

Начало работы с системой

Данное руководство предназначено для пользователей системы Дистанционного Банковского Обслуживания, выполняющих генерацию запроса на получение Сертификата ключа подписи, необходимого для дальнейшей работы в системе. В настоящем документе будет описана процедура генерации запроса на получение сертификата и установки сопутствующего программного обеспечения на примере операционной системы Microsoft Windows 7 с обозревателем Internet Explorer 11 и электронных ключей семейства JaCarta ГОСТ от компании Аладдин-РД.

Также работа системы возможна в операционных системах Microsoft Windows 10, Mac OS X, Linux и в обозревателях Safari, Google Chrome и др.

Не гарантируется работа на одном ПК с другими интернет-банками.

Для установки плагина JC-WebClient необходимы права администратора.

1. Предварительная настройка

Откройте веб-сайт системы Дистанционного Банковского Обслуживания (далее - ДБО) в обозревателе Internet Explorer. Для этого:

- ✓ Откройте Internet Explorer, щелкнув значок Internet Explorer на панели задач или в меню Пуск.
- ✓ В строке адреса наберите <https://online.round.ru/> и нажмите кнопку «Перейти» (на рисунке ниже выделена красной рамкой)

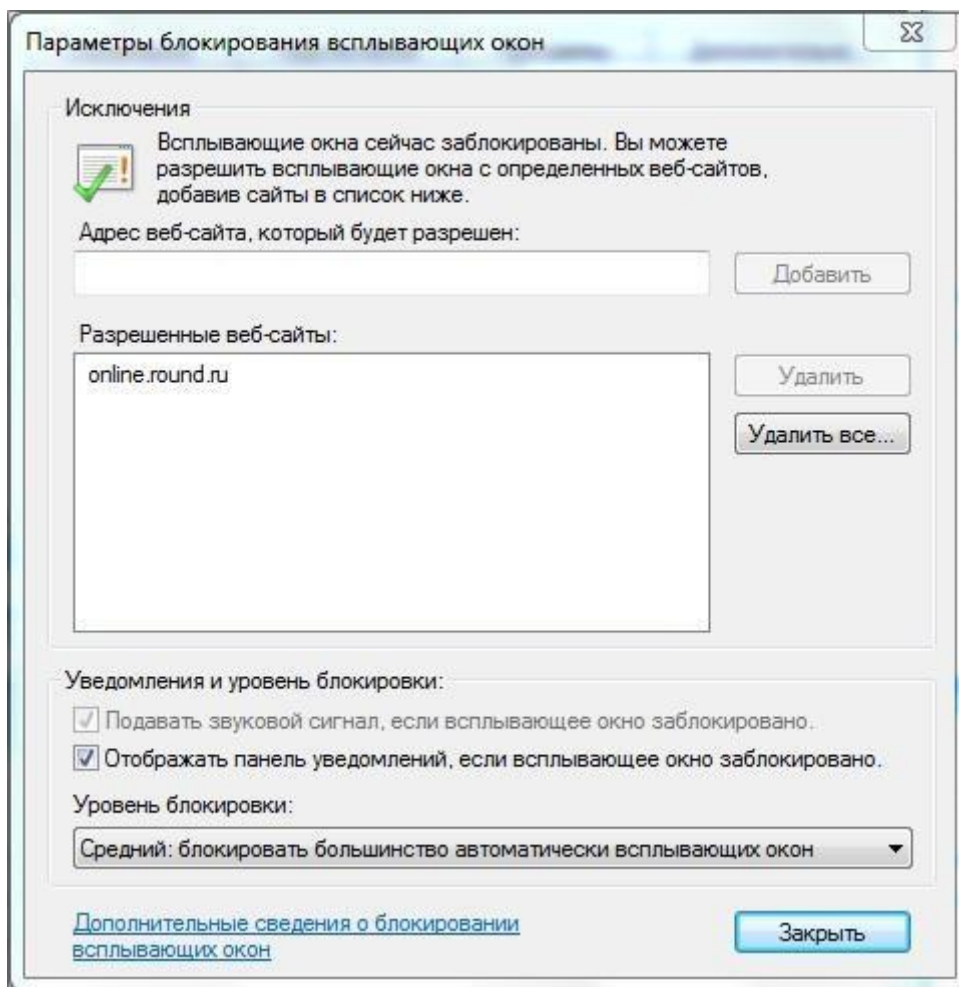


или щелкните мышью по ссылке выше.

Перед использованием необходимо выполнить настройки безопасности обозревателя.

1.1. Разрешение всплывающих окон.

- 1.1.1. Нажмите кнопку **Сервис**  и выберите **Свойства браузера**.
- 1.1.2. На вкладке **Конфиденциальность** в разделе "Блокирование всплывающих окон" нажмите кнопку **Параметры**.
- 1.1.3. В строке **Адрес веб-сайта, который будет разрешен** введите <https://online.round.ru/> и нажмите кнопку **Добавить**. Окно будет выглядеть так:



1.1.4. В окне **Параметры блокирования всплывающих окон** нажмите кнопку **Закреть**.

1.2. Добавление адреса системы ДБО в надежные узлы

- 1.2.1. Нажмите кнопку **Сервис** и выберите пункт **Свойства веб-обозревателя**.
- 1.2.2. Щелкните вкладку **Безопасность** и затем щелкните зону безопасности **Надежные узлы**.
- 1.2.3. Щелкните **Сайты**.
- 1.2.4. Веб-узел должен появиться в поле **Добавить в зону следующий узел**. Щелкните **Добавить**.
- 1.2.5. Нажмите кнопку **Закреть** и затем нажмите **ОК**.



2. Вход в систему

2.1. Откройте веб-сайт системы ДБО

2.2. Вскройте конверт с данными для входа, полученный в офисе Банка

Общий вид содержимого конверта представлен на рисунке:

Создано в системе ДБО Раунд. Банк ООО "банк Раунд".

