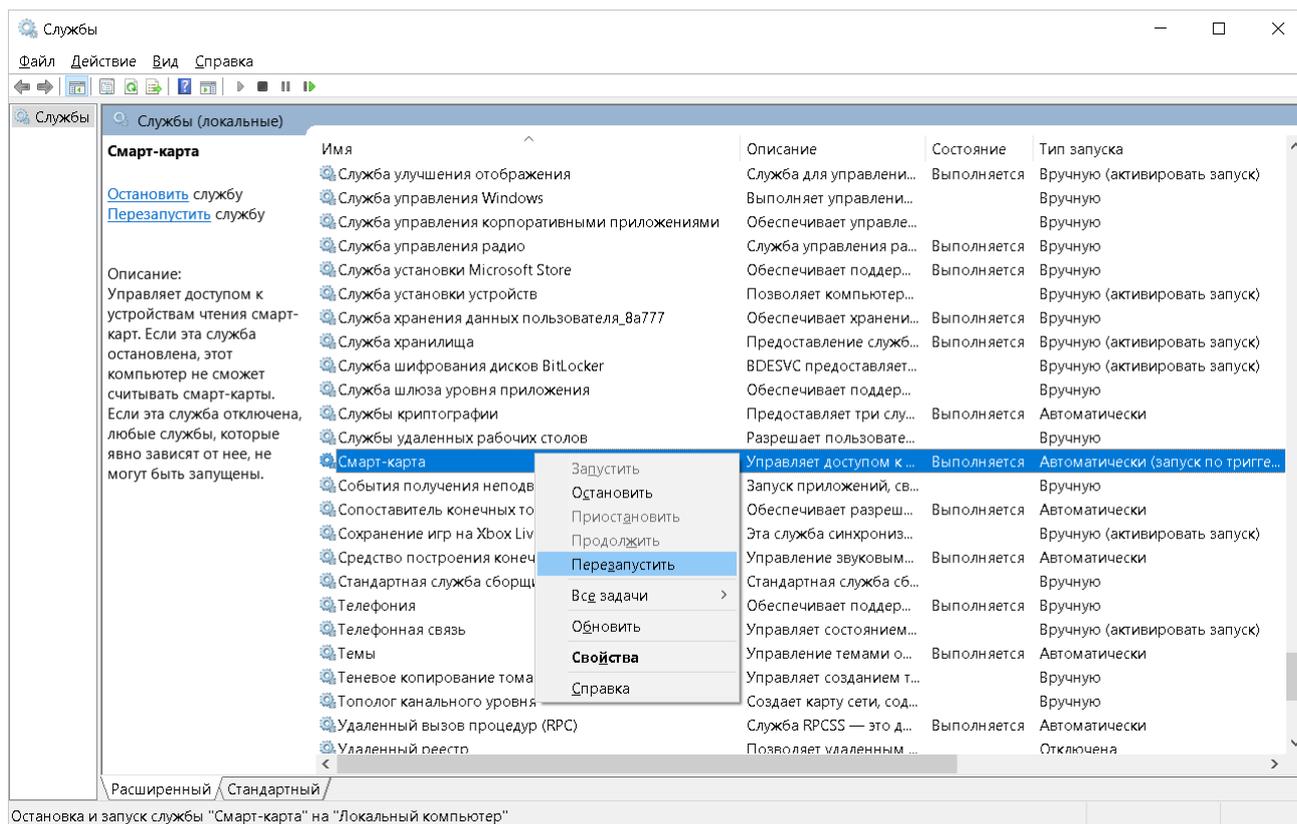


Рис. 40. Окно настроек служб Windows. Перезапуск службы Смарт-карта

- Проверьте, что установленное на компьютере антивирусное программное обеспечение не блокирует работу BIFIT Signer. Отключите антивирусное ПО на время проверки и настройки BIFIT Signer;
- Переустановите BIFIT Signer, запустив инсталлятор от имени администратора.

