

**АКЦИОНЕРНЫЙ КОММЕРЧЕСКИЙ БАНК  
«БАЛТИЙСКИЙ БАНК РАЗВИТИЯ»  
(закрытое акционерное общество)**

**СОГЛАШЕНИЕ**

**об оказании клиентам - юридическим лицам и индивидуальным предпринимателям  
услуги «Электронный банк»**

к Договору банковского счета № \_\_\_\_\_ от « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

г. Владивосток

« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

Акционерный коммерческий банк «Балтийский Банк Развития» (закрытое акционерное общество), именуемое в дальнейшем «Банк», в лице Заместителя Управляющего ФАКБ "Балтийский Банк Развития", Владивосток Просяникова Алексея Викторовича, действующего на основании доверенности № 1.1-10-2/119 от 22.07.2010 г., с одной стороны, и \_\_\_\_\_, именуемый(ое) в дальнейшем «Клиент», в лице \_\_\_\_\_, действующего (ей) на основании \_\_\_\_\_, с другой стороны, вместе именуемые Стороны, заключили настоящее Соглашение о нижеследующем.

**1. Понятия, используемые в настоящем Соглашении**

**Система «iBank 2»** – совокупность программных средств, устанавливаемых в помещениях СТОРОН и согласованно эксплуатируемых СТОРОНАМИ с целью предоставления КЛИЕНТУ услуги "Электронный банк". Далее часть системы, устанавливаемая в помещении БАНКА, называется Абонентский пункт БАНКА (АП БАНКА), а часть системы, устанавливаемая в помещении КЛИЕНТА – Абонентский пункт КЛИЕНТА (АП КЛИЕНТА.)

**Услуга "Электронный банк"** – предоставление КЛИЕНТУ возможности проведения безналичных расчетов и иных операций с использованием электронных документов (ЭД) путем подготовки и отправки в БАНК, а также получения из БАНКА электронных документов по открытым каналам связи. В рамках услуги «Электронный банк» БАНК передает КЛИЕНТУ в пользование специализированное программное обеспечение (ПО), необходимое и достаточное для создания на территории КЛИЕНТА абонентского пункта (АП) Системы «iBank 2».

**Электронно-цифровая подпись (ЭЦП)** – аналог собственноручной подписи уполномоченного лица Банка или уполномоченного лица Клиента под электронным документом, полученный с использованием секретного (закрытого) ключа ЭЦП, позволяющий идентифицировать владельца сертификата ключа подписи и подтверждающий отсутствие искажения информации в электронном документе. Наличие необходимых ЭЦП в электронном документе, полученном по Системе «iBank 2», является необходимым и достаточным условием, позволяющим установить, что электронный документ исходит от Стороны по Соглашению.

**Электронный документ (ЭД)** – документ, представленный в электронной форме, подписанный (защищенный) ЭЦП и имеющий равную юридическую силу с аналогичным документом на бумажном носителе, подписанным собственноручными подписями уполномоченных лиц и заверенным оттиском печати.

В системе предусмотрены следующие виды документов:

- Платежное поручение
- Инкассовое поручение
- Платежное требование
- Аккредитив
- Заявление об акцепте
- Заявление на перевод валюты
- Поручение на покупку иностранной валюты
- Поручение на продажу иностранной валюты

Банк \_\_\_\_\_

Клиент \_\_\_\_\_

- Межбанковский перевод
- Распоряжение на обязательную продажу иностранной валюты
- Поручение на обратную продажу иностранной валюты
- Паспорт сделки по контракту
- Паспорт сделки по кредитному договору
- Поручение на конвертацию валюты
- Документ свободного формата (письмо)
- Запрос на отзыв документа
- Справка о валютных операциях
- Справка о поступлении валюты Российской Федерации
- Справка о подтверждающих документах
- Сведения о выгодоприобретателе – юридическом лице
- Сведения о выгодоприобретателе – физическом лице

Все электронные документы, подписанные ЭЦП, полученные и направленные Сторонами друг другу, хранятся в Системе в течение установленных сроков хранения документов. Просмотр электронного документа и проверка ЭЦП возможен в любое время с рабочего места сотрудника Банка. Банк или какие-либо третьи лица не имеют возможности вносить изменения в электронный документ, хранящийся в Системе.

**Владелец сертификата ключа подписи** – физическое лицо, на имя которого выдан сертификат ключа подписи в соответствии с правилами настоящего соглашения.

**Технические средства** – IBM-совместимый персональный компьютер, необходимые телекоммуникационные средства для передачи электронных документов.

**Программные средства** – программное обеспечение, с помощью которого выполняются установленные настоящим Соглашением процедуры формирования, отправки и приема электронных документов, а также формирование и проверка ЭЦП (*средства криптографической защиты информации, АРМ «Интернет Банкинг для корпоративных клиентов» системы «iBANK 2», АРМ «РС-Банкинг» системы «iBANK 2»*).

**Средства криптографической защиты информации (СКЗИ)** – комплекс программных или программно-аппаратных средств, предназначенный для обеспечения конфиденциальности, подлинности и целостности электронных документов, передаваемых по открытым каналам связи. Сертифицированное криптографическое программное и аппаратное обеспечение в части, необходимой для реализации защищенного информационного взаимодействия, поставляется КЛИЕНТУ БАНКОМ отдельно, по акту приема-передачи.

**Ключи ЭЦП** – пара ключей (открытый и секретный (закрытый)), с помощью которых осуществляется формирование и проверка ЭЦП. Секретный ключ хранится только у владельца сертификата ключа подписи и используется для формирования ЭЦП, а открытый ключ служит для проверки ЭЦП и передается Стороне, получающей электронные документы, заверенные ЭЦП. Банк и Клиент обеспечивают хранение в тайне владельцами сертификатов ключей подписи своих секретных ключей и обмениваются друг с другом открытыми ключами ЭЦП. По известному открытому ключу невозможно восстановить парный ему секретный ключ.

