Система «**PSB On-Line**»
Руководство пользователя

Книга **№ 2.** Порядок работы с сертификатом.

Москва, **2016**

Оглавление

1 ВВЕДЕНИЕ 4
1.1 Целевая аудитория 4
1.2 Назначение документа 4
1.3 Перечень эксплуатационной документации по Системе 4
1.4 Версия программы 5
1.5 Необходимая подготовка 5
2 ПОЛУЧЕНИЕ СЕРТИФИКАТА 6
2.1 Электронный сертификат. Общие сведения 6
2.2 Получение электронного Сертификата 8
2.2.1 Описание операции 8
2.2.2 Запуск операции 8
2.2.2.1 С помощью Java-апплета 8
2.2.2.2 С помощью приложения Java Web Start 10
2.2.3 Оформление операции. Запрос на получение Сертификата 12
2.2.4 Получение Сертификата 14
2.2.5 Печать Сертификата 15
2.2.6 Активация Сертификата 16
3 РАБОТА С СЕРТИФИКАТОМ 17
3.1 Открытие окна «Работа с сертификатом» 17
3.1.1 Общие принципы 17
3.1.2 С помощью Java-апплета 17
3.1.3 С помощью приложения Java Web Start 18
3.2 Замена сертификата 19
3.2.1 Общие принципы 19
3.2.2 Формирование запроса на замену сертификата 19
3.2.3. Замена сертификата через модуль системы PSB-Online 23
3.3 Запрос на дополнительный доступ 24
3.3.1 Общие принципы 24
3.3.2 Оформление операции 24

СПИСОК СОКРАЩЕНИЙ

Сокращение	Описание
ПО	Программное обеспечение
ИТ	Информационные технологии
БД	База данных
ДБО	Дистанционное банковское обслуживание

ПЕРЕЧЕНЬ ИСПОЛЬЗУЕМЫХ ТЕРМИНОВ

Термин	Описание
Банк	ПАО «Банк ПСБ»
Система	Программный продукт «PSB On-Line v.2»
Клиент	Юридическое лицо - владелец счета (ов) открытого (-ых) в Банке
Пользователь	Юр. лицо, выполняющее операции в системе
Браузер	Программное обеспечение для поиска, просмотра веб-сайтов, то есть для запроса веб-страниц для их обработки, вывода и перехода от одной страницы к другой
Java-апплет	Программа, загружаемая с сайта Системы и используемая для входа в Систему

1 Введение

1.1 Целевая аудитория

Настоящее руководство предназначено для пользователей системы **«PSB On-Line v.2»**, далее по тексту «система». К пользователям системы относятся Клиенты Банка.

1.2 Назначение документа

Настоящее руководство регламентирует порядок предоставления Клиенту дистанционного банковского обслуживания в Системе.
Настоящий документ содержит информацию следующего характера:

- Последовательность получения сертификата.
- Порядок работы с сертификатом.

В документе не рассматриваются дополнительные возможности пользователя, связанные с правами доступа к разделам интерфейса, не входящим в состав базового набора прав, предоставляемых группе «Пользователи клиентского модуля системы PSB On-Line».

1.3 Перечень эксплуатационной документации по Системе

Комплект документов «Руководство пользователя системы **PSB On-Line»** предназначен для пользователей входящих в группу «Пользователи клиентского модуля системы PSB On-Line». Состав набора документов**:**
Комплект документов **«Руководство пользователя системы PSB On-Line»** предназначен для пользователей, входящих в группу «Пользователи клиентского модуля системы PSB On-Line». Состав набора документов**:**

- **Книга 1. «Общие принципы работы в Системе».**
  Порядок входа и выхода из Системы, описание главного окна системы, общие принципы работы в Системе. В документе приводится справочная информация и не регламентируется порядок оформления конкретных финансовых и документарных операций.
- **Книга 2. «Порядок работы с сертификатом».**
  Последовательность получения сертификата, порядок работы с сертификатом. В документе приводится справочная информация и не регламентируется порядок оформления конкретных финансовых и документарных операций.
- **Книга 3. «Основные операции в Системе»** (2 части).
  Последовательность оформления расчетных и справочных документов в инвалюте и валюте РФ для пользователей системы.
- **Книга 4. «Импорт документов. Служебные операции в Системе. Обработка документов в Системе».**
  Последовательность импорта в систему документов, созданных ранее в другой бухгалтерской программе; порядок выполнения служебных операций в Системе; порядок подписания ранее созданных/загруженных документов в Системе; порядок отправки документов на исполнение в Банк.
- **Книга 5. «Формирование отчетов. Карты в рамках Зарплатного проекта. Порядок работы с сообщениями».**
  Порядок формирования отчетов в Системе; порядок работы с банковскими картами в рамках Зарплатного проекта; порядок работы с корпоративными банковскими картами; описание работы с входящими/исходящими сообщениями.
- **Книга 6. «Пользовательские настройки Системы».**
  Порядок установки пользовательских настроек в Системе.
- **Книга 7. «Порядок работы в модуле «Оператор»**
- **Книга 8. «Порядок работы в модуле Регистратор»**

- **Книга 9. Модуль «Зарплатный проект»**
- **Книга 10 «Порядок работы в модуле "Мультихолдинг»**
- **Книга 11 «Создание отчета по выгрузке служебных сертификатов»**
- **Книга 12 Порядок работы в подсистеме «ЭДО факторинговых операций»**
- **Книга 13 «Порядок работы в модуле " Многофилиальный мультихолдинг»**
- **Приложения А. Справочные сведения.**
  Описание формата импортируемых в Систему документов; порядок работы со справочником контрагенты; общие сведения о приложении JavaWebStart.
- **Приложения Б. Оформление документов для кипрского филиала Банка.**
  Последовательность оформления расчетных и справочных документов в инвалюте и валюте РФ для пользователей системы – клиентов Кипрского филиала Банка.
- **Приложения В. Оформление документов для ЛОРО-банков.**
  Последовательность оформления расчетных и справочных документов в инвалюте и валюте РФ для пользователей системы – ЛОРО банков.

1.4 Версия программы

Данное Руководство относится к версии системы **«PSB On-Line v.2»**. Возможны незначительные расхождения между руководством и последующими версиями программы.

1.5 Необходимая подготовка

Пользователи Системы должны иметь необходимую базовую компьютерную подготовку:

- Обладать сведениями о персональном компьютере и операционной системе Windows.
- Иметь навыки работы с файловой системой компьютера.
- Иметь навыки работы в сети Интернет.

2 Получение сертификата

2.1 Электронный сертификат. Общие сведения

Для работы с системой не требуется установка специализированного программного обеспечения. Работа осуществляется через Интернет[1], на сайте системы:

Наименование банка	Ссылка на сайт системы
Банк ПСБ	http://online.payment.ru

Для работы с системой требуется предварительно получить и активировать электронный цифровой сертификат ключа подписи, далее Сертификат.
Используя Сертификат, пользователь (Клиент либо представитель Клиента) может создать свою уникальную электронную цифровую подпись - аналог собственноручной подписи. Таким образом, электронная цифровая подпись является цифровым удостоверением каждого пользователя и дает право входить в систему и работать с ней.
Каждый сертификат, имеет определенный срок действия, по истечению которого Сертификат становится недействительным. Недействительный Сертификат не может быть использован для входа в систему и должен быть заменен пользователем.
При необходимости, можно заменить сертификат с истекающим сроком действия на новый Сертификат, в целях обеспечения доступа к системе в будущем периоде.
В системе существует возможность разграничить права пользователей на работу с документами. Для этого возможно использование нескольких Сертификатов с различными правами на обработку документов.
Процедура получения Сертификатов с теми или иными правами одинакова. Различные права Сертификату присваиваются сотрудниками Банка, в соответствии с распоряжениями Клиента.
Выделяются следующие наборы прав и полномочий:

- Первая подпись.
- Вторая подпись.
- Исполнитель.
- Контролер.
- Просмотр.
- «Валютный контроль».
- Трейдер.

Сертификат с правами на просмотр документов может быть выдан любому представителю Клиента, на основании его запроса[2]. Сертификат на просмотр позволяет владельцу просматривать ранее созданные документы, а также формировать выписки.
Сертификат с правами на исполнение документов может быть выдан любому представителю Клиента на основании его запроса[3]. Сертификат на исполнение позволяет владельцу создавать и просматривать документы, а также отправлять их на исполнение, после того как они будут подписаны Первой и Второй подписью (с помощью Сертификатов с правами Первой и Второй подписи).

Сертификат с правом Контролер может быть выдан любому представителю Клиента, на основании его запроса[4]. Сертификат с правами контролера предполагает наличие прав на все операции с электронными документами (за исключением отправки на исполнение электронных документов), получение информации по всем доступным Счетам, установку и снятие подписи контролера под электронными документами. Уровень

[1] Интернет соединение должно удовлетворять требованиям Банка, изложенным в книге 1, пункте 2.3.2.
[2] Как сотруднику организации, так и любому другому лицу.
[3] Как сотруднику организации, так и любому другому лицу.
[4] Как сотруднику организации, так и любому другому лицу.

доступа «Контролер» предоставляет возможность организации клиента контролировать платежи своих филиалов, подотчетных юридических лиц, участников холдинга и т. д.

Один сертификат также может включать в себя сразу все возможные наборы прав[5] и полномочий, в случае если Клиент, в соответствии с банковской карточкой не нуждается в разграничении прав доступа к Системе.

