
**Удостоверяющий Центр
ПАО «МТС-Банк»**

Руководство пользователя

1. Требования к системе для работы с Удостоверяющим Центром (УЦ).

Для работы с Удостоверяющим Центром необходимо следующее программное обеспечение:

- Операционная система Microsoft Windows 2007 и выше
- Microsoft Internet Explorer" версии 9.0 или выше
- Драйвера для работы с защищенными ключевыми носителями (при необходимости)
- Средство криптографической защиты информации (СКЗИ) [КриптоПро CSP](#).
- Утилиту для создания и проверки электронной подписи (ЭП) на веб-страницах [КриптоПро ЭЦП browser plug-in](#) (**Важно! Не работает** в браузере EDGE, предустановленном по умолчанию в Windows 10)
- [Сертификат Удостоверяющего центра](#) ;

Наряду с этим, необходимо наличие доступа со стороны пользователя к Удостоверяющему Центру по стандартному протоколу HTTP (порт 80) и по защищенному протоколу HTTPS (порт 443).

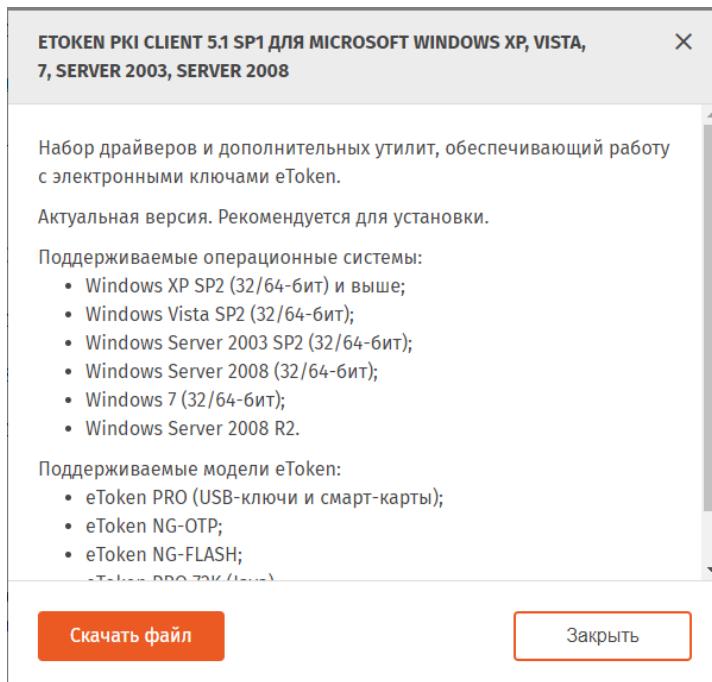
2. Установка драйвера ключевого носителя

В настоящий момент, Банк использует следующие ключевые носители: eToken PRO (Java) и Рутокен ЭЦП 2.0. Подробную информацию по данным устройствам, а также найти информацию об эксплуатации и настройке ПО других устройств можно всегда на официальных сайтах производителей этих устройств.

2.1 Установка драйвера ключевого носителя eToken

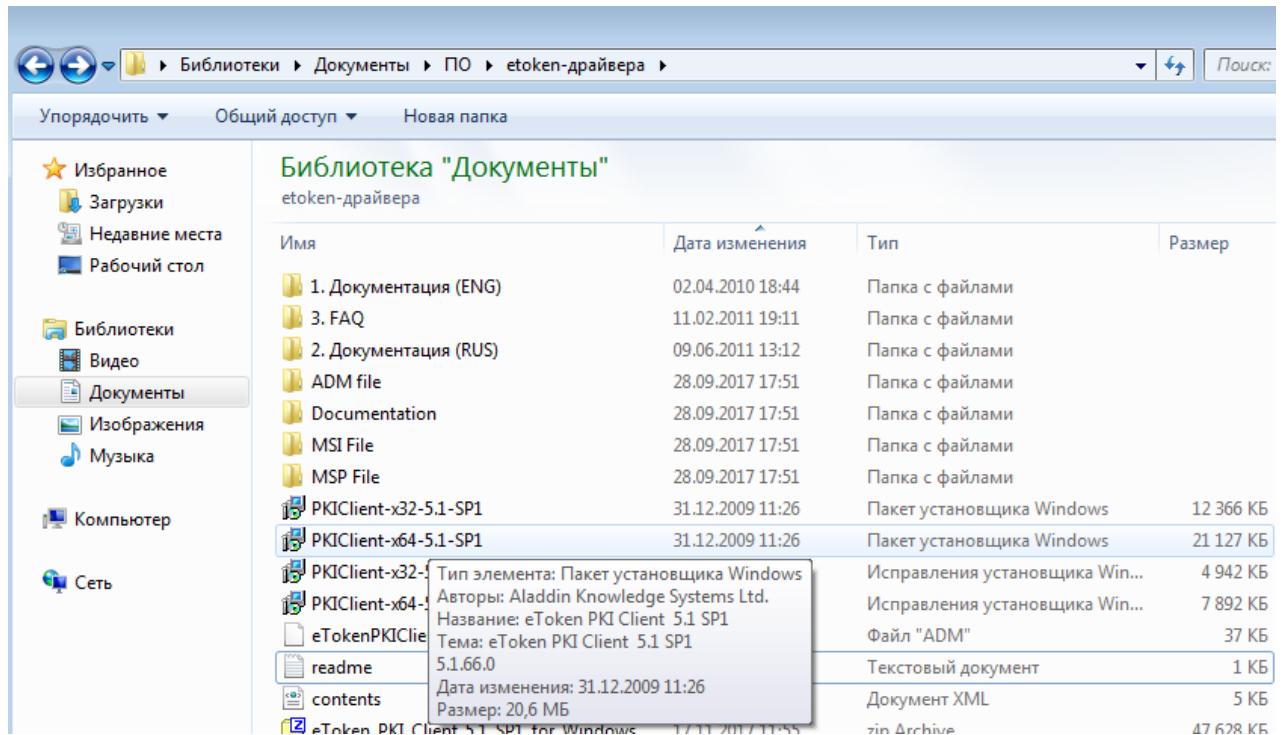
Для получения актуальной версии драйвера для работы с ключевыми носителями eToken необходимо перейти на официальный сайт компании «Аладдин Р.Д.» <http://www.aladdin-rd.ru/support/downloads/etoken/>, далее необходимо выбрать и загрузить версию драйвера под используемую операционную систему на рабочем месте.

Ниже рассмотрен пример установки драйвера eToken - с официального сайта компании «Аладдин Р.Д.» была загружена последняя версия драйвера eToken PKI Client 5.1 SP1 для



Переходим в каталог загруженных файлов и распаковываем скачанный архив в папку на диске.

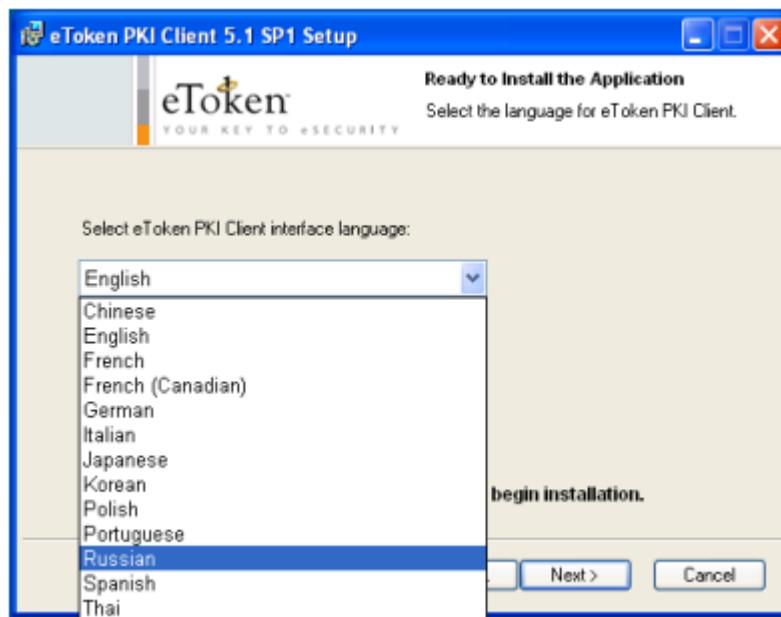
Переходим в каталог с распакованными файлами драйвера и запускаем установочный пакет Windows Installer для той операционной системы, которая установлена на рабочем месте (x32 или x64).



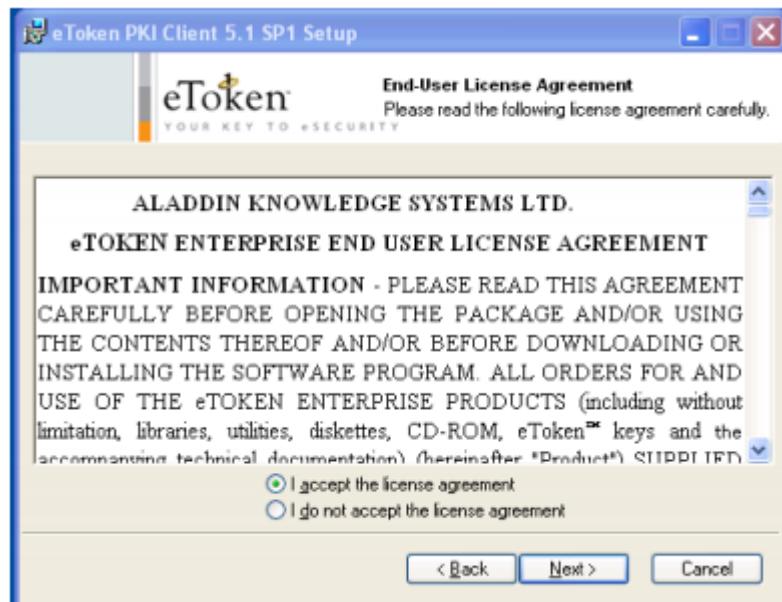
Далее появится окно установки драйвера eToken, нажимаем кнопку «Next»



В следующем окне необходимо выбрать язык графического интерфейса программы:



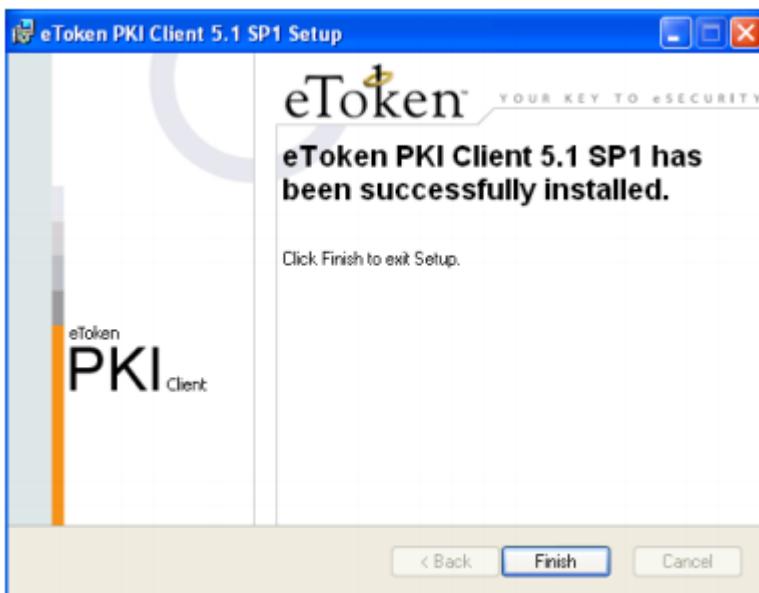
Прочтите лицензионное соглашение, если Вы с ним согласны, то необходимо выбрать пункт «I accept the license agreement» и нажать «Next»:



В следующем окне установщика указывается каталог установки драйвера eToken. По умолчанию установка производится в каталог ***«C:\Program Files\Aladdin\etoken»***, если на диске такой папки не существует, то она будет создана автоматически. Можно изменить путь установки нажатием кнопки. В данном примере путь установки оставляем по умолчанию и нажимаем кнопку «Next»:



Далее будет произведена установка драйвера eToken, по завершению появится окно завершения установки, где необходимо нажать кнопку «Finish»:



2.2 Установка драйвера ключевого носителя Рутокен

Для получения актуальной версии драйвера для работы с ключевыми носителями Рутокен необходимо перейти на официальный сайт USB- идентификаторов Рутокен <http://www.rutoken.ru/support/download/drivers-forwindows/>, далее необходимо выбрать и загрузить версию драйвера под используемую операционную систему на рабочем месте.

