## Условия обслуживания банковских счетов юридических лиц и индивидуальных предпринимателей с использованием системы дистанционного банковского обслуживания iBank2 – ЗАО «Аврора Банк» (Условия ДБО)

## 

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

**АБС** –автоматизированная банковская система.

**Авторство документа** – принадлежность документа одной из Сторон Договора на ДБО. Авторство электронного документа определяется принадлежностью Ключа электронной подписи под документом конкретному пользователю Системы ДБО.

**Администратор информационной безопасности Системы ДБО Банка** – работник Банка, обязанности которого связаны с контролем за обеспечением информационной безопасности в Системе ДБО.

**Администратор Системы ДБО Банка** – работник Банка, осуществляющий администрирование Системы ДБО.

**Акт приема–передачи сертификата ключа проверки ЭП** – электронный документ или документ на бумажном носителе, подтверждающий принадлежность ключа проверки ЭП владельцу СКП ЭП. Сертификат включает в себя открытый ключ ЭП, который выдается Банком Клиенту для подтверждения подлинности ЭП и идентификации подписи владельца сертификата открытого ключа ЭП.

**Акта приема–передачи СКЗИ** – документ по форме Банка, в котором фиксируются серийные номера токенов, выданных Клиенту.

**Активный ключ ПЭП Клиента** – ключ проверки электронной подписи Клиента, зарегистрированный Банком в Системе ДБО, и используемый Клиентом в текущее время для работы.

**АРМ** – автоматизированное рабочее место – программно–технический комплекс, установленный на стороне Клиента и подключенный к сети Интернет, предназначенный/используемый для работы с Системой ДБО.

**Безопасность информации (информационная безопасность)** – состояние информации, информационных ресурсов и информационных систем, при которых с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, нарушения доступности, а также обеспечиваются условия неотказуемости.

**Владелец ключа** – Клиент или ответственный сотрудник, которому Клиент делегировал право хранения и использования Ключевого носителя с ЭП от своего имени.

**Группа подписи «Право первой подписи»** – дает возможность проведения любых операций в Системе ДБО, право подписания расчетных (платежных) и официальных документов. Это право предоставляется единоличному исполнительному органу Клиента или иному лицу, действующему от имени Клиента без доверенности, наделенного правом подписи.

**Группа подписи «Право второй подписи»** – дает возможность проводить любые операции в Системе ДБО, право подписания расчетных (платежных) и официальных документов.

**Ключевой документ** – ключевой носитель с ключом электронной подписи.

**Ключевой носитель** – в рамках настоящих правил – USB–токен, со встроенным СКЗИ или использующийся в качестве хранилища СКЗИ и закрытых ключей ЭП.

**Ключ электронной подписи (далее – «Закрытый ключ ЭП»)** – уникальная последовательность символов, предназначенная для создания электронной подписи. Используется для формирования ЭП под финансовыми документами и другими исходящими от Клиента распоряжениями.

**Ключ проверки электронной подписи (далее – «Открытый ключ ЭП»)** – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи. Проверка ЭП клиента осуществляется на стороне Системы ДБО в момент подписи Клиентом документов, а также Шлюзом при выгрузке документов в АБС Банка. Открытые ключи ЭП Клиентов хранятся в Банке в виде Акта приема–передачи сертификата ключа проверки ЭП.

**Блокировочное слово** – слово, определяемое Клиентом лично при оформлении Заявления на ДБО, либо слово, генерируемое программно-аппаратным комплексом Банка и направляемое Клиенту на указанную в Заявлении на ДБО электронную почту, и используемое Клиентом при обращении в Банк лично, по телефону или с использованием других средств связи для:

* прекращения действия Ключа ЭП в Системе. Ввод в Систему Кодового слова означает согласие Клиента с тем, что Банк будет производить прекращение действия соответствующих Ключей на основании обращения;
* идентификации уполномоченного сотрудника Клиента при подтверждении разблокировки сомнительных платежей.

**Корректная ЭП Клиента** – ЭП электронного документа Клиента, дающая положительный результат ее проверки открытым ключом ЭП Клиента.

**Компрометация ключа ЭП** – утрата доверия к тому, что используемые ключи обеспечивают безопасность информации. К событиям, связанным с компрометацией ключей, относятся:

* разглашение или подозрение на разглашение содержания Ключевого документа с ключом ЭП;
* утрата (в том числе – временная) Ключевого документа с ключом ЭП;
* перевод на другую работу или увольнение работников, имеющих доступ к Ключу ЭП и (или) к его ключевому носителю;
* нарушение правил хранения Ключевого документа с ключом ЭП;
* несанкционированное копирование или подозрение в копировании Ключей ЭП;
* возникновение подозрений на утечку конфиденциальной информации или ее искажение;
* несанкционированное нарушение печати на хранилище/сейфе, в котором хранятся Ключевые документы с ключом ЭП;
* случаи, когда нельзя достоверно установить, что произошло с ключевым документом (в том числе, случаи, когда Ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника);
* факт или попытка несанкционированного списания денежных средств со счета Клиента с использованием рабочих ключевых пар;
* иные обстоятельства, прямо или косвенно свидетельствующие о доступе или возможности доступа к содержимому закрытого ключа неуполномоченных лиц.

**Логин** – уникальная последовательность символов, состоящая из латинских букв и цифр, позволяющая Банку однозначно идентифицировать Клиента.

**Пара ключей ЭП Клиента** – закрытый ключ ЭП Клиента и соответствующий ему открытый ключ ЭП Клиента.

**Пароль** – известная только Клиенту последовательность символов, вводимых с клавиатуры компьютера (или без использования клавиатуры за счет средств автоматизации, имитирующих клавиатурный ввод) в целях аутентификации Клиента.

**Персональный аппаратный криптопровайдер (ПАК)** – часть ЭСП, специализированное устройство по защите персональной информации, реализованное в виде USB–токена, обеспечивающего неизвлекаемость (невозможность считывания) ключа ЭП Клиента.

**Проверка ЭП** – проверка с использованием криптографических средств и открытого ключа лица, подписавшего ЭД, принадлежности электронной подписи в электронном документе владельцу указанного ключа подписи и отсутствия искажений в подписанном данной электронной подписью электронном документе.

**Программные средства (ПО)** – программное обеспечение Системы ДБО.

**Система ДБО** – система дистанционного банковского обслуживания iBank2 – ЗАО «Аврора Банк»,представляющая собой комплекс программно–аппаратных средств, устанавливаемых на территории Клиента и Банка, и согласовано эксплуатируемых Клиентом и Банком в соответствующих частях и обеспечивающих подготовку, защиту, передачу Клиентом в Банк электронных документов, обработку Банком электронных документов, формирования Банком и предоставления Клиенту выписок о движении денежных средств и прочих сообщений с использованием электронно–вычислительных средств обработки информации.

**Служба технической поддержки** – подразделения и отдельные специалисты Банка, осуществляющие организационную и техническую поддержку работы клиентов в Системе ДБО.

**Средства авторизации** – совокупность логина и пароля уполномоченного представителя клиента, вводимые им для осуществления входа в системы, позволяющие однозначно идентифицировать физическое лицо осуществившее вход.

**Средства криптографической защиты информации (СКЗИ)** – сертифицированные средства криптографической защиты информации, реализующие хотя бы одну из следующих функций – создание ЭП, проверка ЭП, создание ключа ЭП и ключа проверки ЭП. В рамках настоящих Условий ДБО – встроенная в USB–токен многоплатформенная криптографическая библиотека, сертифицированная ФСБ РФ, используемая для функций криптографической защиты в Системе «Клиент–Банк».

**Уполномоченное лицо Клиента** – руководитель, главный бухгалтер, сотрудник Клиента, уполномоченный распоряжаться счетом Клиента на основании доверенности или распорядительного акта Клиента и включенный в Карточку с образцами подписей и оттиска печати либо Альбом подписей, и одновременно уполномоченные на использование аналога собственноручной подписи (в соответствии с требованиями нормативных актов Банка Абхазии).

**Уполномоченное лицо Банка** – должностное лицо Банка, официально назначенное и уполномоченное на основании доверенности на подписание собственноручной или электронной подписью документов на бумажных носителях и в электронном виде в пределах предоставленных ему полномочий.

**Электронный документ (ЭД)** – документ, в котором информация представлена в электронно–цифровой форме.

**Электронная подпись (ЭП)** – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

1. ОБЩИЕ ПОЛОЖЕНИЯ
   1. Настоящие Условия ДБО регулируют обслуживание Клиента и обмен электронными документами с использованием Системы дистанционного банковского обслуживания iBank2 – ЗАО «Аврора Банк» (далее – Система ДБО) на основании заключенных договоров и в соответствии с Тарифами Банка.
   2. Заключение Договора ДБО оформляется подписанием Клиентом и акцептом Банком Заявления о присоединении к условиям дистанционного банковского обслуживания в системе ДБО (далее – Заявление на ДБО).
   3. Подписание Клиентом Заявления на ДБО означает принятие им настоящих Условий ДБО, Тарифов Банка и обязательство неукоснительно их соблюдать. Договором ДБО является совокупность настоящих Условий ДБО и Заявления на ДБО, надлежащим образом заполненное и подписанное Клиентом.
   4. Договор на ДБО считается заключенным с даты акцепта Банком поданного Клиентом в Банк надлежащим образом оформленного и подписанного Клиентом Заявления или Заявления на ДБО.
   5. Настоящие Условия ДБО устанавливают общие принципы осуществления обмена ЭД между Сторонами, а также взаимные права и обязанности Сторон в связи с осуществлением электронного документооборота между Сторонами, требования по обеспечению безопасности использования СКЗИ, ключевых носителей, ЭП, средств авторизации и меры по их реализации.
   6. Заключая Договор ДБО на обслуживание Клиента по Системе ДБО, Клиент присоединяется к Правилам работы сервиса «iBank2» (размещенным на сайте [https://bk.aurora-bank.com/ibank2/#/](http://https://bk.aurora-bank.com/ibank2/#/)), Стороны Договора признают, что:

* используемые в системе ДБО СКЗИ обеспечивают шифрование, контроль целостности, создание ЭП и достаточны для защиты информации от несанкционированного доступа, подтверждения подлинности и авторства ЭД, а также разрешения конфликтных споров при условии положительного результата проверки ЭП Клиента и Банка. Стороны признают и считают бесспорной идентичность ЭД, подписанных ЭП, документам на бумажном носителе, подписанным уполномоченными представителями Клиента и Банка, подтвержденными печатями и порождающим аналогичную юридическую силу, права и обязанности сторон в рамках заключенными между ними соглашений, дополнительных соглашений к ним, договоров и приложений к ним. Стороны также договариваются не оспаривать законность и действительность указанных документов только на том основании, что они совершены в электронном виде. ЭД без ЭП Клиента не имеют юридической силы, Банком не рассматриваются и не исполняются;
* все ЭД, формируемые в Системе ДБО с использованием СКЗИ подписываются ЭП;
* при произвольном изменении ЭД, содержащего ЭП, становятся некорректными, то есть проверка ЭП дает отрицательный результат и ЭД Банком не принимается к исполнению;
* Ключ проверки ЭП, указанный в заверенном подписью руководителя и оттиском печати Клиента Акте приема–передачи сертификата Ключа проверки ЭП Клиента, принадлежит Клиенту;
* началом действия Ключа ЭП и Ключа проверки ЭП является дата регистрации Клиентом акта приема–передачи сертификата ключа проверки ЭП в Системе ДБО Банка.
* началом действия является дата регистрации Банком логина/пароля Клиента в системе ДБО и момент отправки Логина на адрес электронной почты Уполномоченного представителя Клиента, указанный в Заявлении или в Заявлении на ДБО.
  1. Стороны признают применение СКЗИ и использование ЭП в соответствии с Условиями ДБО достаточными для обеспечения конфиденциальности и целостности информации и невозможности ее фальсификации.
  2. Банк предоставляет Клиенту следующие услуги с использованием Системы ДБО:
* безналичное расчетное обслуживание Клиента, предусмотренное Договором банковского счета с использованием электронных документов;
* обмен служебно–информационными документами между Банком и Клиентом;
* информирование об операциях, совершенных по счетам Клиента, в рамках Системы ДБО;
* прием от Клиента и предоставление Клиенту электронных документов в соответствии с условиями отдельных заключенных Сторонами договоров, которые предусматривают электронный документооборот с использованием Системы ДБО.
  1. Электронные документы, передаваемые со стороны Клиента, включают, но не ограничивают, следующие виды документов:
* платежное поручение;
* запрос выписки по лицевому счету;
* запрос на отзыв документа;
* подтверждение остатков;
* ;
* документы свободного формата, передаваемые Банку.
  1. Электронные документы, передаваемые со стороны Банка, включают, но не ограничивают, следующие виды документов:
* выписки по лицевому счету;
* ;
* справки;
* запрос на подтверждение остатков;
* иные документы (письма, уведомления, акцепты, подтверждения и т.п.).
  1. Основные нормативные документы, регулирующие порядок осуществления операций в рамках данных Условий ДБО:
* Гражданский кодекс Республики Абхазия;
* Закон Республики Абхазия от 15.06.2015 N 3810-с-V "Об электронной подписи" (принят Народным Собранием-Парламентом Республики Абхазия 01.06.2015);
* Закон Республики Абхазия от 02.08.2006 N 1442-с-XIV "Об электронной цифровой подписи в банковской системе" (принят Народным Собранием-Парламентом Республики Абхазия 28.07.2006);
  1. В случае внесения изменений в действующее законодательство РА и Устав Банка, Условия ДБО действуют в части, не противоречащей законодательным актам и Уставу Банка.