Сертификат с правом Первой или (и) Второй подписи выдается исключительно должностным лицам, указанным в банковской карточке в качестве обладателей данных прав. Сертификат с правом Первой или (и) Второй подписи позволяет владельцу создавать и подписывать документы в системе.

Сертификат с правом Трейдер выдается исключительно должностным лицам, указанным в банковской карточке в качестве обладателей данных прав. Сертификат с правами трейдера предполагает наличие прав на все операции, связанных с совершением конверсионных сделок. Один сертификат может совмещаться с правами 1-й, 2-й подписью и Исполнителя.

Сертификат в сочетании прав Трейдер и 1-ой и 2-ой подписи позволяет владельцу создавать, подписывать и автоматически отправлять из системы PSB-Online только документы конверсии.

В системе реализована возможность ограничения доступа к счетам организации, к службам, к сформированным документам. Эта функция используется по желанию клиента и реализуется путем наложения ограничений на конкретный сертификат.

Под службами следует понимать совокупность операций, используемых пользователями для формирования типовых документов и последующего их просмотра. Например, в службе «Кредиты» формируются кассовые документы, такие как заявление на досрочное погашение кредита, заявление на выдачу транша по кредитной линии и т.п.

Ограничению подлежат следующие службы: «ДО», «ВК», «Безнал», «Касса», «Прочие», «Кредиты», «Депозиты», «Карты», «Факторинг».

Для того чтобы Клиент мог управлять счетами нескольких своих дочерних компаний, в системе существует возможность привязать к одному сертификату несколько организаций.

При работе с таким сертификатом потребуется указать, от имени какой организации оформляются документы. Доступ к счетам нескольких дочерних компаний может быть разрешен в рамках полномочий того или иного сертификата.

Данные сертификата могут быть размещены:

- на любом носителе информации, в файле, защищенном паролем. Таким образом, для того, чтобы воспользоваться сертификатом, необходимо иметь файл Сертификата и знать пароль.
- на USB ключе (eToken) – специальном средстве защиты от несанкционированного доступа. Таким образом, для того чтобы воспользоваться сертификатом, необходимо иметь USB ключ.

> **Внимание!** Сертификат с правом Трейдер, Первой или (и) Второй подписи может быть размещен только на USB ключе (eToken).

[5] Исключение составляет право доступа «Контролер», которое можно совмещать только с правами «Просмотр» или «Исполнитель».

2.2 Получение электронного Сертификата

2.2.1 Описание операции

Для того чтобы получить электронный сертификат следует:

1. Отправить запрос на получение Сертификата на сайте системы.
2. Получить Сертификат и сохранить его данные на выбранном носителе информации/USB ключе.
3. Распечатать данные Сертификата.
4. Активировать Сертификат в офисе Банка.

> **Внимание!** Перед активацией Сертификата, Клиенту следует подписать необходимые документы[6]. Подписание документов и активация Сертификата могут быть осуществлены единовременно, в рамках одного визита представителя Клиента в офис Банка.

2.2.2 Запуск операции

2.2.2.1 С помощью Java-апплета

Перед оформлением операции следует убедиться, что подключение к сети Интернет доступно[7].

Для того чтобы перейти к получению Сертификата следует в адресной строке браузера указать ссылку[8] на сайт системы и нажать на клавиатуре клавишу **[ENTER]**, Рис.1. Будет открыта главная страница сайта Системы, Рис. 2.

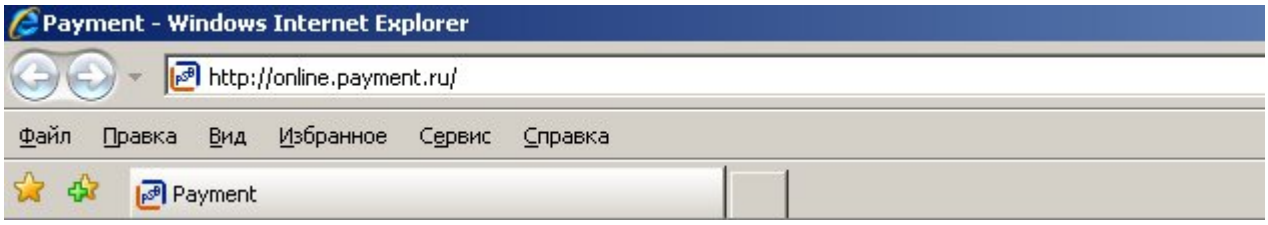

Рис.1 Адресная строка браузера

Далее, на главной странице сайта системы следует перейти по ссылке «Подключение к системе, замена сертификатов», Рис. 2. Будет открыта страница «Вход в систему», Рис.3.

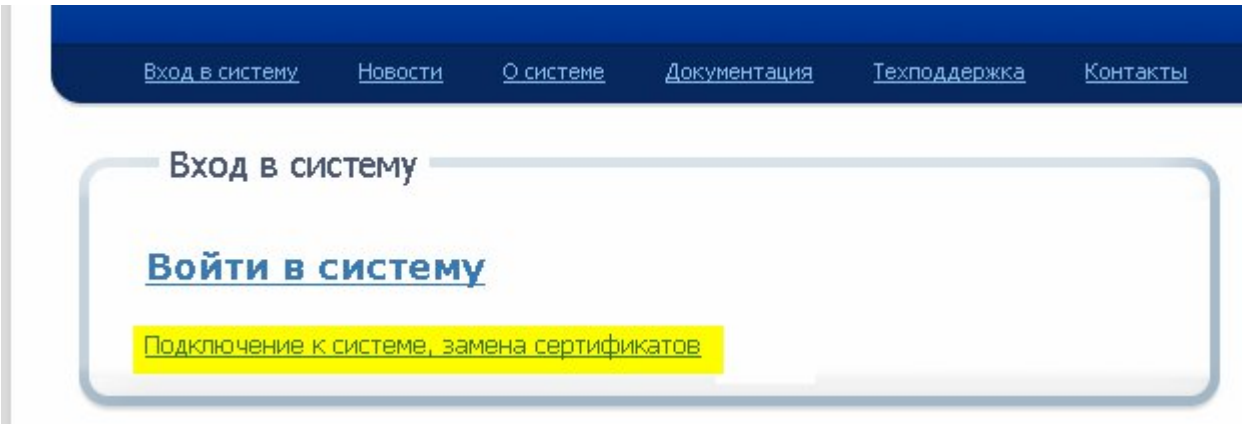

Рис. 2 Главная страница сайта Системы

---

[6] Бланки документов размещены на сайте Системы в разделе «Документация».
[7] Интернет-соединение должно удовлетворять требованиям Банка, изложенным в книге 1, пункте 2.3.2.
[8] Ссылки на сайт системы приведены в разделе «Электронный сертификат. Общие сведения».

Далее, на странице «Вход в систему» перейти по ссылке «Получение сертификата», Рис.3. Будет открыто окно «Сертификат», Рис.4.

Рис.3 Страница «Вход в систему»

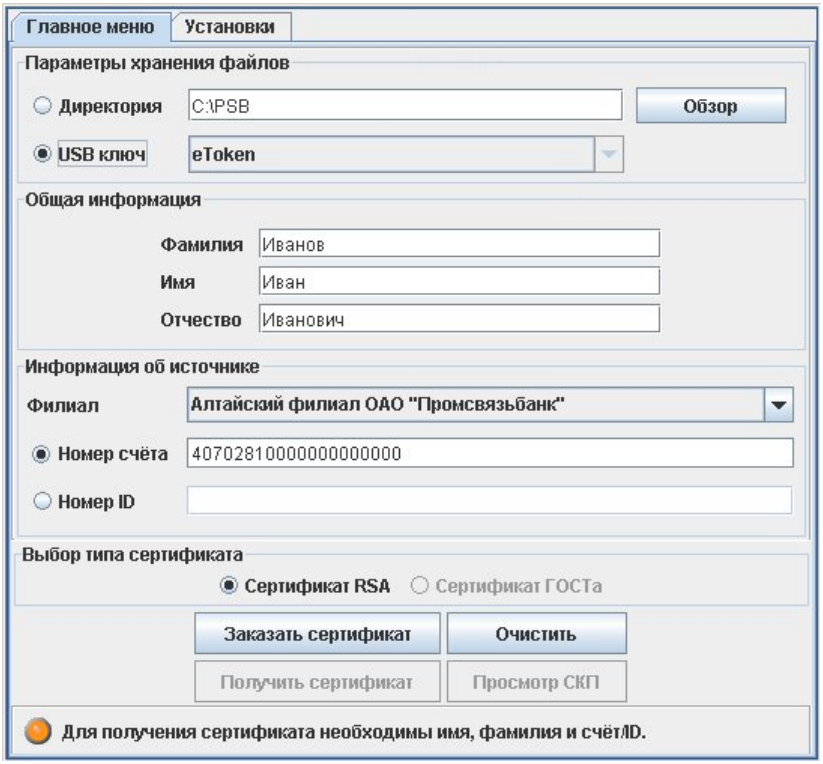

Рис.4 Окно «Сертификат»

> **Внимание!** В зависимости от настроек браузера, перед загрузкой окна «Сертификат» на экран может быть выведено окно «Предупреждение», содержащее сведения о поставщике программы. Пользователю, в этом случае необходимо будет подтвердить свое согласие на загрузку программы, Рис.5.