**Сертификат ключа подписи** – электронный файл, содержащий заверенные ЭЦП уполномоченного лица Банка идентификационные данные и открытый ключ владельца сертификата открытого ключа подписи - уполномоченного лица Клиента. Сертификат ключа изготавливается в Системе автоматически в процессе генерации ключей. Сертификат ключа Клиента необходим для проверки его ЭЦП и должен находиться в Банке. Сертификаты (в том числе утратившие силу) хранятся в Системе весь срок действия Договоров банковского счета, указанных в [Приложении 2](#) к настоящему Соглашению, а также в течение не менее чем трех лет после окончания срока действия указанных Договоров. Одновременно с формированием сертификата в электронном виде, оформляются два экземпляра Сертификата ключа подписи на бумажных носителях ([Приложение 4](#)), которые заверяются собственноручными подписями владельца сертификата ключа подписи и уполномоченного лица Банка. Один экземпляр выдается владельцу сертификата ключа подписи, второй – остается в Банке.

**Договор** – договор (договоры) банковского счета, указанный(ые) в [Приложении 2](#) к настоящему Соглашению, к которому(ым) применяются правила настоящего Соглашения.

**USB-токен «iBank 2 Key»** (далее USB-токен) - специализированное аппаратное устройство с интерфейсом Universal Serial Bus (USB), предназначенное для генерации пары ключей электронно-цифровой подписи (ЭЦП), хранения сгенерированных секретных ключей ЭЦП и формирования ЭЦП под документами при осуществлении электронного документооборота между КЛИЕНТОМ и БАНКОМ в системе «iBank 2»

**IP фильтрация** – режим ограничения (блокирования) доступа к Системе с IP адресов сети Интернет, не перечисленных в карточке Клиента.

## **2. Предмет соглашения**

2.1. БАНК обязуется предоставить, а КЛИЕНТ оплатить услугу "Электронный банк" на условиях настоящего Соглашения, договора (договоров) банковского счета и действующих тарифов БАНКА.

2.2. Обязанность Сторон осуществлять прием и исполнение электронных документов наравне с аналогичными документами, переданными на бумажном носителе, возникает с момента подписания Акта приемки-сдачи работ по подключению клиента к услуге «Электронный банк» (Приложение 5).

2.3. Возможность направления КЛИЕНТОМ распоряжений в электронной форме в порядке, установленном настоящим Соглашением, не исключает обязанности БАНКА по приему распоряжений КЛИЕНТА на бумажном носителе.

2.4. Стороны признают юридическую силу ЭД, подписанных ЭЦП (при положительном результате проверки ЭЦП) и оформленных в соответствии с требованиями действующего законодательства Российской Федерации, равной юридической силе документов на бумажном носителе, оформленных в соответствии с требованиями действующего законодательства Российской Федерации.

2.5. Система используется для работы со счетами КЛИЕНТА, указанными в Приложениях 2 и 6.

2.6. Внесение изменений в список обслуживаемых счетов, изменение реквизитов клиента, добавление и удаление ключей ЭЦП, режима IP фильтрации, заказ USB-токенов и т.д. осуществляется на основании клиентского Заявления на изменение параметров подключения к услуге по форме Приложения 6.

## **3. Права и обязанности сторон**

3.1. Стороны обязуются:

3.1.1. Принимать на себя в полном объеме все обязательства, связанные с ЭД, удостоверенными от их имени корректной ЭЦП.

3.1.2. При проведении электронных расчетов с использованием Системы руководствоваться действующим законодательством Российской Федерации, нормативными актами Банка России, определяющими порядок и правила проведения безналичных расчетов, технической документацией на Систему, а также требованиями настоящего Соглашения.

3.1.3. За собственный счет приобретать и поддерживать в работоспособном состоянии технические средства и общесистемное программное обеспечение, необходимые для функционирования Системы «iBank 2», а также обеспечивать функционирование Системы в частях, относящихся к АП каждой из Сторон.

3.1.4. Обеспечить надлежащее хранение Ключей ЭЦП в целях исключения несанкционированного доступа к ним.

3.1.5. При компрометации или возникновении подозрений на компрометацию секретных ключей участников Системы незамедлительно прекратить обработку ЭД и сообщить об этом другой Стороне любыми доступными каналами связи, с обязательной отправкой в тот же рабочий день уведомления в письменном виде.

3.1.6. Сторона, получившая уведомление о прекращении обработки ЭД, обязана не позднее следующего банковского дня связаться с ответственным представителем другой Стороны для согласования порядка дальнейшего использования Системы.

3.1.7. Возобновление обработки ЭД производится на основании соответствующего письменного уведомления, направленного Стороной, инициировавшей прекращение обработки.

3.1.8. При возникновении разногласий и споров, связанных с настоящим Соглашением, решать их путем переговоров в порядке, установленном настоящим Соглашением.

3.2. Стороны признают, что:

Банк \_\_\_\_\_

Клиент \_\_\_\_\_

3.2.1. Применяемая в Системе СКЗИ обеспечивает конфиденциальность, целостность и подлинность ЭД и достаточна для оказания услуги "Электронный банк" с использованием открытых сетей передачи данных при условии использования нескомпрометированных секретных ключей.