Далее будет рассмотрен пример установки драйвера Рутокен для операционных систем Microsoft Windows. С официального сайта USB-идентификаторов Рутокен была загружена последняя версия драйвера Рутокен для Microsoft Windows (x86 и x64)

The screenshot shows the official Rutoken website. At the top, there is a red header bar with the Rutoken logo. Below it, a navigation bar includes links for 'Продукты', 'Решения', 'Технологии', 'Поддержка', 'Заказ', and 'Центр загрузка'. The main content area has a breadcrumb navigation: Главная > Поддержка > Центр загрузки > Драйверы для Windows. A large section title 'ДРАЙВЕРЫ ДЛЯ WINDOWS' is centered above a list of download options. On the left, a sidebar titled 'ЦЕНТР ЗАГРУЗКИ' lists various driver categories. The first item in the list is 'Драйверы для Windows', which is highlighted in red. To its right, under the heading 'Пользователям Рутокен', there is a note about installing drivers and a download link for 'Драйверы Рутокен для Windows, EXE'. Below this, there are sections for 'Системным администраторам' and 'Утилиты'.

Во время загрузки прочтите лицензионное соглашение, если Вы с ним согласны, то необходимо выбрать пункт «Условия Лицензионного соглашения прочитаны и приняты в полном объеме» и нажать «Условия приняты»:

ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ

Перед использованием программных продуктов и/или онлайн-сервисов Рутокен (Rutoken), ознакомьтесь с условиями Лицензионного соглашения. Любое использование программных продуктов и/или онлайн-сервисов Рутокен (Rutoken) означает полное и безоговорочное принятие его условий.

[Загрузить Лицензионное соглашение в виде отдельного PDF-документа](#)

Утверждено
Приказом генерального директора
ЗАО «Актив-софт»
№ 01-ЛС от 31.08.2012 г.

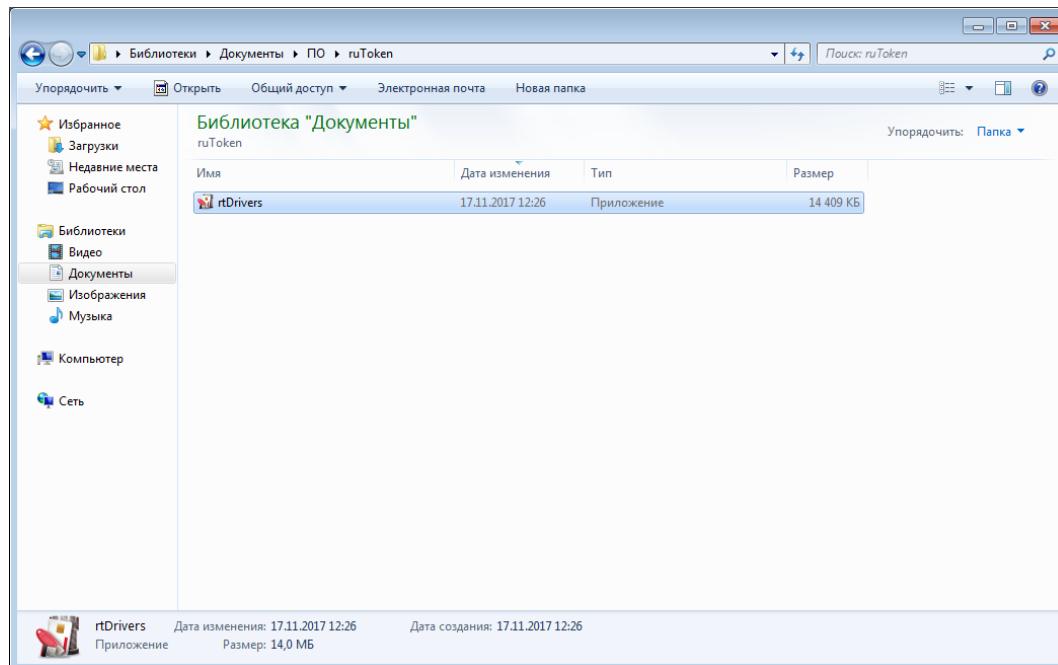
Лицензионное соглашение
на использование программных продуктов
и/или онлайн-сервисов Рутокен (Rutoken)
Редакция №1 от 31.08.2012 г.

Настоящий документ представляет собой предложение Закрытого акционерного общества «Актив-софт» (далее – «Правообладатель») заключить соглашение на изложенных ниже условиях.

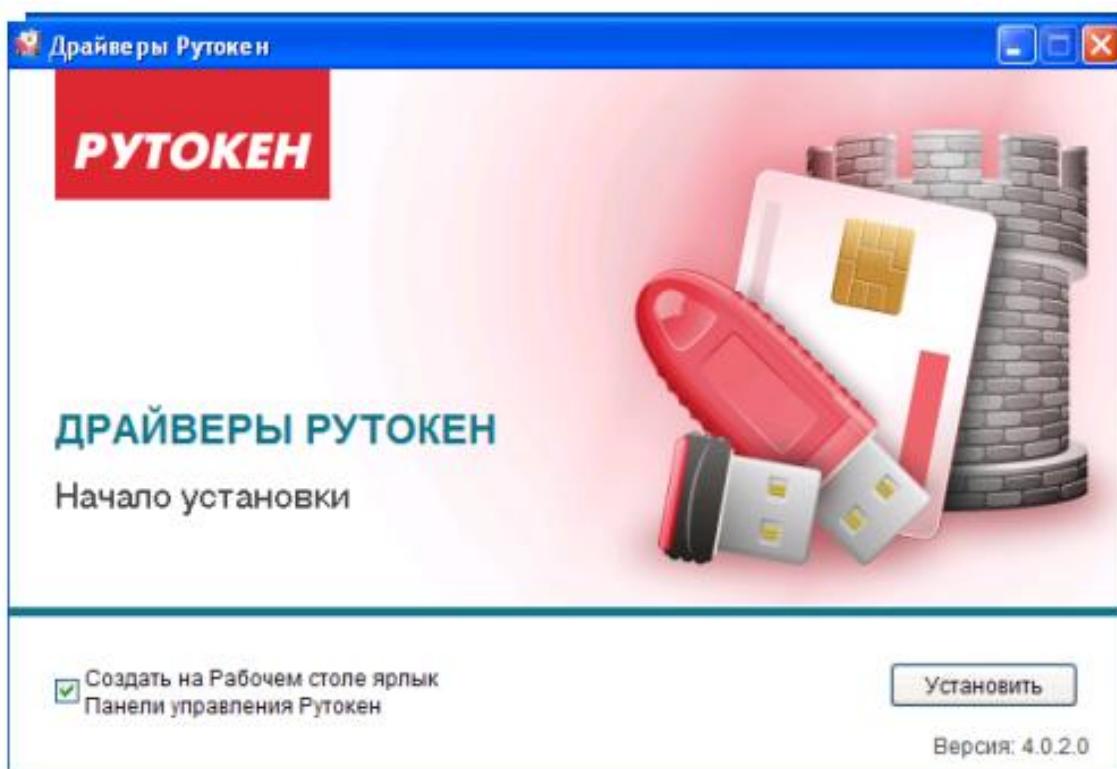
Условия Лицензионного соглашения прочитаны и приняты в полном объеме.

УСЛОВИЯ ПРИНЯТЫ

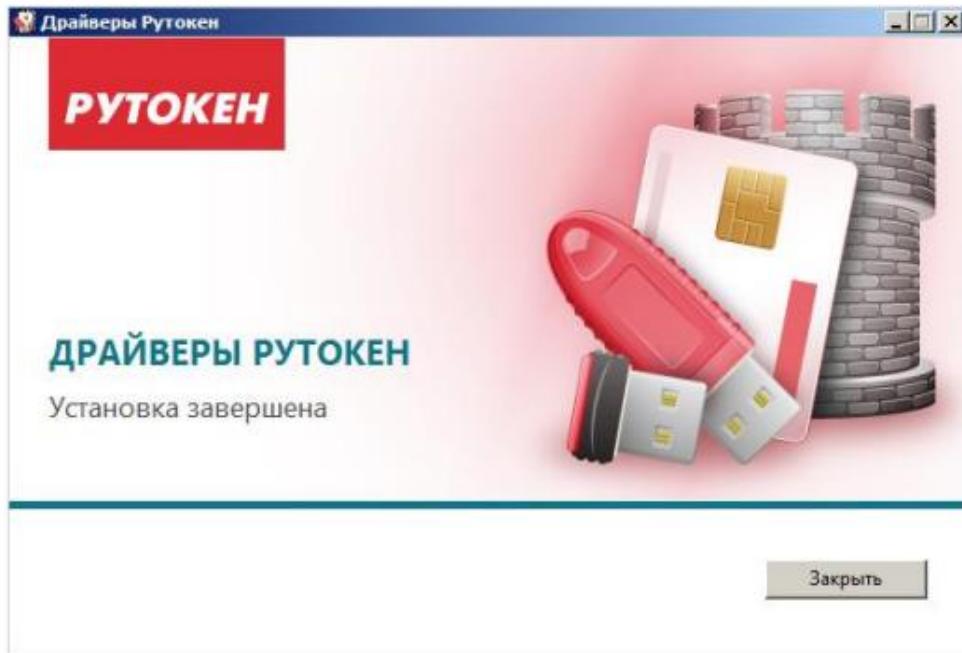
Переходим в каталог загруженных файлов и запускаем скачанный файл:



Далее появится окно установки драйвера РУТОКЕН, нажимаем кнопку «Установить». Если Вам не нужно создавать ярлык панели управления Рутокен на рабочем столе – необходимо снять соответствующую галку.



Далее будет произведена установка драйвера РУТОКЕН, по завершению появится окно завершения установки, где необходимо нажать кнопку «Закрыть»:

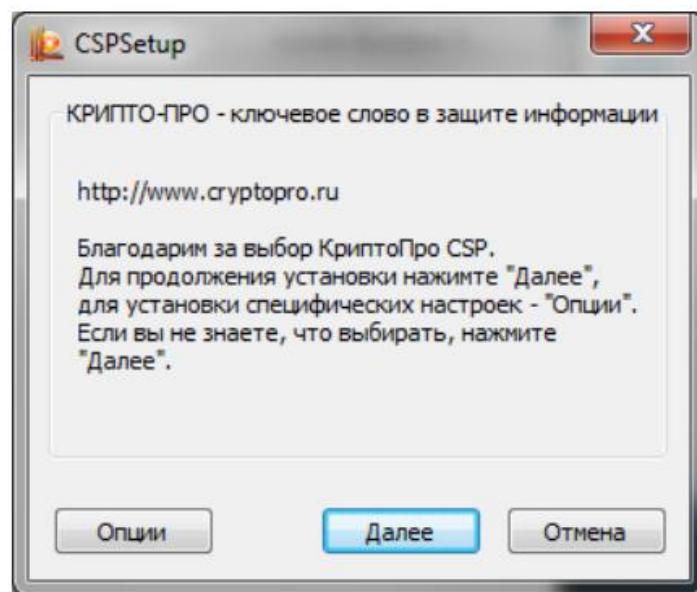


3. Установка средства криптографической защиты информации (СКЗИ) "КриптоPro CSP" версии 4.0

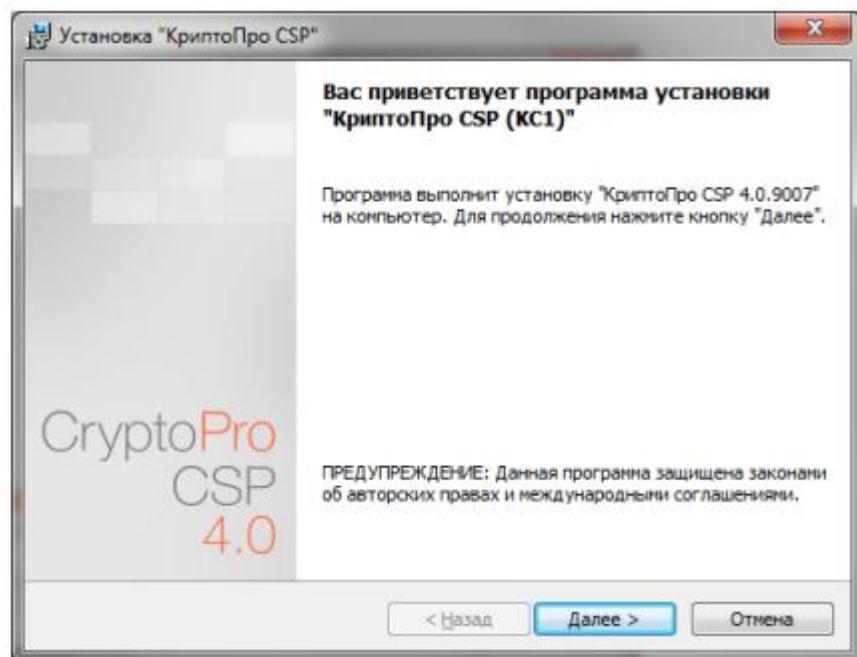
Внимание: Установка СКЗИ "КриптоPro CSP" должна производиться пользователем, имеющим **права администратора на локальном компьютере** (пароль локального администратора не должен быть пустым). Перед установкой ПО, удалите все ранее установленные (устаревшие) версии данного программного обеспечения. Для этого используйте следующие пункты основного меню системы Windows: **Пуск – Настройка – Панель Управления – Установка и удаление программ.**

