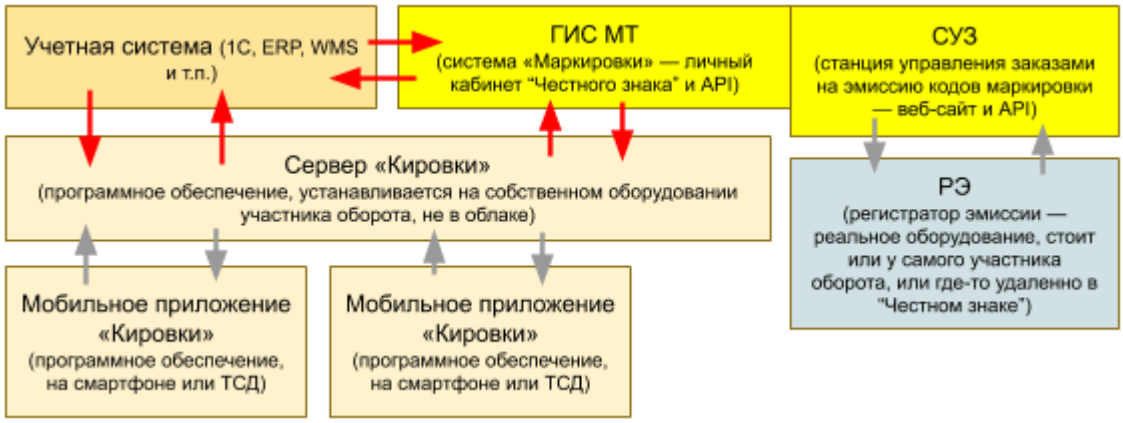
Архитектура системы и варианты развертывания «Кировки» для маркировки обуви

Последние изменения: 2024-03-26

Перед тем как начать работать с «Кировкой». необходимо настроить обмен данных с ГИС МТ и СУЗ. Такой обмен может быть нескольких видов:

- Обмен «Кировки» с ГИС МТ. В таком случае, коды маркировки можно заказывать и вводить в оборот прямо в приложении на мобильном устройстве.
- Обмен «Кировки» с учетной системой, которая затем обменивается с системой маркировки.
- Смешанный вариант.

Общая структура обмена «Кировки» с ГИС МТ



Учетная система — предназначена для хранения и обработки данных, а также для обмена ими с мобильным устройством пользователя.

ГИС МТ (государственная информационная система маркировки товаров) — система мониторинга товаров, куда заносятся данные по товарам и заказываются КМ. Для работы с данной системой необходимо иметь личный кабинет пользователя.

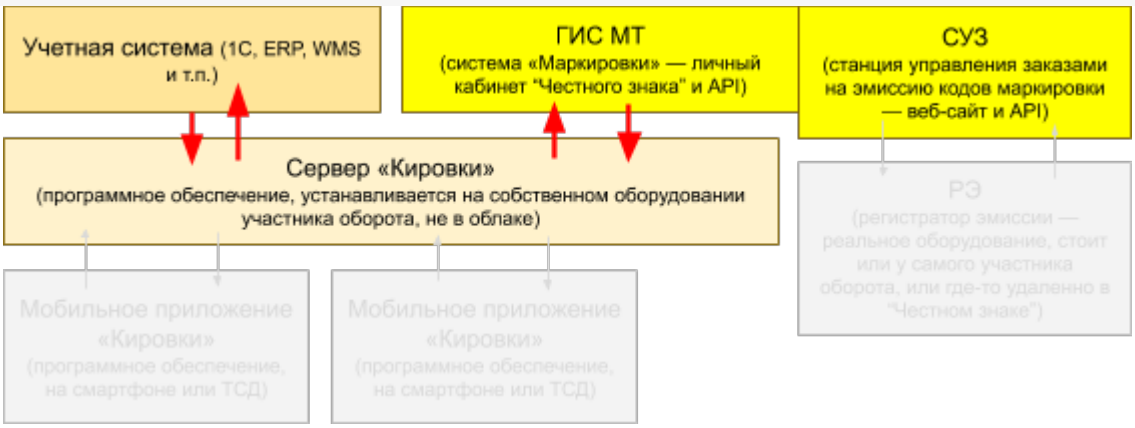
СУЗ — станция управления заказами КМ.

РЭ (регистратор эмиссии) — устройство для заказа КМ и регистрации сведений о маркированных товарах. Участникам оборота, которые не производят и не импортируют обувь, вместо физического РЭ предоставляется доступ к облачному.

Сервер «Кировки» (также сервер Mobile SMARTS) — программное обеспечение, которое должно быть установлено на ПК пользователя.

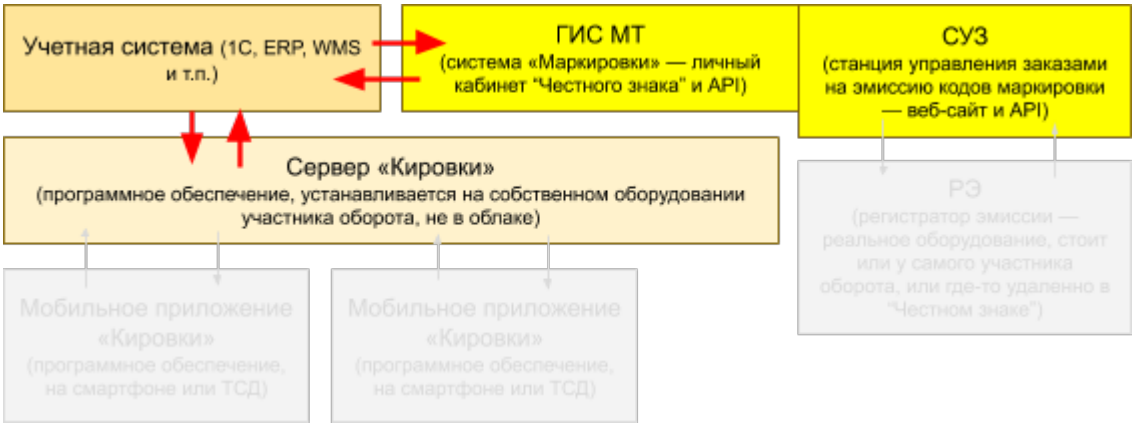
Мобильное приложение «Кировки» — ПО, устанавливается на мобильное устройство (ТСД) пользователя и подключается к базе «Кировки», с которой затем происходит работа.

Вариант самостоятельного обмена «Кировки» с ГИС МТ



В случае если «Кировка» сама обменивается с «Честным знаком», то серверу «Кировка» необходим доступ к ключу КЭП для электронной подписи документов.

Вариант обмена «Кировки» только с учетной системой



Также возможен смешанный вариант обмена, включающий в себя черты предыдущих. Например, можно заказывать коды маркировки в учетной системе, а после этого передавать их в «Кировку» для печати и ввода в оборот.

Варианты развертывания «Кировки»

Для корректной работы системы нужен сервер, к которому подключен КЭП (электронная подпись для маркировки товаров), и комплект «Кировки», который включает в себя мобильное устройство, принтер и ПО «Кировка». В условиях постоянного доступа к сети Интернет, такой комплект будет работать из любой точки мира.

Основные варианты развертывания системы:

1. Централизованное развертывание с доступом со всего мира

   При таком варианте используется установленный сервер «Кировки» в дата-центре с КЭП, подключенным через USB-порт, а также комплект «Кировки» в любой точке мира с доступом в интернет.

   Удобство данного способа заключается в том, за рубежом не находится никаких серверов, только мобильный комплект.

2. Переносной вариант развертывания

   В таком случае необходим сервер «Кировки» — ноутбук с КЭП и возможностью доступа в Интернет для обмена с ГИС МТ, а также комплект «Кировки» с доступом в интернет.

   Этот вариант удобен своей мобильностью и возможностью работать в любом месте и условиях.

Не нашли что искали?

Задать вопрос в техническую поддержку

Автообновление платформы Mobile SMARTS и продуктов на её основе

Последние изменения: 2024-03-26

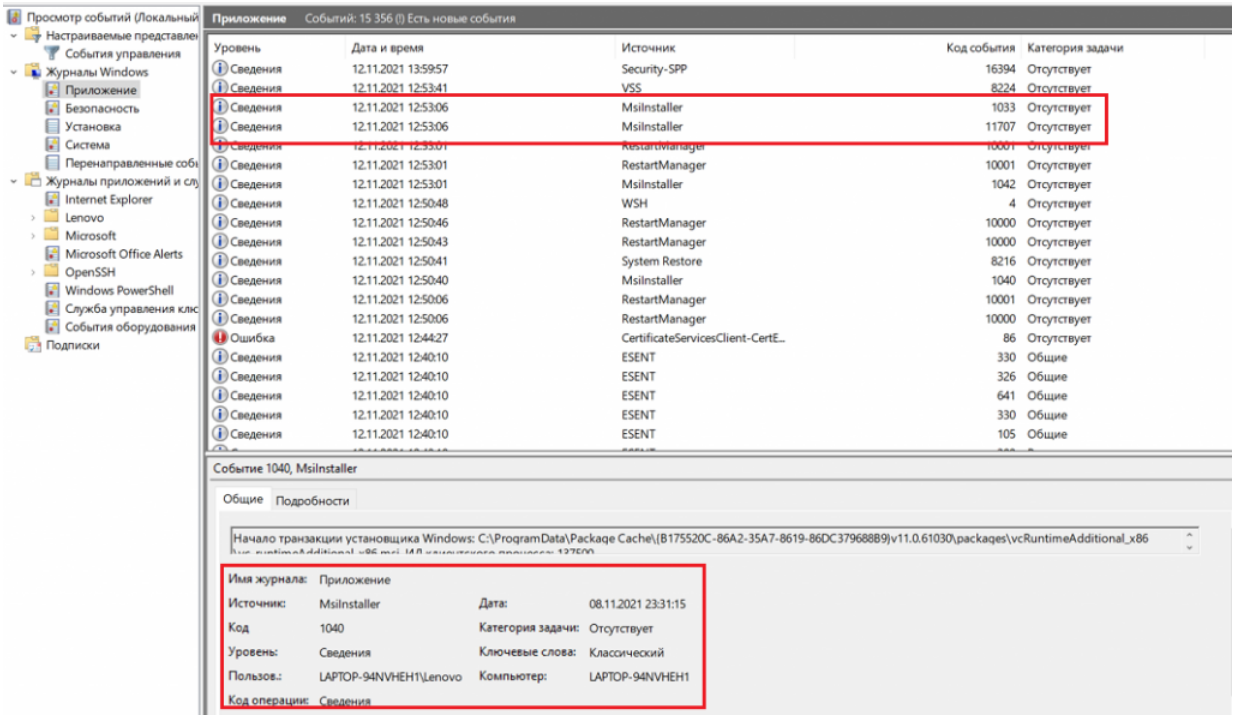
В платформу Mobile SMARTS заложена возможность автоматического обновления самой платформы и продуктов на ее основе. Это позволяет пользователю не следить за выходом обновлений Mobile SMARTS, но при этом всегда вовремя переходить на последнюю версию ПО с новым функционалом и исправленными багами прошлых релизов. Данная функция работает только для баз Mobile SMARTS, установленных на локальных ПК и не использующих облачный обмен.

Автообновление Mobile SMARTS не означает, что база или платформа обновляются втайне от пользователя. Подразумевается, что компетентному сотруднику на ПК с установленной платформой приходит автоматическое уведомление о том, что «Клеверенс» выпустил новую версию обеспечения, и далее пользователь должен самостоятельно скачать и установить её под полным своим контролем.

Обновляются ли программы «Клеверенс» самостоятельно в фоне?

Нет, программы от «Клеверенс» самостоятельно в фоне не обновляются, во всех случаях нужен компетентный сотрудник, который нажмет на уведомление о доступном обновлении, скачает обновление и установит его вручную.

С помощью журнала событий Windows можно проверить, кто и когда произвел обновление Mobile SMARTS, т.к. «MsiInstaller» вносит новую запись в журнал после завершения установки.

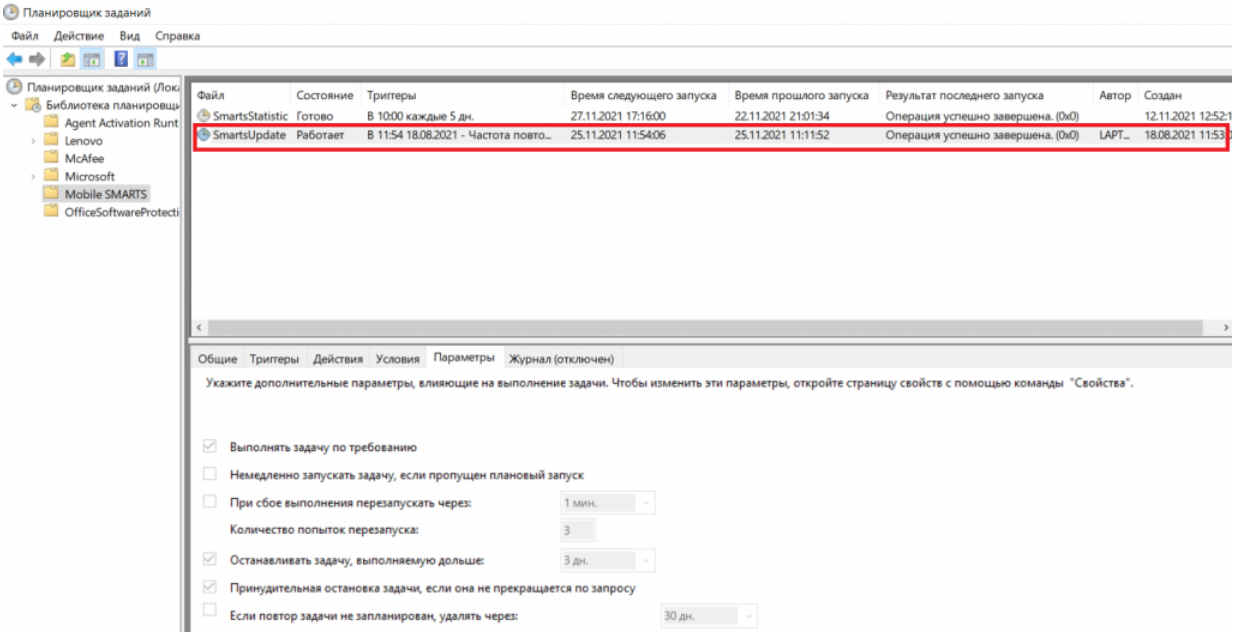


Как и когда происходит автообновление баз Mobile SMARTS

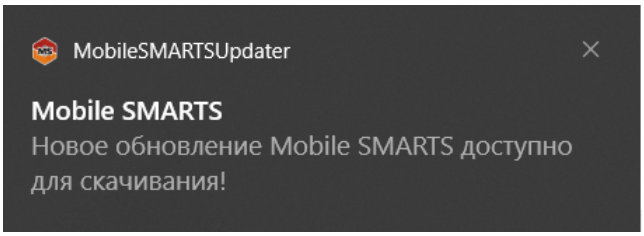
> Базы Mobile SMARTS — это по сути экземпляры установленных продуктов от «Клеверенса» («Магазин 15», «Склад 15» и т. д.).

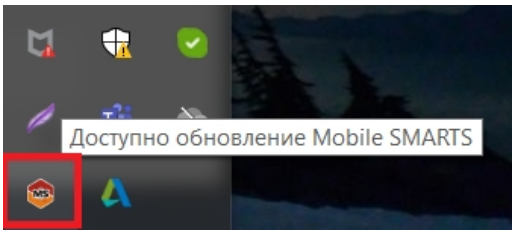
При установке платформы Mobile SMARTS на ПК в планировщик заданий Windows добавляется задача «SmartsUpdate», регулярно запускающая приложение «MobileSMARTSUpdater.exe» (путь по умолчанию «C:\Program Files (x86)\Cleverence Soft\Mobile SMARTS\AppsManager\MobileSMARTSUpdater.exe»), которое проверяет наличие обновлений Mobile SMARTS на сайте «Клеверенса». По умолчанию данная проверка

происходит каждые 4 часа. Некоторые параметры данного задания можно настраивать самостоятельно (например, запускать его по требованию, не дожидаясь пока пройдут очередные 4 часа).

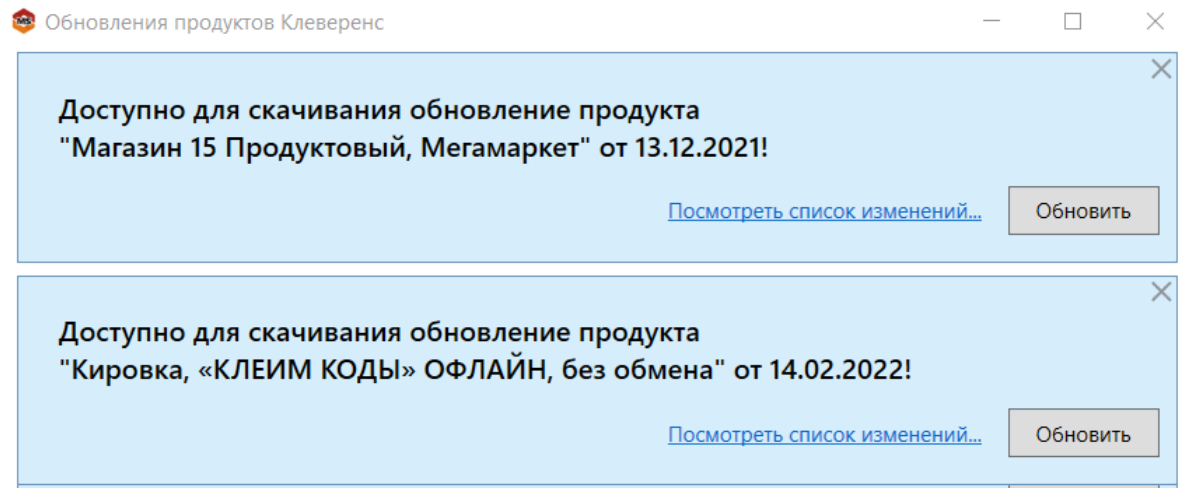


Если в результате такой проверки окажется, что на сайте «Клеверенса» (раздел «Загрузки») появилась новая версия продукта, на экране ПК отобразится соответствующее сообщение, а в области уведомлений появится иконка Mobile SMARTS.





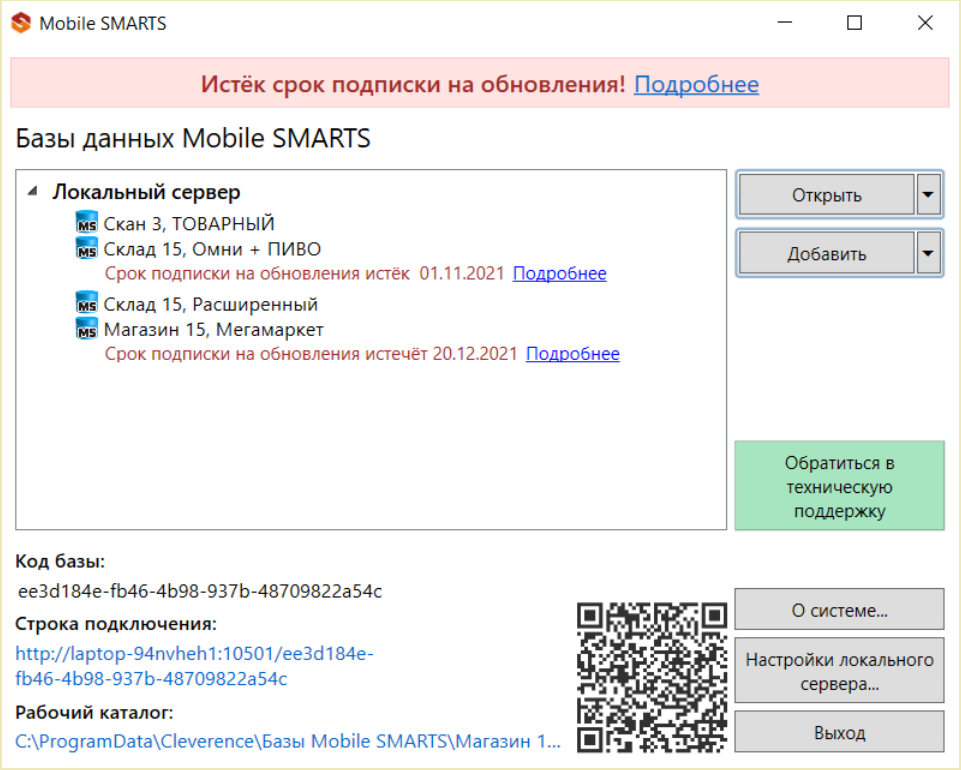
При нажатии на уведомление или иконку откроется окно со списком доступных обновлений для баз Mobile SMARTS, установленных на данном ПК. Обновления продуктов отмечаются синим цветом.



> Если вы используете файрвол (сетевой фильтр, шлюз безопасности, брандмауэр), то для получения обновлений Mobile SMARTS (для баз и мобильного приложения) потребуется открыть порты 80 и 443 для адреса 138.201.29.215.

После этого вы можете скачать файл обновления для нужного продукта с помощью кнопки «Обновить» и установить его на ПК.

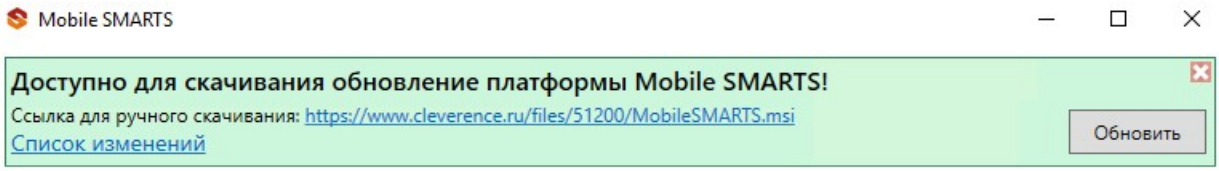
Для того, чтобы новые версии Mobile SMARTS были доступны для скачивания, необходимо иметь активную подписку на обновления. В противном случае обновления будут недоступны. Информация о текущем состоянии подписки на обновления отображается в менеджере баз и в менеджере лицензий.



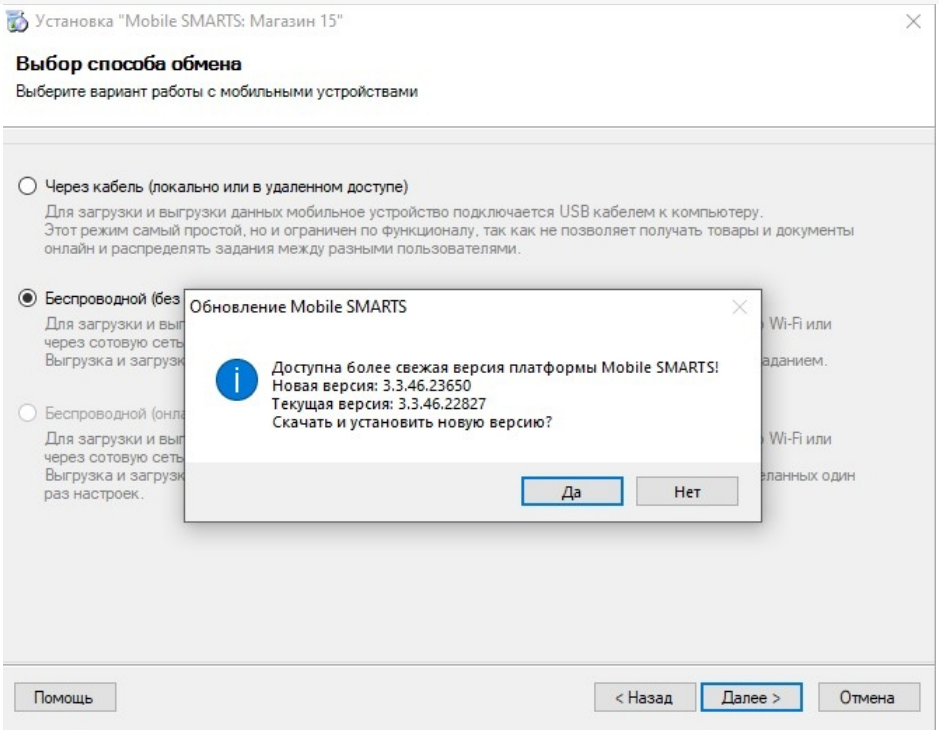
Как и когда происходит автообновление платформы Mobile SMARTS

Проверка наличия доступных обновлений для самой платформы Mobile SMARTS происходит по тому же сценарию, что и для баз, немного отличаются только цвет уведомления и выводимая информация.

После того как обновление платформы будет обнаружено, вы можете скачать его и установить на ПК.



Также предложение об установке более свежей версии платформы отображается при установке базы на предыдущую версию платформы.



Как и когда происходит обновление мобильного приложения Mobile SMARTS

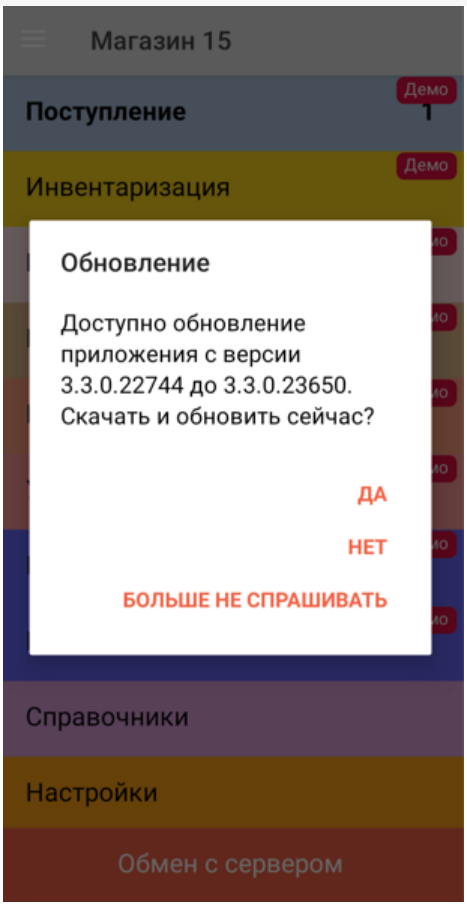
Для устройств с ОС Win Mobile (CE)

Мобильное устройство на ОС Win Mobile (CE) проверяет наличие обновлений на приложение Mobile SMARTS при каждом обмене с сервером Mobile SMARTS. Если ранее на ПК было установлено обновление платформы с более новой версией клиента Mobile SMARTS, то при подключении мобильного устройства к серверу будет предложено обновить приложение Mobile SMARTS (подробнее в статье «Автоматическое обновление клиента на ТСД по Wi-Fi»).

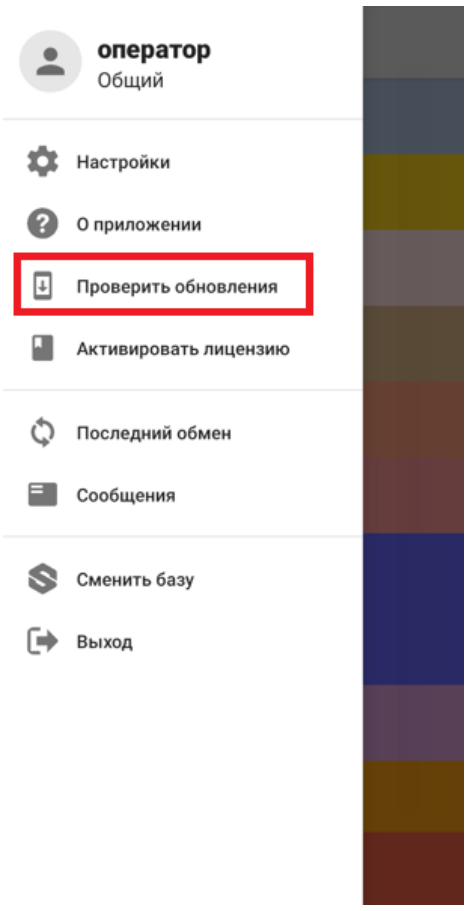
Для устройств с ОС Android

Обновление клиентского приложения Mobile SMARTS на устройстве с ОС Android происходит несколькими способами:

- клиент проверяет наличие новой версии приложения на сайте «Клеверенса» и, если оно там есть, на экран ТСД выводится соответствующее сообщение:



- **пользователь может самостоятельно проверить наличие обновлений с помощью пункта меню «Проверить обновления»;**



- **пользователь может самостоятельно обновить приложение из Play Market.**

Не нашли что искали?

Задать вопрос в техническую поддержку

Виртуализация ключа КЭП USB для подписи документов сервером Mobile SMARTS

Последние изменения: 2024-03-26

Иногда нет возможности подключить ключ КЭП непосредственно к USB-порту ПК, на котором расположен сервер «Кировки». В этом случае на помощь приходит ПО для доступа и использования USB через интернет или локальную сеть.

Что для этого нужно:

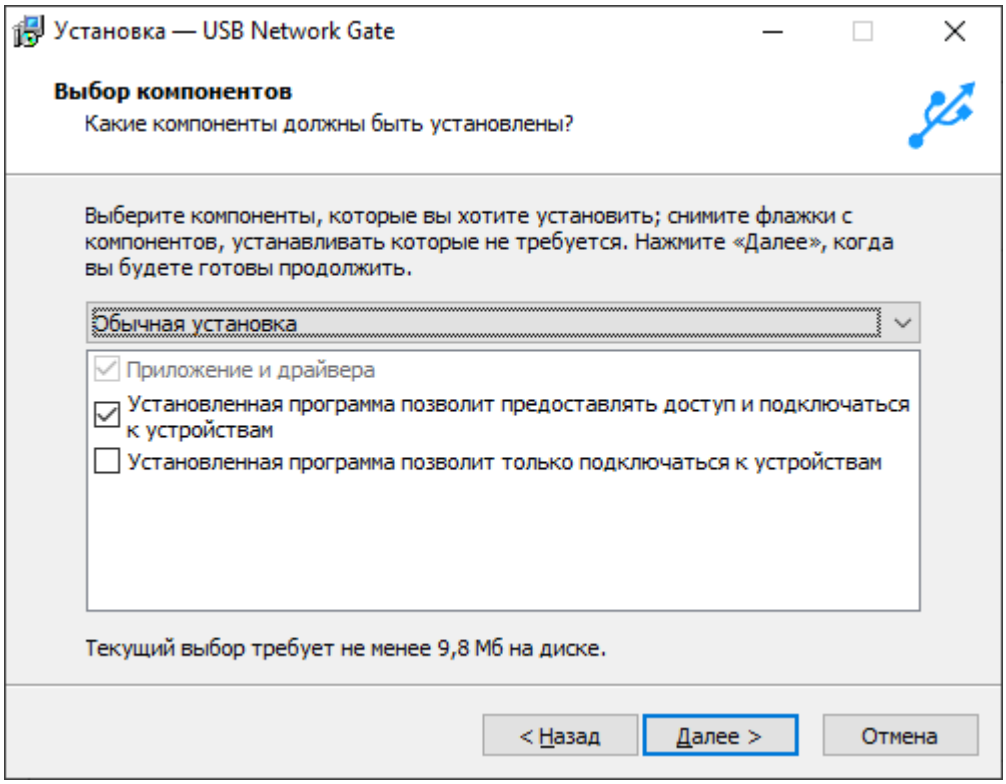
1. **ПО для для совместного использования USB посредством сети.**
2. **ПК-1, подключённый к локальной сети или интернет, с USB-портом, в который вставлен ключ КЭП.**
3. **ПК-2, на котором планируется работа сервера «Кировки», подключённый к той же сети, что и ПК-1.**

При написании этой статьи использовался USB Network Gate, но это может быть любое другое ПО со схожими функциями.

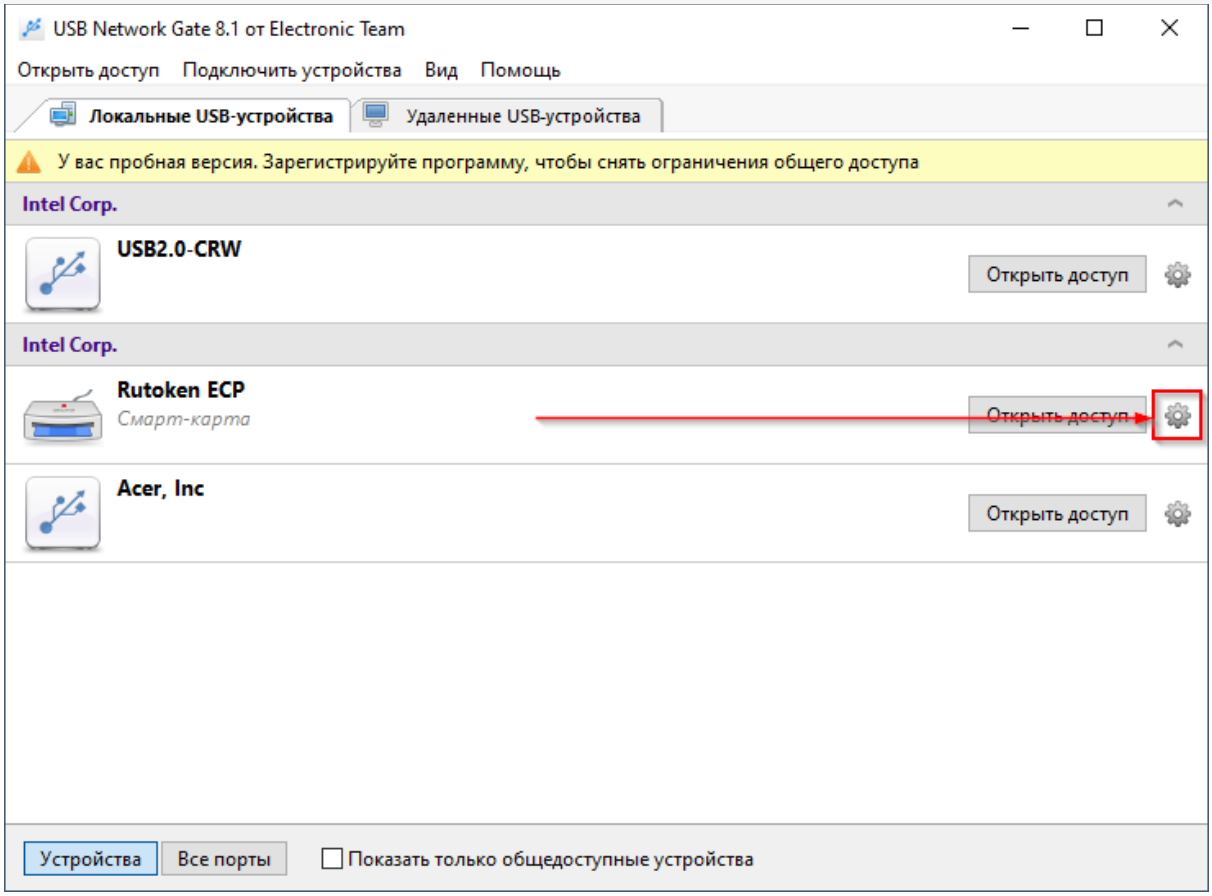
Установка ПО и настройки на ПК-1

Ключ КЭП должен быть вставлен в USB-порт.

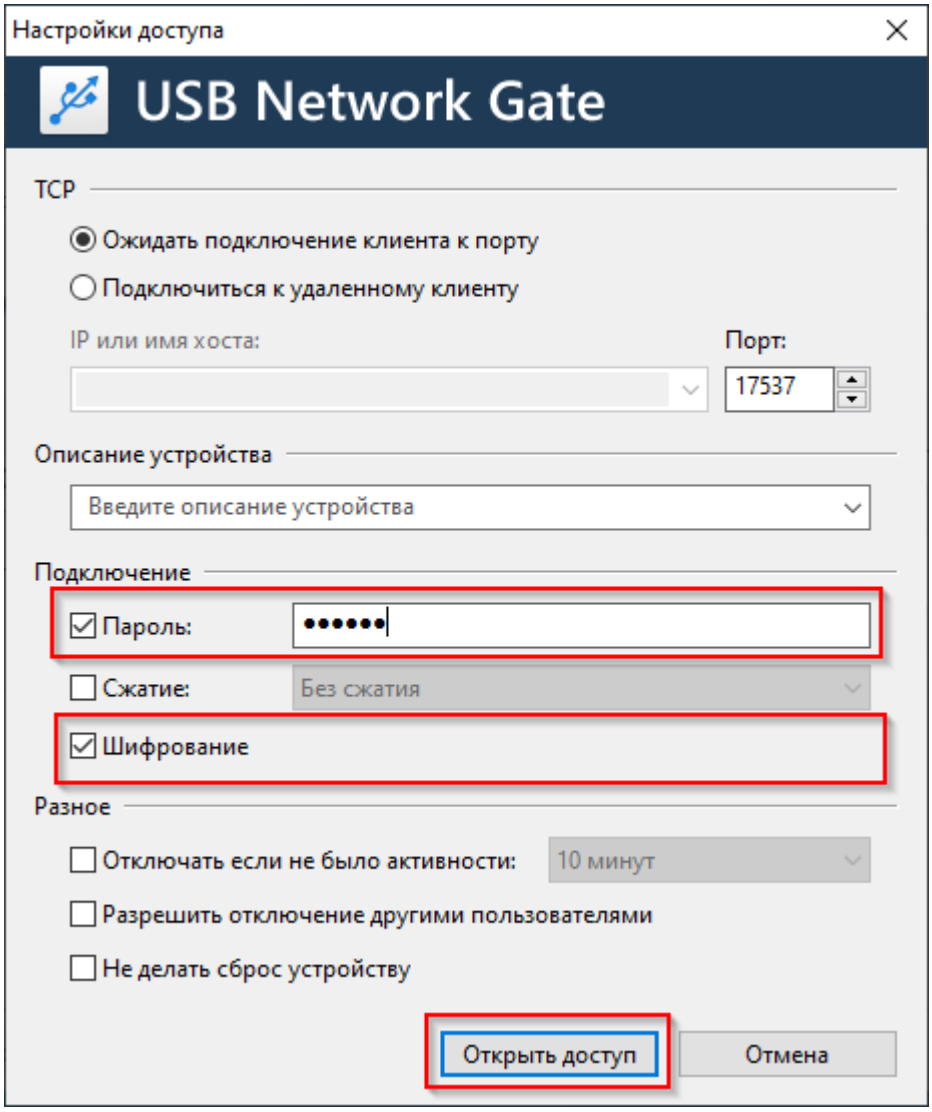
1. **Скачиваем и устанавливаем USB Network Gate, при установке выбираем вариант «Обычная установка»:**



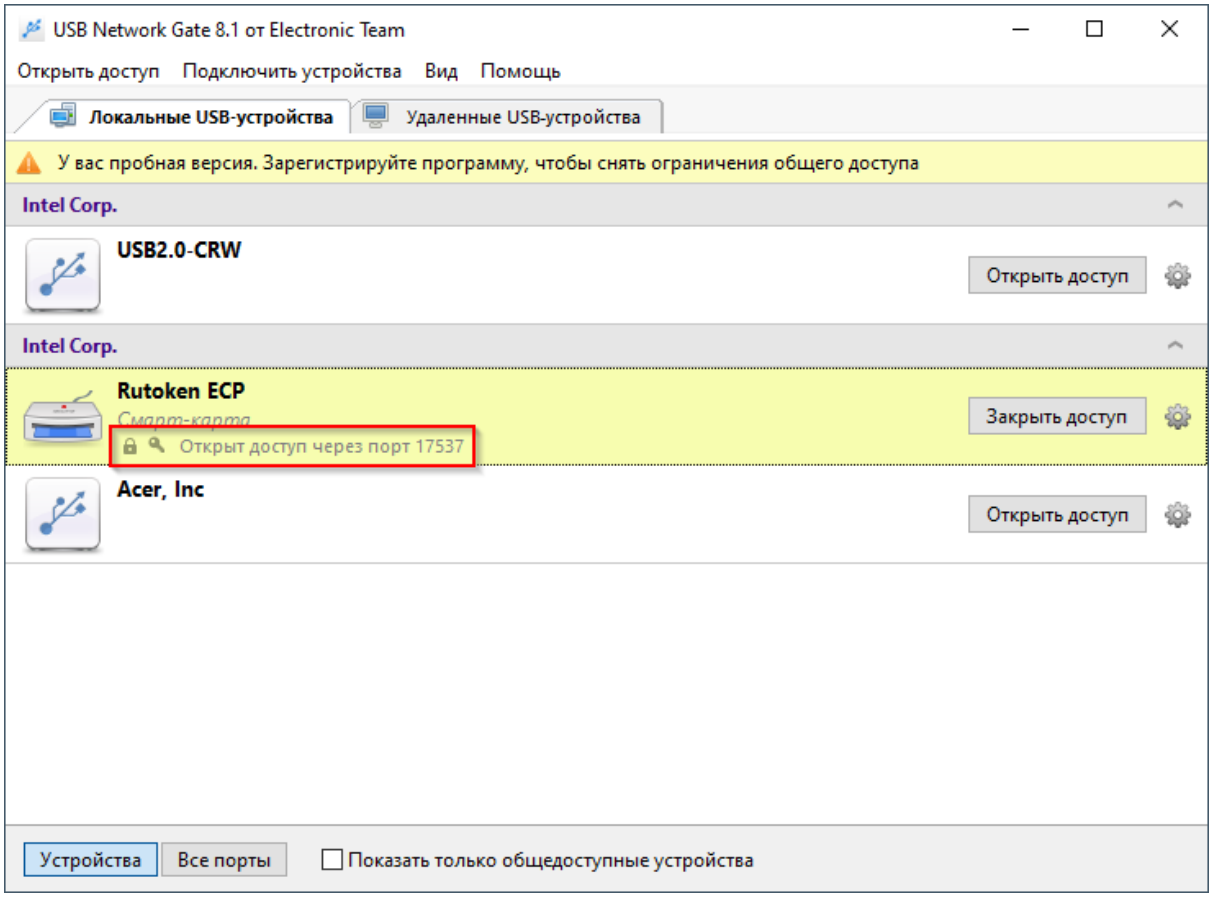
2. **После запуска выбираем ключ КЭП среди локальных USB-устройств и нажимаем кнопку настроек:**



3. **Указываем пароль, который потребуется для подключения к этому устройству, включаем опцию шифрования и нажимаем кнопку «Открыть доступ»:**



4. Теперь к ключу КЭП открыт доступ:

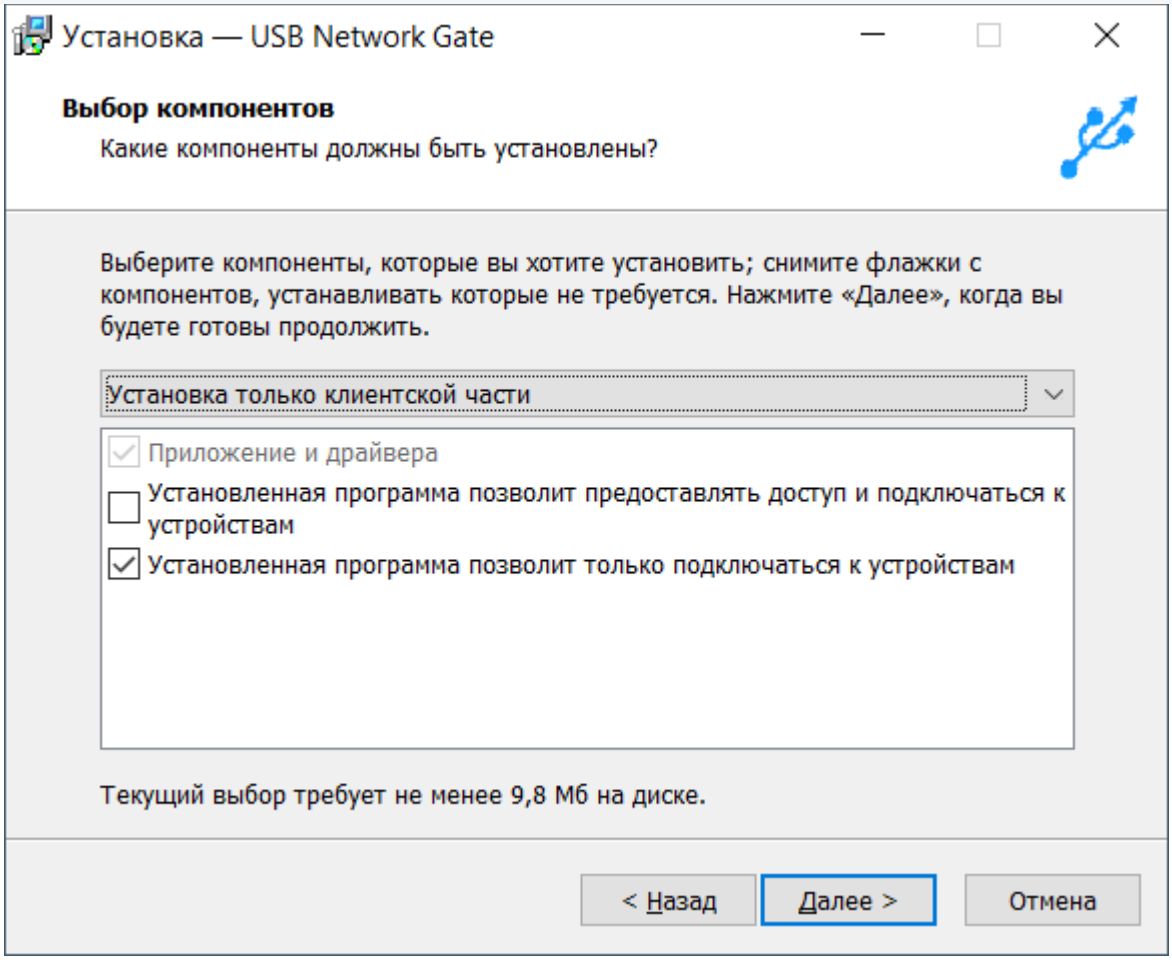


На этом настройка ПК-1 завершена, переходим к ПК2.