1. ПРАВА И ОБЯЗАННОСТИ
   1. **Банк обязуется:** 
      1. До заключения с Клиентом Договора ДБО информировать Клиента об условиях использования Системы ДБО, в том числе о любых ограничениях способов и мест использования, случаях повышенного риска использования Системы ДБО.
      2. После выполнения Клиентом всей совокупности действий, предусмотренных Условиями ДБО и необходимых для осуществления допуска к осуществлению электронного документооборота, обеспечить Клиенту возможность осуществлять электронный документооборот в соответствии с Условиями ДБО.
      3. Организовывать работу Клиенту в Системе ДБО с использованием его ЭП в объеме и в соответствии с порядком, определяемыми Условиями ДБО.
      4. Соблюдать режим конфиденциальности информации, касающийся ключей ЭП , в связи с выполнением Банком своих функций в соответствии с Условиями ДБО.
      5. Предоставить Клиенту необходимое, оплаченное в соответствии с Тарифами Банка, количество ПАК с СКЗИ по Акту приема–передачи СКЗИ. Доставка Клиенту пакетов с ПАК может осуществляться компаниями, специализирующимися на предоставлении услуг по экспресс доставке почтовой корреспонденции и имеющими соответствующие лицензии и соглашения (договоры) с Банком.
      6. Подключить или переподключить Клиента к Системе ДБО с использованием средств ПАК в течение 2 (двух) рабочих дней с момента получения уполномоченным сотрудником Банка полного комплекта необходимых для подключения к Системе ДБО документов.
      7. При подключении или переподключении Клиента к Системе ДБО с использованием средств ПАК проинструктировать Клиента по условиям работы, мерам информационной безопасности и безопасности применения СКЗИ.
      8. Подключить или переподключить Клиента к Системе ДБО в течение 2 (двух) рабочих дней с момента получения уполномоченным сотрудником Банка полного комплекта необходимых для подключения к Системе ДБО документов.
      9. Обеспечивать сохранность и безопасность данных, указанных Клиентом при формировании расчетного (платежного) документа, подписанного ЭП Клиента в Системе ДБО с момента принятия сервером обмена Системы ДБО расчетного (платежного) документа, подписанного ЭП Клиента, т.е. с момента перехода данного расчетного (платежного) документа в состояние «отправлен в Банк». До момента перехода данного расчетного (платежного) документа в состояние «отправлен в Банк» сохранность и безопасность данных, указываемых Клиентом в расчетном (платежном) документе, обеспечивается Клиентом.
      10. Обеспечить сохранность и конфиденциальность данных, обработка которых осуществляется в Системе ДБО, а также архивных данных в течение срока требованиями законодательства РА.
      11. Информировать Клиента о совершении каждой операции в Системе ДБО путем направления Клиенту в соответствии со способом, выбранным Клиентов в Заявлении на ДБО:

* направления сообщения по электронной почте по желанию Клиента – бесплатно,
* SMS – уведомления – по желанию клиента в соответствии с Тарифами Банка,

В случае если Клиентом не определен ни один из указанных способов, информирование осуществляется электронным сообщением по средствам Системы ДБО.

* + 1. По письменному требованию Клиента предоставлять Клиенту документы и информацию, которые связаны с использованием Системы ДБО в рамках Договора ДБО.
    2. Рассматривать заявления Клиента, в том числе при возникновении споров, связанных с использованием Клиентом его электронного средства платежа, а также предоставить Клиенту возможность получать информацию о результатах рассмотрения заявлений, в том числе в письменной форме по требованию Клиента. Рассмотрение Банком заявлений не может превышать сроков, установленных законодательством Российской Федерации для таких заявлений.
    3. При получении требования Клиента о блокировке его работы в Системе ДБО блокировать работу Клиента в Системе ДБО до получения соответствующего письменного уведомления от Клиента о разблокировке.
    4. По письменному требованию Клиента блокировать доступ в Систему ДБО.
    5. Автоматически блокировать доступ уполномоченного представителя Клиента в случае окончания срока действия его полномочий, истечения срока действия сертификата ключа проверки электронной подписи.
    6. Информировать Клиента об изменении либо введении новых Тарифов Банка, порядка и сроков принятия к исполнению ЭД путем размещения информации на стенде объявлений по месту обслуживания Клиента, на официальном сайте Банка <https://www.aurora-bank.com/>, а также посредством рассылки через Систему ДБО не позднее, чем за 10 (Десять) рабочих дней до введения в действие указанных изменений.
    7. В случае приостановки Банком обслуживания Клиента с использованием Системы ДБО согласно условиям настоящих Условий ДБО возобновить обслуживание Клиента с использованием Системы ДБО только после выполнения всех следующих условий:
* личного обращения в Банк физического лица, исполняющего функции единоличного исполнительного органа Клиента (под физическим лицом, исполняющим функции единоличного исполнительного органа Клиента, понимаются физическое лицо, выступающее единоличным исполнительным органом Клиента – юридического лица; одно из физических лиц, исполняющих полномочия единоличного исполнительного органа Клиента – юридического лица, в случае, если полномочия единоличного исполнительного органа предоставлены нескольким физическим лицам; физического лица, выступающего единоличным исполнительным органом юридического лица, которому предоставлены полномочия единоличного исполнительного органа иного юридического лица);
* предоставления выписки из ЕГРЮЛ, подтверждающей актуальность сведений о Клиенте, представителе Клиента, выгодоприобретателе, бенефициарном владельце;
* проведения анализа представленных Клиентом документов, информации, объяснений, в том числе об источниках происхождения денежных средств и (или) иного имущества Клиента, и в совокупности с выполнением иных, установленных настоящим пунктом условий, принятия по результатам рассмотрения положительного решения о возобновлении обслуживания Клиента с использованием Системы ДБО.
  + 1. Выполнять иные обязанности перед Клиентом, возникающие в соответствии с Условиями ДБО.
  1. **Банк имеет право:**
     1. Требовать от Клиента осуществления электронного документооборота в Системе ДБО в соответствии с Условиями ДБО.
     2. В одностороннем порядке вносить изменения и/или дополнения в Условия ДБО, а также прекращать их действие.
     3. При возникновении в Системе ДБО ситуаций, признаваемых форс–мажорными, принимать меры, в соответствии с Условиями ДБО, направленные на преодоление форс–мажорных ситуаций, а также требовать от Клиента совершения действий или воздержания от совершения действий в связи с осуществлением мер, предпринимаемых в соответствии с Условиями ДБО для преодоления форс–мажорных ситуаций.
     4. Определять размер и порядок осуществления оплаты за услуги по дистанционному банковскому обслуживанию Клиента.
     5. В одностороннем порядке расторгнуть Договор ДБО в случае неисполнения или ненадлежащего исполнения Клиентом обязанностей, предусмотренных Условиями ДБО, включая нарушение Клиентом установленного Условиями ДБО порядка урегулирования спорных ситуаций.
     6. Переходить на другие виды средств защиты в связи с изменением технологии работы или другими обстоятельствами.
     7. По своему усмотрению предоставлять полный или ограниченный набор услуг с использованием Системы ДБО в каждом из своих обособленных или внутренних структурных подразделений в конкретный период времени, а также расширять перечень предоставляемых услуг.
     8. Осуществлять иные права, предусмотренные или возникающие в соответствии с Условиями ДБО.
  2. **Клиент обязуется:**
     1. До подписания Заявления на ДБО ознакомиться с Условиями ДБО.
     2. Установить необходимые аппаратные средства, клиентское программное и информационное обеспечение, а также поддерживать их в работоспособном и актуальном состоянии.
     3. Выполнить всю совокупность действий, необходимых для получения допуска к осуществлению электронного документооборота и предусмотренных Условиями ДБО.
     4. Обеспечить сохранность программных средств, Ключей ЭП, а также конфиденциальность одноразовых паролей (кодов), направляемых SMS-сообщениями на номер мобильного телефона Клиента. Клиент обязуется сохранять SIM-карту, за которой закреплен его номер мобильного телефона, указанный в соответствующем Заявлении на ДБО, как фактор аутентификации, обеспечить защиту от вирусов при использовании SIM-карты в смартфонах.
     5. Принять на себя риск убытков, связанных с несанкционированным доступом (в том числе физическим или с использованием вредоносного программного обеспечения) к электронным носителям, куда отправляется личная информация Клиента по системе iBank2
     6. в целях оперативного информирования Банком о проведенных с использованием Системы ДБО операциях, а также предотвращения мошеннических действий в отношении денежных средств Клиента, предоставить Банку в Заявлении на ДБО информацию о подключенном и обслуживаемом номере телефона сотовой (подвижной радиотелефонной) связи и адресе электронной почты, подконтрольных лицу, уполномоченному организацией Клиента на работу в Системе ДБО. В случае указания только номера оператора стационарной (линейно–кабельной) связи Клиент осознает риски, связанные с отсутствием возможности Банка оперативного информирования о работе Системы ДБО, в таком случае Клиент принимает на себя риск убытков, которые у него могут возникнуть в результате неполучения оперативной информации.
     7. Получить необходимое количество ПАК со СКЗИ по Акту приема–передачи СКЗИ.
     8. Создать Пары ключей ЭП Клиента по количеству уполномоченных лиц, самостоятельно на сайте Удостоверяющего центра сформировать закрытый ключ ЭП на Ключевом носителе (ПАК), для активации ЭП клиенту необходимо предоставить в Банк Заявление на выдачу сертификата ключа проверки электронной подписи и Акт приема–передачи сертификата ключа проверки электронной подписи, заверенные подписью и печатью.
     9. Ознакомить с Условиями ДБО своих уполномоченных представителей, зарегистрировавших в Системе ДБО Ключ проверки ЭП.
     10. Заполнять ЭД в Системе ДБО в соответствии с действующими нормативными документами Банка Абхазии, соблюдая форму и правильность заполнения реквизитов документа.
     11. Использовать предоставленные СКЗИ исключительно только в Системе ДБО, без права отчуждения или передачи каким–либо иным способом третьим лицам.
     12. Пользоваться Системой ДБО в соответствии с техническими требованиями, приведенными в Условиях ДБО.
     13. Обеспечить конфиденциальность логинов, паролей и ПАК с Ключами ЭП Клиента, используемыми в Системе ДБО.
     14. В случае досрочного прекращения либо истечения срока полномочий представителя Клиента, зарегистрировавшего в Системе ДБО Ключ проверки ЭП Клиента, обладающего правом подписи расчетных (платежных) документов, сгенерировать новые Пары ключей ЭП Клиента и зарегистрировать новые Ключи проверки ЭП Клиента в Банке на всех своих представителей, обладающих правом подписи расчетных (платежных) документов или представить документы, подтверждающие их право подписи.
     15. В случае расторжения Договора ДБО вернуть Банку средства ПАК и СКЗИ самостоятельно по Акту приема-передачи СКЗИ (по установленной Клиентом форме) одновременно с расторжением Договора ДБО.
     16. Незамедлительно после обнаружения, но не позднее дня, следующего за днем получения от Банка уведомления, предусмотренного п. 3.1.11 Условий ДБО, уведомить Банк об обнаружении любой попытки несанкционированного доступа к электронной Системе ДБО, утраты (хищения) электронного средства платежа и (или) о его использовании без согласия Клиента любым из следующих способов:
* лично в любом удобном для него офисе Банка в соответствии с графиком работы офиса Банка,
* путем направления уведомления в адрес Банка в Системе ДБО,
* лично в Службу технической поддержки по телефонам +7 940 940-04-50 или +7 940 940-04-55.

Все сообщения подтверждаются Кодовым словом на блокировку.

* + 1. Регулярно, не реже одного раза в день, на постоянной основе осуществлять контроль состояния денежных средств на своих счетах путем просмотра информации в Системе ДБО, SMS и почтовых сообщений на телефонном номере и электронной почте, указанных в Заявлении или в Заявлении на ДБО в соответствии с п. 3.1.11 настоящих Условий ДБО.
    2. Регулярно самостоятельно отслеживать поступление информации из Банка по Системе ДБО в разделе «Письма». Информация считается полученной Клиентом по истечению 10 минут с момента ее направления в адрес Клиента.
    3. В случаях утери, кражи, пропажи и иных случаях утраты SIM–карт, телефонов сотовой связи, а также смены SIM–карт или их передачи третьим лицам по любым основаниям, немедленно уведомить об этом Банк. Банк не несет ответственности за предоставление информации неуполномоченным лицам на телефон сотовой связи Клиента, если он не был уведомлен об утере, краже, пропаже и иных случаях утраты SIM–карт такого телефона сотовой связи Клиента.
    4. Регулярно заходить на вебсайт Банка в сети Интернет по адресу <https://www.aurora-bank.com/>с целью ознакомления с Тарифами, изменениями, вносимыми в Условия ДБО, и иными документами, касающимися работы в Системе ДБО.
    5. Оплачивать услуги Банка по обслуживанию Клиента с использованием Системы ДБО согласно Тарифам Банка в порядке, установленном настоящими Условиями ДБО.
    6. Предоставлять Банку по его запросу документы, информацию, объяснения, необходимые для выполнения Банком условий Договора ДБО, и проведения мероприятий, установленных условиями настоящих Условий ДБО и действующим законодательством Российской Федерации. Документы, информация, объяснения должны быть оформлены надлежащим образом и предоставлены Клиентом в полном объеме не позднее 2 (Двух) рабочих дней с даты получения соответствующего запроса Банка.
    7. Осуществлять электронный документооборот в соответствии с Условиями ДБО.
    8. Выполнять организационно–технические требования по обеспечению безопасности информации, установленные Требованиями по обеспечению безопасности использования средств криптографической защиты информации и электронной подписи и меры по их реализации.
    9. Исполнять решения Банка, касающиеся электронного документооборота.
    10. Использовать полученные в Банке программно–технические средства только для целей осуществления электронного документооборота в рамках Системы ДБО, не передавать без письменного согласия Банка данные средства третьим лицам.
    11. Не производить декомпиляцию, модификацию программных средств, не совершать относительно указанных программно–технических средств других действий, нарушающих действующее законодательство РА.
    12. Не совершать действий, способных привести к нарушению целостности Системы ДБО, а также незамедлительно сообщать Банку о ставших известными Клиенту попытках третьих лиц совершить действия, способные привести к нарушению целостности Системы ДБО.
    13. При возникновении в Системе ДБО ситуаций, признаваемых форс–мажорными в соответствии с Условиями ДБО, признавать и исполнять решения, принимаемые уполномоченными органами Банка в соответствии с Условиями ДБО.
    14. Соблюдать порядок урегулирования спорных ситуаций, установленный Условиями ДБО.
    15. Выполнять иные обязанности перед Банком, возникающие в соответствии с Условиями ДБО.
  1. **Клиент имеет право:**
     1. Участвовать в системе электронного документооборота в соответствии с Условиями ДБО.
     2. После выполнения всей совокупности действий, необходимых для осуществления допуска к осуществлению электронного документооборота, получить от Банка возможность осуществлять электронный документооборот в соответствии с Условиями ДБО.
     3. Требовать от Банка организации работы в Системе ДБО с использованием ЭП Клиента в объеме и в соответствии с порядком, определяемым Условиями ДБО.
     4. Досрочно прекратить действие своих Активных ключей проверки ЭП Клиента и потребовать от Банка заблокировать эти ключи.
     5. По своему усмотрению генерировать новые Пары ключей ЭП Клиента и регистрировать в Банке новые Ключи проверки ЭП Клиента.
     6. По своему усмотрению приостановить использование Системы ДБО путем направления в Банк письменного заявления в произвольной форме на бумажном носителе за подписью руководителя Клиента или путем отправки письма по Системе ДБО.
     7. Осуществлять иные права, предусмотренные Условиями ДБО.