Рис.5 Окно «Предупреждение»

2.2.2.2 С помощью приложения Java Web Start

Перед оформлением операции следует убедиться, что подключение к сети Интернет доступно[9].

Для того, чтобы перейти к получению Сертификата следует в адресной строке браузера указать ссылку[10] на сайт Системы и нажать на клавиатуре клавишу [**ENTER**], Рис.6. Будет открыта главная страница сайта системы, Рис.7.

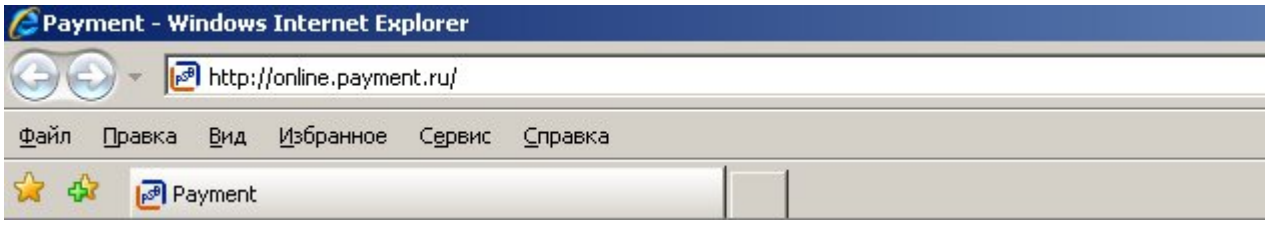

Рис.6 Адресная строка браузера

Далее, на главной странице сайта системы следует перейти в пункт меню «Вход в систему» сайта системы, Рис.7. Будет открыта страница «Вход в систему», Рис.8.

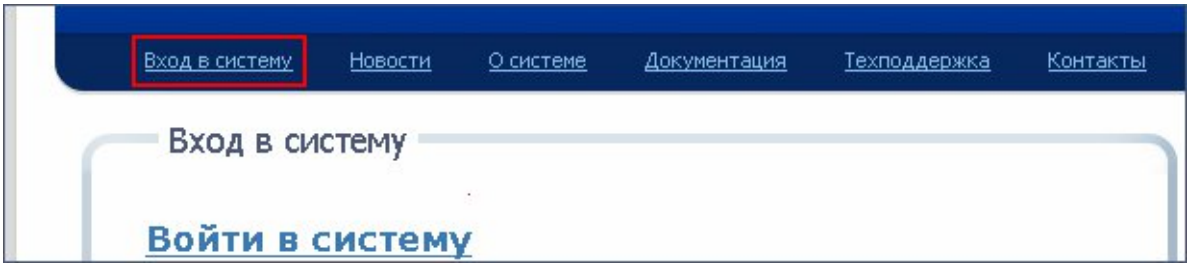

Рис.7 Главная страница сайта Системы

Далее, на странице «Вход в систему» следует перейти по ссылке «Вход через **WebStart**», Рис.8. Будет открыта страница «Вход через **WebStart**», Рис.9.

[9] Интернет-соединение должно удовлетворять требованиям Банка, изложенным в книге 1, пункте 2.3.2.
[10] Ссылки на сайт системы приведены в разделе «Электронный сертификат. Общие сведения».

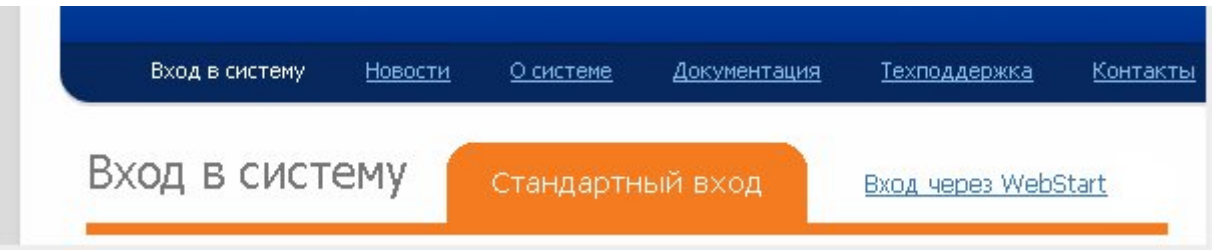

Рис.8 Страница «Вход в Систему»

Далее, на странице «Вход через **WebStart**» следует перейти по ссылке «Получение сертификата», Рис.9. Будет открыта страница «Запуск **Java Web Start**», Рис.10. Будет открыто окно «Сертификат», Рис.11.

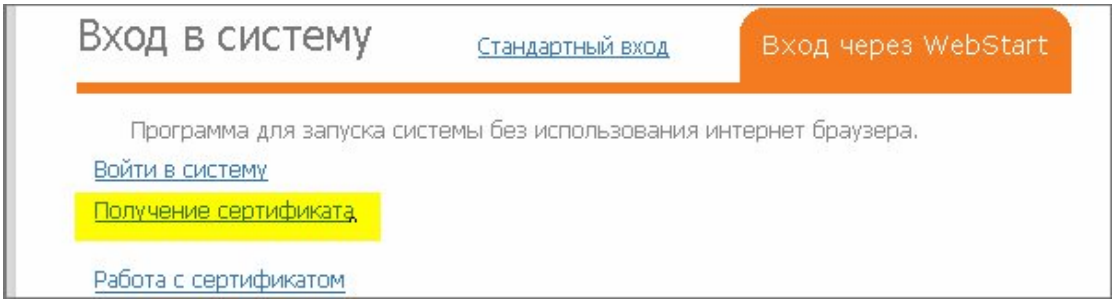

Рис.9 Страница «Вход через Webstart»

Рис.10 Окно «Запуск Java Web Start»

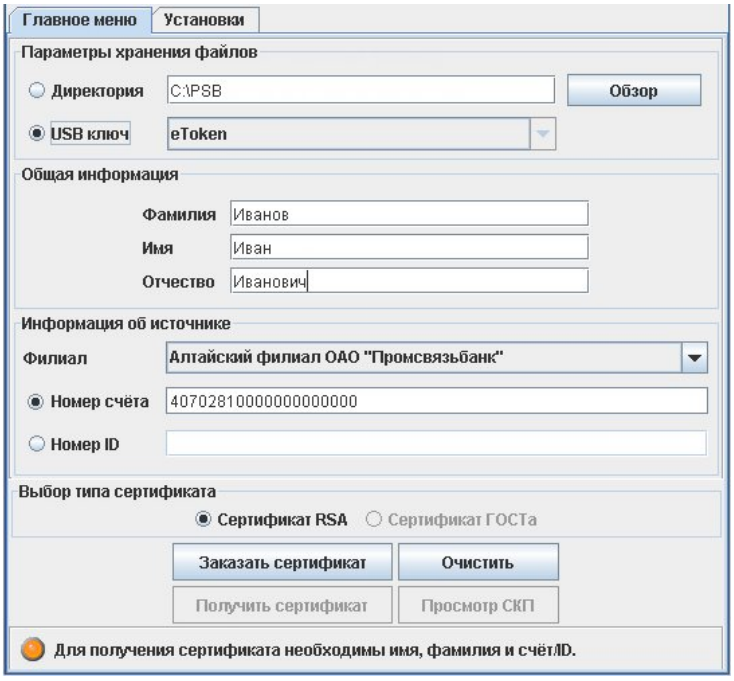

Рис.11 Окно «Сертификат»

Внимание! В зависимости от настроек браузера, перед загрузкой окна «Сертификат» на экран может быть выведено окно «Предупреждение», содержащее сведения о поставщике программы. Пользователю, в этом случае необходимо будет подтвердить свое согласие на загрузку программы, Рис.12.

Рис.12 Окно «Предупреждение»

2.2.3 Оформление операции. Запрос на получение Сертификата

Для того чтобы отправить запрос на получение Сертификата в Банк, в окне[11] «Получение сертификата» следует (Рис.13):

1. Активировать одну из следующих опций:
   - Директория - если сертификат будет сохранен на жестком диске, либо на съемном носителе информации. Дополнительно необходимо будет указать путь к папке, в которую будет сохранен сертификат.
   - **USB** ключ - если сертификат будет сохранен на USB ключе Клиента[12].

Внимание! При выборе опции «**USB** ключ» поле «Директория» все равно должно быть заполнено для сохранения печатной формы сертификата.

2. Указать персональные данные пользователя, на которого запрашивается Сертификат (фамилия, имя, отчество).

Внимание! Поле «Отчество» может быть не заполнено, если оно отсутствует в документе, удостоверяющем личность. При этом во всех печатных формах, порождаемых клиент-банком отчество также не будет указано.

3. Нажать на кнопку и выбрать наименование обслуживающего данного пользователя филиала банка из впадающего списка.
4. Активировать одну из следующих опций:
   - Номер счета – если расчетный счет клиента открыт в банке ПАО «Банк ПСБ»;

Внимание! При появлении окна «Сертификат» (Рис.11) на экране поле Номер счета заполнен двадцатью символами «#» (по количеству цифр в счете). При заполнении этого

[11] Порядок открытия окна «Сертификат» подробно описан в разделе «Электронный сертификат. Общие сведения».

[12] Необходимо убедиться в том, что USB ключ подключен к USB порту компьютера.

поля необходимо установить курсор в левой границе поля и вводить цифры счета, заменяя ими символы «#».

- Номер **ID** – если расчетный счет не открыт в банке ПАО «Банк ПСБ» и организация обслуживается в рамках зарплатного проекта. Необходимо ввести 9-тизначный внутренний номер[13].