Банк ООО "банк Раунд"

Система ДБО Раунд

Комплект со средствами авторизации

Номер конверта: XXXXXX

Для входа в ДБО Раунд используйте:

Адрес: <https://online.round.ru>

(Оформите адрес сайта на используемом языке: "рус" / "en")

Логин: clntXXXXXX

Пароль: XXXXXX

С уважением,

Отдел дистанционного обслуживания клиентов

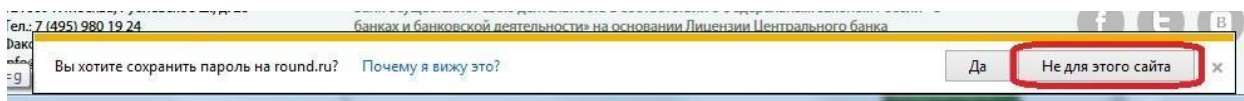
Банк ООО "банк Раунд"

2.3 Вставьте электронный ключ, полученный в офисе Банка, в USB-разъем вашего компьютера и дождитесь автоматической установки драйверов.

2.4 Введите логин и пароль с конверта на странице системы ДБО и нажмите **Войти**

The screenshot displays the login interface of the Round internet banking system. At the top, the Round logo is on the left, and navigation links 'Вход в интернет-банк' and 'Сайт банка' are in the center. On the right, the support service contact information 'Служба поддержки: +7 (495) 980 19 24' is shown. The main content area features a large background image of hands interacting with a document. Overlaid on this is a white circular login form titled 'ВХОД В ИНТЕРНЕТ-БАНК'. It contains two input fields: the first for the login 'clntXXXXXX' and the second for the password, represented by dots. Below the password field is a green 'ВОЙТИ' button. Underneath the button is a link for 'Рекомендации по безопасности'. At the bottom of the page, there is a 'Новости' section and a banner for 'Кредиты малому бизнесу'.

2.5. После успешного ввода учетных данных появится страница «Проверка входа». Если при этом у Вас появляется снизу сообщение о запоминании пароля, то настоятельно рекомендуется выбрать **Не для этого сайта**:



3. Генерация запроса сертификата

3.1. Щелкните мышью по кнопке **Получить сертификат**

ПРОВЕРКА ВХОДА

Вы зашли с устройства 392368cd. Данное устройство не является ДОВЕРЕННЫМ. Если вы хотите добавить его в список доверенных устройств, то подпишите простой электронной подписью "Заявление о добавлении устройства в список доверенных"

Для дополнительной аутентификации необходимо использовать Сертификат ключа подписи. Выберите личный сертификат.

Токен/смарт-карта

ПОЛУЧИТЬ СЕРТИФИКАТ **МОИ СЕРТИФИКАТЫ** **ПРОДОЛЖИТЬ** **ВЫХОД**

3.2. На странице заполнения данных для получения сертификата может появиться сообщение вида:

Плагин JC-WebClient не установлен

round 20.10.2017 13:24
интернет-банк

Фамилия Имя Отчество Тестовый клиент - Сокращенное наименование
20.10.2017 IP:
[Выход](#)

ПРОВЕРКА ВХОДА

Вы зашли с устройства 392368cd. Данное устройство не является ДОВЕРЕННЫМ. Если вы хотите добавить его в список доверенных устройств, то подпишите простой электронной подписью "Заявление о добавлении устройства в список доверенных"

Для дополнительной аутентификации необходимо использовать Сертификат ключа подписи. Выберите личный сертификат.

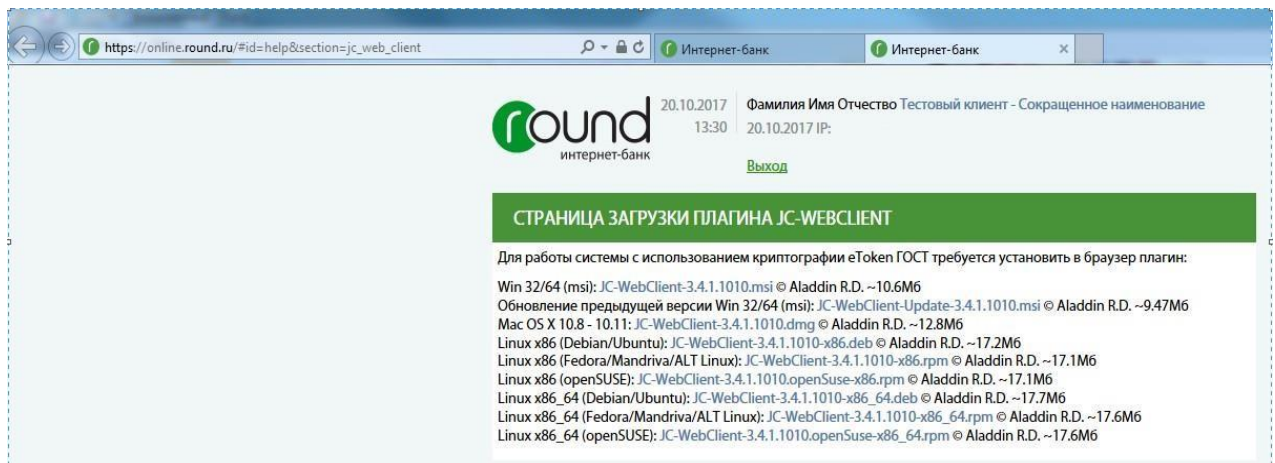
Плагин JC-WebClient не установлен. Для загрузки плагина проследуйте по [ссылке](#).

ПОЛУЧИТЬ СЕРТИФИКАТ **МОИ СЕРТИФИКАТЫ** **ПРОДОЛЖИТЬ** **ВЫХОД**

3.3. Для установки плагина найдите в конце страницы строку:

Плагин JC-WebClient не установлен. Для загрузки плагина проследуйте по [ссылке](#).