Разработчиком КриптоPro CSP является компания "КРИПТО-ПРО", занимающая лидирующее положение на отечественном рынке программных СКЗИ. На сегодняшний день есть сразу три разные версий КриптоPro CSP: 3.6, 3.9 и 4.0. Они различаются между собой по поддерживаемым операционным системам, поддерживаемым криптографическим алгоритмам и срокам действия сертификатов соответствия, выдаваемых ФСБ России. На сайте "КРИПТО-ПРО" размещены таблицы сравнений версий, там также доступна информация о действующих сертификатах соответствия. Скачать дистрибутив СКЗИ "КриптоPro CSP" Вы сможете на сайте разработчика ПО после прохождения процедуры регистрации: <http://www.cryptopro.ru/downloads>

Запустите программу установки КриптоПро CSP 4.0 для Windows (x86-x64).exe

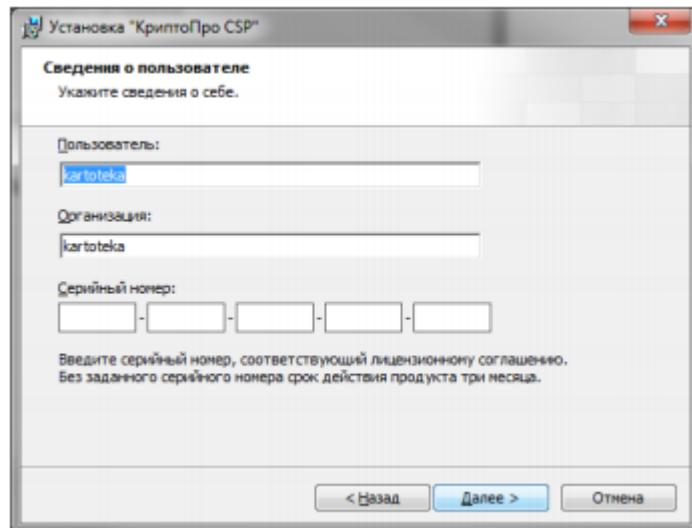


Нажмите "Далее".

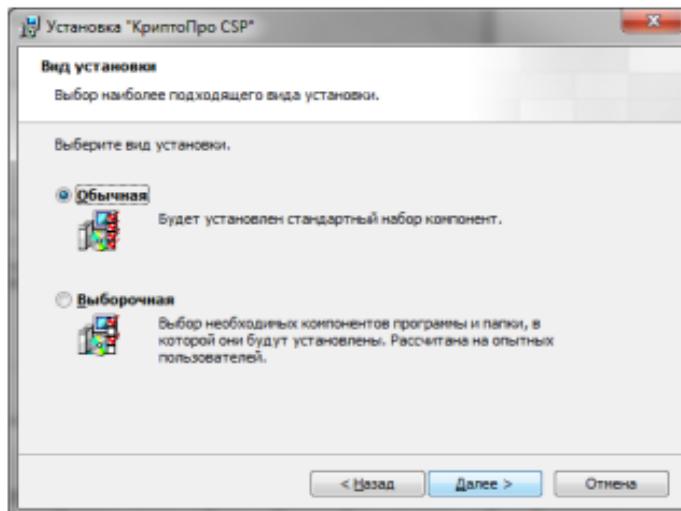


Нажмите "Далее". Прочтайте лицензионное соглашение. Выберите: «Я принимаю условия лицензионного соглашения» и нажмите «Далее».

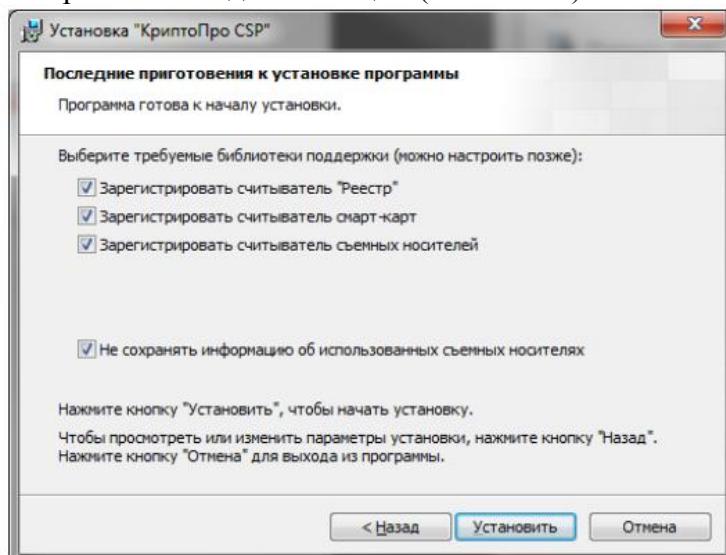
Введите номер лицензии:



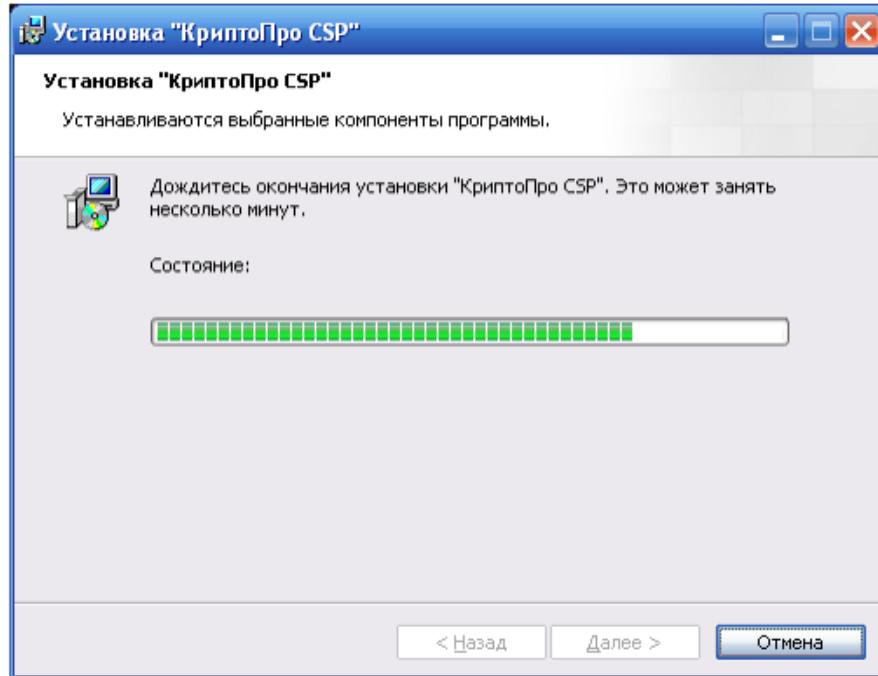
Нажмите «Далее» и выберите вид установки («Обычная»):



Нажмите «Далее». Выберите необходимые опции (можно все) и нажмите «Установить»



Начнется процесс установки программы.

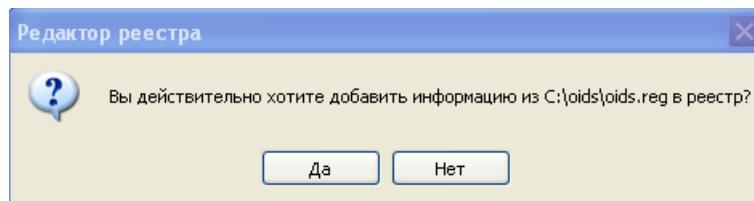


Дождитесь окончания установки и перезагрузите компьютер.

Установка программы завершена.

4. Настройка перечня объектных идентификаторов (OID).

Для возможности обозначения области применения сертификата необходимо загрузить и установить файл со страницы загрузки УЦ: <http://ca.mtsbank.ru/soft/oids.zip>
Установка данного файла возможна только с правами локального администратора.



5. Установка сертификата Удостоверяющего центра

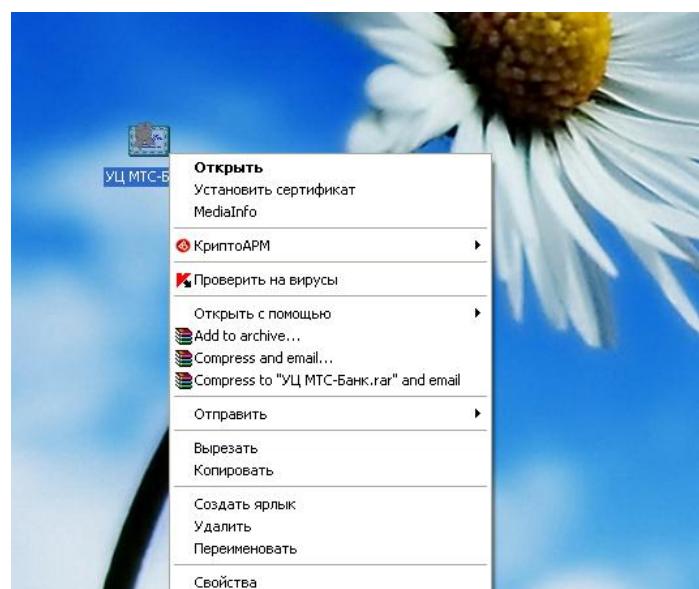
Сертификат можно скачать с Web-сервера Удостоверяющего центра <http://ca.mtsbank.ru/>,

The screenshot shows a web browser window with the URL <http://ca.mtsbank.ru/>. The page content includes:

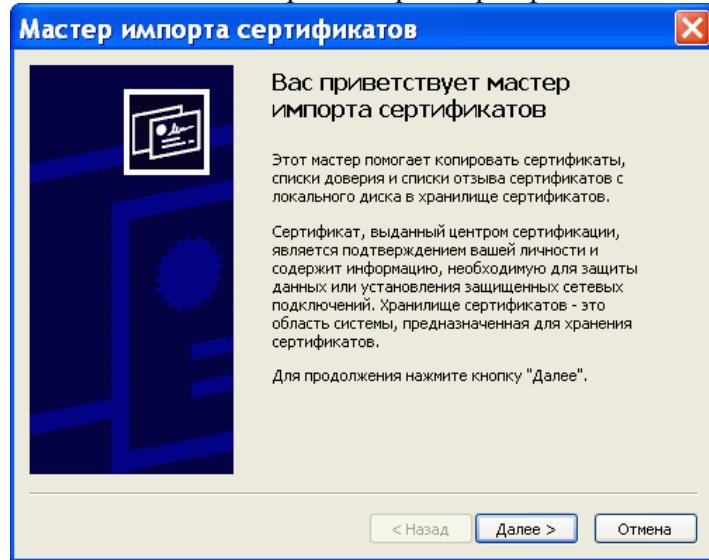
- Подсистема удаленного (Web) доступа пользователей к Центру Регистрации позволяет Вам:**
 - Зарегистрироваться и получить свой первый сертификат открытого ключа, с помощью которого будет осуществляться взаимодействие с Центром Регистрации.
 - Формировать служебные ключи пользователя.
 - Создавать и отправлять запросы на формирование сертификатов для различных назначений по шаблонам, установленным в нашем Удостоверяющем Центре.
 - Производить плановую смену ключей и сертификатов.
 - Формировать и отправлять запросы на отзыв сертификатов.
 - Отслеживать состояние отправленных запросов.
 - Получать, устанавливать и распечатывать выпущенные сертификаты.
- Для обеспечения конфиденциальности, авторства и целостности информации обмен данными с Центром Регистрации Удостоверяющего Центра осуществляется посредством защищенного протокола TLS с двухсторонней аутентификацией.**
- Установка необходимого программного обеспечения** Для работы с Удостоверяющим Центром требуется установить на Вашем компьютере программное обеспечение:
 - "Microsoft Internet Explorer" версии 9.0 или выше
 - Средство криптографической защиты информации (СКЗИ) [КриптоПро CSP](#).
 - Утилиту для создания и проверки электронной подписи (ЭП) на веб-страницах [КриптоПро ЭЦП browser plug-in](#) и обновить страницу
 - [Сертификат Удостоверяющего центра](#)
- Более подробную информацию о порядке установки программного обеспечения и правилах работы с сертификатами Вы можете получить из Руководства пользователя Удостоверяющего Центра в разделе Документация (таблица ниже).**
- Если Вы уже зарегистрированы в Удостоверяющем Центре ПАО МТС-Банк, для входа нажмите кнопку:** Вход для зарегистрированных пользователей
- Если Вы сотрудник банка для регистрации в Удостоверяющем Центре МТС-Банк нажмите кнопку:** Вход для регистрации сотрудников банка
- Если Вы Клиент банка для регистрации в Удостоверяющем Центре МТС-Банк нажмите кнопку:** Вход для регистрации Клиентов банка
- Адрес электронной почты Удостоверяющего Центра: ca@mtsbank.ru**
- Контактный телефон: (495) 921-28-00, доб. 33-30, 33-39**
- Меню навигации:** Сертификат Удостоверяющего центра | Справка загрузки ПО | Документация
- Адрес в браузере:** http://ca.mtsbank.ru/soft/УЦ%20МТС-Банк.r7b

Файл сертификата Удостоверяющего Центра ПАО «МТС-Банк» необходимо сохранить в любой папке Вашего компьютера (например, на рабочем столе).