Внимание! Для получения внутреннего номера необходимо обратиться в обслуживающий офис.

5. Выбрать тип сертификата (тип криптографического алгоритма, который будет использован при создании Сертификата[14]).
6. Нажать на кнопку «Заказать сертификат». Будет открыто окно «Введите пароль», Рис.14.

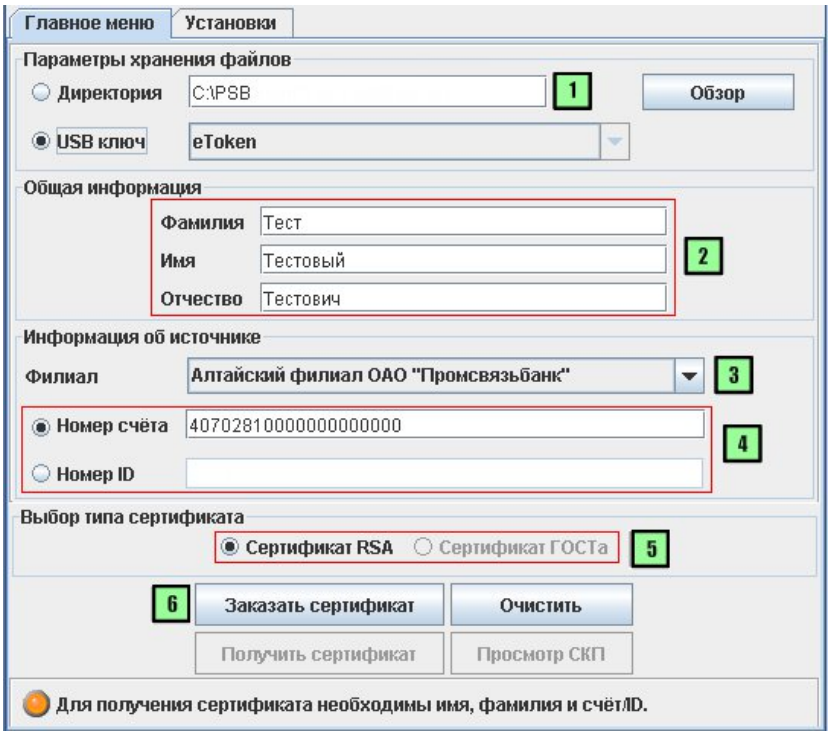

Рис.13 Окно «Сертификат»

Далее, в окне «Введите пароль», следует (Рис.14.):

1. Указать пароль пользователя в полях ввода:
   - Введите пароль.
   - Подтвердите ввод.
2. Нажать на кнопку «Ввод». Окно «Введите пароль» будет закрыто.

Примечание: Если сертификат будет сохранен на USB ключ, то необходимо ввести пароль для USB ключа.

Внимание! В окне «Сертификат» будет отображено информационное сообщение, содержащее сведения о том, что запрос на Сертификат был успешно отправлен в Банк, Рис.15.

[13] Для получения внутреннего номера, необходимо обратиться в обслуживающий офис.
[14] В настоящий момент доступен только вариант «Сертификат RSA».

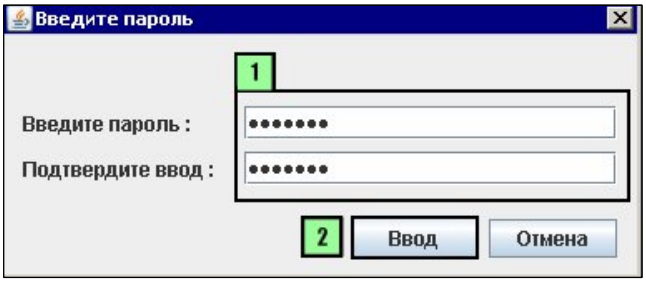

Рис.14 Окно «Введите пароль»

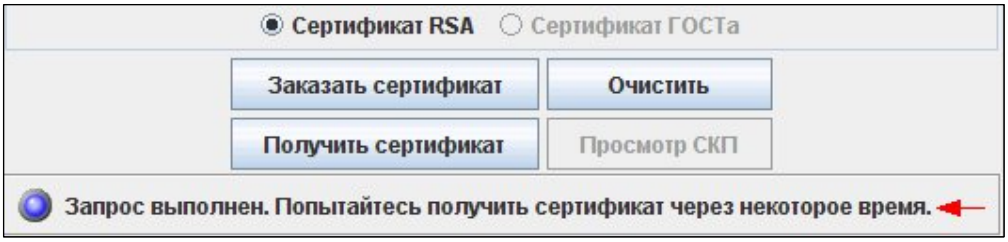

Рис.15 Окно «Сертификат»

2.2.4 Получение Сертификата

После того как пользователь успешно отправил запрос на получение Сертификата в Банк[15], через некоторое время необходимо получить Сертификат, т.е. сохранить данные Сертификата в ранее выбранной папке или на USB ключе.

> Примечание: Время на получение Сертификата после отправки запроса невелико, и не рекомендуется прерывать описываемую процедуру до получения Сертификата.

Для того чтобы получить Сертификат, в окне[16] «Получение сертификата» следует нажать на кнопку «Получить сертификат», Рис.16. Будет открыто окно «Введите пароль», Рис.17.

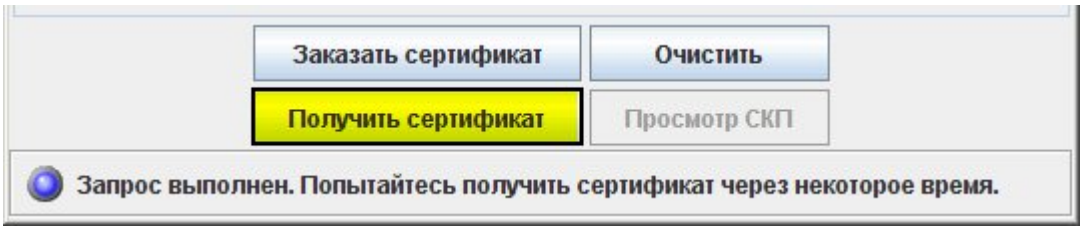

Рис.16 Окно «Сертификат»

Далее, в окне «Введите пароль», следует (Рис.17):

1. Указать пароль пользователя.
2. Нажать на кнопку «OK». Будет открыто окно «Изменение пароля»[17], Рис.18.

Рис.17 Окно «Проверка пароля»

---

[15] Порядок отправки запроса на получение Сертификата описан в разделе «Оформление операции. Запрос на получение Сертификата.»

[16] Порядок открытия окна «Сертификат» подробно описан в разделе «Получение электронного Сертификата.»

[17] Если сертификат будет сохранен на USB-ключ, то данное окно открыто не будет.

Далее, в окне «Изменение пароля» выбрать один из вариантов (Рис.18):

- Изменить пароль. В этом случае нажать кнопку «Да» и указать новый пароль.
- Оставить пароль без изменения. В этом случае нажать кнопку «Нет».

Будет открыто окно «Сертификат». В окне «Сертификат» будет отображено информационное сообщение, содержащее сведения о том, что Сертификат получен[18].

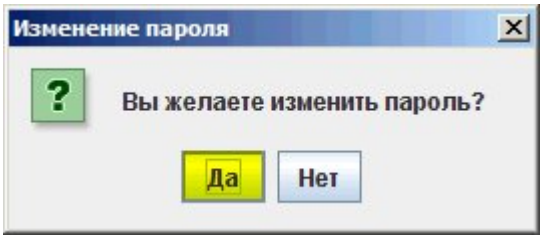

Рис.18 Окно «Изменение пароля»

2.2.5 Печать Сертификата

После получения[19] Сертификата, будет открыто окно сообщения о получение сертификата «**Message**», Рис.19.

Для того чтобы перейти к печати Сертификата, в окне «**Message**» следует нажать на кнопку «ОК», Рис.19. Будет открыта web–страница, содержащая сведения о Сертификате, предназначенные к выводу на печать.

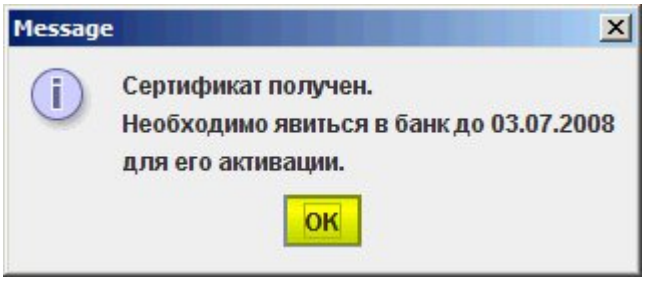

Рис.19 Окно ««Message»

Далее следует распечатать web-страницу с данными Сертификата в двух экземплярах, Рис.20.

[18] Т.е. данные сертификата загружены в ранее указанную пользователем папку.

[19] Порядок получения Сертификата описан в разделе «Получение сертификата.»

> **Внимание!** В том случае, если страница с данными Сертификата будет случайно закрыта пользователем, существует возможность открыть ее повторно. Для этого необходимо открыть файл act.html, хранящийся в папке с данными Сертификата.

