АО «Мидзухо Банк (Москва)»

Руководство по настройке рабочего места клиента системы ДБО

Руководство пользователя

Москва

Оглавление

***Техническая поддержка системы ДБО**: +7 (495) 212-03-40, +7 (495) 741-45-79; support@mhcb.ru*

Общие сведения

Данная инструкция описывает процесс установки и первоначальной настройки рабочего места клиента системы дистанционного банковского обслуживания (далее по тексту СДБО) АО «Мидзухо Банк (Москва)» (далее по тексту Банк) на платформе Windows.

Целевая аудитория – пользователи системы ДБО, а также технические специалисты, обслуживающие программно-аппаратные средства, обеспечивающие доступ к СДБО Банка.

Взаимодействие с СДБО осуществляется с использованием поддерживаемых веб браузеров Microsoft Internet Explorer 11, Google Chrome или Mozilla Firefox. Все данные клиентской части системы при этом хранятся на сервере СДБО Банка.

Для обеспечения защиты информации в СДБО используются сертифицированные системы криптографической защиты информации:

1. (СКЗИ) «RuToken ЭЦП 2.0». Дополнительная информация по СКЗИ «RuToken ЭЦП 2.0» а также техническая документация доступна на сайте разработчика https://www.rutoken.ru/
2. (СКЗИ) «Message-Pro». Дополнительная информация по СКЗИ «Message-Pro» а также техническая документация доступна на сайте разработчика http://www.signal-com.ru/

Технические требования

Ниже указаны минимальные требования к конфигурации персонального компьютера, используемого для работы с системой ДБО:

Конфигурация аппаратных средств:

- компьютер IBM PC или 100% совместимый с ним
- тактовая частота процессора 600 МГц и выше
- ОЗУ 128 Мбайт и выше
- Видеоадаптер не ниже SVGA (800*600, 256 цветов)
- Не менее 100 Мбайт свободного пространства на жёстком диске
- Свободный USB-порт

Системное программное обеспечение:

- Операционная система Microsoft Windows 10, Windows 11 **Внимание! Поддерживаются только русская и английская версии операционных систем!**
- Веб-браузер Microsoft Internet Explorer 11, Google Chrome, Mozilla Firefox

Требования к коммуникациям:

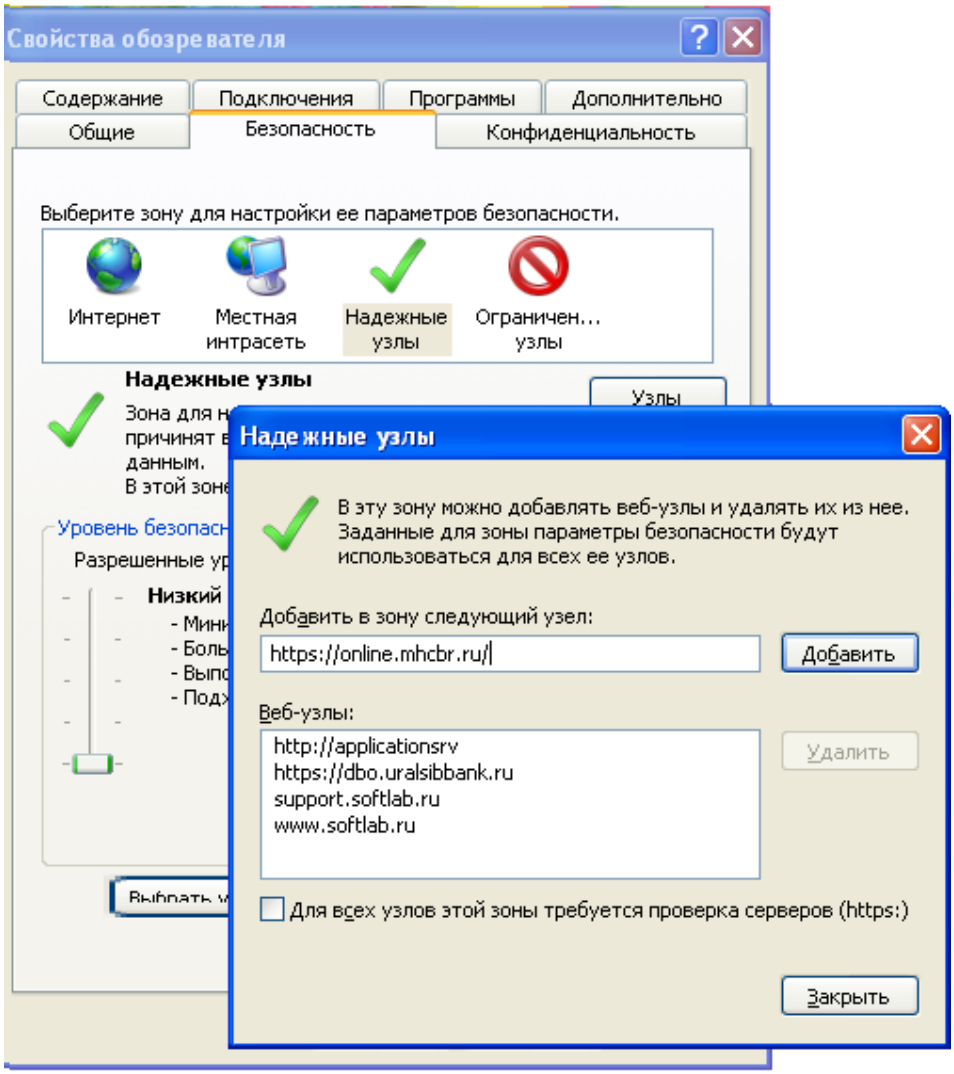
- наличие доступа в сеть Internet.

