СОДЕРЖАНИЕ:

1. Общие сведения

«Рутокен ЭЦП 2.0» представляет собой компактное USB-устройство с аппаратной реализацией российских стандартов электронной подписи (ЭП), шифрования и хеширования.

Рис. 1. Рутокен ЭЦП 2.0

«Рутокен ЭЦП 2.0» предназначен для безопасной двухфакторной аутентификации пользователей, генерации и защищенного хранения ключей электронной подписи, И выполнения электронной подписи в самом устройстве.

«Рутокен ЭЦП 2.0» поддерживает:

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

Аппаратная реализация криптографических алгоритмов электронной подписи (далее ЭП) внутри устройства обеспечивает:

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

Основу «Рутокен ЭЦП 2.0» составляет современный защищенный микроконтроллер и встроенная защищенная память, в которой безопасно хранятся ключи ЭП .

В составе микроконтроллера содержится СКЗИ, сертифицированное ФСТЭК и ФСБ РФ:

- Сертификат ФСТЭК № 2592 от 19.03.2012 г. – действителен до 19.03.2018г.
- Сертификат ФСБ РФ рег. № СФ/124-2771 от 25.12.15 г. – действителен до 25.12.2018г.

Примечание:

В системе «iBank 2» поддерживается работа USB-токенов «Рутокен ЭЦП 2.0» в специальной конфигурации, предназначенной для использования исключительно в системе «iBank 2».

Использование USB-токенов «Рутокен ЭЦП 2.0» с иными конфигурациями и/или приобретенных не через ПАО МОСОБЛБАНК ввиду отсутствия поддержки работы таких устройств в системе «iBank 2».

2. Подготовка «Рутокен ЭЦП 2.0» к работе

2.1 Настройка для Windows

Для полноценной работы «Рутокен ЭЦП 2.0» рекомендуетсяустановить 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 2.0» от USB-порта компьютера.

Установка драйвера может понадобится для версий ОС MS Windows 2008R2 и ниже.

.

Установочный файл можно получить с сайта разработчика «Рутокен ЭЦП 2.0» компании ЗАО «Актив-софт»:

- для 64-битных систем

  Поддерживаемые ОС: MS Windows 10/8.1/2012R2/8/2012/7/2008R2/Vista/2008/XP/2003
- для 32-битных систем

Поддерживаемые ОС: MS Windows 10/8.1/2012R2/8/2012/7/2008R2/Vista/2008/XP/2003

Запустите программу установки драйвера «Рутокен ЭЦП 2.0» и следуйте ее указаниям.

Далее представлены основные этапы работы мастера установки (см. рис. 2 – 4). По умолчанию мастер установки предлагает создать ярлык для запуска панели управления на рабочем столе.