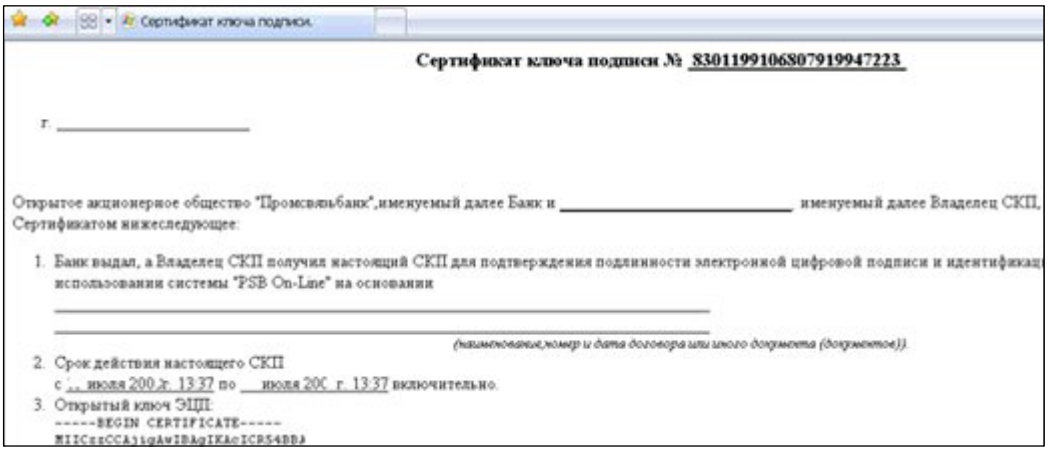

Рис.20 Web-страница с данными сертификата

2.2.6 Активация Сертификата

Сертификат необходимо активировать в офисе Банка.
Перед активацией Сертификата Клиенту следует подписать необходимые документы[20].
Подписание документов и активация Сертификата могут быть осуществлены единовременно в рамках одного визита представителя Клиента в офис Банка.

[20]Перечень и бланки необходимых документов размещены на сайте http://online.payment.ru/ в разделе «Документация». Документы печатаются и подписываются в двух экземплярах.

3 Работа с сертификатом

3.1 Открытие окна «Работа с сертификатом»

3.1.1 Общие принципы

Запуск работы с сертификатом осуществляется в одноименном окне.
Открыть окно «Работа с сертификатом» возможно одним из следующих способов:

- С помощью Java-апплета.
- С помощью приложения Java Web Start.

В том случае, если настоящее окно открыто с помощью Java-апплета, то работа с сертификатом будет осуществляться с использованием интернет-браузера.
В том случае, если настоящее окно открыто с помощью приложения Java Web Start, то работа с сертификатом будет осуществляться без использования интернет-браузера.

3.1.2 С помощью Java-апплета

Запуск работы с сертификатом осуществляется в одноименном окне. Для того чтобы открыть окно «Работа с сертификатом», следует в адресной строке браузера указать ссылку[21] на сайт системы и нажать на клавиатуре клавишу **[ENTER]**, Рис.21. Будет открыта главная страница сайта системы, Рис.22.

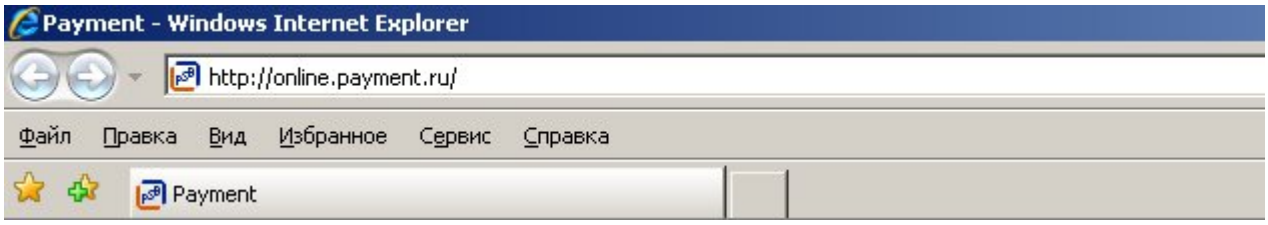

Рис.21 Адресная строка браузера

Далее, на главной странице сайта системы нажмите на пункт меню «Вход в систему» сайта системы. Будет открыта страница «Вход в систему», Рис.23.

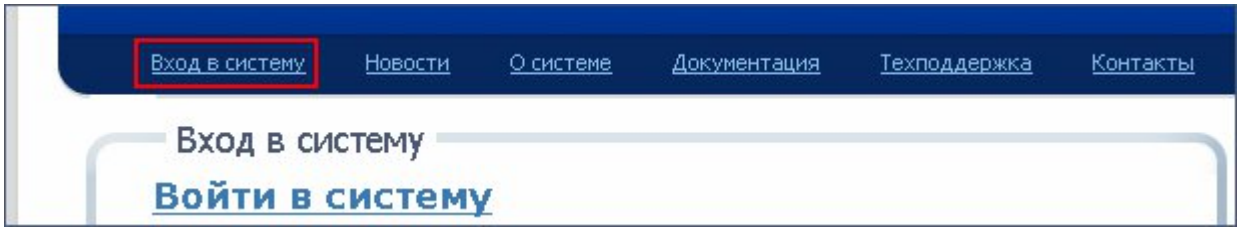

Рис.22 Главная страница сайта Системы

На странице «Вход в систему» следует перейти по ссылке «Работа с сертификатом», Рис.23. Будет открыто окно «Работа с сертификатом. Выбор действия над сертификатом».

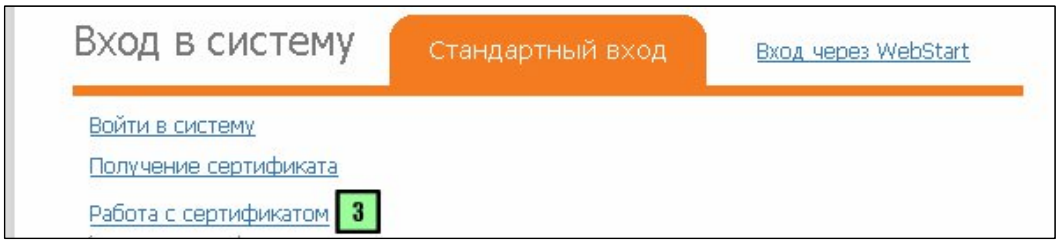

Рис.23 Страница «Вход в Систему»

[21] Ссылки на сайт системы приведены в разделе 2.1 Электронный сертификат. Общие сведения.

3.1.3 С помощью приложения Java Web Start

Перед оформлением операции следует убедиться, что подключение к сети Интернет доступно[22].

В системе, для того чтобы открыть окно «Работа с сертификатом», следует в адресной строке браузера указать ссылку[23] на сайт системы и нажать на клавиатуре клавишу [**ENTER**], Рис.24. Будет открыта главная страница сайта Системы, Рис.25.

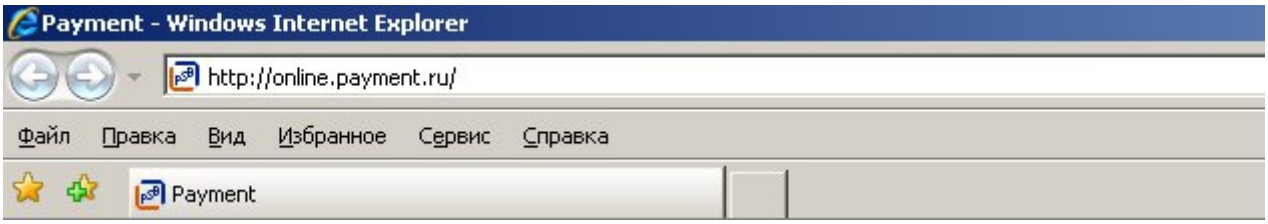

Рис.24 Адресная строка браузера

Далее, на главной странице сайта системы следует нажать на пункт меню «Вход в систему» сайта Системы, Рис.25. Будет открыта страница «Вход в систему», Рис.26.

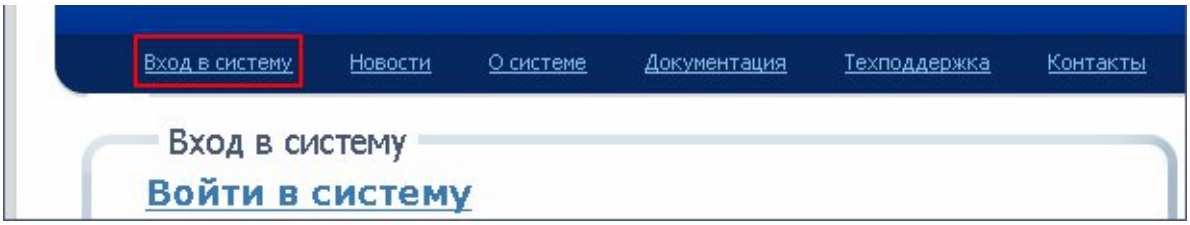

Рис.25 Главная страница сайта Системы

Далее, на странице «Вход в систему» следует навести курсор на ссылку «Вход через **WebStart**» и нажать на левую кнопку мыши, Рис.26. Будет открыта страница «Вход через **WebStart**», Рис.27.