Настройки безопасности браузеров

Перед подключением к системе ДБО необходимо предварительно настроить параметры безопасности браузеров.

Настройка безопасности:

- Откройте Свойства обозревателя (через Панель управления Windows).
- Перейдите к вкладке **Безопасность.**
- Выберите зону **«Надежные сайты».**
- Добавьте адрес сайта **https://online.mhcbr.ru/** в зону **Надежные сайты**;
- Установите уровень безопасности для зоны **Надежные сайты** – **Низкий;**



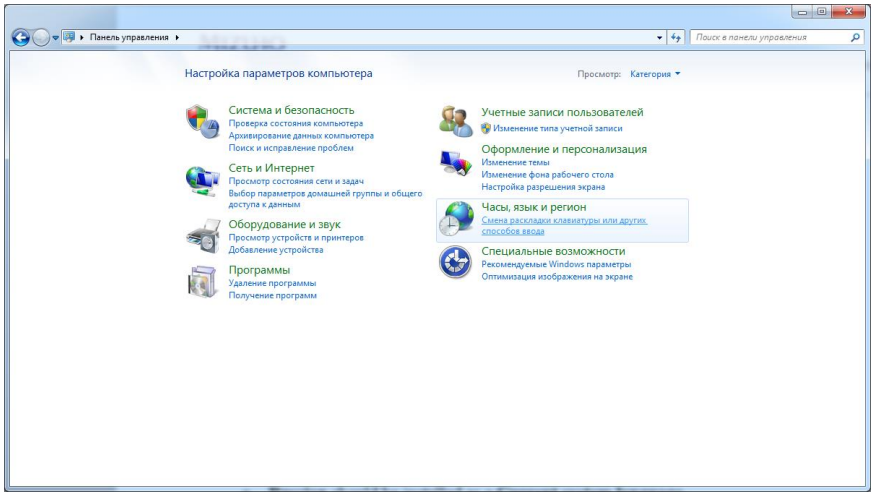
- Закройте окно
- Нажмите последовательно кнопку **Применить**, затем кнопку **ОК** для сохранения сделанных изменений.

Техническая поддержка системы ДБО: +7 (495) 212-03-40, +7 (495) 741-45-79; support@mhcb.ru

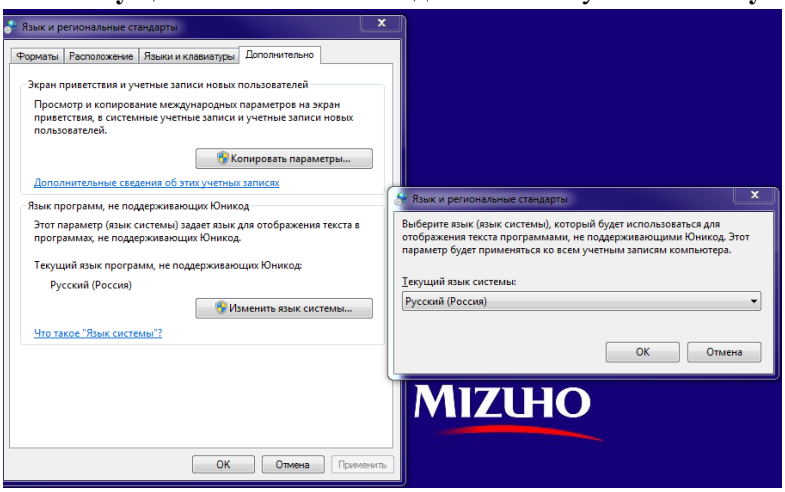
Настройки ОС Windows

Выбор языка программ, не поддерживающих Юникод (при изменении требуется перезагрузка):