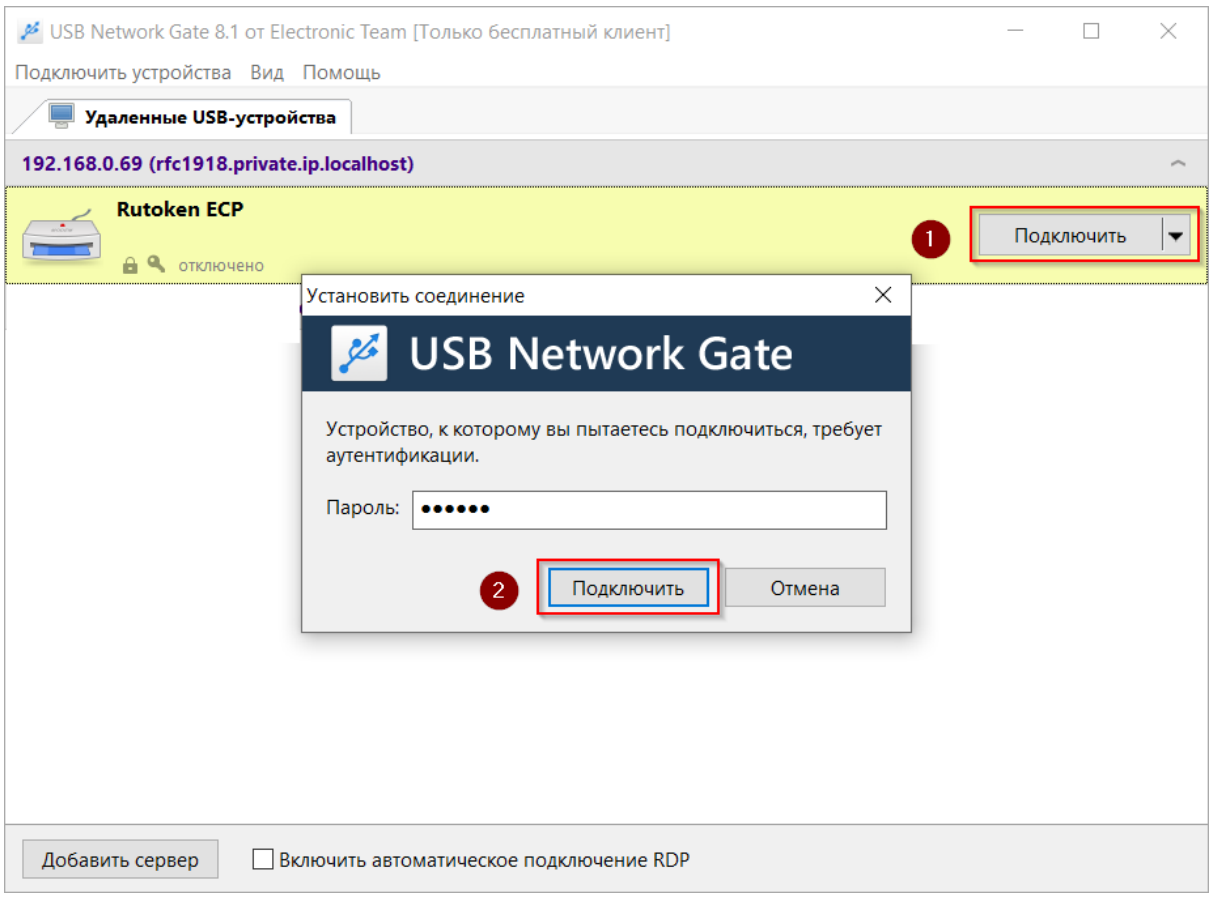
Установка ПО и настройки на ПК-2

Ключ КЭП должен быть вставлен в USB-порт.

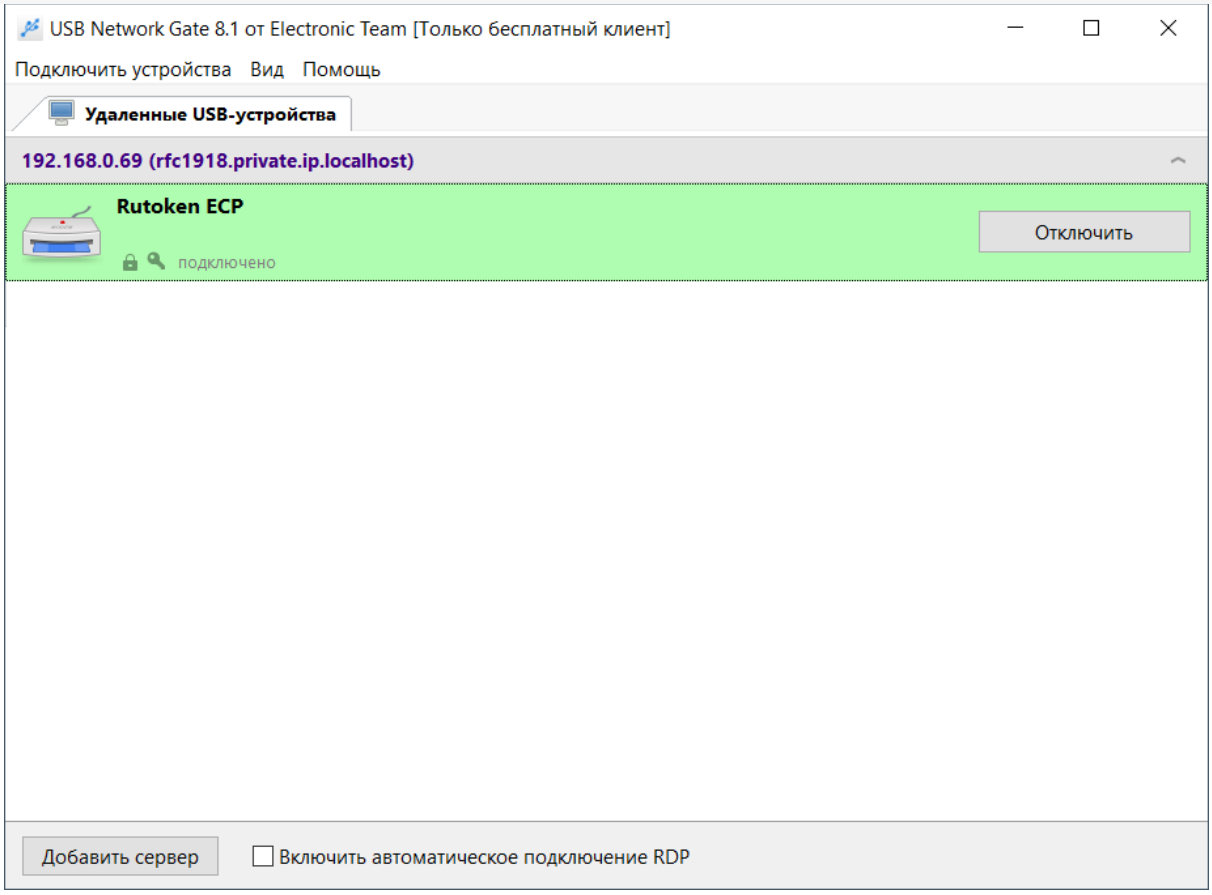
1. Устанавливаем USB Network Gate, при установке выбираем вариант «Установка только клиентской части»:



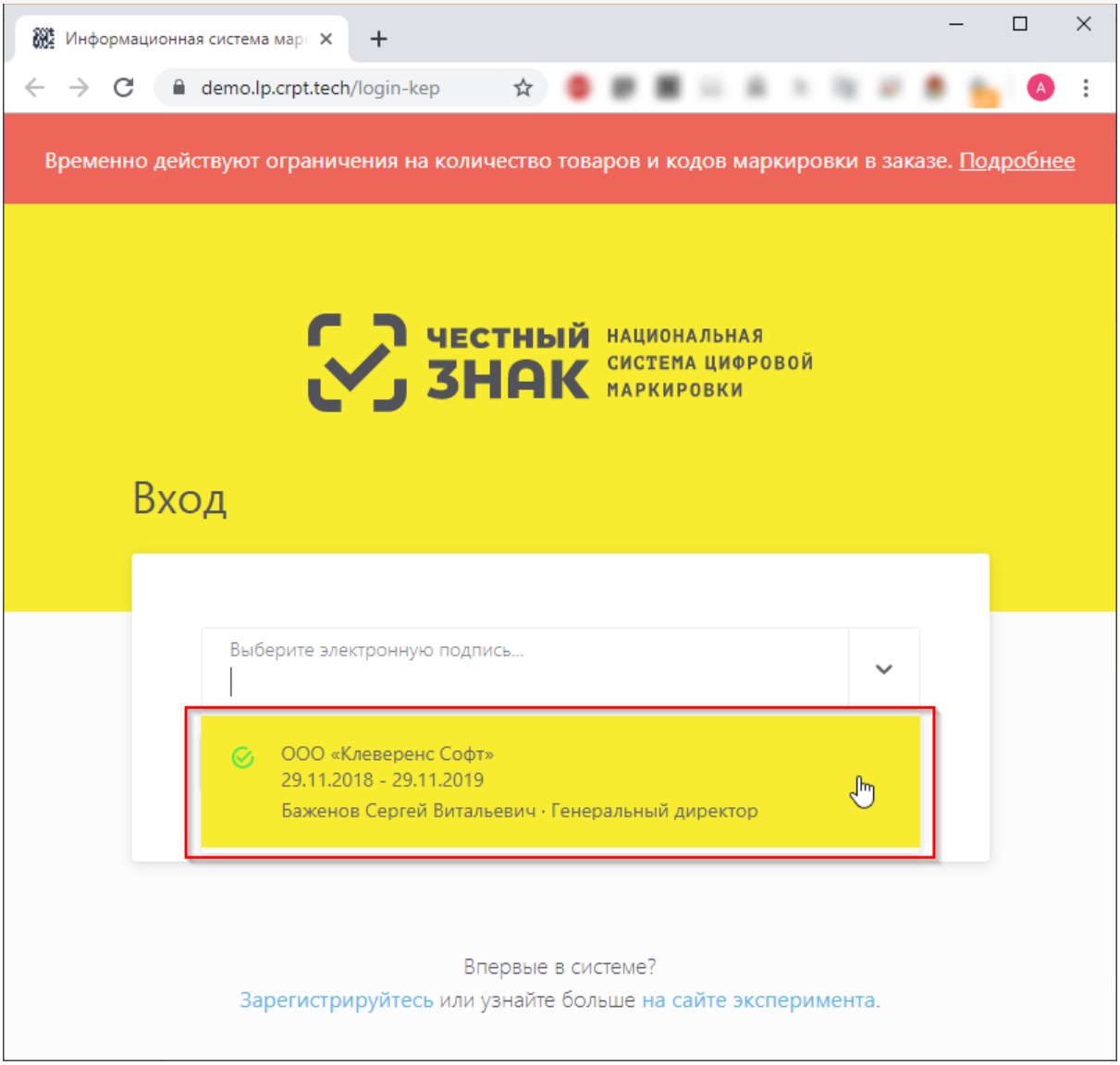
2. **При первом запуске будет произведён поиск доступных для подключения устройств. Выбираем наш ключ и нажимаем «Подключить», вводим пароль, который указывали в настройках на ПК-1 и подключаем устройство:**



3. **Готово, ключ КЭП подключён:**



В качестве проверки используется вход в личный кабинет на сайте ИС МП:



Теперь на ПК-2 ключ КЭП может использоваться так же, как если бы он был вставлен непосредственно в локальный USB-порт.

Не нашли что искали?

Задать вопрос в техническую поддержку

Получение «OMS ID» и «ID соединения» для доступа в СУЗ для «Кировки»

Применимо к продуктам: Кировка

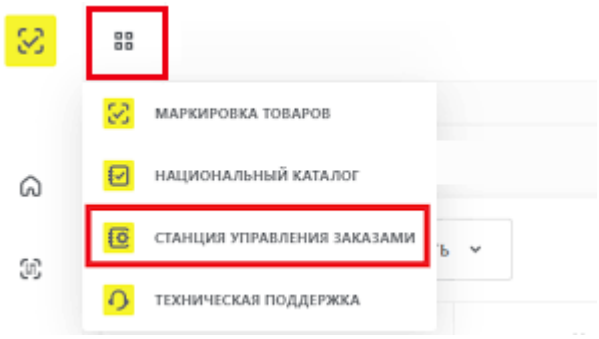
Последние изменения: 2024-03-26

Продукт «Кировка» интегрирован со станцией управления заказами (СУЗ), которая предоставляет возможность заказа и выпуска кодов маркировки. Для того чтобы пользоваться этой возможностью, компания должна быть зарегистрирована в ГИС МТ и иметь там свой личный кабинет.

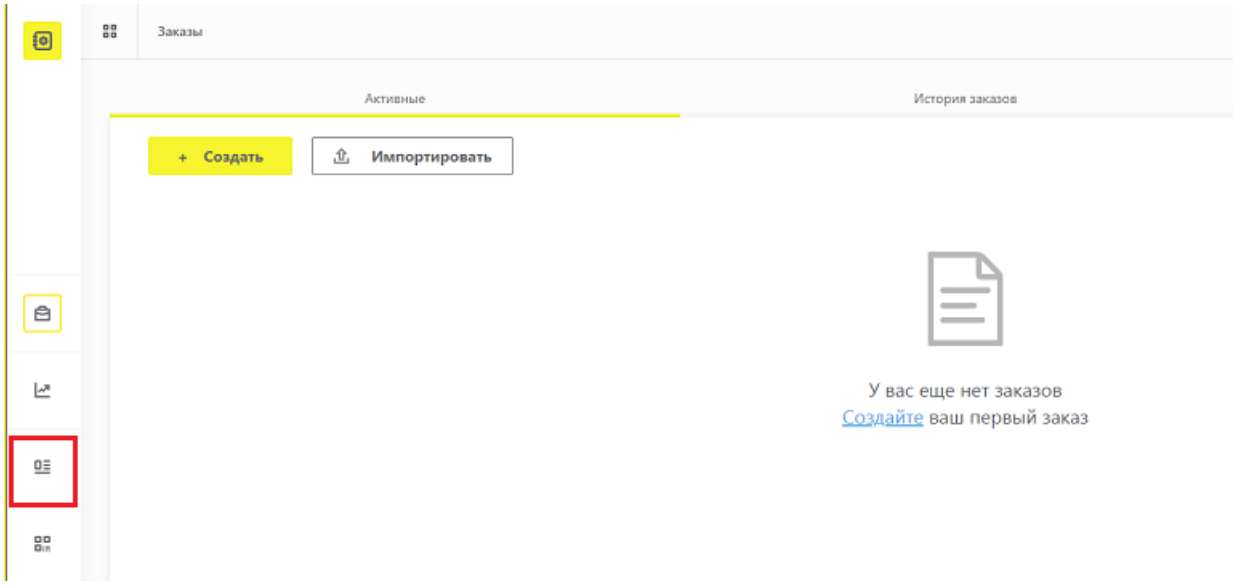
> Для каждой новой базы «Кировки» необходимо создавать отдельное устройство в СУЗ.

Для заказа и выпуска кодов маркировки с помощью «Кировки» необходимо иметь OMS ID и идентификатор соединения с СУЗ. Получить их можно, следуя следующей инструкции:

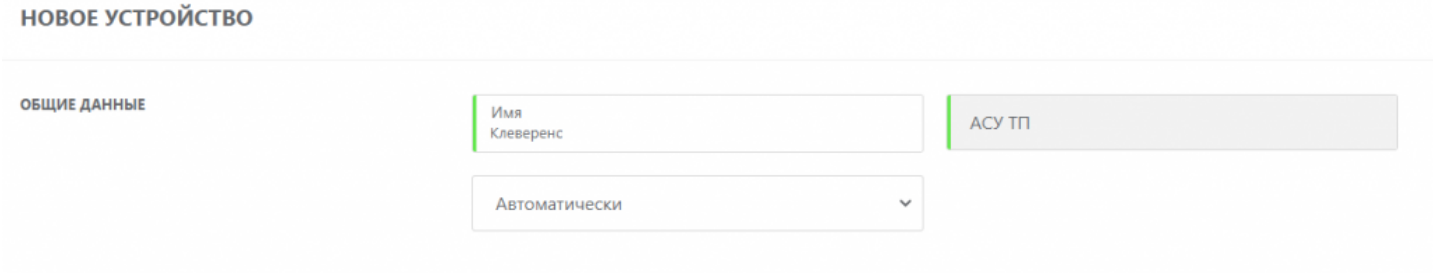
1. Войти в личный кабинет ГИС МТ и в верхнем левом меню выбрать пункт «Станция Управления Заказами».



2. Далее откроется станция управления заказами. Для добавления нового устройства, с которым вы будете работать, необходимо нажать кнопку «Устройства» --> «Создать устройство».

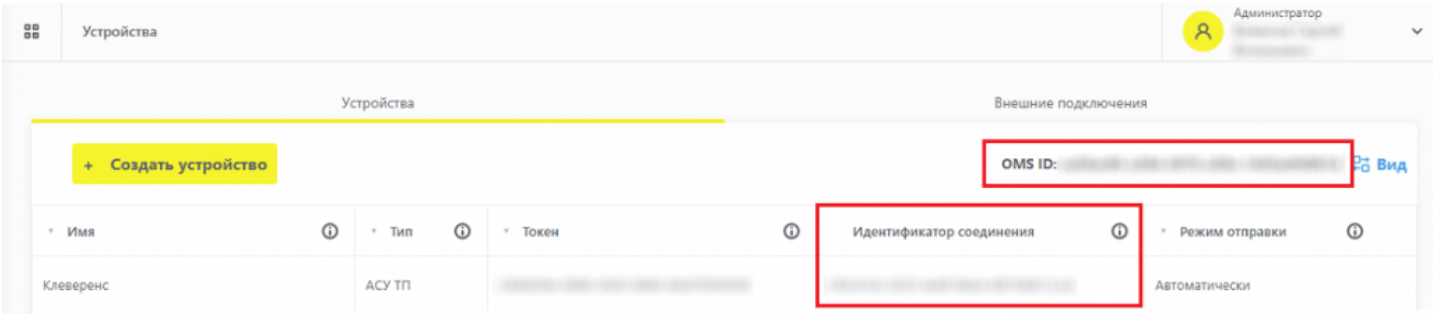


3. В открывшемся окне нужно указать следующие параметры:



- **«Имя» — имя вашего клиентского устройства (ТСД), указывается произвольно. Необходимо в случае, если ваша компания использует несколько терминалов сбора данных или несколько АСУ ТП.**
- **«Тип» — предустановлено АСУ ТП.**
- **«Режим отправки отчетов» — выбираем «Автоматически».**

4. **После того, как все поля заполнены, нажмите кнопку «Создать» в правом нижнем углу экрана. После этого новое устройство отобразится в списке всех добавленных устройств, и можно будет узнать его OMS ID и идентификатор соединения (у каждого участника он разный).**



Кировка, v1.0.9.795

Не нашли что искали?

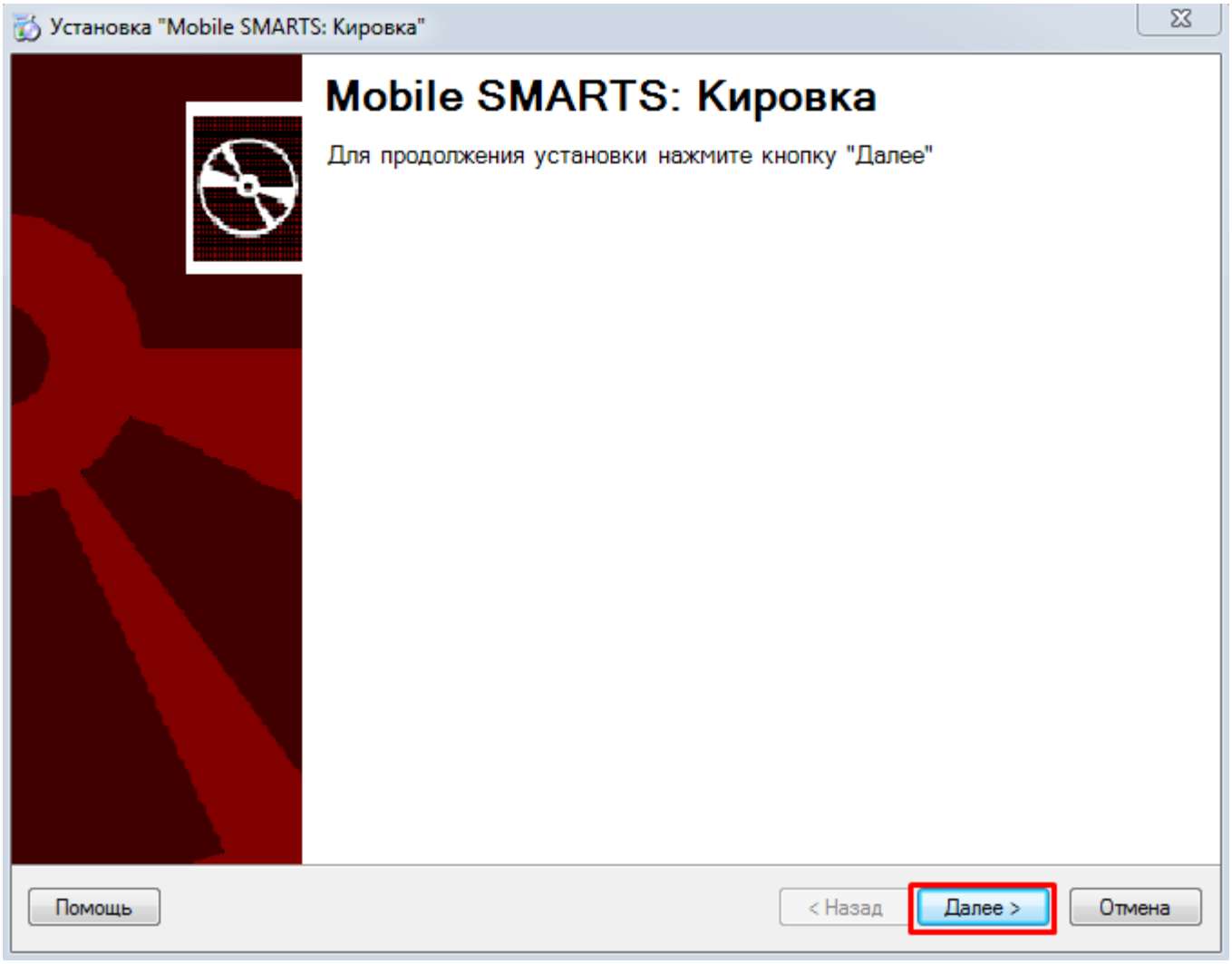
Задать вопрос в техническую поддержку

Установка «Кировки» на ПК

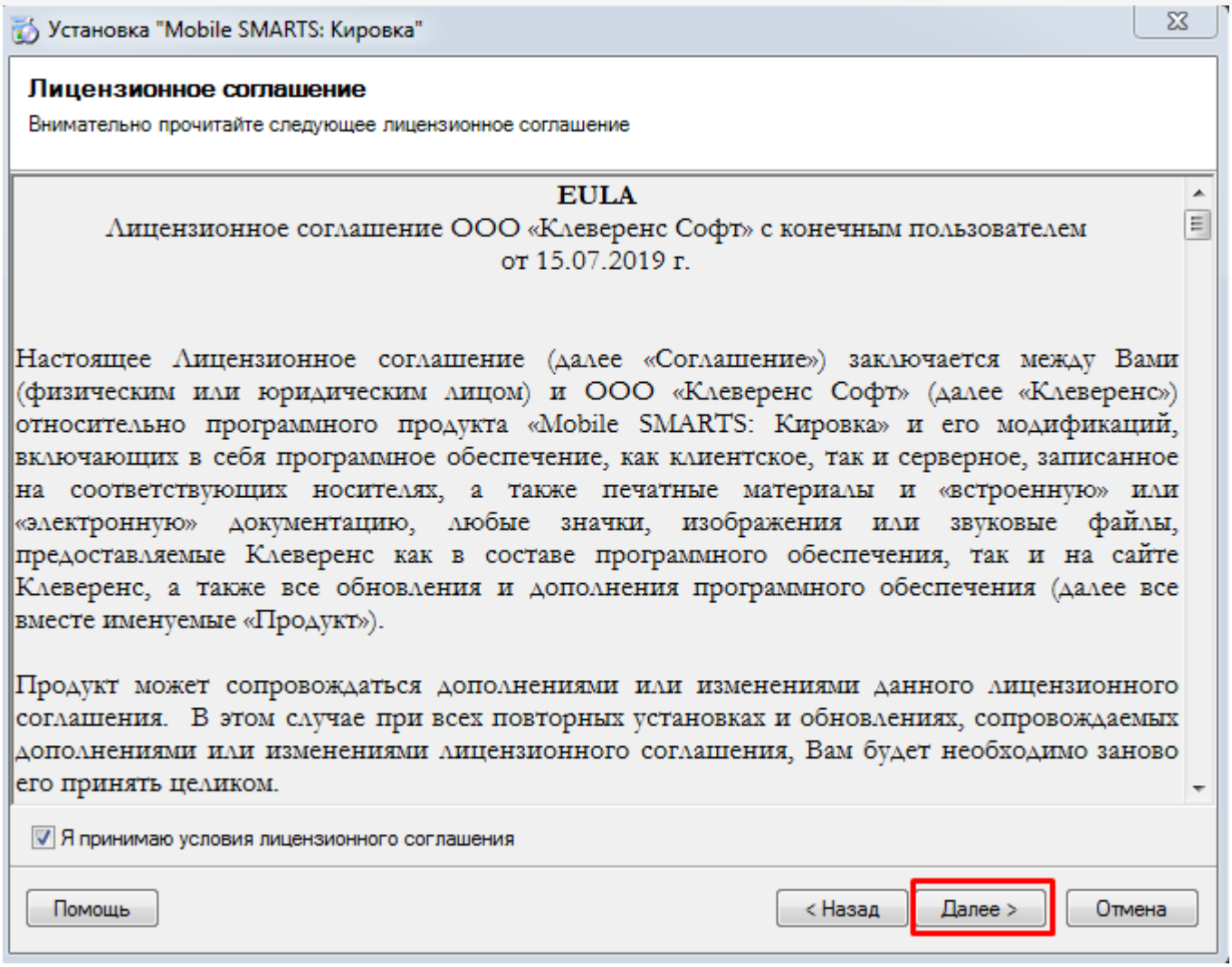
Последние изменения: 2024-03-26

Для установки «Кировки» необходимо воспользоваться специальным мастером установки Kirovka.InstallWizard.exe.

После запуска откроется окно установщика.

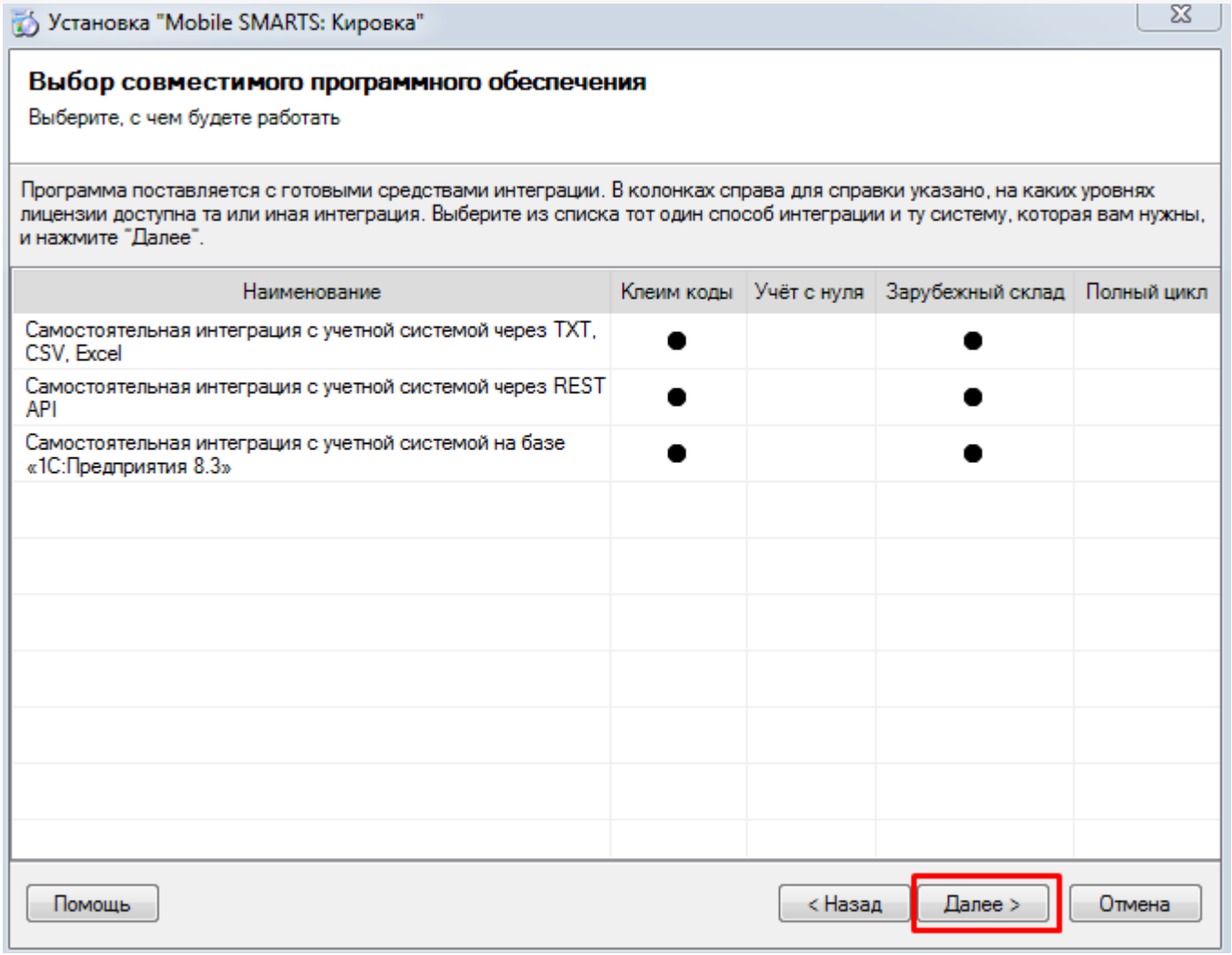


Необходимо принять условия лицензионного соглашения и нажать кнопку «Далее».

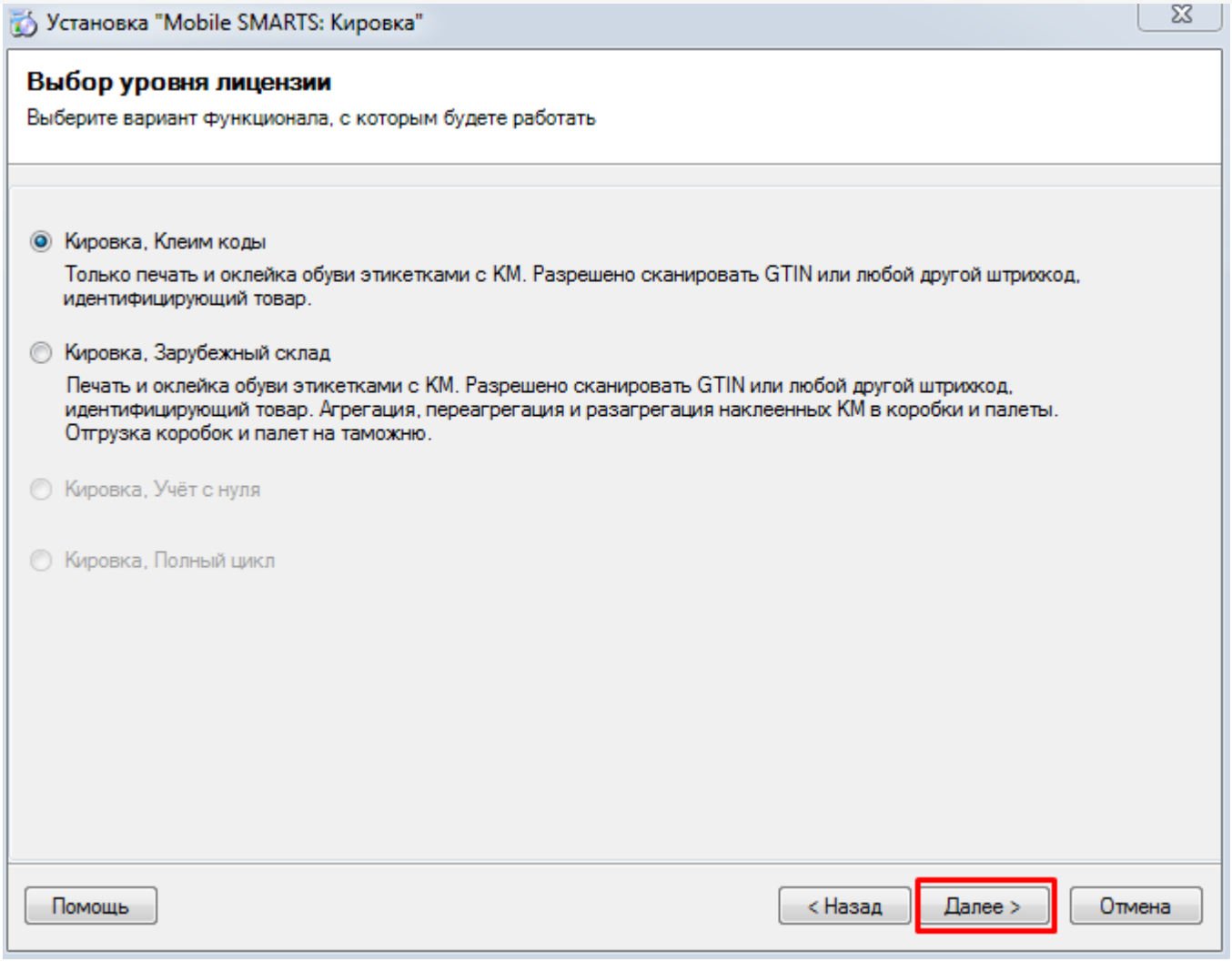


Выбираем средство интеграции учетной системы с сервером Mobile SMARTS. На данный момент доступно три варианта интеграции, но в будущем список будет пополнятся.

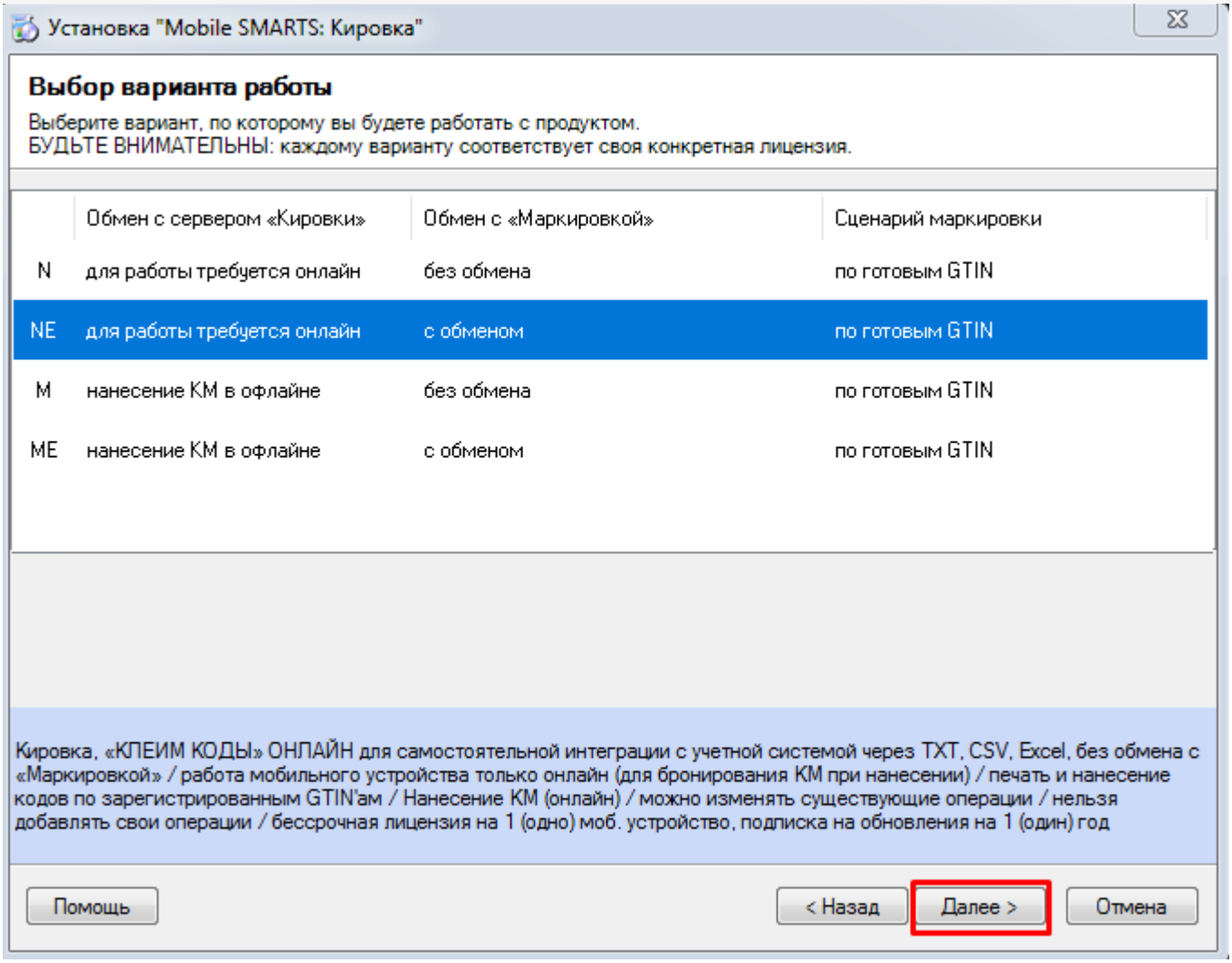
Для примера рассмотрим вариант «Самостоятельная интеграция с учетной системой через TXT, CSV, Exel».



Выбираем уровень лицензии. На данный момент доступны уровни «Клеим коды» и «Зарубежный склад».



Далее следует выбрать вариант работы с продуктом «Кировка».

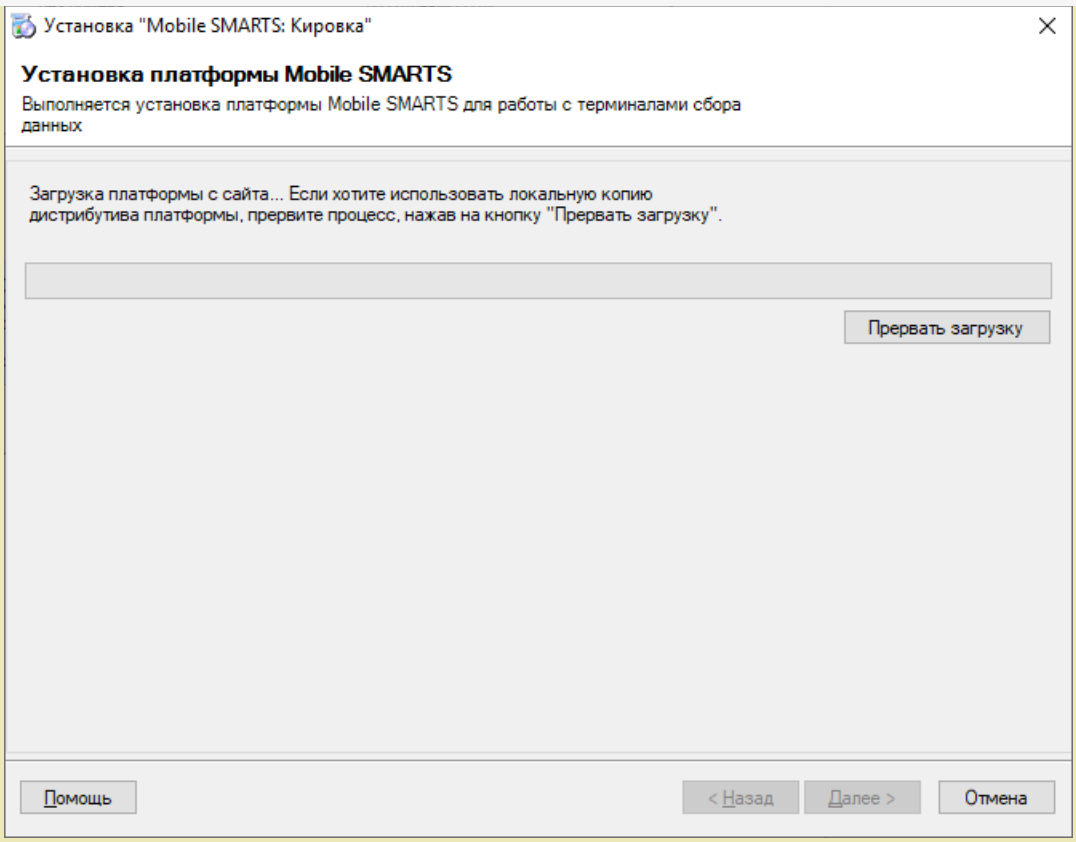


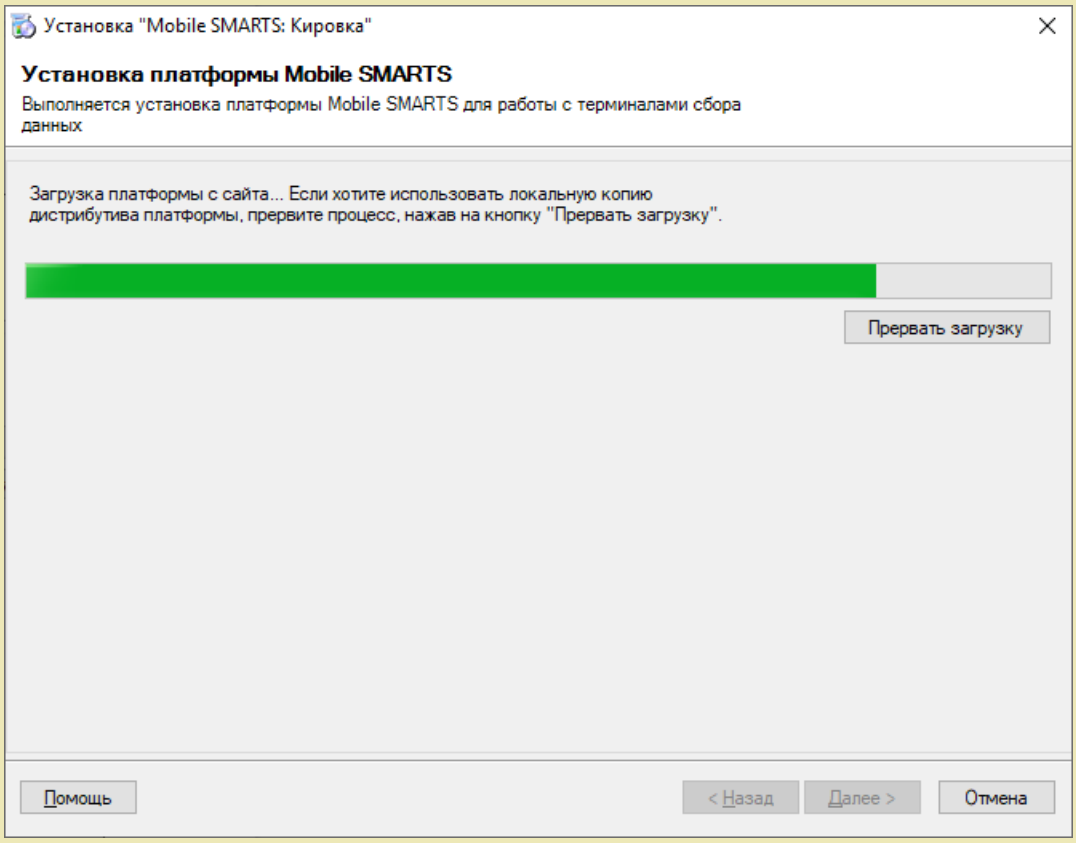
Варианты работы подразделяются на группы по двум основным критериям: по обмену данными с сервером «Кировки» и обмену с «Маркировкой» (с системой «Честного Знака»).

- **обмен с сервером «Кировки»**
  - **для работы требуется онлайн — в данном случае мобильное устройство постоянно обменивается данными с сервером «Кировки». В режиме реального времени происходит отслеживание доступных кодов маркировки, что позволяет избежать ситуации, когда один код маркировки наклеен на несколько товаров. Данный режим работы позволяет использовать несколько ТСД для работы с одним документом. Необходимо постоянное подключение к сети.**
  - **нанесение КМ в оффлайне — при таком режиме работы на каждый ТСД заранее выгружается документ с необходимыми кодами маркировки, а для остальных терминалов эти коды блокируются.**

- **обмен с «Маркировкой»**
  - **с обменом — можно заказывать и вводить в оборот коды маркировки прямо с мобильного устройства (ТСД).**
  - **без обмена — заказ кодов маркировки происходит в другом месте. Например, в учетной системе.**

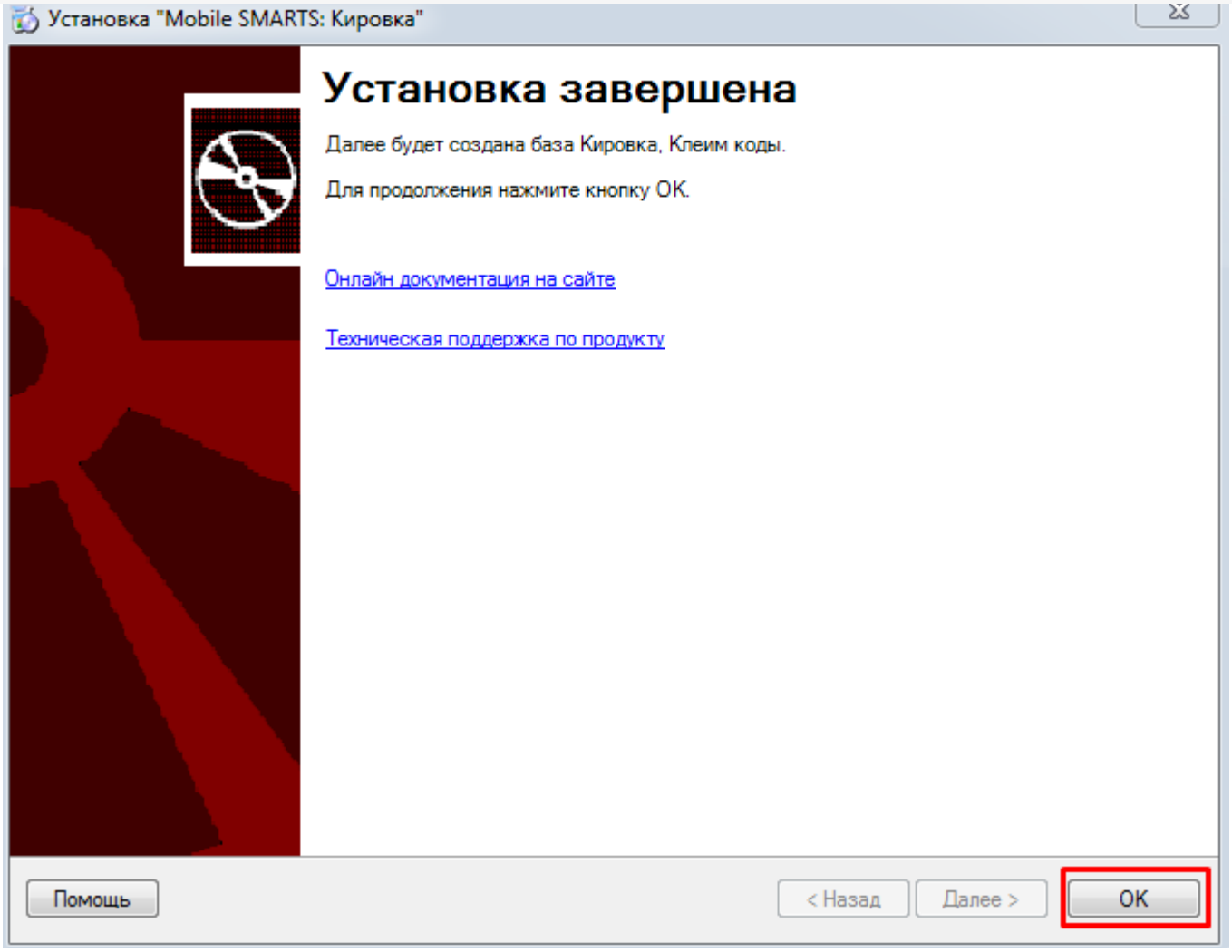
В случае если платформа Mobile SMARTS не была ранее установлена самостоятельно, на следующем экране будет предложено скачать и установить ее. Рекомендуется не пропускать данный этап, так как установщик всегда скачивает актуальную версию, необходимую для корректной работы.