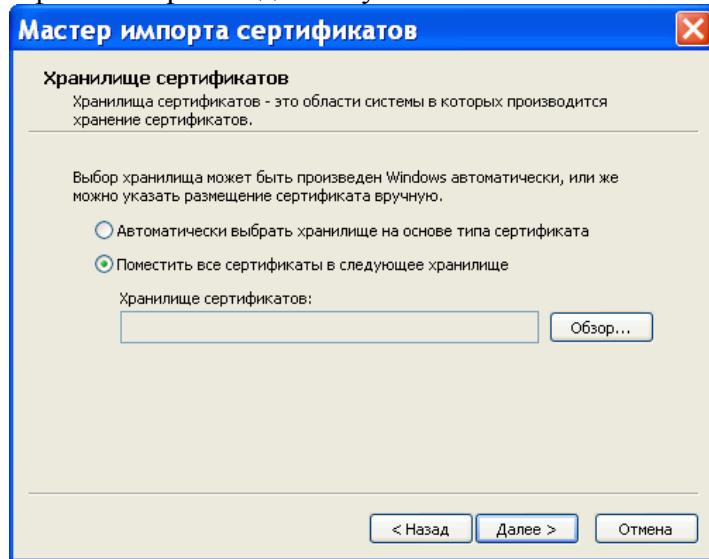
Для установки сертификата Удостоверяющего Центра щелкните по нему правой кнопкой мыши и в открывшемся контекстном меню выберите пункт **«Установить сертификат»**.

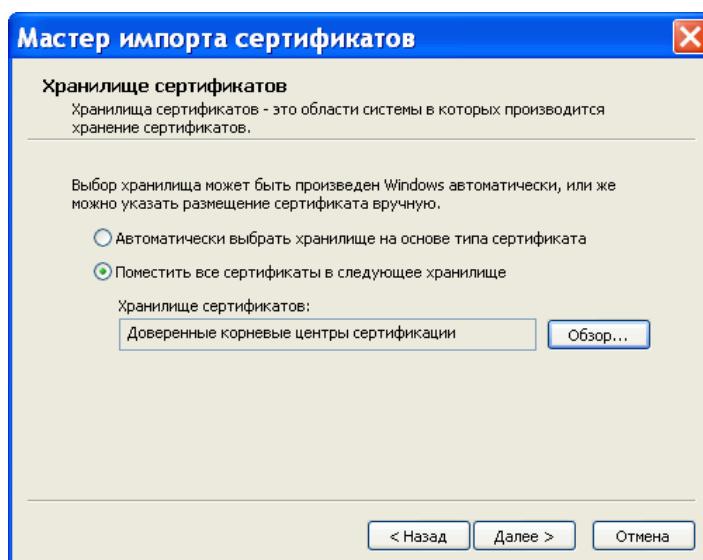
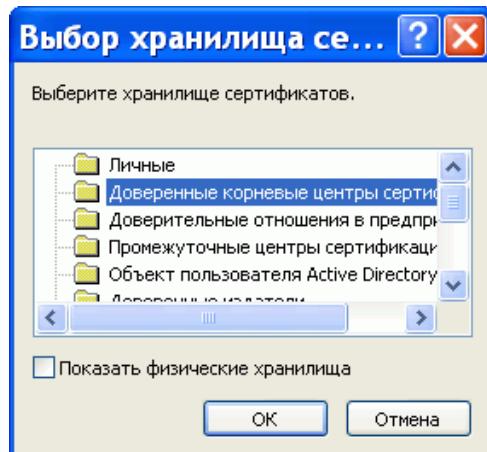


Далее необходимо с помощью Мастера импорта сертификатов

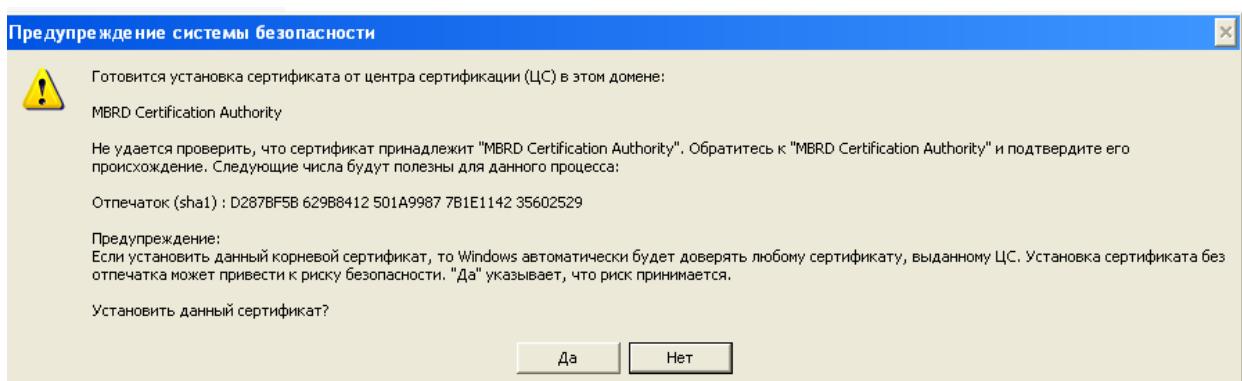


произвести установку сертификата в раздел «**Доверенные корневые центры сертификации**» хранилища сертификатов текущего пользователя. Выбор необходимого раздела хранилища сертификатов производится путем нажатия кнопки «**Обзор**»





В случае появления сообщения о добавлении сертификата в корневое хранилище необходимо нажать кнопку «Да». Появление подобного сообщения свидетельствует об успешной установке сертификата Удостоверяющего Центра. Отсутствие подобного сообщения свидетельствует о том, что сертификат Удостоверяющего Центра ранее уже был установлен на данный компьютер или сертификат не является корневым.



6. Установка плагина КриптоPro CSP в браузере Internet Explorer

КриптоPro ЭЦП browser plug-in (он же КриптоPro CADESCOM) - плагин, необходимый для создания и проверки электронной подписи на web-страницах с использованием КриптоPro CSP. Используется для работы на торговых площадках и порталах. Дистрибутив доступен на сайте КриптоPro в разделе Продукты / КриптоPro ЭЦП Browser plug-in http://www.cryptopro.ru/products/cades/plugin/get_2_0.

Системные требования:

- Установка плагина возможна на следующих операционных системах: Win XP SP3, Win Vista SP2, Win 2003 SP2, Win 2008 SP2, Win 7, Win 2008 R2, Win 8, Win8.1, Win10.
- Работает с браузерами: IE 8 — 11, Opera, Mozilla Firefox, Google Chrome, Yandex Browser
- **Не работает в браузере EDGE, предустановленном по умолчанию в Windows 10.**
- Требуется предустановленная КриптоPro CSP версии не ниже 3.6 R2

В Internet Explorer необходимо сделать следующие настройки:

- Добавить адрес сайта, на котором работаете с плагином, в надёжные узлы (Свойства браузера / безопасность / надёжные сайты / сайты / добавить адрес сайта).
- Если работа ведётся в Internet Explorer 11, то попробовать работу в режиме совместимости.
- Проверить, что адрес сайта добавлен в надёжные узлы плагина. Чтобы проверить, что сайт добавлен в надежные узлы плагина, нужно перейти в Пуск — Все программы — КРИПТО-ПРО - Настройки КриптоPro ЭЦП Browser plug-in. Откроется окно браузера, в котором нужно будет позволить разблокировать все содержимое страницы/разрешить доступ.

7. Регистрация пользователя в Удостоверяющем центре Банка

Перед началом работы пользователю Удостоверяющего Центра (далее УЦ) необходимо пройти процедуру регистрации в Реестре УЦ через Web-сайт <http://ca.mtsbank.ru/>. Для этого необходимо выбрать кнопку «*Вход для регистрации Клиентов банка*»

Более подробную информацию о порядке установки программного обеспечения и правилах работы с сертификатами Вы можете получить из **Руководства пользователя Удостоверяющего Центра** в разделе Документация (таблица ниже).

Если Вы уже зарегистрированы в Удостоверяющем Центре ПАО МТС-Банк, для входа нажмите кнопку: Если Вы сотрудник банка для регистрации в Удостоверяющем Центре МТС-Банк нажмите кнопку: Если Вы Клиент банка для регистрации в Удостоверяющем Центре МТС-Банк нажмите кнопку:

[Вход для зарегистрированных пользователей](#) [Вход для регистрации сотрудников банка](#) [Вход для регистрации Клиентов банка](#)

Адрес электронной почты Удостоверяющего Центра: ca@mtsbank.ru

Контактный телефон: (495) 921-28-00, доб. 33-30, 33-39

[Сертификат Удостоверяющего центра](#) [Страница загрузки ПО](#) [Документация](#)

Откроется страница самостоятельной регистрации. **Вводимые для регистрации данные должны полностью совпадать с данными в отправленном в Удостоверяющий центр Заявлении на регистрацию пользователя** (форма Заявления предусмотрена Договором (Соглашением) банковского обслуживания). **Логин и пароль необходимо запомнить!**

Регистрация пользователя

Общее имя*

Иванов Иван Иванович

Страна/регион

Российская Федерация ▾

Область

Город

Г. Москва

Организация

АО "Серп и Молот"

Подразделение

Адрес E-Mail

test@test.ru

Логин*

ivanovii.2017

Пароль*

5944260337

Уже есть логин

Внимание! Логин и пароль необходимо запомнить или записать.

Регистрация

После ввода полей экранной формы необходимо нажать кнопку «**Регистрация**». При этом происходит формирование запроса на регистрацию и постановка его в очередь на обработку на Центре Регистрации.

Обработка запроса на регистрацию производится администратором/оператором Центра Регистрации только в случае полного соответствия регистрационных атрибутов идентификационным данным, указанным в заявлении на регистрацию. Изменение идентификационных данных пользователя после подачи запроса на регистрацию невозможно.

После постановки запроса на регистрацию в очередь в окне обозревателя Microsoft Internet Explorer отображается следующая экранная форма

Заявка на регистрацию отправлена на обработку.

Воспользуйтесь [здесь](#) указанным именем входа и паролем для определения статуса вашей заявки или продолжения процесса регистрации (получения сертификата) в случае, если Ваша заявка была одобрена администратором.

Запрос на регистрацию размещается в очереди на обработку без уведомления администратора/оператора Центра Регистрации (ЦР).

В период рассмотрения запроса на регистрацию пользователь должен самостоятельно контролировать статус обработки запроса. Для этого необходимо воспользоваться ссылкой на Web-сайте центра регистрации «Вход для зарегистрированных пользователей».

The screenshot shows a web browser window for the MTS Bank Certification Center. The URL in the address bar is <https://ca.mtsbank.ru/ui/Default.aspx>. The page title is "Удостоверяющий Центр ПАО «МТС-Банк»". The main content area displays a message: "Добро пожаловать в Удостоверяющий Центр!" (Welcome to the Certification Center!). Below this, there is a note about the center's role in issuing and managing certificates. A list of tasks available via the Web interface follows. Further down, there is information about TLS security and instructions for setting up the software environment. At the bottom, there are three buttons for different user roles: "Вход для зарегистрированных пользователей" (for registered users), "Вход для регистрации сотрудников банка" (for bank staff registration), and "Вход для регистрации Клиентов банка" (for client registration). The footer contains the address for electronic mail and the contact phone number.