1. ОТВЕТСТВЕННОСТЬ СТОРОН
   1. За невыполнение или ненадлежащее выполнение обязательств по Договору ДБО Стороны несут гражданско–правовую ответственность в пределах суммы доказанного реального ущерба, причиненного Стороне невыполнением или ненадлежащим выполнением обязательств другой Стороной.
   2. Ни одна из Сторон не отвечает за неполученные доходы (упущенную выгоду), которые бы получила другая Сторона.
   3. Стороны несут ответственность в соответствии с действующим законодательством Российской Федерации за действия своих сотрудников, а также иных лиц, получивших или имеющих доступ (независимо от того был ли этот доступ прямо санкционирован Стороной или произошел по ее вине) к используемым ими аппаратным средствам, программному, информационному обеспечению, криптографическим ключам и иным средствам, обеспечивающим электронный документооборот в соответствии с Договором ДБО.
   4. Стороны освобождаются от ответственности за частичное или полное неисполнение своих обязательств в соответствии с настоящими Условиями ДБО, если это неисполнение явилось следствием обстоятельств непреодолимой силы (форс–мажор), возникших после присоединения к настоящим Условиями ДБО, или в результате событий чрезвычайного характера, а также сбоев, неисправностей и отказов оборудования, сбоев и ошибок программного обеспечения, сбоев, неисправностей и отказов систем связи, энергоснабжения, кондиционирования и других систем жизнеобеспечения, не позволяющих осуществлять эксплуатацию необходимого для выполнения Договора ДБО оборудования, которые Стороны не могли предвидеть или предотвратить.
   5. В случае возникновения обстоятельств непреодолимой силы срок выполнения Сторонами своих обязательств в соответствии с Договором ДБО отодвигается соразмерно времени, в течение которого действуют такие обстоятельства и их последствия. Сторона, для которой стало невозможным выполнение своих обязательств в виду действия обстоятельств непреодолимой силы, обязана в течение трех календарных дней сообщить другой Стороне о начале и прекращении действия обстоятельств, воспрепятствовавших выполнению договорных обязательств.
   6. Обязанность доказывать существование обстоятельств непреодолимой силы лежит на Стороне, которая ссылается на их действие.
   7. По прошествии обстоятельств непреодолимой силы Стороны обязуются принять все меры для ликвидации последствий и уменьшения причиненного реального ущерба.
   8. В случае форс–мажорных ситуаций Банк незамедлительно информирует (в том числе путем публикации на сайте Банка <https://www.aurora-bank.com/>) Клиента о невозможности направления ему информации по Системе ДБО по совершенным им операциям. Клиент обязан не позднее следующего рабочего дня получить выписки по всем лицевым счетам, в том числе в офисе Банка, при невозможности их получения в Системе ДБО, а Банк обязан предоставить Клиенту запрошенные им выписки по лицевым счетам в Системе ДБО в порядке, установленном Договором ДБО, или в офисе Банка в порядке, установленном Договором расчетного счета.
2. ДОСТУП КЛИЕНТА К СИСТЕМЕ ДБО
   1. Условия доступа Клиента к Системе ДБО
      1. Клиент допускается к осуществлению документооборота в Системе ДБО после выполнения им всей совокупности следующих действий:

* Подписания заявления о присоединении к условиям ДБО (заключения Договора ДБО),
* оплаты комиссий согласно Тарифам Банка,
* соответствия техническим требованиям, предъявляемым к персональному компьютеру Клиента, работающего под операционной системой семейства Windows, указанным на сайте [https://bk.aurora-bank.com/ibank2/#/](http://https://bk.aurora-bank.com/ibank2/#/);
* установки необходимых аппаратных средств, клиентского программного обеспечения и получения ПАК с СКЗИ/Логина и пароля.
  1. Подключение Клиента к Системе ДБО осуществляется в порядке, изложенном в Приложении 3 к настоящим Условиям ДБО.
  2. Ограничения доступа в Систему ДБО и возобновления оказания услуг в Системе ДБО
     1. Банк имеет право ограничить доступ к Системе ДБО Клиенту в следующих случаях:
        1. окончание сроков полномочий лица (лиц), наделенного (наделенных) правом подписи,
        2. смена лица (лиц), наделенного (наделенных) правом подписи,
        3. компрометация закрытого (закрытых) ключей ЭП Клиента,
        4. расторжение Договора банковского счета,
        5. при наличии фактов, свидетельствующих о нарушении Клиентом действующего законодательства РА, нормативных документов Банка Абхазии, требований, установленных Условиями ДБО, а также в случае выявления сомнительных операций Клиента,
        6. издания соответствующих распорядительных документов Банка.
     2. Для возобновления работы в Системе ДБО в случаях, указанных в п. 5.3.1.1, п. 5.3.1.2 Клиенту необходимо:
* представить документы, подтверждающие наличие соответствующих полномочий, сотруднику Банка,
* самостоятельно на сайте [https://bk.aurora-bank.com/ibank2/#/](http://https://bk.aurora-bank.com/ibank2/#/) сформировать закрытый ключ ЭП на Ключевом носителе (ПАК). После завершения процедуры регистрации распечатать Акт приема–передачи сертификата ключа проверки ЭП, и заверить его в установленном порядке подписью и печатью;
* передать сотруднику Банка Акт приема–передачи сертификата ключа проверки ЭП в трех экземплярах на каждую подпись.
  + 1. Для возобновления работы в Системе ДБО в случаях указанных в п. 5.3.1.3, п. 5.3.1.4 Клиенту необходимо:
* самостоятельно на сайте [https://bk.aurora-bank.com/ibank2/#/](http://https://bk.aurora-bank.com/ibank2/#/) сформировать закрытый ключ ЭП на Ключевом носителе (ПАК). После завершения процедуры регистрации распечатать Акт приема–передачи сертификата ключа проверки ЭП и заверить его в установленном порядке подписью и печатью.
* передать сотруднику Банка Акт приема–передачи сертификата ключа проверки ЭП в трех экземплярах на каждую подпись,
  + 1. Для возобновления работы в Системе ДБО в случаях, указанных в п. 5.3.1.5, п. 5.3.1.6, п. 5.3.1.7 Клиенту необходимо обратиться к менеджеру Банка за консультациями.

1. ПОРЯДОК ОБСЛУЖИВАНИЯ КЛИЕНТА
   1. Банк осуществляет прием документов, передаваемых по Системе ДБО, по рабочим дням с 09:00 до 17:30. При невозможности передачи документов в Банк с использованием Системы ДБО, Клиент представляет в Банк документы в виде оригинала на бумажном носителе.
   2. Техническая поддержка Системы ДБО осуществляется в рабочие дни по телефонам через Службу технической поддержки по телефонам +7 940 940-04-50 или +7 940 940-04-55 по графику:

* понедельник – пятница – с 08.00 до 19.00
* суббота, воскресенье – выходной
* в предпраздничные дни – с 09.00 до 18.00

время московское.

* 1. ЭД Клиента, подписанные необходимым количеством ЭП Клиента, считаются доставленными в Банк с момента перехода данного расчетного (платежного) документа в состояние «Принят Банком».
  2. Банк обеспечивает сохранность и безопасность данных, указанных Клиентом при формировании расчетного (платежного) документа, подписанного ЭП Клиента в Системе ДБО с момента принятия сервером обмена Системе ДБО расчетного (платежного) документа, подписанного ЭП Клиента, т.е. с момента перехода данного расчетного (платежного) документа в состояние «Принят Банком». До момента перехода данного расчетного (платежного) документа в состояние «Принят Банком» сохранность данных, указываемых Клиентом в расчетном (платежном) документе, обеспечивается Клиентом.
  3. Документы, передаваемые Клиентом и принятые Банком по Системе ДБО, исполняются Банком в сроки, установленные Тарифами Банка.
  4. Банк осуществляет обработку расчетных (платежных) документов, переданных в Банк по Системе ДБО, согласно условиям настоящих Условий ДБО, банковским правилам и требованиям действующего законодательства РА.
  5. При поступлении ЭД Банк производит проверку корректности ЭП Клиента, проверку правильности заполнения реквизитов ЭД, проверку на возможность возникновения дебетового сальдо на Расчетном счете Клиента. Электронный документ, содержащий некорректную информацию как в части реквизитов, так и в части платежа, Банком к исполнению не принимается, о чем Клиенту в обязательном порядке направляется уведомление.
  6. Банк фиксирует направленные Клиенту и полученные от Клиента уведомления, а также хранит соответствующую информацию не менее пяти лет с момента отправки/получения.
  7. Использование Клиентом Системы ДБО может быть приостановлено или прекращено Банком на основании полученного от Клиента уведомления или по инициативе Банка при нарушении Клиентом порядка использования Системы ДБО, а также по иным основаниям, установленным настоящими Условиями ДБО.
  8. Приостановление или прекращение работы Клиента в Системе ДБО не прекращает обязательств Клиента и Банка, возникших до момента приостановления или прекращения указанного использования.

1. ПОРЯДОК ОБРАБОТКИ ДОКУМЕНТОВ В СИСТЕМЕ ДБО
   1. Требования, предъявляемые к электронному документу
      1. Стороны признают, что переданные Клиенту/Банку по Системе ДБО Электронные документы (в том числе как вложение в сообщения свободного формата), предусмотренные Условиями ДБО, [подписанные](http://msksdo11.vtb/C32571570040221C/0/00C16CCE354E4D9844257A320047BF66/$file/390_2012Н_1.doc/#p_2_pril_1_390_2012) ЭП , являются эквивалентными подобным документам на бумажных носителях, имеют равную им юридическую силу, влекут аналогичные им права и обязанности Сторон и не требуют дополнительного дублирования на бумажном носителе.
      2. Электронный документ, используемый в Системе ДБО, считается надлежащим образом оформленным при условии соответствия действующему законодательству РА, нормативным документам Банка Абхазии и требованиям, установленным Условиями ДБО.
      3. Электронный документ, не отвечающий требованиям, установленным Условиями ДБО в качестве электронного документа, не рассматривается (исключение составляет документооборот между Банком и Клиентом электронными письмами (сообщениями).
   2. Использование ЭП в электронном документообороте
      1. Электронные документы с ЭП принимаются к исполнению при выполнении условий для признания юридического значения электронной подписи.
      2. Электронный документ считается подписанным уполномоченным лицом, если он подписан с использованием закрытого ключа ЭП, для которого изготовлен сертификат открытого ключа ЭП.
      3. Замена закрытых и открытых ключей ЭП не влияет на статус электронного документа, если он был подписан действующим на момент подписания закрытым ключом ЭП в соответствии с Условиями ДБО.

ЭП Клиента используется в качестве аналога собственноручной подписи.