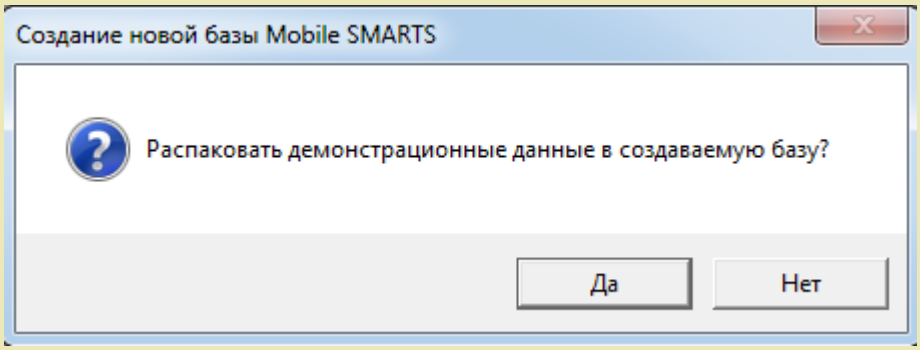
После того как загрузка платформы завершена, автоматически открывается окно мастера установки Mobile SMARTS. О том, что делать дальше, читайте в статье «Установка платформы Mobile SMARTS».

Установка завершена.



В каждой базе «Кировки» присутствуют демонстрационные штрихкоды, вне зависимости от распаковки демонстрационных данных. Найти их можно в «C:\ProgramData\Cleverence\Databases\"Имя вашей базы"\XlsCsv».

Во время установки «Кировки» будет предложено распаковать демонстрационные данные в базу:

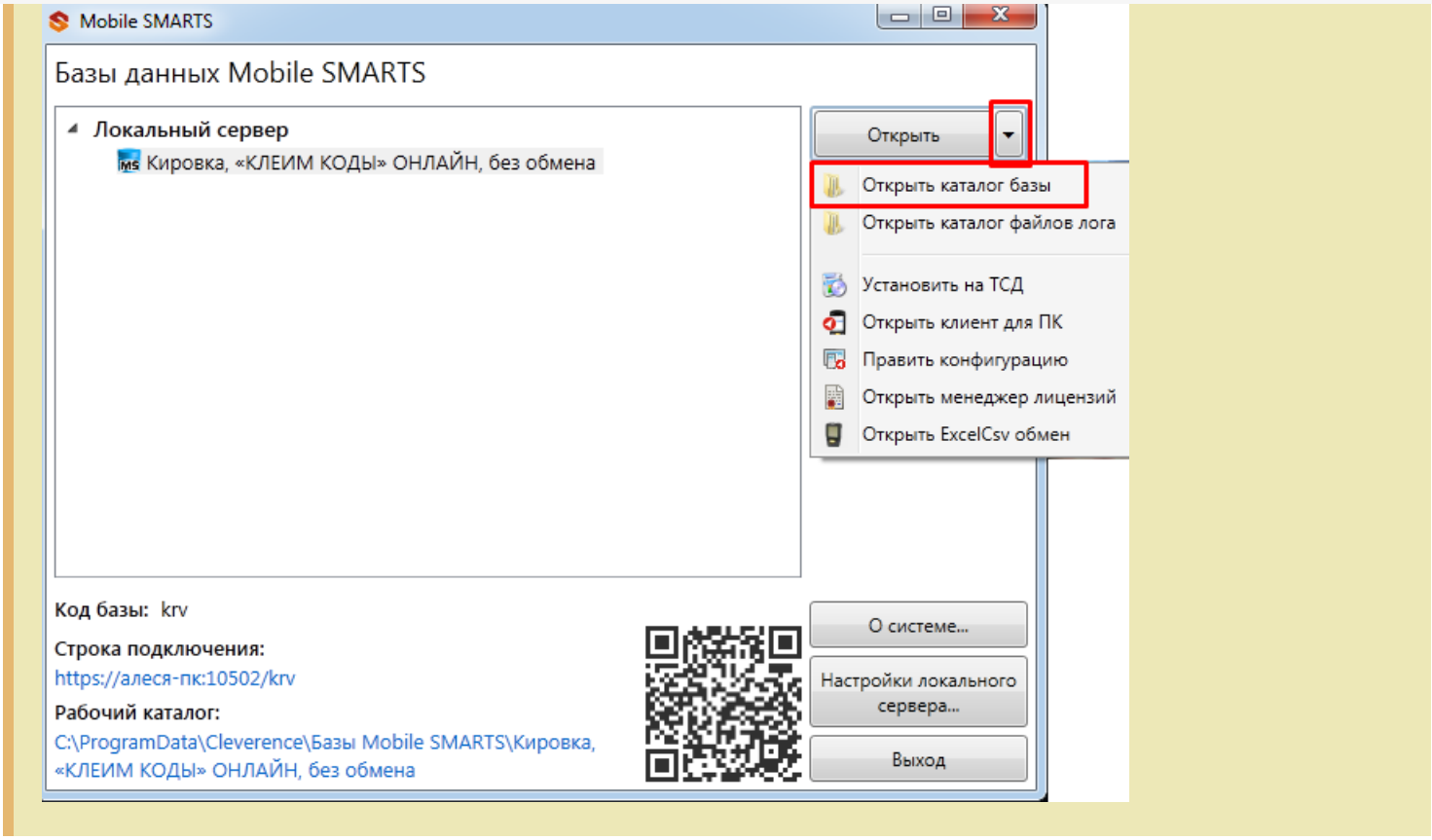


Если вы ответите «Да», демонстрационные данные будут выгружены в базу данных «Кировки» и готовы к работе.

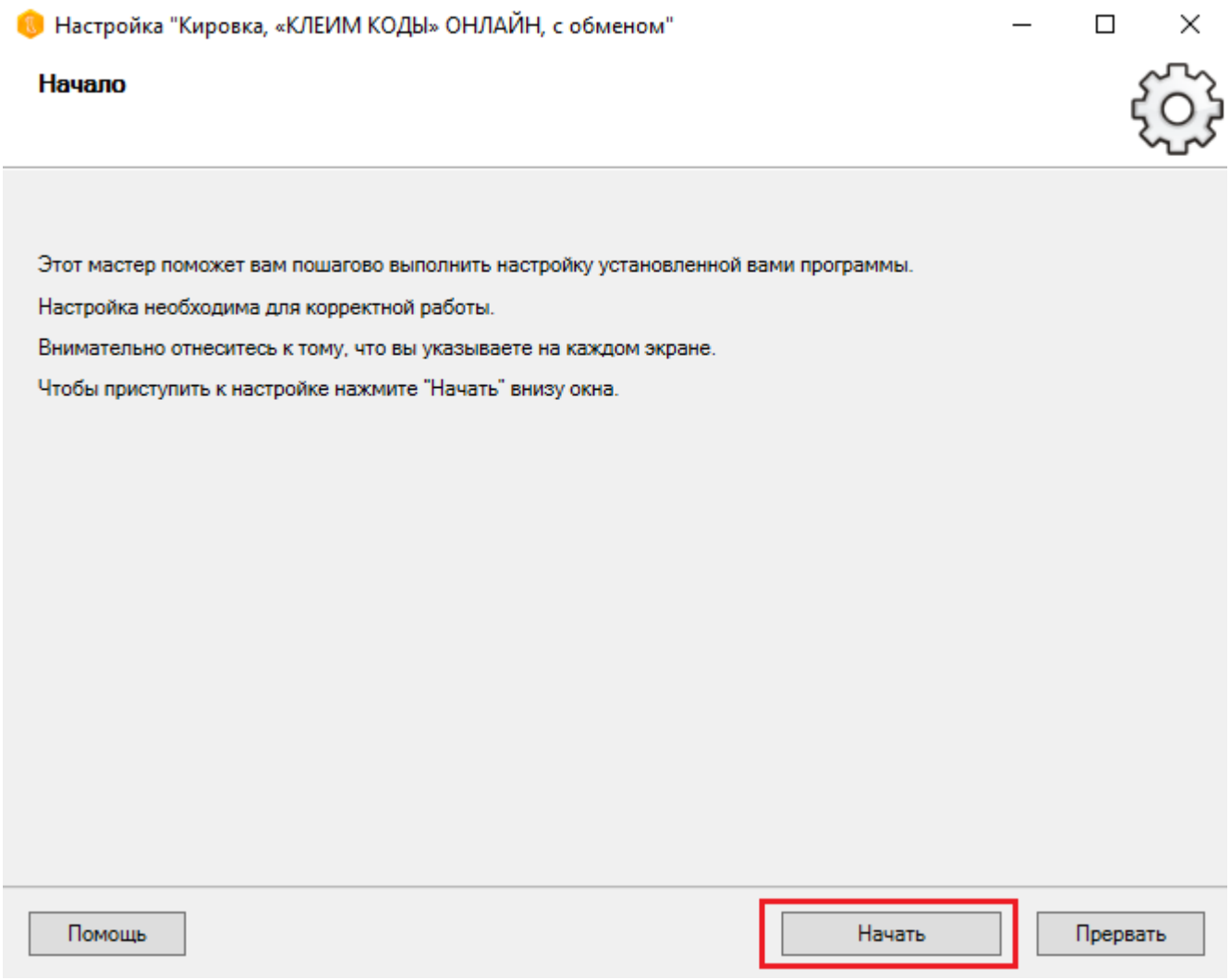
Если вы ответите «Нет», справочник номенклатуры и таблица КМ будут пусты.

Вне зависимости от выбранного варианта, демонстрационные данные всегда можно выгрузить с помощью утилиты обмена Excel/ CSV в любое время позже. Данные на выгрузку находятся в папке «C:\ProgramData\Cleverence\Databases\"Имя вашей базы"\XlsCsv\На терминал».

Для того чтобы открыть вышеуказанные папки, необходимо воспользоваться менеджером баз Mobile SMARTS:



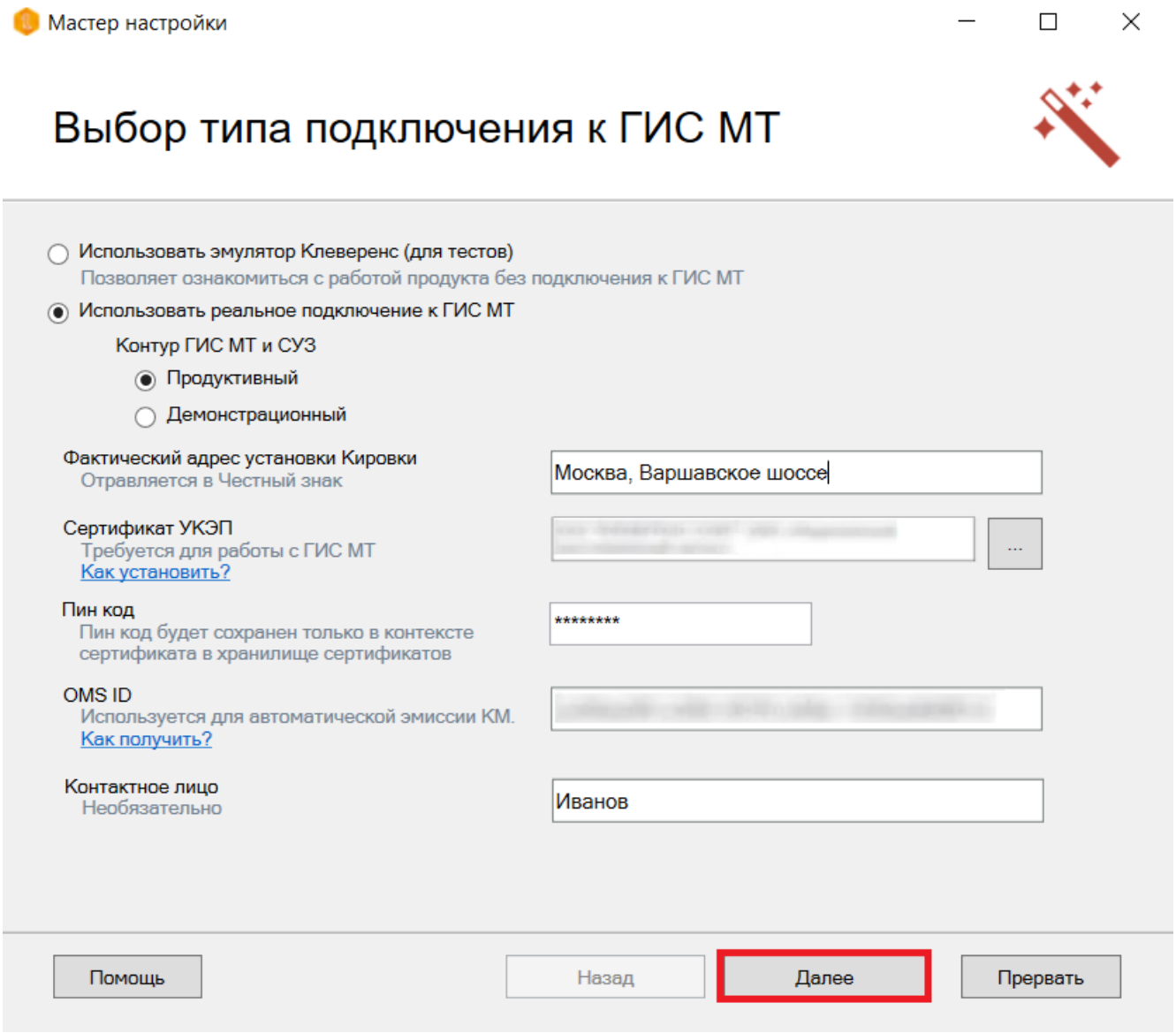
Далее для корректной работы продукта необходимо пройти начальную настройку. Окно настройки открывается автоматически.



Выберите тип подключения к ГИС МТ. Эмулятор приложения подходит, если вы хотите нанести пробные коды маркировки, протестировать приложение. Но полноценная работа в эмуляторе невозможна, т.к. его коды

маркировки не будут иметь законного статуса.

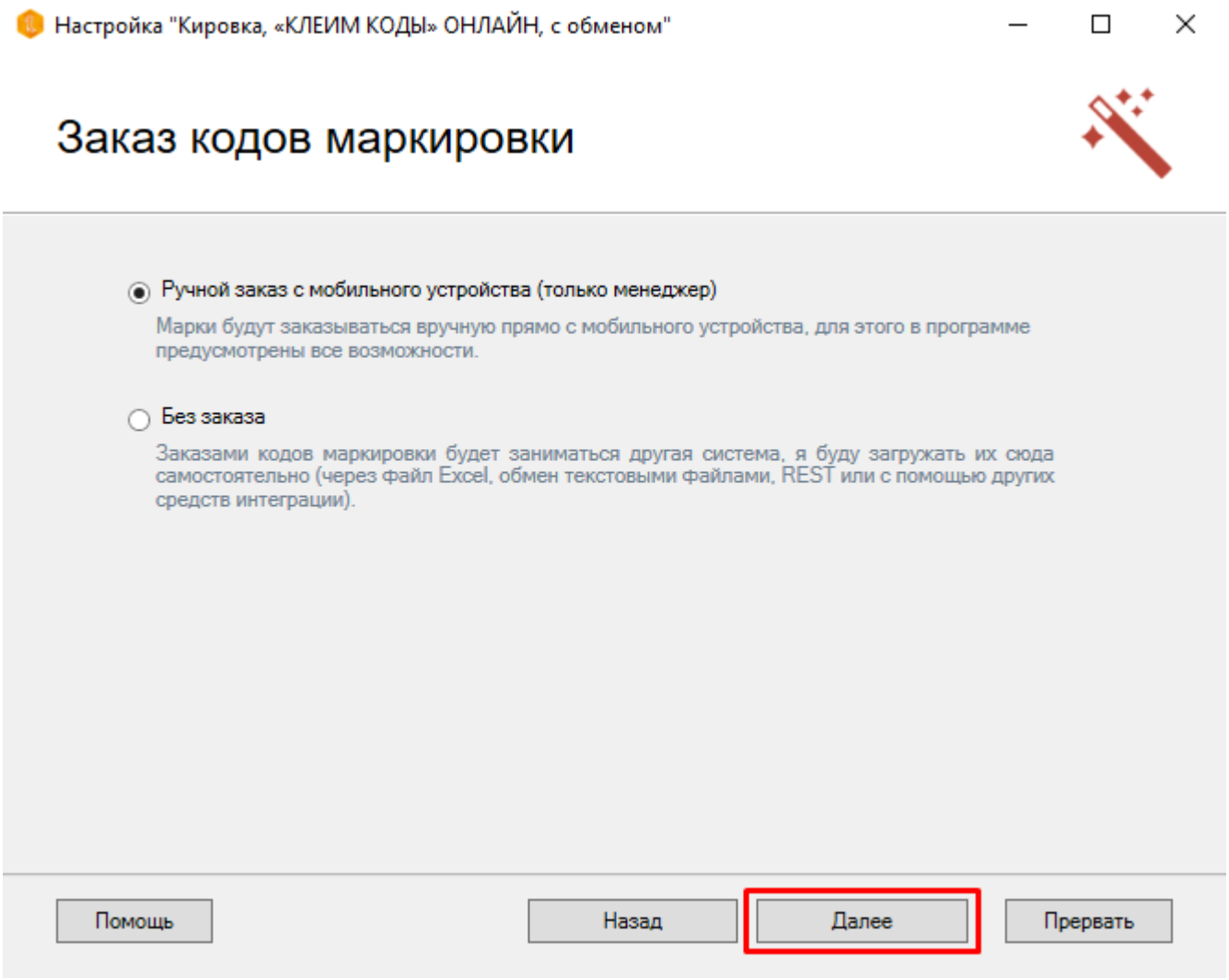
Подключение к ГИС МТ позволит начать работу с реальными кодами маркировки. Но подключение к демонстрационному контуру дает возможность протестировать ограниченный функционал системы (например, маркировку товаров, оформление движения товаров). Для полноценной работы необходимо подключить «Кировку» к продуктивному (реальному) контуру и указать все данные, которые будут использоваться для подключенияк нему.



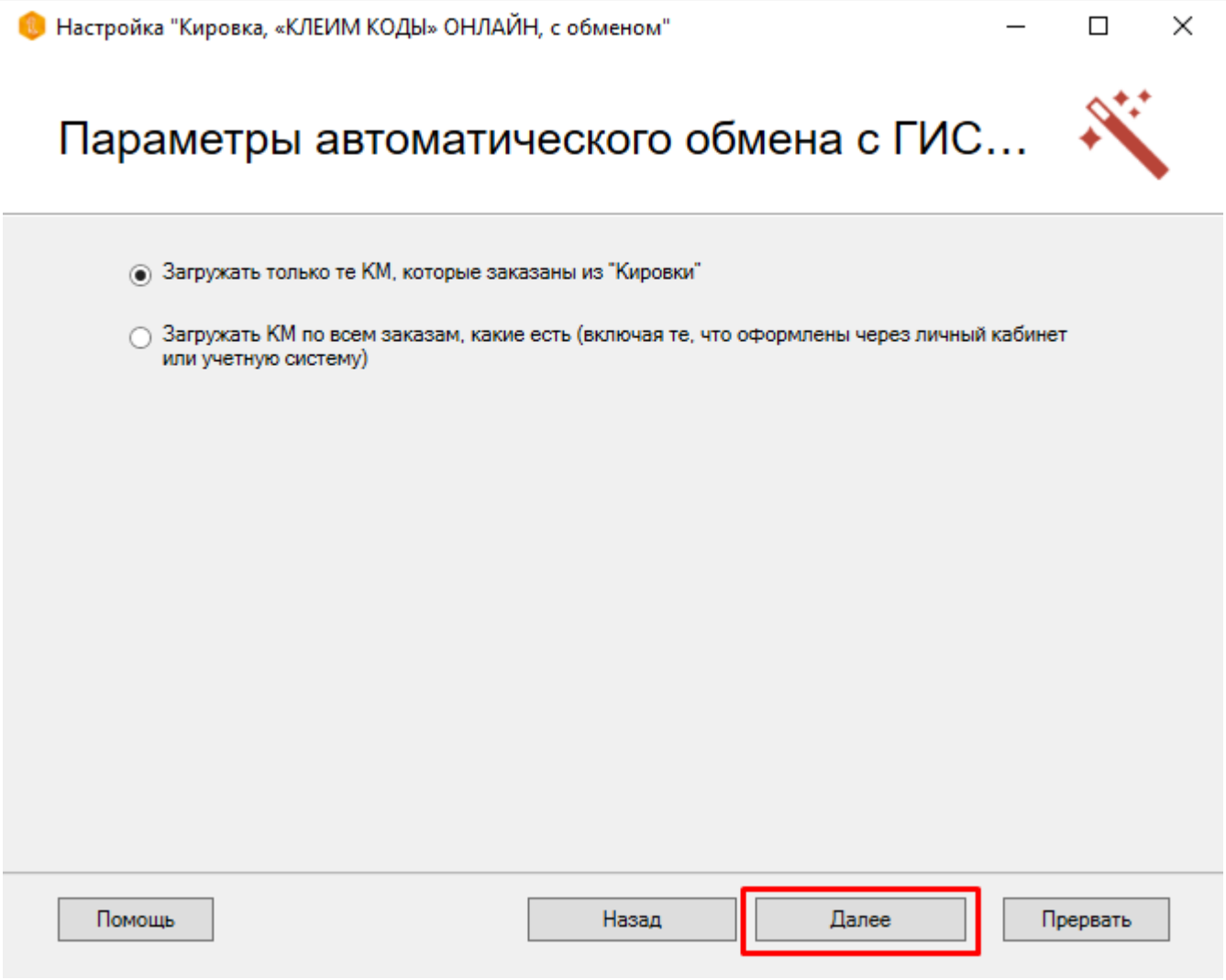
- фактический адрес установки «Кировки» — производится для регистрации установленного расширения. Необходимо ввести реальный адрес установки базы «Кировки», т.к успешная установка базы блокирует возможность смены данного адреса (по причине того что данная информация отправляется в ЦРПТ). В случае если вы хотите зарегистрировать базу «Кировки» на другой адрес, потребуется установить новую базу;
- сертификат УКЭП (усиленная квалифицированная электронная подпись). УКЭП должен быть вставлен в компьютер;
- пин-код от УКЭП;
- OMS ID;
- контактное лицо (необязательно).

Все эти пункты необходимы для заказа кодов маркировки и ввода их в оборот с ТСД. После того как все поля заполнены, нажмите кнопку «Далее».

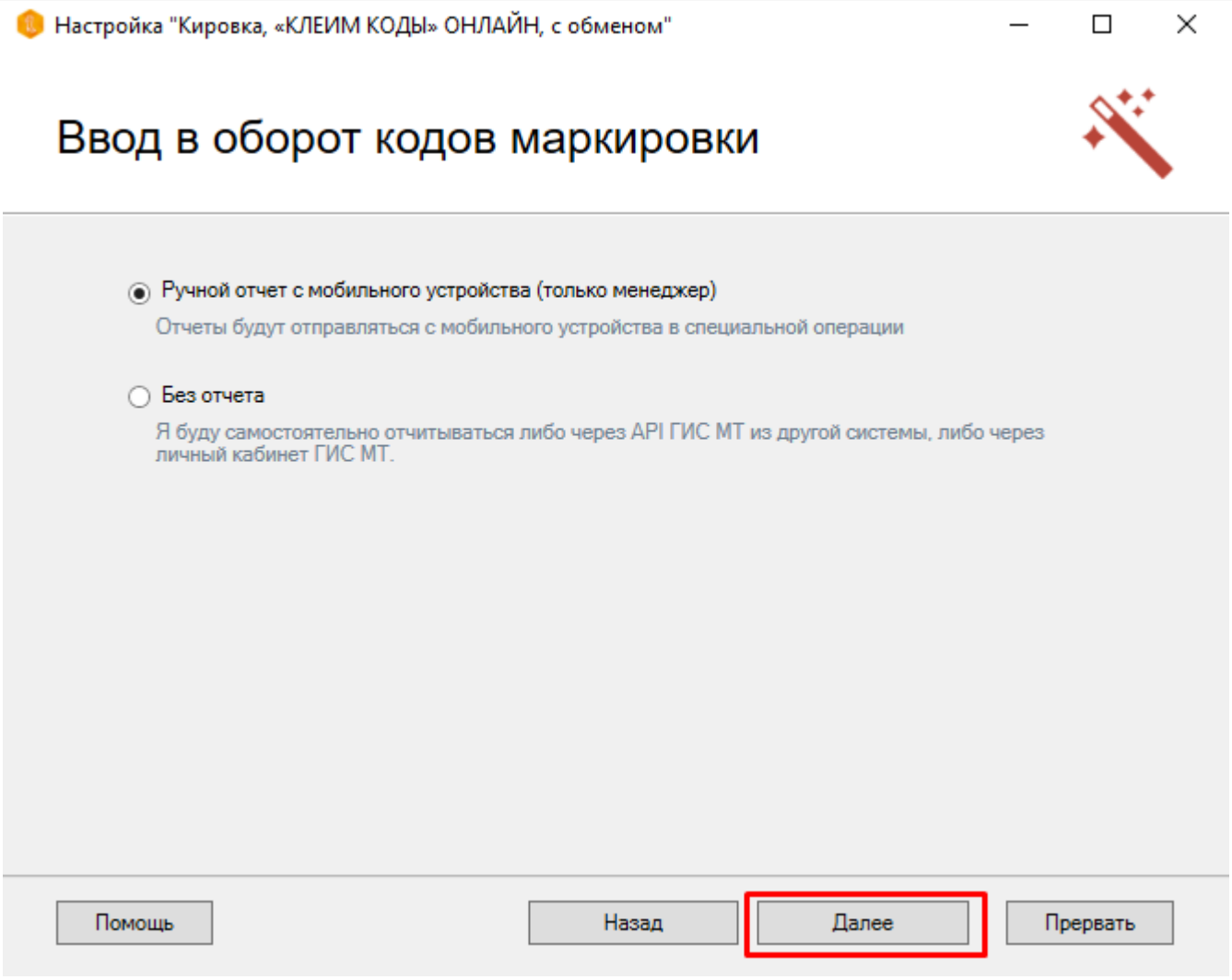
Далее выберите способ заказа кодов маркировки.



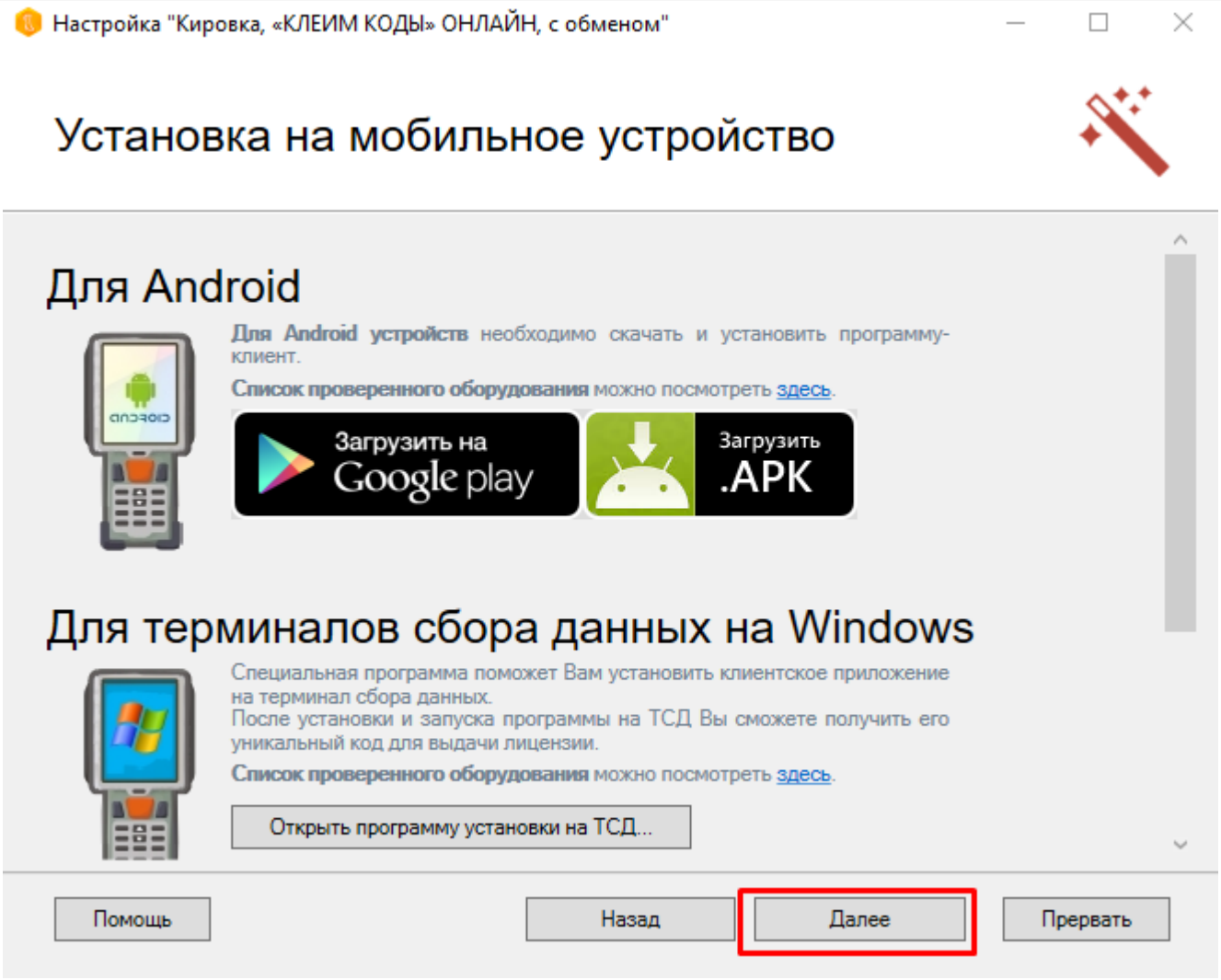
Укажите параметры автоматического обмена с системой ГИС МТ.



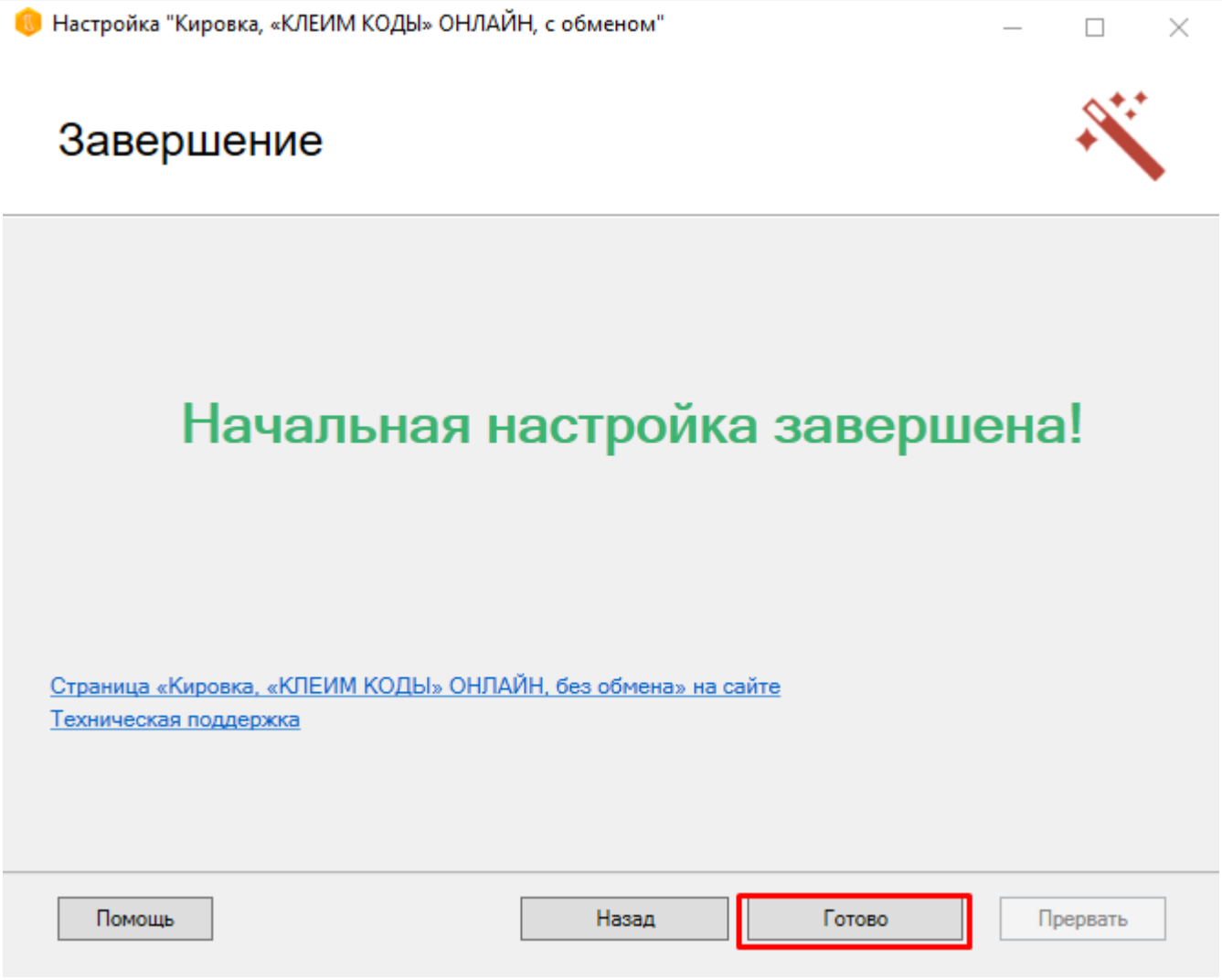
Выберите способ предоставления отчета за введенные в оборот коды маркировки.



Далее подключаем терминал к компьютеру и устанавливаем на него клиентское приложение «Кировка».



Далее необходимо получить лицензию на продукт. Для этого необходимо открыть мастер лицензий с помощью одноименной кнопки и выбрать способ получения лицензии. Как это делается, читайте в статье «Мастер получения лицензий».



Начальная настройка завершена.

> **Далее для полноценной работы «Кировки» потребуется сформировать и выгрузить файл с номенклатурой из личного кабинета GS1 в базу «Кировки». Это можно сделать с помощью утилиты обмена Excel/ CSV или других средств интеграции.**

Не нашли что искали?

Задать вопрос в техническую поддержку

Установка «Кировки» на мобильное устройство и подключение к базе на ПК

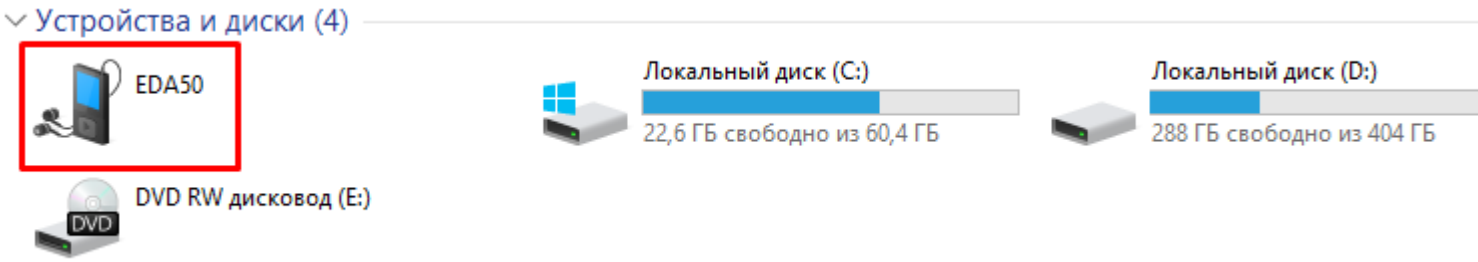
Последние изменения: 2024-03-26

Для работы с «Кировкой» на мобильном устройстве (ТСД, смартфоне, планшете) необходимо установить на него специальное клиентское приложение.

> «Кировка» работает только на мобильных устройствах с ОС Android!

Для этого необходимо:

1. Подключить ваше мобильное устройство к ПК с помощью USB кабеля (устройство должно быть подключено в режиме «как USB накопитель»).



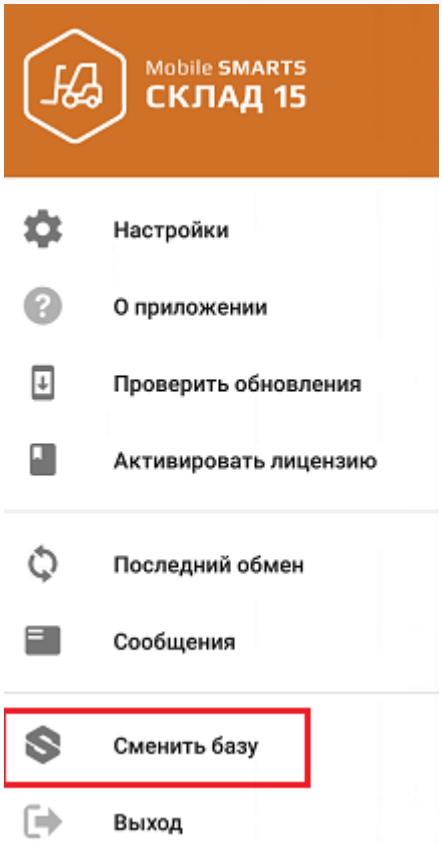
2. Скачайте установочный файл клиентского приложения со страницы продукта и скопируйте скачанный файл на подключённое устройство.

3. Запустите этот файл на устройстве с помощью файлового менеджера. Начнется установка приложения на устройство.

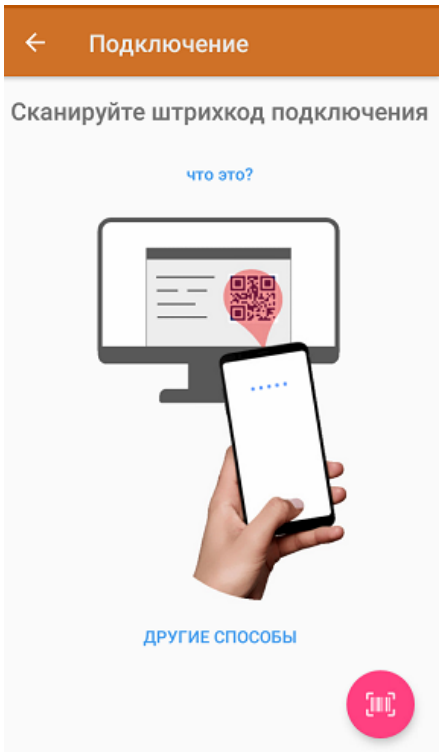
4. После того как клиент установлен, необходимо дать ему необходимые разрешения и подключить устройство к базе, с которой вы собираетесь работать.

   Для того, чтобы подключиться к базе, необходимо:

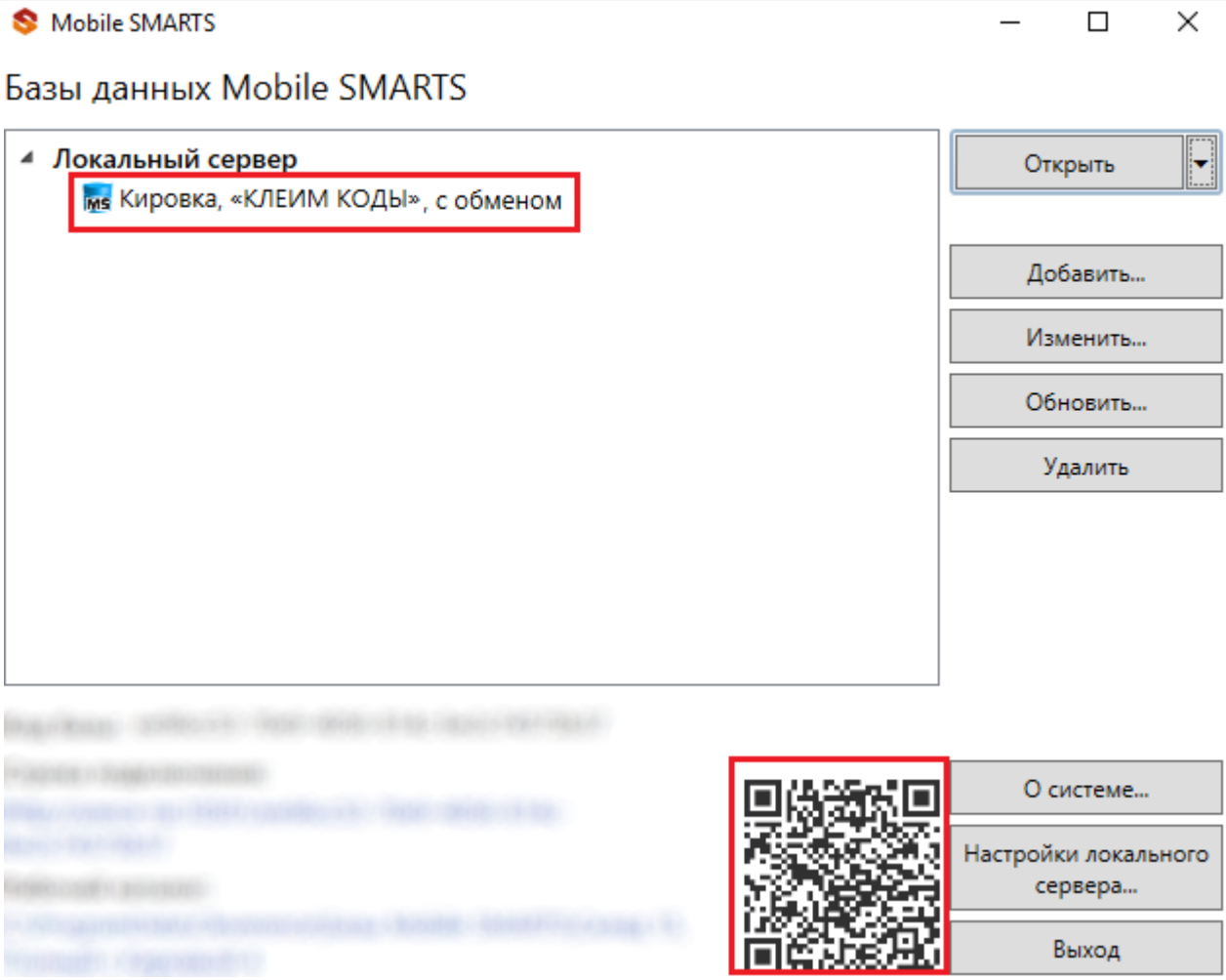
   - Войти в боковое меню приложения и выбрать там пункт «Сменить базу».