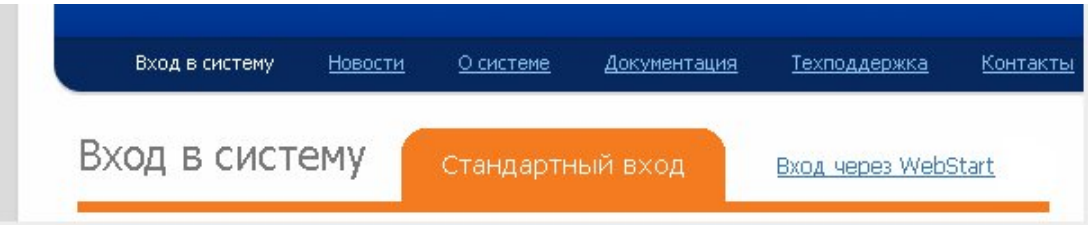

Рис.26 Страница «Вход в Систему»

Далее, на странице «Вход через **WebStart**» следует перейти по ссылке «Работа с сертификатом», Рис.27. Будет открыта страница «Запуск **Java Web Start**». Будет открыто окно «Работа с сертификатом».

[22] Интернет-соединение должно удовлетворять требованиям Банка, изложенным в книге 1, пункте 2.3.2.
[23] Ссылки на сайт системы приведены в разделе 2.1 Электронный сертификат. Общие сведения.

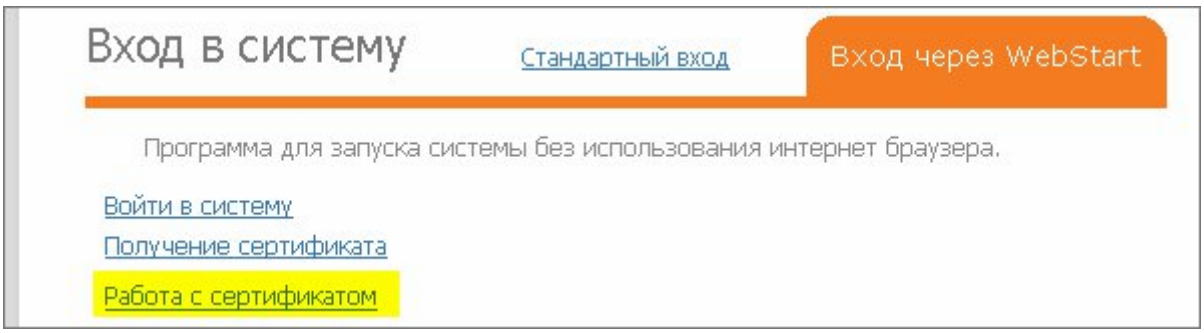

Рис.27 Страница «Вход через Webstart»

3.2 Замена сертификата

3.2.1 Общие принципы

Замену сертификата следует выполнять в следующих случаях:

- Если существует подозрение на то, что сертификат был скомпрометирован[24].
- При смене пароля на вход в систему.

Примечание: Замена сертификата при смене пароля в систему выполняется только при работе с файловыми сертификатами (но не с USB ключами).

- Если необходима своевременная замена сертификата, в целях обеспечения доступа к системе в будущие периоды[25].

3.2.2 Формирование запроса на замену сертификата

Далее, для того чтобы заменить сертификат, в окне[26] «Работа с сертификатом» следует (Рис.28):

1. Установить кнопку выбора в следующее положение:
   - Директория: если сертификат хранится на жестком диске, либо на съемном носителе информации. Дополнительно необходимо будет указать путь к папке, в которую будет сохранен сертификат.
   - **USB** ключ: если сертификат сохранен на USB ключе.
2. Указать пароль на сертификат.
3. Нажать на кнопку «Ввод». В том случае, если пароль был указан верно, то данные сертификата будут загружены в систему, в окне «Работа с сертификатом» будут отображены данные сертификата и станет доступна кнопка «Далее». Нажать на кнопку «Далее». Будет открыто окно «Работа с сертификатом. Выбор действия над сертификатом», Рис.31.

[24] Под компрометацией сертификата третьими лицами следует понимать случаи, когда обнаружена пропажа носителя информации, на котором был сохранен сертификат или существует подозрение на то, что сертификат был скопирован. Если сертификат утерян, его замена возможна при наличии резервной копии.

[25] См. раздел Электронный сертификат. Общие сведения.

[26] Порядок запуска операции «Замена сертификата» подробно описан в разделе Открытие окна «Работа с сертификатом».

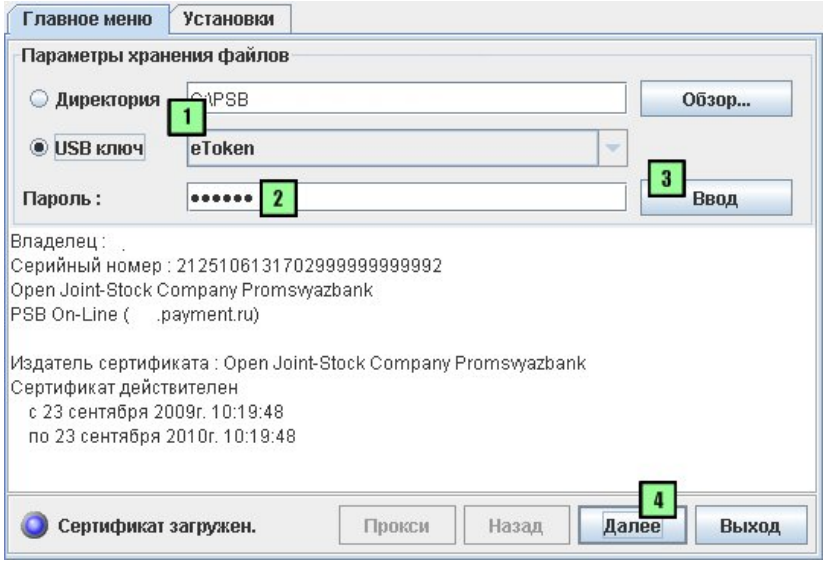

Рис.28 Страница «Работа с сертификатом»

Если используется USB ключ, то будет открыто дополнительное информационное окно «**Message**», Рис.29. В окне «**Message**» следует нажать кнопку «ОК». Будет закрыто окно «**Message**» и открыто окно «Выберите каталог для сохранения файлов заменяемого сертификата» (Рис.30).

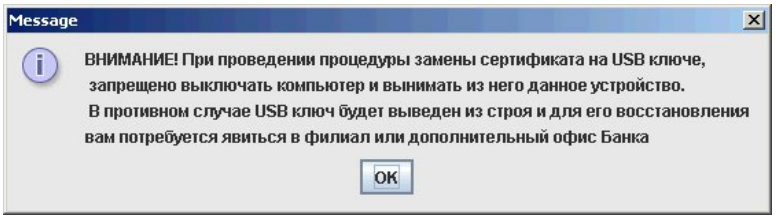

Рис.29 Информационное сообщение

Далее, в окне «Выберите каталог для сохранения файлов заменяемого сертификата» следует:

1. Выбрать директорию для сохранения файла.

> Внимание! Сертификат в каталоге не сохранится. В каталоге будут сохранены временные файлы и печатная форма сертификата.

2. Нажать кнопку «Выбрать». Будет закрыто окно «Выберите каталог для сохранения файлов заменяемого сертификата» и открыто окно «Работа с сертификатом», Рис.31.

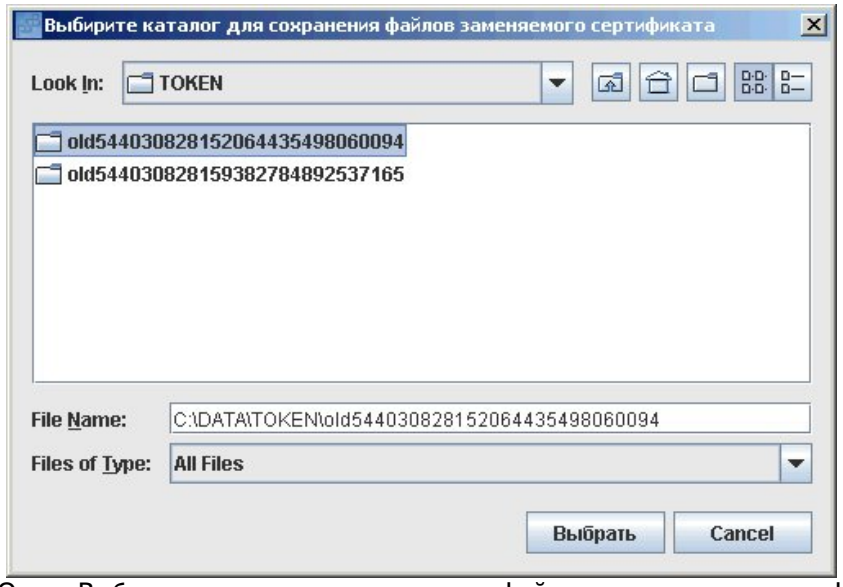

Рис.30 Окно «Выберите каталог для сохранения файлов заменяемого сертификата»

Далее, в окне «Работа с сертификатом» следует:

1. Активировать опцию «Запрос на замену сертификата», Рис.31.
2. Нажать на кнопку «Далее», Рис.31. Будет отправлен запрос на получение нового сертификата и будет доступна кнопка выбора «Получение сертификата», Рис.31.

> **Внимание!** В системе запрос на получение сертификата обрабатывается некоторый промежуток времени (около минуты), после которого следует переходить к этапу получения сертификата.