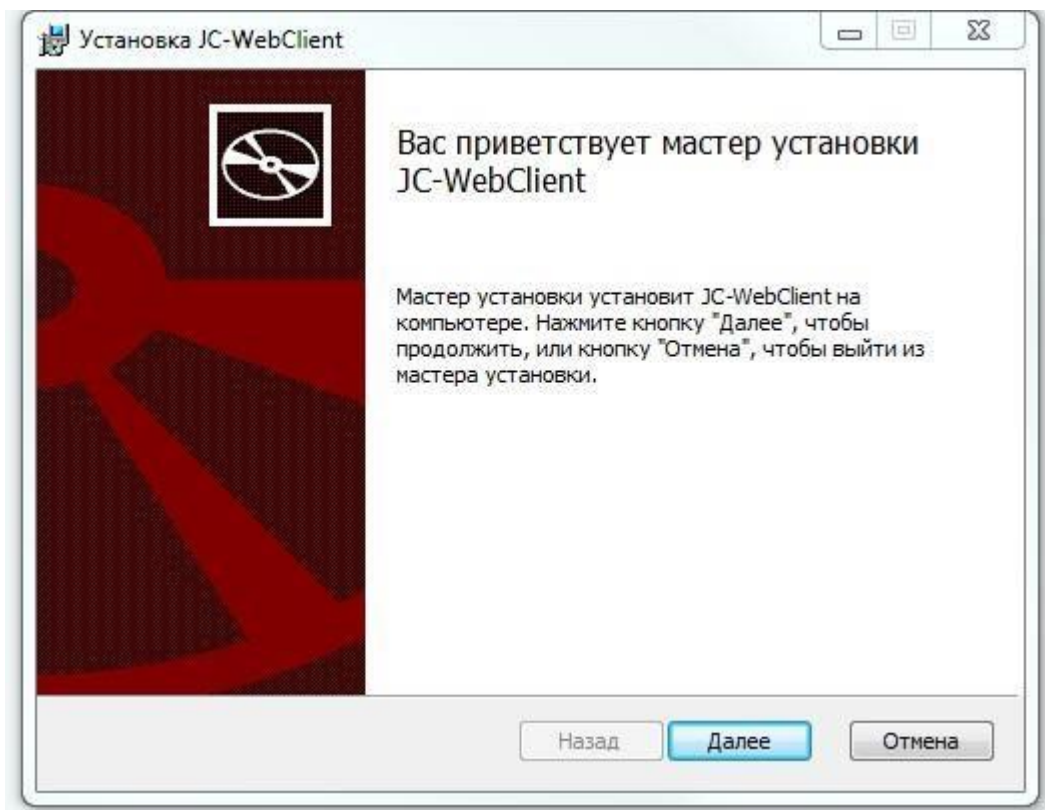
3.4. Щелкните мышью на слове «[ссылке](#)». Откроется новая вкладка обозревателя:



3.5. Щелкните мышью по ссылке «JC-WebClient-3.4.1.1010.msi», расположенной после слов «Win 32/64» (Внимание! Цифры могут отличаться от указанных в настоящем руководстве.) В появившемся окне нажмите **Выполнить**.



и дождитесь появления окна мастера установки:



3.6. В появившемся окне нажмите последовательно кнопки **Далее** и **Готово**.

3.7. Перейдите в Internet Explorer и закройте вкладку, открывшуюся в п. 3.4

3.8. На страничке Генерация запроса на сертификат нажмите кнопку «**Выход**» и **повторите действия, описанные в пп. 2.3 и 3.1**. Если установка плагина и настройки браузера выполнены корректно, в поле «Токен/смарт - карта» отобразится идентификатор токена

Генерация запроса на сертификат

ТИП СУБЪЕКТА

☒ Сотрудник юридического лица
☐ Индивидуальный предприниматель

Криптобиблиотека: JaCarta GOST

Токен/смарт-карта: 0b53001040326967

Имя владельца сертификата

Организация

Отдел

Должность

ИНН

ОГРН

Код страны: RU

Область/край

Город

Email

Введите текст с картинки: 42 37 64

Сменить картинку

OK

3.9. Заполните поля формы (Поля, выделенные жирным шрифтом – обязательны к заполнению)

✓ В поле **Имя владельца сертификата** введите полностью Фамилию Имя Отчество лица, на которого выпускается сертификат;

✓ в поле **ИНН** необходимо вводить ИНН организации. Если длина ИНН составляет 10 цифр, то его необходимо дополнить слева 00, например, 001234567890.

После заполнения полей формы введите текст с картинки. Заполненная форма будет выглядеть так:

Генерация запроса на сертификат

ТИП СУБЪЕКТА

☒ Сотрудник юридического лица
☐ Индивидуальный предприниматель

Криптобиблиотека: JaCarta GOST

Токен/смарт-карта: 0b53001040326967

Имя владельца сертификата: Фамилия Имя Отчество

Организация: ООО "Тестовый клиент"

Отдел:

Должность:

ИНН: 001234567890

ОГРН: 1027700140111

Код страны: RU

Область/край:

Город: Москва

Email: info@email

Введите текст с картинки
190445

Сменить картинку

OK

- 3.10. Нажмите кнопку **ОК**. В появившемся окне введите ПИН-код электронного ключа (Банком установлен ПИН-код «1234567890») и нажмите **ОК**
- 3.11. После генерации запроса открывается новая вкладка с печатной формой заявления:



23.10.2017 16:55

Фамилия Имя Отчество Тестовый клиент - Сокращенное наименование
 23.10.2017

[Выход](#)

ПРОВЕРКА ВХОДА

Вы зашли с устройства 392368cd. Данное устройство не является ДОВЕРЕННЫМ. Если вы хотите добавить его в список доверенных устройств, то подпишите простой электронной подписью "Заявление о добавлении устройства в список доверенных"

Для дополнительной аутентификации необходимо использовать Сертификат ключа подписи. Выберите личный сертификат.