* 1. Порядок работы в Системе ДБО
     1. После идентификации Клиента в Системе ДБО он получает доступ к Системе ДБО и начинает работу в ней.
     2. Клиент заполняет или редактирует формы ЭД в формате, определенном в экранной форме клиентской части Системы ДБО, и заверяет созданные ЭД своей (своими) ЭП. ЭП подтверждает авторство созданного в Системе ДБО электронного документа и является средством проверки неизменности его содержания, так как любое изменение ЭД после заверения его ЭП нарушает целостность ЭП.
     3. Электронный документ должен быть заверен ЭП лица (лиц) в соответствии с действующей Карточкой с образцами подписей и оттиска печати либо в соответствии с Соглашением о количестве и сочетании электронных подписей лиц в случае, если Клиентом Карточка с образцами подписей и оттиска печати не оформлялась. При наличии нескольких подписей в Карточке с образцами подписей и оттиска печати/Соглашении о количестве и сочетании электронных подписей, документ заверяется ЭП в соответствии со списком лиц, наделенных правом подписи. Клиентом дополнительно может быть установлена иная процедура заверения электронных документов ЭП в соответствии с условиями, установленными договором на отдельные продукты Банка.
     4. Клиент фильтрует и просматривает по датам выписки и платежные поручения, следит за исходящим и входящим остатком на счете, просматривает обороты по дебету и кредиту за выбранную им дату.
     5. Система автоматически отображает сведения о текущем этапе обработки Клиентом и/или Банком Электронного документа посредством присвоения Электронному документу определенного статуса в Системе ДБО.
     6. Система присваивает электронным документам следующие статусы:
* **Новый**. Присваивается при создании и сохранении нового документа, при редактировании и сохранении существующего документа, а также при импорте документа из файла. Документ со статусом **Новый** не рассматривается и не обрабатывается на банковской стороне.
* **Подписан.** Присваивается в случае, если документ подписан, но число подписей под документом недостаточное для отправки в банк документа. При внесении изменений в документ с таким статусом и его последующем сохранении статус документа меняется на **Новый.**
* **Требует подтверждения.** Присваивается платежному поручению после получения необходимого количества подписей в случае использования на банковской стороне дополнительных мер защиты документа. Если на банковской стороне используется механизм подтверждения платежных поручений, то для доставки в банк такого документа клиенту необходимо указывать код подтверждения. Код подтверждения может быть сгенерирован MAC-токеном BIFIT, МАС-токеном, OTP-токеном, или получен в SMS-сообщении на номер, зарегистрированный в банке.
* **Доставлен.** Присваивается документу, когда число подписей под документом соответствует необходимому для рассмотрения документа на банковской стороне. Статус **Доставлен** является для банка указанием начать обработку документа (исполнить или отвергнуть).
* **На обработке.** Присваивается при принятии документа в банке на обработку.
* **На исполнении**. Присваивается при принятии документа в банке на исполнение.
* **В картотеке**. Присваивается платежному поручению при недостаточности средств на счете клиента (см. раздел Отчет «Картотека»). При поступлении средств на счет клиента деньги списываются в соответствии с очередностью платежа, установленной в платежном поручении. При этом для проведения таких списаний формируются платежные ордера. Если была произведена частичная оплата, то статус **В картотеке** отображается на форме документа в виде ссылки, при нажатии на которую открывается диалог **Частичная оплата.**
* **Исполнен.** Присваивается документу при исполнении документа на банковской стороне и проведении в балансе проводкой. Для документов в статусе **Исполнен** в разделе **Настройки** задается количество дней, за которое отображаются соответствующие документы.
* **Отвергнут.** Присваивается документу, не принятому на банковской стороне к исполнению. Можно или отредактировать и сохранить документ (статус изменится на **Новый**), или удалить документ (статус изменится на **Удален**). Возможность редактирования отвергнутых документов определяется настройками на стороне банка.
* **Удален.** Присваивается документу, удаленному пользователем. Удалению подлежат только документы в статусе **Черновик, Новый, Подписан** или **Отвергнут**. Документы в статусе **Черновик, Новый** и **Подписан** удаляются безвозвратно. Документы, удаленные после отвержения, можно просмотреть, используя фильтр. Количество дней, за которое отображаются удаленные документы, задается в разделе **Настройки.**
* **На акцепт.** Присваивается платежному поручению или заявлению на перевод в случаях нарушения правил контроля, заданных центром финансового контроля. Статус также присваивается, если установлено принудительное акцептование центром финансового контроля всех документов подчиненной компании.
  + 1. Информация, переданная Банком Клиенту по Системе ДБО, считается доведенной до сведения Клиента по истечении 1 (одного) рабочего дня с момента ее передачи Банком (начиная с даты передачи информации) в том составе и в том виде, в котором ее передал Банк, независимо от фактического восприятия такой информации Клиентом. Клиент обязан с периодичностью не реже одного рабочего дня осуществлять просмотр информации, переданной ему Банком по Системе ДБО, или получать выписки по всем лицевым счетам в порядке, установленном Условиями ДБО. Клиент признает, что Банк информирует его об исполнении Банком электронного документа посредством автоматического отображения сведений в Системе ДБО о текущем статусе каждого электронного документа. Банк вправе использовать дополнительные способы информирования Клиента об исполнении Банком электронного документа в порядке, установленном Условиями ДБО.
    2. После отправки Клиентом ЭД и проверки ЭП Системой ДБО ЭД присваивается статус «Доставлен в Банк». В случае если статус «Доставлен в Банк» для ЭД не меняется в течение 2 часов на статус «Принят Банком» Клиенту необходимо обратится в Службу технической поддержки для устранения ошибки в отправленном, но не обработанном Банком ЭД.
    3. Банк осуществляет проверку ЭД и принимает его к исполнению при условии положительного результата проверки.
    4. Результат проверки ЭД считается положительным, если ЭД оформлен в соответствии с:
* действующим законодательством РА,
* нормативными документами Банка Абхазии,
* требованиями, установленными настоящими Условиями ДБО,

и заверен надлежащей (надлежащими) ЭП, прошел в Банке проверку корректности ЭП.

* + 1. ЭД, оформленные с нарушением требований, приему не подлежат. Таким ЭД присваивается статус «Возвращен».
    2. Порядок предоставления выписки по счету и приложений к ней Клиенту, подключенному к Системе ДБО:
* выписка по счету формируется Банком на следующий банковский день после осуществления операций в Системе ДБО,
* Клиент получает выписку и приложения к ней (платежные документы) по счету в электронном виде по Системе ДБО путем запроса в Системе ДБО за период, начиная со дня подключения Банком Клиента к Системе ДБО по текущую дату,
* Клиент признает, что Банк предоставляет ему выписку с приложениями по счету в электронном виде по Системе ДБО,
* в случае если Клиенту, подключенному к Системе ДБО, необходимо получить выписку и приложения к ней на бумажном носителе, то данная выписка с приложениями считается дубликатом.
  + 1. Документооборот за день в Системе ДБО архивируется Банком ежедневно на следующий рабочий день. Банк и Клиент обязуются хранить архив документооборота по Системе ДБО в течение пяти лет с даты, следующей за датой отправки ЭД.
  1. Порядок документооборота с использованием почтовых ящиков в Системе ДБО
     1. Документооборот электронными письмами (сообщениями) в Системе ДБО осуществляется через почтовые ящики, созданные Банком для маршрутизации информации между Клиентом и профильными подразделениями Банка в целях оперативной обработки данных.
     2. Электронное письмо, отправленное Клиентом на соответствующий адрес почтового ящика, будет обработано сотрудником Банка в случае соответствия темы и содержания электронного письма назначению почтового ящика.
     3. Отправленным по Системе ДБО некорректным электронным письмам Банк присваивает статус «Возвращен».
     4. Под некорректными письмами, отправленными Клиентом по Системе ДБО в Банк, считаются следующие письма:
* без указания темы сообщения,
* несоответствие темы сообщения назначению почтового ящика,
* несоответствие темы сообщения содержанию письма.
  + 1. Создание нового письма осуществляется путем нажатия кнопки «Создать». Для направления письма в определенное подразделение Банка необходимо выбрать соответствующий наименованию подразделения пункт в разделе «Получатель»
    2. В письме могут содержаться вложенные файлы: ведомости, приложения к расчетным документам и другие документы установленной Банком формы, общий размер которых не должен превышать 5,0 Мб.
  1. Порядок информирования Клиента об операциях в Системе ДБО
     1. Банк уведомляет Клиента об этапах и результатах обработки ЭД, подготовленных с использованием Системы ДБО, путем предоставления информации через Систему ДБО в соответствии с п. 7.3.5 настоящих Условий ДБО.
     2. Клиент, в свою очередь, обязан по рабочим дням (в соответствии с законодательством РА) до момента получения информации об исполнении либо об отказе в исполнении ЭД, но не позднее чем в течение 24 часов с момента отправки ЭД в Банк, отслеживать информацию об этапах и результатах обработки в разделах Системы ДБО, предназначенных для подготовки и хранения соответствующих ЭД.
     3. Ответственность за риски, возникающие в случае отсутствия или несвоевременного контроля Клиентом за результатами обработки ЭД, несет Клиент.
     4. Клиент признает надлежащим уведомление об этапах и результатах обработки ЭД, подготовленных с использованием Системы ДБО, направляемых Банком в соответствии с п. 7.3.5 настоящих Условий ДБО.
     5. О положительном результате всех предусмотренных законодательством и договорами, заключенными между Банком и Клиентом, процедур приема расчетных ЭД (распоряжений) к исполнению и о приеме ЭД к исполнению Банк информирует Клиента одновременно с направлением ему уведомления об исполнении расчетного ЭД. Об исполнении Банком расчетного ЭД Банк уведомляет Клиента посредством направления ему по Системе ДБО выписки по счету, а также SMS–уведомления (согласно Тарифам, установленным Банком) и/или ЭС по электронной почте, на адреса и телефонный номер, указанные в Заявлении или в Заявлении на ДБО.
     6. Об отрицательном результате процедур приема расчетных ЭД к исполнению, об отказе в исполнении, Банк информирует Клиента путем перевода ЭД в статус «Отвергнут».
     7. Сроки направления уведомлений/извещений определяются в соответствии с законодательством и заключенными между Сторонами договорами банковского счета.
     8. Клиент признает надлежащим уведомление о совершении операций с использованием Системы ДБО, направляемое Банком в соответствии с настоящими Условиями ДБО.
     9. Банк не несет ответственности перед Клиентом в случае, если Клиент не получил указанное в п. 7.5.9 ЭС/SMS–сообщение, либо получил данное ЭС/SMS –сообщение с задержкой по времени, а также в случае если ЭС/SMS – сообщение было ошибочно направлено иному получателю, либо Клиенту ошибочно поступило ЭС/SMS –сообщение, адресованное иному получателю, если данные обстоятельства произошли в связи с техническими сбоями, а также по иным причинам, не зависящим от Банка.
  2. Стоимость услуг и порядок расчетов
     1. За установку и обслуживание Системы ДБО с Клиента взимается плата в соответствии с Тарифами Банка.
     2. Банк вправе без распоряжения Клиента осуществлять списание с Расчетного счета Клиента суммы причитающихся Банку комиссий по Договору ДБО. Клиент согласен с данным положением Условий ДБО и предоставляет Банку право списывать комиссии с расчетного счета Клиента без распоряжения Клиента (на условиях заранее данного акцепта).
     3. Размер платы за подключение или переподключение Клиента к Системе ДБО устанавливается согласно действующим на момент подключения или переподключения Тарифам Банка, и взимается Банком единовременно путем списания денежных средств с Расчетного счета(ов) Клиента в Банке не позднее следующего рабочего дня за днем заключения Клиентом Договора ДБО. При этом Клиент безусловно акцептует списание денежных средств согласно настоящему пункту Условий ДБО.
     4. Размер платы за возобновление оказания Клиенту услуг по использованию Системы ДБО после приостановления оказания услуг по инициативе Клиента устанавливается согласно действующим Тарифам Банка на момент возобновления (подключения) и взимается Банком единовременно путем списания денежных средств с Расчетного счета(ов) Клиента в Банке не позднее следующего рабочего дня за днем заключения Клиентом Договора ДБО. При этом Клиент безусловно акцептует списание денежных средств согласно настоящему пункту Условий ДБО (заранее данный Клиентом акцепт).
     5. Клиент обязан обеспечить наличие денежных средств на счете(ах) Клиента в Банке в размере, достаточном для оплаты услуг Банка по настоящим Условиям ДБО в полном объеме согласно действующим Тарифам Банка.
     6. Банк имеет право в одностороннем порядке:
* ограничить доступ Клиента к Системе ДБО и приостановить оказание услуг в рамках Договора ДБО в случаях, предусмотренных п. 5.4.1 настоящих Условий ДБО без возмещения оплаты за время ограничения доступа, приостановки оказания услуг или в случае досрочного расторжения Договора ДБО,
* приостановить оказание платных услуг в Системе ДБО в случае отсутствия или недостаточности на дату оплаты на счете(ах) Клиента в Банке необходимых денежных средств или если Клиент не осуществил оплату данной услуги Банка иным способом в установленные для оплаты сроки,
* возобновить оказание услуг в рамках Договора ДБО при выполнении условий предоставления и наличия оснований, предусмотренных настоящими Условиями ДБО, а также после погашения задолженности Клиента перед Банком за предоставленные платные услуги.
  + 1. Незнание Клиента об изменении либо введении новых Тарифов Банка, порядка и сроков принятия к исполнению ЭД, когда Клиент не ознакомился с информацией, размещенной Банком на информационном стенде в помещении Банка, либо на официальном сайте Банка, либо в рассылке через Систему ДБО, не освобождает Клиента от уплаты соответствующих сумм согласно действующим на момент проведения операции Тарифам Банка. Клиент согласен, что при совершении им операций по счету на основании полученного Банком ЭД после изменения либо введения новых Тарифов Банка плата за предоставляемые Банком услуги будет взиматься в размере, установленном Тарифами Банка, действующими на день совершения операции.

1. СРОК ДЕЙСТВИЯ ДОГОВОРА ДБО
   1. Договор ДБО вступает в силу с даты акцепта Банком поданного Клиентом в Банк надлежащим образом оформленного и подписанного Клиентом Заявления на ДБО и действует неопредленное время.
   2. Договор ДБО может быть расторгнут по обоюдному согласию Сторон.
   3. Каждая Сторона имеет право в одностороннем внесудебном порядке расторгнуть Договор ДБО при условии исполнения Сторонами своих обязательств в соответствии с настоящими Условиями ДБО.
   4. Сторона, изъявившая желание расторгнуть Договор ДБО, обязана уведомить другую Сторону об этом не позднее чем за 10 (десять) календарных дней до предполагаемой даты расторжения Договора ДБО путем направления:

* соответствующего со стороны Банка уведомления,
* со стороны Клиента письменного заявления в произвольной форме, подписанного должным образом уполномоченными представителем (представителями) соответствующей Стороны о таком расторжении.
  1. Договор ДБО прекращается в случае закрытия всех счетов Клиента, открытых в Банке, обслуживание которых осуществлялось с использованием Системы ДБО в рамках Договора ДБО.
  2. Договор на ДБО может быть расторгнут Клиентом в одностороннем внесудебном порядке при условии оплаты Банку услуг по Договору ДБО.
  3. Договор на ДБО может быть расторгнут Банком в одностороннем внесудебном порядке при использовании Клиентом Системы ДБО не по прямому назначению.

1. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ
   1. В случае возникновения между Сторонами спорных ситуаций по Договору ДБО, Стороны предпримут все меры для их разрешения путем переговоров.
   2. Банк рассматривает заявления Клиента, в том числе при возникновении споров, связанных с использованием Клиентом его электронного средства платежа, а также предоставляет Клиенту возможность получать информацию о результатах рассмотрения заявлений, в том числе в письменной форме по требованию Клиента, в срок не более 30 дней со дня получения таких заявлений, а также не более 60 дней со дня получения заявлений в случае использования электронного средства платежа для осуществления трансграничного перевода денежных средств. Все заявления Клиента Банком регистрируются.
   3. Разногласия, возникающие между Сторонами в процессе выполнения Договора ДБО, рассматриваются Сторонами для достижения взаимоприемлемых решений с обязательным соблюдением досудебного претензионного порядка урегулирования спора в соответствии с «Положением о порядке проведения технической экспертизы при возникновении спорных ситуаций».
   4. При недостижении соглашения по вопросам, вытекающим из Договора ДБО, споры рассматриваются в Арбитражном суде РА.
   5. Клиент не вправе уступать третьим лицам права и обязанности по Договору ДБО.
   6. Если Сторонам не удастся разрешить спорные ситуации путем переговоров, совместным решением обеих Сторон создается комиссия из уполномоченных представителей Сторон с равным количеством членов комиссии с каждой Стороны.
   7. Претензия предъявляется соответствующей Стороной в письменной форме путем официального вручения с проставлением отметки в получении другой Стороне или направления по почте заказным письмом с уведомлением о вручении. Претензия оформляется со стороны Клиента по форме, утвержденной в Банке, со стороны Банка – в произвольной форме.
   8. Получив претензию соответствующая Сторона официально в письменной форме информирует другую Сторону о результатах ее рассмотрения в течение 5 (Пяти) рабочих дней с даты получения претензии.
   9. Сторона, предъявившая претензию, в течение 5 (Пяти) рабочих дней после получения результатов рассмотрения претензии от другой Стороны должна рассмотреть представленные объяснения и письменно уведомить другую Сторону о снятии претензии или о несогласии с представленными объяснениями.
   10. Если Сторона не согласна с представленными объяснениями, Стороны обязаны в течение 5 (Пяти) рабочих дней с даты уведомления о несогласии сформировать комиссию для рассмотрения и разрешения указанного спора по существу.
   11. До передачи спора на рассмотрение комиссии Сторонам следует удостовериться, что причиной возникновения спора не является нарушение целостности программного обеспечения, произошедшее в результате сбоев аппаратуры, воздействия компьютерных вирусов, в том числе полученных через Интернет, а также не соблюдение настоящих Условий ДБО.
   12. В случае уклонения одной из Сторон от принятия решения по претензии, другая Сторона вправе самостоятельно привлечь экспертов, указанных в п. 9.10 настоящих Условий ДБО, для разрешения конфликтной ситуации.
   13. Комиссия проводит техническую экспертизу спорных ситуаций.

Приложение № 1 к Условиям обслуживания банковских счетов

с использованием системы дистанционного банковского обслуживания iBank2 – ЗАО «Аврора Банк»

**Требования по обеспечению безопасности использования средств криптографической защиты информации и электронной подписи и меры по их реализации к Условиям дистанционного банковского обслуживания iBank2 – ЗАО «Аврора Банк»**

1. **Требования к организации режима обеспечения безопасности помещения, в котором эксплуатируется СКЗИ и применяется ЭП**
   1. Клиентом должны быть приняты меры по исключению несанкционированного доступа посторонних лиц (включая и собственных сотрудников, не имеющих допуск к работе) в помещение, в котором осуществляется хранение ключей ЭП и размещены СКЗИ.
   2. В случае необходимости присутствия посторонних лиц в указанном помещении должен быть обеспечен контроль их действий во избежание негативных воздействий с их стороны на ключи ЭП, средства криптографической защиты информации и передаваемую информацию.
   3. Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключи ЭП.
2. **Требования по защите информации от несанкционированного доступа к СКЗИ, общесистемному и специальному программному обеспечению АРМ**
   1. Необходимо разработать и применить политику назначения и смены паролей (для входа в операционную систему, BIOS и т.д.) в соответствии со следующими правилами:

* длина пароля должна быть не менее 6 символов;
* в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, \*, % и т.п.);
* пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов, даты рождения и т.д.), а также сокращения (USER, ADMIN, root, и т.д.);
* при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;
* личный пароль Клиент (Владелец ключа ЭП) не имеет права никому сообщать;
* периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 90 календарных дней.
  1. При использовании ключей ЭП АРМ должен быть сконфигурирован с учетом следующих требований:
* не использовать нестандартные, измененные или отладочные версии операционных систем;
* исключить возможность загрузки и использования операционной системы, отличной от предусмотренной штатной работой;
* исключить возможность удаленного управления, администрирования и модификации операционной системы и ее настроек;
* на АРМ должна быть установлена только одна лицензионная операционная система;
* все неиспользуемые сетевые компоненты системы необходимо отключить (протоколы, сервисы и т.п.);
* режимы безопасности, реализованные в операционной системе, должны быть настроены на максимальный уровень;
* необходимо предусмотреть меры, максимально ограничивающие доступ к ресурсам системы (в соответствующих условиях возможно полное удаление ресурса или его неиспользуемой части):
* системному реестру;
* файлам и каталогам;
* временным файлам;
* журналам системы;
* файлам подкачки;
* кэшируемой информации (пароли и т.п.);
* отладочной информации.
  1. АРМ необходимо использовать в однопользовательском режиме. В отдельных случаях, при необходимости использования АРМ несколькими лицами, эти лица должны обладать равными правами доступа к информации.
  2. Администрирование АРМ должно осуществляться доверенными лицами.
  3. Программное обеспечение, используемое на АРМ, не должно содержать возможностей, позволяющих:
* модифицировать содержимое произвольных областей памяти;
* модифицировать собственный код и код других подпрограмм;
* модифицировать память, выделенную для других подпрограмм;
* передавать управление в области собственных данных и данных других подпрограмм;
* несанкционированно модифицировать файлы, содержащие исполняемые коды при их хранении на жестком диске;
* повышать предоставленные привилегии;
* модифицировать настройки операционной системы;
* использовать недокументированные фирмой–разработчиком функции операционной системы.
  1. На АРМе необходимо:
* исключить попадание в систему программ, позволяющих использовать ошибки операционной системы, для повышения предоставленных привилегий;
* регулярно устанавливать пакеты обновлений безопасности операционной системы, обновлять антивирусные базы, а также исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий.
  1. При подключении АРМ к общедоступным сетям передачи данных необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов, полученных с ресурсов или с использованием общедоступных сетей передачи данных (в том числе Интернет), без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети. С целью исключения возможности несанкционированного доступа к системным ресурсам АРМ, в окружении которых функционируют СКЗИ, со стороны указанных сетей, должны использоваться дополнительные методы и средства защиты (например, установка межсетевых экранов, организация VPN–сетей и т.п.). Все средства защиты, должны иметь сертификат уполномоченного органа по сертификации средств защиты.
  2. Необходимо организовать и использовать:
* систему аудита, организовать регулярный анализ результатов аудита.
* комплекс мероприятий по антивирусной защите, включающий установку отдельного антивирусного программного обеспечения с постоянно включенной защитой.
  1. Клиент обязан определить своих уполномоченных сотрудников (желательно не менее двух, основного сотрудника и лица, его замещающего в случае отсутствия), которые имеют право осуществлять подтверждение легитимности платежей и представить данную информацию в Банк путем подписания Заявления или Заявления на ДБО, при этом в Заявлении или в Заявлении на ДБО указываются только телефоны мобильной связи.
  2. В случае смены (в результате увольнения или прекращения по другим причинам полномочий) уполномоченных сотрудников Клиента, имеющих право осуществлять подтверждение легитимности платежей, Клиент обязан в течение не более 5 (пяти) рабочих дней предоставить об этом обновленную информацию в Банк путем повторного подписания Заявления на ДБО с одновременным предоставлением нового Кодового слова.

1. **Требования по обеспечению информационной безопасности при обращении с носителями ключевой информации, содержащими ключи квалифицированной электронной подписи**
   1. Меры защиты ключей электронной подписи:

* ключи электронной подписи при их создании должны записываться только на ключевые носители (ПАК), полученные в Банке, которые поддерживаются используемыми СКЗИ согласно технической и эксплуатационной документации к ним;
* ключи электронной подписи на ключевом носителе должны быть защищены паролем (ПИН–кодом). При этом пароль (ПИН–код) формирует лицо, выполняющее процедуру создания ключей, в соответствии с требованиями на используемое средство ЭП;
* ответственность за конфиденциальность сохранения пароля (ПИН–кода) возлагается на Владельца ключа ЭП.
  1. Обращение с ключевой информацией и ключевыми носителями:
* Клиент может иметь необходимое ему количество Ключевых носителей с ЭП (ключевых документов);
* Ключевые носители должны использоваться только их владельцем либо уполномоченным лицом на использование данного носителя, и храниться в месте не доступном третьим лицам (сейф, опечатываемый бокс, закрывающийся металлический ящик и т.д.);
* ключевой носитель должен подключаться в считывающее устройство только на время непосредственного выполнения СКЗИ операций формирования и проверки электронной подписи. Запрещается оставлять ПАК подключенным в USB–порт при отсутствии лица, уполномоченного на работу в Системе ДБО. Размещение ключевого носителя в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключевой информации третьими лицами;
* на носителе ключевой информации недопустимо хранить иную информацию (в том числе рабочие или личные файлы);
* в случае расторжения Договора на ДБО Клиент обязан в течение 10 (десяти) дней комиссионно уничтожить по акту (по форме устанавливаемой Клиентом) ПАК с СКЗИ и криптографическими ключами.

1. **Срок действия ключей ЭП, порядок смены ключей**
   1. Срок действия ключа ЭП в Системе ДБО определяется Банком, как правило, в соответствии со сроком полномочий распоряжаться средствами на счете Клиента Владельца ключа, наделенного правом подписи, указанной в Карточке с образцами подписей и оттиска печати/ Соглашении о количестве и сочетании электронных подписей, но не может быть более срока действия, установленного разработчиком СКЗИ.
   2. Срок действия ключа Клиента может быть изменен Администратором Системы ДБО в следующих случаях:

* выявление угрозы безопасности дальнейшего использования данного ключа Клиентом, о чем Банк уведомляет Клиента по Системе «Клиент–Банк»;
* внесение изменений в сроки действия полномочий уполномоченных лиц в Карточке с образцами подписей/ Соглашении о количестве и сочетании электронных подписей Владельца ключа.
  1. Система «Клиент–Банк» автоматически уведомляет Клиента при каждом сеансе связи об истечении срока действия ключа, начиная с 30 суток до момента полной блокировки ключа, исключая случаи, описанные в п. 4.2.
  2. Генерация нового ключа ЭП производится на Ключевой носитель, при этом приобретать новый Ключевой носитель не обязательно, генерацию можно произвести на ранее используемый Клиентом Ключевой носитель.
  3. После процедуры генерации ключа ЭП необходимо распечатать Сертификат открытого ключа ЭП в двух экземплярах на каждую подпись и предоставить сертификат менеджеру в Банк.
  4. По окончании срока действия ключи подлежат обязательной перегенерации Клиентом, при этом прежние ключи Клиента, по которым истек срок действия, считаются недействительными.
  5. Сертификат открытого ключа ЭП Клиента аннулируется Банком в следующих случаях:
* по истечении срока его действия;
* если Банку стало достоверно известно о прекращении действия документов, на основании которых Клиенту оформлен Сертификат открытого ключа ЭП;
* по заявлению в письменной форме владельца Сертификата открытого ключа ЭП;
* при расторжении Договора на ДБО, за исключением случаев переоформления (перезаключения) Договора на ДБО.

1. **Действия при компрометации ключей электронной подписи**
   1. К событиям, относящимся к утрате конфиденциальности (компрометации) ключей ЭП, относятся следующие ситуации:

* ознакомление неуполномоченного лица (лиц) с ключами ЭП;
* утрата ключевого носителя с ключами ЭП;
* увольнение владельца ключа ЭП;
* нарушение целостности печатей на сейфах (шкафах, хранилищах), предназначенных для хранения ключевых носителей;
* утрата ключей от сейфов (шкафов, хранилищ) в случае нахождения в них ключевых носителей;
* случаи, когда невозможно достоверно установить, что произошло с ключевыми носителями, в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника, утрата ключевого носителя с последующим обнаружением.
  1. Клиент (Владелец ключа ЭП) должен самостоятельно определить факт утраты конфиденциальности (компрометации) ключа электронной подписи и оценить значение этого события.
  2. Мероприятия по розыску и локализации последствий компрометации конфиденциальной информации, переданной с использованием средств ЭП, организует и осуществляет сам Клиент (Владелец ключа ЭП).
  3. В случае утраты конфиденциальности (компрометации) Ключей ЭП или подозрении на их компрометацию, в том числе утраты электронного средства платежа и (или) о его использовании без согласия Клиента, а также при внезапном выходе из строя АРМ Клиента, возникновении любых подозрений на компрометацию среды исполнения (наличие в компьютере вредоносных программ, нестандартная работа системного программного обеспечения и т.д.), Клиент обязан:
* прекратить использование ключа ЭП и соответствующего сертификата ключа проверки электронной подписи;
* незамедлительно сообщить в Банк любым из следующих способов и заблокировать Ключи проверки ЭП:
* лично в любом удобном для него офисе Банка в соответствии с графиком работы офиса Банка п путем подачи уведомления в произвольной форме;
* путем направления уведомления в адрес Банка в Системе ДБО;
* лично в Службу технической поддержки по телефонам –

+7 940 940-04-50 или +7 940 940-04-55.

* Все сообщения и блокировка Ключей проверки ЭП подтверждаются Кодовым словом на блокировку.
  1. Получив сообщение о компрометации ключа ЭП, Банк останавливает обработку ЭД, подписанных на скомпрометированном или предположительно скомпрометированном ключе ЭП. Электронные документы со статусом «На подтверждении», «Исполнено» на момент получения сообщения о компрометации ключа ЭП отзыву (отмене) не подлежат, в случае если платеж отправлен в МЦИ Банка России.
  2. В случае физической порчи Ключевого носителя и отсутствия Ключевого носителя с резервным ключом ЭП Клиент получает в Банке по Акту приема–передачи СКЗИ новые ПАК, производит генерацию ключей и предоставляет в Банк новые сертификаты ключей проверки ЭП, после регистрации которых продолжает работу в Системе ДБО.