- Откройте панель управления Windows (Control Panel)
- Выберите пункт **Смена раскладки клавиатуры или других способов ввода** в группе **Часы, язык и регион**



- Перейдите на вкладку **Дополнительно**
- В области **Язык программ, не поддерживающих Юникод** нажмите **Изменить язык системы**
- В качестве **Текущего языка системы** должен быть установлен **Русский.**



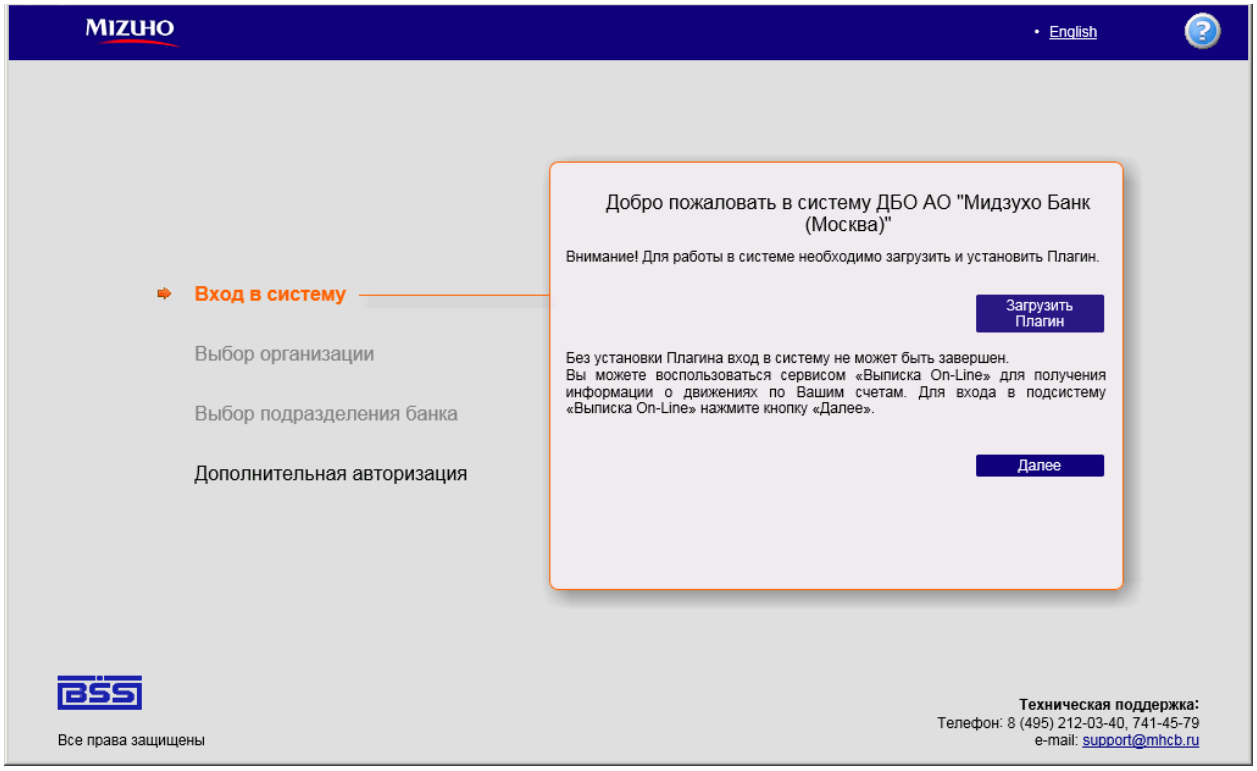
- Нажмите **Ок – Применить – Ок** для сохранения настройки**.**

Техническая поддержка системы ДБО: +7 (495) 212-03-40, +7 (495) 741-45-79; support@mhcb.ru