3.2.2. Электронные документы с электронными цифровыми подписями Клиента, хранящиеся в Системе на АП БАНКА, являются доказательным материалом для решения спорных вопросов в соответствии с п. 9 настоящего Соглашения. Электронные документы, не имеющие необходимого количества электронных цифровых подписей, при наличии спорных вопросов, не являются доказательным материалом.

3.2.3. ЭД, удостоверенные корректными ЭЦП в количестве, соответствующем карточке с образцами подписей и оттиска печати КЛИЕНТА, обладают юридической силой и подтверждают наличие между СТОРОНАМИ правовых отношений.

3.2.4. ЭД, подписанные некорректными ЭЦП, в обработку не принимаются.

3.2.5. Единой шкалой времени при работе в Системе является Владивостокское поясное время по показаниям системных часов АП БАНКА. Временем поступления ЭД КЛИЕНТА в БАНК считается время записи документа в базу данных Системы на АП БАНКА.

3.2.6. Применяемая в USB-токене «iBank 2 Key» технология генерации и хранения секретного ключа ЭЦП и формирования ЭЦП под документом полностью исключает возможность получения прямого доступа к секретному ключу ЭЦП с целью его копирования, переноса на внешний носитель или использования для формирования ЭЦП вне USB-токена. Использование USB-токена «iBank 2 Key» принципиально исключает возможность хищения секретного ключа ЭЦП отдельно от хищения самого USB-токена.

3.3. КЛИЕНТ обязуется:

3.3.1. Передавать в БАНК должным образом оформленные ЭД, своевременно получать в БАНКЕ выписки движения денежных средств по счету и контролировать состояния отправленных ЭД, подтверждающие их прохождение в БАНКЕ.

3.3.2. Исполнять требования и рекомендации БАНКА по обеспечению информационной безопасности на АП КЛИЕНТА, изложенные в [Приложении 1](#) к настоящему Соглашению.

3.3.3. Незамедлительно в письменном виде уведомлять Банк о факте утраты, компрометации или подозрении на компрометацию ключей ЭЦП. При получении такого уведомления, а также по истечению срока действия сертификата ключа подписи, и/или если Банку стало известно о прекращении действия документа, на основании которого оформлен сертификат ключа подписи, а также в иных случаях, установленных нормативно-правовыми актами, Банк аннулирует действие сертификата ключа подписи, выданного конкретному владельцу сертификата ключа подписи, и не принимает электронные документы, подписанные от имени Клиента ЭЦП указанного лица. Замена ключей ЭЦП производится на основании Заявления на активацию (замену) ключей (Приложение 7).

3.3.4. Предоставить оборудование, средства и каналы связи, общесистемное программное обеспечение, необходимые для организации автоматизированного рабочего места Клиента и подключения к Системе, в том числе:

- IBM совместимый персональный компьютер с параметрами: Intel Celeron 300 MHz или выше, объем ОЗУ 64 Мб или выше, операционная система Windows Vista/XP Service Pack 2/2000 Service Pack 4 или выше.
- Наличие USB порта для использования USB-токенов;
- русифицированный принтер;
- интернет-браузер Explorer 6.0 или выше;
- JAVA RUNTIME ENVIRONMENT v6.0 (предоставляется при необходимости Банком)
- Канал в Интернет, либо модем. Для работы с системой достаточно обеспечить скорость соединения 14.4 Кбит/сек. Рекомендуемая скорость соединения 33.6 Кбит/сек.
- При работе через Интернет, обеспечить возможность исходящего соединения с рабочего места по протоколу TCP к серверу ФАКБ «Балтийский Банк Развития», Владивосток по адресу **ibankvl.bbrbank.ru на порты 443 и 9091.**

3.3.5. Использовать АП КЛИЕНТА исключительно в целях, предусмотренных настоящим Соглашением;

3.3.6. Назначить лиц, уполномоченных обеспечивать функционирование АП КЛИЕНТА;

3.3.7. Соблюдать правила пользования предоставленными ему программными средствами;

3.3.8. Оплачивать услуги Банка, оказываемые согласно настоящему Соглашению в соответствии с действующими тарифами Банка;

3.3.9. Перед началом эксплуатации Системы получить в Банке и установить на АП КЛИЕНТА средства криптографической защиты информации. Получение Клиентом СКЗИ оформляется Актом приема-передачи средств криптографической защиты информации по форме Приложения 3;

3.3.10. Использовать предоставленные СКЗИ, в том числе USB-токены, только в Системе «iBank 2», без права ее продажи или передачи каким-либо другим способом иным физическим или юридическим лицам, обеспечивать возможность контроля со стороны федеральных органов за соблюдением требований и условий осуществления лицензионной деятельности.

3.3.11. По требованию Банка, в случае прекращения действия сертификата на встроенные в USB-токен средств шифрования, Клиент обязуется прекратить использование полученного USB-токена.

3.3.12. Обеспечивать сохранность и целостность программного комплекса Системы в течение всего периода эксплуатации, включая предоставленные БАНКОМ средства криптографической защиты информации, не вносить в них изменения или дополнения. Не передавать третьим лицам программное обеспечение системы, а также не оказывать третьим лицам услуги в области шифрования с использованием программного комплекса Системы.

3.4. БАНК обязуется:

3.4.1. Не позднее следующего банковского дня с момента получения от КЛИЕНТА оформленных и подписанных Сертификатов открытых ключей подключить КЛИЕНТА к Системе для оказания услуги "Электронный банк", а также изменять параметры подключения в соответствии с настоящим Соглашением.

3.4.2. Исполнять оформленные должным образом ЭД КЛИЕНТА в соответствии с настоящим Соглашением.

3.4.3. Исполнять распоряжения КЛИЕНТА на списание безналичных денежных средств не позднее рабочего дня, следующего за днем поступления платежного документа в Банк.