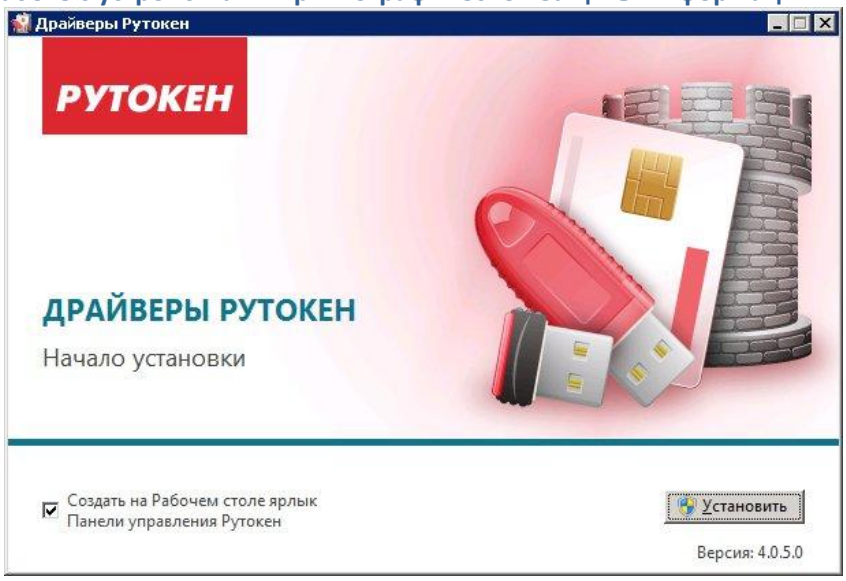


Рис. 2. Мастер установки драйвера

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

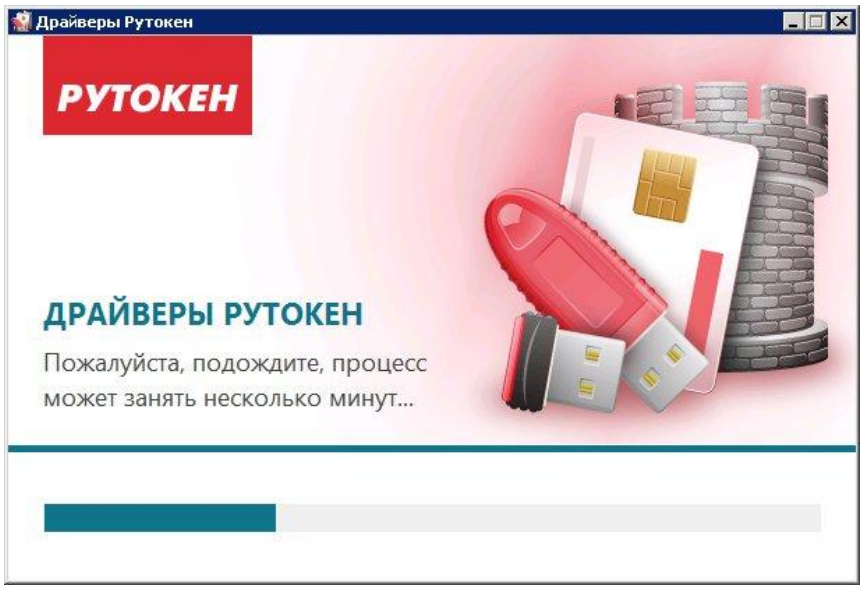


Рис. 3. Мастер установки драйвера

Далее необходимо дождаться окончания установки драйвера (см. рис. 3) и нажать

кнопку**Закрыть** (см. рис. 4).

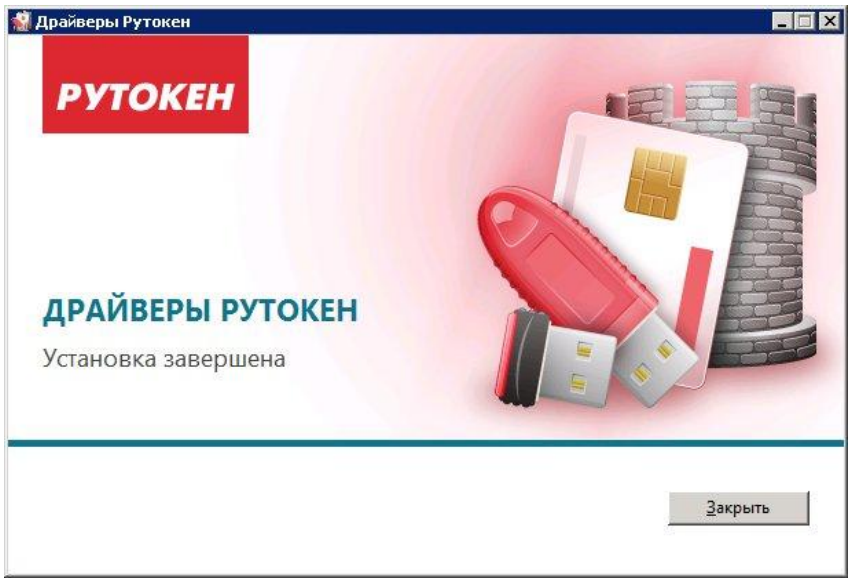


Рис. 4. Мастер установки драйвера

После окончания установки драйвера подключите «Рутокен ЭЦП 2.0» 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).

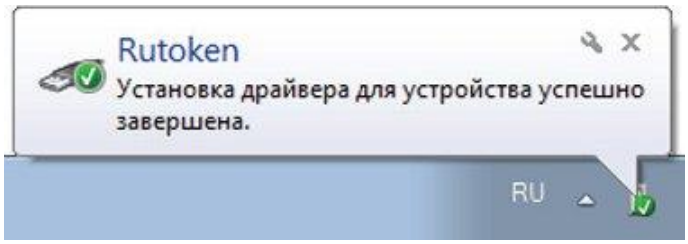


Рис. 5. Панель задач. Сообщение об успешной установке

2.2 Настройка для Linux и Mac OC X

Установка драйвера для «Рутокен ЭЦП 2.0» в современных операционных системах GNU\Linux (версия libccid не ниже 1.3.11) и Mac OC X (версия 10.7 и выше) не требуется, т.к.«Рутокен ЭЦП 2.0» – это устройство поддерживающее стандарт CCID
В операционных системах GNU/Linux и Mac OC X за поддержку стандарта CCID в pcsc-lite отвечает модуль libccid
У libccid существует конфигурационный файл, содержащий описание идентификаторов устройств, которые проверены автором libccid на совместимость.

Внести запись о «Рутокен ЭЦП 2.0» в конфигурационный файл может потребоваться:
- пользователям устаревших дистрибутивов GNU/Linux;
- пользователям Mac OC X 10.6 Snow Leopard и предыдущих версий.

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

В GNU/Linux конфигурационный файл обычно находится в /usr/lib/pcsc/drivers/ifd-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>
    <string>0x3478</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>

2.2.1 Проверка работоспособности:

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, то все в порядке (см. рис. 9).

```
ubuser@ubuntu:~$ sudo pcscd -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/libccidtwin
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. 9. Отладочный лог для GNU\Linux

2. Остановите сервис pcscd, если он запущен. Запустите pcscd вручную в отладочном режиме: # /usr/ sbin/pcscd -afddddd если устройство работает, то при подключении/отключении вы заметите его упоминание в отладочном логе (см. рис. 10).