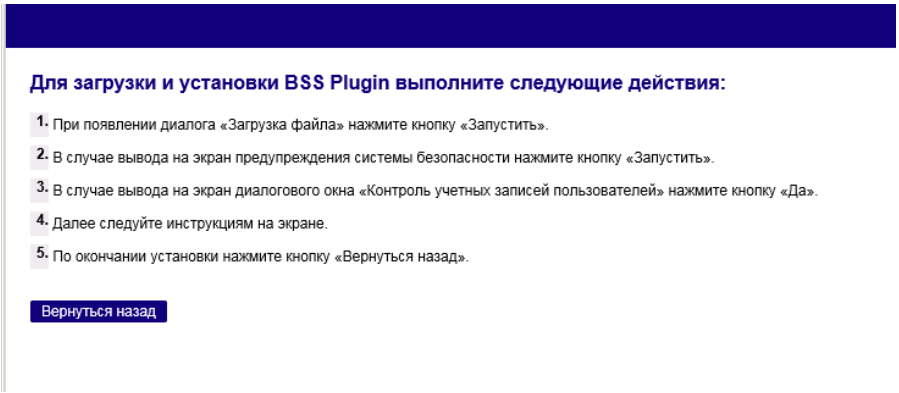
Установка / обновление компонентов Интернет-Клиента

Для подключения к системе ДБО необходимо выполнить следующие действия:

1. Откройте поддерживаемый браузер и перейдите по адресу https://online.mhcbr.ru
2. Нажмите кнопку «Загрузить Плагин»



3. Следуйте инструкции из открывшегося окна



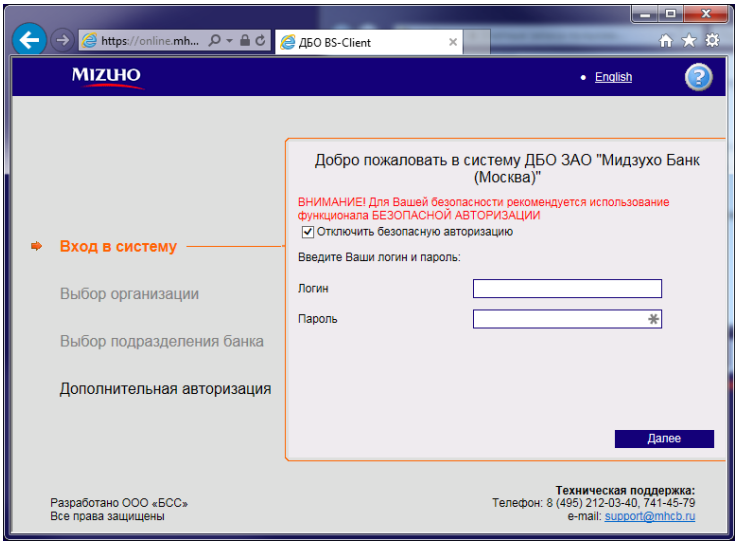
4. Дождитесь окончания установки плагина.

Первоначальный вход в систему / Первичная генерация ключа

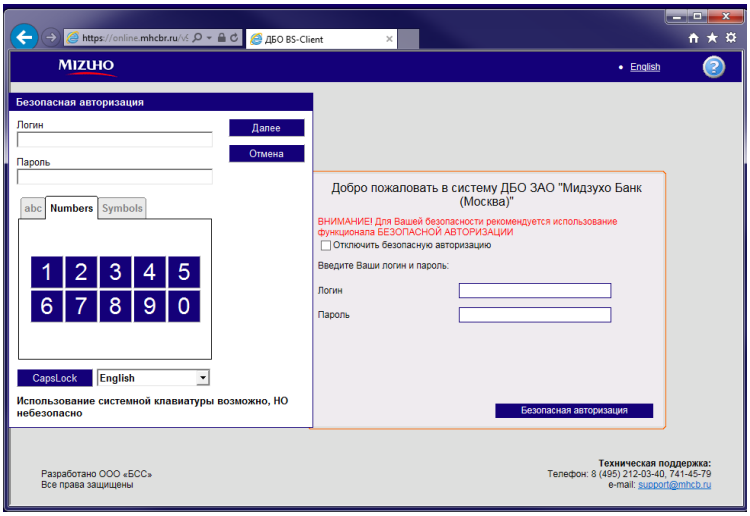
1. Перед подключением к СДБО установите полученный в банке электронный ключ **RuToken ЭЦП 2.0** в USB порт компьютера

Если это первоначальное подключение, необходимо дождаться пока ОС Windows установит драйвер ключа. В случае проблем с установкой драйвера необходимо обратиться в службу технической поддержки

2. Откройте поддерживаемый браузер и перейдите по ссылке **https://online.mhcbr.ru/**
3. В появившемся окне входа в систему:

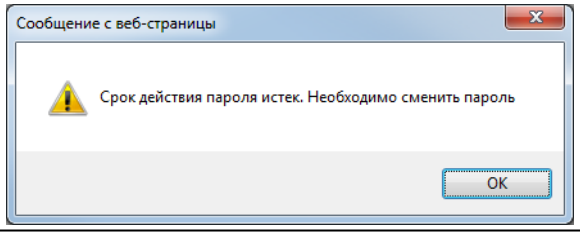


Вариант 1: щелкните по полю ***Отключить безопасную авторизацию,*** **(не рекомендуется)** затем введите логин и пароль (идентификатор доступа к системе ДБО, полученный в Банке) и нажмите ***Далее***