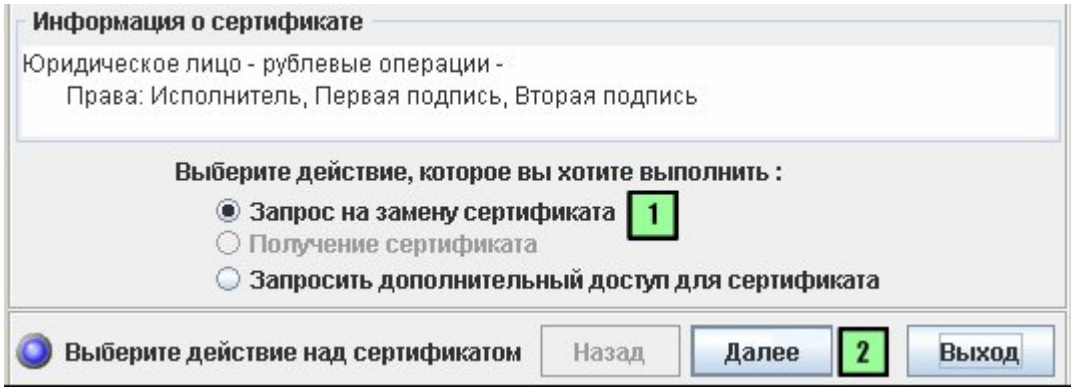

Рис.31 Страница «Работа с сертификатом. Выбор действия над сертификатом»

Далее, в окне «Работа с сертификатом. Выбор действия над сертификатом» следует:

1. Активировать опцию «Получение сертификата», Рис.32.
2. Нажать на кнопку «Далее». В случае если работа производится с файловым сертификатом, будет открыто окно «Изменение пароля», Рис.33.

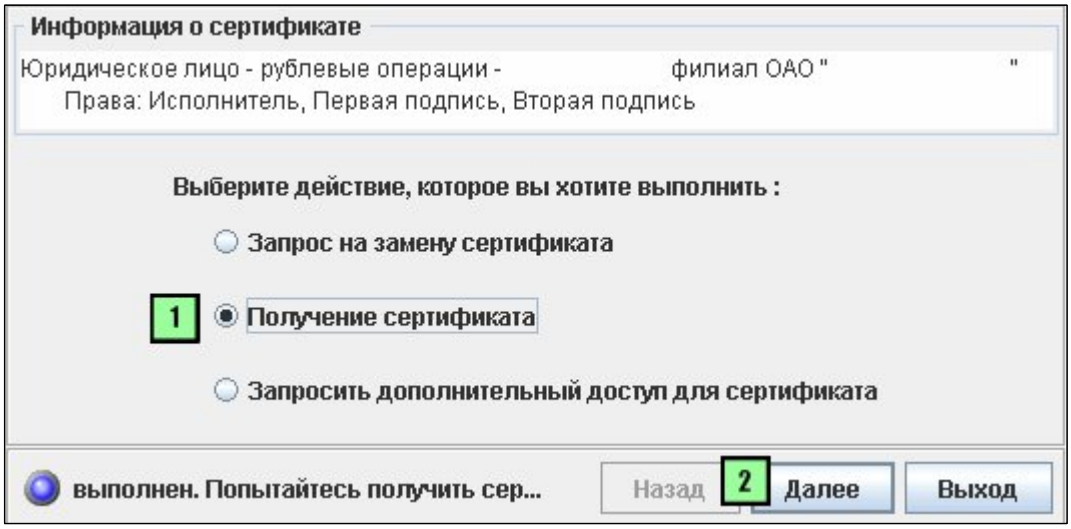

Рис.32 Страница «Работа с сертификатом. Выбор действия над сертификатом»

В этом случае (т.е. при работе с файловым сертификатом) в окне «Изменение пароля» следует выбрать один из вариантов:

- Изменить пароль. В этом случае нажать на кнопку «Да» и указать новый пароль.
- Оставить пароль без изменения. В этом случае нажать на кнопку «Нет», Рис.33.

Будет открыто окно «Работа сертификата. Сертификат сохранен», Рис.34.

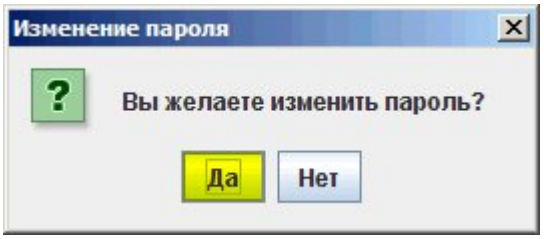

Рис.33 Окно «Изменение пароля»

Далее, в окне «Работа сертификата. Сертификат сохранен» следует нажать на кнопку «Выход», Рис.34. Будет закрыто окно «Работа сертификата. Сертификат сохранен».

> Внимание! По умолчанию новый сертификат будет сохранен в ту папку, в которой ранее хранился замененный сертификат. В свою очередь, замененный сертификат будет перемещен в папку, путь к которой будет отображаться в окне «Работа сертификата. Сертификат сохранен», Рис.34.

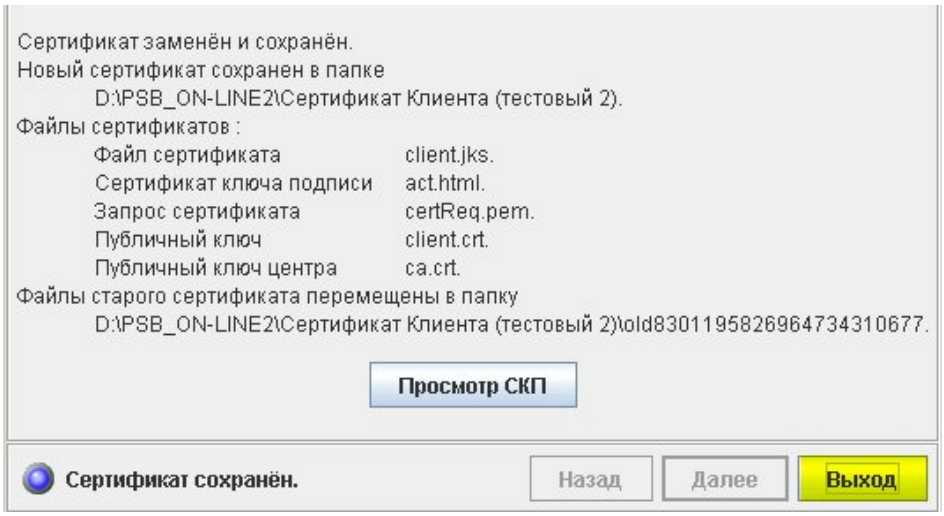

Рис.34 Страница «Работа сертификата. Сертификат сохранен»

3.2.3. Замена сертификата через модуль системы PSB-Online

Замену сертификата с истекающим сроком действия можно произвести также через модуль системы PSB On-line.

Если у владельца сертификата по которому осуществляется вход заканчивается срок действия полномочий, в основном окне системы будет откро информационное окно «Внимание».

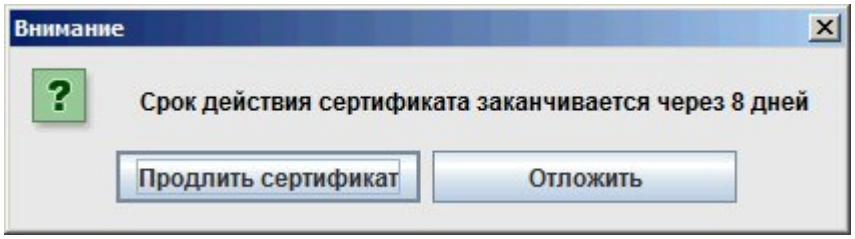

Рис. 35 Информационное окно «Внимание»

Для продления сертификата, в информационном окне «Внимание» следует нажать на кнопку «Продлить сертификат». Будет открыта форма «Работа с сертификатом».

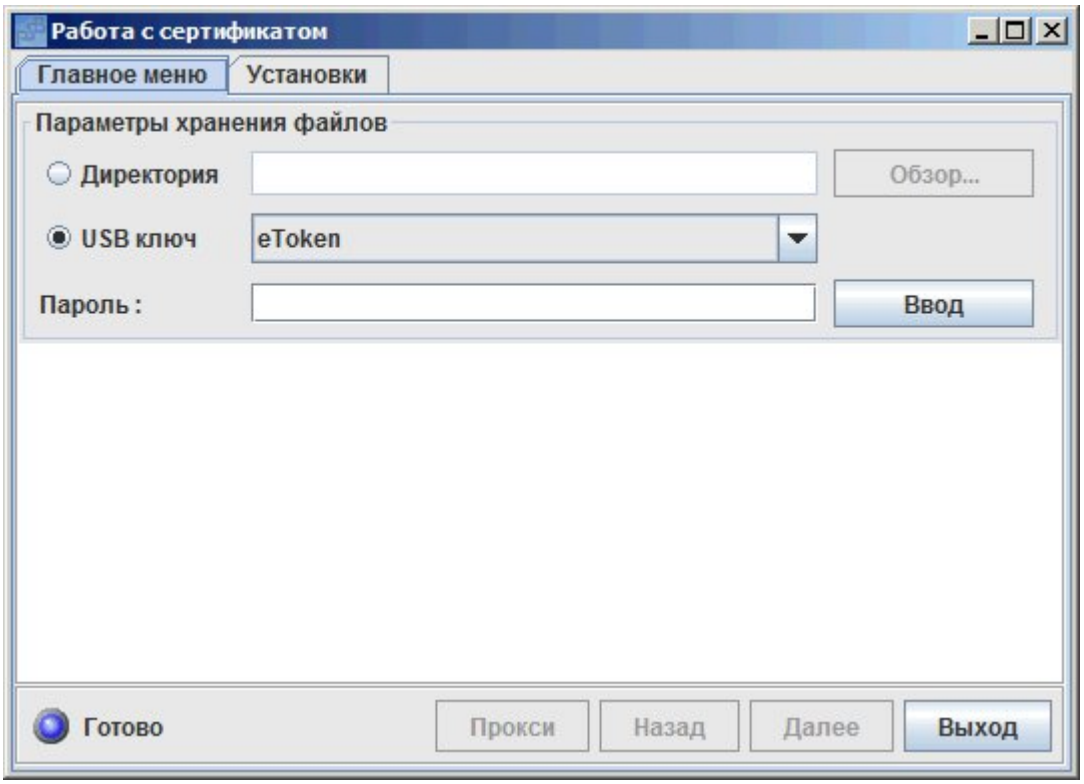

Рис.36 форма «Работа с сертификатом»

3.3 Запрос на дополнительный доступ

3.3.1 Общие принципы

Под запросом на дополнительный доступ следует понимать порядок предоставления прав сертификату клиента на управление счетом[27] дочерней компании.