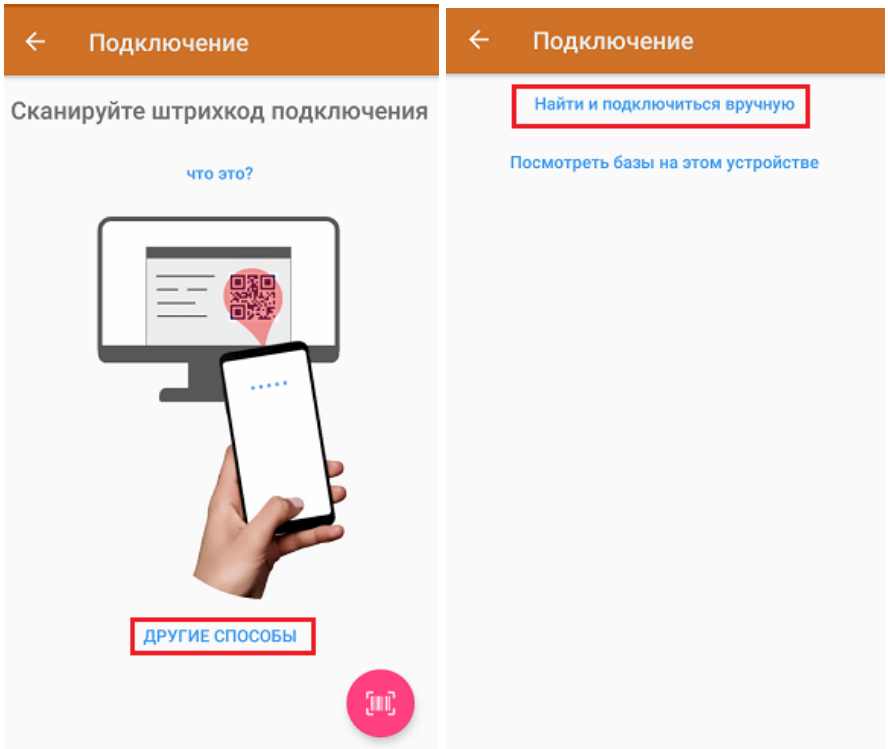
- **Далее можно либо сканировать QR-код подключения к базе, либо просмотреть список баз на сервере (или на устройстве) и выбрать из этого списка нужную.**



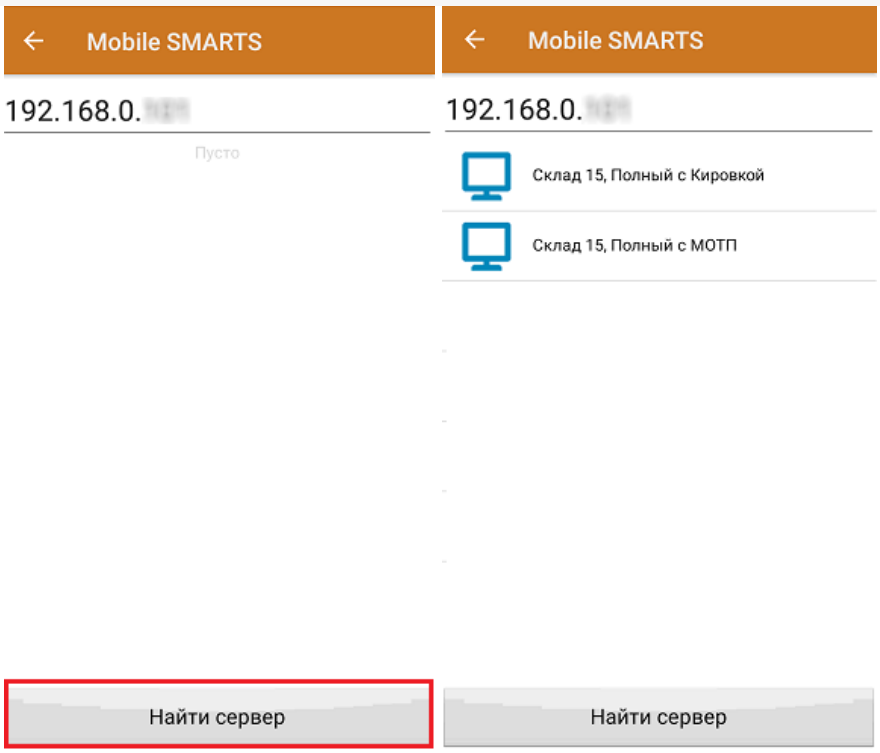
Сканировать QR-код:



Подключиться к базе вручную:

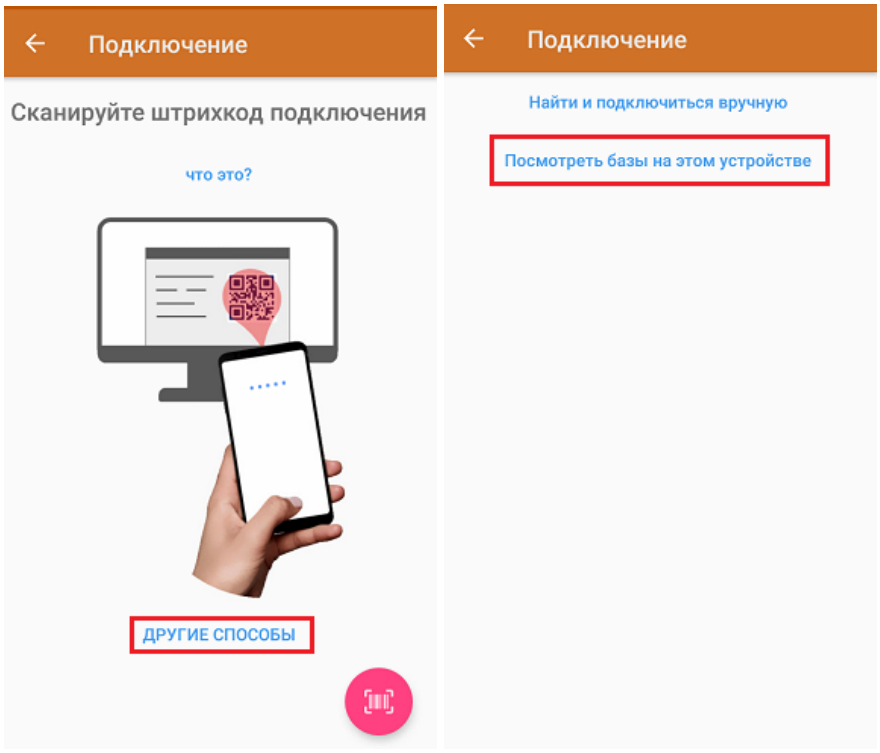


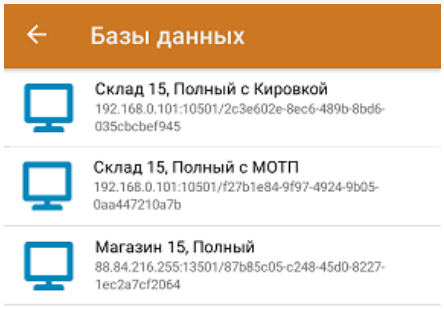
В таком случае необходимо подключиться к ПК, на котором установлен сервер Mobile SMARTS. Для этого введите адрес сервера и нажмите на кнопку «Найти сервер». Далее из открывшегося списка баз выберите ту, к которой вы хотите подключиться.



Просмотреть список баз на устройстве:

Отображается список баз Mobile SMARTS, к которым ранее подключалось данное устройство, из которых можно выбрать нужную.





Данный способ подключения к базе не используется при первом запуске приложения, так как этот список будет пустым.

Не нашли что искали?

Задать вопрос в техническую поддержку

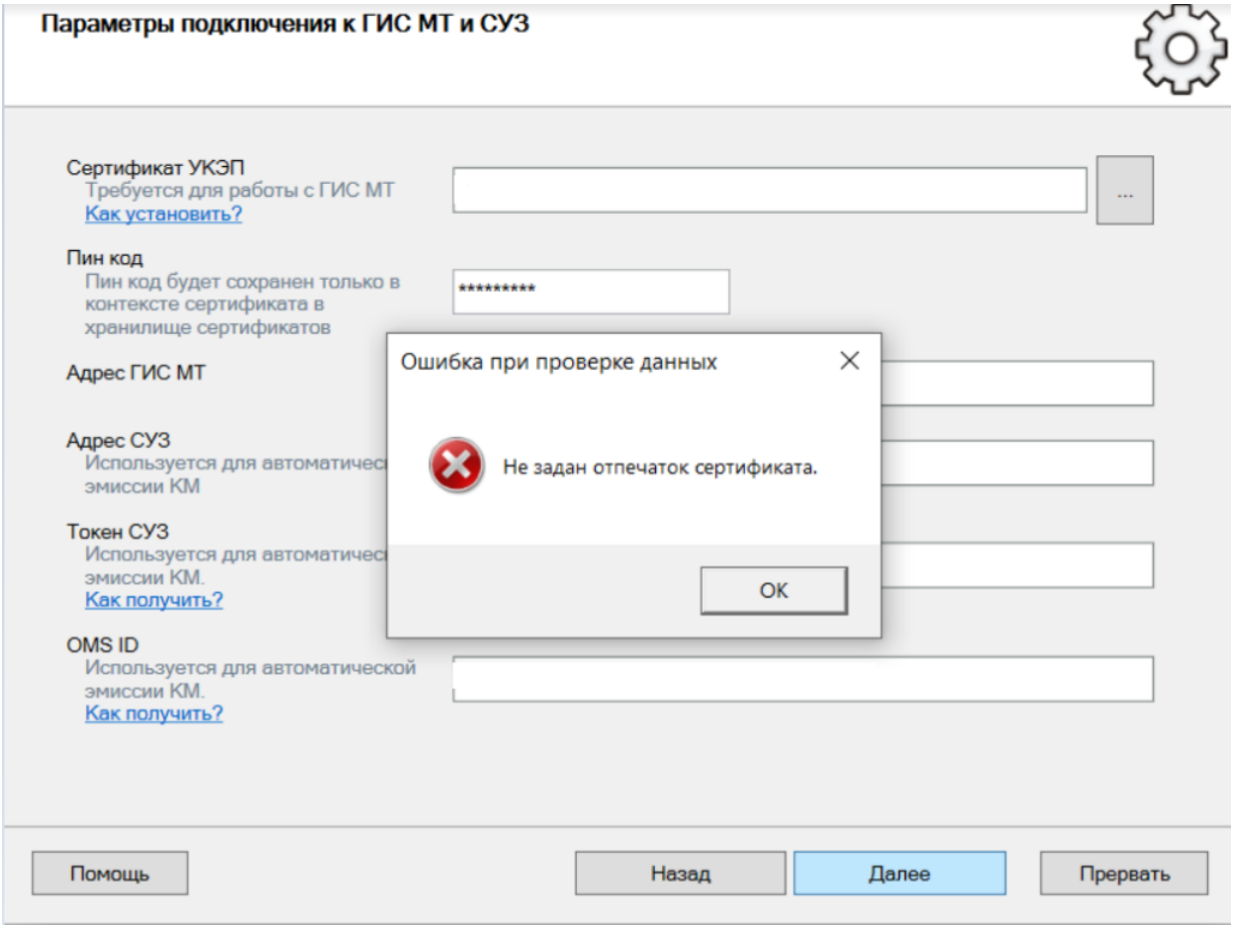
Основные ошибки при установке и настройке «Кировки» и способы их устранения

Последние изменения: 2024-03-26

1. Не задан отпечаток сертификата.
2. Нет прав на доступ к контейнеру приватного ключа в реестре.
3. Ошибка при сохранении пин-кода в контекст сертификата (1).
4. Ошибка подключения к СУЗ (неверный адрес).
5. Ошибка при разворачивании базы из шаблона.
6. Ошибка подключения к ГИС МТ.

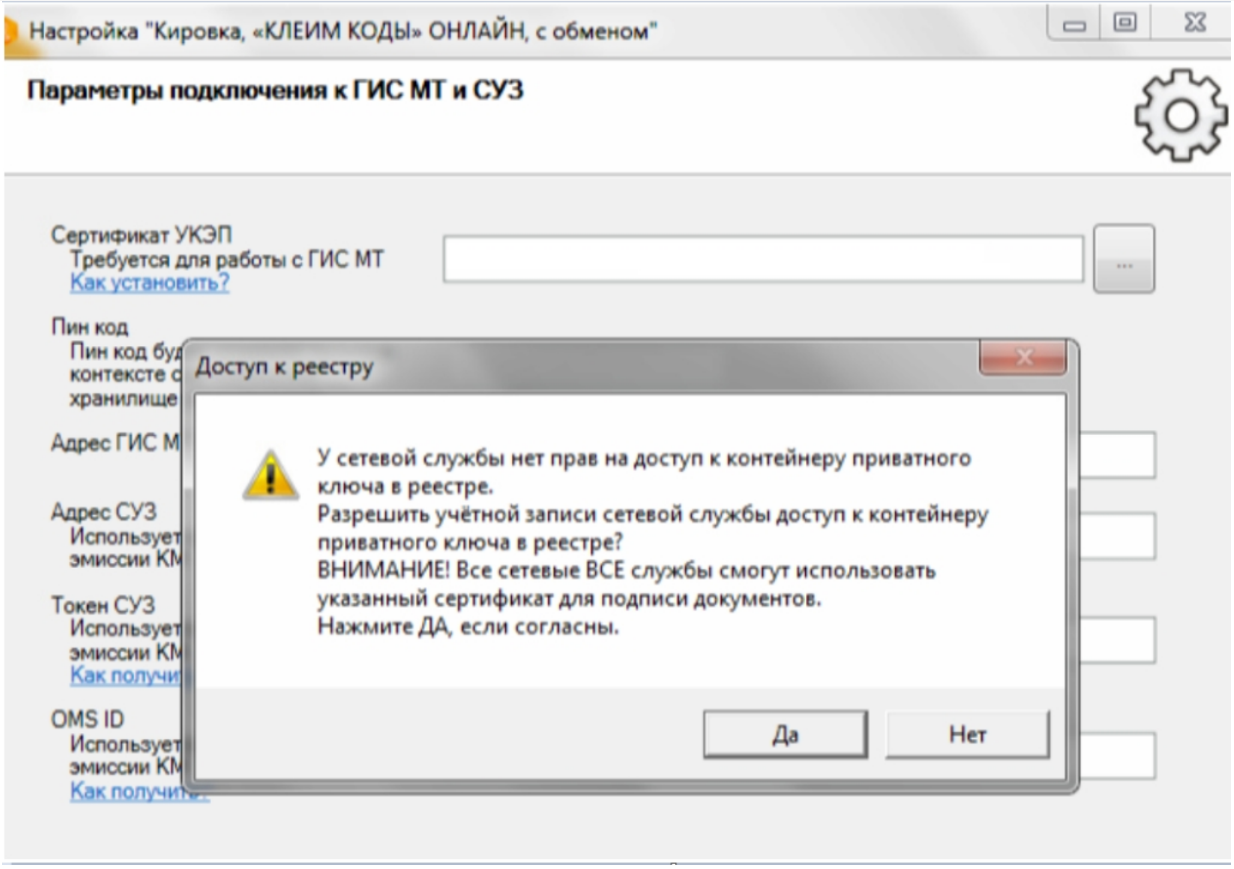
В процессе установки и настройки «Кировки» пользователь может допускать ошибки, из-за которых дальнейшая работа продукта может оказаться невозможной. Рассмотрим некоторые возможные ошибки и способы их устранения.

1. **Не задан отпечаток сертификата.**

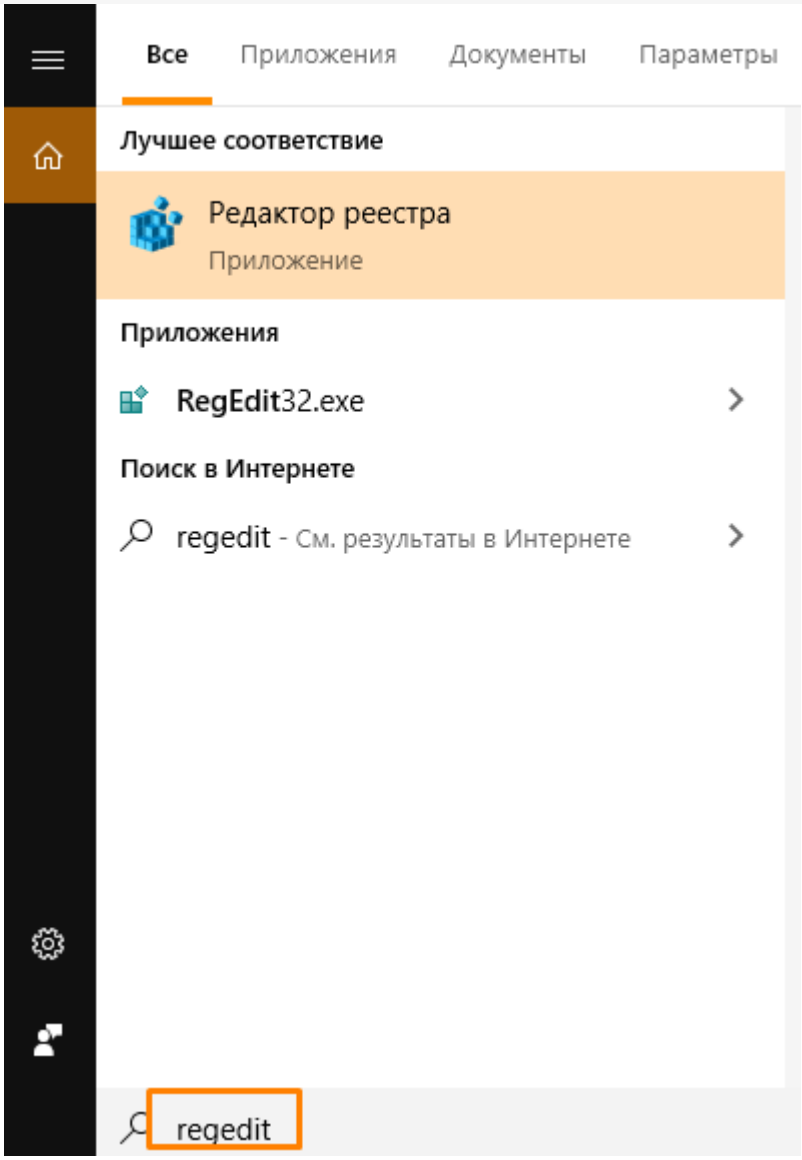


Решение: установить сертификат УКЭП.

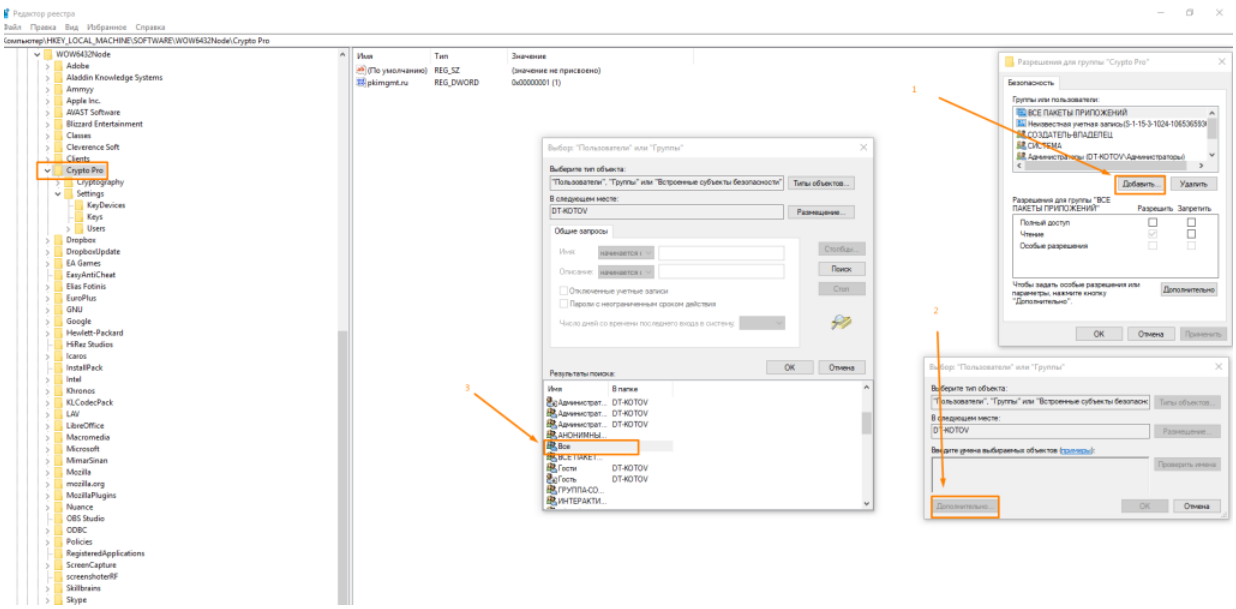
2. **Нет прав на доступ к контейнеру приватного ключа в реестре.**



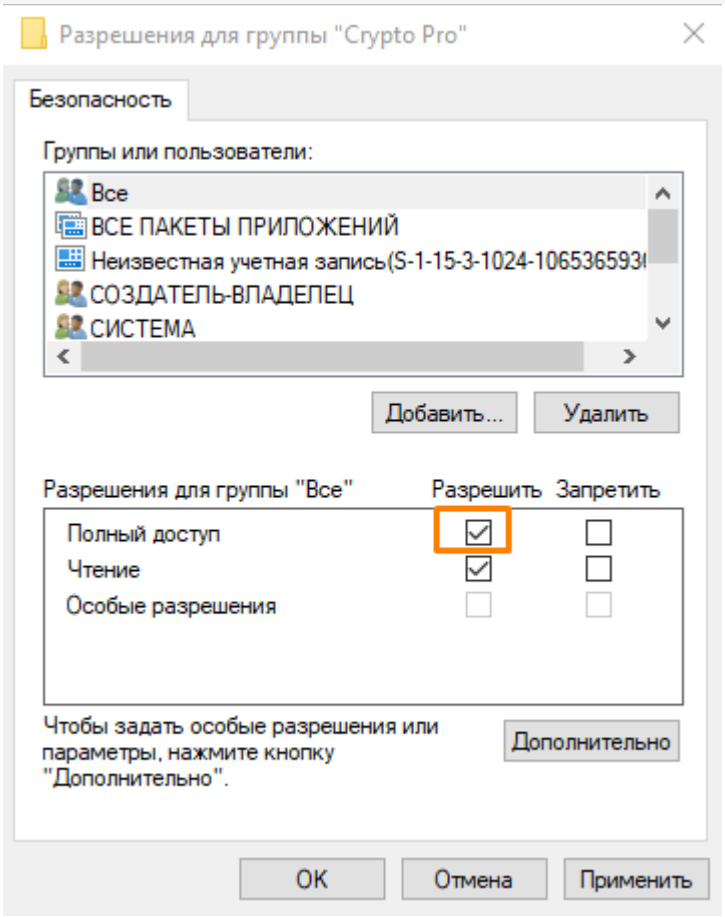
Решение: необходимо дать полные права для КриптоПРО в реестре (кнопка «Пуск» → «Поиск» → ввести «regedit» → правой кнопки мышки по найденному ярлыку «Редактор реестра» → «Запустить от имени администратора»).



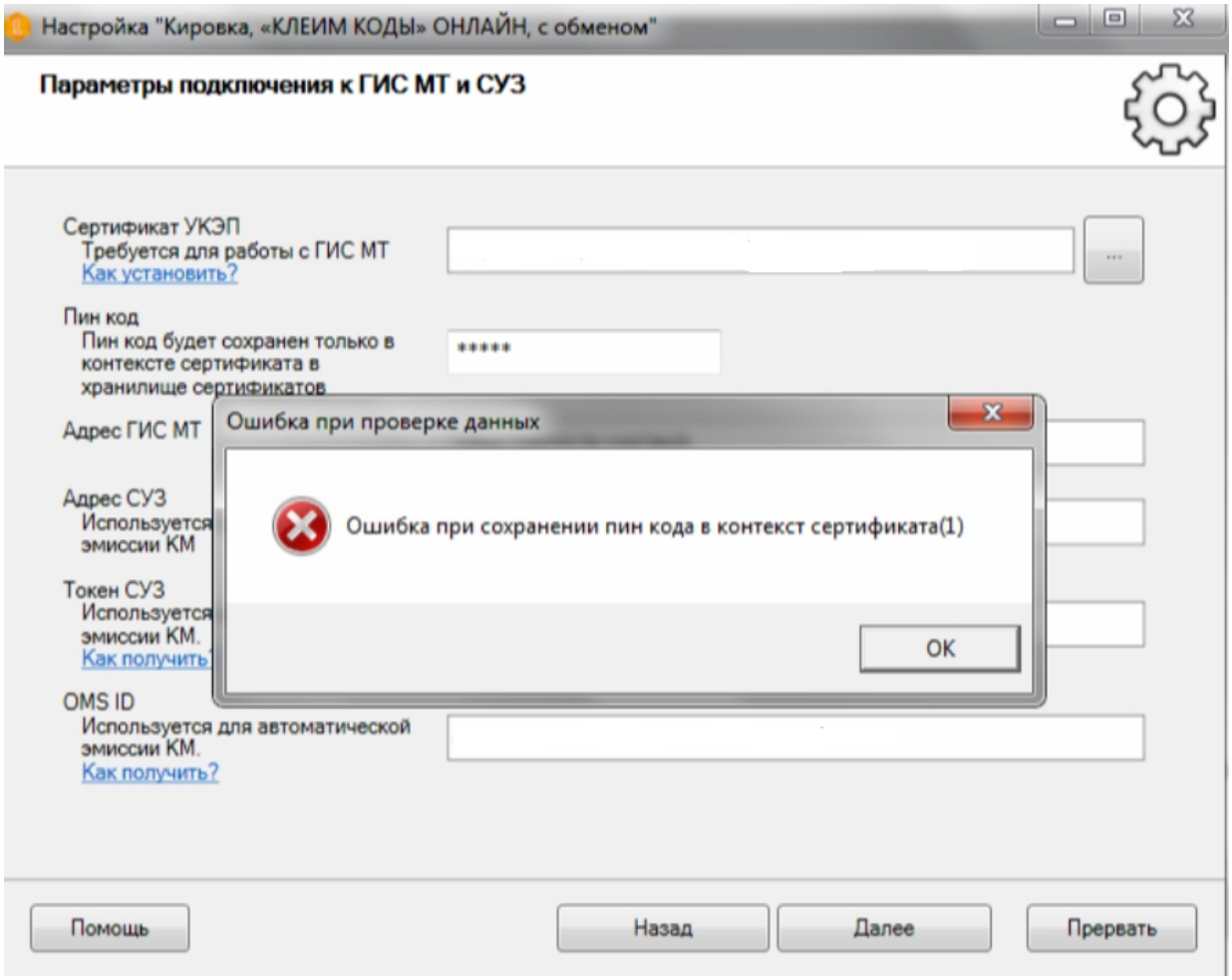
Дать полные права в ветках реестра отдельно для каждой папки «Settings» и «Keys» (HKLM\SOFTWARE{0}\Crypto Pro\Settings\Keys). Для этого также нажмите правой кнопкой мыши на нужной папке реестра и в контекстном меню выберите «Разрешения».



Установите флажок напротив пункта «Полный доступ» и нажмите «ОК».

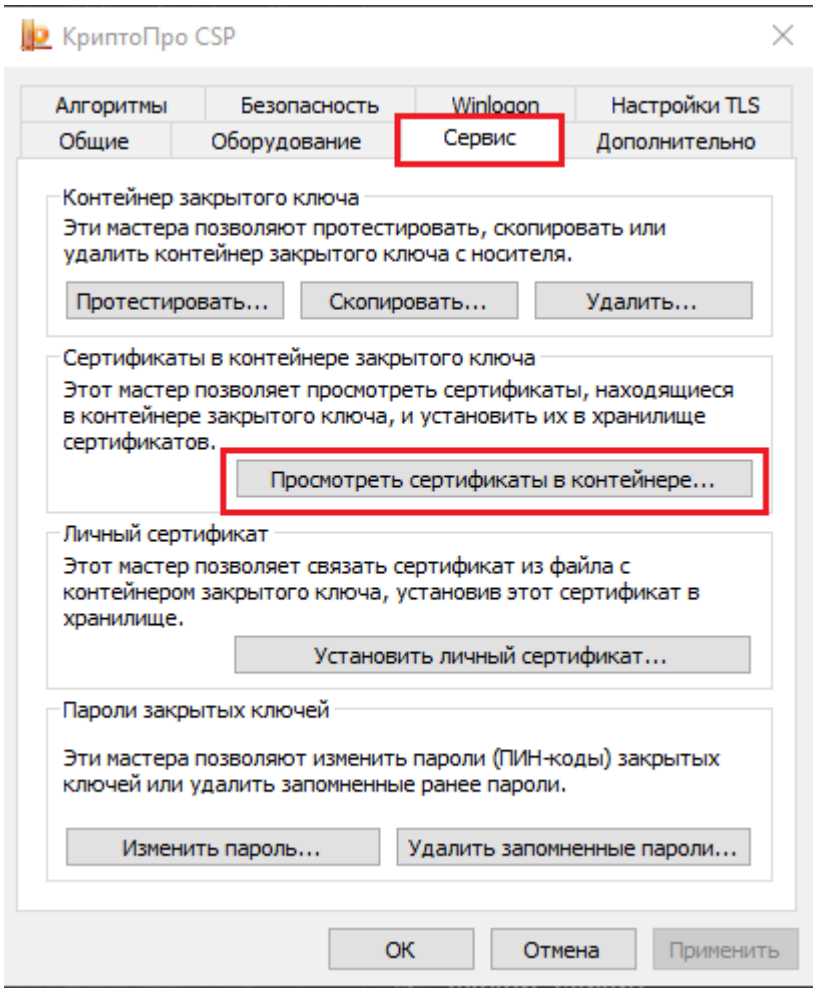


3. **Ошибка при сохранении пин-кода в контекст сертификата (1).**

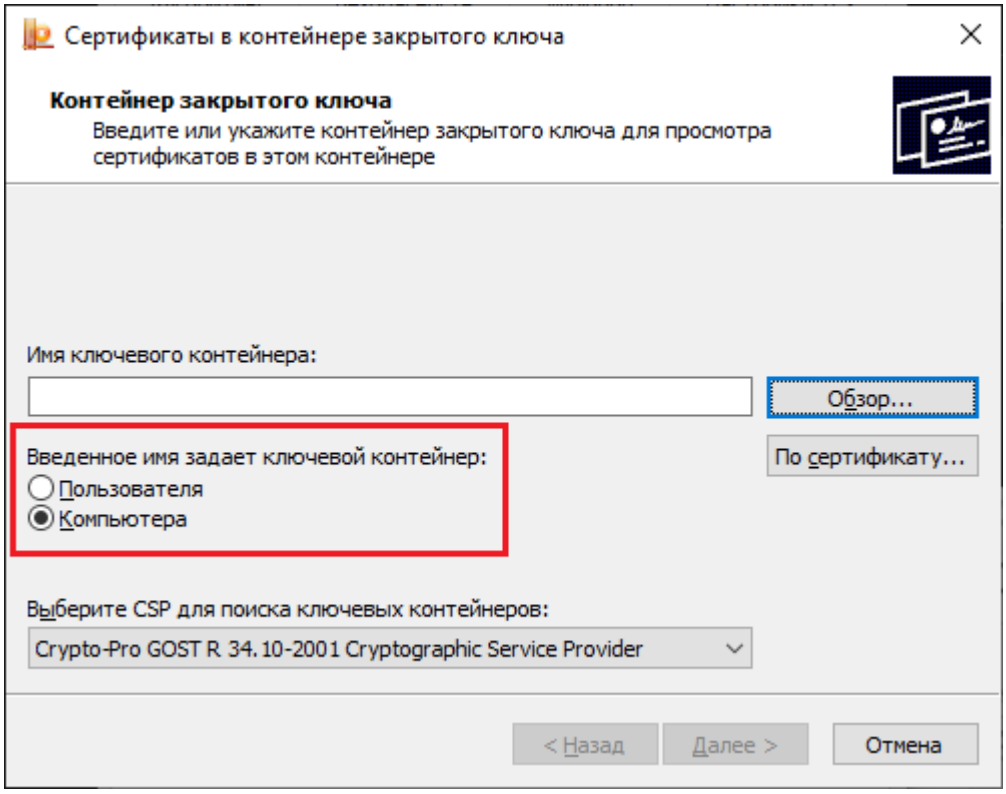


Решение: запустите КриптоПРО от имени администратора (кнопка «Пуск» → «Поиск» → ввести «КриптоПро» → правой кнопки мышки по ярлыку «КриптоПРО» → «Запустить от имени администратора»).

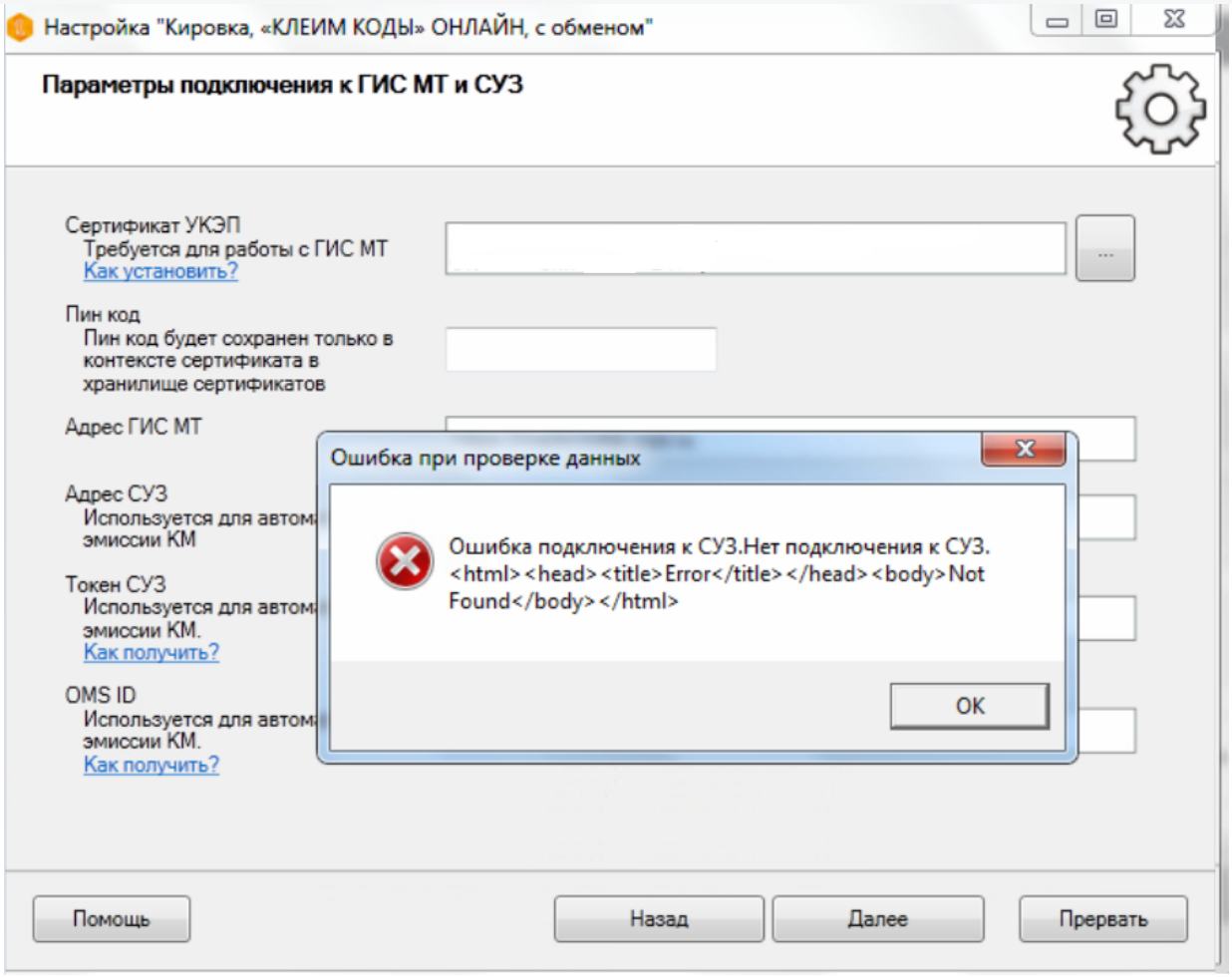
В открывшейся программе «КриптоПРО"выберите на вкладку «Сервис» и нажмите кнопку «Просмотреть сертификаты в контейнере».



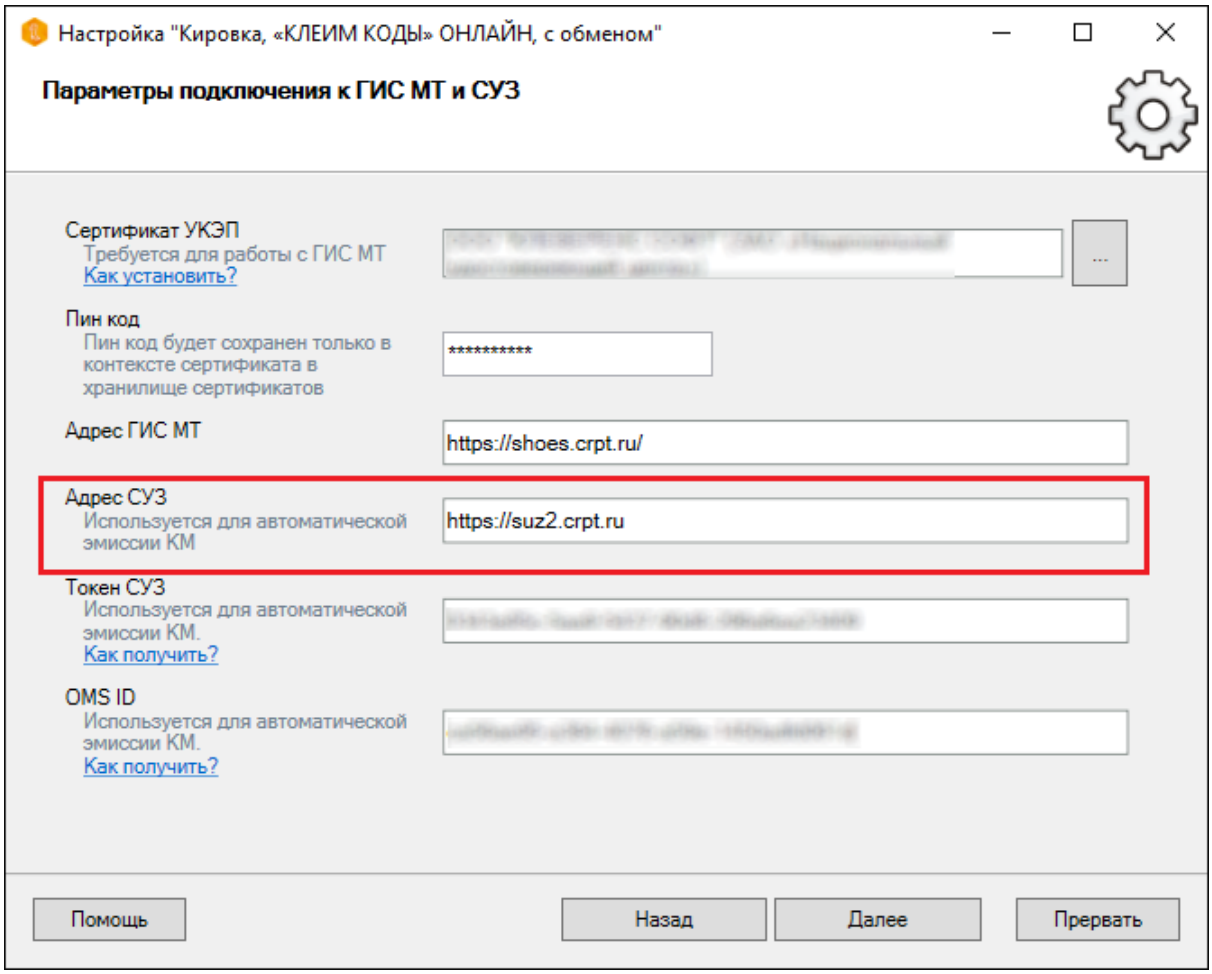
Далее нужно задать сертификат как общий, поставив флажок в пункте «Компьютера».



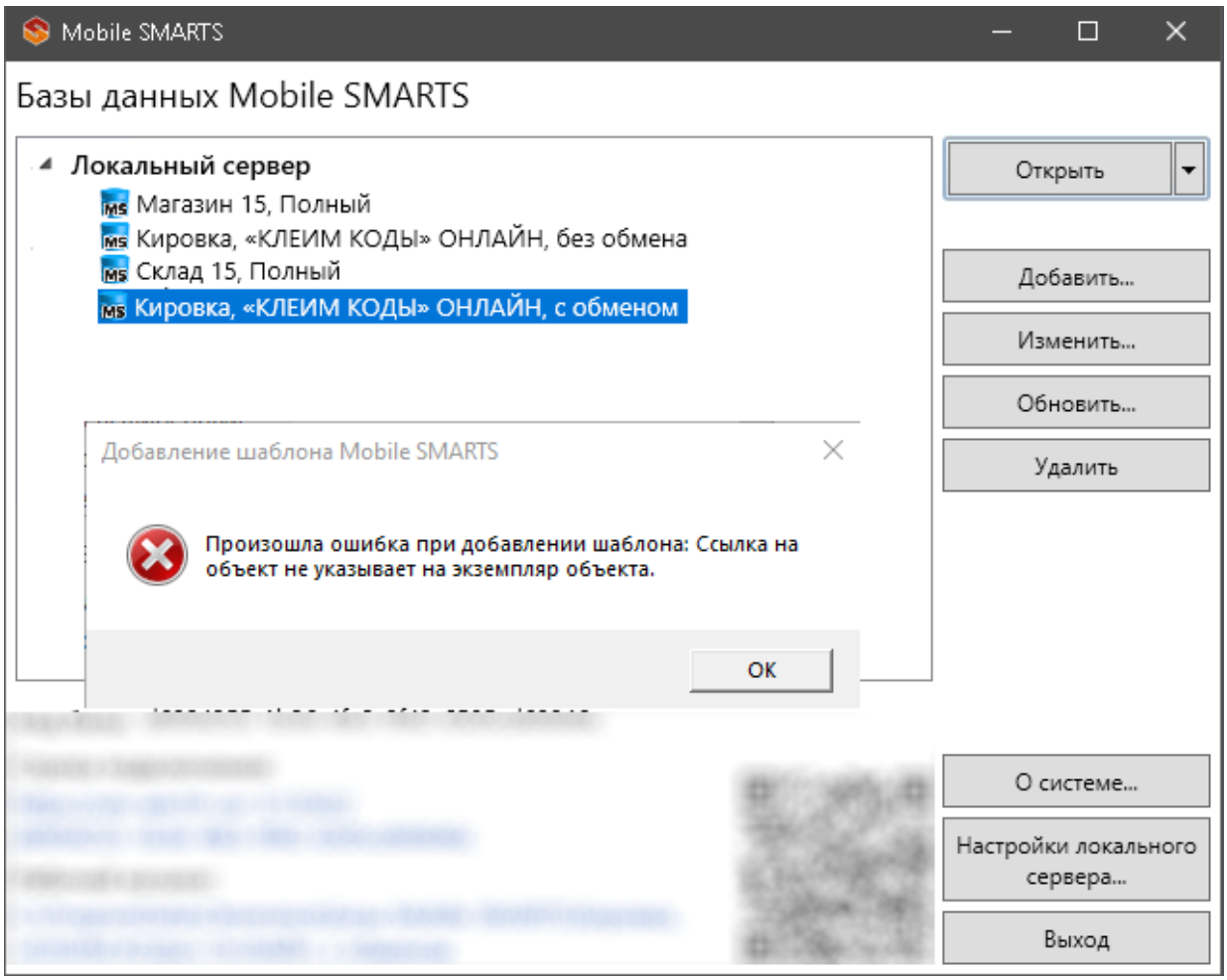
4. **Ошибка подключения к СУЗ (неверный адрес).**

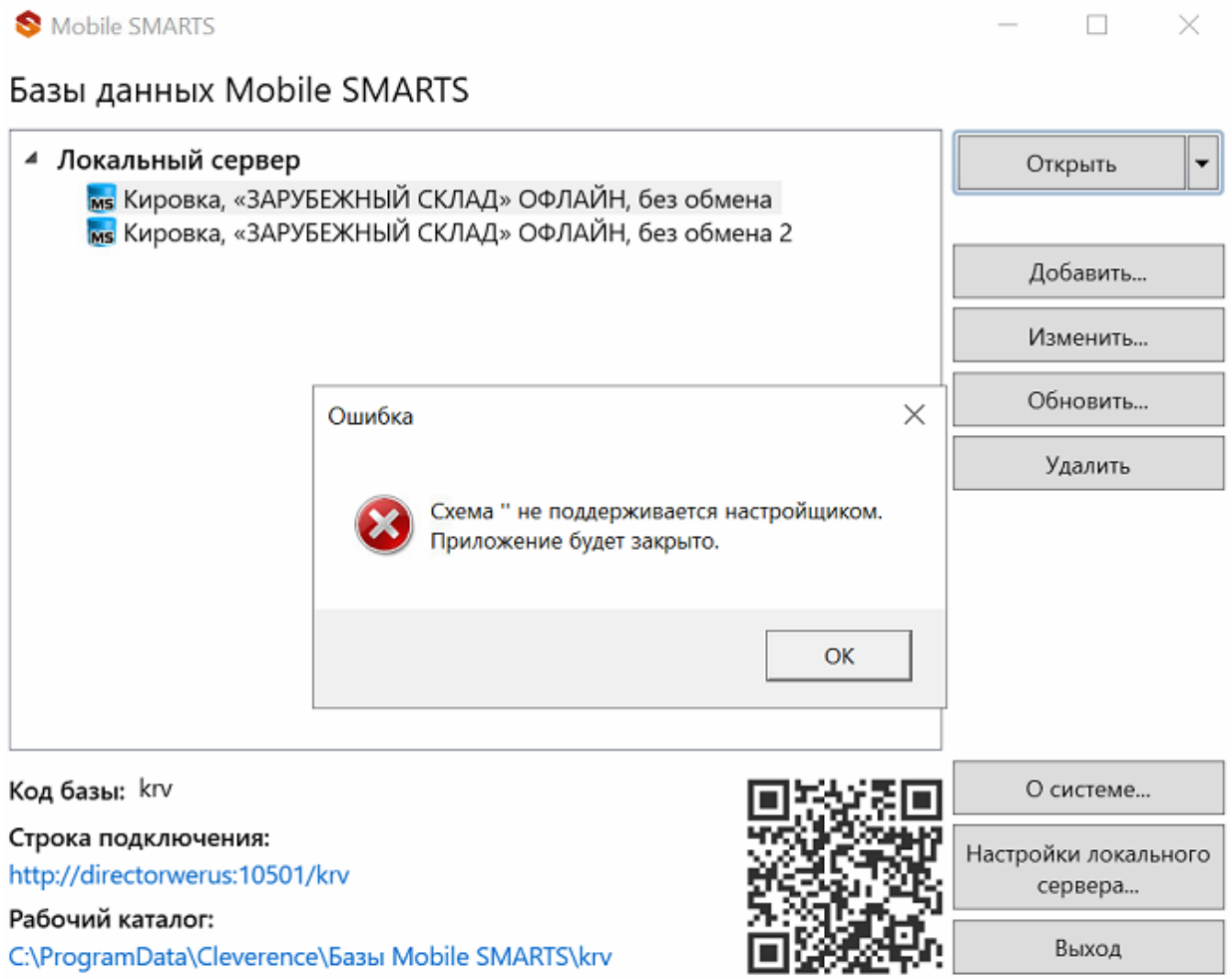


Решение: указать верные реквизиты (см.ниже).