Решение для операционных систем семейства Linux

Возможные причины неисправности и их решение:

- Не установлены библиотеки `libccid` `pcscd` `libpcsclite1` или `PKCS11`
 - Скачайте и установите соответствующую библиотеку
- Отсутствуют позиционно-зависимые записи о USB-токене в конфигурационном файле `Info.plist`
 1. Добавьте записи в конфигурационный файл `Info.plist` (см. [Настройка для Linux и MacOS](#)).
 2. Проверьте работоспособность USB-токена (см. [Проверка работоспособности](#)).

Решение для операционной системы Apple OS X

Возможные причины неисправности и их решение:

- Отсутствуют записи о USB-токене в конфигурационном файле `libccid`
 1. Добавьте записи в конфигурационный файл `Info.plist` (см. [Настройка для Linux и MacOS](#))
 2. Проверьте работоспособность USB-токена (см. [Проверка работоспособности](#)).

Ошибка в ходе установки библиотеки `rtPKCS11ECP`

Неисправность проявляется при запуске установочного файла `RutokenInstaller.pkg`

При установке библиотеки `rtPKCS11ECP` или `PKCS#11` инсталлятор завершает работу с ошибкой (см. [рис. 41](#)).

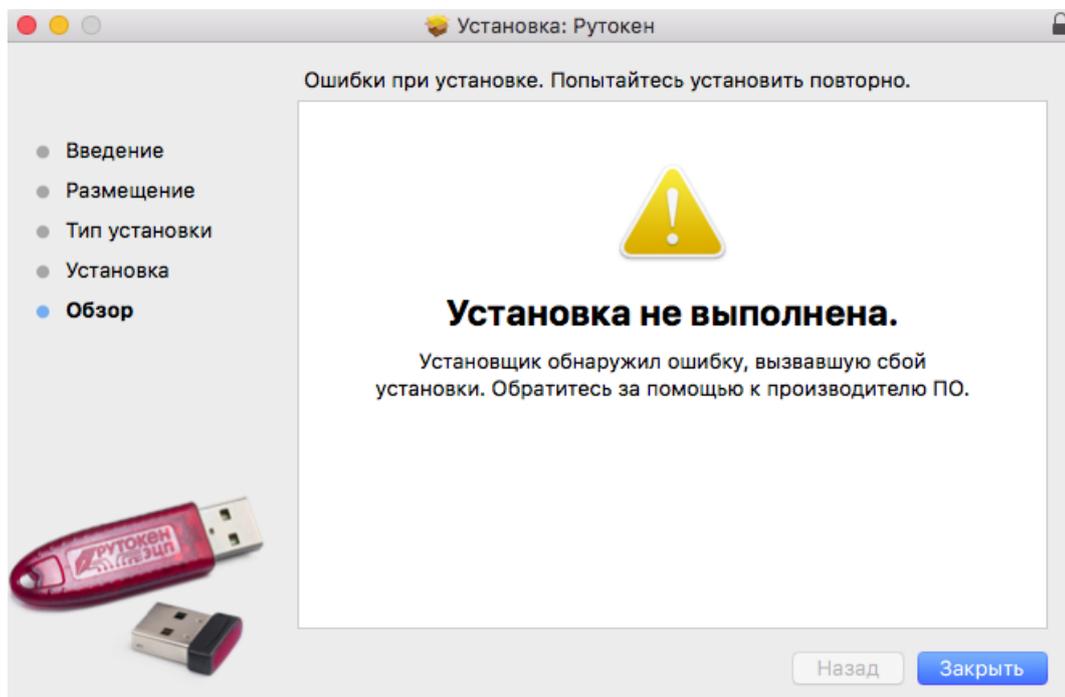


Рис. 41. Ошибка инсталлятора

Неисправность вызвана файлом `lib` размещенным в директории `local`. Для устранения неисправности необходимо удалить файл, например, следующим способом:

1. Вызовите контекстное меню для значка **Finder** и выберите пункт **Переход к папке...** (см. [рис. 42](#)).