Фамилия Имя Отчество

▼

Токен/смарт-карта

Token (s/n 0C53002318556034)

▼

ПОЛУЧИТЬ СЕРТИФИКАТ

МОИ СЕРТИФИКАТЫ

ПРОДОЛЖИТЬ

ВЫХОД

4.2. Нажмите кнопку «мои сертификаты».

СЕРТИФИКАТЫ












Криптобиблиотека

Действует на дату

▼

📅

☒	Идентификатор сертификата	Владелец	Начальная дата	Конечная д
☒	273850926351172755260450	Фамилия Имя Отчество	23.10.2017 11:31:00	23.01.2019

<

>

НАЗАД

В открывшемся окне выберете необходимый сертификат и нажмите кнопку с изображением принтера.

4.3. В новой вкладке откроется печатная форма акта признания открытого ключа следующего вида

АКТ
признания открытого ключа (сертификата) для обмена сообщениями

23 октября 2017 г.

г. Москва

Настоящим Актом признаётся открытый ключ шифрования, принадлежащий уполномоченному представителю организации Фамилия Имя Отчество (ООО "Тестовый клиент").

Наименование организации: ООО "Тестовый клиент"
Юридический адрес: _____
Телефон: _____ Факс: _____
Фамилия, имя, отчество владельца ключей: Фамилия Имя Отчество
Должность: _____
Удостоверение личности: _____

Личная подпись владельца ключа _____

Параметры ключа:

Алгоритм: ГОСТ Р 34.10-2001 (1.2.643.2.2.19), Параметры:

Начало срока действия: 23-10-17 11:31:00

Окончание срока действия: 23-01-19 11:41:00

Текст открытого ключа:

0440 CA2B EF11 79F8 A50C 8D2B 632C 53A6 D6B6 3AF2 B9CF A516 53D9 EC91 AABA 1A6E 5C07 C3A2 76BA C091
E7AE 6C82 ECFD A6B2 035B B9D1 8A5B 533F 62F5 4E9D 1249 B2D8 15CC

Дополнительные поля открытого ключа (сертификата):

Серийный номер ключа: 39 fd 7d 0c 00 00 00 04 22
Имя владельца ключей: Фамилия Имя Отчество
Дополнительная информация о владельце ключа:
Код страны: RU
Город: Москва
Организация: ООО "Тестовый клиент"
Должность: специалист отдела
ИНН: 001234567890
ОГРН: 1027700140111
E-mail: info@email
Параметры издателя (центра сертификации):
Имя: Round Bank Signing CA
Данные об издателе: RU; Москва; ООО банк Раунд; ca@round.ru

Ключ зарегистрирован и может использоваться для обмена сообщениями.
Группа подписи - Единственная подпись.

БАНК

ООО "банк Раунд"

КЛИЕНТ

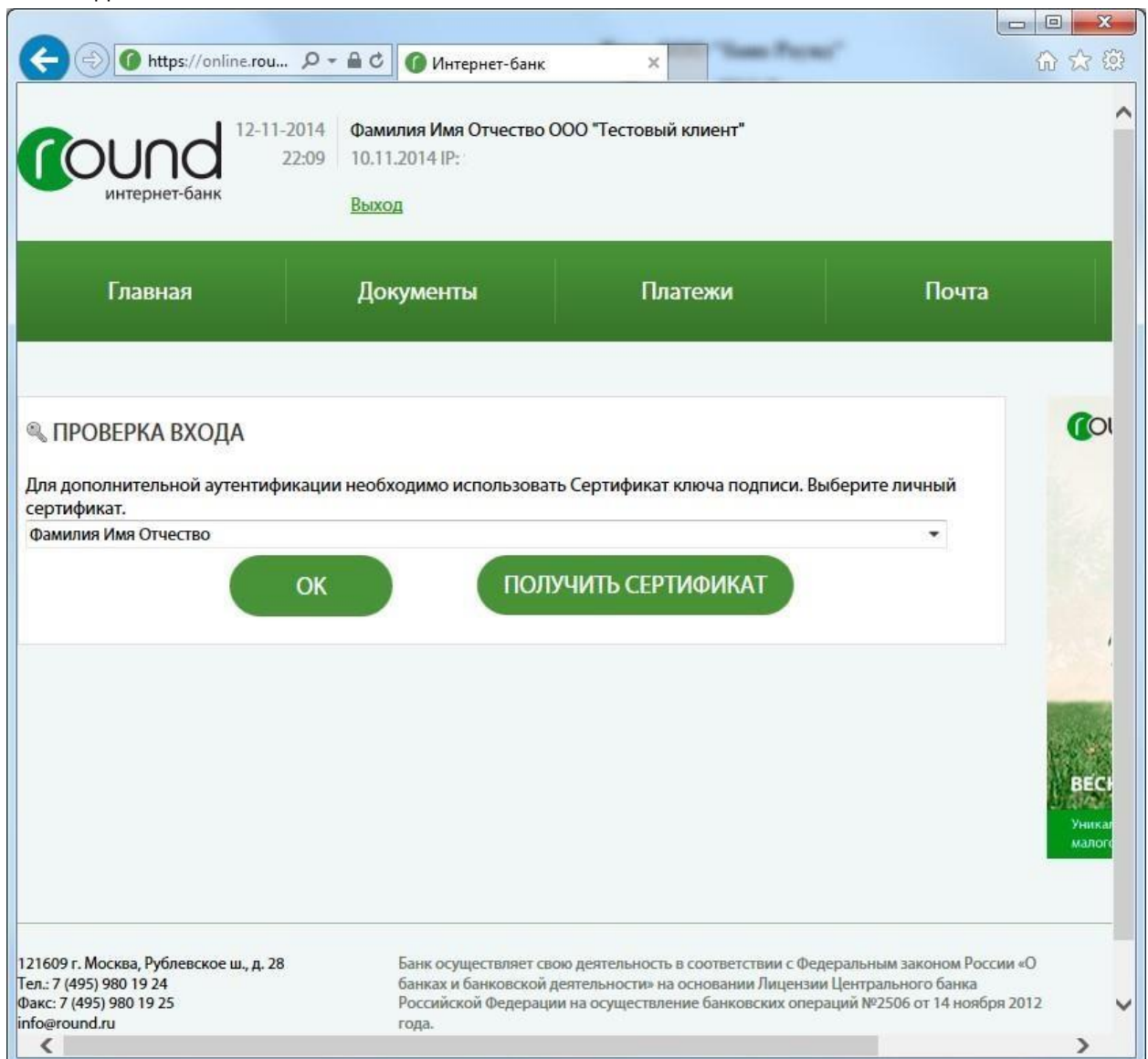
ООО "Тестовый клиент"