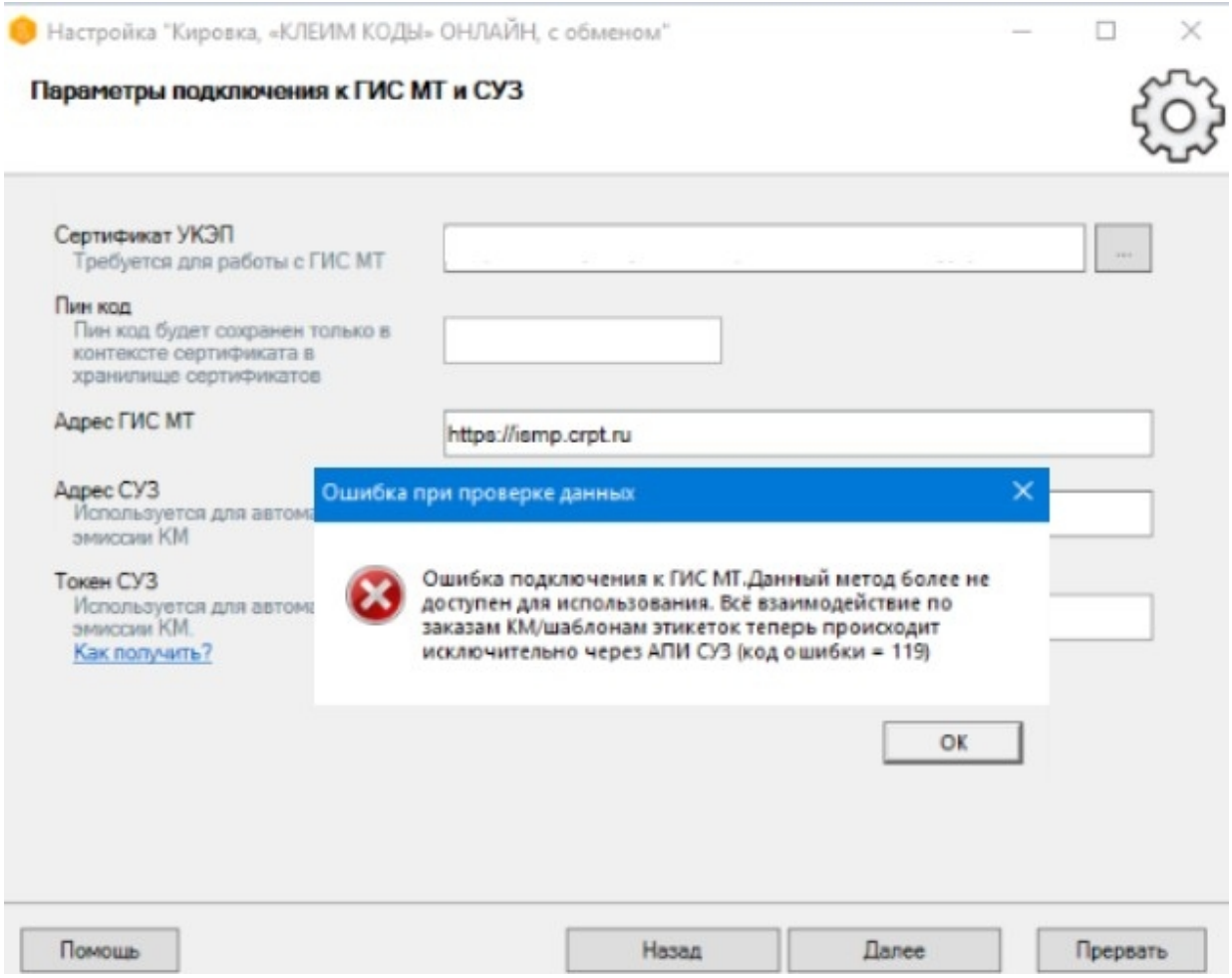
5. **Ошибка при разворачивании базы из шаблона.**





Решение: разворачивать базу из специального установщика Кировки.

6. **Ошибка подключения к ГИС МТ.**



Решение: установлен старый релиз. Скачайте актуальную версию «Кировки».

Адрес подключения к ГИС МТ — https://markirovka.crpt.ru/.

Не нашли что искали?

Задать вопрос в техническую поддержку

Веб-версия приложения «Кировка»

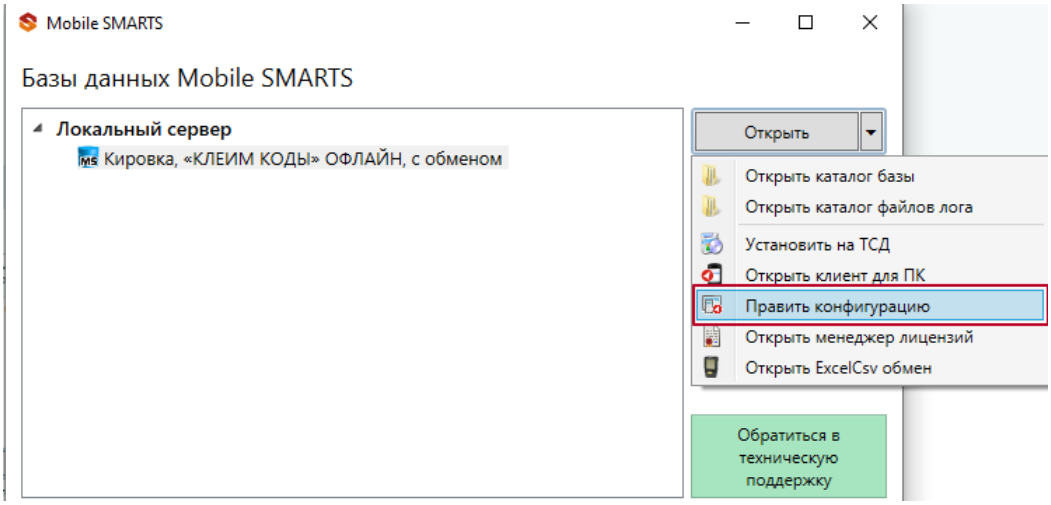
Последние изменения: 2024-03-26

Веб-версия приложения базы данных Mobile SMARTS – это возможность подключиться к уже установленной базе Mobile SMARTS с любого ПК, используя браузер.

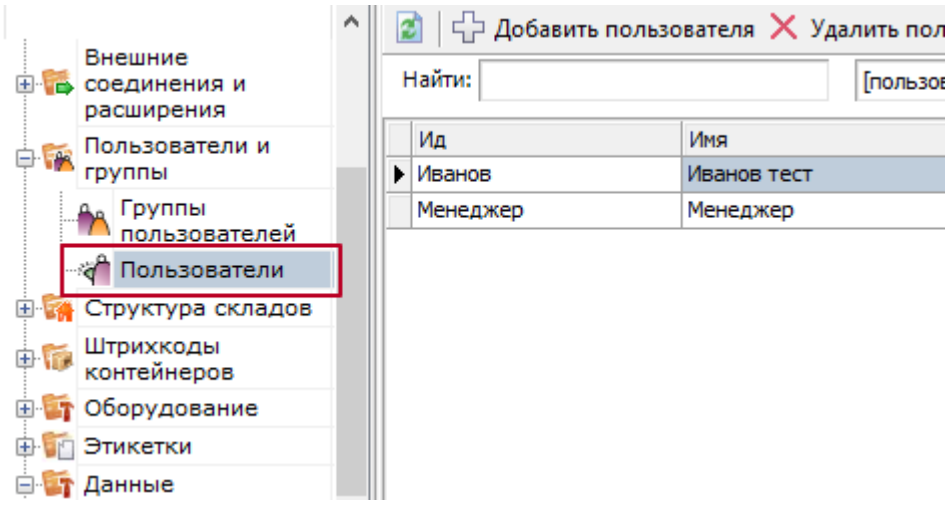
Предварительная настройка

Перед тем как начать работу с веб-приложением, необходимо разрешить доступ к нему некоторым пользователям или группам пользователей. Для этого:

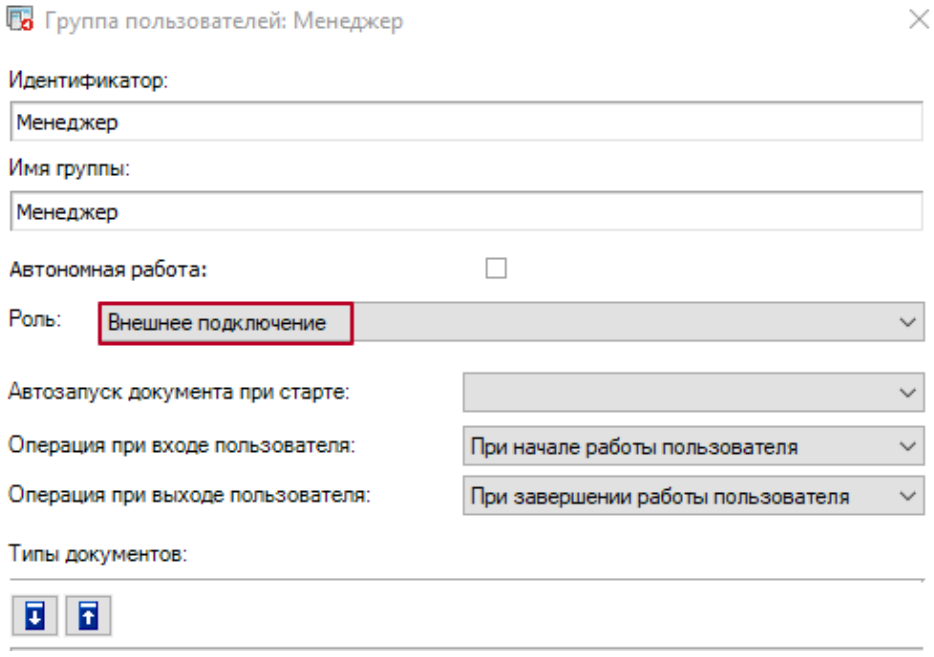
- **Запустите панель управления Mobile SMARTS.**



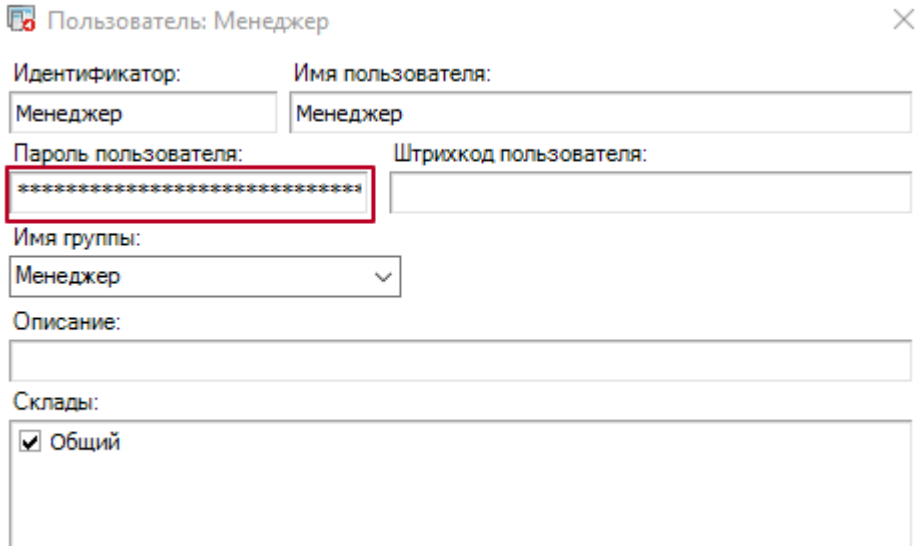
- **Выберите пункт «Пользователи и группы». Там вы можете выбрать группу из уже существующих, или завести нового пользователя.**



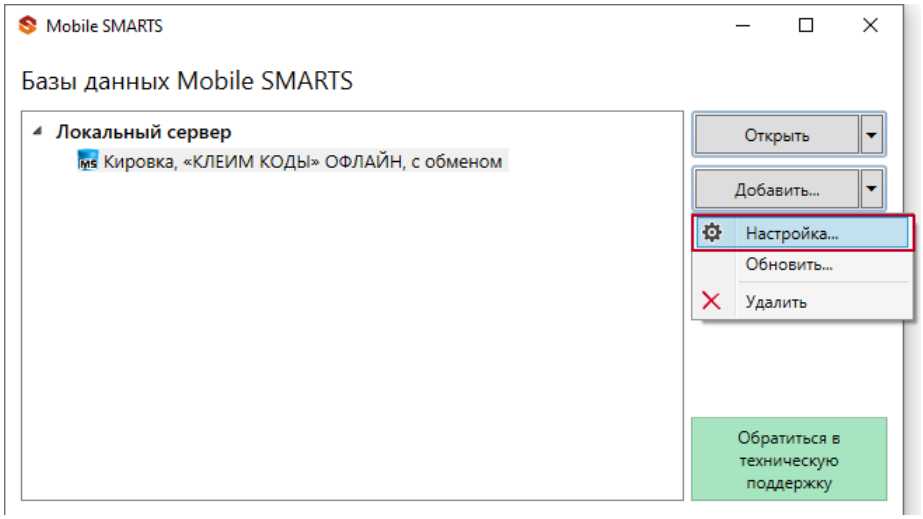
- **Назначьте роль «Администратор» или «Внешнее подключение» той группе пользователей, которой вы хотите дать доступ к веб-приложению.**

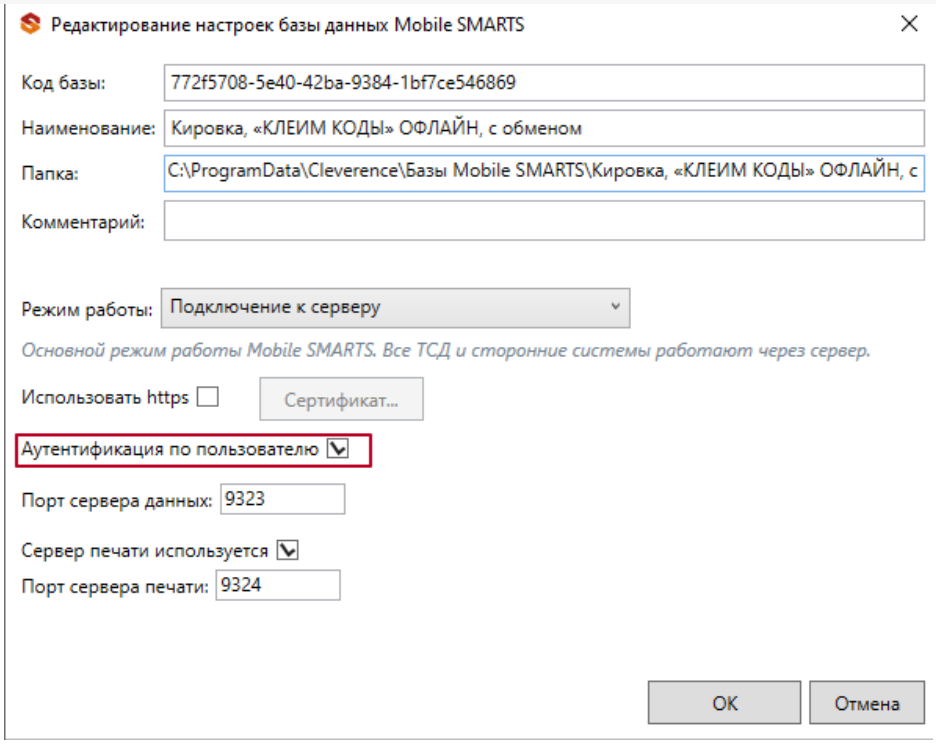


- **Заведите пользователей и назначьте для них пароли.**



- **Включите аутентификацию по пользователю для вашей базы.**





Важно! Убедитесь, что до активации данной функции у всех пользователей назначены пароли. Так как никто из пользователей не сможет без паролей подключиться к базе Mobile SMARTS, пока функция аутентификации будет активна, в том числе и операторы терминалов сбора данных!

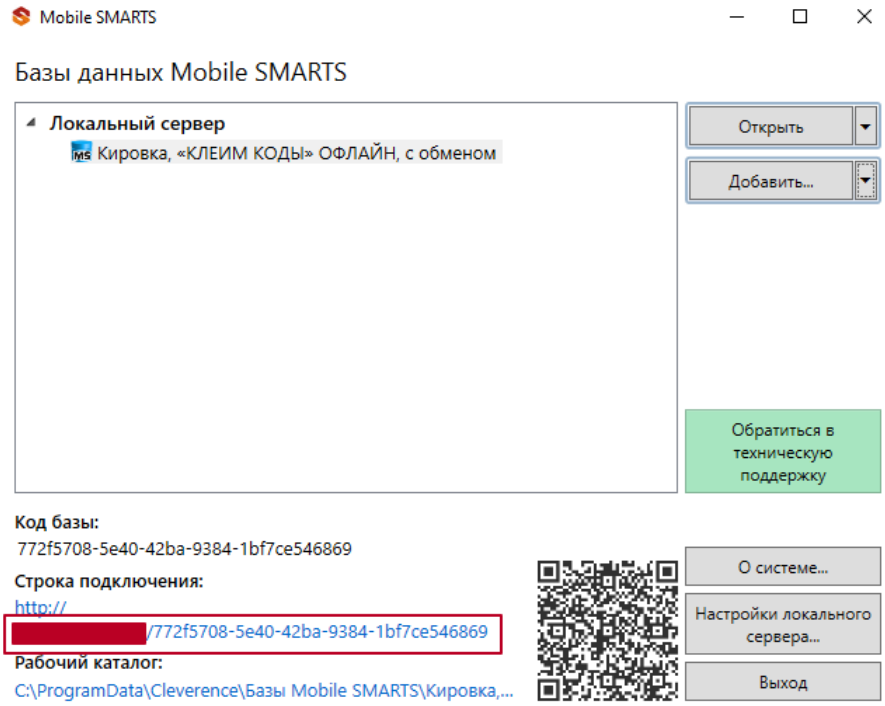
После этого вы можете подключаться к веб-приложению.

Подключение

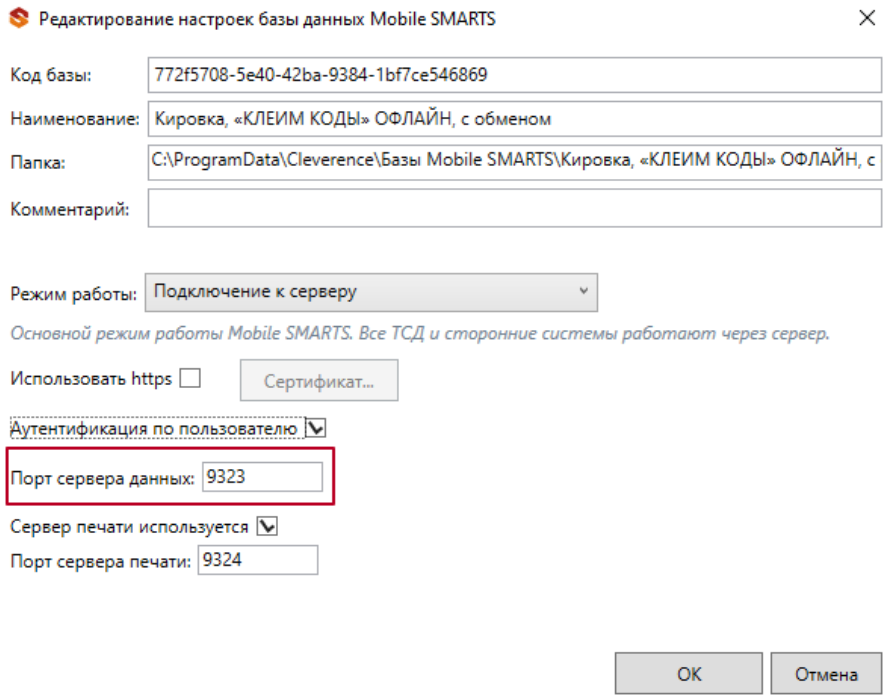
> Для работы с веб-приложением базы Mobile SMARTS рекомендуем использовать браузеры Google Chrome, Mozilla, Edge последних версий.

Для подключению к веб-приложению вам необходимо вписать в строку браузера URL: «адрес веб-сервера Mobile SMARTS: порт базы/www/».

IP-адрес веб-сервера, на котором размещена ваша база Mobile SMARTS, вы можете узнать в менеджере баз.



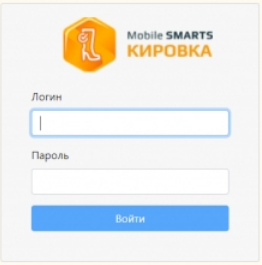
Порт базы вы можете посмотреть в окне редактирования настроек базы Mobile SMARTS (там же где и указывали настройку «Аутентификацию по пользователю»).



Если ваш ПК и сервер Mobile SMARTS находятся в одной локальной сети, вы можете указать адрес для подключения «http://localhost: порт базы/».

При подключении через веб-приложение к базе Mobile SMARTS, которая находится на удаленном сервере, используется метод перенаправления (проброса) портов. Проброс портов – это процесс пересылки трафика, адресованного конкретному сетевому порту с одного сетевого узла на другой. Подробно данный процесс описан в статье «Подключение мобильного устройства к удаленному серверу Mobile SMARTS» .

После подключения главное окно веб-приложения выглядит следующим образом:

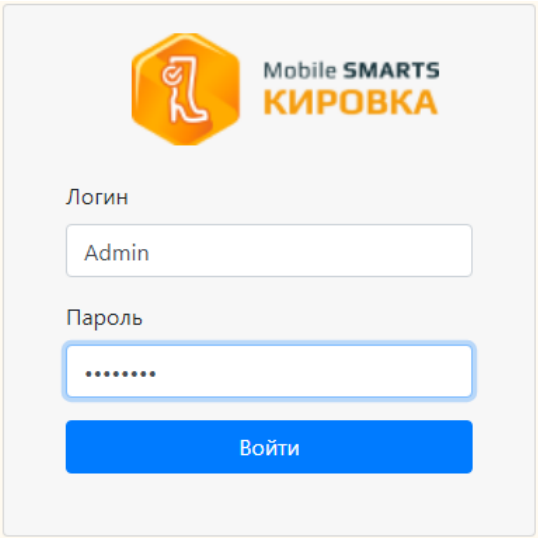


Функционал веб-приложения

Авторизация

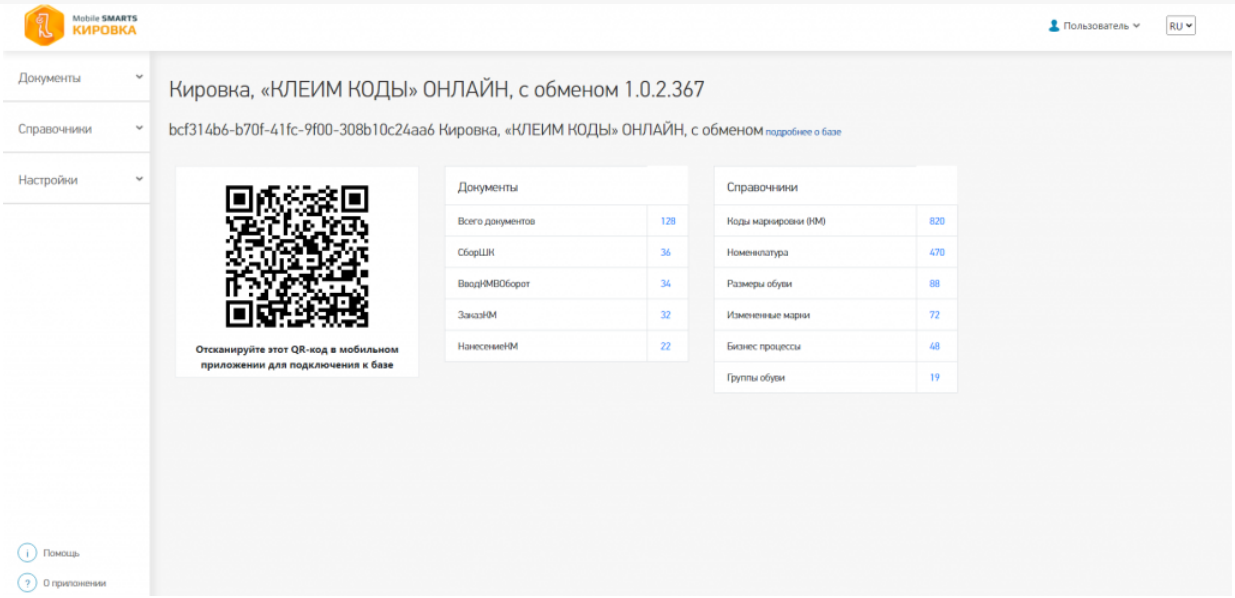
Для подключения к базе Mobile SMARTS через веб-приложение необходимо пройти авторизацию по логину и паролю.

Логин - это имя пользователя базы Mobile SMARTS (в текущей версии веб-приложения поддерживается использование только латинских символов), пароль – это пароль пользователя.



Главная страница

После успешной авторизации открывается главная страница веб-приложения со следующими элементами:



- **Быстрая навигация по основным документам и справочникам.**

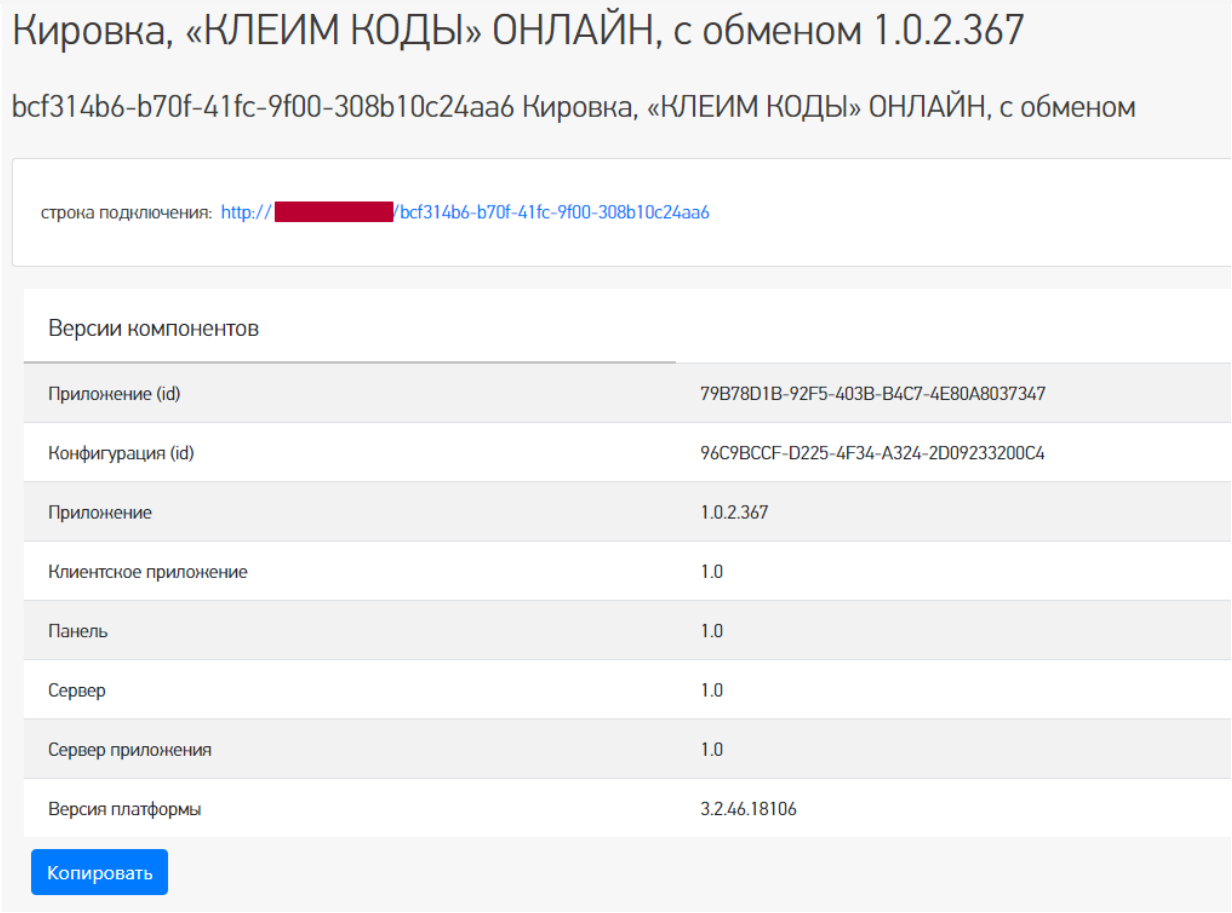
Документы	
Всего документов	128
СборШК	36
ВводКМВОборот	34
ЗаказКМ	32
НанесениеКМ	22

Справочники	
Коды маркировки (КМ)	820
Номенклатура	470
Размеры обуви	88
Измененные марки	72
Бизнес процессы	48
Группы обуви	19

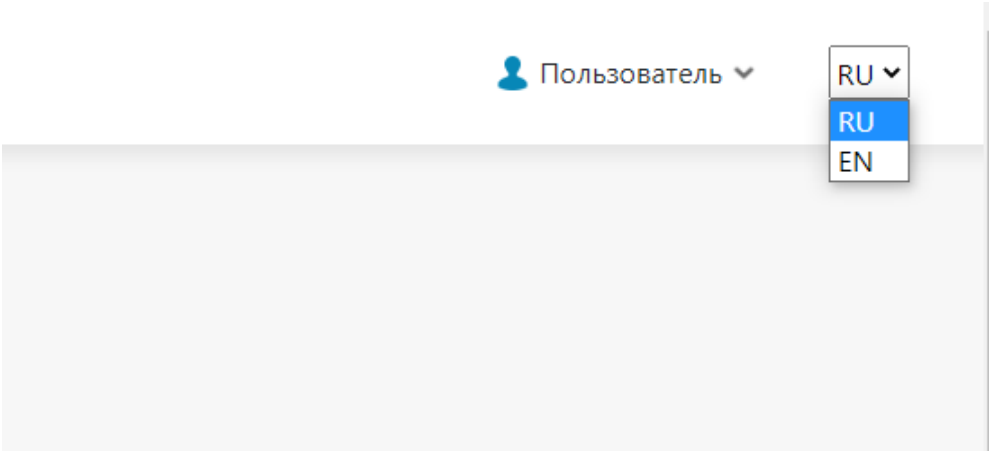
- **QR-код, который можно отсканировать в мобильном приложении для подключения мобильного устройства к базе.**

Отсканируйте этот QR-код в мобильном приложении для подключения к базе

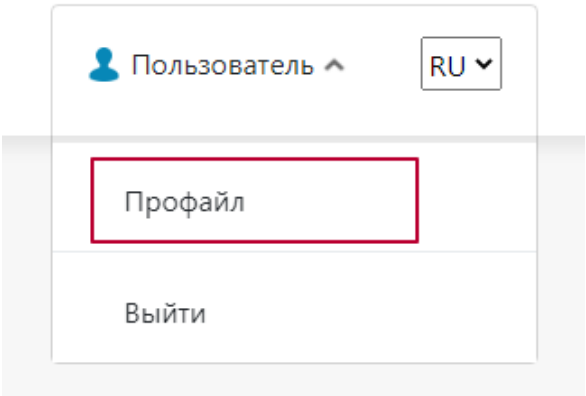
- **Ссылка «Подробнее о базе», по которой можно узнать версию базы и приложения, а также путь подключения к базе.**



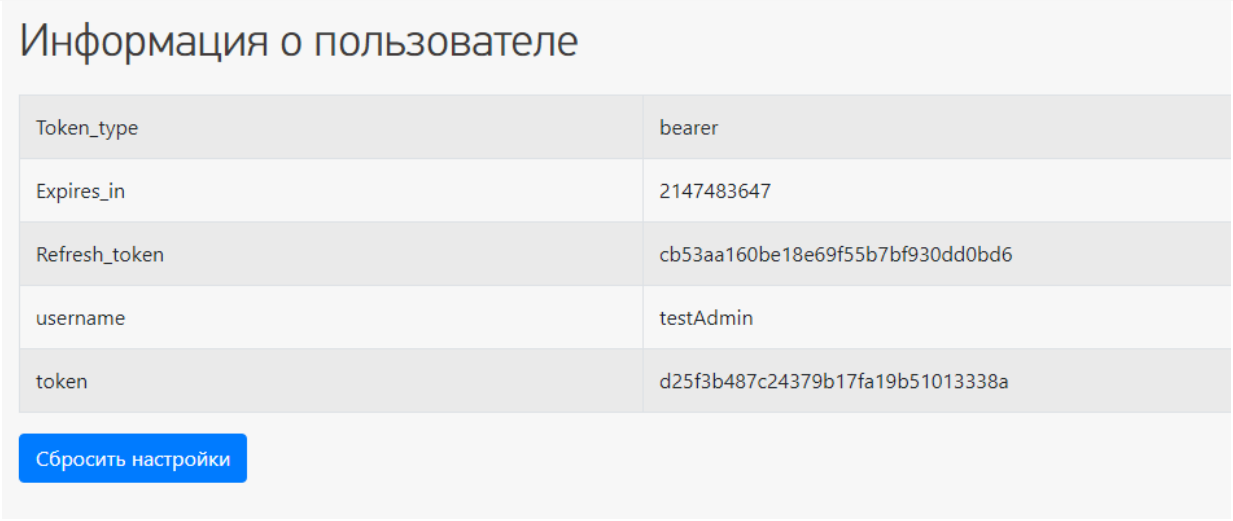
- **Переключение языка интерфейса с русского на английский и наоборот.**



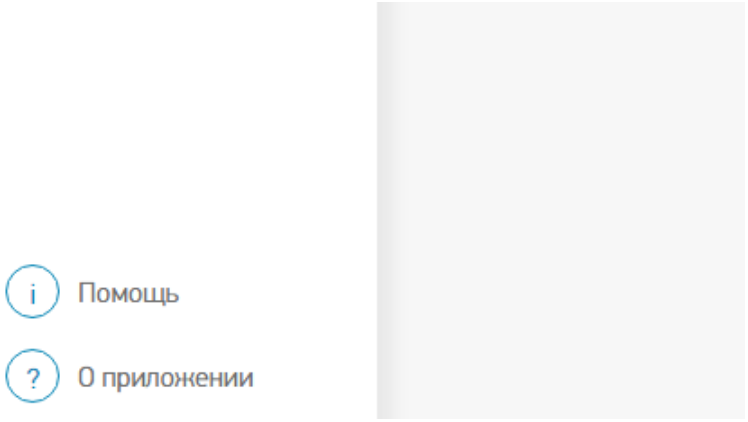
- **Страница профиля пользователя.**



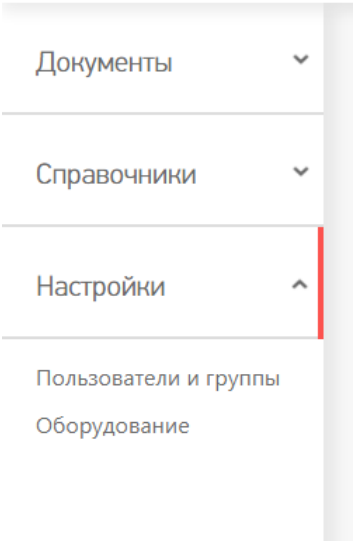
Здесь вы можете сбросить настройки, связанные с отображением столбцов в таблице, группировкой колонок.



- **Ссылки на страницу продукта и базу знаний по продукту.**



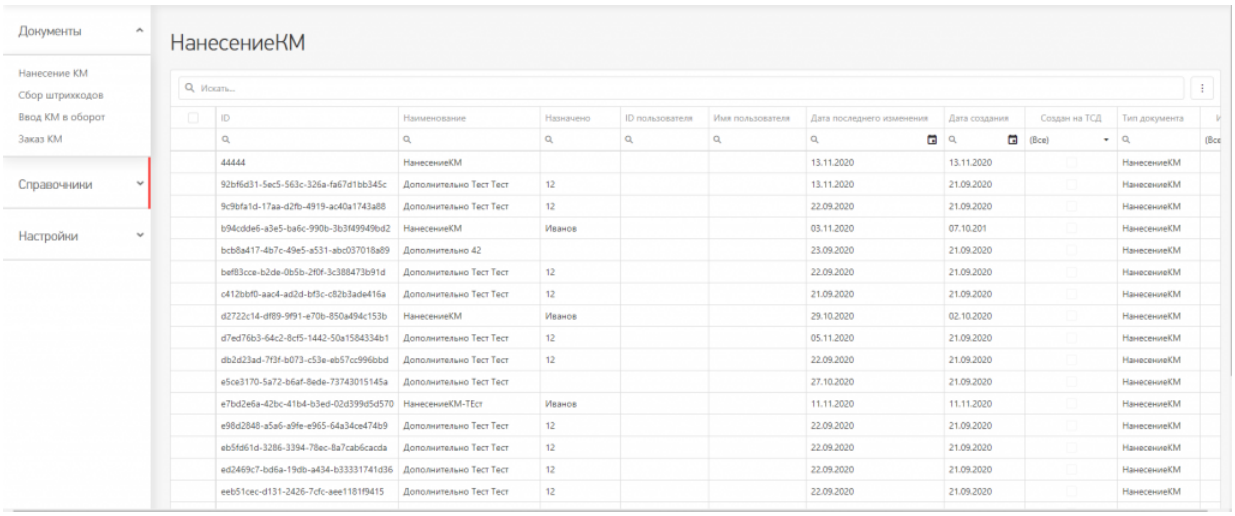
- **Основное меню в виде выпадающего списка, где вы можете посмотреть таблицы документов, номенклатуры и остальных справочников, а также информацию о пользователях базы и мобильных устройствах, подключенных к базе.**



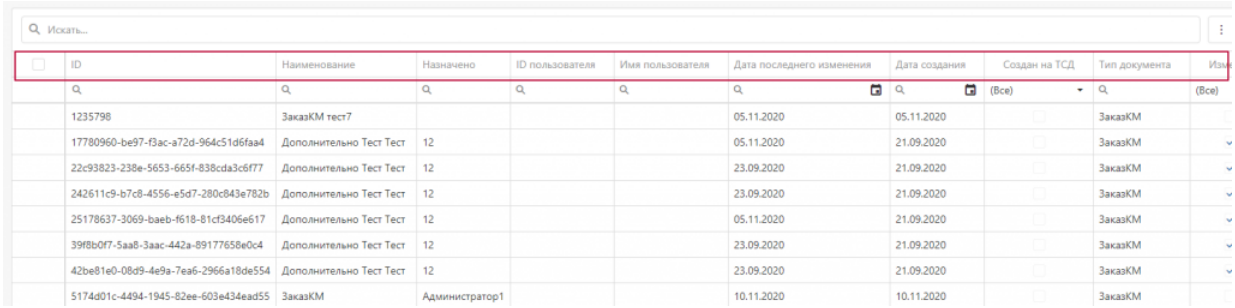
Основное меню

Документы

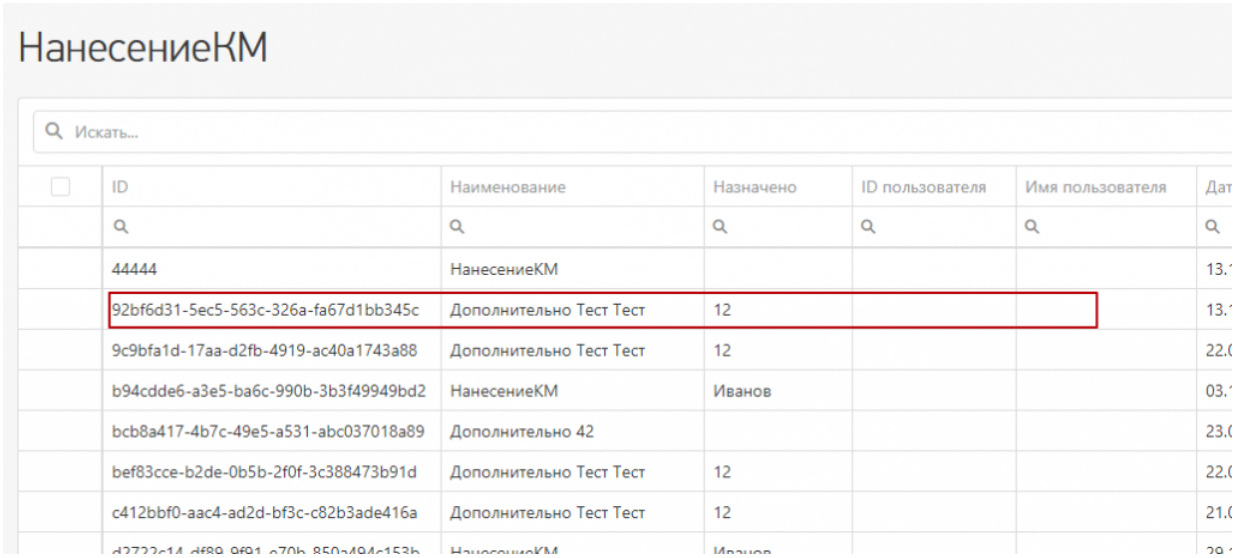
В данном разделе вы можете просмотреть документы базы Mobile SMARTS. Все документы рассортированы согласно их типу.

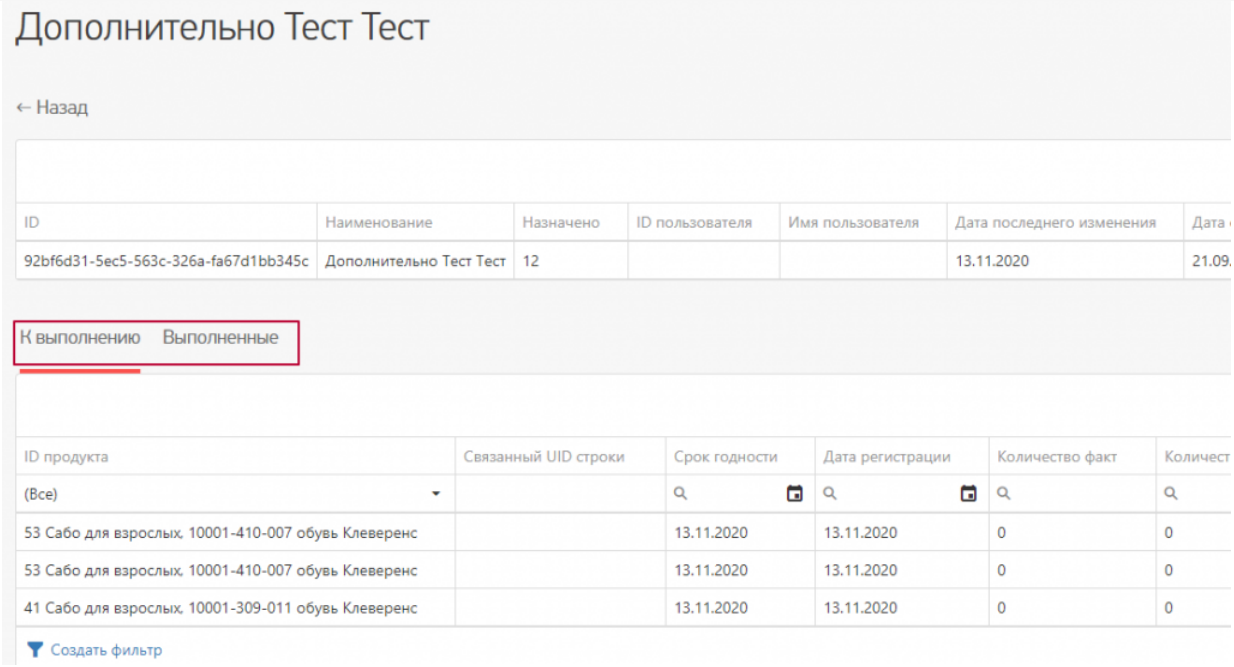


Основные и дополнительные поля документов находятся в шапке таблицы.



Содержание документов, списки «К выполнению» и «Выполнено» находятся внутри документа. Для перехода к этим вкладкам необходимо два раза кликнуть на необходимый вам документ в списке.

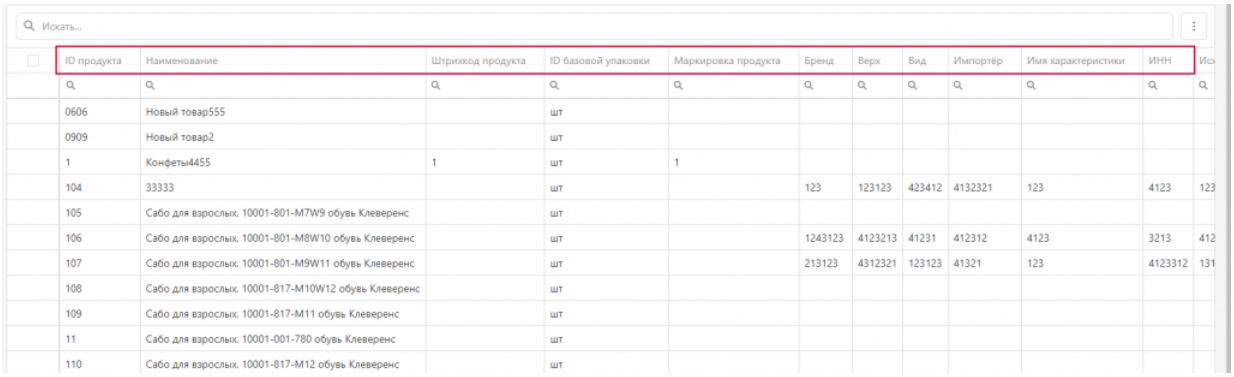




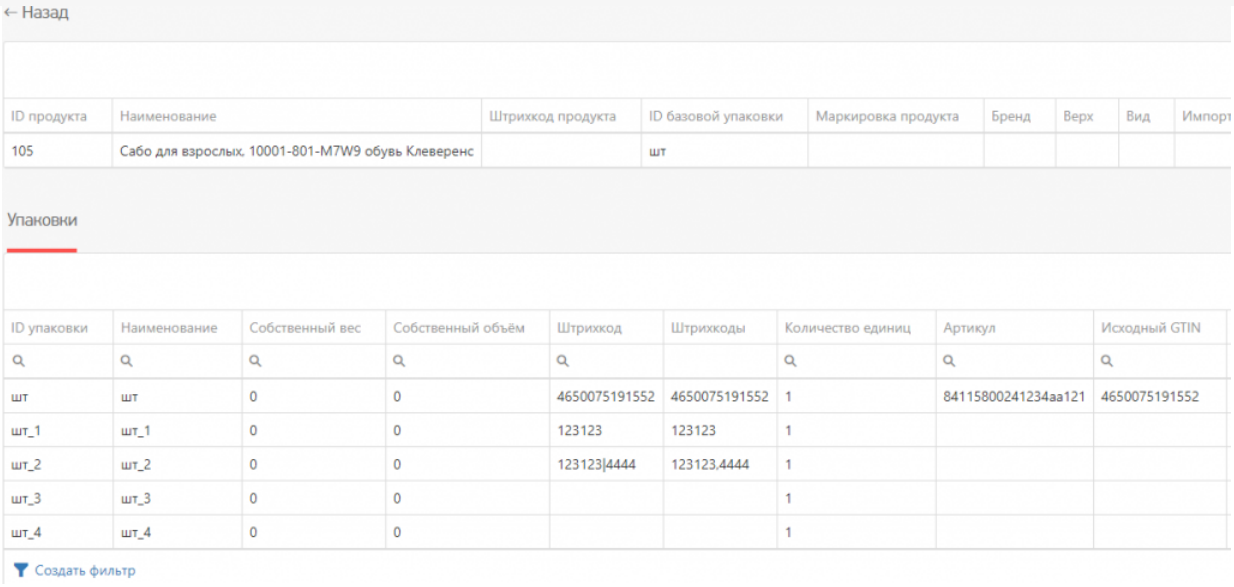
Внутри документа вы сможете переключиться между вкладками «К выполнению» и «Выполнено» и просмотреть список товаров/номенклатуры, которые требуется обработать на мобильном устройстве по данному документу.

Номенклатура

В таблице «Номенклатура» вы можете просмотреть весь список товаров, которые находятся на сервере Mobile SMARTS. В данной таблице основные и дополнительные поля номенклатуры выведены в общий список, то есть между ними нет различий.