3.4.4. Поддерживать в актуальном состоянии на АП БАНКА корпоративные справочники, используемые в Системе.

3.4.5. При изменении порядка и/или правил проведения безналичных платежей и оформления расчетных документов своевременно производить модернизацию ПО АП КЛИЕНТА.

3.4.6. Поддерживать на АП БАНКА в актуальном состоянии выписки по счетам КЛИЕНТОВ обслуживаемых по Системе;

3.4.7. Не принимать к исполнению документы КЛИЕНТА в случае их ненадлежащего оформления и/или в случае, если проверка на подлинность ЭЦП дала отрицательный результат;

3.4.8. Осуществлять установку системы силами специалистов БАНКА на основании Заявления на подключение к услуге (Приложение 2) в течение пяти рабочих дней с момента получения БАНКОМ указанного Заявления;

3.4.9. Осуществлять устранение неполадок на АП КЛИЕНТА на основании письменного заявления КЛИЕНТА (Приложение 8). Выезд специалиста БАНКА в адрес КЛИЕНТА для устранения неполадок в системе осуществляется не позднее пяти рабочих дней с момента получения письменного заявления. Факт выполнения работ оформляется актом приема-передачи выполненных работ по форме Приложения 9. Оплата соответствующей комиссии Банка осуществляется путем списания БАНКОМ с расчетного счета КЛИЕНТА в безакцептном порядке соответствующей суммы согласно действующим Тарифам БАНКА.

3.4.10. В течение гарантийного срока, установленного поставщиком, осуществлять замену неисправных USB-токенов. Гарантия не распространяется на ущерб, возникший в результате неправильной эксплуатации, транспортировки, хранения USB-токенов.

#### 4. Порядок подключения к Системе

4.1. Одновременно с подписанным настоящим Соглашением КЛИЕНТ направляет в БАНК оформленное Заявление на подключение к услуге "Электронный банк" (Приложение 2). Ответственный сотрудник БАНКА имеет право не принимать к исполнению Заявление КЛИЕНТА, в котором допущены ошибки при заполнении пп. 1, 2, 3. Необходимые консультации КЛИЕНТ может получить по телефону службы технической поддержки, указанному в Заявлении, либо у ответственного сотрудника БАНКА, обслуживающего Клиента.

4.2. По желанию КЛИЕНТА установка и настройка АРМ может быть выполнена сотрудниками БАНКА, о чем КЛИЕНТ ставит соответствующую пометку в Заявлении на подключение к услуге (Приложение 2). Срок и порядок установки согласовывается сотрудником службы технической поддержки БАНКА непосредственно с уполномоченным сотрудником КЛИЕНТА дополнительно.

4.3. В перечень владельцев ключей ЭЦП (п.3. Приложения 2) включаются только лица имеющие, согласно карточке образцов подписей и оттиска печати, право первой/второй (единственной) подписи, либо лица, имеющие право получения выписок движения денежных средств по счету при наличии в Банке документов, подтверждающих их полномочия.

4.4. В качестве дополнительной меры безопасности, исключающей возможность работы с Системой с любой точки сети Интернет, рекомендуется указывать в Заявлении список разрешенных к доступу IP адресов (подсетей). По умолчанию, если Клиент не изъявил обратного желания, всем Клиентам при первичной регистрации включается режим ограничения разрешенных к работе IP адресов.

Пополнение списка разрешенных IP адресов производится в дальнейшем в соответствии с режимом указанным в Заявлении, т.е. либо только на основании соответствующего письменного заявления Клиента, либо в устной форме<sup>1</sup>, при условии успешной идентификации Клиента.

Если режим добавления новых IP адресов Клиентом в Заявлении не указан, то разрешается прием заявлений в устной форме.

4.5. До начала работы с Системой КЛИЕНТ должен получить в БАНКЕ программное обеспечение автоматизированного рабочего места Клиента, криптографическое программное обеспечение, документацию и инструкцию по его установке. Передача осуществляется на любом электронном носителе, доступом для КЛИЕНТА. Факт передачи средств криптографической обработки информации фиксируется Актом приема-передачи по форме Приложения 3.

4.6. В качестве меры безопасности, исключающей возможность несанкционированного копирования или хищения секретных ключей электронной цифровой подписи сотрудников Клиента, отдельно от хищения самого USB-токена, в качестве хранилища ключевой информации для ключей с правом подписи обязательны к использованию специальные аппаратные устройства – USB-токены «iBank 2 Key».

**Банк регистрирует (активирует) клиентские ключи с правом подписи, только если они были сохранены на USB-токены.**

Необходимое количество USB-токенов<sup>2</sup> Клиент получает в БАНКЕ, о чем делается соответствующая отметка в Заявлении на подключение к услуге (Приложение 2) при оформлении договора, либо оформляется Заявление на изменение параметров подключения к услуге по форме Приложения 6. Передача USB-токенов фиксируется Актом приема-передачи по форме Приложения 10.

4.7. Клиент самостоятельно, либо силами сотрудников Банка (в соответствии с Заявлением) выполняет подготовку к работе автоматизированного рабочего места, следуя полученным из Банка инструкциям по установке Системы.

---

<sup>1</sup> Идентификация клиента осуществляется Банком следующим образом:

- По телефону, службой технической поддержки Банка, если Клиент правильно назвал блокировочное слово, либо паспортные данные должностного лица Клиента, имеющего право подписи;
- При личной явке в Банк должностного лица, имеющего право подписи, при предъявлении документа удостоверяющего личность.