```
MacBook-Pro-rutoken:~ rutoken$ sudo arch -x86_64 /usr/sbin/pcscd -adfffff
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/debuglog.c:222:DebugLogSetLevel() debug level=debug
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/pcscdaemon.c:389:main() pcscd set to foreground with debug send to stderr
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/pcscdaemon.c:389:main() pcscd set to foreground with debug send to stderr
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/pcscdaemon.c:389:main() pcscd set to foreground with debug send to stderr
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/pcscdaemon.c:389:main() pcscd set to foreground with debug send to stderr
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/pcscdaemon.c:389:main() pcscd set to foreground with debug send to stderr
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/pcscdaemon.c:585:main() pcsc-lite 1.4.0 daemon ready.
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/readerfactory.c:1545:ReaderCheckArchitecture() Send respawn signal to pcscd (pid=76664)
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/pcscdaemon.c:678:signal_respawn() Got signal to respawn in 32 bit mode
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/pcscdaemon.c:294:SVCServiceRunLoop() Preparing to exit...
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/readerfactory.c:1047:RFCleanupReaders() entering cleaning function
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/debuglog.c:222:DebugLogSetLevel() debug level=debug
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/pcscdaemon.c:389:main() pcscd set to foreground with debug send to stderr
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/pcscdaemon.c:389:main() pcscd set to foreground with debug send to stderr
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/pcscdaemon.c:389:main() pcscd set to foreground with debug send to stderr
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/pcscdaemon.c:389:main() pcscd set to foreground with debug send to stderr
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/pcscdaemon.c:389:main() pcscd set to foreground with debug send to stderr
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/pcscdaemon.c:585:main() pcsc-lite 1.4.0 daemon ready.