Для того, чтобы просмотреть список упаковок, принадлежащий конкретной номенклатуре/товару, необходимо войти «внутрь» номенклатуры, кликнув по нужной позиции в таблице два раза.



В данном списке содержатся все упаковки, принадлежащие конкретной номенклатуре. Основные и дополнительные поля упаковок содержатся в общем списке.

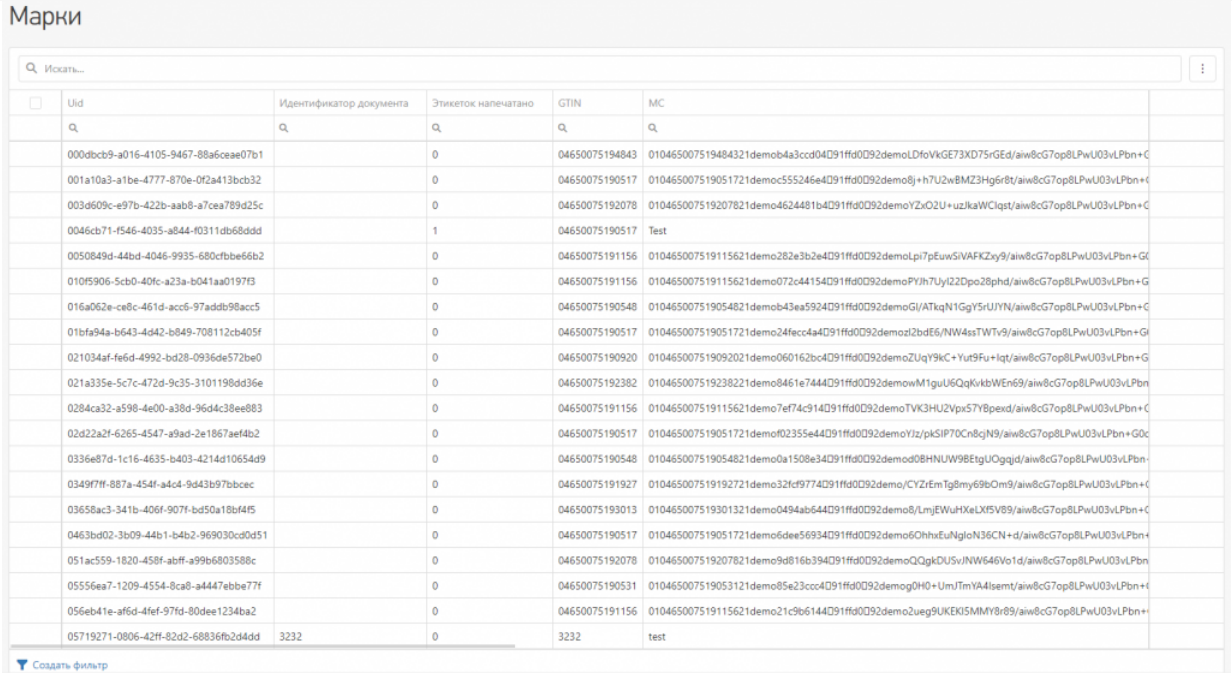
Остальные справочники

К остальным справочникам относятся все таблицы из базы Mobile SMARTS.

В веб-приложении они будут расположены в меню под номенклатурой.

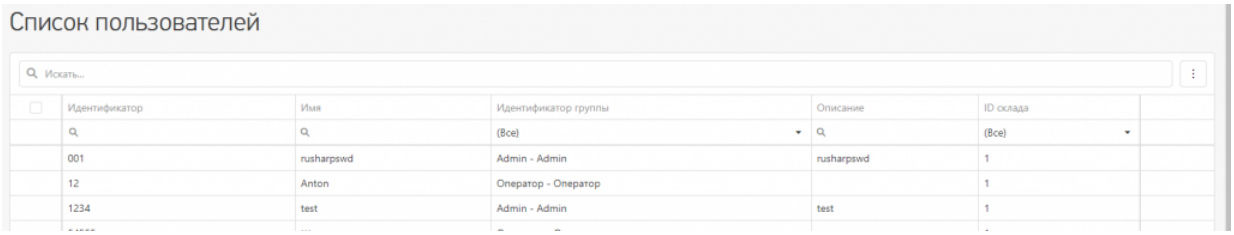
- Бизнес процессы
- Группы обуви
- Измененные марки
- Коды принятых решений
- Контрагенты
- Коды маркировки (КМ)
- Пол обуви
- Размеры обуви
- Сертификаты
- Способ ввода
- Страна производства
- Тип маркировки
- ТНВЭД
- Удаленные заказы
- Узлы
- Виды нанесения
- Виды обуви
- Временные коды

Каждая таблица вынесена отдельно, согласно своему типу. У каждой таблицы имеется свой набор полей.



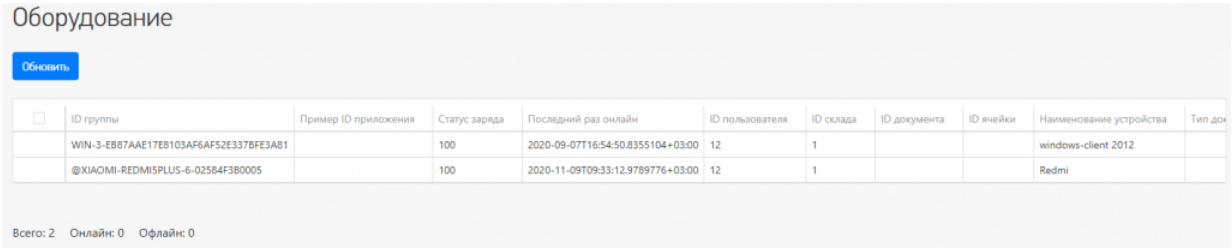
Пользователи и группы

В данном разделе отображается информация о всех пользователях, которые заведены в базе Mobile SMARTS.

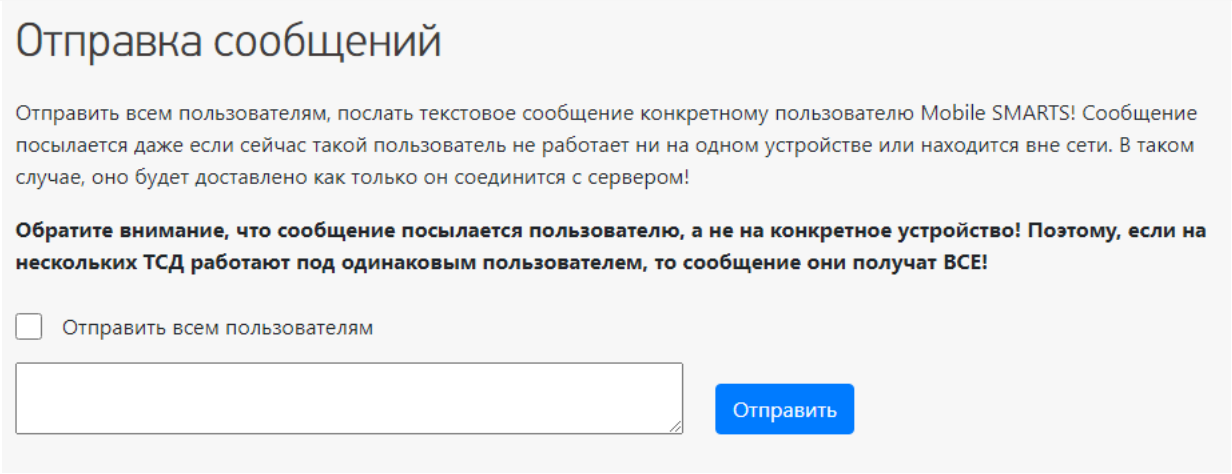


Оборудование

Здесь можно просмотреть список мобильных устройств, которые подключены к базе Mobile SMARTS.



Также вы можете отправить сообщение на мобильное устройство, и пользователь увидит его у себя на устройстве.

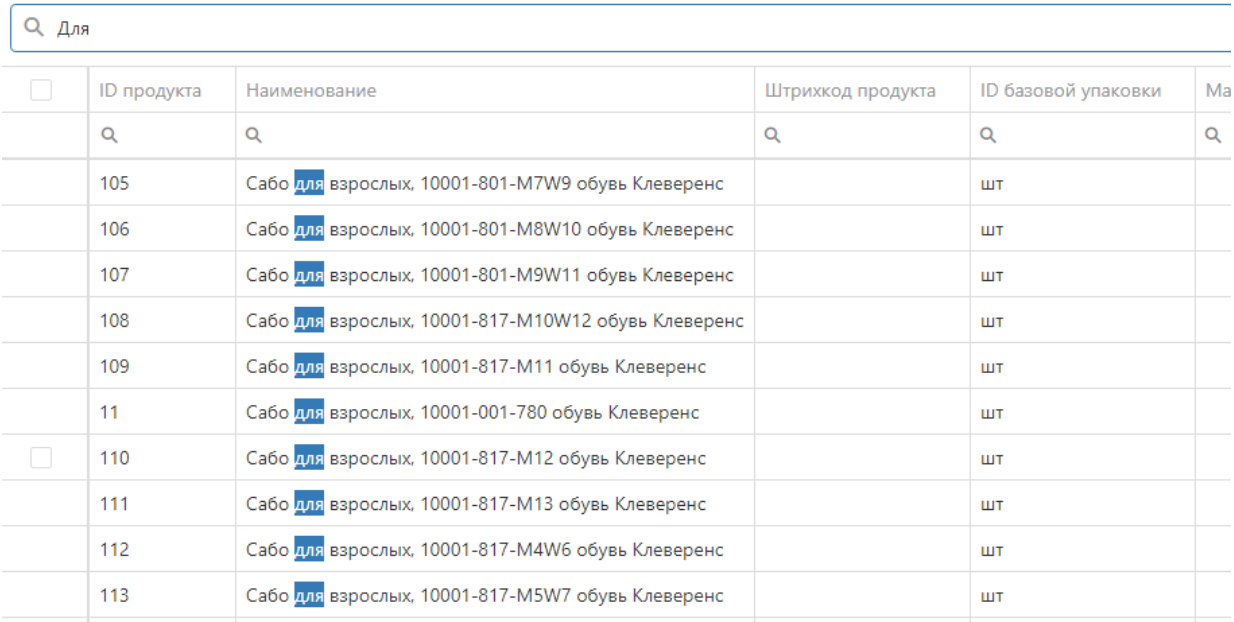


Работа с таблицами

В веб-приложении возможны следующие операции с таблицами документов, номенклатуры и остальными справочниками:

- **Общий поиск на странице конкретного раздела.**

  Вы можете искать как по точному совпадению наименования, так и по его части. Поиск будет осуществляться по всем ячейкам.

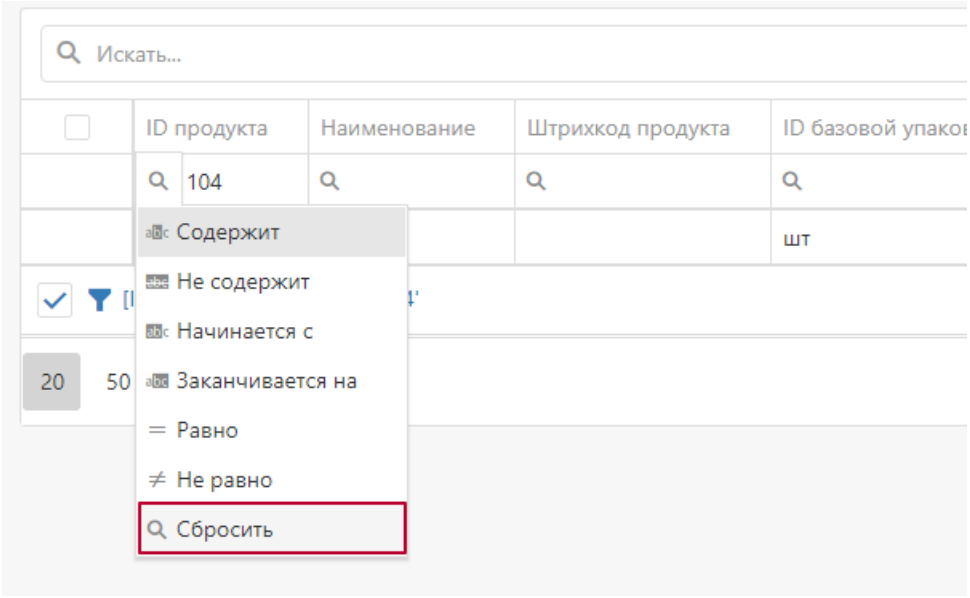


  Возможен поиск по номеру столбца таблицы, как по точному совпадению, так и по части.

Искать...

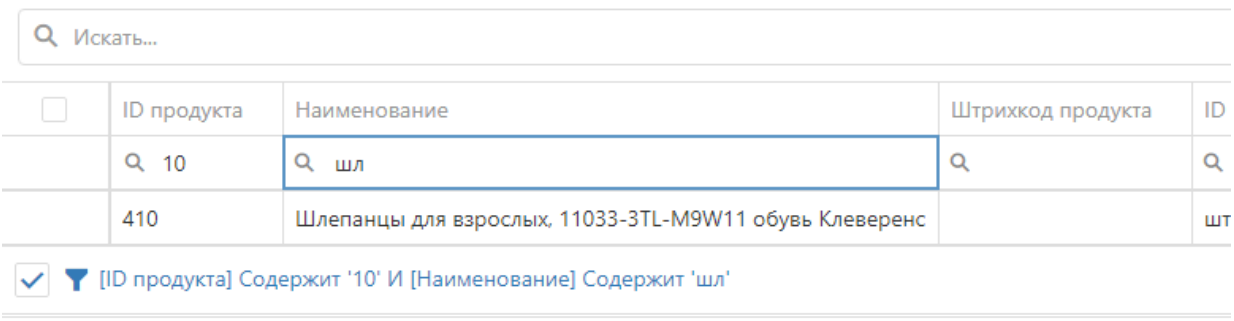
ID продукта	Наименование	Штрихкод продукта	ID базовой упаковки
10			
104	33333		шт
105	Сабо для взрослых, 10001-801-M7W9 обувь Клеверенс		шт
106	Сабо для взрослых, 10001-801-M8W10 обувь Клеверенс		шт
107	Сабо для взрослых, 10001-801-M9W11 обувь Клеверенс		шт
108	Сабо для взрослых, 10001-817-M10W12 обувь Клеверенс		шт
109	Сабо для взрослых, 10001-817-M11 обувь Клеверенс		шт
110	Сабо для взрослых, 10001-817-M12 обувь Клеверенс		шт
210	Сабо для взрослых, 10126-410-258 обувь Клеверенс		шт
310	Сабо для взрослых, 11016-50Q-M7W9 обувь Клеверенс		шт
410	Шлепанцы для взрослых, 11033-3TL-M9W11 обувь Клеверенс		шт

Сбросить фильтр поиска вы можете в самой ячейке, нажав на кнопку поиска с помощью кнопки «Сбросить».



Также в нижнем правом углу таблицы находится кнопка «Очистить», если задано значение поиска в ячейке.

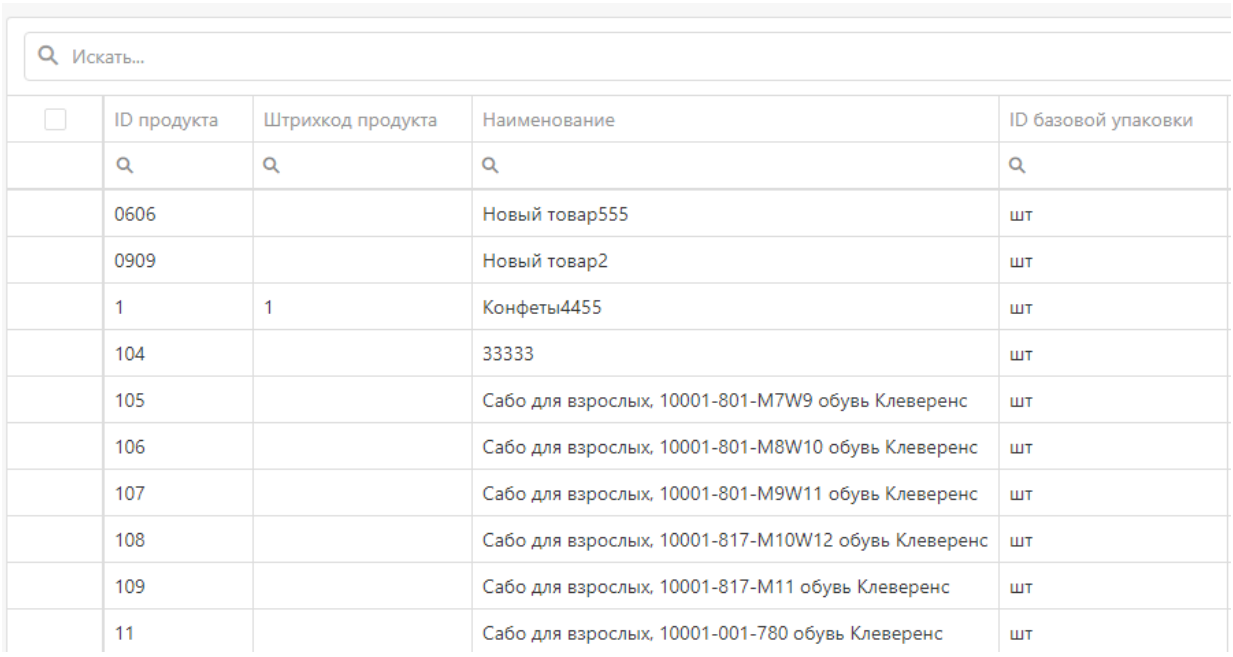
Вы можете искать одновременно по нескольким столбцам таблицы, это позволит более тонко настроить работу с данными (сортировка и поиск).



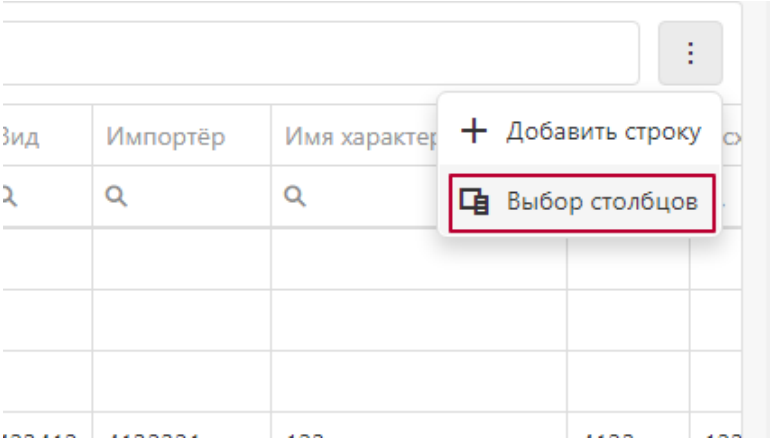
- **Сортировка и отображение столбцов.**

  Во всех таблицах веб-приложения есть возможность настроить последовательность столбцов под себя. Необходимо в шапке таблицы нажать на наименование столбца и, не отпуская, перетащить его на ту

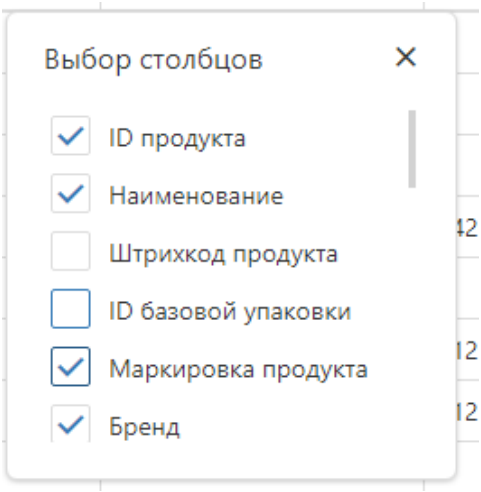
позицию в списке столбцов, которая вам будет удобна для просмотра конкретной таблицы. Данные изменения будут сохранены до очистки кеша браузера.



В настройках таблиц есть функция скрыть/отобразить необходимые столбцы/поля. По умолчанию все поля доступны для просмотре пользователя. Данный функционал находится в верхнем правом углу таблицы.

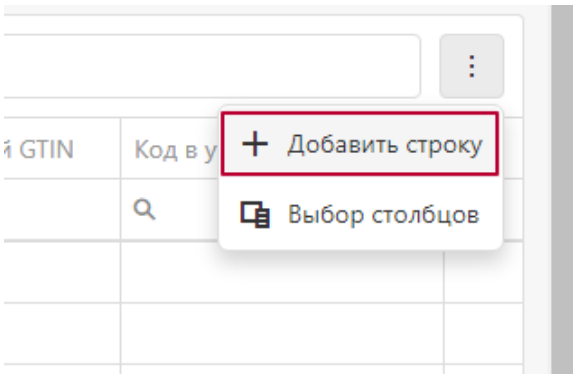


После нажатия кнопки «Выбор столбцов» появится список полей, которые вы можете скрыть или отобразить, если они были ранее скрыты.

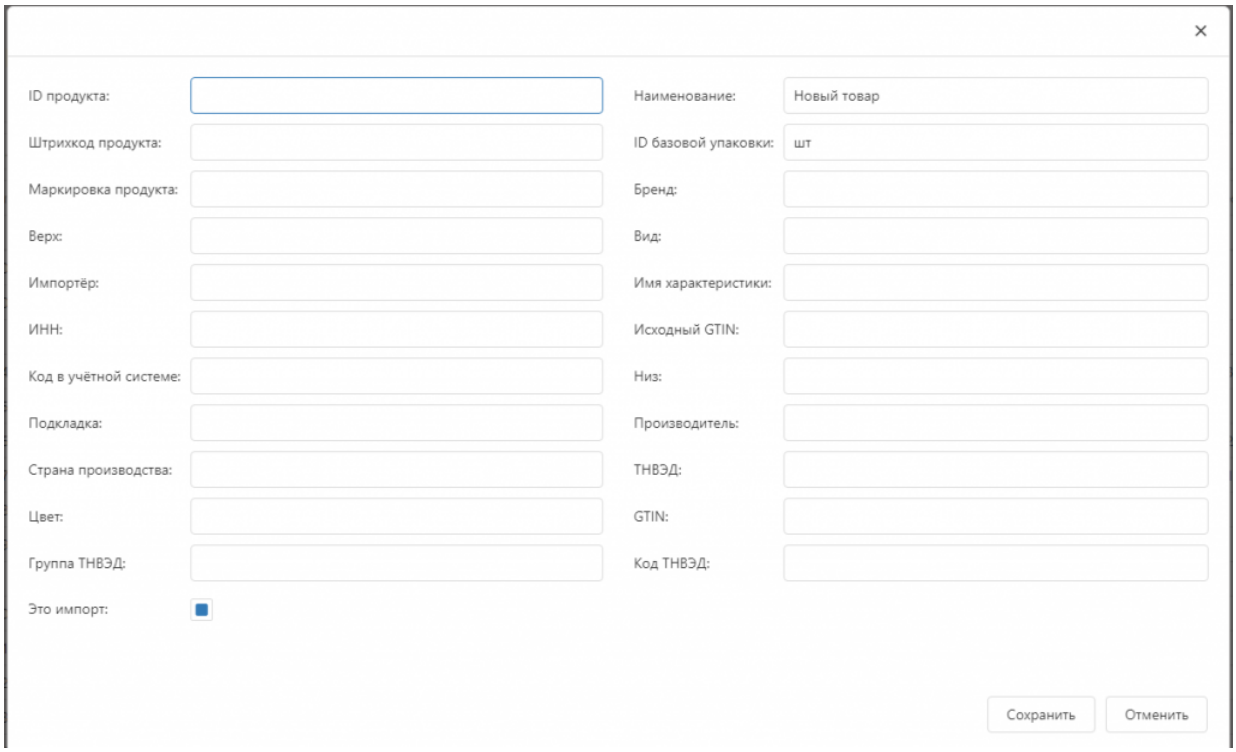


- **Добавление строки.**

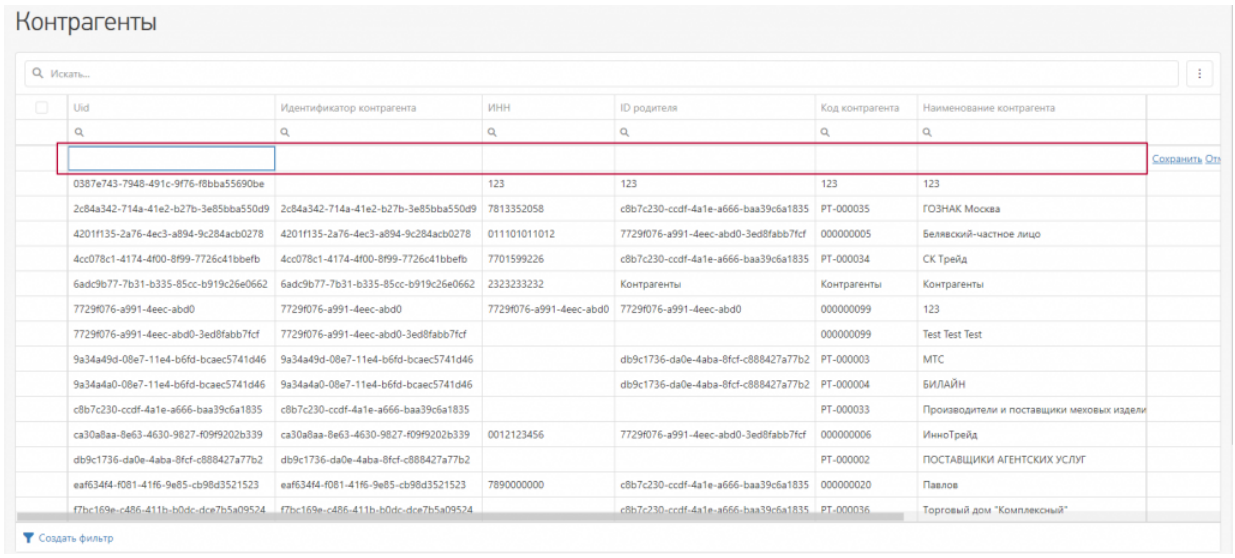
В каждой таблице (кроме «Оборудования»), есть возможность добавить новую строку.



«Документы» и «Номенклатура» заполняются в отдельном всплывающем окне.



Все остальные справочники заполняются в таблице.

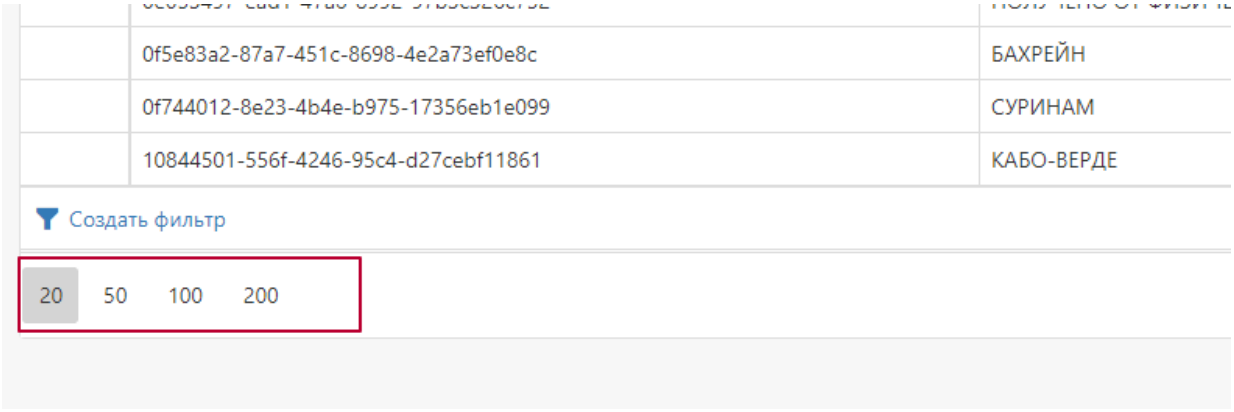


После заполнения всех необходимых полей информацией необходимо сохранить результаты, после чего данные будут отправлены на сервер Mobile SMARTS.

> Данной функционал необходимо использовать, если вы действительно понимаете, для чего вам понадобилась новая запись в справочнике, в документах или номенклатуре, так как с некорректно введенными данными вы не сможете работать.

- **Пагинация.**

Также реализована возможность переключить количество отображаемых строк в таблице в нижнем левом углу таблиц.



В правом нижнем углу таблиц реализована пагинация и переход на следующую страницу списка при большом количестве строк в таблице.

Не нашли что искали?

Задать вопрос в техническую поддержку

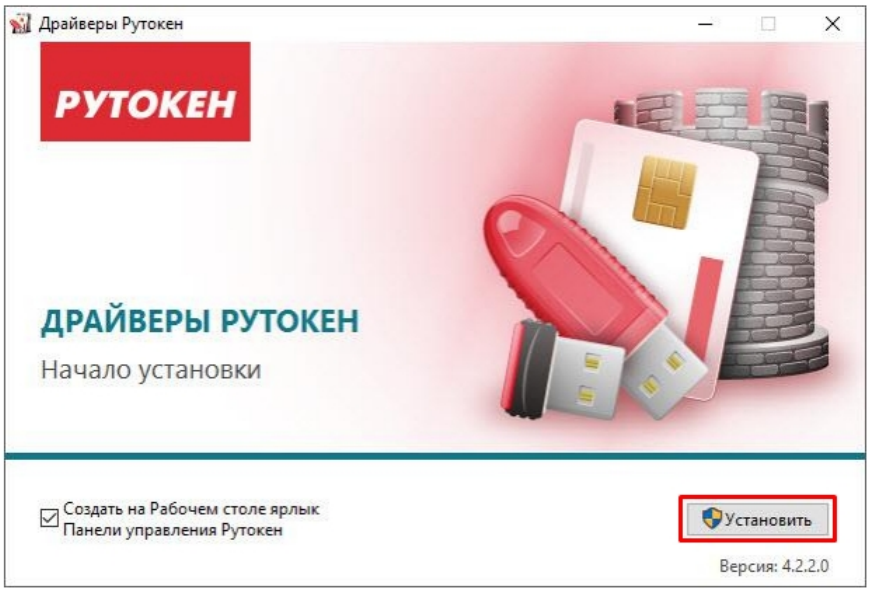
Установка необходимых драйверов и утилит для работы с носителями ЭП

Последние изменения: 2024-03-26

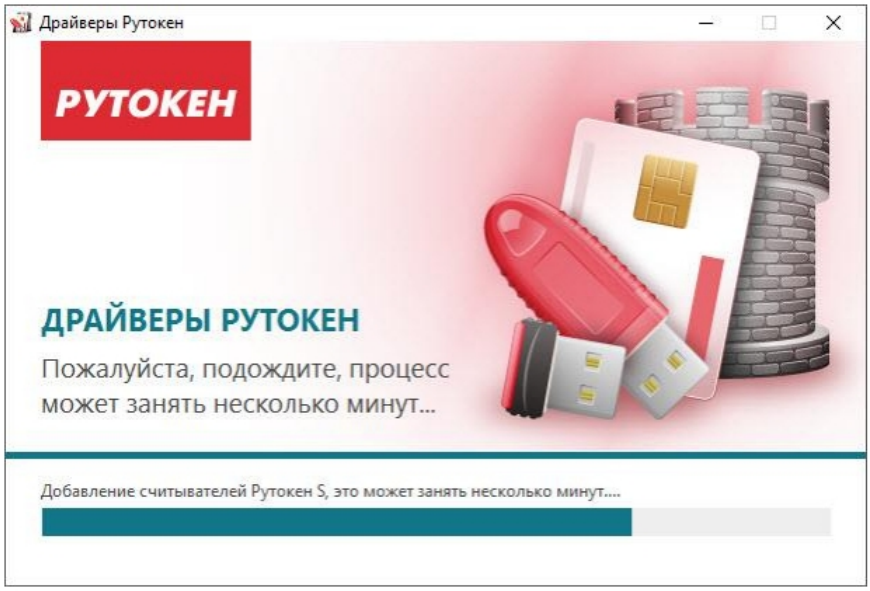
Драйверы Рутокен для Windows

- Скачайте актуальную версию комплекта «Драйверы Рутокен для Windows».

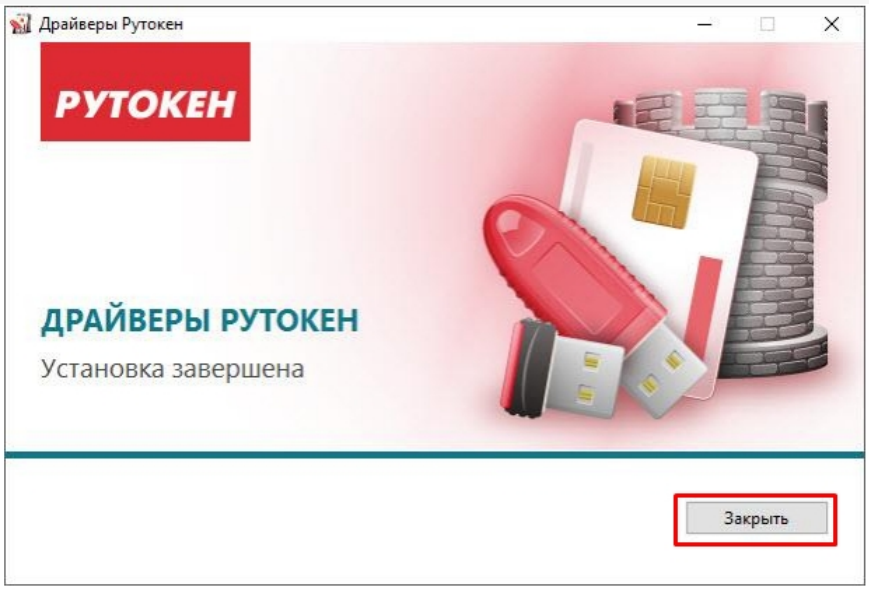
- Запустите программу установки комплекта драйверов для Windows и нажмите на кнопку «Установить».



- В окне с запросом на разрешение изменений на компьютере нажмите на кнопку «Да». В результате запустится процесс установки комплекта драйверов.



- После завершения процесса установки нажмите на кнопку «Закрыть».



- Подключите устройство Рутокен к компьютеру.

Рутокен Плагин в Windows

В Windows Рутокен Плагин работает в следующих браузерах:

- Google Chrome.
- Mozilla Firefox.
- Яндекс Браузере.
- Internet Explorer.
- Opera.

Скачать актуальную версию плагина можно здесь.

Не нашли что искали?

Задать вопрос в техническую поддержку

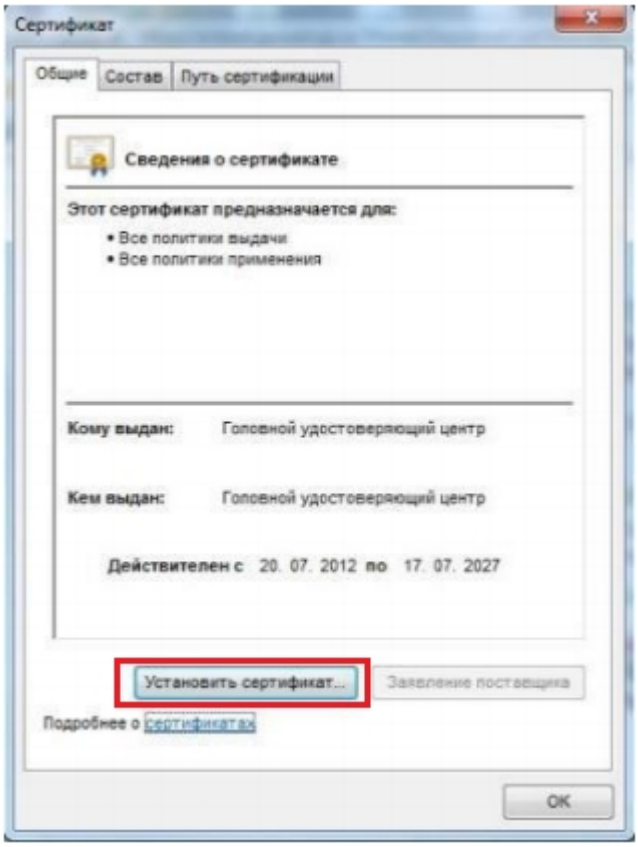
Установка корневых сертификатов в хранилища

Последние изменения: 2024-03-26

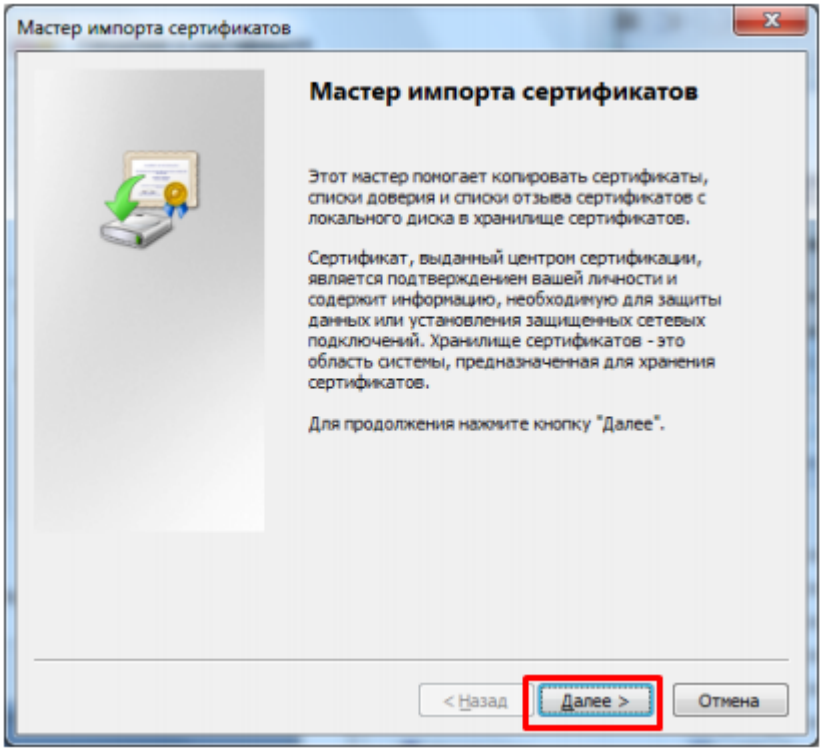
Корневой сертификат Головного Удостоверяющего Центра

Для установки сертификата вам потребуется перейти по ссылке и открыть скачанный сертификат.

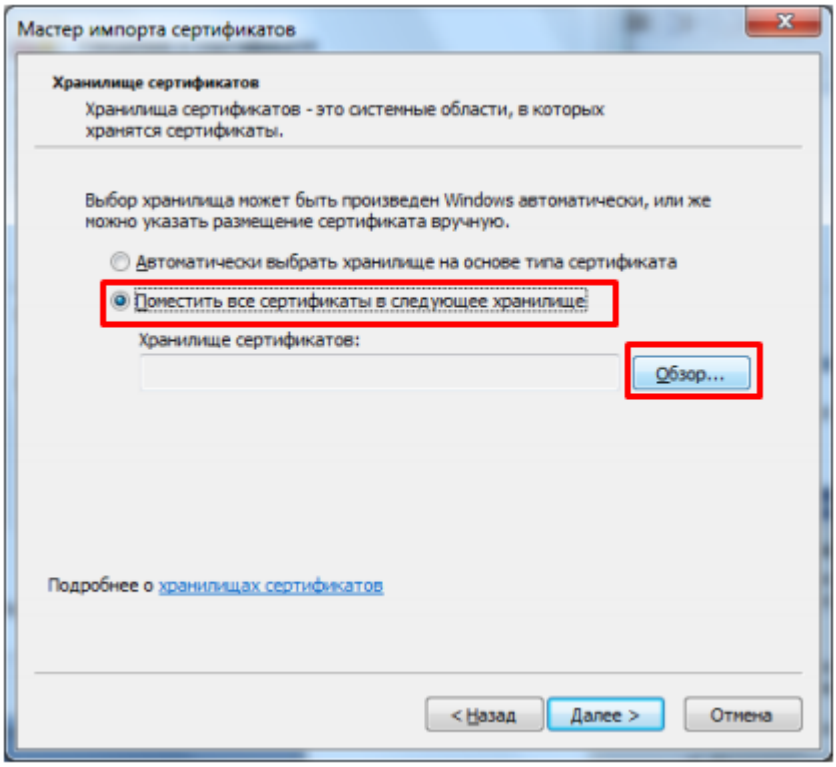
- Нажмите «Установить сертификат».



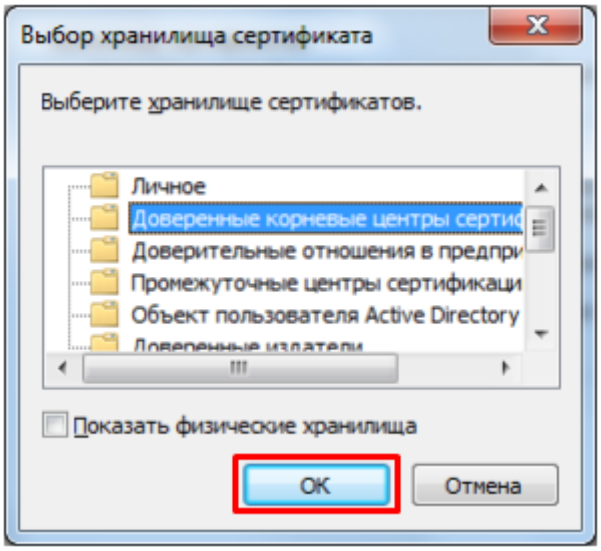
- В открывшемся окне мастера импорта сертификатов нажмите «Далее».



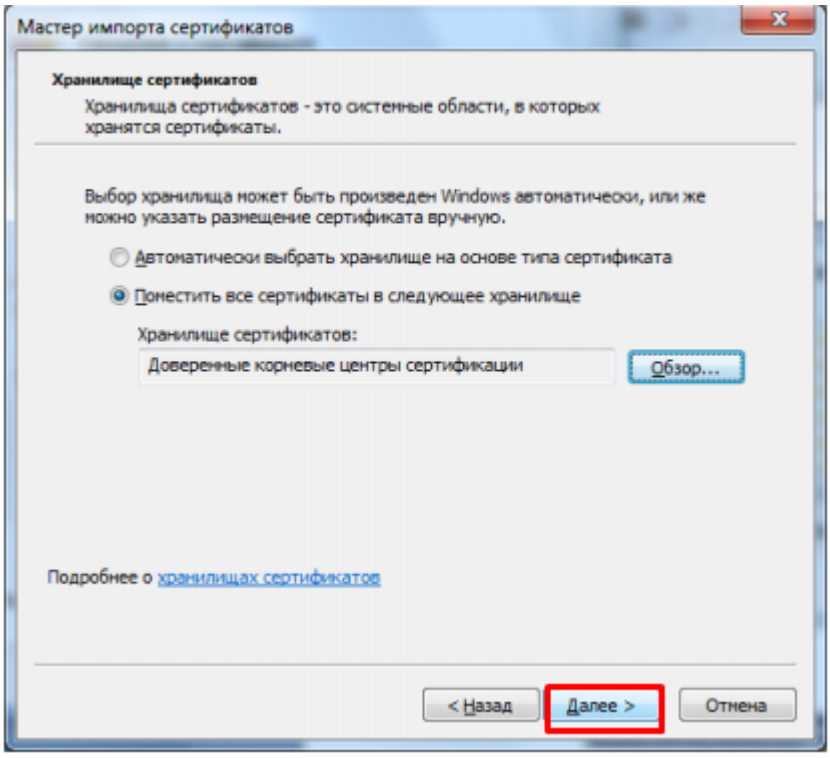
- **Выберите «Поместить все сертификаты в следующее хранилище», после чего нажмите «Обзор...».**



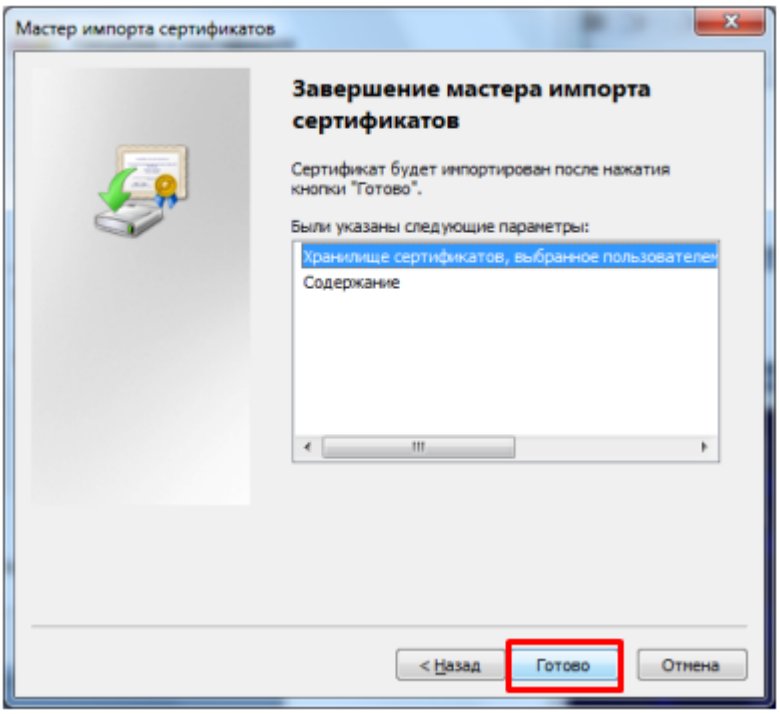
- **Укажите «Доверенные корневые центры сертификации», нажмите «ОК».**



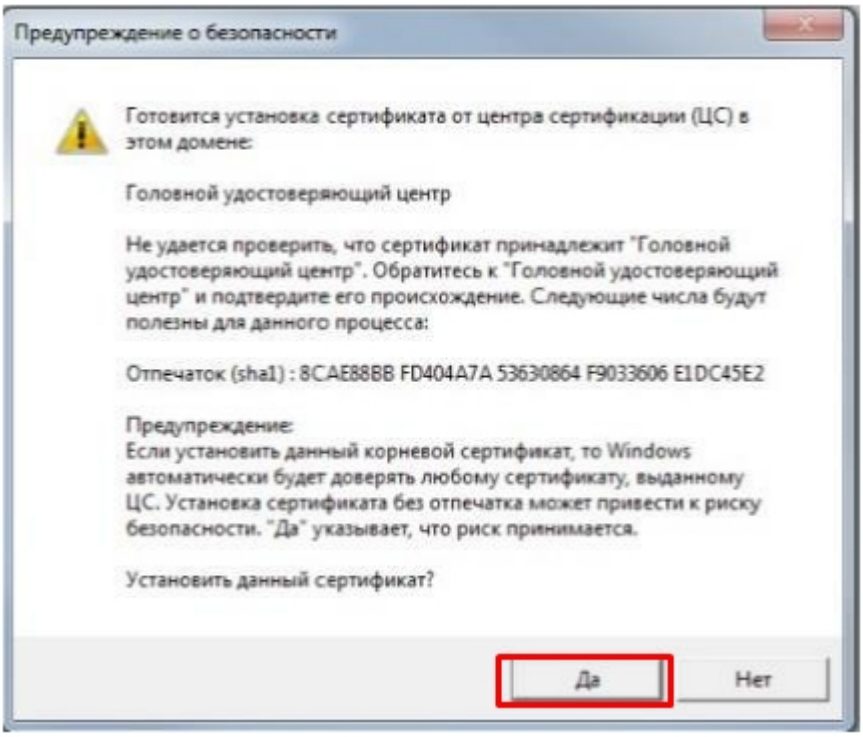
- Нажмите «Далее».