<sup>2</sup> При расчете необходимого количества USB-токенов необходимо иметь в виду следующее:

- Секретные ключи хранящиеся внутри токена не могут быть никуда скопированы - ни на другой носитель, ни на другой токен (продублированы). Это нужно иметь в виду в случае необходимости работы с нескольких рабочих мест в разных офисах.
- На одном токене возможно хранение до шестидесяти четырех секретных ключей ЭЦП. В соответствии с требованиями безопасности допускается хранение на одном токене ключей только одного физического лица. Технические ограничений на хранение на одном токене ключей разных юридических лиц, а также от систем разных банков нет, но при выборе хранилища ключей следует соблюдать требования предъявляемые имеющимися договорами по предоставлению услуг.

4.8. При отсутствии у КЛИЕНТА постоянного доступа в Интернет, либо по усмотрению Клиента, на рабочем месте клиента может быть выполнена установка отдельной программы «PC-Banking», с возможностью подготовки документов в режиме Off-Line. В состав дистрибутива программы входят сразу и криптографические средства и необходимое общесистемное программное обеспечение (JAVA RUNTIME ENVIRONMENT). Инструкция по его установке также передается Клиенту способом указанным в п.4.5.

4.9. Клиент самостоятельно, либо силами сотрудников Банка (согласно заявлению) выполняет со своего автоматизированного рабочего места процедуру регистрации предприятия в Системе и генерацию криптографических ключей, следуя имеющимся инструкциям. Необходимые консультации Клиент может получить по телефону службы технической поддержки, указанному в Заявлении на подключение к услуге (Приложение 2).

4.10. Генерация ключей ЭЦП выполняется лично владельцем сертификата ключа подписи. Результатом выполнения процедуры генерации ключа на клиентском рабочем месте являются файлы с секретными ключами ЭЦП. Основные требования и рекомендации по обеспечению информационной безопасности при их использовании и хранении изложены в Приложении 1 к Соглашению. Кроме того по окончании процедуры генерации ключа ЭЦП автоматически выполняется распечатка Сертификата сформированного открытого ключа подписи.

4.11. После выполнения процедуры регистрации Клиента на АП Банка и генерации ключей ЭЦП, оформленные и подписанные со стороны КЛИЕНТА Сертификаты ключей подписи передаются в БАНК.

4.12. Ответственный сотрудник БАНКА проверяет правильность оформления Сертификатов открытых ключей подписи, их соответствие карточке образцов подписей и оттиска печати и Заявлению на подключение к услуге (Приложение 2), и дополнительно вносит информацию о сроке окончания действия ключа подписи. Один экземпляр Сертификата открытого ключа после подписания остается в БАНКЕ, второй возвращается КЛИЕНТУ.

4.13. В случае правильного оформления поступивших документов, БАНК не позднее следующего рабочего дня осуществляет окончательную регистрацию КЛИЕНТА, активацию ключей и подключение Клиента к услуге.

4.14. При использовании Клиентом для хранения ключей USB-токенов, полученных не в Банке, с Клиента взимается комиссия согласно действующим Тарифам Банка, за каждый, вновь (первично) регистрируемый в Системе в процессе активации ключа Клиента, USB токен.

4.15. Завершение процедуры подключения Клиента оформляется Актом приема-сдачи работ по подключению КЛИЕНТА к услуге "Электронный банк" (Приложение 5), который является основанием для списания со счета КЛИЕНТА без дополнительного распоряжения КЛИЕНТА платежным требованием в безакцептном порядке комиссии за подключение к услуге согласно действующим тарифам БАНКА.

4.16. Включение КЛИЕНТА в реальную работу осуществляется БАНКОМ после получения им от КЛИЕНТА надлежащим образом оформленного и подписанного Акта, указанного в п. 4.15. настоящего Соглашения.

## **5. Порядок замены криптографических ключей.**

5.1. Плановая, либо внеплановая смена ключей ЭЦП осуществляется Клиентом непосредственно перед истечением срока действия сертификата должностного лица Клиента, в случае утраты, компрометации или подозрении на компрометацию ключей ЭЦП (см. также п. 3.3.3), а также в других случаях, при необходимости аннулирования сертификата ключа ЭЦП. В частности замена сертификата производится Клиентом в случае изменения любых реквизитов указанных в сертификате ключа ЭЦП: признаков идентифицирующих должностное лицо Клиента (документа удостоверяющего личность, должности, фамилии т.п.), признаков идентифицирующих юридическое лицо (наименования, юр. адреса и т.п.), изменения сроков действия полномочий, образца подписи и т.д.

Банк при получении от Клиента уведомления об утрате или компрометации ключа ЭЦП, либо заявления на смену ключа ЭЦП, блокирует работу ключа ЭЦП, и не принимает к исполнению электронные документы, подписанные данной ЭЦП от имени Клиента.

5.2. Клиент выполняет процедуру генерации, оформления и подписания новых криптографических ключей, в соответствии с пунктами 4.7 - 4.11 настоящего Соглашения. Замена ключей ЭЦП производится на основании Заявления на активацию (замену) ключей (Приложение 7), либо Заявления на изменение параметров подключения к услуге (Приложение 6).

## **6. Изменение параметров подключения.**

6.1. При необходимости изменения параметров подключения к услуге "Электронный банк", а также в случаях:

- изменении учредительных документов Клиента и прочих реквизитов, включая Ф.И.О., паспортные данные должностных лиц, наименование Клиента, изменение адреса и в остальных случаях требующих переоформления банковской карточки образцов подписей;
- добавления/удаления счетов клиента в список обслуживаемых по системе счетов;
- необходимости удаления или добавления владельцев ключей ЭЦП;

Клиент направляет в Банк, по месту обслуживания, оформленное и подписанное в двух экземплярах "Заявление на изменение параметров подключения к услуге "Электронный банк" по форме Приложения 6 (далее, в этом разделе, по тексту Заявление).