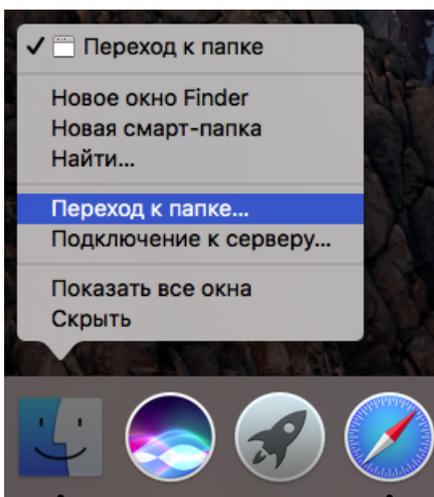


Рис. 42. Finder. Контекстная команда "Переход к папке..."

- В пути к каталогу укажите директорию `/usr/local` (см. рис. 43).

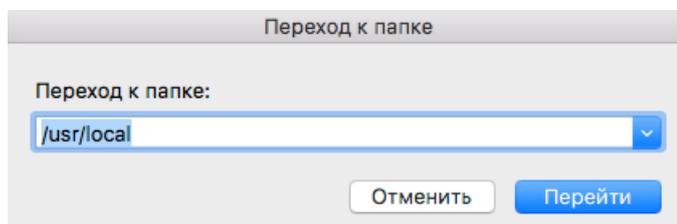


Рис. 43. Путь директории

- В открывшемся каталоге `local` удалите файл `lib` (см. рис. 44).

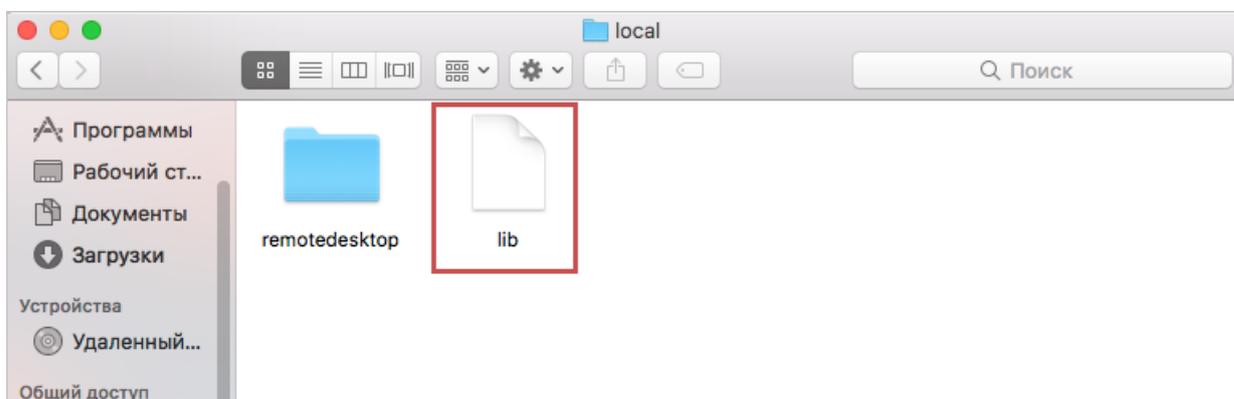


Рис. 44. Каталог local. Удаление файла lib

- Запустите установочный файл `RutokenInstaller.pkg`

Нестабильная работа USB-токена

Неисправность проявляется следующим образом:

- Нестабильная работа USB-токена;
- С USB-токена удаляются рабочие ключи;
- Ключ не отображается в разделе Управление ключами;
- Ошибки при выполнении операций в АРМах системы.

Возможные причины неисправности:

- Извлечение USB-токена из USB-порта во время работы;
- Наличие USB-удлинителей или USB хабов;
- Ненадлежащее состояние USB-порта на компьютере или USB-токене.