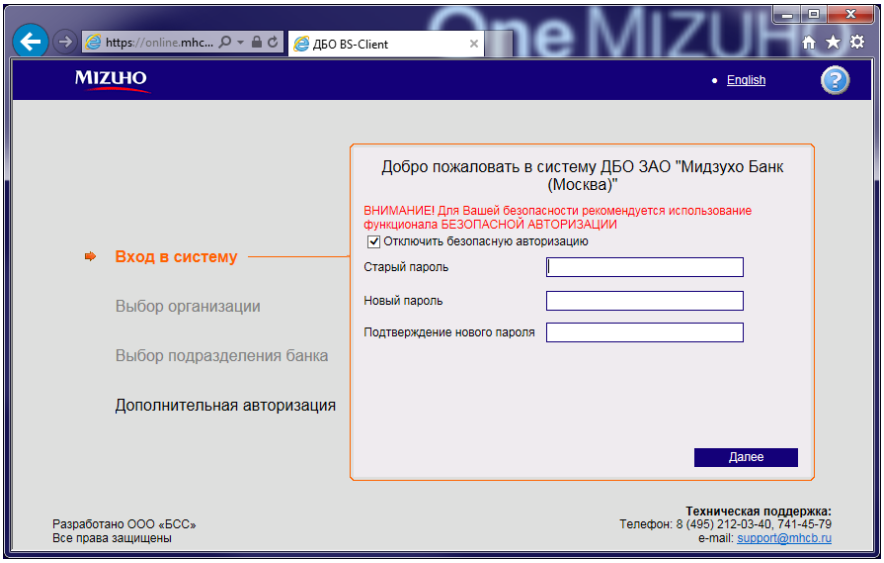
Вариант 2: нажмите ***Безопасная авторизация*** и в открывшемся окне при помощи появившейся экранной клавиатуры введите с использованием указателя «мышки» логин и пароль (идентификатор доступа к системе ДБО, полученный в Банке) и нажмите ***Далее***

4. В случае первого входа в систему откроется окно смены пароля - нажмите ***ОК***:

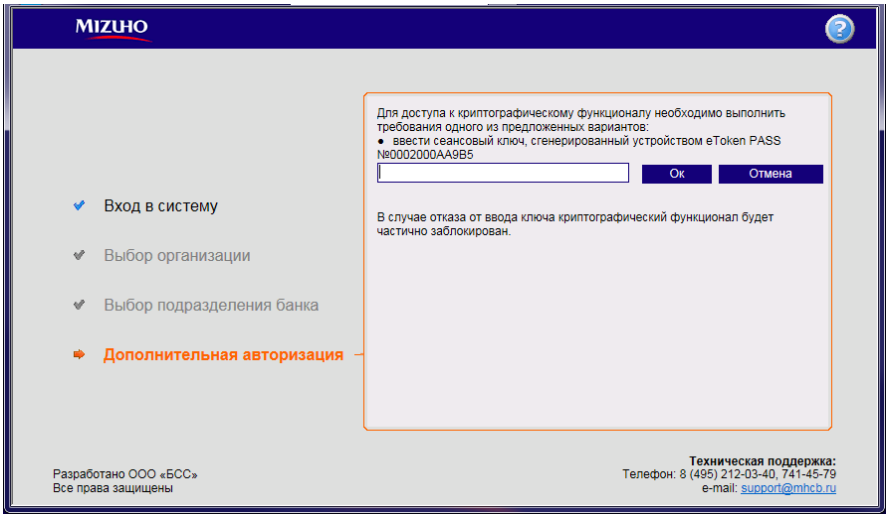


Техническая поддержка системы ДБО: +7 (495) 212-03-40, +7 (495) 741-45-79; support@mhcb.ru

5. Используя **безопасную авторизацию** (рекомендуется) или отключив ее произведите смену пароля введя **Старый пароль, Новый пароль** и **Подтверждение нового пароля (**в качестве пароля могут использоваться буквы, цифры и спецсимволы, длина пароля от 8 до 10 знаков**):**