Удостоверяющий Центр ПАО «МТС-Банк»

Добро пожаловать в Удостоверяющий Центр!

Удостоверяющий Центр МТС Банка осуществляет выпуск и сопровождение сертификатов ключей электронной подписи и шифрования для Клиентов и сотрудников ПАО «МТС-Банк»

Подсистема удаленного (Web) доступа пользователей к Центру Регистрации позволяет Вам:

- Зарегистрироваться и получить свой первый сертификат открытого ключа, с помощью которого будет осуществляться взаимодействие с Центром Регистрации.
- Формировать служебные ключи пользователя.
- Создавать и отправлять запросы на формирование сертификатов для различных назначений по шаблонам, установленным в нашем Удостоверяющем Центре.
- Производить плановую смену ключей и сертификатов.
- Формировать и отправлять запросы на отзыв сертификатов.
- Отслеживать состояние отправленных запросов.
- Получать, устанавливать и распечатывать выпущенные сертификаты.

Для обеспечения конфиденциальности, авторства и целостности информации обмен данными с Центром Регистрации Удостоверяющего Центра осуществляется посредством защищенного протокола TLS с двухсторонней аутентификацией.

Установка необходимого программного обеспечения Для работы с Удостоверяющим Центром требуется установить на Вашем компьютере программное обеспечение:

- "Microsoft Internet Explorer" версии 9.0 или выше
- Средство криптографической защиты информации (СКЗИ) [КриптоПро CSP](#).
- Утилиту для создания и проверки электронной подписи (ЭП) на веб-страницах [КриптоПро ЭЦП browser plug-in](#) и обновить страницу
- [Сертификат Удостоверяющего центра](#)

Более подробную информацию о порядке установки программного обеспечения и правилах работы с сертификатами Вы можете получить из **Руководства пользователя Удостоверяющего Центра** в разделе Документация (таблица ниже).

Если Вы уже зарегистрированы в Удостоверяющем Центре ПАО МТС-Банк, для входа нажмите кнопку: [Вход для зарегистрированных пользователей](#)

Если Вы сотрудник банка для регистрации в Удостоверяющем Центре МТС-Банк нажмите кнопку: [Вход для регистрации сотрудников банка](#)

Если Вы Клиент банка для регистрации в Удостоверяющем Центре МТС-Банк нажмите кнопку: [Вход для регистрации Клиентов банка](#)

Адрес электронной почты Удостоверяющего Центра: ca@mtsbank.ru

Контактный телефон: (495) 921-28-00, доб. 33-30, 33-39

В открывшейся странице необходимо вести логин и пароль, который Вы сохранили при регистрации.

Выполнить вход

[Вход по сертификату](#)

Основной вход для зарегистрированных пользователей, которые имеют закрытый ключ и действующий сертификат открытого ключа удаленного защищенного доступа. Используйте эту ссылку только после того, как процедура регистрации пользователя успешно проидена, а сертификат открытого ключа удаленного доступа получен и установлен.

[Вход по паролю временного доступа](#)

Продолжение процесса регистрации пользователя Удостоверяющего центра при наличии логина и пароля временного доступа.

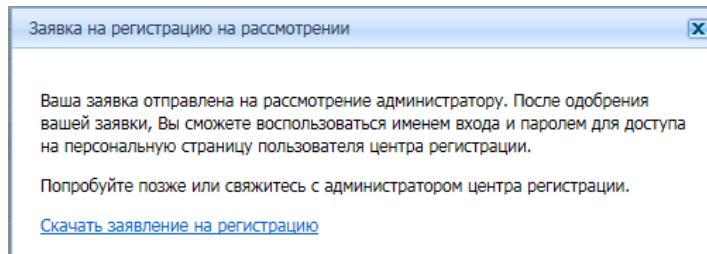
Сведения учетной записи

Логин:	ivanovii.2017
Пароль:	*****
<input type="button" value="Выполнить вход"/>	

[Регистрация](#)

Начало регистрации пользователя Удостоверяющего центра. Начинайте регистрацию только после того, как необходимое программное обеспечение будет установлено на компьютер.

Если запрос до сих пор находится в стадии обработки, то вы увидите следующее сообщение:



Если в течение 24 часов запрос остается не обработанным, следует направить соответствующий вопрос администратору ЦР по электронной почте ca@mtsbank.ru. После завершения обработки запроса на регистрацию, экранная форма отображения статуса запроса принимает следующий вид:

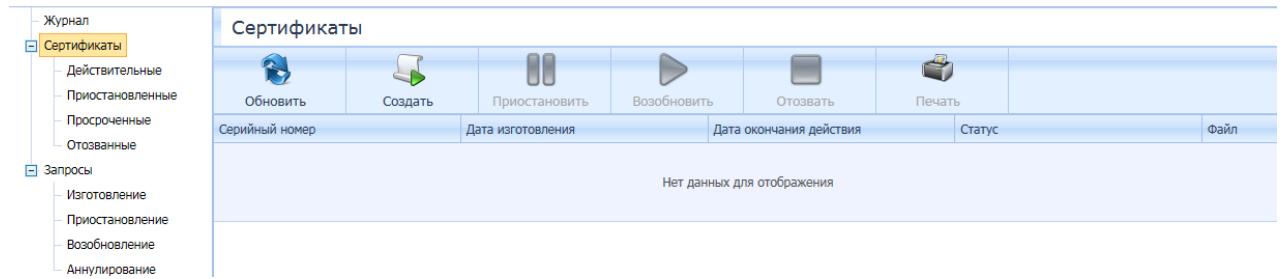
Сертификаты

Серийный номер	Дата изготовления	Дата окончания действия	Статус	Файл
Нет данных для отображения				

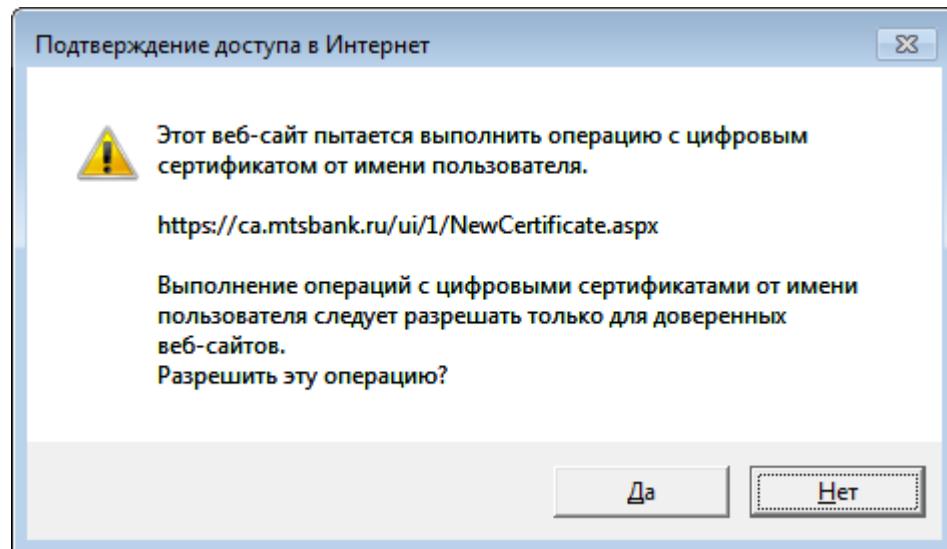
8. Формирование ключей и установка сертификата проверки открытого ключа

8.1. Создание запроса на сертификат

В случае успешного завершения обработки запроса на регистрацию выберите в левом контекстном меню «Сертификаты». В появившейся странице выберите «Создать»



Перед формированием запроса у Вас может появится предупреждающее окно с информацией – нажмите кнопку «Да».



Выбрав требуемый шаблон сертификата, в соответствии с предполагаемой областью действия сертификата открытого ключа и данными отправленного в УЦ Заявления на регистрацию пользователя. При этом чистый, заранее отформатированный носитель, на который будет произведена запись генерированных ключей, должен находиться в устройстве считывания.

При выборе шаблона сертификата все данные необходимо оставить без изменений.

Запрос на сертификат

Шаблон сертификата

Клиент системы защищенного электронного документооборота

Аванпост

Клиент системы защищенного электронного документооборота

Клиент системы Интернет-Трейдинг

Клиент системы Клиент-Банк

Подписи
 Шифрования

Размер ключа

Алгоритм хеширования

Срок действия сертификата

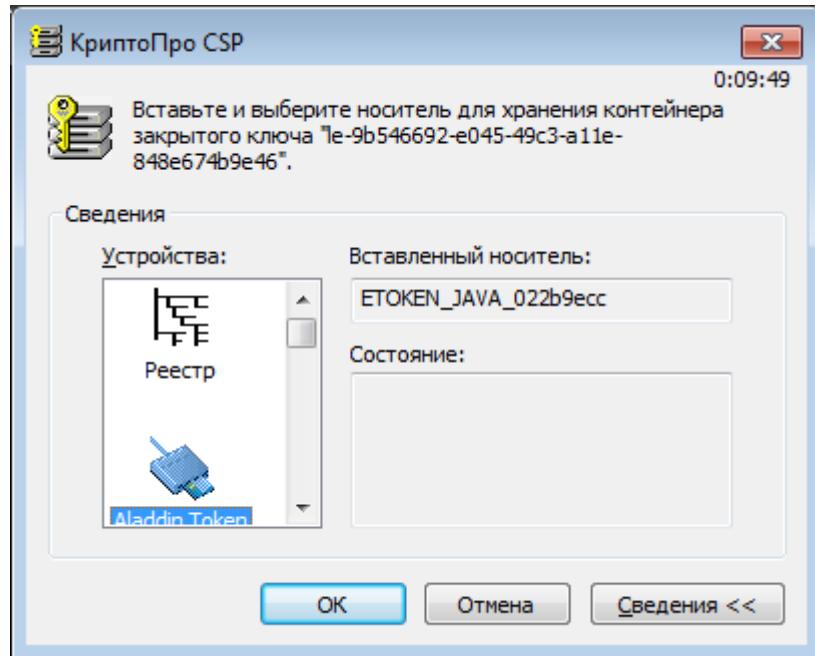
Срок действия ключа

Комментарий

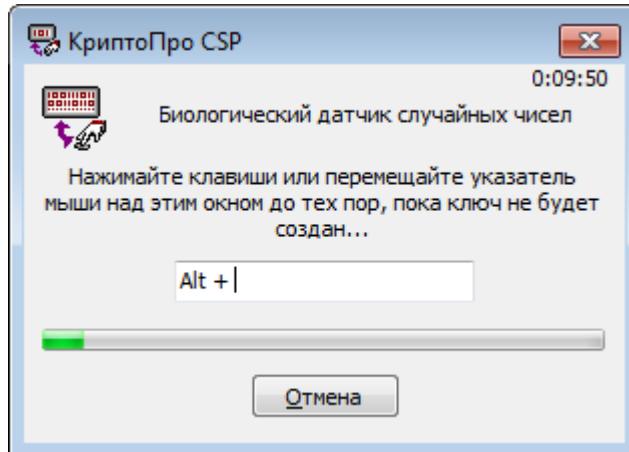
Создать

После выбора шаблона сертификата нажмите кнопку «Создать»

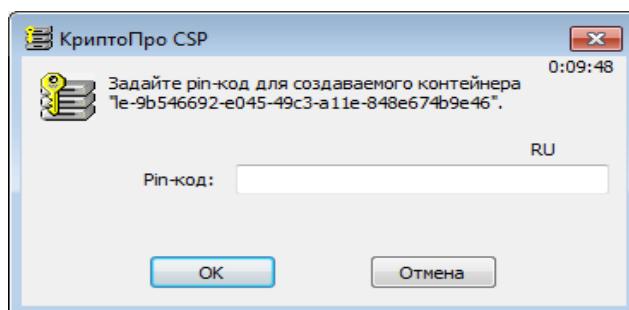
В случае если предварительная настройка программного обеспечения СКЗИ «КриптоПро CSP» была произведена на использование нескольких считывателей, генерация ключей будет сопровождаться выводом сообщения о выборе носителя:



Процесс генерации ключей производится с использованием биологического датчика случайных чисел



Для обеспечения дополнительной защиты закрытых ключей от несанкционированного доступа на контейнер хранения ключей необходимо установить пароль.