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/readerfactory.c:780:RFInitializeReader() Attempting startup of Aktiv Rutoken ECP 00 00 using
/SourceCache/SmartCardServices_Executables/SmartCardServices-55105/src/PCSC/readerfactory.c:506:RFBindFunctions() Binding driver functions
```

Рис. 10. Отладочный лог для Mac OC X

2.2.2 Установка библиотеки на MAC OC X для работы «Рутокен ЭЦП 2.0» в системе «iBank 2»

Для работы «Рутокен ЭЦП 2.0» в системе «iBank 2» на MAC OC X необходимо установить кроссплатформенную библиотеку rtPKCS11ECP, работающую с RSA и ГОСТ-алгоритмами. Для этого:

1. Получите библиотеку с сайта разработчика «Рутокен ЭЦП 2.0» компании ЗАО «Актив-софт»: Библиотека rtPKCS11ecp для MAC OC X.
2. Поместите файл librtpkcs11ecp.dylib в каталог /Users/bifit/Library/Java/Extensions/ (если его нет, необходимо создать каталог /Java/Extensions/) .

3 Работа с «Рутокен ЭЦП 2.0»

3.1 Требования к эксплуатации

«Рутокен ЭЦП 2.0» 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:

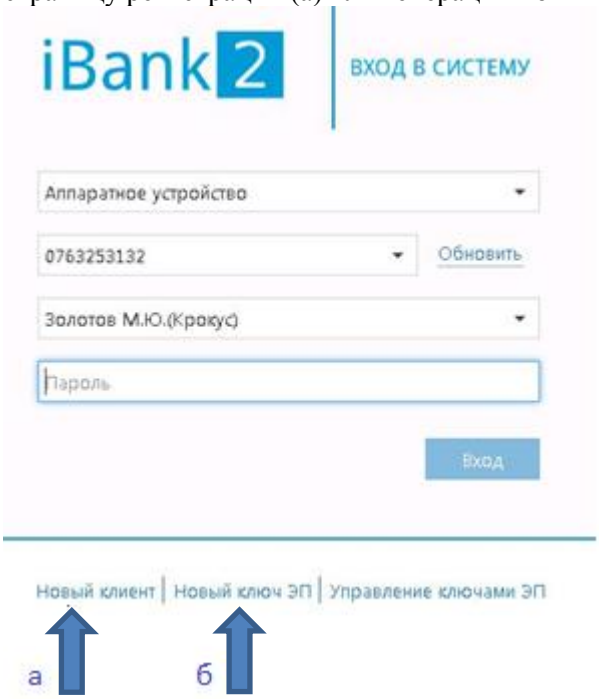
- Оберегайте устройство от механических воздействий (ударов, падения, сотрясения, вибрации и т. п.), от воздействия высоких и низких температур, агрессивных сред, высокого напряжения.
- Не прилагайте излишних усилий при подсоединении устройства к порту компьютера.
- Не допускайте попадания на устройство (особенно на его разъем) пыли, грязи, влаги и т. п. При засорении разъема примите меры для его очистки. 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 2.0» 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 2.0» 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 2.0» 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 2.0» подключенным к компьютеру, когда он не используется.
- В случае неисправности или неправильного функционирования «Рутокен ЭЦП 2.0» обращайтесь в отделение банка по месту обслуживания.

Внимание!

• Не передавайте «Рутокен ЭЦП 2.0» третьим лицам! Не сообщайте третьим лицам пароли от ключей электронной подписи!
• Подключайте «Рутокен ЭЦП 2.0» к компьютеру только на время работы с системой «iBank 2».
• В случае утери (хищения) или повреждения «Рутокен ЭЦП 2.0» немедленно обратитесь в отделение банка по месту обслуживания.

3.2 Использование «Рутокен ЭЦП 2.0» при регистрации/генерации новых ключей ЭП в системе «iBank 2»