3.3.2 Оформление операции

Для того чтобы оформить запрос на получение дополнительного доступа, в окне[28] «Работа с сертификатом», следует:

1. Активировать одну из следующих опций:
   - Директория: если сертификат хранится на жестком диске, либо на съемном носителе информации. Дополнительно необходимо будет указать путь к папке, в которую будет сохранен сертификат, Рис.37.
   - **USB ключ:** если сертификат хранится на USB ключе Клиента[29].
2. Указать пароль на сертификат.
3. Нажать на кнопку «Ввод». В том случае, если пароль был указан верно, на экране будут отображены данные сертификата и станет доступна кнопка «Далее».
4. Нажать на кнопку «Далее». Будет открыто окно «Работа с сертификатом. Выбор действия над сертификатом», Рис.38.

---

[27] Открытом ранее в одном из подразделений Банка.

[28] Порядок запуска операции «Запрос на дополнительный доступ» подробно описан в разделе 3.1 Открытие окна «Работа с сертификатом».

[29] Необходимо убедиться в том, что USB ключ подключен к USB порту компьютера.

Примечание: После нажатия на кнопку «Далее», в системе будут обработаны данные о сертификате. Процесс обработки данных может занять некоторое время, по истечении которого будет открыто окно «Работа с сертификатом. Выбор действия над сертификатом».

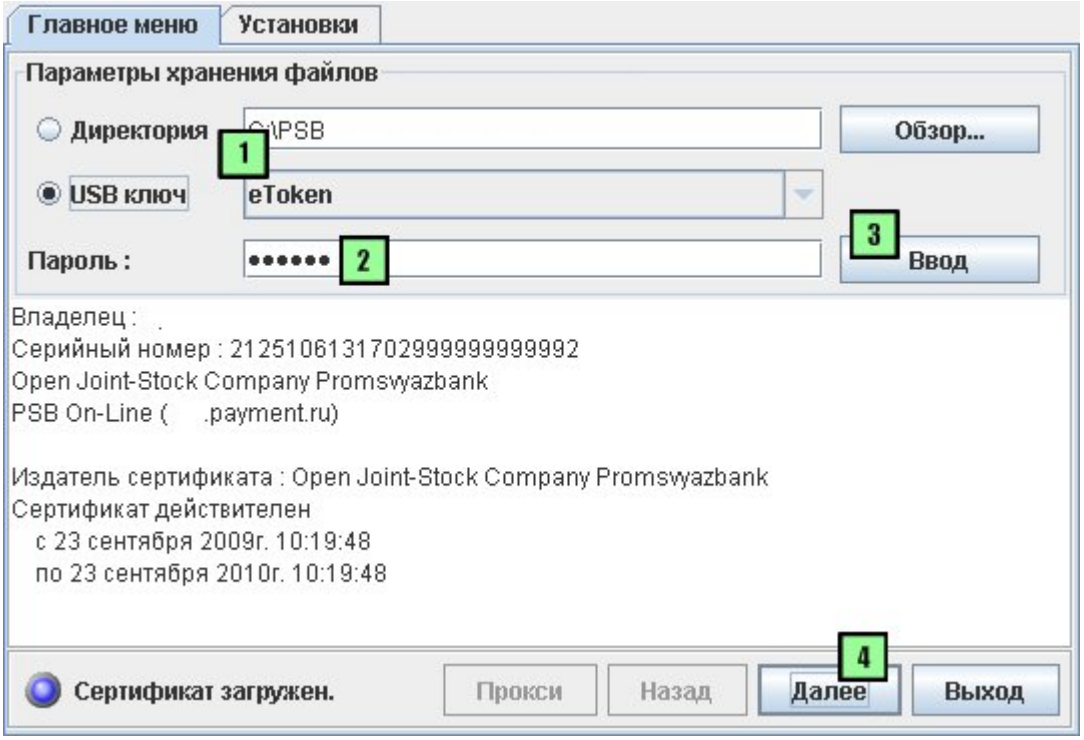

Рис.37 Страница «Работа с сертификатом»

Далее, в окне «Работа с сертификатом. Выбор действия над сертификатом», следует:

1. Активировать опцию «Запросить дополнительный доступ для сертификата».
2. Нажать на кнопку «Далее», Рис.38. Будет открыто окно «Запрос сертификата», Рис.39.

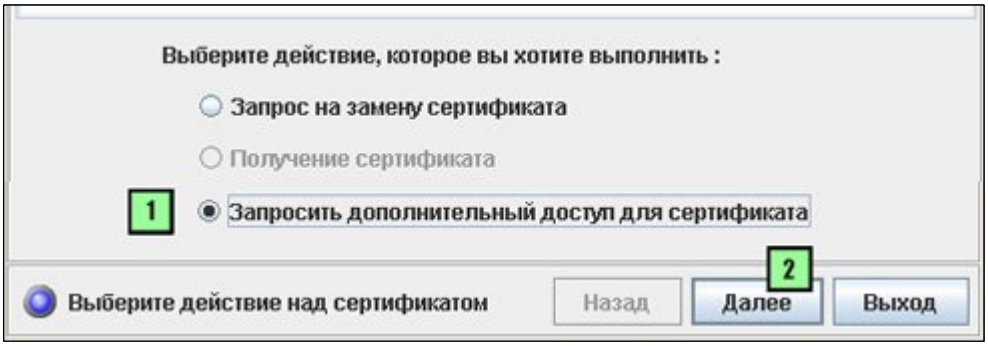

Рис.38 Окно «Работа с сертификатом. Выбор действия над сертификатом»

Далее, в окне «Работа с сертификатом» следует (Рис.39):

1. Выбрать из раскрывающегося списка наименование филиала, в котором открыт счет.
2. Указать номер счета, к которому следует получить доступ.
3. Нажать на кнопку «Далее». В окне «Работа с сертификатом» будет отображена запись о том, что запрос на доступ к счету отправлен, Рис.40.

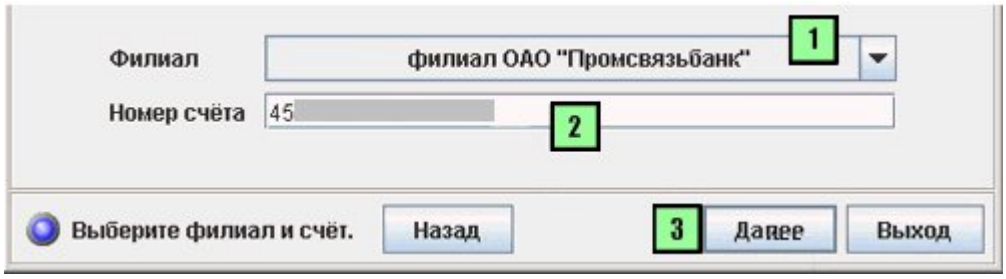

Рис.39 Окно «Работа с сертификатом»

Далее, в окне «Работа с сертификатом», следует нажать на кнопку «Выход», Рис.40. Будет закрыто окно «Работа с сертификатом».

> Примечание: После того как запрос на дополнительный доступ будет отправлен, полномочному представителю Клиента следует явиться в филиал Банка, для того чтобы зарегистрировать[30] СКП и оформить необходимые документы.

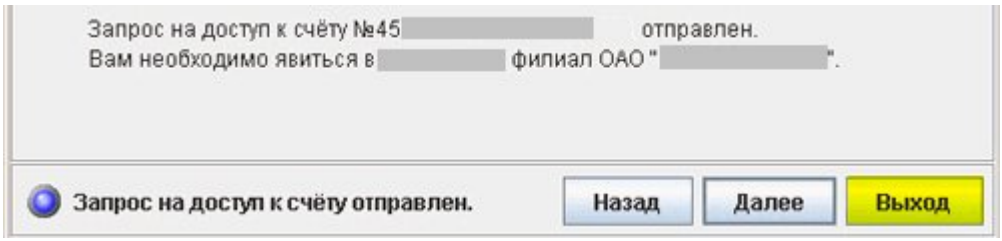

Рис.40 Окно «Работа с сертификатом»

[30] СКП Клиента может быть активирован только после регистрации в том филиале Банка, в котором открыт счет дочерней компании.