После завершения процесса генерации ключей происходит формирование запроса на сертификат и отправка запроса в Центр регистрации УЦ. Обработка запроса на выпуск сертификата пользователя Удостоверяющего Центра производится в автоматическом режиме.

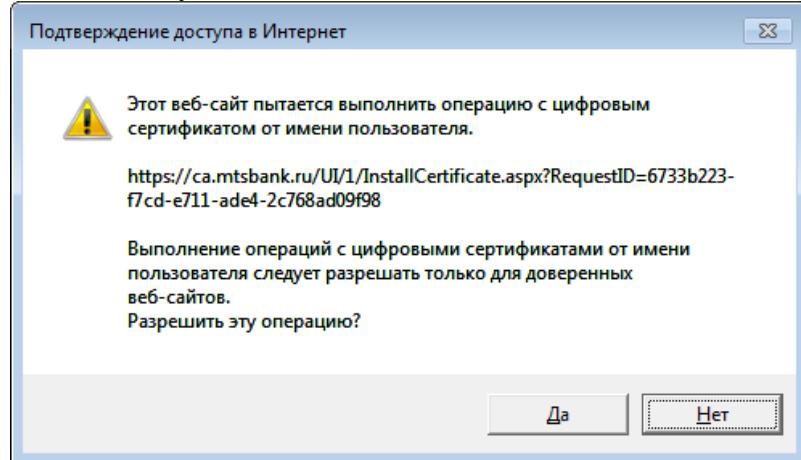
8.2. Получение и установка сертификата в контейнер секретного ключа.

После завершения процесса генерации контейнера секретного ключа и получения от УЦ сертификата Вы попадете на страницу зарегистрированного пользователя. Выберите в левом контекстном меню «Запросы» -«Изготовленные»

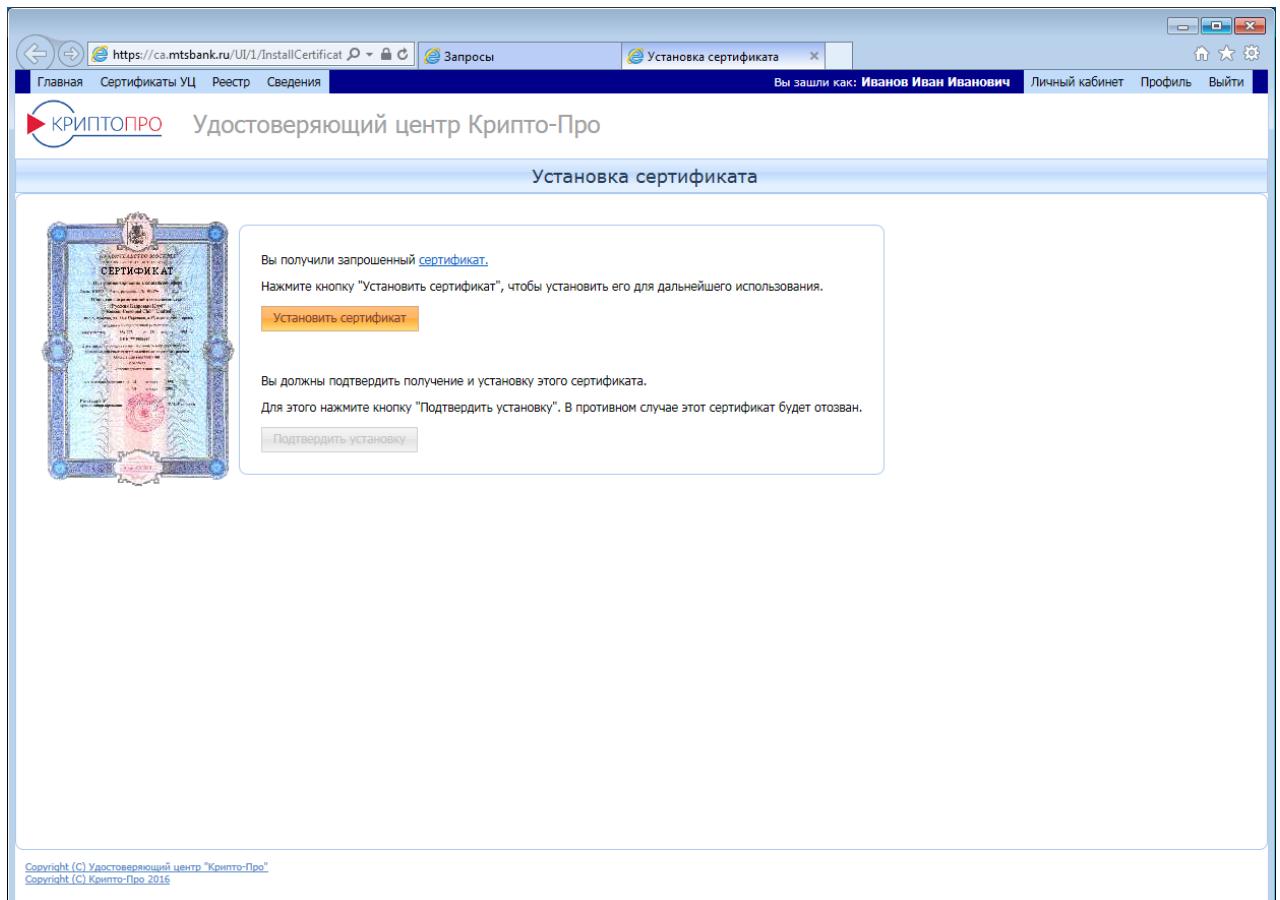
Дата создания	Статус	Дата одобрения	Сертификат	Установка	Комментарий менеджера
20.11.2017 16:31:41	Завершен	20.11.2017 16:31:41	06b09fd08a762c884e711fcdad9e9323	Установить	

В графе «Установка» нажмите «Установить».

Перед формированием запроса у Вас снова может появится предупреждающее окно с информацией – нажмите кнопку «Да».

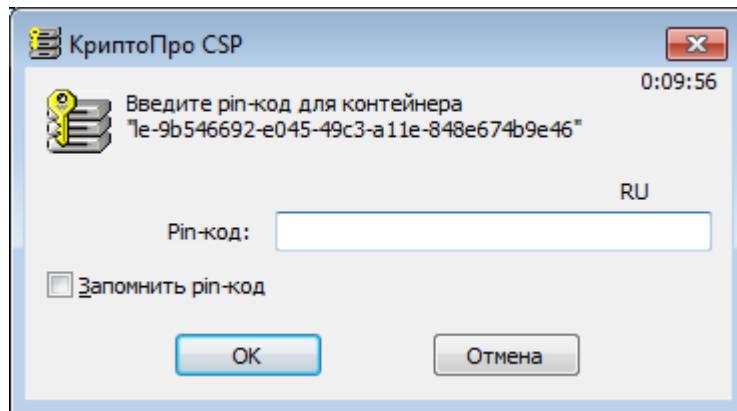


Нажмите кнопку «Установить сертификат».

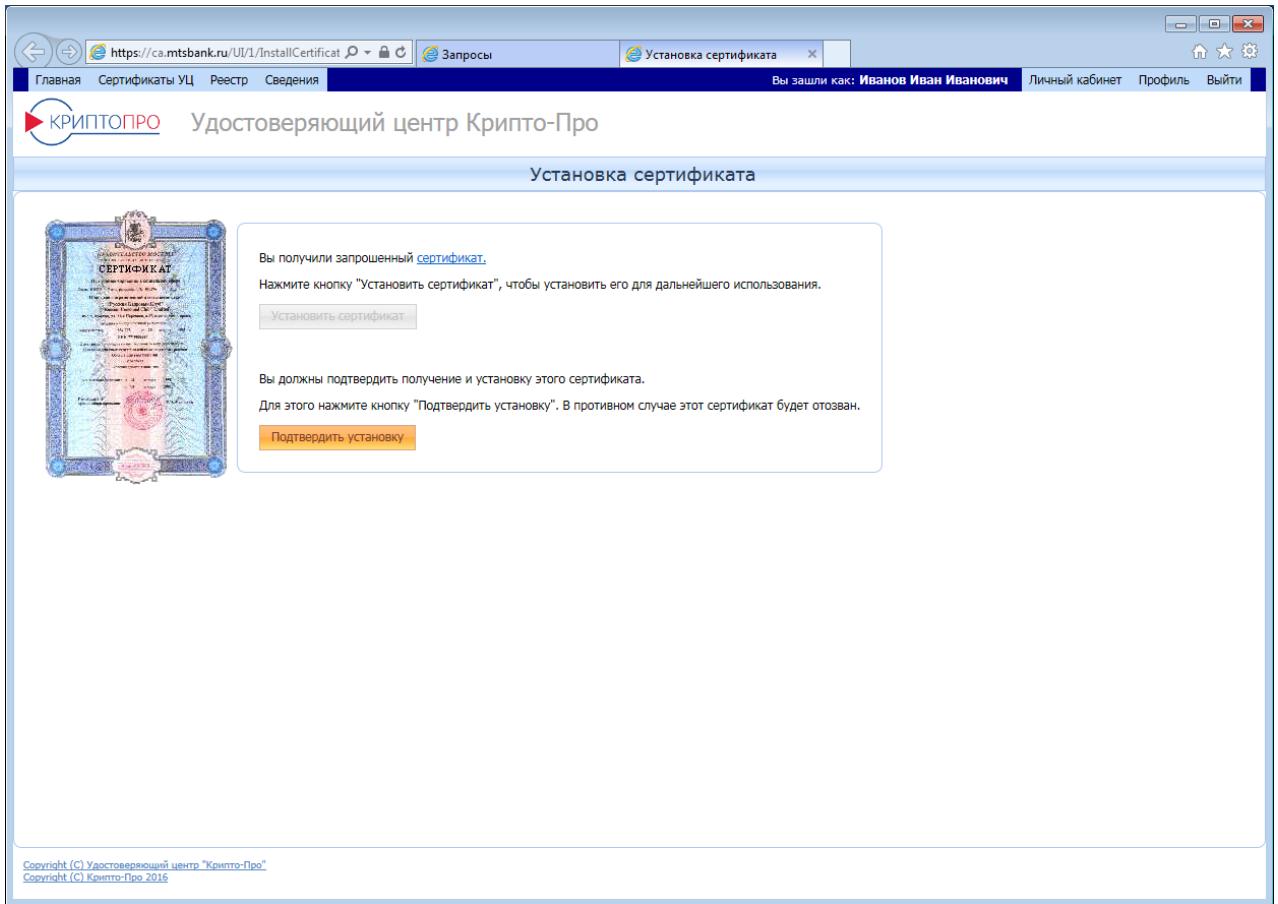


При нажатии кнопки «Установить сертификат», происходит установка выпущенного сертификата в раздел «**Личные**» хранилища сертификатов текущего пользователя и установка в контейнер секретного ключа на выбранном вами носителе.

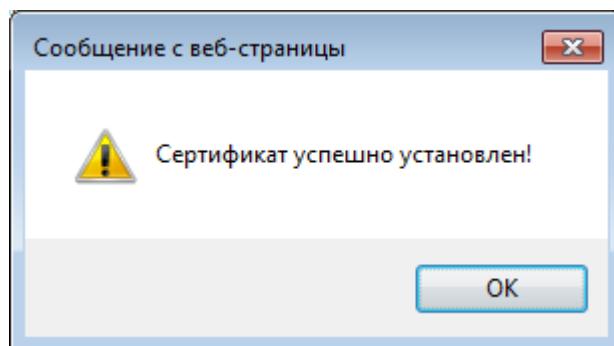
При установке Вас попросят ввести пин-код:



После установки сертификата, необходимо подтвердить его установку:



Появление следующего сообщения свидетельствует об успешной установке данного сертификата в хранилище:

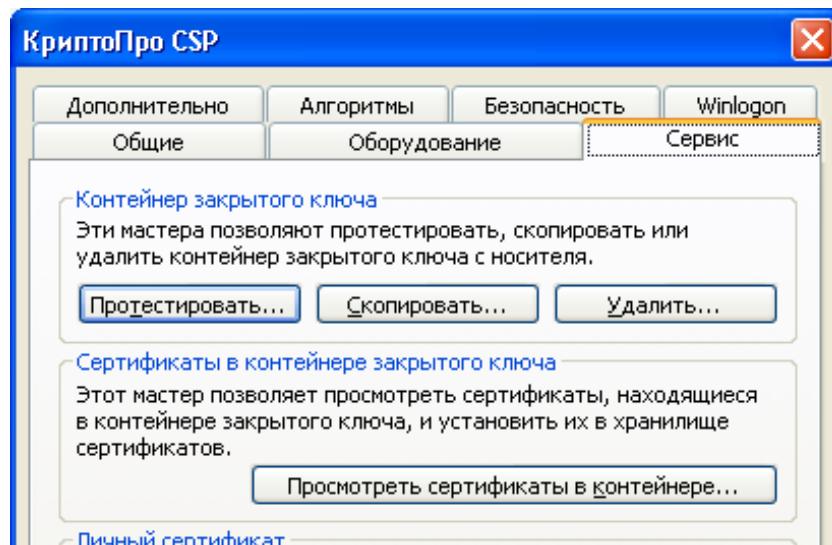


Пользователь может перейти в личный кабинет и распечатать бланк сертификата.