1. Для регистрации подключитесь к Интернету, запустите Web-браузер и перейдите на страницу регистрации (а) или генерации новых ключей ЭП (б).



2. Подключите «Рутокен ЭЦП 2.0» к USB-порту компьютера.

3. Пройдите все этапы регистрации. На восьмом шаге в качестве Хранилища ключей выберите из списка пункт **Аппаратное устройство** (см. рис. 11, рис. 12).

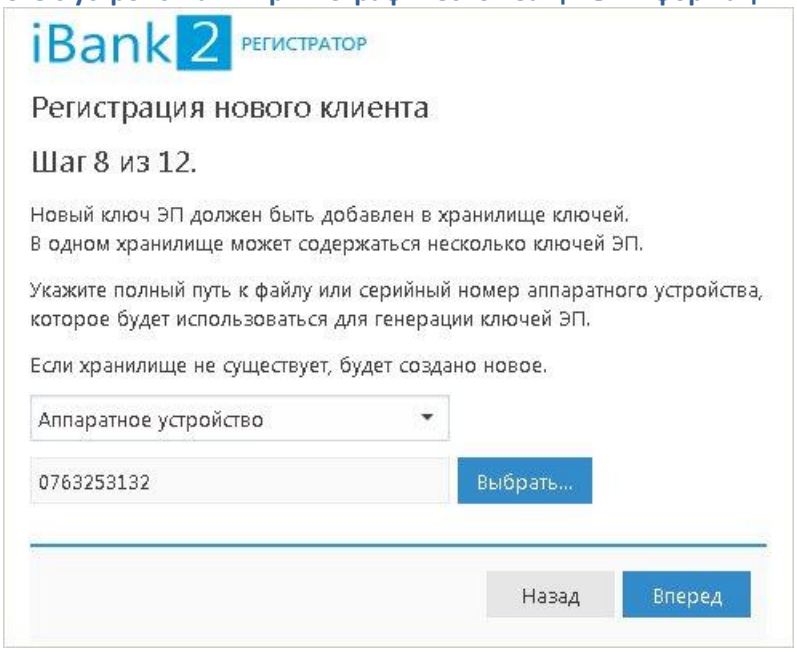


Рис. 11. «Internet-Банкинг для корпоративных клиентов (web)». Предварительная регистрация. Шаг 8 из 12

На следующих шагах регистрации вам необходимо указать наименование и пароль к создаваемому ключу ЭП.

Примечание:

Внимание!

Для того чтобы ваш пароль был безопасным:

• 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.

Внимание!

Неправильно указать пароль к ключу ЭП, который находится в памяти «Рутокен ЭЦП 2.0», можно не более 15 раз подряд. После этого ключ ЭП блокируется навсегда.

3.3 Администрирование ключей ЭП

Порядок действий по управлению ключами ЭП, хранящимися в памяти «Рутокен ЭЦП 2.0»:

а. Перейдите на страницу **Вход в сервис** (см. рис. 14) и нажмите кнопку **Управление ключами ЭП**. Откроется страница **Регистратор. Администрирование ключей ЭП**.

Рис. 14. Вход в сервис

б. Укажите тип хранилища ключей ЭП **Аппаратное устройство**.

в. В поле выбора аппаратных устройств отобразится серийный номер подключенного к компьютеру устройства. При необходимости вы можете выбрать другое подключенное устройство, нажав кнопку **Выбрать**. Под серийным номером отобразится список ключей ЭП (см. рис. 15).

г. Выберите ключ ЭП.

д. Выберите необходимое действие, нажав соответствующую кнопку (возможные действия с ключами ЭП см. в разделе Администрирование ключей ЭП).

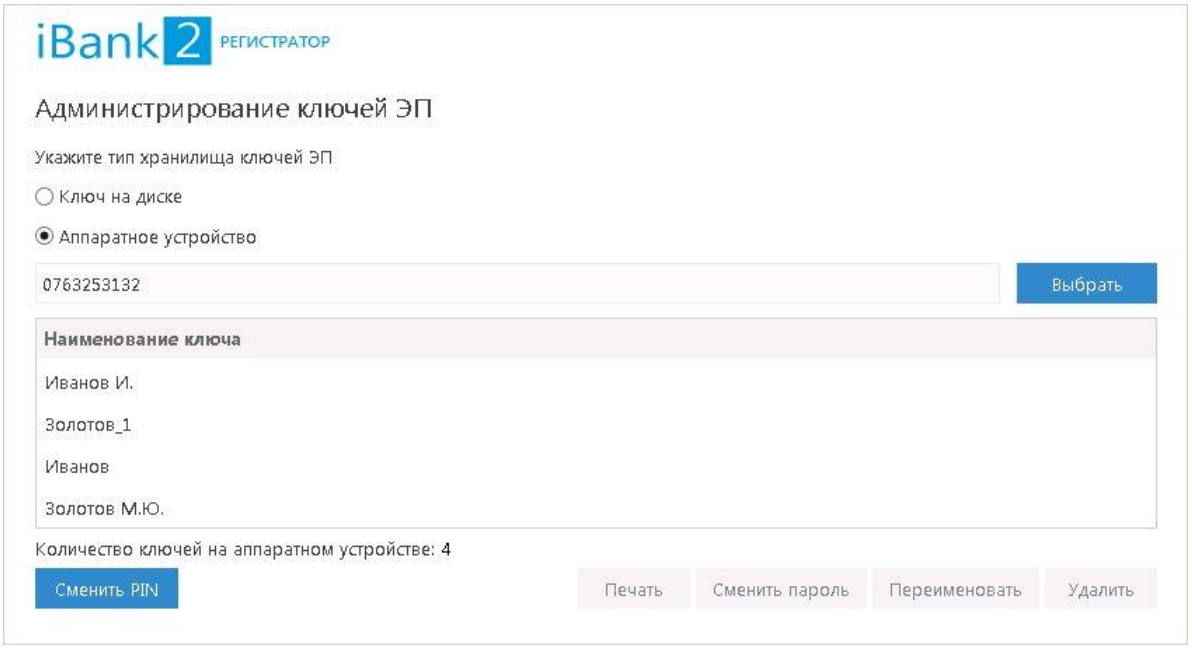


Рис. 15. Регистратор. Администрирование ключей ЭП

Возможны следующие действия с ключами ЭП:

- Печать сертификата ключа проверки ЭП
- Смена пароля для доступа к ключу ЭП
- Смена наименования ключа ЭП
- Удаление ключа ЭП

Внимание!
Задание и смена PIN-кода устройства осуществляется через **Панель управления «Рутокен ЭЦП 2.0»**, которая устанавливается вместе с драйвером устройства. При попытке сменить PIN-код устройства из системы «iBank 2» выдается соответствующее предупреждение.