1. **Порядок смены Кодового слова**
   1. В случае компрометации Кодового слова (разглашение или подозрение на разглашение Кодового слова, увольнения или прекращения по другим причинам полномочий сотрудников, допущенных к работе с Кодовым словом) – Кодовое слово подлежит обязательной смене в срок не более 5 (пяти) рабочих дней.
   2. Для смены Кодового слова, Участник предоставляет в Банк заполненное Заявление на ДБО в 2 (двух) экземплярах.
   3. После простановки отметки Банка о принятии Заявления или Заявления на ДБО.
   4. Производить смену Кодового слова может только Руководитель Клиента (уполномоченное лицо Клиента), чьи данные внесены в Карточку с образцами подписей и оттиска печатей/ Соглашение о количестве и сочетании электронных подписей и обладающий соответствующими полномочиями.
   5. Заявление или Заявление на ДБО предоставляется только на бумажном носителе при личном присутствии в Банке. Направление заполненного Заявления или Заявления на ДБО иными каналами связи (факс, почта, электронный документооборот) не допускается.
   6. Кодовое слово считается обновленным по истечению не более 24 часов после предоставления Банку заполненного Заявления или Заявления на ДБО.
2. **Обязанности Клиента (Владельца ключа ЭП).** 
   1. Клиент (Владелец ключа ЭП) обязан:

* обеспечить конфиденциальность ключей электронных подписей;
* применять для формирования электронной подписи только действующий ключ ЭП;
* не применять ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена (ключ скомпрометирован или есть подозрение в его компрометации);
* применять ключ электронной подписи с учетом ограничений, содержащихся в сертификате ключа проверки электронной подписи, если такие ограничения были установлены;
* немедленно обратиться в Банк с заявлением на блокировку работы в Системе ДБО в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи;
* не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который аннулирован, действие которого прекращено или приостановлено;
* использовать для создания и проверки электронных подписей, создания ключей электронной подписи и ключей проверки электронной подписи сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи;
* хранить в тайне ПИН – коды и пароли для доступа к ключам ЭП, СКЗИ и вычислительной технике;
* при обнаружении на рабочем месте, оборудованном СКЗИ, посторонних программ или вирусов, нарушающих работу указанных средств, работа со средствами [защиты информации](http://pandia.ru/text/category/zashita_informatcii/) на данном рабочем месте должна быть прекращена и должны быть организованы мероприятия по анализу и ликвидации негативных последствий данного нарушения.
  1. Владельцу ключа ЭП запрещается:
* осуществлять несанкционированное копирование ключей;
* разглашать содержимое ключевых носителей или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и иные средства отображения информации;
* использовать ключевые носители в режимах, не предусмотренных штатным режимом использования ключевого носителя;
* вносить какие–либо изменения в программное обеспечение средств ЭП;
* записывать на ключевые носители постороннюю информацию;
* оставлять средства вычислительной техники с установленными СКЗИ без контроля после ввода ключевой информации;
* использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который аннулирован, действие которого прекращено или приостановлено;
* удалять ключевую информацию с ключевого носителя до истечения срока действия, аннулирования или прекращения действия сертификата ключа проверки электронной подписи.
* устанавливать на рабочее место с размещенными средствами ЭП средства разработки и отладки приложений, а также средства, позволяющих осуществлять несанкционированный доступ к системным ресурсам.

1. **Общие правила эксплуатации и хранения ПАК**

* необходимо оберегать ПАК от воздействия влаги и агрессивных сред сильных механических воздействий (падения с высоты, сотрясения, вибрации, ударов и т. п.), воздействия высоких и низких температур. При резкой смене температур (вносе охлажденного ПАК с мороза в теплое помещение) не рекомендуется использовать ПАК в течение 3 часов во избежание повреждения ПАК из–за сконденсированной на его электронной схеме влаги. Необходимо оберегать ПАК от попадания на него прямых солнечных лучей;
* недопустимо воздействие на ПАК сильных магнитных, электрических или радиационных полей, высокого напряжения и статического электричества;
* при подключении ПАК к компьютеру недопустимо прилагать излишние усилия;
* ПАК в нерабочее время необходимо всегда держать закрытым во избежание попадания на разъем ПАК пыли, грязи, влаги и т. п. При засорении разъема USB–токена нужно принять меры для его очистки. Для очистки корпуса и разъема используйте сухую ткань. Использование воды, растворителей и прочих жидкостей недопустимо. Не следует разбирать ПАК, это ведет к потере гарантии. В случае неисправности или неправильного функционирования ПАК необходимо обратиться в Банк.

Приложение № 2 к Условиям обслуживания банковских счетов с использованием системы дистанционного банковского обслуживания iBank2 – ЗАО «Аврора Банк»

**Положение о порядке проведения технической экспертизы при возникновении спорных ситуаций к Условиям дистанционного банковского обслуживания iBank2 – ЗАО «Аврора Банк» (далее – Положение)**

1. В настоящем Положении под спорной ситуацией понимается возникновение претензий у Клиента к Банку.
2. Согласно Условиям ДБО основанием для совершения Банком операций по счету Клиента является распоряжение Клиента, направленное в Банк в виде ЭД, подписанного ЭП Клиента. Стороны согласны, что единственным и достаточным доказательным материалом при разрешении спорной ситуации является ЭД, содержащий расчетный (платежный, валютный) документ, подписанный ЭП Клиента.
3. При возникновении спорной ситуации, Клиент представляет Банку заявление, содержащее суть претензии, с указанием на ЭД с ЭП Клиента, на основании которого Банк выполнил операции по счёту Клиента. Банк обязан по письменному запросу информировать Клиента в письменной форме о ходе рассмотрения Заявления.
4. Банк и Клиент обязаны в течение 7 (семи) рабочих дней от даты получения Банком и принятия им к рассмотрению заявления Клиента сформировать разрешительную комиссию для урегулирования возникшей спорной ситуации. Комиссия должна состоять минимум из 3–х человек. В состав комиссии включаются представители Клиента, представители Банка и, при необходимости, независимые эксперты от разработчика Системы ДБО, разработчика СКЗИ и/или ФСБ России. При достижении согласия Сторон привлечённые к работе комиссии независимые эксперты могут наделяться правом голоса. Состав комиссии должен быть зафиксирован в акте, который является итоговым документом, отражающим результаты работы комиссии.
5. Полномочия членов комиссии подтверждаются:

* представителей Банка – копией приказа Председателя Правления Банка о привлечении к работе в составе разрешительных комиссий,
* представителей Клиента – доверенностями, выданными в установленном порядке.

1. Срок работы комиссии – не более 7 (семи) рабочих дней. В исключительных ситуациях этот срок может быть увеличен по взаимной договоренности Сторон. Общий срок рассмотрения заявления Клиента не может превышать сроков, установленных законодательством Российской Федерации, со дня получения такого заявления.
2. Результатом рассмотрения спорной ситуации разрешительной комиссией является определение стороны, несущей ответственность согласно выводу об истинности и корректности ЭП Клиента, содержащейся в ЭД.
3. Разрешительная комиссия проводит техническую экспертизу ЭД, заверенного ЭП Клиента, на основании которого Банком выполнена операция по счету Клиента.
4. Работа разрешительной комиссии включает в себя следующие этапы:

* комиссия определяет на основании какого ЭД Банк осуществил списание денежных средств со счета Клиента,
* комиссия определяет наличие данного ЭД в Системе ДБО,
* комиссия проверяет реквизиты получателя в найденном в Системе ДБО ЭД, на основании которого Банком была осуществлена оспариваемая операция с денежными средствами Клиента,
* комиссия проверяет корректность ЭП Клиента, содержащейся в ЭД.

1. Признание ЭП Клиента, содержащейся в ЭД корректной, основывается на полученных результатах от проведения следующих мероприятий:

* проведение проверки соответствия подписей руководителя, уполномоченного сотрудника Клиента и оттиска печати Клиента, учиненных на оригинале экземпляра Банка Акта приема–передачи Сертификата Ключа проверки ЭП сотрудника Клиента в Системе ДБО с образцами подписей руководителя, уполномоченного сотрудника Клиента и оттиска печати Клиента, указанных в банковской Карточке с образцами подписей и оттиска печати, имеющейся в юридическом деле Клиента, либо в Соглашении о количестве и сочетании электронных подписей при отсутствии оформленной Карточки с образцами подписей у Клиента,
* проведение проверки соответствия идентификатора ключа ЭП Клиента, содержащейся в ЭД Клиента, с идентификатором ключа ЭП , заверенного Клиентом в Сертификате Ключа проверки ЭП сотрудника Клиента в Системе ДБО,
* проведение проверки периода действия Ключей проверки ЭП Клиента и даты исполнения Банком, принятого от Клиента ЭД.

1. Если результаты проверки, проведенной в соответствии с п. 10 настоящего Положения, вызывают сомнения у представителей одной из Сторон, то эта Сторона имеет право инициировать проведение независимой проверки ЭП Клиента, содержащейся в ЭД. С этой целью разрешительная комиссия, используя представленное компанией разработчиком Системы ДБО специальное эталонное программное обеспечение (эталонные утилиты), формирует необходимые материалы и направляет компании разработчику для проведения независимой экспертизы. Оплату работы независимых экспертов компании разработчика Системы ДБО осуществляет Сторона, инициирующая независимую экспертизу.
2. Если по результатам всех проведенных проверок корректности ЭП Клиента, содержащейся в оспариваемом ЭД, ЭП Клиента признана корректной, то авторство оспариваемого ЭД признается разрешительной комиссией установленным.
3. Если авторство оспариваемого ЭД признано разрешительной комиссией установленным, то неправой в споре признается Сторона, действия которой не соответствуют содержанию ЭД.
4. Если по результатам всех проведенных проверок корректности ЭП Клиента, содержащейся в оспариваемом ЭД, ЭП Клиента признана некорректной, то предъявленный для проверки авторства ЭД признается комиссией ложным.
5. Банк несет ответственность перед Клиентом в случае, когда имела место хотя бы одна из следующих ситуаций:

* Банк ошибочно совершил операцию по счету Клиента или не предъявляет ЭД, переданного Клиентом, на основании которого Банк выполнил операции по счёту Клиента,
* Банк совершил операцию по счету Клиента на основании Электронного документа Клиента содержащего некорректную Электронную подпись Клиента,
* В случае совершения Банком операции по счету Клиента на основании принятого Банком от Клиента ЭД при наличии у Клиента уведомления об отмене действия Ключа ЭП и соответствующего ему Ключа проверки ЭП Клиента с отметкой Банка в получении, свидетельствующей о его получении Банком датой ранее, чем совершена операция по счету Клиента по данному ЭД,
* В иных случаях, установленных действующим законодательством РА.

1. По итогам работы разрешительной комиссии составляется акт, в котором в обязательном порядке отражаются:

* состав разрешительной комиссии, место и сроки ее работы, реквизиты документов, на основании которых действуют члены комиссии,
* установленные обстоятельства,
* действия членов разрешительной комиссии,
* выводы разрешительной комиссии, в том числе, основанные на данных проведенной технической экспертизы,
* основания, которые послужили для формирования выводов,
* иные условия по согласованию Сторон.

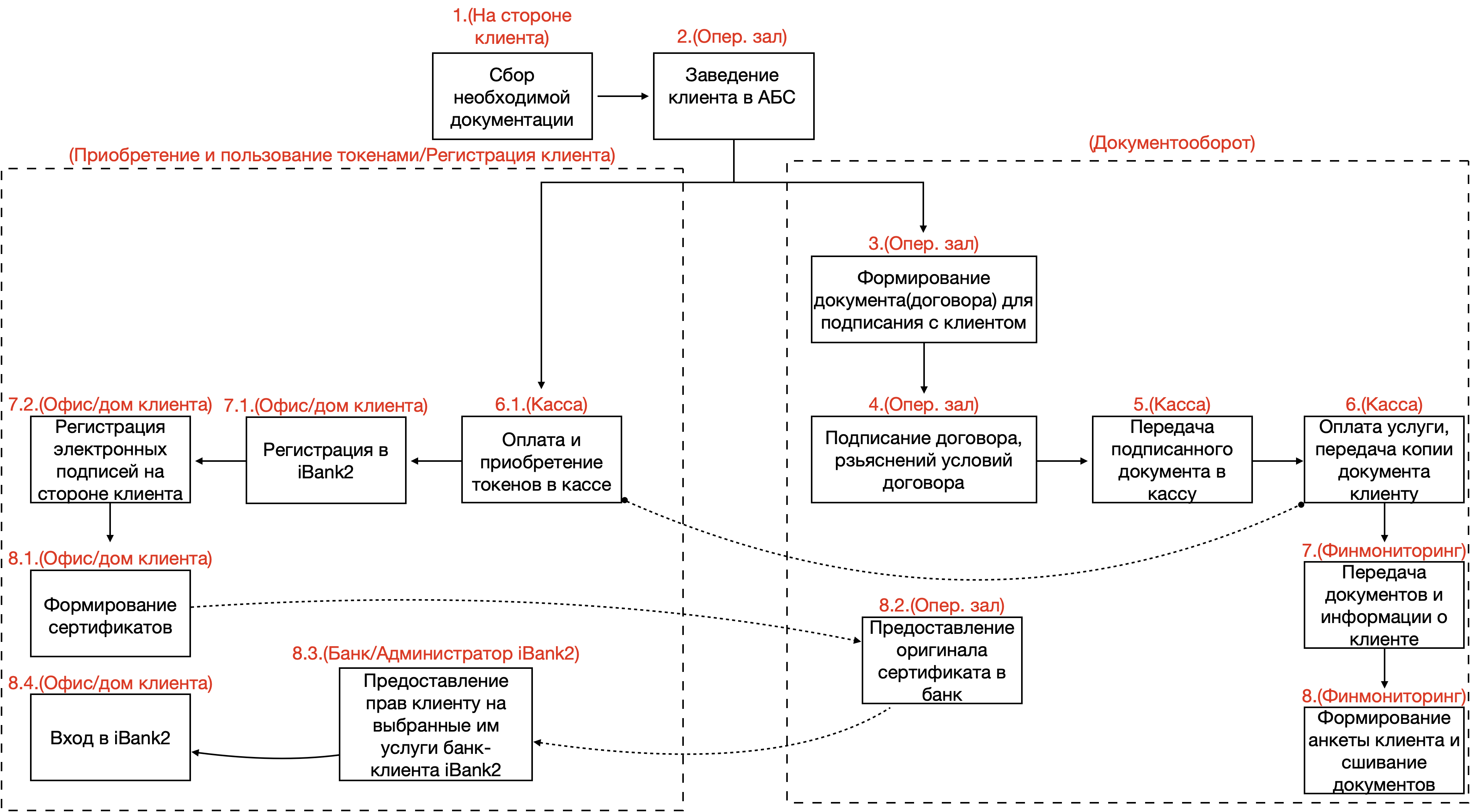
1. Акт признается Сторонами надлежащим, если соблюдены все требования, указанные в п. 16 настоящего Положения.
2. Акт подписывается всеми членами комиссии. Член комиссии, отказывающийся подписать Акт, должен письменно обосновать свой отказ. Письменное обоснование прикладывается к Акту.
3. Акт составляется в двух экземплярах, по одному для каждой Стороны.
4. При рассмотрении в суде споров Стороны обязаны предоставить суду акт, составленный в соответствии с настоящим Положением.