6.2. При оформлении Заявления Клиент может указать, по согласованию с ответственным сотрудником Банка, желаемое время проведения Банком работ, по внесению изменений в учетную запись Клиента.

6.3. В указанный период, на время выполнения работ, Банк блокирует работу учетной записи Клиента для исключения ошибок. При этом Клиент должен заблаговременно отправить в Банк все подготовленные для отправки и подписанные электронные платежные документы.

6.4. В случае расширения состава владельцев ключей Клиент, кроме Заявления, должен предоставить в Банк оформленные и подписанные Сертификаты ключей подписи.

6.5. Отключение, либо включение режима фильтрации IP адресов, с которых разрешена работа Клиенту, производится только на основании письменного заявления Клиента.

6.6. Добавление в список нового IP адреса возможно на основании как письменного, так и устного распоряжения Клиента, при условии его успешной идентификации, и в соответствии с режимом указанным в Заявлении<sup>3</sup>.

## **7. ПРАВИЛА проведения платежей с использованием системы «iBank 2»**

### **7.1. Общие положения**

7.1.1. Организация системы предполагает, что основным хранилищем всех клиентских ЭД является база данных АП БАНКА. При работе КЛИЕНТА с использованием Интернет браузера (модуль Internet-Банкинг), документы напрямую попадают и хранятся в базе данных АП БАНКА. При работе с использованием модуля «РС-Банкинг» документы попадают в базу данных АП БАНКА при выполнении операции «Синхронизация». КЛИЕНТ по желанию может использовать для работы любой из указанных модулей, либо оба.

7.1.2. Как при работе КЛИЕНТА с использованием модуля Internet-Банкинг, так и в случае использования модуля «РС-Банкинг», любой обмен информацией происходит через установленное защищенное соединение. При установке защищенного соединения используются ключи электронно-цифровой подписи клиента.

7.1.3. Любая информация передается по каналам связи только в зашифрованном виде.

7.1.4. Работа оператора на АП КЛИЕНТА в режиме Internet-Банкинга возможна только при наличии у оператора Клиента «секретного» ключа ЭЦП, который необходим для установки защищенного соединения. При работе оператора на АП КЛИЕНТА в модуле «РС-Банкинг», возможен вход в программу и автономная работа (просмотр и ввод документов, импорт, и т.п.) без ключевых носителей. Ключевой носитель с секретными ключами необходим только в момент обмена информацией с АП БАНКА.

---

<sup>3</sup> Идентификация клиента аналогична описанной в п 4.4.

7.1.5. ЭД Клиента, поступившие в БАНК в операционное время, исполняются БАНКОМ (или принимаются им к сведению, если документ не является распоряжением КЛИЕНТА) в сроки, установленные Договором банковского счета, п. 3.4.3. настоящего Соглашения, при условии, что проверка на подлинность ЭЦП дала положительный результат, документ оформлен правильно, не противоречит действующему законодательству Российской Федерации и нормативным актам Банка России.

7.1.6. Все исполненные БАНКОМ ЭД КЛИЕНТА распечатываются, на них проставляются штамп БАНКА и личная подпись сотрудника, после чего ЭД КЛИЕНТА помещаются в документы дня БАНКА.

7.1.7. ЭД Клиента, поступившие в БАНК в операционное время, но оформленные ненадлежащим образом (не соответствующие действующему законодательству Российской Федерации, нормативным документам Банка России), либо требующие предоставления дополнительных документов для их исполнения, не подлежат исполнению БАНКОМ, о чем КЛИЕНТУ в течение текущего рабочего дня направляется соответствующее сообщение с указанием причины не исполнения ЭД.

## 7.2. Подготовка платежных ЭД

7.2.1. КЛИЕНТ осуществляет ввод платежного ЭД в программу, руководствуясь инструкцией по работе с программой, а также нормативными актами Банка России. При наличии соответствующих программных средств платежные ЭД могут импортироваться из бухгалтерской системы предприятия КЛИЕНТА.

7.2.2. Новый платежный ЭД может быть сформирован на основе любого платежного ЭД в выписке КЛИЕНТА (копия документа), либо на основе заранее сформированных шаблонов платежных ЭД.

7.2.3. Текущая стадия обработки платежных ЭД в автоматизированной системе, как на АП КЛИЕНТА, так и на АП БАНКА отображается статусом платежного ЭД. Обновление статусов платежных ЭД на АП КЛИЕНТА происходит при выполнении операции «Обновить/Синхронизировать», после установки соединения, либо выполнении действия «обновить» в текущем рабочем окне.

7.2.4. Подписание платежных ЭД производится владельцами сертификата ключа подписи с использованием ключей ЭЦП, зарегистрированных на АП БАНКА, с правом первой/второй/единственной подписи (согласно Заявлению). Документ получает статус «Подписан».

## 7.3. Передача платежных ЭД в БАНК и их обработка в БАНКЕ.

7.3.1. Процедура обмена информацией с БАНКОМ может быть выполнена на АП КЛИЕНТА только при наличии «ключевой дискеты». При получении подписанных платежных ЭД БАНК проверяет подлинность ЭЦП, используя имеющиеся «открытые» ключи Клиента. В случае успешной проверки ЭЦП в БАНКЕ, документ получает статус «Доставлен».

7.3.2. После получения платежного ЭД КЛИЕНТА на АП БАНКА происходит его следующая обработка:

- АП БАНКА с периодичностью раз в несколько минут производит передачу платежных ЭД в автоматизированную систему БАНКА, при этом выполняется автоматический контроль реквизитов каждого платежного ЭД. В случае успешной проверки платежный ЭД получает статус "На обработке", либо «Отвергнут» в противном случае.