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** (частные клиенты – кнопку **Экспортировать в RTF**). Далее откроется стандартное окно вывода документа на печать.

Смена пароля для 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** (частные клиенты – кнопку **Сменить пароль**). 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 памяти «Рутокен ЭЦП 2.0», 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 ЭП будет безвозвратно удален из Хранилища.

4. Администрирование устройств «Рутокен ЭЦП 2.0»

Администрирование «Рутокен ЭЦП 2.0» осуществляется через **Панель управления «Рутокен ЭЦП 2.0»**, которая устанавливается вместе с драйвером устройства.

Возможны следующие действия с «Рутокен ЭЦП 2.0»:

- Задание PIN-кода доступа
- Настройки политик безопасности PIN-кодов
- Разблокировка PIN-кода

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

По умолчанию для «Рутокен ЭЦП 2.0» установлены следующие значения PIN-кодов:

Пользователь: 12345678
Администратор: 87654321

Задание PIN-кода доступа к «Рутокен ЭЦП 2.0»:

Для обеспечения дополнительной защиты от несанкционированного доступа к ключам ЭП, хранящимся на «Рутокен ЭЦП 2.0», реализована возможность задавать PIN-код доступа к «Рутокен ЭЦП 2.0».
При обращении к «Рутокен ЭЦП 2.0» с заданным PIN-кодом отсутствует возможность получения списка ключей «Рутокен ЭЦП 2.0» и каких-либо действий с ними, до момента ввода корректного PIN-кода.
PIN-код к «Рутокен ЭЦП 2.0», если он установлен, запрашивается у пользователя при выполнении следующих действий:

- аутентификация в системе iBank2;
- обращение к «Рутокен ЭЦП 2.0» в случае его отключения и последующего подключения;
- обращение к «Рутокен ЭЦП 2.0» в ходе администрирования ключей ЭП;
- подпись документов во время работы в системе iBank2.

Задание PIN-кода устройства осуществляется через **Панель управления Рутокен**, которая устанавливается вместе с драйвером устройства.
Запуск панели управления можно осуществить, например через **Пуск/Программы/Rutoken/Панель управления Рутокен**. Откроется главное окно программы (см. рис. 18).

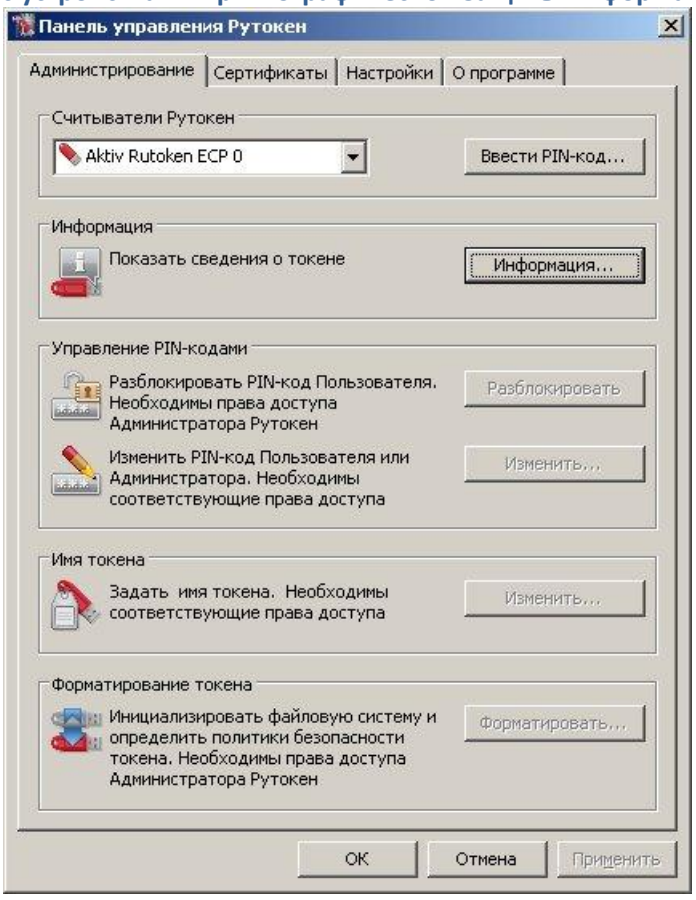


Рис. 18. Панель управления Рутокен. Закладка Администрирование