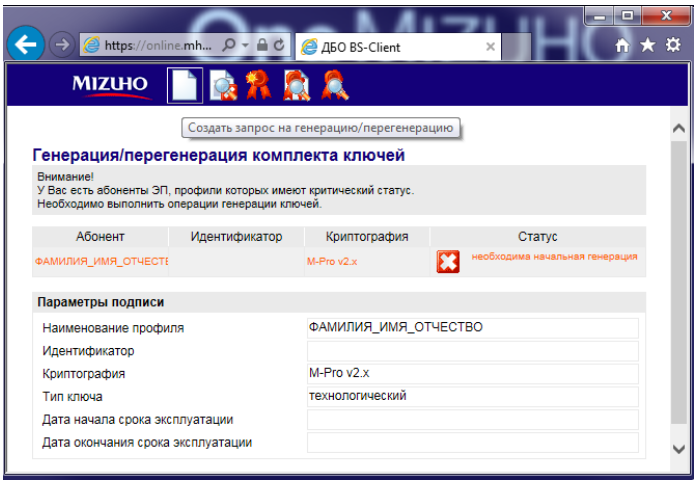
6. В случае использования автономного генератора одноразовых паролей eToken PASS появится окно дополнительной авторизации в котором необходимо нажав кнопку на устройстве eToken PASS ввести сгенерированный устройством сеансовый ключ:



eToken PASS

ВНИМАНИЕ! ДАННОЕ УСТРОЙСТВО ИСПОЛЬЗУЕТСЯ ТОЛЬКО ОДИН РАЗ ПРИ КАЖДОМ ВХОДЕ В СИСТЕМУ. **ПРИ МНОГОКРАТНОМ НЕЦЕЛЕВОМ НАЖАТИИ КНОПКИ УСТРОЙСТВО БУДЕТ ЗАБЛОКИРОВАНО!**

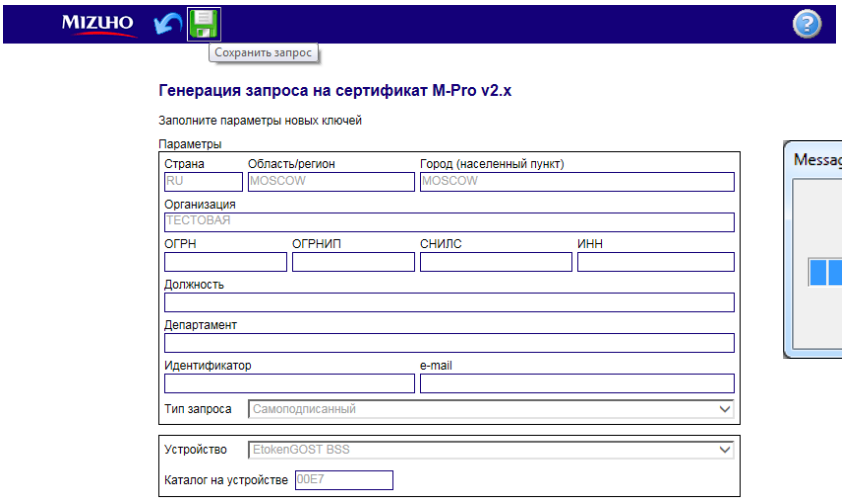
7. В случае, если необходима генерация или перегенерация комплекта ключей пользователя, в появившемся окне необходимо выделить абонента (1 раз щелкнув левой кнопкой мыши по фамилии абонента) затем нажать иконку ***Создать запрос на генерацию/перегенерацию.***

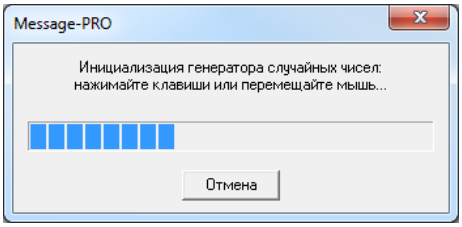


Внимание! На данном этапе к порту USB должен быть подключен полученный в банке **RuToken ЭЦП 2.0** или другой извлекаемый ключевой носитель.

RuToken ЭЦП 2.0

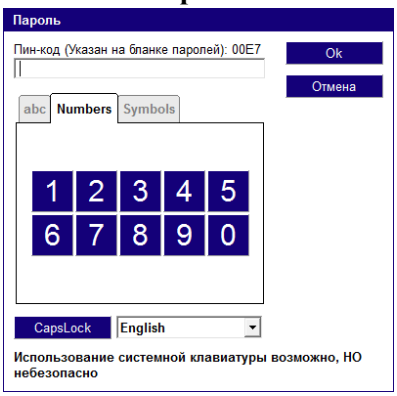
8. В случае первичной генерации в открывшемся окне нажмите иконку ***Сохранить запрос***





Если вы используете USB Flash Drive, в параметре **Устройство** замените букву диска **A** на букву диска подключенного USB Flash Drive.