4.4. Данный акт необходимо распечатать в двух экземплярах и передать в Операционный отдел Банка. Для печати щелкните на странице правой кнопкой мыши и выберите **Печать** из выпадающего меню (или нажмите комбинацию клавиш Ctrl + P).

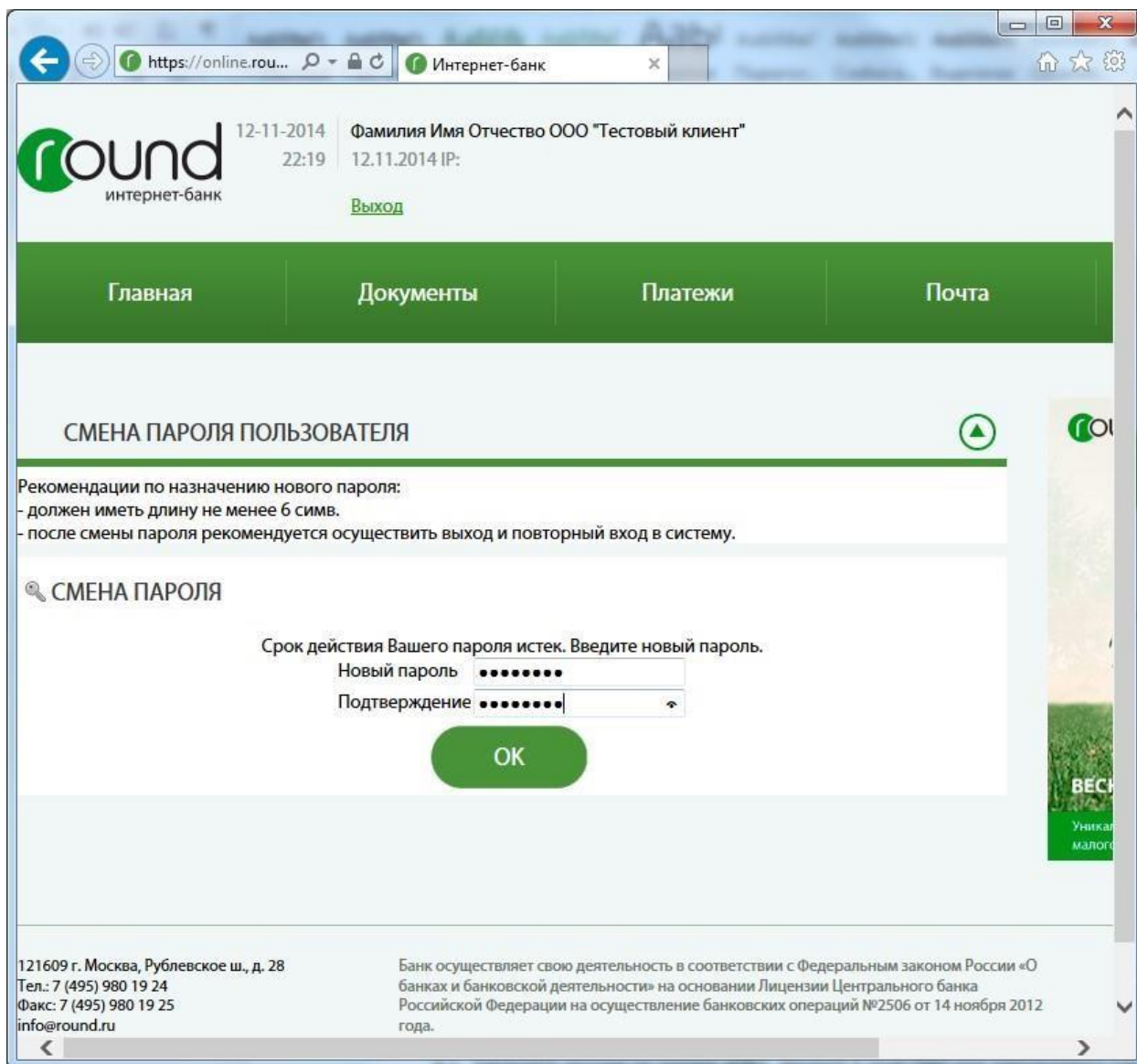
После получения акта Банк в течение 1-2 рабочих дней подтверждает Сертификат ключа подписи, после чего пользователь может полноценно работать в системе ДБО.