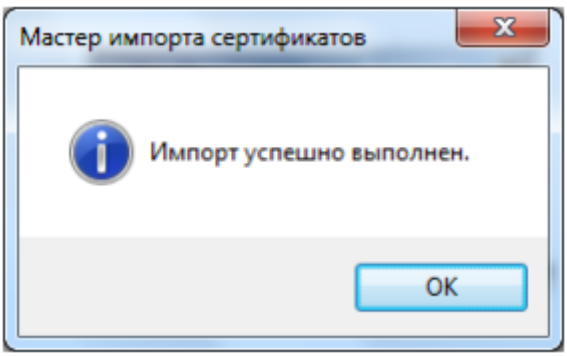


- Для завершения работы мастера импорта сертификатов нажмите «Готово».



- **Если вы переходите с тестового сертификата на рабочий или обратно, появится следующее предупреждение, где необходимо подтвердить установку сертификата, нажав кнопку «Да».**





Корневой сертификат Минкомсвязи России

Произведите установку корневого сертификата Минкомсвязи России аналогично установки корневого сертификата Головного Удостоверяющего Центра. Для установки сертификата вам потребуется перейти по ссылке и открыть скачанный сертификат.

Корневой сертификат Удостоверяющего Центра

Произведите установку корневого сертификата Удостоверяющего Центра, выдавшего вашу электронную подпись, аналогично установки корневого сертификата Головного Удостоверяющего Центра. За сертификатом следует обратиться на сайт УЦ.

Не нашли что искали?

Задать вопрос в техническую поддержку

Установка криптопровайдера КриптоПро CSP

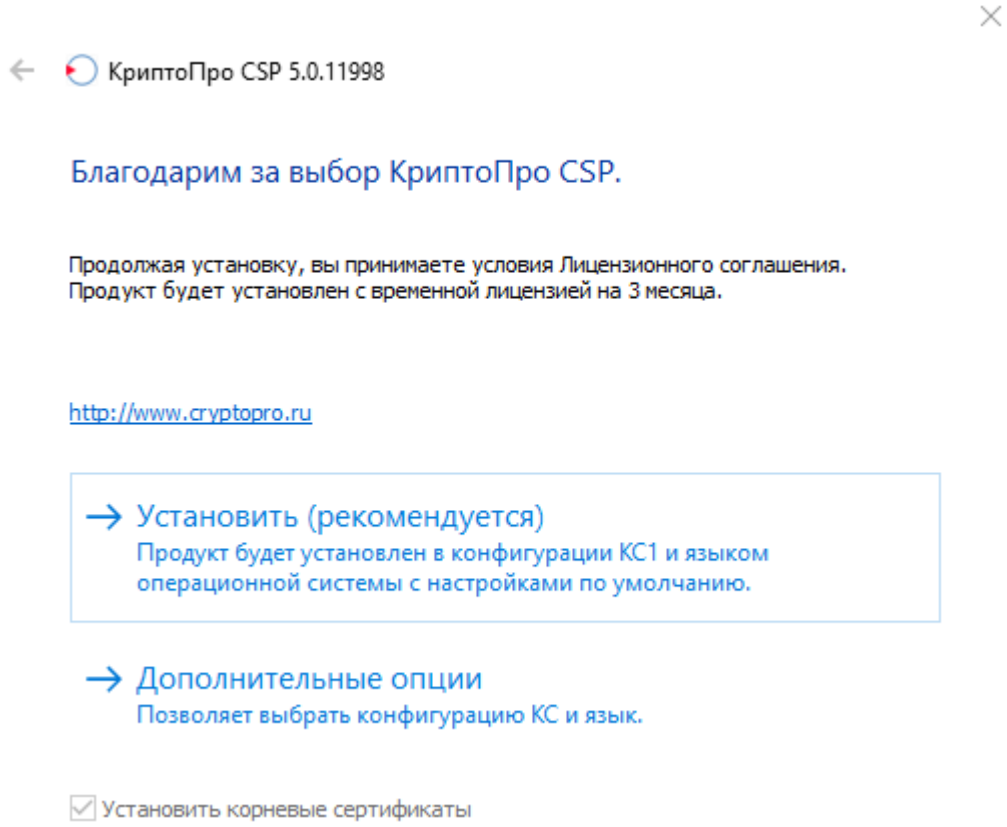
Последние изменения: 2024-03-26

Установка КриптоПро CSP

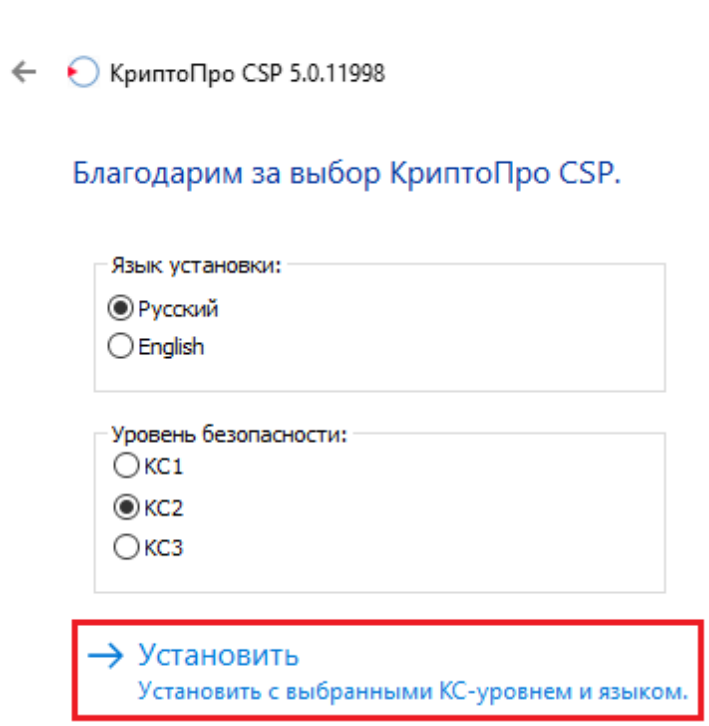
Пройдите процедуру регистрации и загрузите дистрибутив КриптоПро CSP с официального сайта разработчика.

> **Установка дистрибутива СКЗИ КриптоПро CSP должна производиться пользователем, имеющим права администратора.**

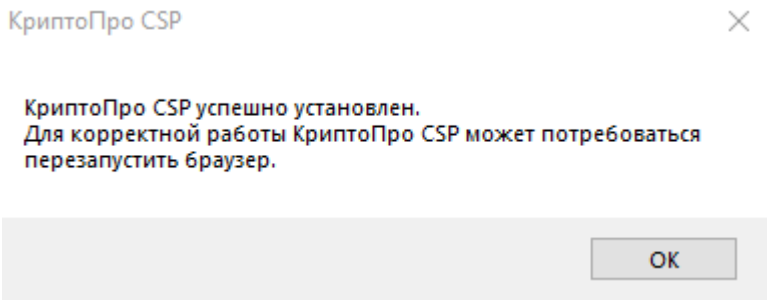
При установке КриптоПро CSP следуйте инструкциям мастера установки:



Рекомендуется устанавливать КриптоПро CSP с автоматическими настройками, но вы можете установить язык и конфигурацию уровня безопасности самостоятельно (с помощью кнопки «Дополнительные опции»).



После завершения установки перезагрузите браузер.



Установка контейнера закрытого ключа

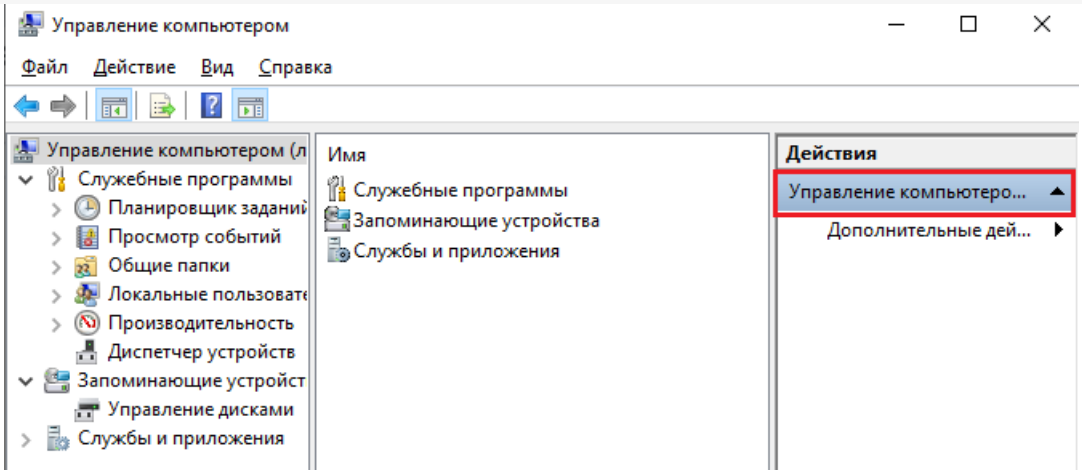
Контейнер закрытого ключа может быть установлен на одном из носителей:

- реестр (для установки в реестр);
- директория;
- съемный диск для хранения ключей (usb-ключ, nfc-карта, виртуальный жесткий диск).

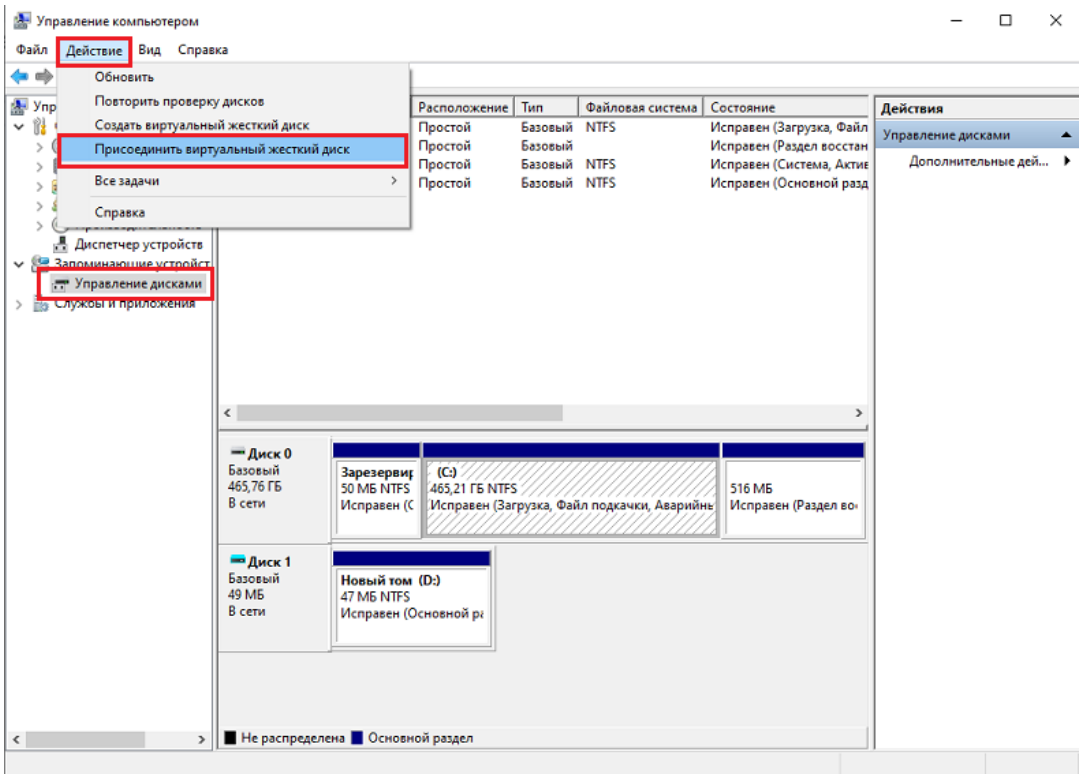
При установке контейнера в реестр или директорию нужно удостовериться, что предоставлены необходимые права на ветку реестра или на папку, в которую устанавливается контейнер.

При установке контейнера на виртуальный жесткий диск, необходимо подключить его следующим путем:

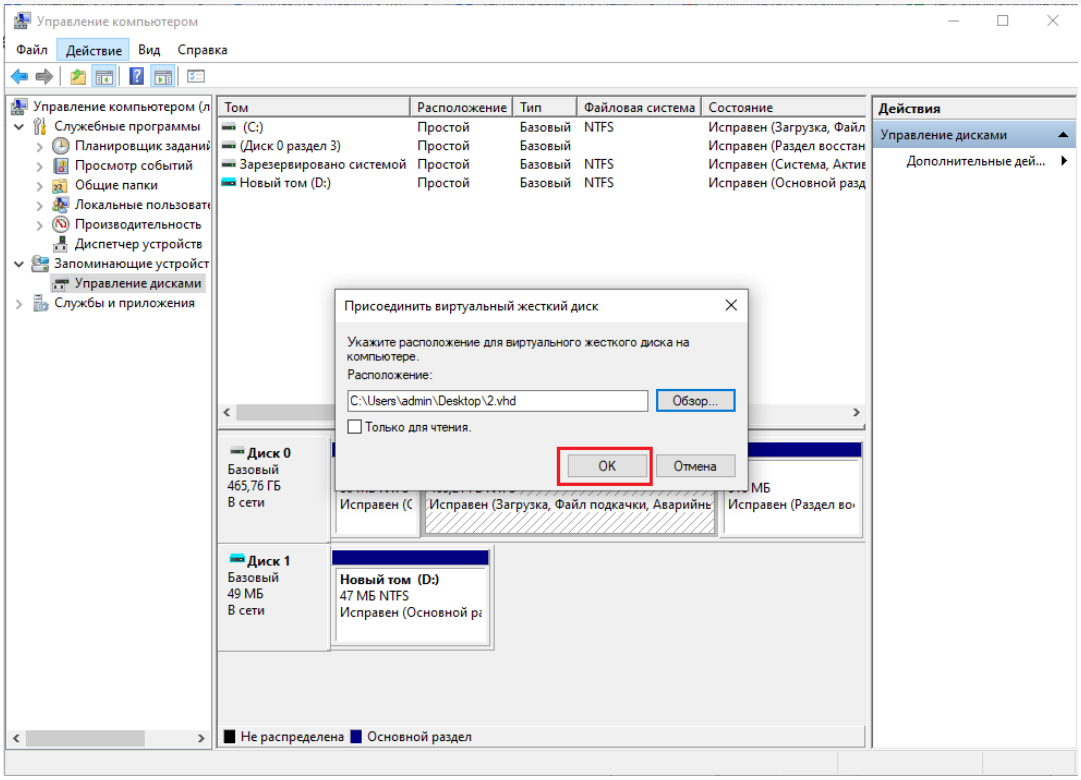
- ПУСК → «Средства администрирования» → «Управление компьютером».



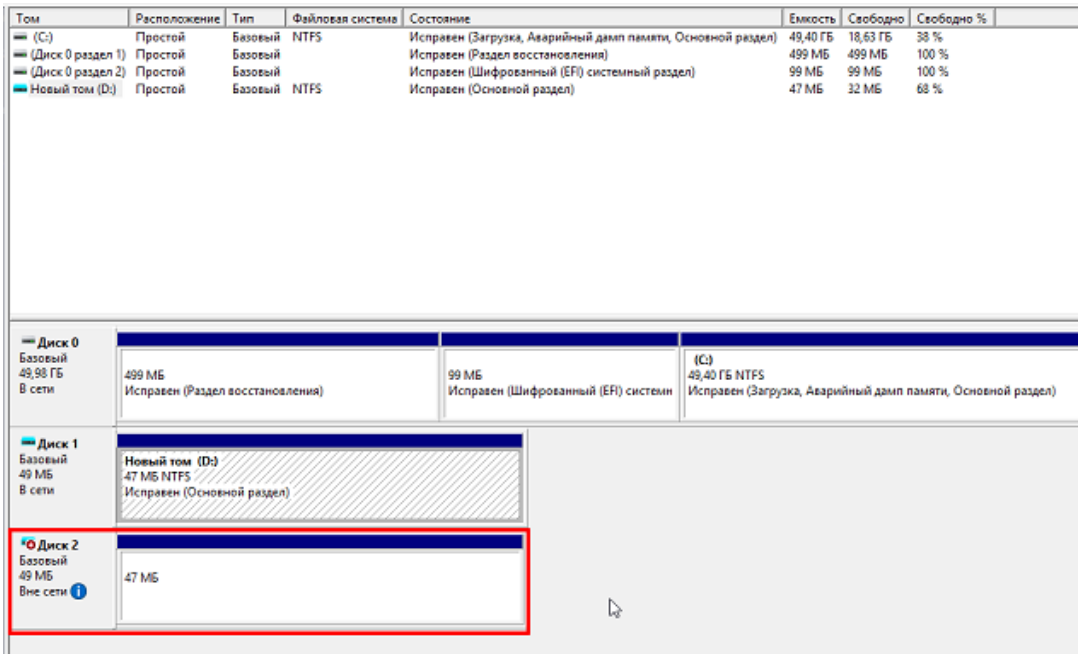
- **Открыть вкладку «Управление дисками», нажать «Действие» → «Присоединить виртуальный жесткий диск».**



- **Выбрать загруженный ранее контейнер, нажать «ОК».**

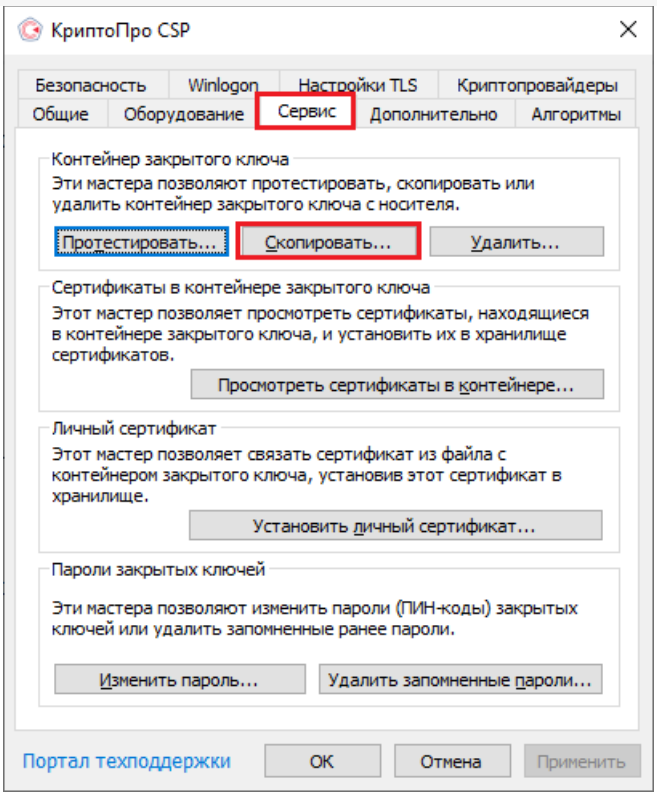


- После этого новый диск будет добавлен.

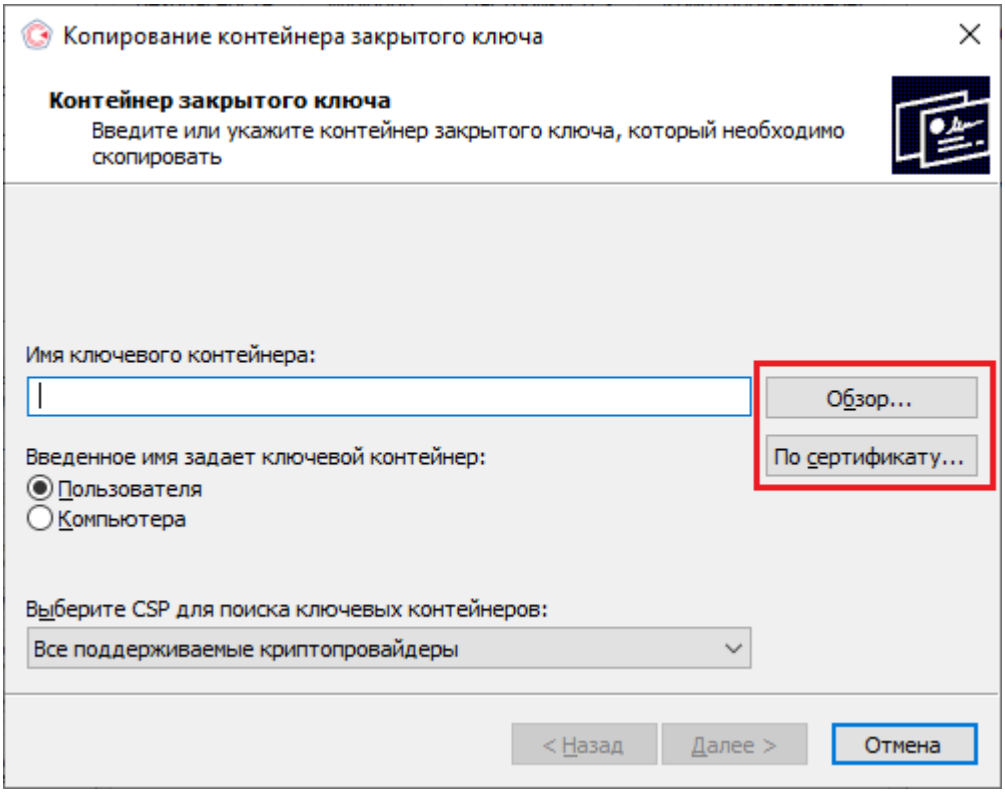


Если хранить контейнер на виртуальном жестком диске, то после перезагрузки ПК этот жесткий диск потребуется подключать заново. Поэтому рекомендуем скопировать контейнер на любой из доступных носителей с помощью программы КриптоПро CSP. Для этого:

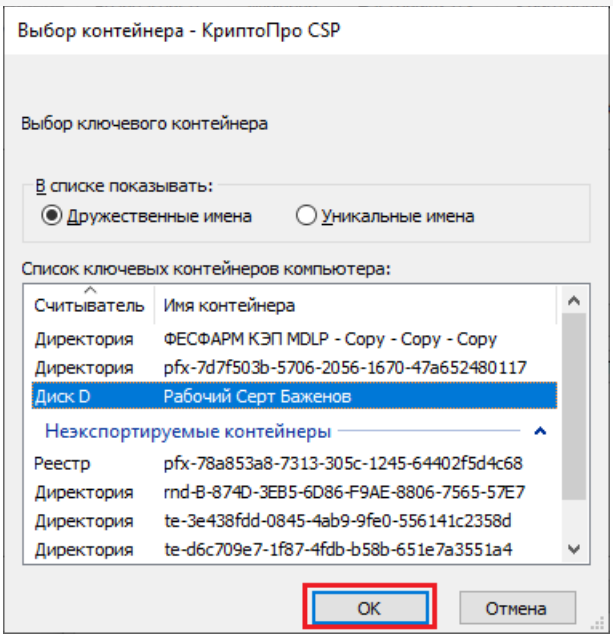
Запустите КриптоПро CSP от имени администратора, откройте вкладку «Сервис» и нажмите на кнопку «Скопировать».



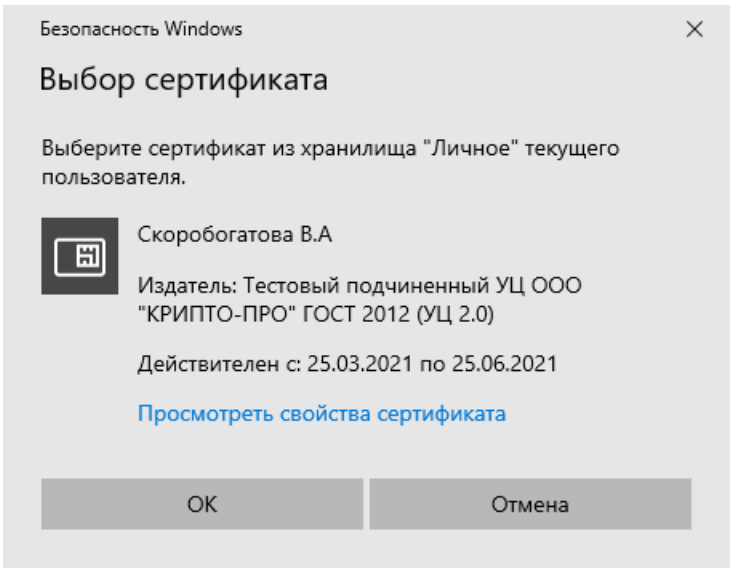
В открывшемся окне необходимо выбрать, где будет располагаться ключевой контейнер (пользователь или компьютер) с помощью кнопки «Обзор» или «По сертификату».



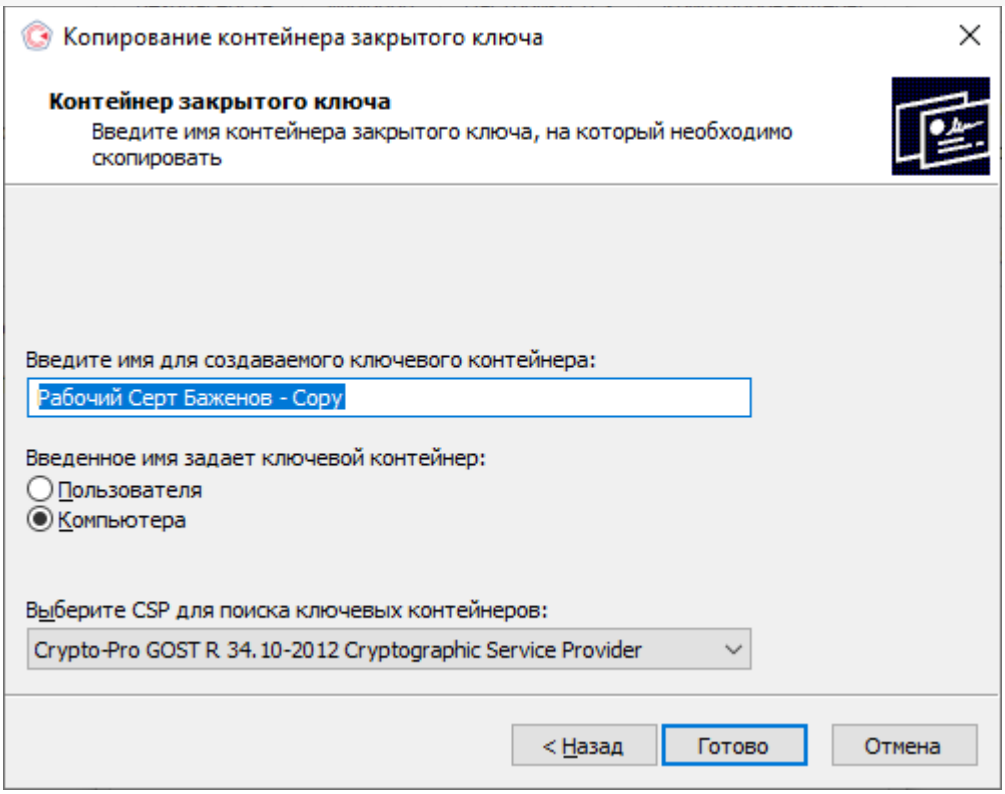
При нажатии на кнопку «Обзор», потребуется выбрать контейнер из списка:



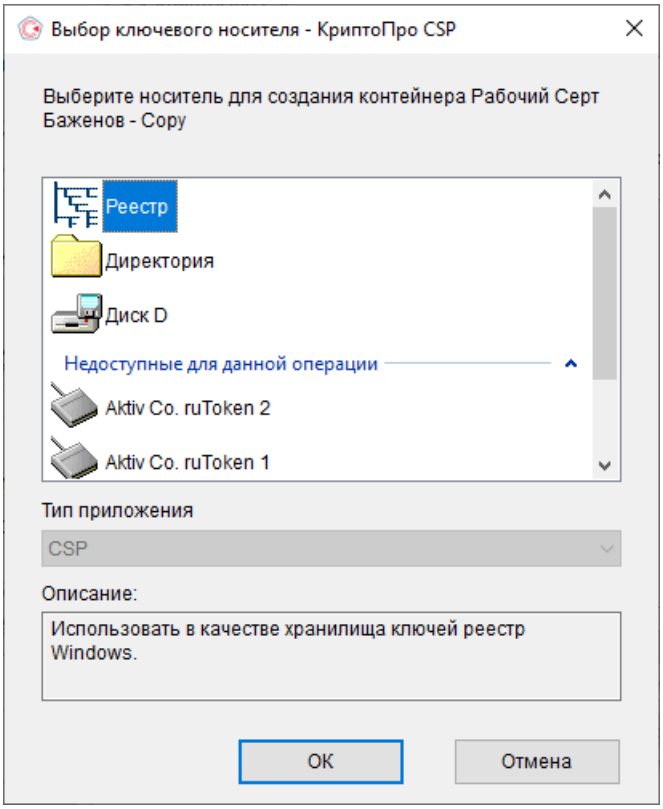
При нажатии на кнопку «По сертификату» потребуется выбрать нужный сертификат.



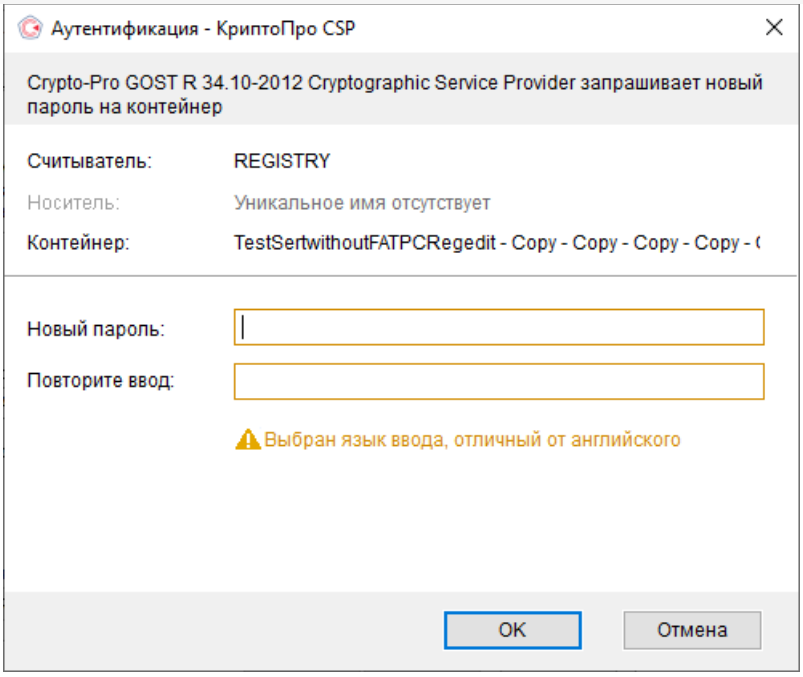
После того как выбран нужный контейнер, выберите имя и доступ сертификата.Нажмите кнопку «Готово».



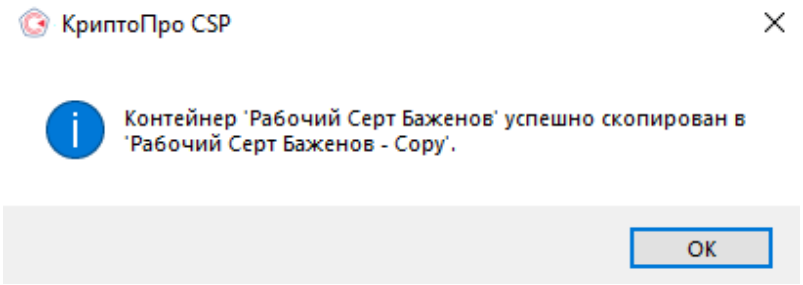
После этого откроется окно выбора ключевого носителя, на который будет копироваться контейнер. укажите нужный и нажмите «ОК».



После выбора ключевого носителя создайте пароль на контейнер. Нажмите «ОК».



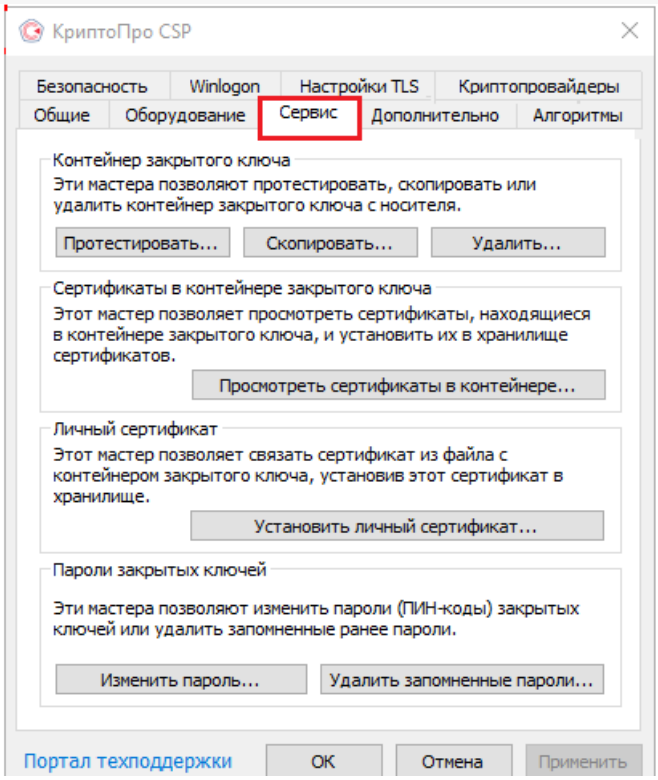
При успешном завершении операции появится следующее уведомление.



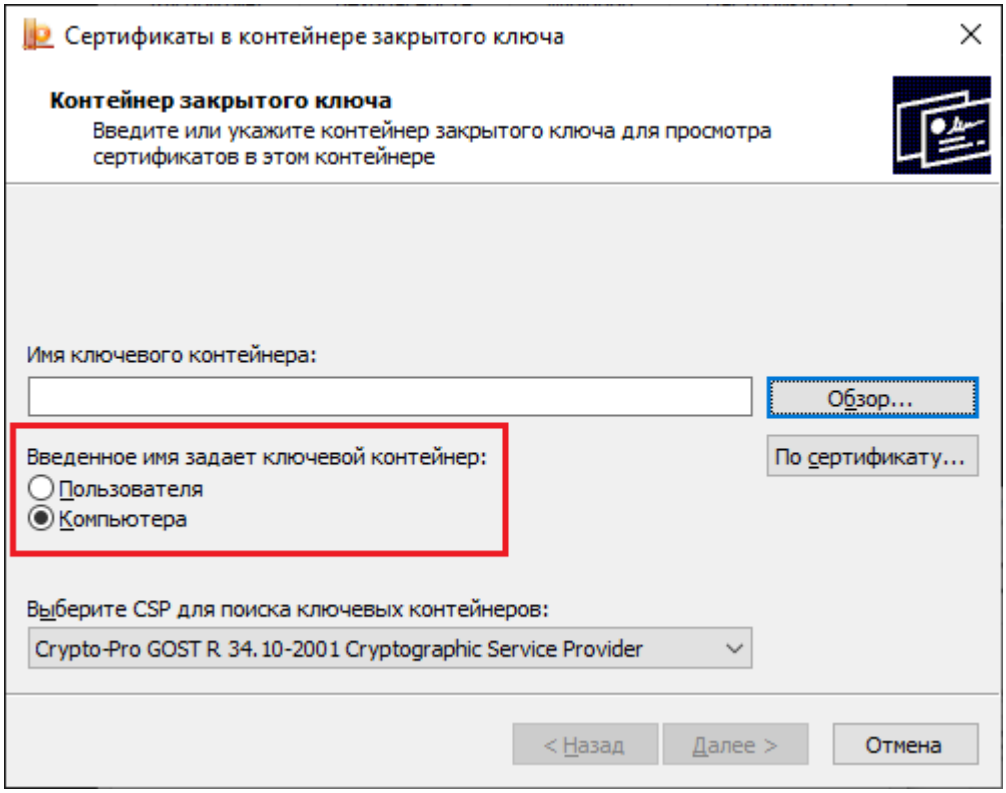
Установка сертификата в Личные

> **Для корректной работы «Кировки» с ГИС МТ, необходимо установить сертификат КЭП в хранилище компьютера (Local Machine).**

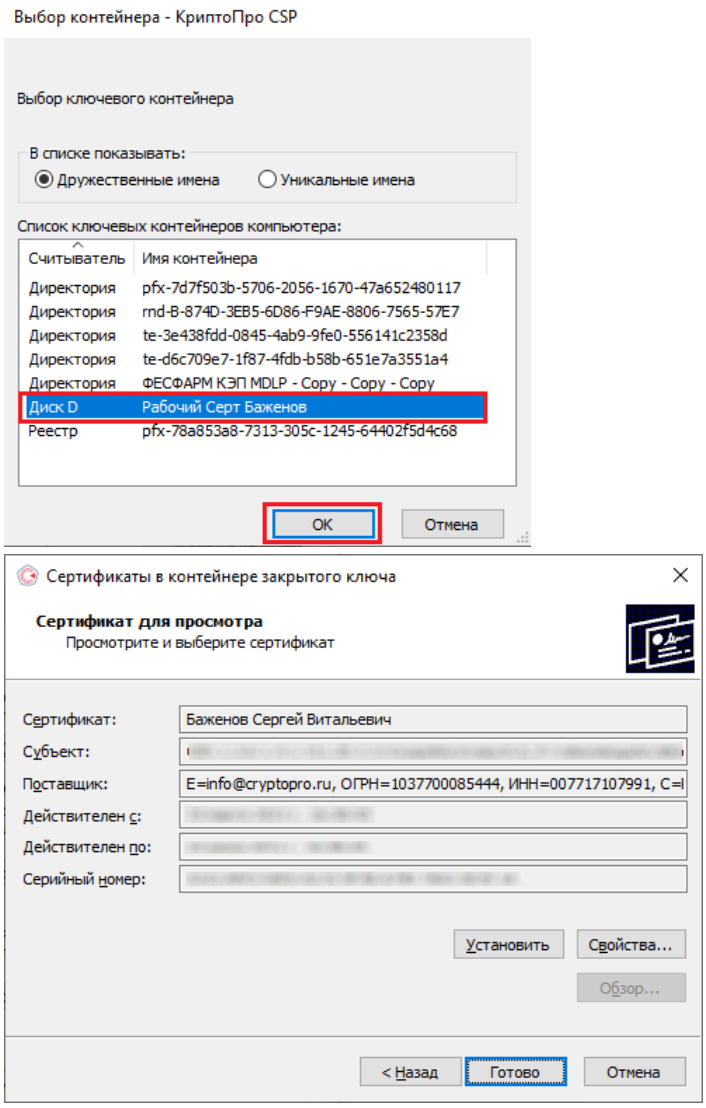
- **Для того чтобы просмотреть сертификат, хранящийся в контейнере закрытого ключа, запустите КриптоПро CSP от имени администатора. Откроется «Панель управления» СКЗИ КриптоПро CSP, где необходимо перейти на вкладку «Сервис».**



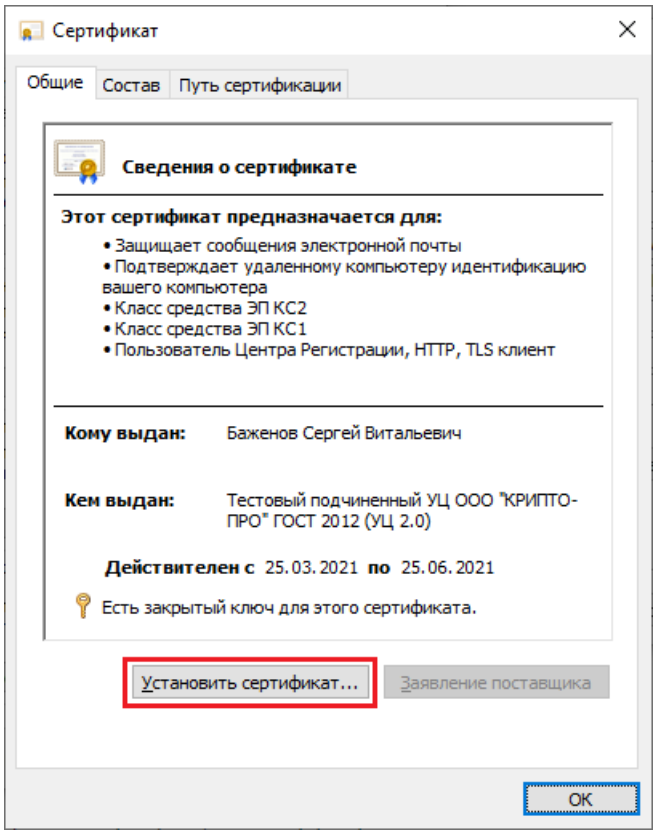
- **Нажмите кнопку «Просмотреть сертификаты в контейнере». Откроется окно «Сертификаты в контейнере закрытого ключа». На этой форме в пункте «Введенное имя задает ключевой контейнер» необходимо установить флаг в пункте «Компьютера» (возможно только в случае если вы открыли КриптоПро CSP от имени администратора).**



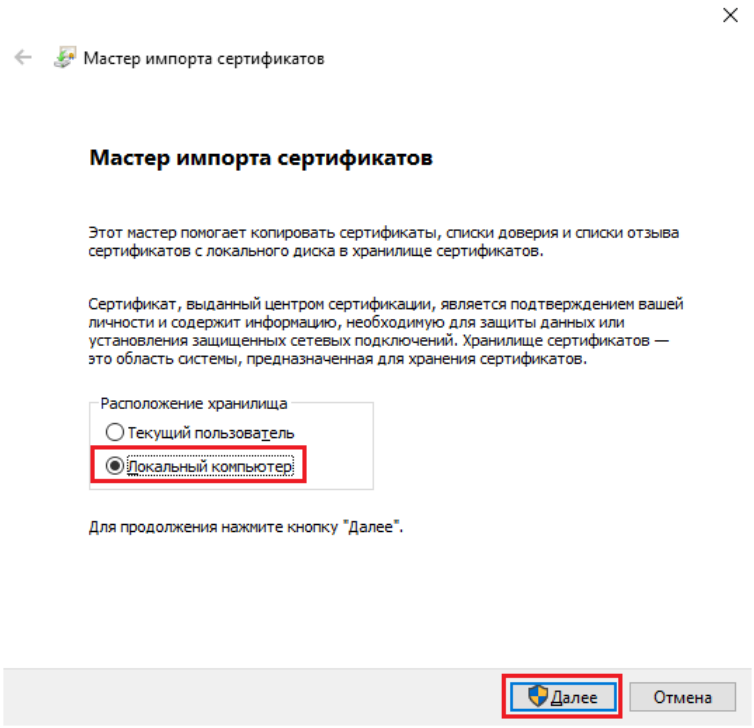
- **Далее необходимо заполнить поле «Имя ключевого контейнера». Оно может быть введено вручную или найдено в списках контейнеров (кнопка «Обзор») или сертификатов (кнопка «По сертификату»). Если сертификат в выбранном контейнере имеется, откроется окно «Сертификат для просмотра».**



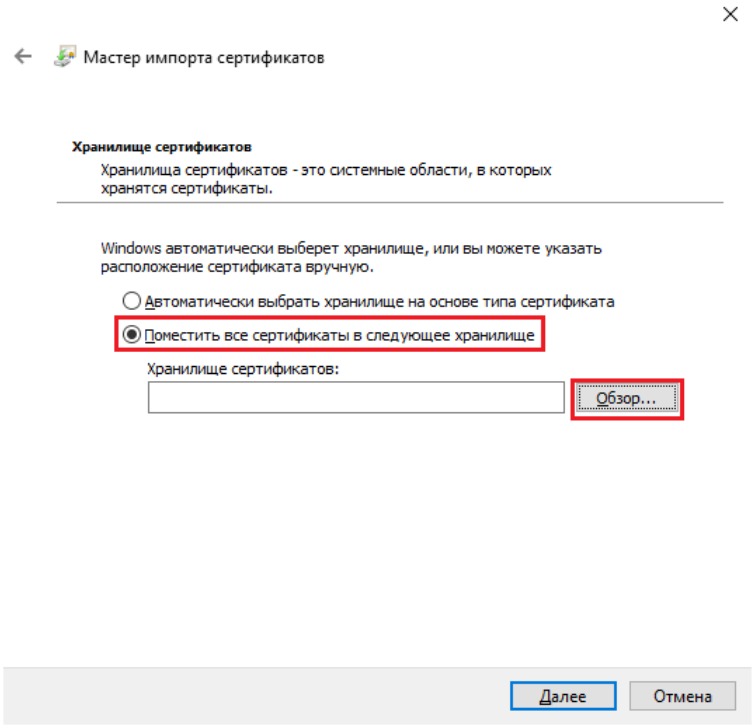
- **В окне «Сертификаты в контейнере закрытого ключа» нажмите кнопку «Установить» (для связи сертификата и закрытого ключа). После этого установите сертификат в личное хранилище («Свойства» → «Установить сертификат»).**

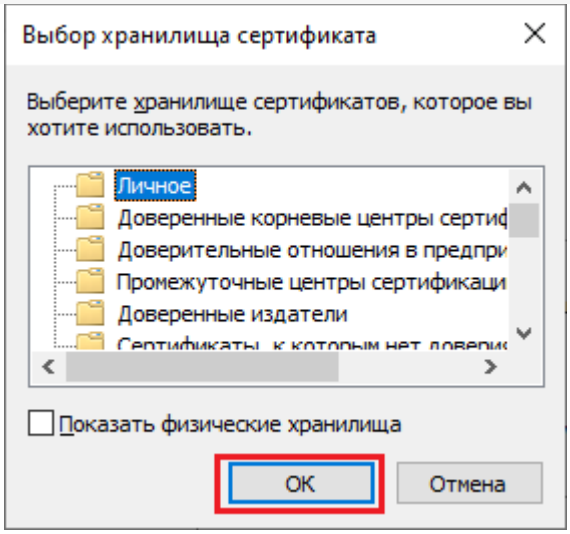


- **В качестве расположения хранилища выберите «Локальный компьютер» и нажмите кнопку «Далее».**



- **В следующем окне выберите пункт «Поместить все сертификаты в следующее хранилище», нажмите кнопку «Обзор» и из списка хранилищ выберите «Личное».**



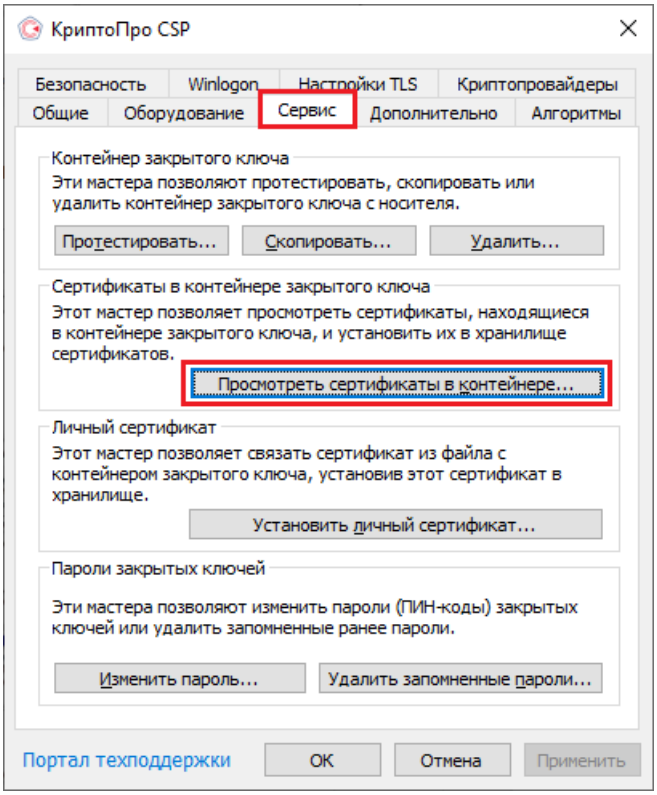


- Нажмите «ОК» → «Далее» → «Готово».