Для аутентификации в программе нажмите кнопку **Ввести PIN-код...** В открывшемся окне (см. рис. 19) выберите тип пользователя, под которым необходимо работать, укажите значение PIN-кода и нажмите кнопку **ОК**.

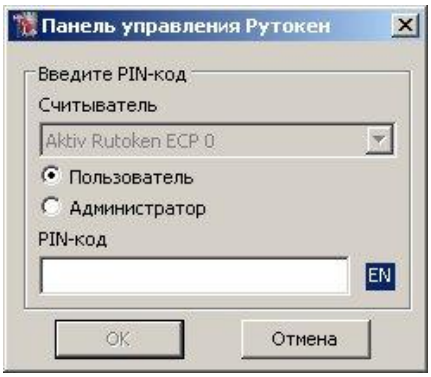


Рис. 19. Панель управления Рутокен

Для смены PIN-кода в блоке **Управление PIN-кодами** нажмите кнопку **Изменить...** В открывшемся окне дважды укажите новое значение PIN-кода (см. рис. 20).
Значение PIN-кода должно соответствовать политикам безопасности.

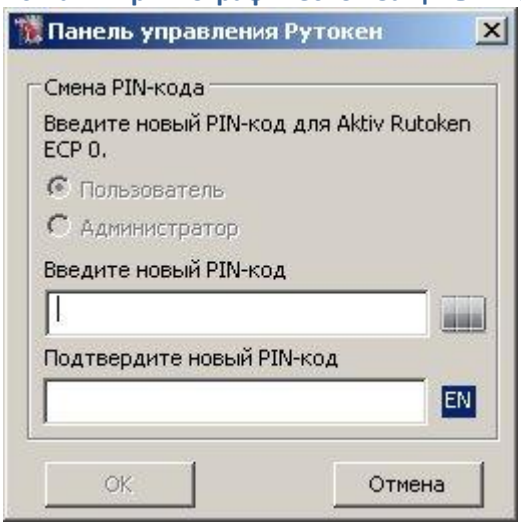


Рис. 20. Панель управления Рутокен

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

Внимание!

Неправильно ввести PIN-код доступа к «Рутокен ЭЦП 2.0» можно не более 9 раз подряд. После этого «Рутокен ЭЦП 2.0» блокируется для использования и его может разблокировать пользователь с правами администратора.

Настройки политик безопасности PIN-кодов

Политики контроля качества PIN-кодов «Рутокен ЭЦП 2.0» используются для повышения уровня информационной безопасности.

По уровню надежности все PIN-коды «Рутокен ЭЦП 2.0» 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 2.0» 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 2.0» 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 2.0» 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. 21.

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

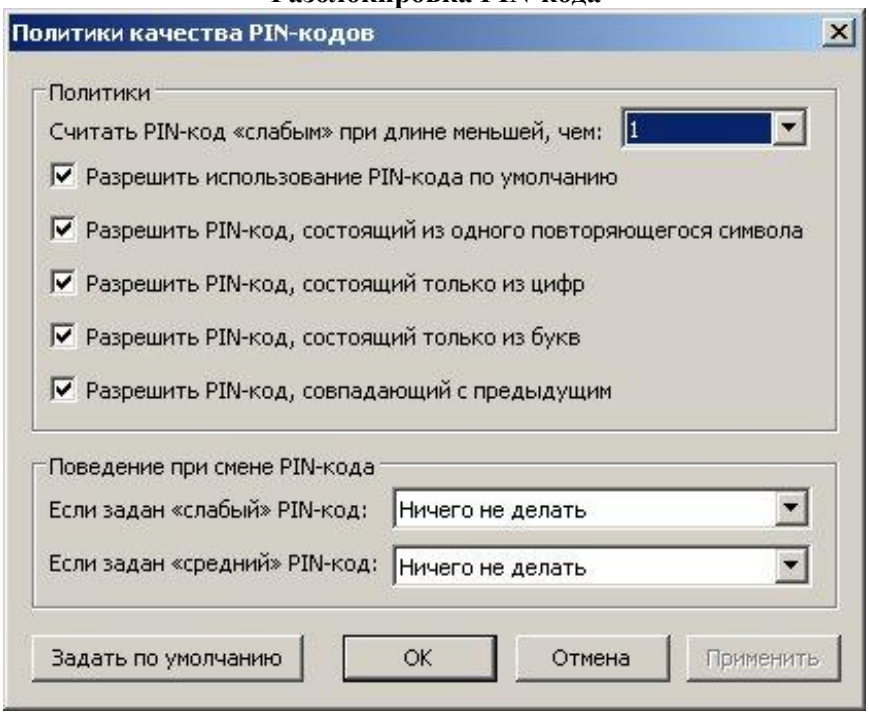


Рис. 21. Политики качества PIN-кодов

Разблокирование PIN-кода пользователя «Рутокен ЭЦП 2.0» 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. 20) 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 значение PIN-кода. Если сделать это не удается, то можно лишь отформатировать «Рутокен ЭЦП 2.0» с потерей всей информации на нем.

Форматирование «Рутокен ЭЦП 2.0»

Внимание!

Форматирование «Рутокен ЭЦП 2.0» приводит к потере всей информации на нем!
Удаленная информация восстановлению не подлежит!

Для форматирования устройства запустите **Панель управления Рутокена**. На закладке **Администрирование** (см. рис. 20) 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. 22).

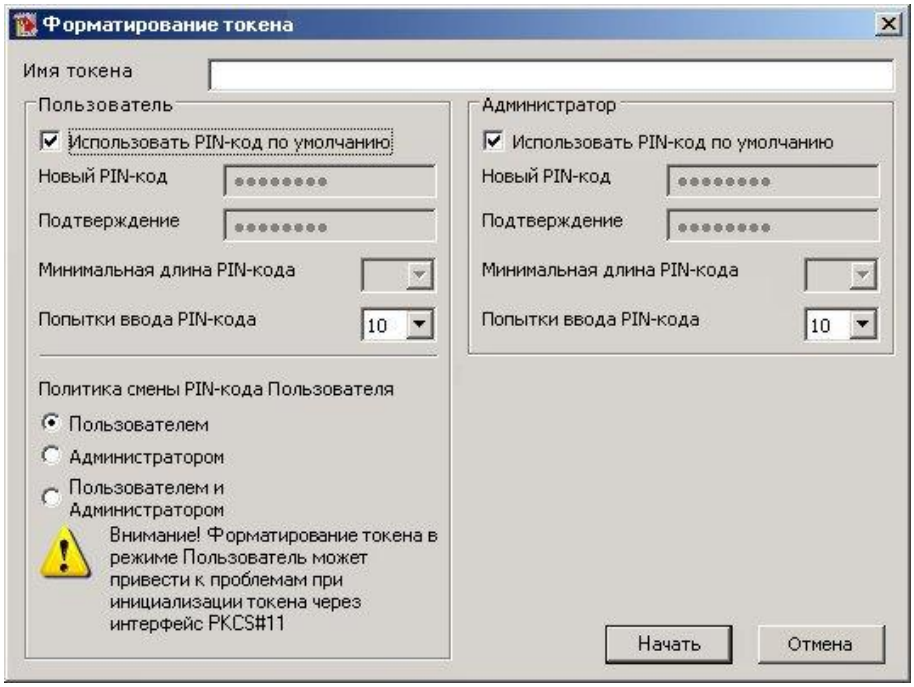


Рис. 22. Форматирование токена

Для продолжения подтвердите свои намерения (см. рис. 23).

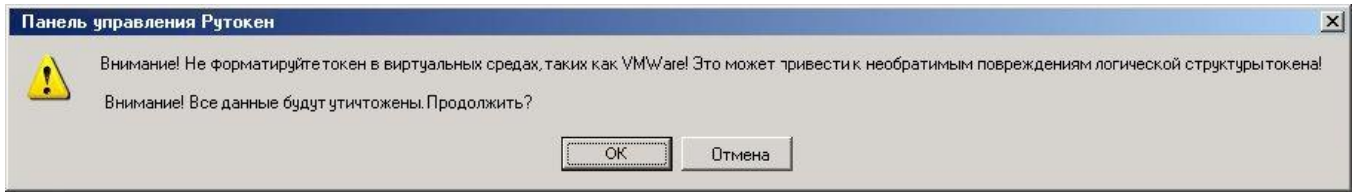


Рис. 23. Предупреждение

Дождитесь окончания форматирования (см. рис. 24 - 25).