5 Действия после выпуска банком сертификата

- 5.1. Откройте Internet Explorer и выполните вход в систему ДБО (шаги 2.1 – 2.4). Если на странице «Проверка входа» в выпадающем списке не появилась строка, содержащая ФИО владельца сертификата – Банк еще не выпустил сертификат. В случае, когда сертификат выпущен окно будет выглядеть так:



- 5.2. Щелкните мышью по кнопке «ОК», введите в окне ПИН-код электронного ключа. Система ДБО предложит поменять пароль от вашей учетной записи:
- 5.3. Введите новый пароль в 2 поля, как показано на рисунке и щелкните мышью по кнопке «ОК»



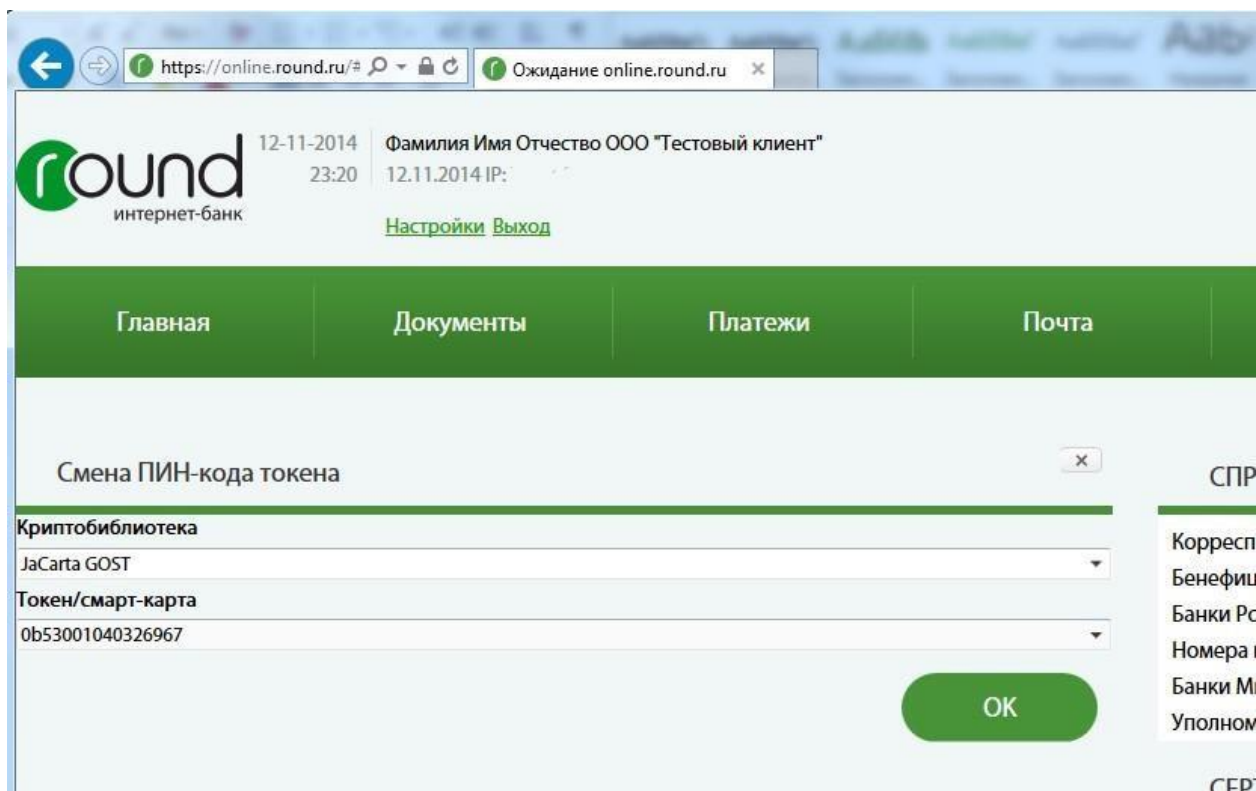
5.4. После смены пароля откроется главная страница системы ДБО.

6 Рекомендуемые к выполнению действия

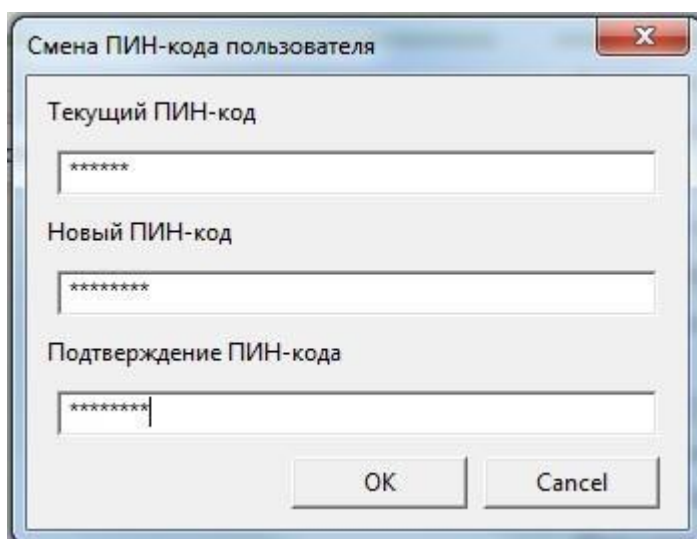
Действия, описанные ниже носят рекомендательный характер.

6.1. Смена ПИН-кода электронного ключа

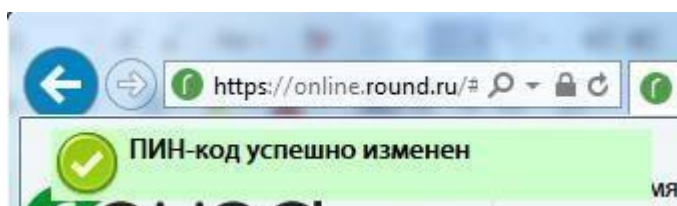
6.1.1. Для смены ПИН-кода щелкните мышью по пункту «Смена ПИН-кода токена» в разделе «Сертификаты». Откроется страница:



6.1.2. Нажмите «**ОК**». Появится окно, в котором нужно ввести действующий ПИН-код и 2 раза новый:



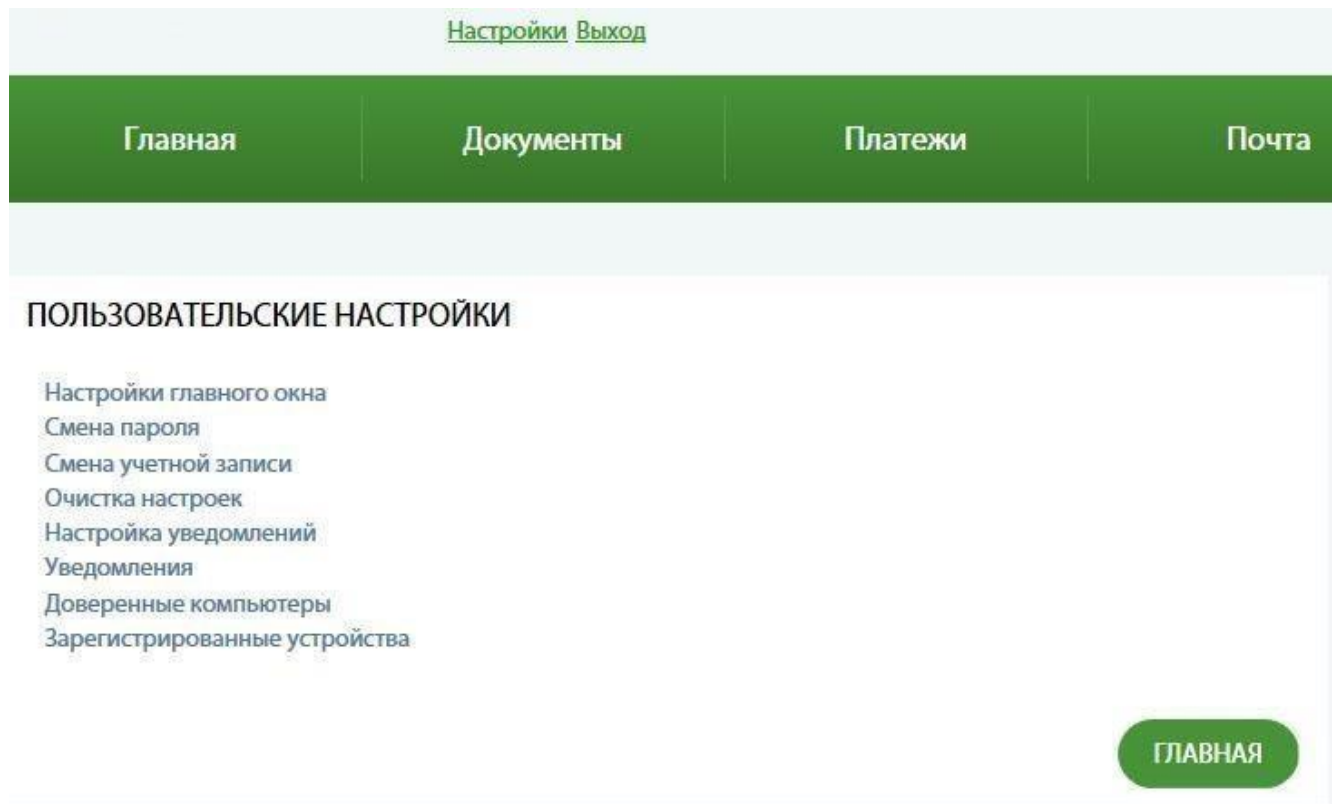
6.1.3. После заполнения всех полей нажмите кнопку «**ОК**». В случае успешной смены ПИН-кода появится сообщение:

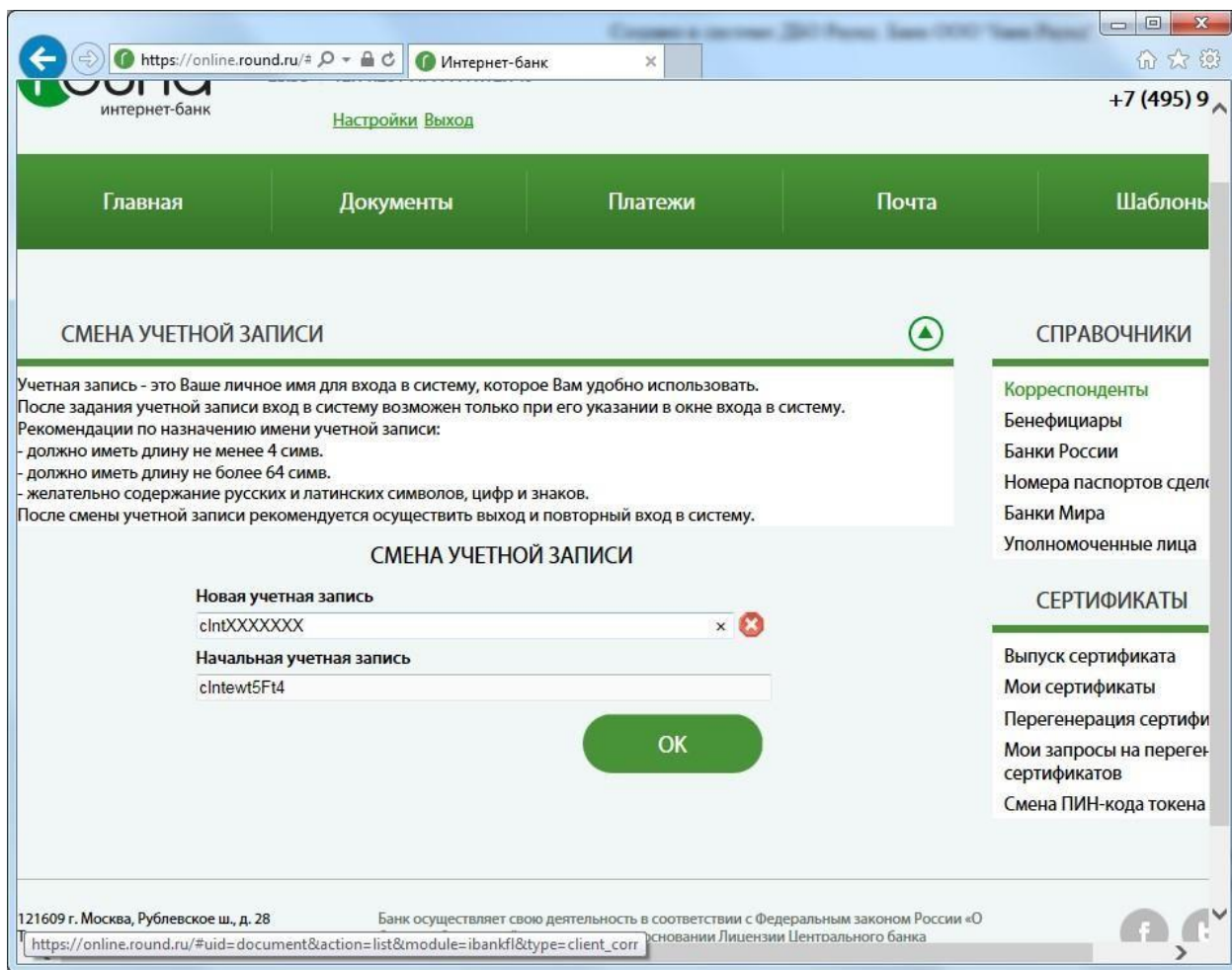


7 Смена учетной записи (по желанию)

Для улучшения удобства пользования системой ДБО можно сменить имя учетной записи, выданное Вам в банке на более удобное.

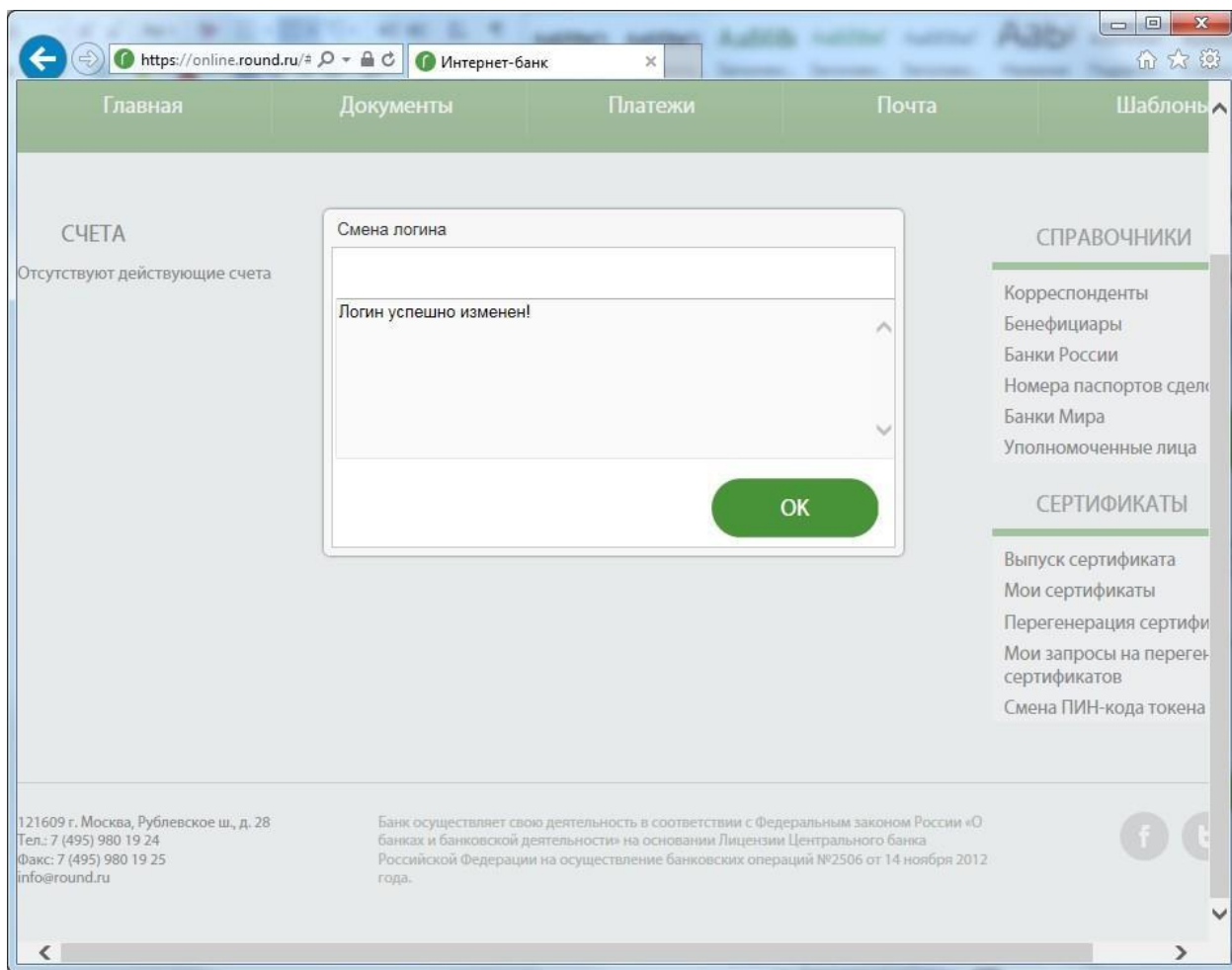
В меню настроек системы выберете пункт **«Смена учетной записи»**. Откроется страница:





7.1.1. В строке «**Новая учетная запись**» введите новое имя входа, следуя рекомендациям на странице и нажмите «**ОК**»

7.1.2. В случае успешной смены учетной записи появится сообщение:



После выполнения всех действий раздела 5 рекомендуется сделать выход и повторный вход в систему ДБО для успешного продолжения работы.