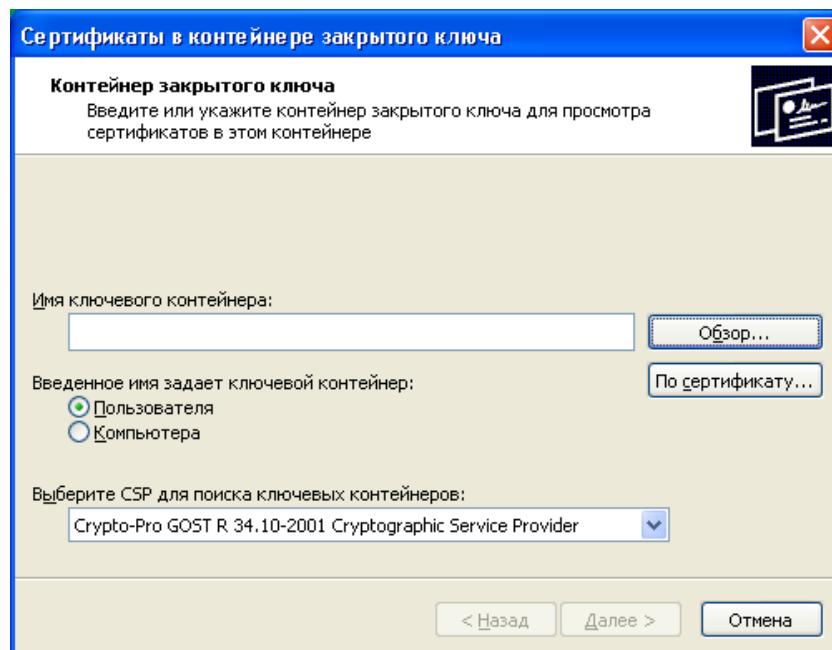
Вы зашли как: Иванов Иван Иванович Личный кабинет Профиль Выйти

Пользователям, использующим сертификат ключа подписи для работы в системе Интернет-дилинг в дополнение к вышеуказанным действиям и при условии успешной установки сертификата на используемом персональном компьютере ИТС QUIK, необходимо:

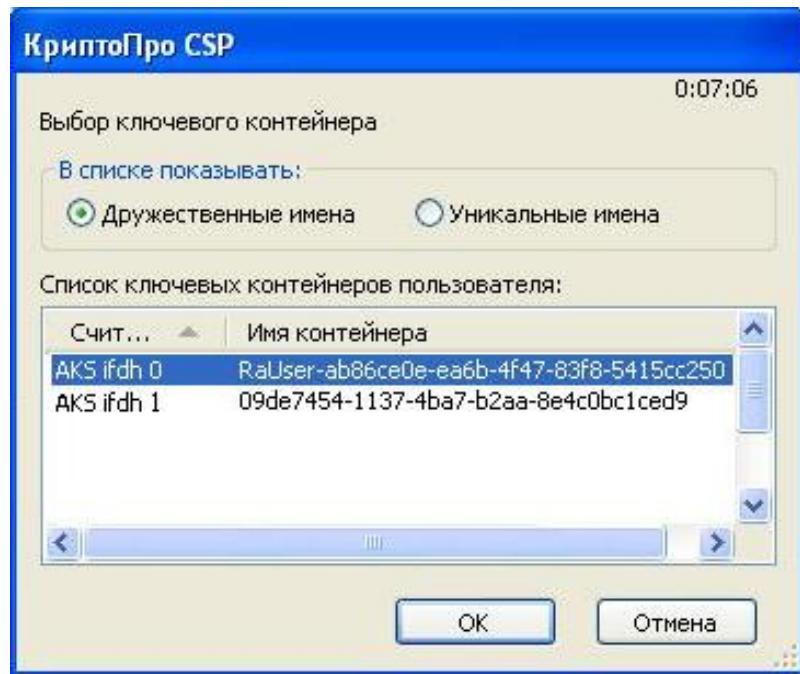
Открыть КриптоПро CSP, в ОС Windows: Пуск – Настройка - Панель управления - КриптоПро CSP и нажать кнопку «**Посмотреть сертификаты в контейнере...**».



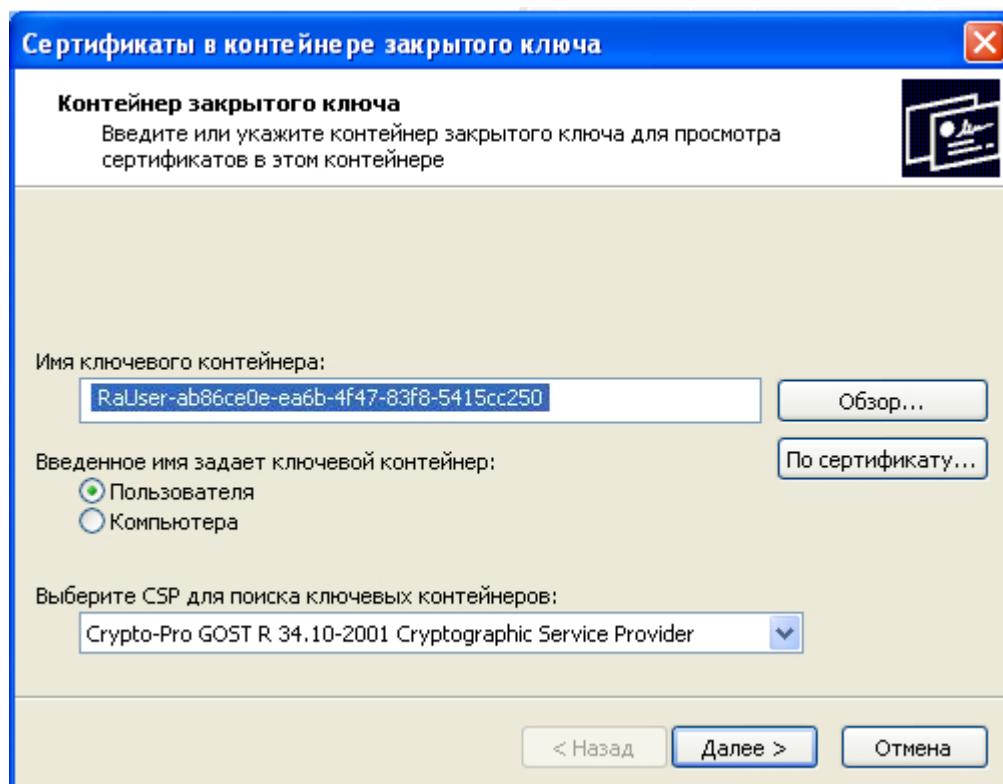
Установите расположение файла сертификата ключа подписи, нажав кнопку «**Обзор**».

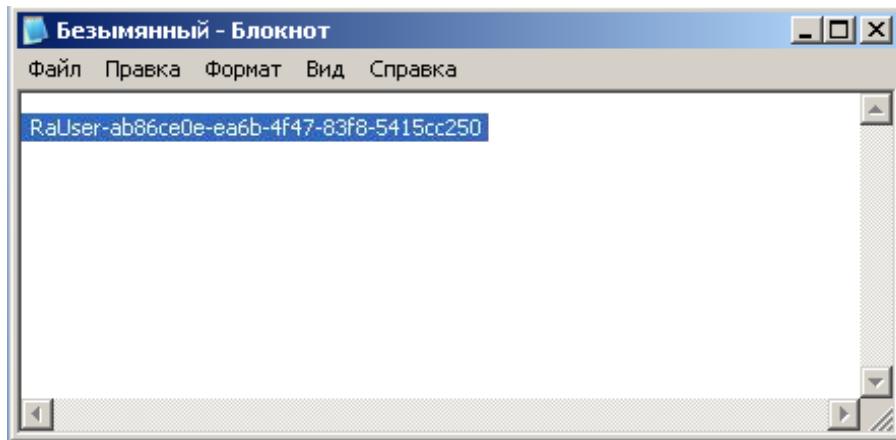


Выберите ключевой контейнер и нажмите кнопку «OK».

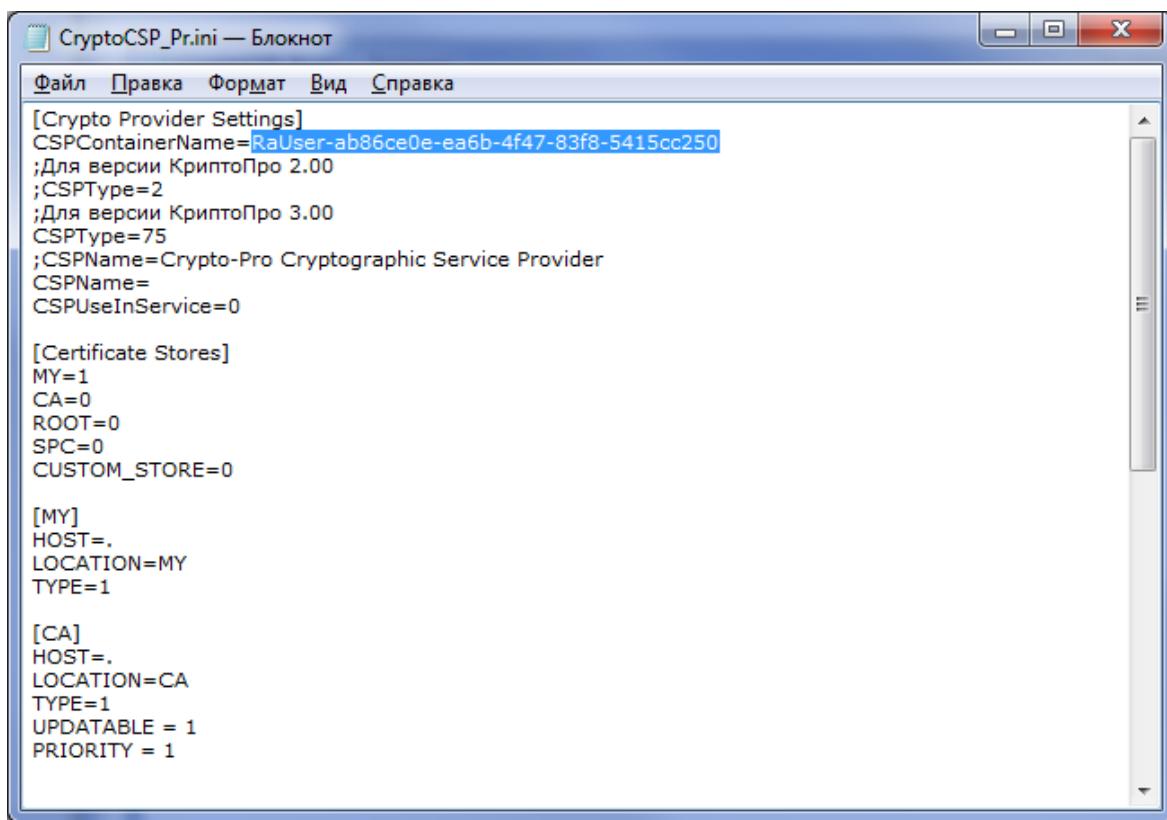


Выделите и скопируйте имя ключевого контейнера в программу «Блокнот», оно Вам понадобится позже.





Откройте файл **CryptoCSP_Pr.ini** в папке с ранее установленным ИТС QUIK и введите имя ключевого контейнера, скопировав его из программы «Блокнот», в строку **CSPContainerName**. В дальнейшем, сохраните и закройте файл **CryptoCSP_Pr.ini**.