- Ответственные сотрудники БАНКА обрабатывает поступающие платежные ЭД в автоматизированной системе БАНКА по мере их поступления. После обработки платежного ЭД в автоматизированной системе БАНКА, ЭД получает статус «На исполнении» (либо «Отвергнут» в зависимости от выполненной операции обработки).

- Технологический цикл обработки платежного ЭД завершается его исполнением в автоматизированной системе БАНКА, после чего, по истечении некоторого периода времени ЭД получает статус «Исполнен» на АП БАНКА.

## 7.4. Обработка в БАНКЕ платежных ЭД КЛИЕНТА в валюте РФ

7.4.1. В Системе «iBank 2» оформление платежного ЭД предполагает указание счета плательщика и счета получателя только в валюте РФ.

7.4.2. В Системе возможны следующие состояния платежных ЭД:

- «Новый» – только что введенный документ, не имеющий подписей ЭЦП КЛИЕНТА;
- «Подписан» – документ, на котором установлено необходимое количество ЭЦП КЛИЕНТА
- «Доставлен» – документ, имеющий необходимое количество ЭЦП КЛИЕНТА и зарегистрированный на АП БАНКА
- «На обработке» – документ, переданный на обработку в АБС БАНКА
- «На исполнении» – документ, принят к исполнению в АБС БАНКА
- «Исполнен» – документ, исполненный в АБС БАНКА. Документ в этом состоянии виден в выписке по счету Клиента
- «Отвергнут» – документ, не прошедший автоматический контроль на АП БАНКА, либо отвергнутый ответственным исполнителем БАНКА, либо отозванный КЛИЕНТОМ.

7.4.3. В Системе, кроме автоматического контроля платежных ЭД на АП БАНКА, производится их контроль ответственными исполнителями БАНКА. Платежный ЭД может быть отбракован ответственным исполнителем вручную, при этом указывается причина отбраковки, а платежный ЭД получает статус “Отвергнут”.

7.4.4. Отзыв КЛИЕНТОМ платежного ЭД осуществляется путем выполнения запроса на отзыв платежного ЭД. Отзыв, так же как и платежный ЭД, подписывается ЭЦП КЛИЕНТА и направляется в БАНК по Системе. В случае если отзываемый платежный ЭД еще не имеет статуса "На исполнении", отзыв исполняется на АП Банка автоматически, в противном случае запрос на отзыв автоматически отвергается. В этом случае, для отзыва ЭД следует обращаться непосредственно к ответственным исполнителям БАНКА. В случае успешной обработки отзыва, отзываемый платежный ЭД получает статус "Отвергнут".

7.4.5. После того как платежный ЭД будет исполнен БАНКОМ, ему присваивается статус «Исполнен».

## 7.5. Обработка в БАНКЕ платежных ЭД КЛИЕНТА в иностранной валюте

7.5.1. В системе реализованы все основные виды платежных валютных документов:

- Заявление на перевод валюты
- Поручение на покупку иностранной валюты
- Поручение на продажу иностранной валюты
- Межбанковский перевод
- Распоряжение на обязательную продажу иностранной валюты
- Поручение на обратную продажу иностранной валюты

7.5.2. Процедура ввода и обработки на АП БАНКА валютных платежных ЭД аналогична процедуре обработки платежных ЭД в валюте РФ.

## 7.6. Получение выписки по счету

7.6.1. Вся информация о движении средств по счетам КЛИЕНТА хранится на АП БАНКА. АП БАНКА регулярно, с периодичностью в один час, обновляет выписки по счетам Клиентов, формируя запросы к АБС БАНКА.

7.6.2. Для просмотра выписки по счету на АП КЛИЕНТА используется соответствующая операция - «Получить» в разделе типов документов «Выписки». При выполнении операции необходимо указать требуемый период. Печать выписки по счету выполняется здесь же после получения выписки по счету на АП КЛИЕНТА и за тот же запрошенный период.

7.6.3. Так как любой обмен информацией с Банком, в том числе и получение выписки, требует наличия у сотрудника Клиента секретных ключей ЭЦП, принята практика оформления ключей ЭЦП без права подписи для сотрудников в обязанности которых входит только просмотр выписок по счетам, при условии наличия в Банке документов подтверждающих их полномочия.

## 8. Действия сторон в случае восприятия аналога собственноручной подписи как фальшивой

8.1. В случае если ЭЦП на ЭД признана на АП БАНКА недействительной, либо при невозможности проверки ЭЦП данного ЭД, КЛИЕНТ вновь создает ЭД, подписывает его ЭЦП и направляет БАНКУ.

8.2. В случае неудачи при повторной проверке ЭЦП на ЭД Стороны осуществляют повторную процедуру обмена ключами ЭЦП в порядке, установленном настоящим Соглашением.

8.3. До завершения процедуры повторного обмена ключами ЭЦП работа КЛИЕНТА в системе блокируется, и стороны переходят на расчетное обслуживание в обычном порядке, т.е. с использованием платежных документов на бумажных носителях.

## **9. Действия Сторон в случае возникновения разногласий по поводу исполнения /неисполнения ЭД (досудебный порядок урегулирования споров)**

9.1. В случае возникновения разногласий у Сторон по поводу исполнения БАНКОМ ЭД, который был подписан ЭЦП КЛИЕНТА, воспринятой БАНКОМ подлинной, а также в случае неисполнения БАНКОМ ЭД, который был подписан ЭЦП, воспринятой БАНКОМ фальшивой, Стороны урегулируют возникшие разногласия следующим образом.