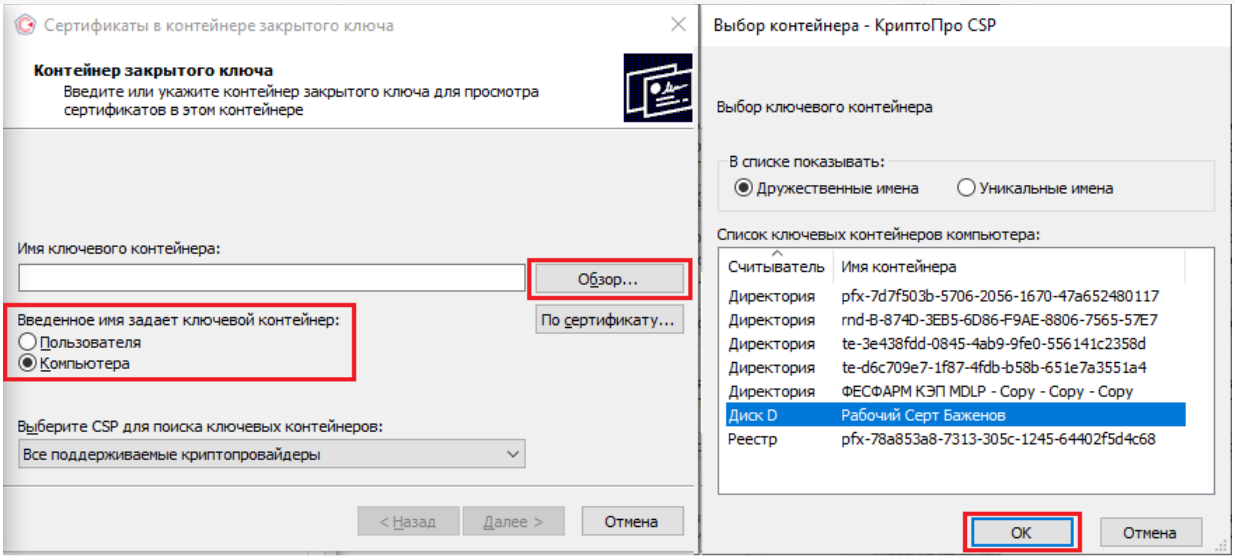
Проверка и сопоставление текущего личного сертификата и сертификата в контейнере

Данное действие можно выполнить двумя способами.

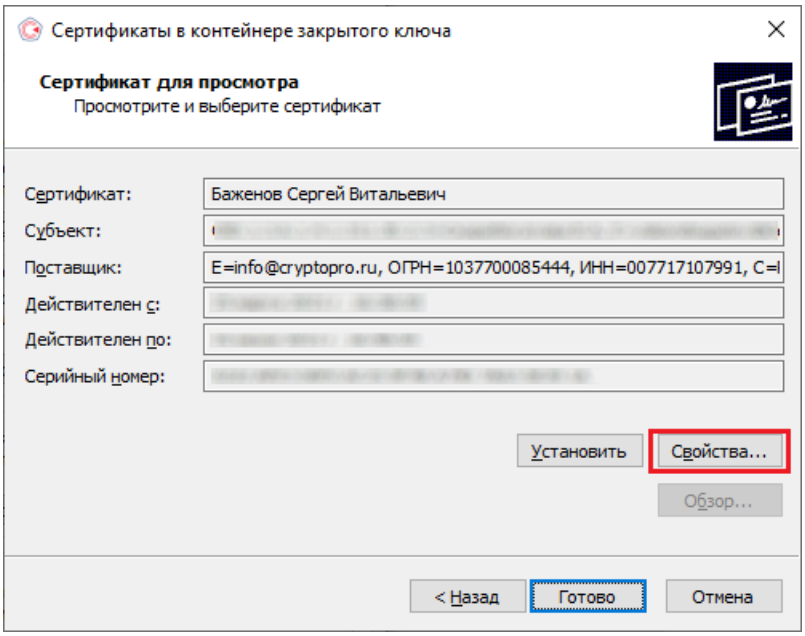
Способ 1. Сравнить отпечатки сертификата в контейнере и сертификата, установленного на ПК. Для проверки сертификата в контейнере нужно запустить КриптоПРО CSP от имени администратора, перейти во вкладку «Сервис» и нажать на кнопку «Просмотреть сертификаты в контейнере».



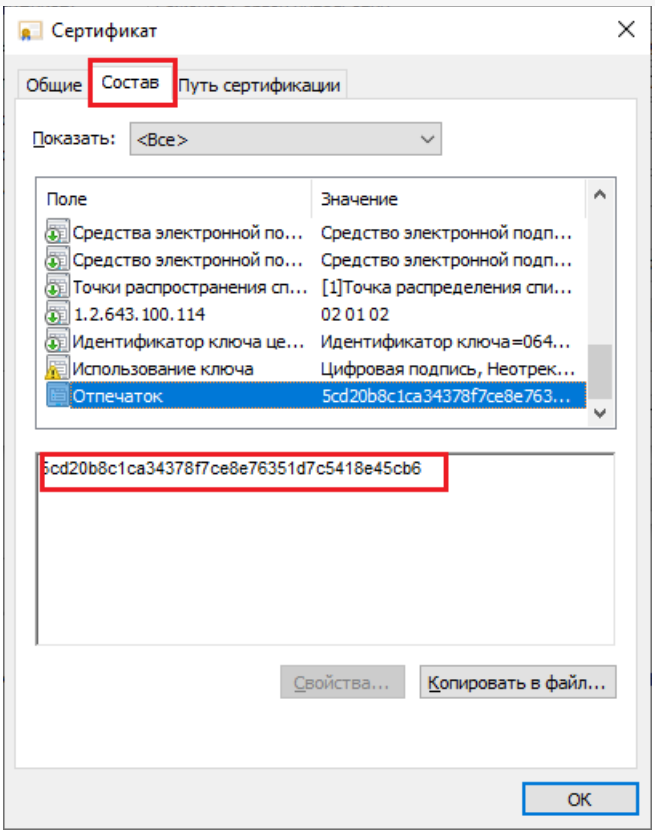
В открывшемся окне нужно выбрать «Введенное имя задает ключевой контейнер» — «Компьютер», далее нажать на кнопку «Обзор», выбрать контейнер из списка и нажать «ОК».



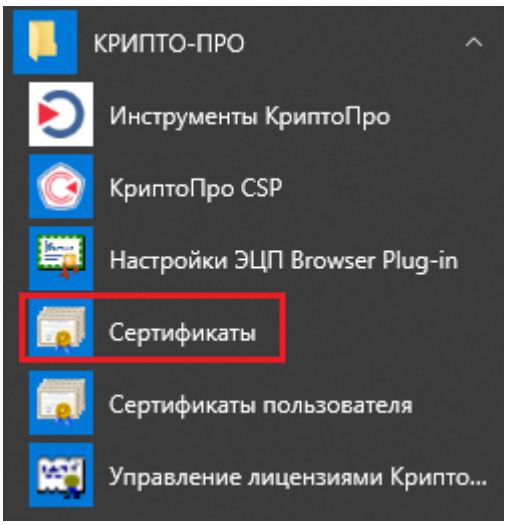
Откроется окно с информацией о сертификате, в котором необходимо нажать на кнопку «Свойства».



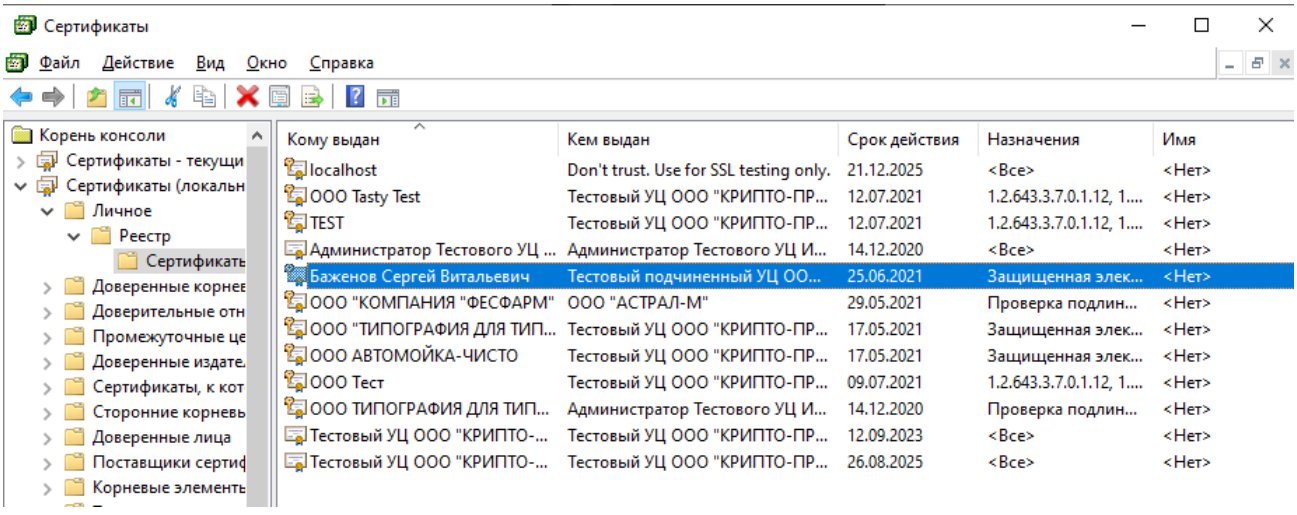
В открывшемся окне перейдите на вкладку «Состав». Вам нужна строка-отпечаток, которую вы можете сравнить наглядно со строкой-отпечатком, установленным на ПК.



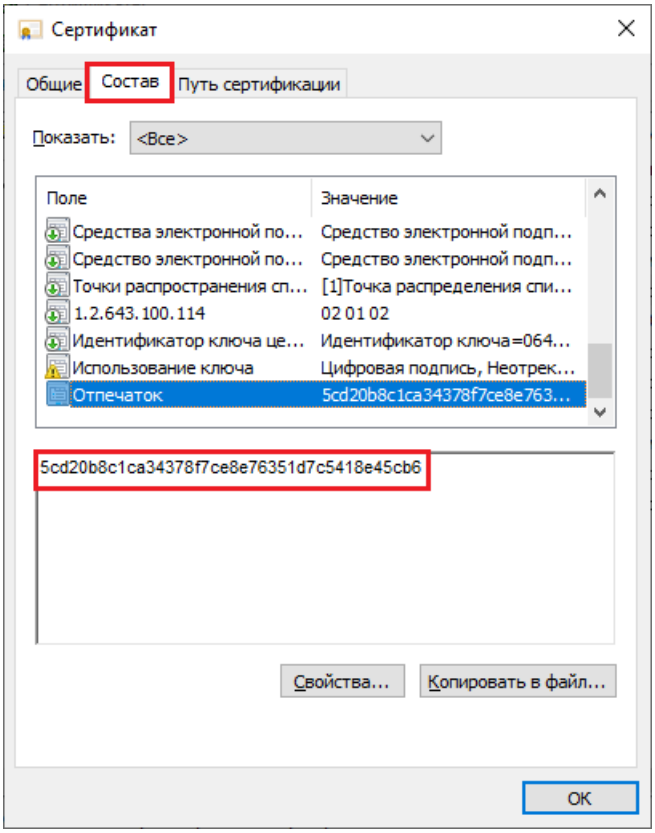
Для того чтобы сверить данный отпечаток с сертификатом, установленным на ПК, необходимо открыть ПУСК → КРИПТО-ПРО → Сертификаты.



В открывшемся окне сертификатов выберите «Сертификаты (локальный компьютер)» → «Личное» → «Реестр» → «Сертификаты», и выберите нужный вам сертификат.

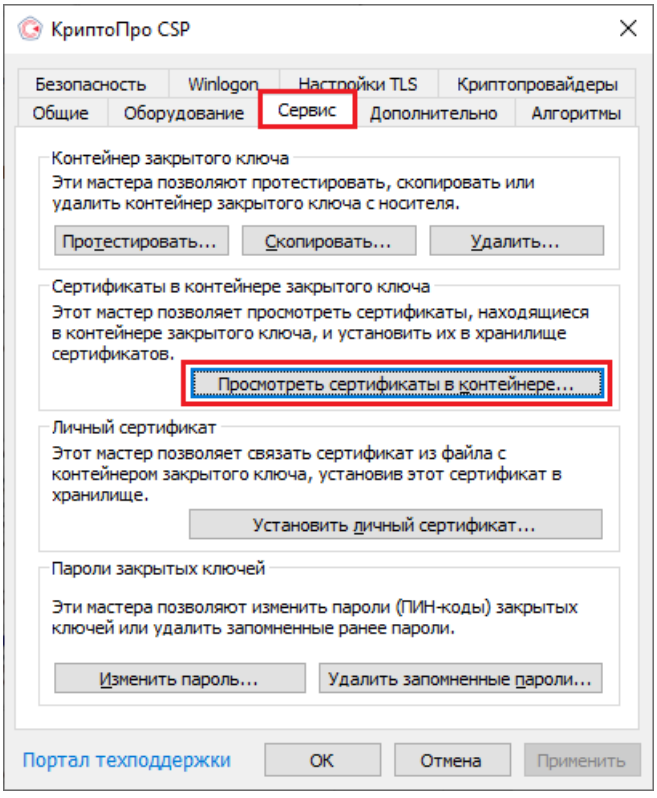


В окне сертификата перейдите на вкладку «Состав», где будет указана строка-отпечаток.

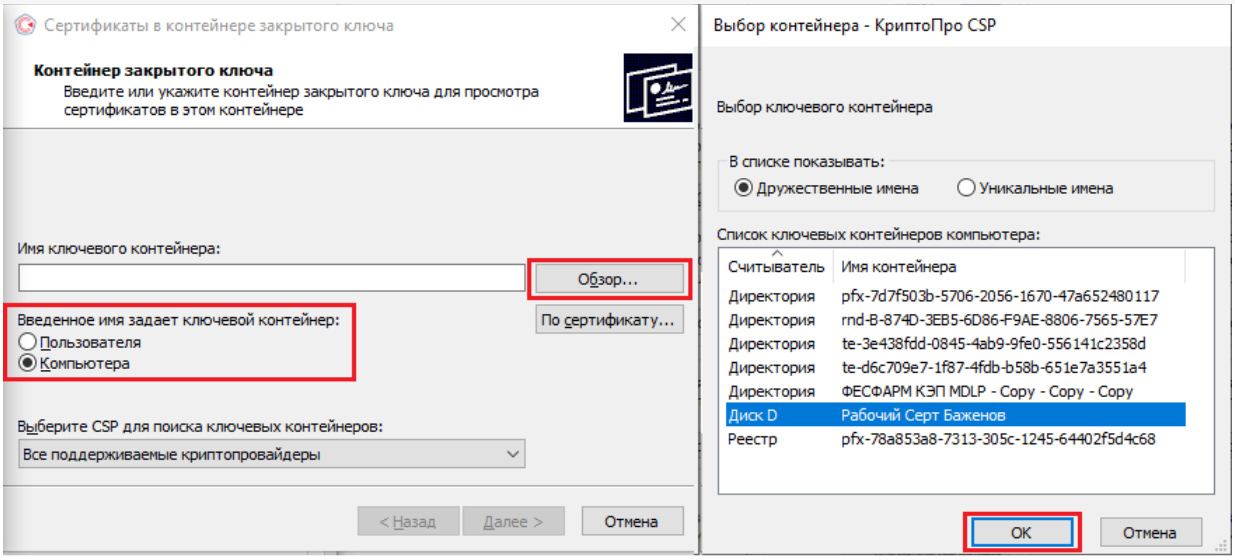


После этого вы можете сравнить два отпечатка.

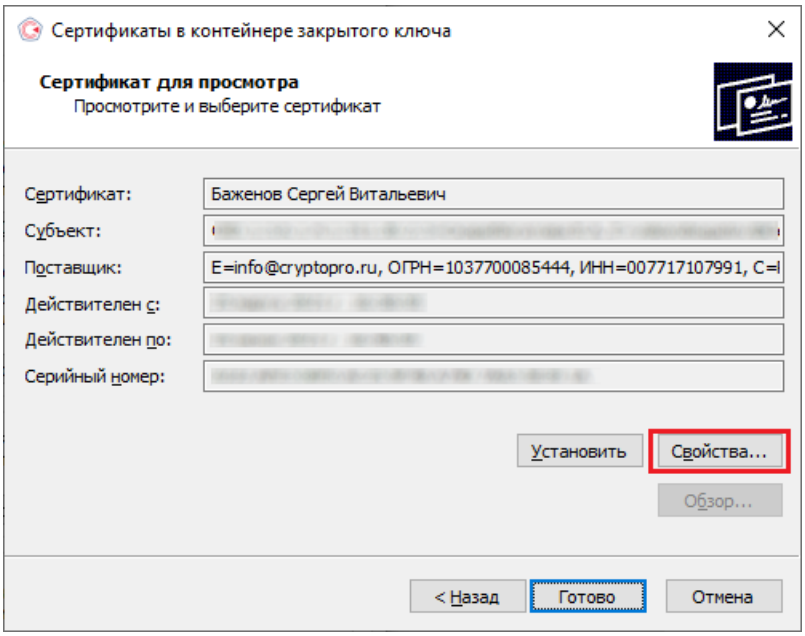
Способ 2. Переустановить сертификат на ПК из контейнера. Для этого запустите КриптоПРО CSP от имени администратора, перейдите во вкладку «Сервис» и нажмите на кнопку «Просмотреть сертификаты в контейнере».



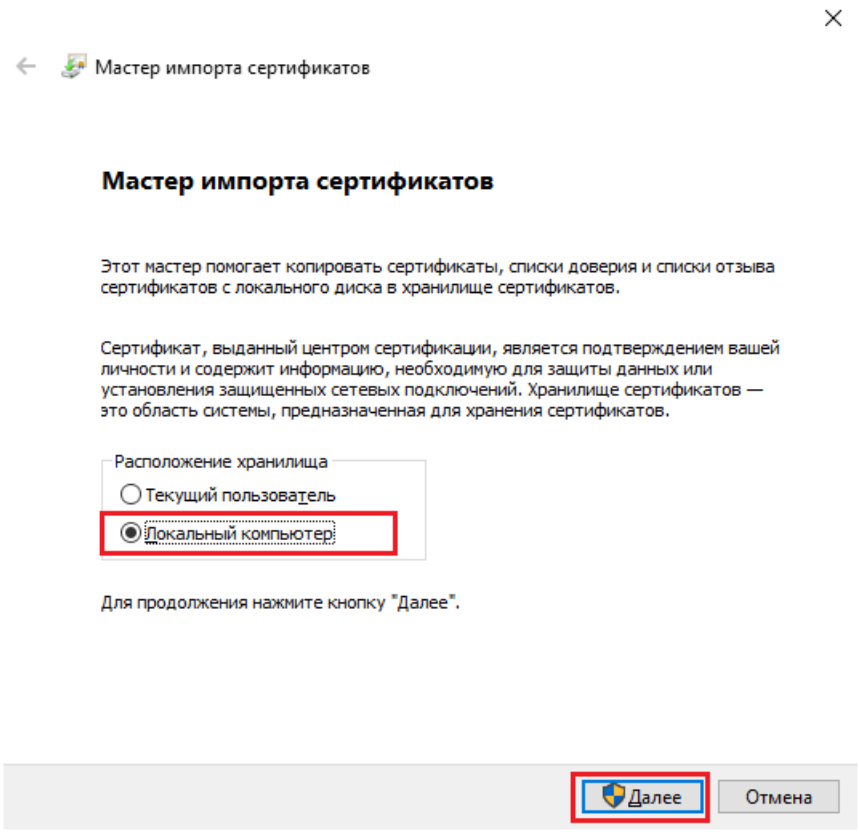
В открывшемся окне нужно выбрать «Введенное имя задает ключевой контейнер» — «Компьютер», далее нажать на кнопку «Обзор», выбрать контейнер из списка и нажать «ОК».



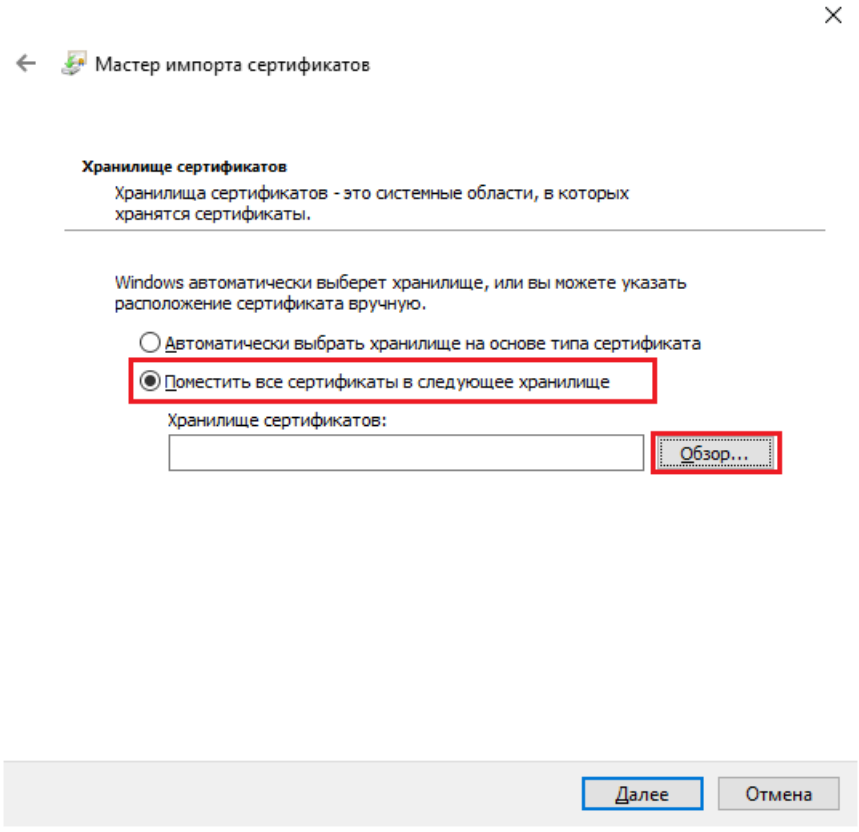
Откроется окно с информацией о сертификате, в котором необходио нажать на «Свойства» → «Установить сертификат».



В качестве хранилища сертификата необходимо выбрать «Локальный компьютер».



В следующем окне необходимо выбрать «Поместить все сертификаты в следующее хранилище» → «Обзор» → «Личное».



Нажмите «Далее» → «Готово». После этого импорт сертификата будет успешно выполнен.

Не нашли что искали?

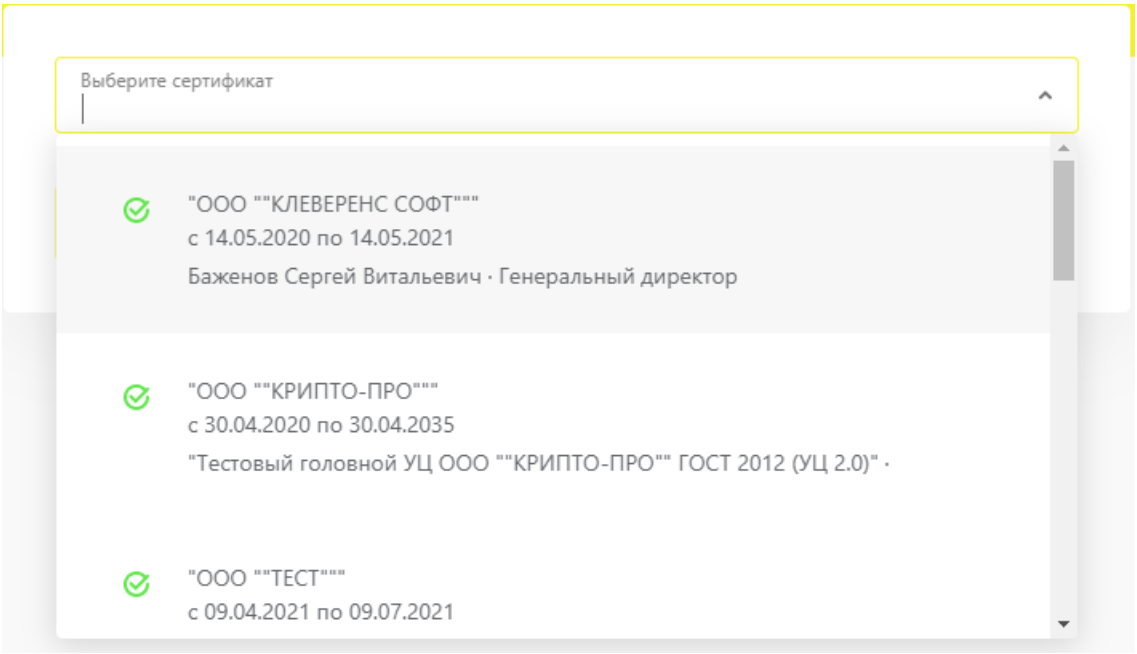
Задать вопрос в техническую поддержку

Подключение к станции управления заказами

Последние изменения: 2024-03-26

Для подключения к СУЗ потребуется установить контейнер закрытого ключа на пользователя. После этого появится возможность подключиться к порталу СУЗ (демонстрационный режим для тестирования).

После установки контейнера на пользователя он будет доступен для выбора на сайте СУЗ.



Не нашли что искали?

Задать вопрос в техническую поддержку

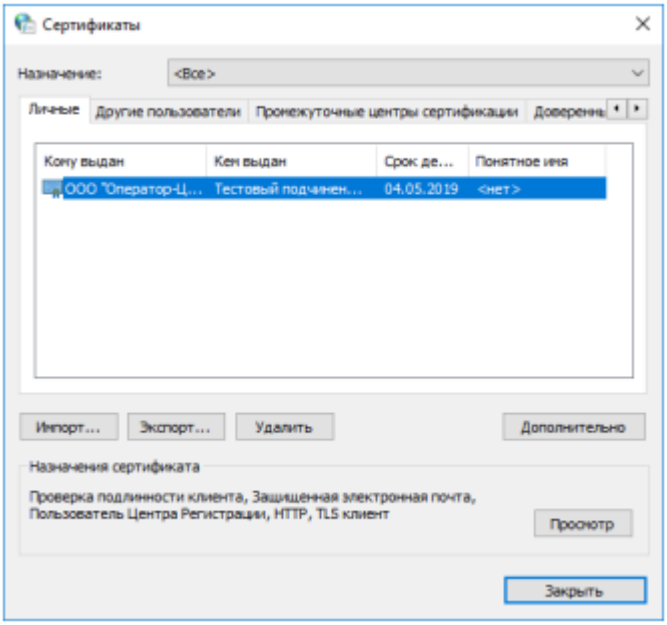
Построение цепочки доверия КСКПЭП

Последние изменения: 2024-03-26

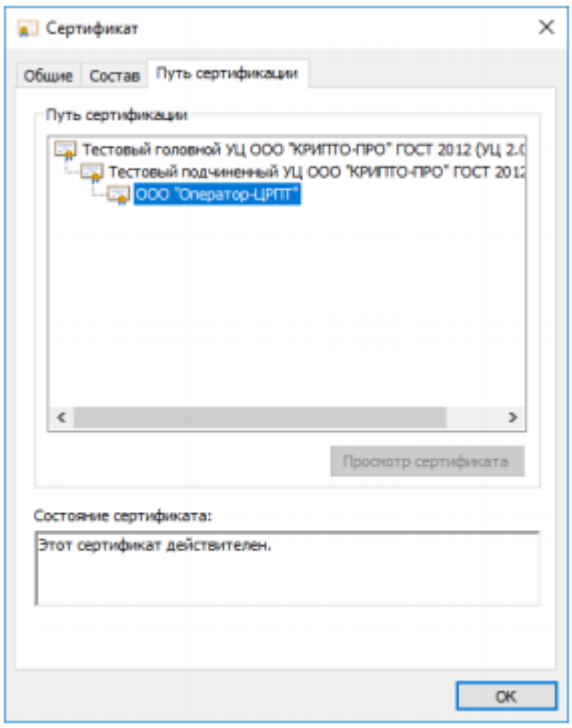
Для того чтобы выстроить цепочку доверия КСКПЭП, необходимо:

- В меню «Пуск» выберите «Панель управления» → «Свойства браузера» → вкладка «Содержание» → «Сертификаты». Откройте вкладку «Личные»:

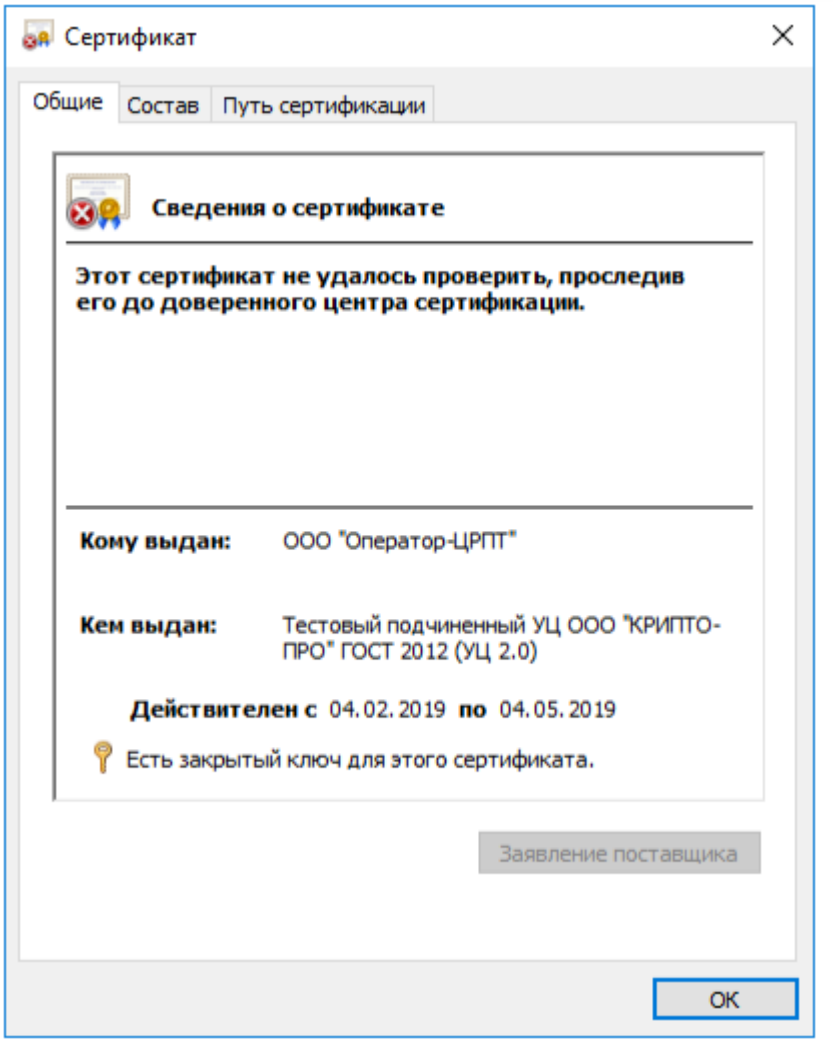
> Если в данном окне не отображаются сертификаты, это значит, что ранее не был произведен импорт сертификатов на пользователя. Чтобы сертификаты отображались во вкладке «Личные», необходимо после их установки прописать их и на локальный компьютер, и на текущего пользователя.
> Если после этих действий сертификаты все равно не отображаются, а работа происходит в тестовой среде, то следует скачать и установить промежуточный сертификат тестового удостоверяющего центра, импортировать их и на локальный компьютер, и на пользователя, а затем вновь открыть вкладку с сертификатами.



- Выберите установленный сертификат, кликнув по нему два раза левой кнопкой мыши. Перейдите на вкладку «Путь сертификации»:

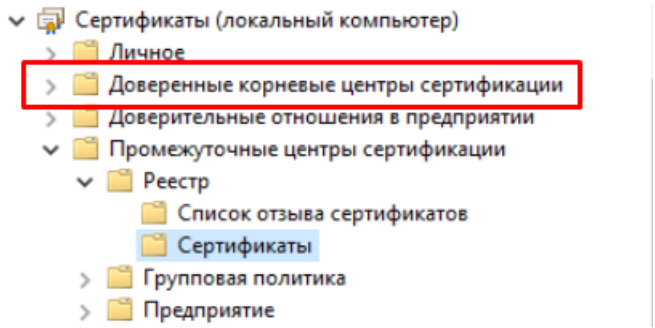


- На вкладке «Путь сертификации» должна отображаться цепочка сертификатов, с помощью которых устанавливается доверие. Если цепочка не сформирована, потребуется добавить сертификаты самостоятельно (см. ниже). Если какой-то из этих сертификатов не будет установлен, то при подключении к СУЗ будут появляться ошибки.
  В поле «Состояние сертификата» должно отображаться сообщение о действительности сертификата.
  В случае если во вкладке «Общие"→ «Сведения о сертификате» отображается «Этот сертификат не удалось проверить, проследив его до доверенного центра сертификации» — необходимо установить корневой сертификат ГУЦ и удостоверяющего центра, выдавшего вашу электронную подпись (как это сделать с помощью мастера импорта сертификатов, смотрите пункт 3).

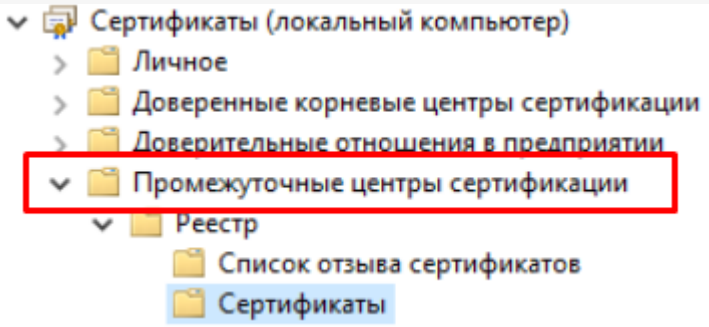


У демонстрационного и рабочего сертификата разные цепочки сертификации, поэтому если будет установлены данные частично от одного и от другого сертификата, ничего работать не будет.

Сертификат Головного Удостоверяющего Центра и удостоверяющего центра, выдавшего КСКПЭП юридическому лицу, будут размещаться в хранилище сертификатов «Доверенные корневые центры сертификации».



Остальные сертификаты цепочки будут размещаться в хранилище сертификатов «Промежуточные центры сертификации». Как их туда добавить самостоятельно с помощью мастера импорта сертификатов, описано в пункте 3, с отличием в том, что при выборе хранилища сертификатов указываются «Промежуточные центры сертификации».



Не нашли что искали?

Задать вопрос в техническую поддержку

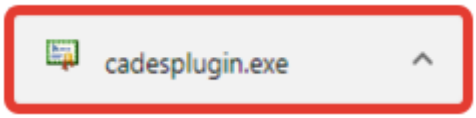
Установка КриптоПро ЭЦП Browser plug-in

Последние изменения: 2024-03-26

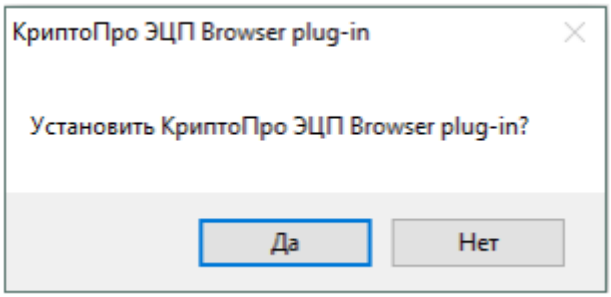
Для корректного функционирования веб-страниц, использующих КриптоПро ЭЦП Browser plug-in, недостаточно расширения для браузера. Сначала необходимо скачать установочный файл и установить его.

Для работы плагина требуется установленный КриптоПро CSP версии 3.6 R4 и выше. Дистрибутив и инструкцию по установке можно получить по ссылке.

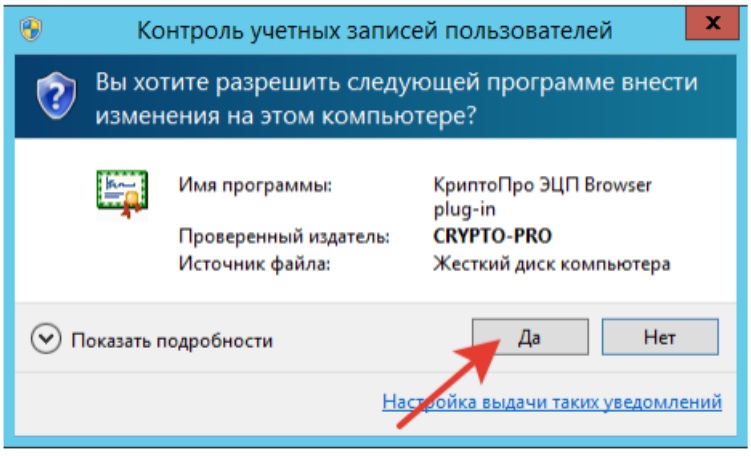
- Скачайте программу установки. КриптоПро ЭЦП Browser plug-in доступен по ссылке.
- Запустите исполняемый файл cadesplugin.exe.



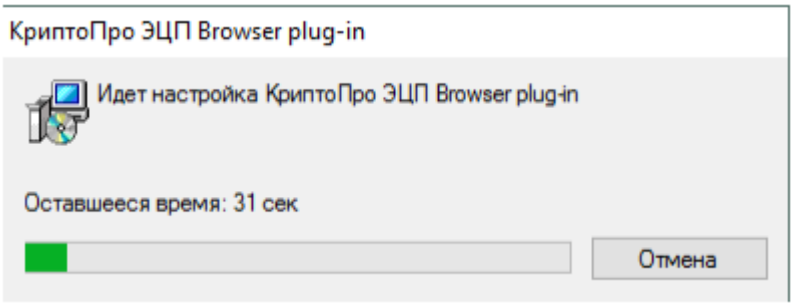
- Подтвердите установку КриптоПро ЭЦП Browser plug-in.



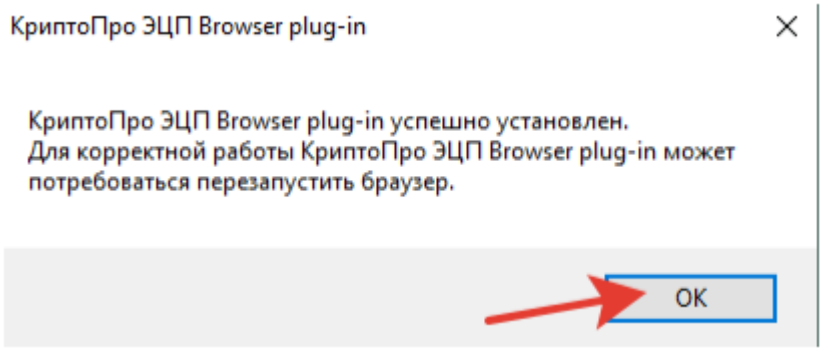
- Если потребуется, разрешите КриптоПро ЭЦП Browser plug-in внести изменения путем нажатия кнопки «Да».



- Дождитесь окончания установки КриптоПро ЭЦП Browser plug-in.

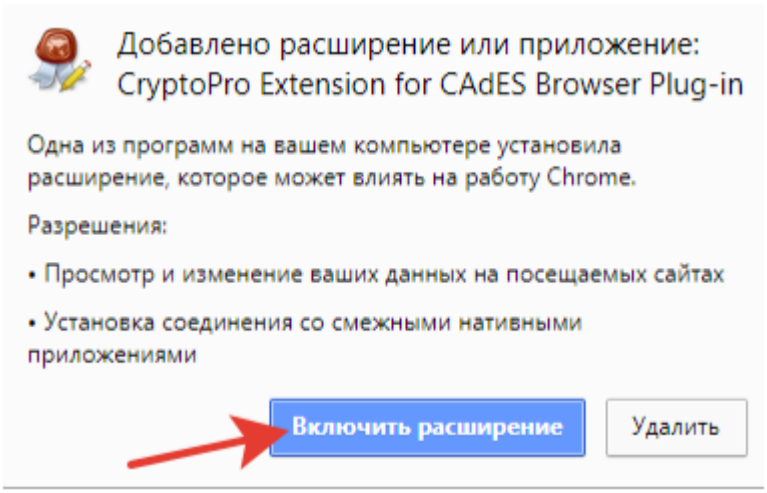


- После окончания установки КриптоПро ЭЦП Browser plug-in нажмите ОК.

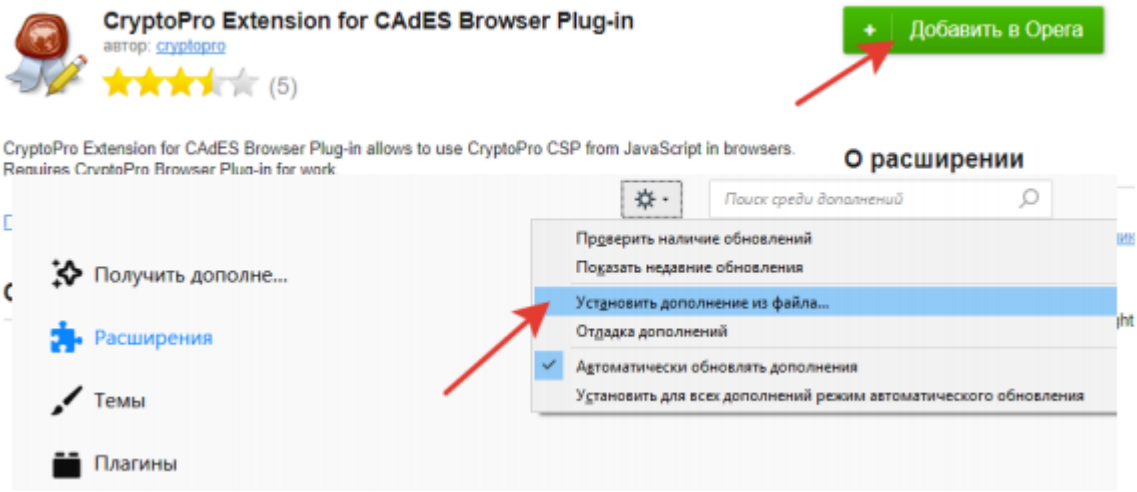


- Дальнейшие настройки различаются в зависимости от используемого браузера.

  Браузер Chrome: запустите Chrome и дождитесь оповещения об установленном расширении «CryptoPro Extension for CAdES Browser Plug-in». Включите это расширение. Если на Вашем компьютере ранее уже выполнялась установка КриптоПро ЭЦП Browser plug-in, а потом он был удален, потребуется отдельно установить расширение. Для этого перейдите по ссылке и установите расширение из интернет-магазина Chrome.



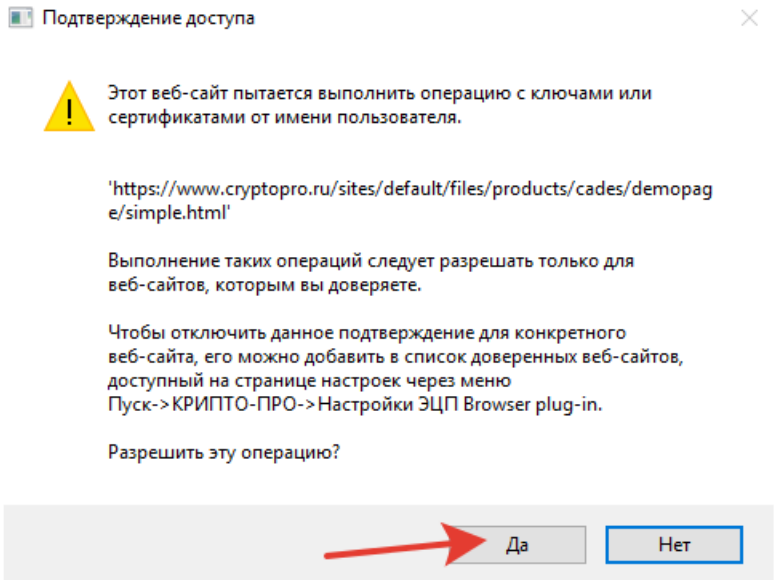
  Браузер Opera или Яндекс.Браузер: расширение доступно по ссылке.



Браузер Firefox: скачайте расширение по ссылке и установите в браузер самостоятельно.

Браузер Microsoft Internet Explorer: не требуется дополнительных настроек.

- Проверьте корректность установки на странице проверки плагина. Для этого в открывшемся окне подтвердите доступ путем нажатия кнопки «Да».



- Если установка КриптоПро ЭЦП Browser plug-in прошла успешно, появится окно с надписью «Плагин загружен», указанием его версии и используемой Вами версии КриптоПро CSP.

Не нашли что искали?

Задать вопрос в техническую поддержку