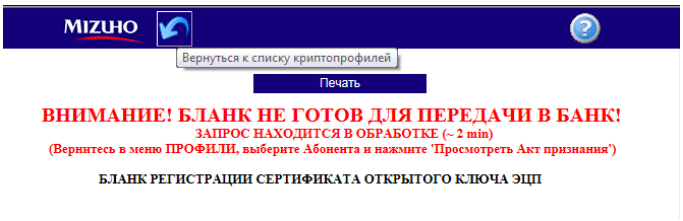
9. Введите пароль на **RuTiken ЭЦП 2.0**, полученный в банке - **ПИН-КОД ключа указанный на бланке паролей.**



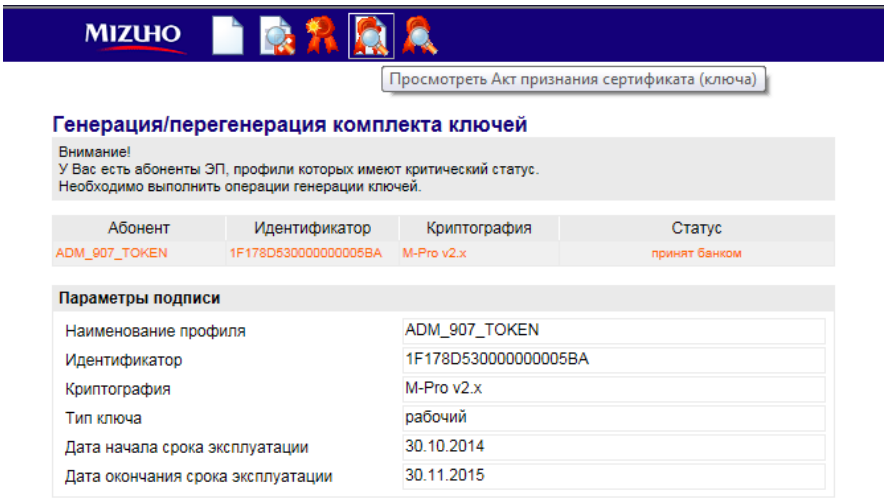
ВАЖНО! ПИН-КОД УКАЗАН НА БЛАНКЕ ПАРОЛЕЙ!
НА ДАННОМ ЭТАПЕ НЕ ИСПОЛЬЗУЙТЕ ГЕНЕРАТОР ОДНОРАЗОВЫХ ПАРОЛЕЙ - УСТРОЙСТВО e-token PASS!!!

Техническая поддержка системы ДБО: +7 (495) 212-03-40, +7 (495) 741-45-79; support@mhcb.ru

10. В процессе генерации на носителе будет создан закрытый ключ и в банк отправится запрос на регистрацию. На стороне клиента откроется бланк регистрации сертификата. Если вы видите красную надпись, то запрос еще не обработан. Нажмите иконку ***Вернуться к списку критопрофилей***



11. Необходимо подождать 2~3 минуты, затем выделить абонента (1 раз щелкнув левой кнопкой мыши по фамилии абонента) и нажать иконку ***Просмотреть Акт признания сертификата (ключа)***

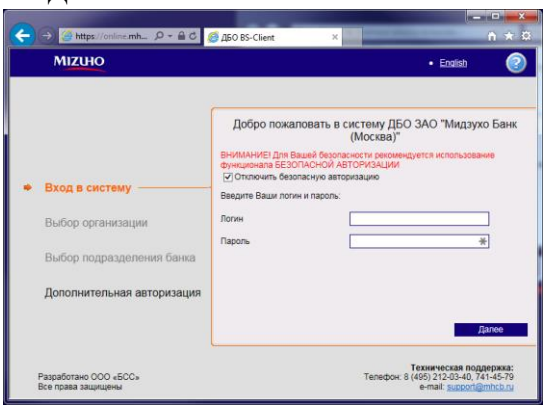


12. Открывшийся бланк (без красной надписи) необходимо распечатать в двух экземплярах. Каждый бланк подписывается владельцем ключа и руководителем организации, ставится печать. Бланки необходимо передать в банк.