Приложение № 3 к Условиям обслуживания банковских счетов с использованием системы дистанционного банковского обслуживания iBank2 – ЗАО «Аврора Банк»

**Руководство по подключению к системе дистанционного**

**банковского обслуживания iBank2 – ЗАО «Аврора Банк»**

1. **Схема подключения к системе дистанционного банковского обслуживания iBank2 – ЗАО «Аврора Банк» (далее – система ДБО):**



1. **Документы, необходимые для подключения к системе ДБО:**
   1. **Для новых Клиентов:**

* **Юридическим лицам:**
* заявление об открытии счета (оформляется Банком);
* свидетельство о государственной регистрации юридического лица;
* учредительные документы юридического лица;
* лицензии (разрешения), выданные юридическому лицу в установленном законодательством Республики Абхазия порядке на право осуществления деятельности, подлежащей лицензированию, в случае если данные лицензии (разрешения) имеют непосредственное отношение к правоспособности клиента заключать договор банковского счета соответствующего вида;
* карточка (оформляется Банком);
* документы, подтверждающие полномочия лиц, указанных в карточке, на распоряжение денежными средствами, находящимися на банковском счете;
* документы, подтверждающие полномочия единоличного исполнительного органа юридического лица;
* свидетельство о постановке на учет в налоговом органе;
* справка из Пенсионного фонда Республики Абхазия о постановке на учет;
* информационное письмо с указанием статистических кодов;
* заявление о присоединении к Условиям ДБО.
* **индивидуальным предпринимателям:**
* заявление на открытие счета (оформляется Банком);
* документ, удостоверяющий личность физического лица;
* карточка (оформляется Банком);
* документы, подтверждающие полномочия лиц, указанных в карточке, на распоряжение денежными средствами, находящимися на банковском счете (если такие полномочия передаются третьим лицам);
* свидетельство о постановке на учет в налоговом органе;
* свидетельство о государственной регистрации в качестве индивидуального предпринимателя;
* лицензии (патенты), выданные индивидуальному предпринимателю или лицу, занимающемуся частной практикой, в установленном законодательством Республики Абхазия порядке, на право осуществления деятельности, подлежащей лицензированию (регулированию путем выдачи патента);
* справка из Пенсионного фонда Республики Абхазия о постановке на учет;
* информационное письмо с указанием статистических кодов;
* заявление о присоединении к Условиям ДБО.
  1. **Для действующих Клиентов – юридических лиц и ИП:**
* заявление о присоединении к Условиям ДБО;
* выписка из ЕГРЮЛ.

1. **Порядок действий Клиента для подключения к системе ДБО:**
   1. **Подписание и передача в отдел по обслуживанию клиентов Банка заявления о присоединении к Условиям ДБО;**
   2. **Оплата аренды электронного ключа (USB-токена) путем списания денежных средств со счета Клиента или внесения наличных денежных средств в кассу Банка;**
   3. **Получение электронного ключа (USB-токена) в кассе Банка и подписание Акта приема-передачи;**
   4. **Регистрация в системе ДБО.**
2. **Порядок регистрации Клиента в системе ДБО**
   1. **Для регистрации в системе ДБО Клиенту необходимо совершить следующие действия:**

* перейти по ссылке [https://bk.aurora-bank.com/ibank2/#/](http://https://bk.aurora-bank.com/ibank2/#/) и нажать на кнопку в нижнем левом углу «Регистрация и создание ЭП» (рис. 1);

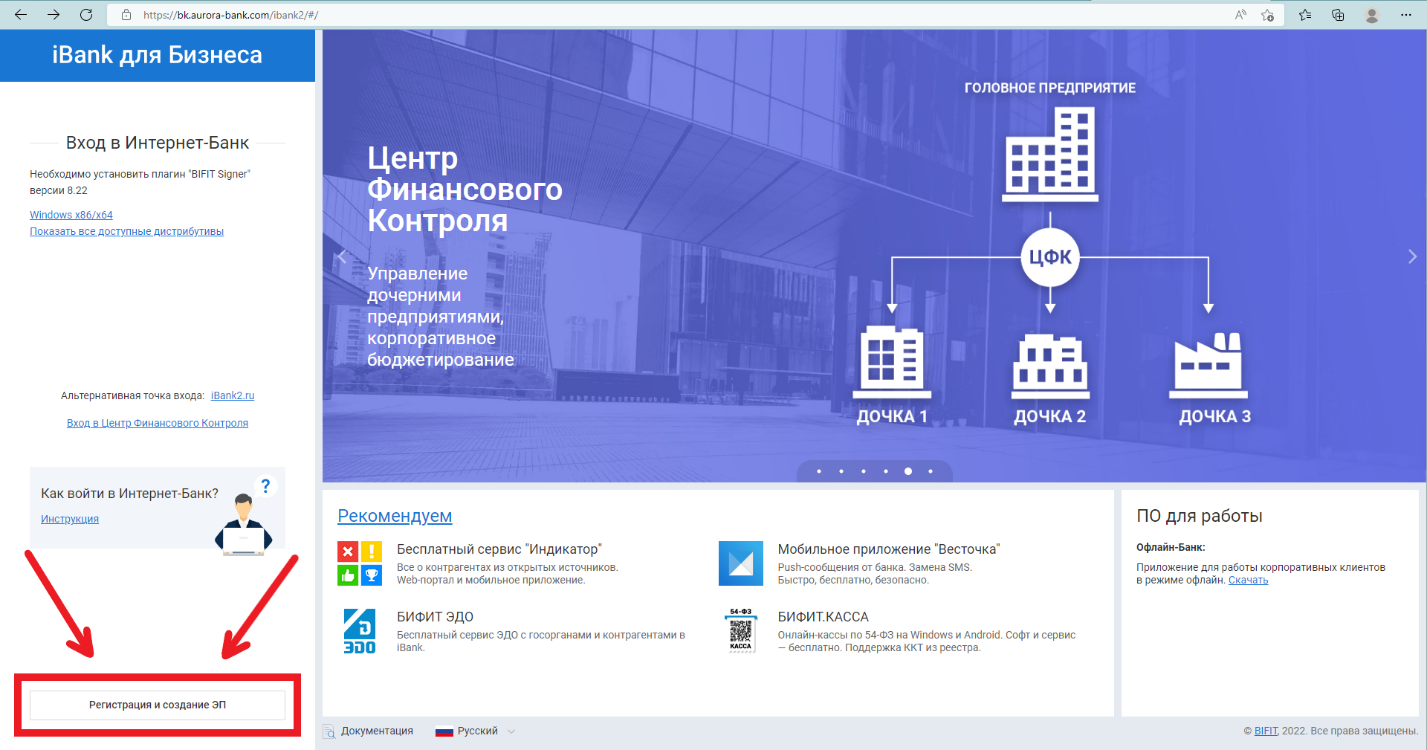


Рисунок Регистрация

* далее нужно нажать на кнопку «Подключение к системе» (рис. 2)

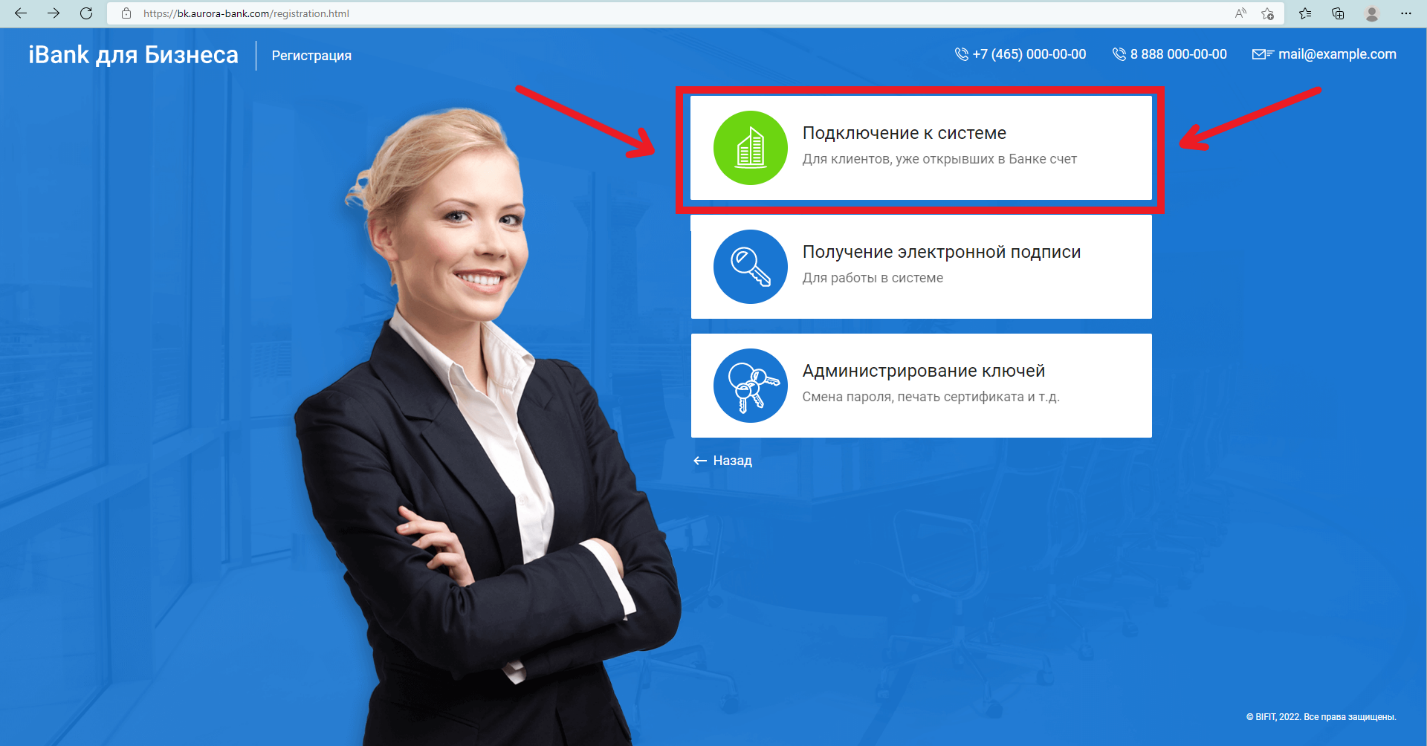


Рисунок Подключение к системе

* далее система предложит Клиенту скачать приложение «bifit\_signer», для скачивания нужно перейти по ссылке/кнопке «Windows x86/x64» (рис. 3)

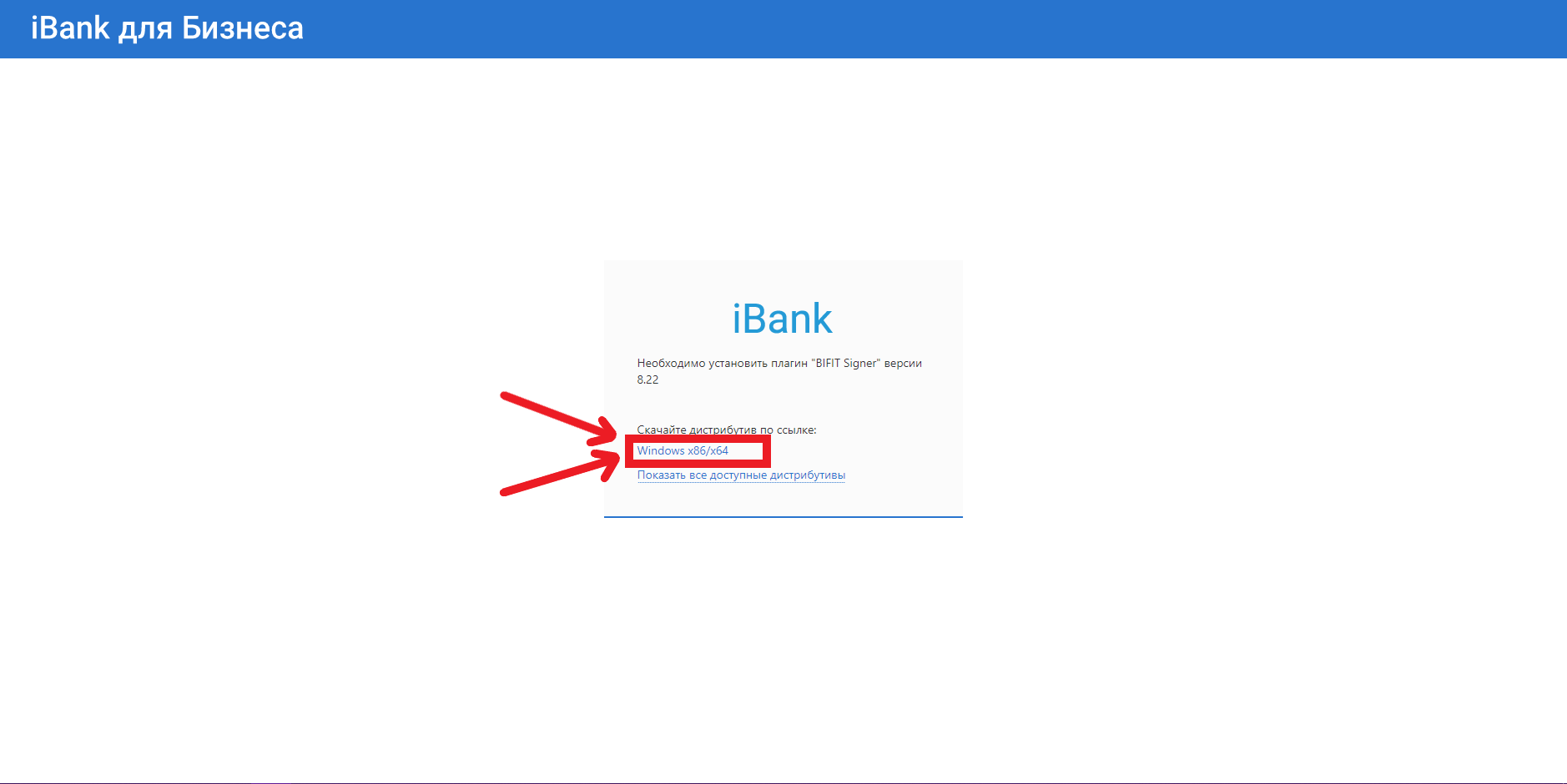


Рисунок Скачивание bifit\_signer

* после того как Клиент скачал bifit\_signer\_ ему необходимо обновить страницу, либо снова перейти по кнопке «подключение к системе» (см. рис. 2) и у Клиента появится окно регистрации, состоящее из нескольких шагов (рис. 4)