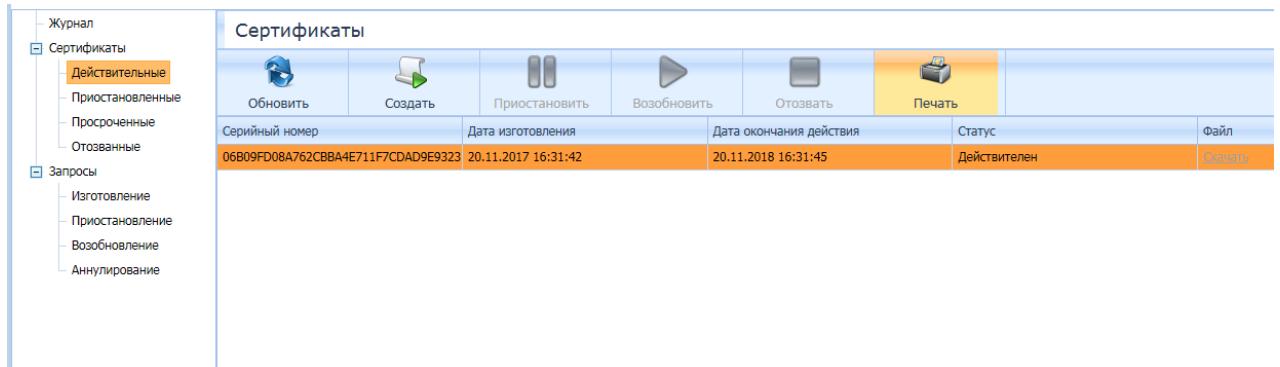


В результате сертификат закрытого ключа ЭП будет использоваться для подписания транзакций, сформированных посредством ИТС QUIK.

8.3. Печать бланка сертификата открытого ключа.

Формирование печатной формы сертификата, а так же вывод ее на бумажный носитель выполняется пользователем до начала использования сертификата ключа в работе.

Для печати сертификата необходимо выбрать в левом контекстном меню «сертификат», на странице выбрать действующий сертификат и нажать на иконку «Печать»:



В результате в новом окне обозревателя Microsoft Internet Explorer будет сформирована печатная форма сертификата открытого ключа пользователя.

Print the report

Удостоверяющий Центр ПАО МТС-Банк
Сертификат ключа проверки электронной подписи

Сведения о сертификате:

Версия: 3
Серийный номер: 06B09FD08A762CBBA4E711F7CDAD9E9323
Издатель сертификата: CN=MTS Bank Certification Authority, O=PJSC MTS Bank, L=Moscow, C=RU, E=ca@mtsbank.ru
Владелец сертификата: CN=Иванов Иван Иванович, O=АО "Серп и Молот", L=г. Москва, C=RU, E=test@test.ru

Срок действия:
Действителен с: 20.11.2017 16:21:45
Действителен по: 20.11.2018 16:31:45

Ключ проверки электронной подписи:
Алгоритм: ГОСТ Р 34.10-2001 (1.2.643.2.2.19)
Параметры: 30 12 06 07 2A 85 03 02 02 24 00 06 07 2A 85 03 02 02 1E 01
Значение: 0440 09BA 0187 5BEF A247 4F0C C2A9 4BE5 9369 820E 4EB5 8D16 DD74 0CC2 02FD BFA8 EC9A B187 63FC FDC0 3D83 A1C5 192B F81A F3DB 3ACF 68BF 1689 B461 068A A536 94FB 489D

Расширение сертификата X.509

Расширение: Key Usage (критичное)
Идентификатор: 2.5.29.15
Значение: Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment (f0)

Расширение: Subject Key Identifier
Идентификатор: 2.5.29.14
Значение: 1d 38 94 cd d1 89 aa d4 5a 13 07 b0 fe 54 c5 c3 22 36 12 9e

Расширение: Authority Key Identifier
Идентификатор: 2.5.29.35
Значение: KeyID=57 79 23 27 e0 97 50 9d 7a c3 e8 87 49 5c b9 bb bb a7 2d, Certificate Issuer: Directory Address:CN=MTS Bank Certification Authority, O=PJSC MTS Bank, L=Moscow, C=RU, E=ca@mtsbank.ru, Certificate SerialNumber=4e c9 3c f0 63 37 61 9f 4b c0 c1 4e 5f d6 ba 1f

Расширение: Enhanced Key Usage
Идентификатор: 2.5.29.37
Значение: Client Authentication (1.3.6.1.5.5.7.3.2), Secure Email (1.3.6.1.5.5.7.3.4), Document Signing (1.3.6.1.4.1.311.10.3.12), Unknown Key Usage (1.2.643.4.16.4.2)

Расширение: Период использования ключа электронной подписи
Идентификатор: 2.5.29.16

Подписанные владельцем бланки сертификатов в количестве 2-х экземпляров следует передать в Удостоверяющий центр Банка. После получения Удостоверяющим центром бланков сертификата открытого ключа 1 экземпляр бланка сертификата, подписанный Уполномоченным лицом Удостоверяющего Центра и заверенный печатью Банка, будет возвращен пользователю.

В региональных филиалах Банка бланки сертификатов заверяются уполномоченным лицом (к примеру, Управляющим или его заместителем), назначенным Приказом Председателя Правления Банка заверять сертификаты ключей электронной цифровой подписи.

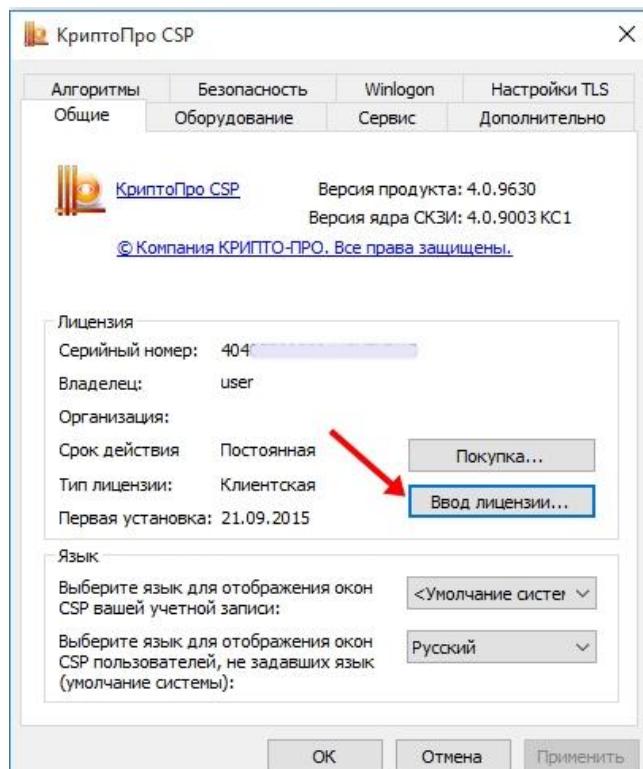
8.4. Ввод данных лицензии на программное обеспечение СКЗИ «КриптоПро CSP».

По условиям лицензионного соглашения срок использования демонстрационной версии КриптоПро CSP ограничен 90 днями с момента установки. Важное уточнение, демонстрационный период предоставляется лишь при первой установке программы на компьютере, при повторных установках получить его невозможно.

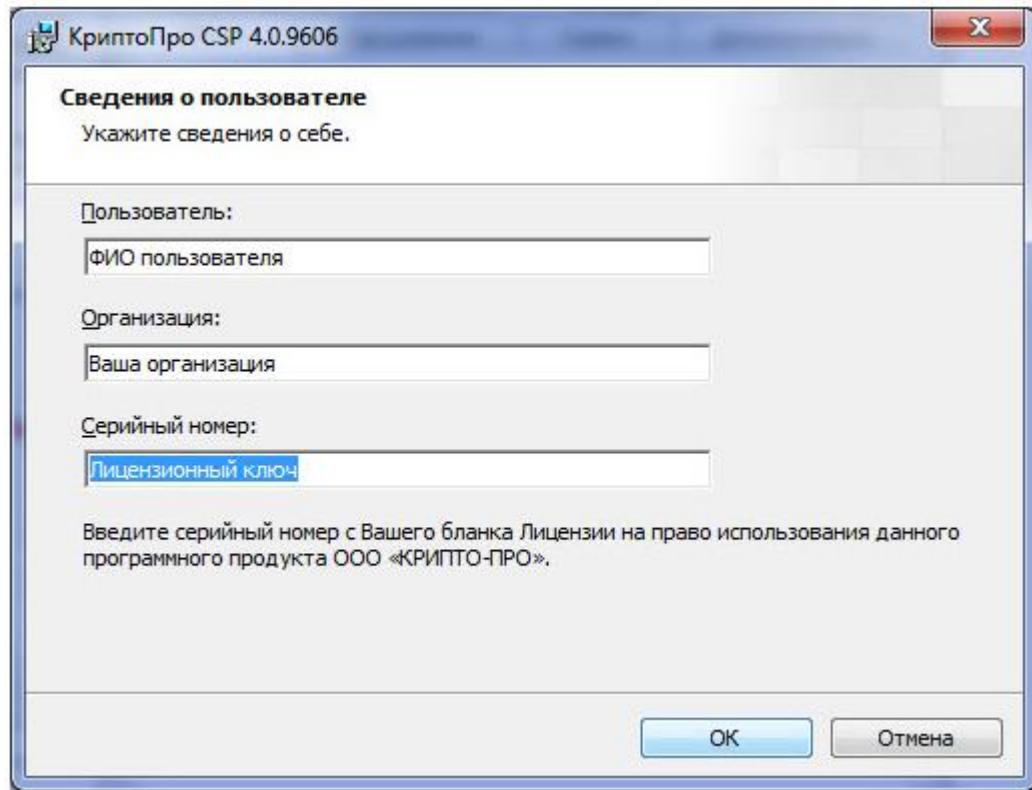
Чтобы посмотреть информацию о типе лицензии и сроке действия, откройте приложение КриптоПро CSP.

*В Windows 10 удобно воспользоваться поиском приложений (значок "Лупа" справа от кнопки "Пуск"), наберите "криптопро" и выберите КриптоПро CSP.

Во вкладке "Общие" КриптоПро CSP обратите внимание блок "Лицензия". В левой ее части указываются серийный номер (не полностью), имя владельца лицензии, название организации, срок действия, тип лицензии (клиентская либо серверная) и дата первой установки. В правой части можно запустить процесс онлайн покупки и ввести серийный номер лицензии.



Если указанная в графе срок действия дата не истекла, Вы можете пользоваться программой. В другом случае, нужно приобрести лицензию на программу. Для ввода ключа (серийного номера) нажмите на кнопку "Ввод лицензии".



Это все, что необходимо сделать для установки лицензии.

9. Защита информации в электронной почте.

Для Клиентов «Системы защищенного электронного документооборота» для настройки обмена зашифрованной электронной почтой с использованием электронной цифровой подписи рекомендуется воспользоваться информационным документом разработчика средств криптографической защиты информации ООО Крипто-Про, он доступен на сайте Удостоверяющего центра Банка в разделе «Документация» <http://ca.mtsbank.ru/docs/smime.pdf>

10. Плановая смена сертификата ключа пользователя

Срок действия сертификата ключа подписи 1 год.

Важно! Перед плановой сменой своего личного сертификата не забудьте установить НОВЫЙ корневой сертификат Удостоверяющего центра (5 раздел данной инструкции).

Для продолжения возможности использования защищенной почты необходимо провести плановую смену сертификата ключа. Для этого зайдите на страницу зарегистрированного пользователя web-сервера центра регистрации УЦ <https://ca.mtsbank.ru> по ссылке «Вход для зарегистрированных пользователей» (необходимым условием является вставленный ключевой носитель с Вашим действующим на данный момент сертификатом).

Выполнить вход

[Вход по сертификату](#)

Основной вход для зарегистрированных пользователей, которые имеют закрытый ключ и действующий сертификат открытого ключа удаленного защищенного доступа. Используйте эту ссылку только после того, как процедура регистрации пользователя успешно пройдена, а сертификат открытого ключа удаленного доступа получен и установлен.

[Вход по паролю временного доступа](#)

Продолжение процесса регистрации пользователя Удостоверяющего центра при наличии логина и пароля временного доступа.

Выберите действующий сертификат. Введите пин-код. Вы попали в личный кабинет.

Для получения нового сертификата необходимо повторить все действия из пункта 8.1 и 8.2

Серийный номер	Дата изготовления	Дата окончания действия	Статус	Файл
Нет данных для отображения				

Установите новый полученный сертификат, подтвердите установку, распечатайте и подпишите бланки сертификатов до начала использования их в работе.

Важно! После смены сертификата необходимо заменить старый сертификат на новый в настройках защиты электронной почты Microsoft Outlook, нажав «Выбрать», выберите полученный сертификат для «Сертификата подписи» и «Сертификата шифрования».