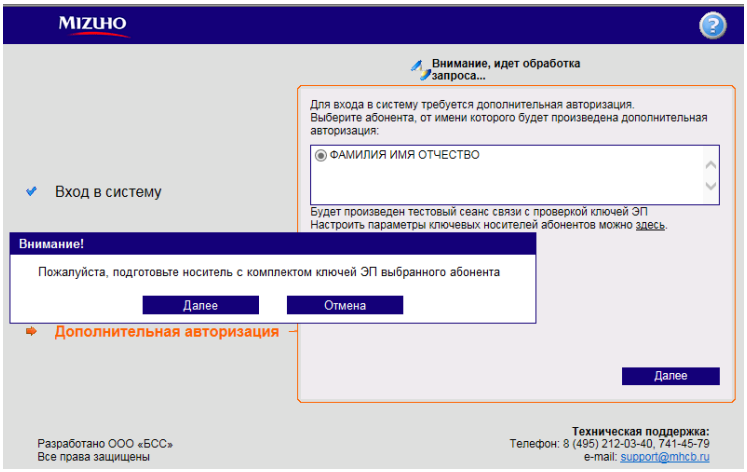
***Техническая поддержка системы ДБО**: +7 (495) 212-03-40, +7 (495) 741-45-79; support@mhcb.ru*

Вход в систему и завершение регистрации ключа подписи абонента

1. Администратор безопасности системы ДБО Банка, получив оригиналы регистрационных бланков сертификатов открытых ключей, завершает регистрацию нового ключа абонента.
2. Для завершения процедуры регистрации нового ключа абоненту необходимо зайти в систему ДБО:



Введите логин/пароль

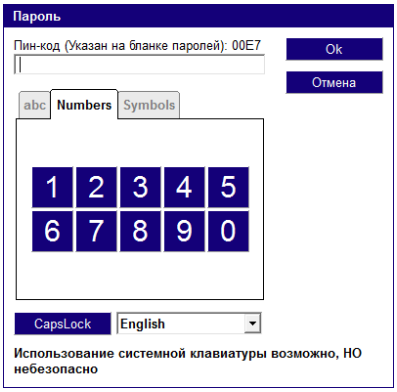


На странице дополнительной авторизации необходимо нажать ***Далее***

На данном этапе должен быть установлен полученный в банке **RuToken ЭЦП 2.0** или другой ключевой носитель.

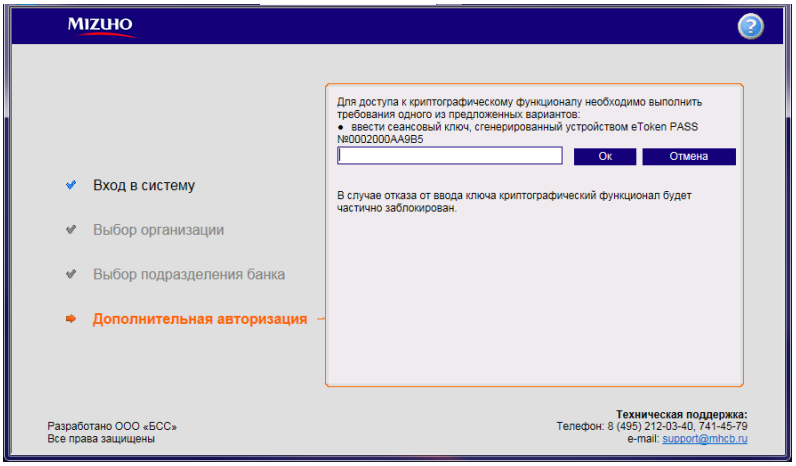
RuToken ЭЦП 2.0

3. Введите пароль на **RuToken ЭЦП 2.0**, полученный в банке - **ПИН-КОД ключа указанный на бланке паролей.**



ВАЖНО! ПИН-КОД УКАЗАН НА БЛАНКЕ ПАРОЛЕЙ!
НА ДАННОМ ЭТАПЕ НЕ ИСПОЛЬЗУЙТЕ !!! ГЕНЕРАТОР ОДНОРАЗОВЫХ ПАРОЛЕЙ - УСТРОЙСТВО e-token PASS

4. В случае использования автономного генератора одноразовых паролей eToken PASS необходимо нажав кнопку на устройстве ввести сеансовый ключ:



eToken PASS

ВНИМАНИЕ! ДАННОЕ УСТРОЙСТВО ИСПОЛЬЗУЕТСЯ ТОЛЬКО ОДИН РАЗ ПРИ КАЖДОМ ВХОДЕ В СИСТЕМУ. ПРИ МНОГОКРАТНОМ НЕЦЕЛЕВОМ НАЖАТИИ КНОПКИ УСТРОЙСТВО БУДЕТ ЗАБЛОКИРОВАНО!

5. Процедура перегенерации ключей на этом завершена, и вы можете приступать к работе в СДБО.

***Техническая поддержка системы ДБО**: +7 (495) 212-03-40, +7 (495) 741-45-79; support@mhcb.ru*