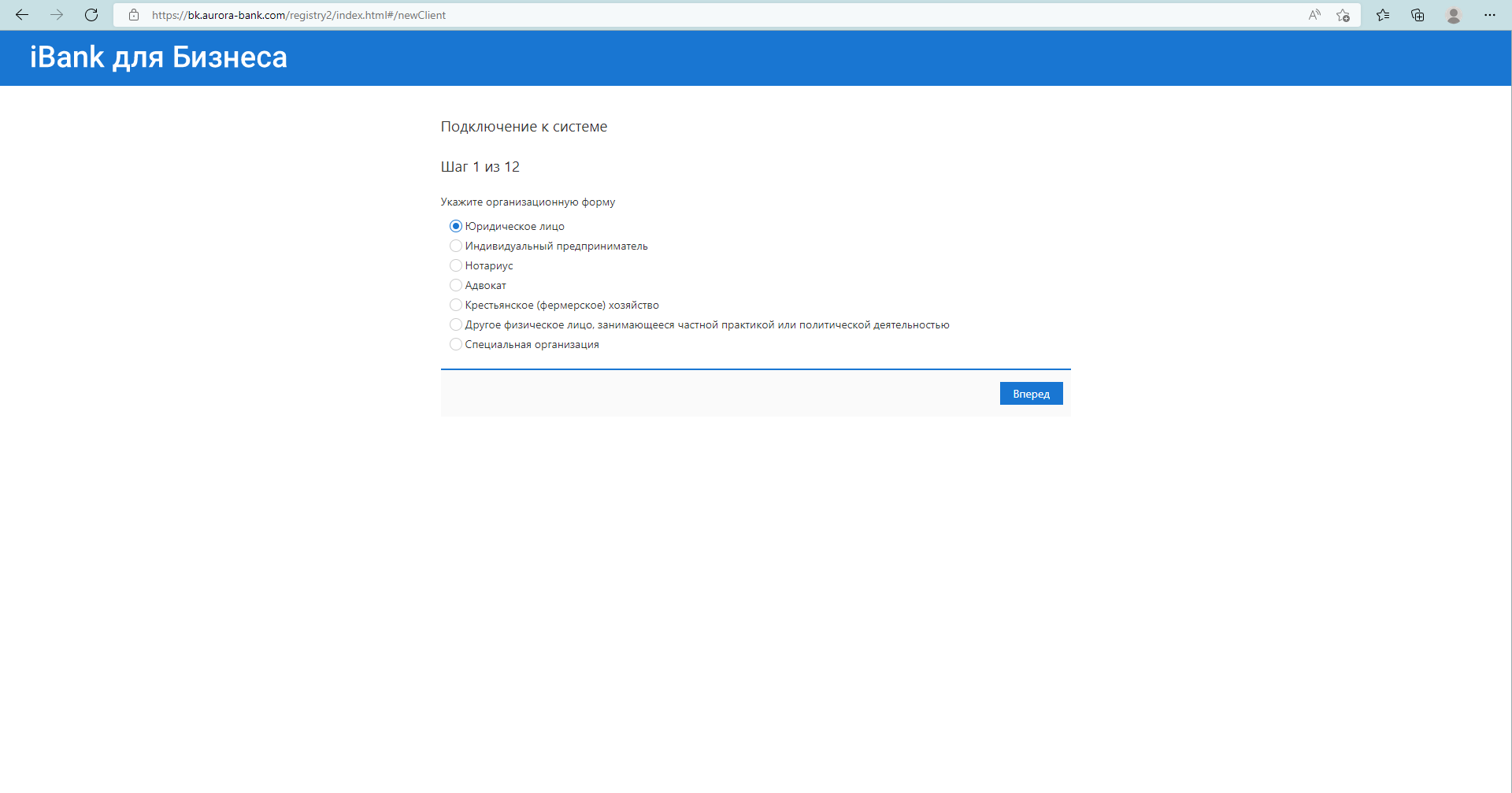


Рисунок Подключение к системе, регистрация

* после того как Клиент прошел регистрацию, состоящую из нескольких шагов, он должен зарегистрировать электронные подписи. Для этого нужно перейти по кнопке «Получение электронной подписи» (рис. 5)

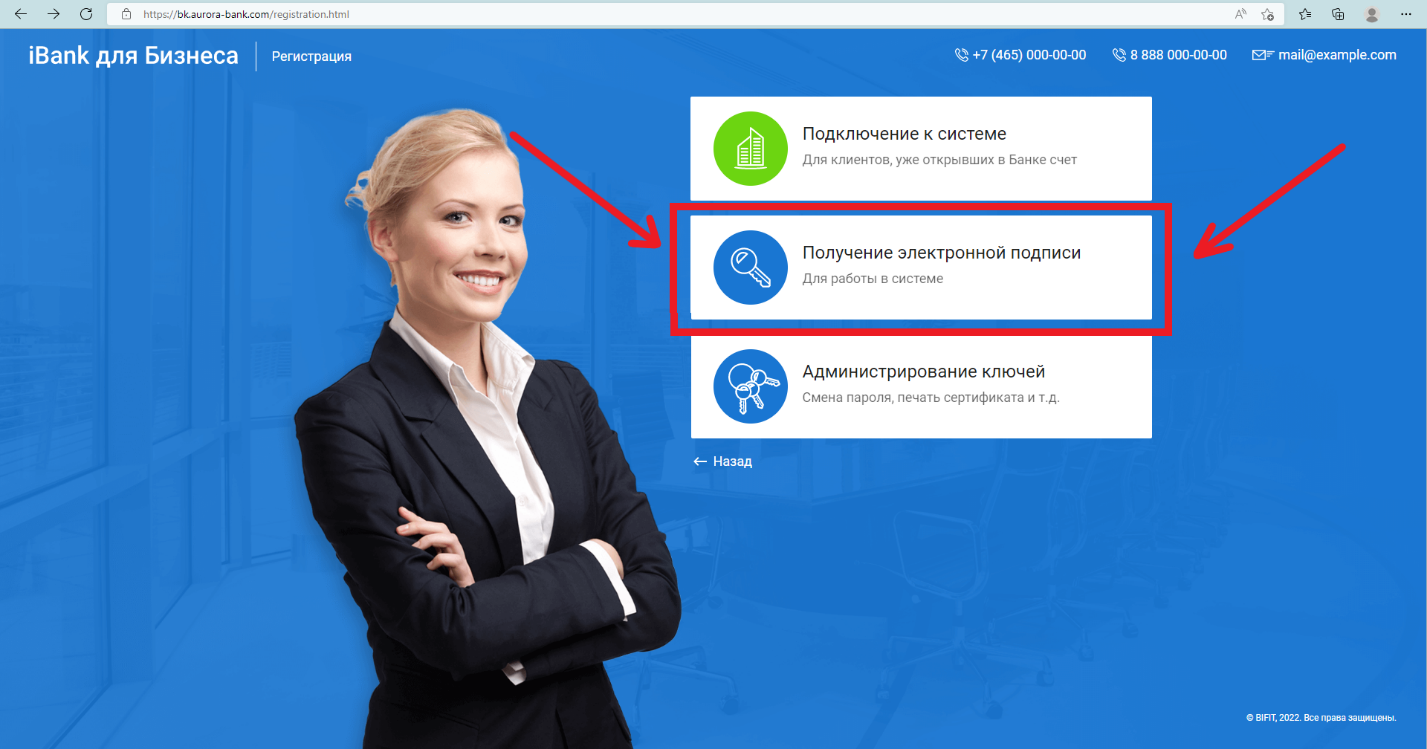


Рисунок Получение электронной подписи

* далее Клиента перенаправит на страницу регистрации электронных подписей, где он должен пройти несколько шагов регистрации (рис. 6)

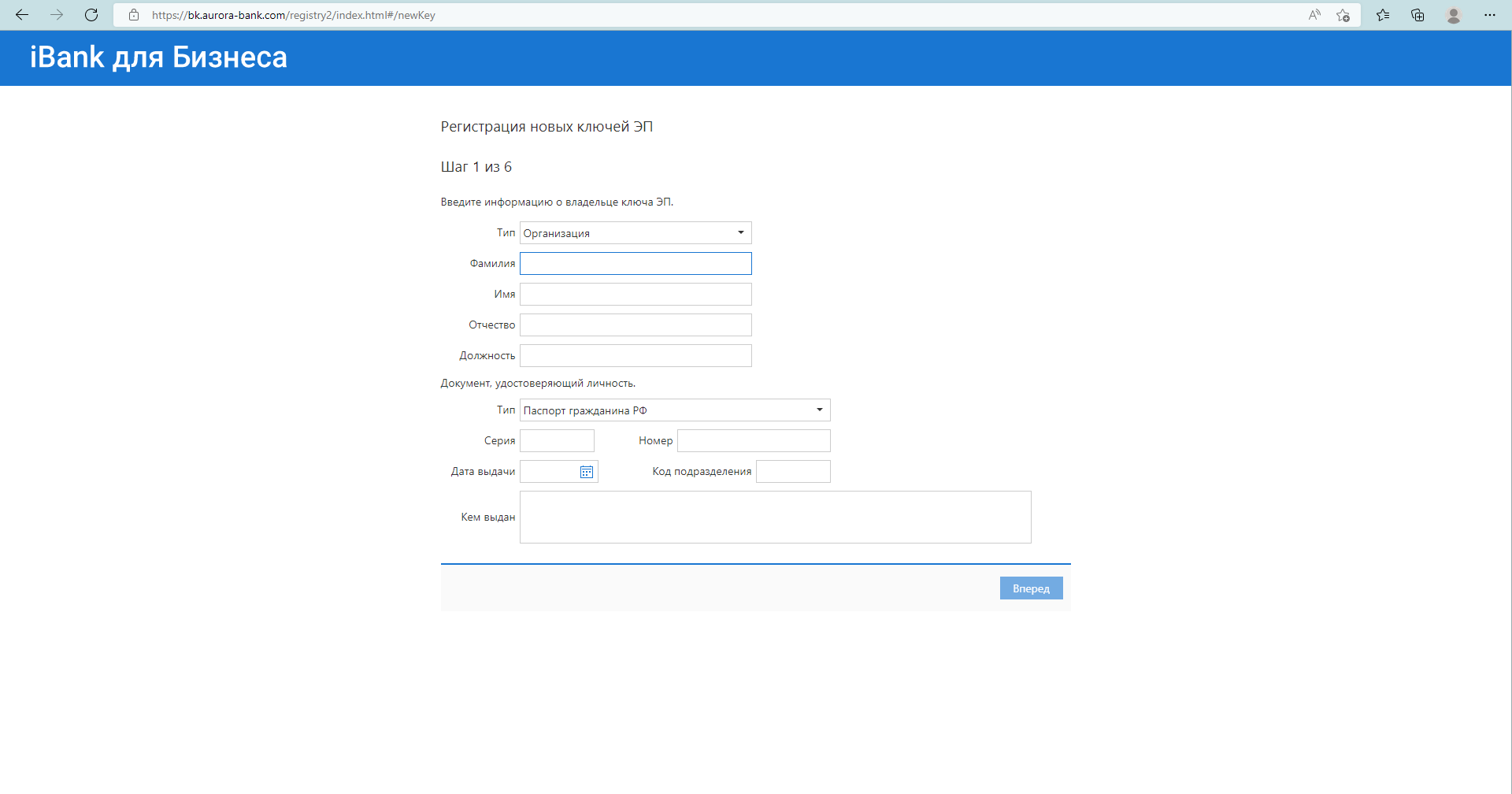


Рисунок Регистрация новых ключей ЭП

* формирование сертификатов – после того как Клиент зарегистрировал электронную подпись, ему будет предложено распечатать сертификат, который необходимо распечатать в двух экземплярах;
* предоставление оригинала сертификата в Банк – после того как клиент распечатал сертификаты, он приносит их в Банк, для подтверждения создания личного кабинета и электронной подписи;
* предоставление прав Клиенту на выбранные им услуги системы ДБО – после того как Клиент принес сертификат, этот сертификат передается администратору (работник Банка) системы ДБО, который предоставляет права Клиенту на выбранные услуги системы ДБО (баланс счета, просмотр выписок, их распечатка и проведение платежей);
* вход в систему ДБО – после всех проведенных выше процедур, Клиент может войти в систему ДБО и пользоваться ее функциями.