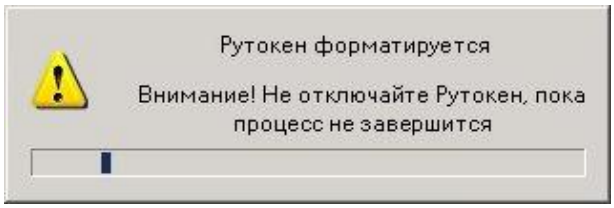


Рис. 24. Предупреждение

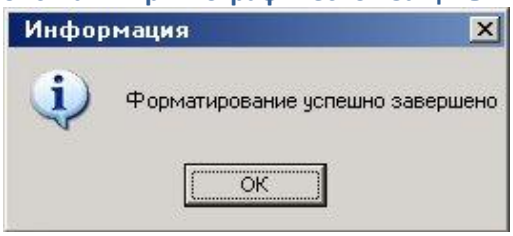


Рис. 25. Предупреждение

Внимание!

Если операция форматирования «Рутокен ЭЦП 2.0» не будет завершена («Рутокен ЭЦП 2.0» 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 2.0» самостоятельно. После исчерпания попыток ввода корректного PIN-кода администратора кнопка **Форматировать** становится доступной.

5. Использование «Рутокен ЭЦП 2.0» при авторизации в системе «iBank 2»

а. Зайдите на сайт системы iBank2 https://ibank2.mosoblbank.ru/ibank2/ и подключите «Рутокен ЭЦП 2.0» к USB-порту компьютера.
б. Первое окно АРМ, **Вход в систему**, предназначенное для аутентификации пользователя, представлено на рис. 26.

Рис. 26. Вход в систему

В этом окне необходимо выполнить следующие действия:

- В поле **Тип хранилища** выберите **Аппаратное устройство**. В поле **Идентификатор** отобразится серийный номер выбранного устройства.
- Из списка поля **Ключ** выберите наименование ключа ЭП. Укажите пароль для доступа к

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

• Для входа в систему нажмите кнопку **Вход**.

6. Использование «Рутокен ЭЦП 2.0» при подписи документов

При подписи документа «Рутокен ЭЦП 2.0» с ключами ЭП должен быть подключен к компьютеру.

После выбора операции подписи для документа, подпись которого производится с помощью «Рутокен ЭЦП 2.0», откроется окно **Предупреждение** (см. рис. 27).

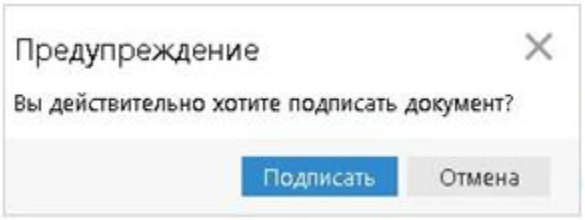


Рис. 27. Предупреждение

Нажмите кнопку **Подписать**.

7. Обновление драйверов «Рутокен ЭЦП 2.0» для Windows

Перед началом обновления драйверов рекомендуется отключить «Рутокен ЭЦП 2.0» 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/XP/2003

Запустите загруженный файл и следуйте указаниям мастера установки (см. рис. 29 – 31).

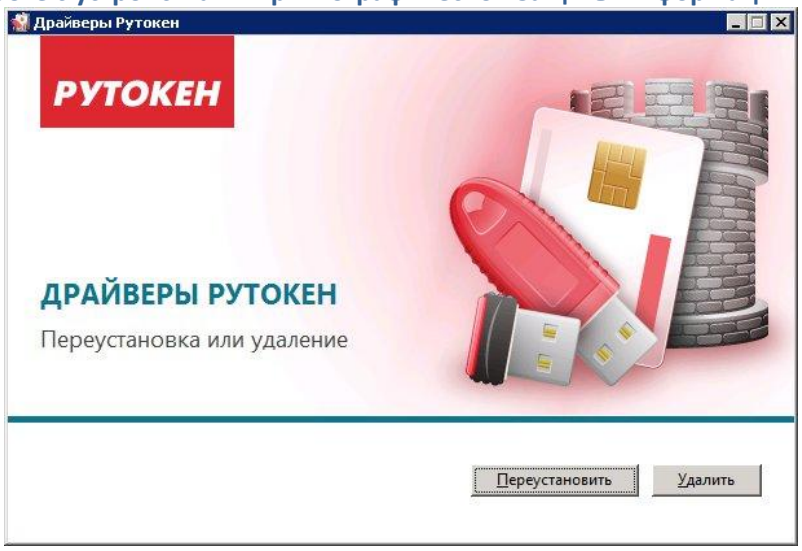


Рис. 29. Мастер установки драйвера

Для переустановки драйвера нажмите кнопку **Переустановить**, для удаления драйвера с компьютера кнопку **Удалить**.
Далее необходимо дождаться окончания установки драйвера (см. рис. 30)

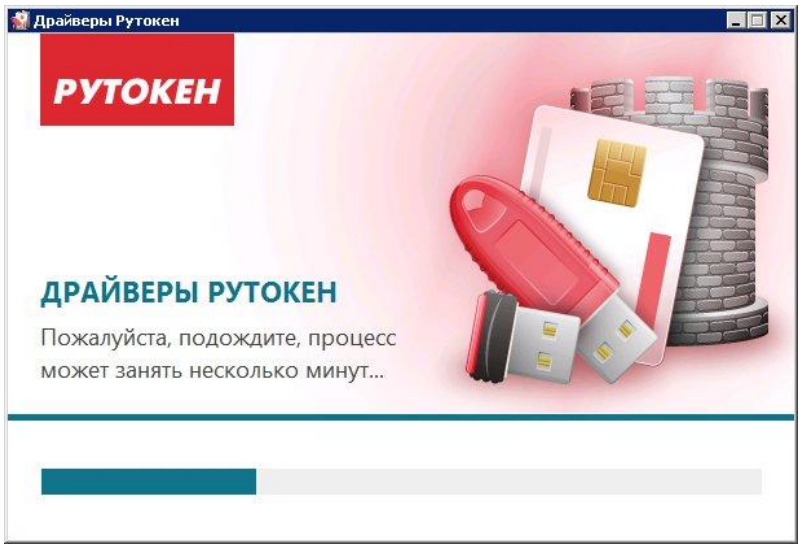


Рис. 30. Мастер установки драйвера

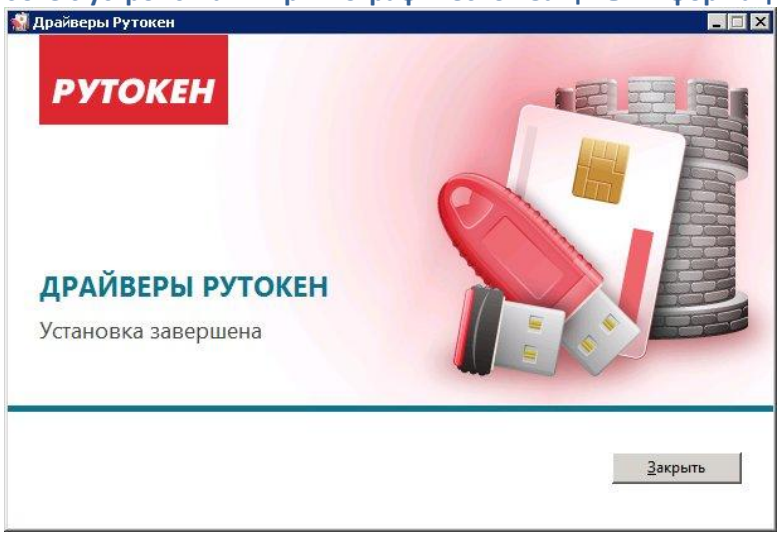


Рис. 31. Мастер установки драйвера

и нажать кнопку **Закрыть** (см. рис. 31).