9.2. КЛИЕНТ представляет БАНКУ заявление, содержащее существо претензии с указанием на электронный документ, на основании которого БАНК выполнил оспариваемую операцию по счёту КЛИЕНТА.

9.3. Не позднее 10-ти рабочих дней с момента возникновения разногласий Сторонами создается Согласительная комиссия. В состав комиссии включаются по два представителя от каждой из сторон. При необходимости в состав комиссии могут быть включены представители компании-разработчика Системы – ООО «БИФИТ», а по специальному требованию одной из Сторон – независимые эксперты. Члены комиссии назначаются решением каждой Стороны.

9.4. В случае если КЛИЕНТ не направляет своих представителей он лишается права предъявления каких-либо возражений по выводам Согласительной комиссии.

9.5. Стороны обязуются способствовать работе Согласительной комиссии и не допускать отказа от предоставления необходимых документов.

9.6. Стороны обязуются предоставить Согласительной комиссии возможность ознакомления с условиями и порядком работы своих программных и аппаратных средств, используемых в Системе.

9.7. В ходе работы Согласительной комиссии каждая Сторона обязана доказать, что она исполнила обязательства по настоящему Соглашению надлежащим образом.

9.8. Согласительная комиссия проводит рассмотрение заявления в течение пяти дней. Рассмотрение заявления включает следующие этапы:

- Проверка идентичности открытого ключа ЭЦП, хранящегося в Системе, открытому ключу ЭЦП, хранящемуся в БАНКЕ на бумажном носителе. При обнаружении расхождений ситуация далее не рассматривается как не соответствующая заявленной.

- Оценка хранящегося в Системе оспариваемого ЭД путем проверки наличия и корректности ЭЦП КЛИЕНТА, на основании которого БАНКОМ выполнены оспариваемые КЛИЕНТОМ действия. Выполнение процедуры проверки ключей ЭЦП осуществляется в штатном ПО Системы – модуль «Операционист». Выбирается необходимый ЭД и выполняется операция “Проверить ЭЦП”. При невозможности получить доступ к ЭД через модуль «Операционист», могут использоваться специализированные утилиты от разработчика Системы – компании «БИФИТ», для выгрузки ЭД из базы данных Системы и автономной его проверки.

9.9. По результатам работы Согласительной комиссией составляется акт, содержащий:

- фактические обстоятельства, послужившие основанием возникновения разногласий;
- порядок работы членов комиссии;
- вывод о подлинности (ложности, приеме, передаче, отзыве и т.п.) оспариваемого ЭД и его обоснование.

9.10. Указанный Акт признается Сторонами в качестве окончательного документа, разрешающего возникшие разногласия.

9.11. Услуги эксперта оплачиваются Сторонами в равных долях. В случае если КЛИЕНТ не направил своих представителей для участия в работе Согласительной комиссии, он обязан возместить БАНКУ расходы, связанные с оплатой услуг эксперта в полном объеме.

9.12. БАНК несет ответственность перед КЛИЕНТОМ в случае, когда имело место хотя бы одна из следующих ситуаций:

- БАНК не предъявил ЭД, переданного КЛИЕНТОМ, на основании которого БАНК выполнил оспариваемую операцию по счёту КЛИЕНТА;
- Хотя бы одна ЭЦП КЛИЕНТА в ЭД оказалась некорректной;
- ЭД подписан недействующей ЭЦП. ЭЦП признается недействующей, если заблаговременно КЛИЕНТ уведомил БАНК об отмене действия секретного и соответствующего ему открытого ключа ЭЦП КЛИЕНТА путем направления в БАНК соответствующего заявления, подписанного уполномоченным лицом КЛИЕНТА и имеющего оттиск печати КЛИЕНТА (Приложение 6 или Приложение 7), с обязательным проставлением на заявлении «входящего» штампа БАНКА. При этом дата получения БАНКОМ заявления и дата, с которой согласно п. 7 заявления вводится новая ЭЦП, должна быть раньше даты получения БАНКОМ оспариваемого ЭД.

9.13. В случае если БАНК предъявляет оспариваемый ЭД, электронно-цифровая подпись КЛИЕНТА, которой подписан ЭД, признана разрешительной комиссией корректной, и принадлежность открытых ключей ЭЦП КЛИЕНТУ подтверждена, БАНК ответственности перед КЛИЕНТОМ по выполненным операциям по счёту КЛИЕНТА не несет.

9.14. Если КЛИЕНТ настаивает на том, что данный ЭД он не создавал и/или не подписывал одной или несколькими ЭЦП, разрешительная комиссия может вынести определение о компрометации секретного ключа (ключей) ЭЦП Клиента. При этом риск убытков, вызванных исполнением БАНКОМ такого ЭД, несет КЛИЕНТ.

## 10. Ответственность сторон

10.1. За неисполнение или ненадлежащее исполнение обязательств, принятых на себя в соответствии с настоящим Соглашением, стороны несут ответственность, предусмотренную действующим законодательством Российской Федерации.

10.2. Каждая сторона имеет право требовать от другой стороны возмещения убытков, возникших у нее в связи с несоблюдением другой стороной условий настоящего Соглашения.

10.3. КЛИЕНТ несет риск убытков, связанных с получением третьими лицами несанкционированного доступа к ключам ЭЦП, до момента получения БАНКОМ уведомления от КЛИЕНТА об указанном факте;

10.4. КЛИЕНТ несет риск убытков, связанных с невозможностью передачи ЭД (неисправности электронной техники, сбой в передаче информации по сети, нарушение программ шифрования электронных документов и т.д.);

10.5. КЛИЕНТ несет риск убытков, связанных с неисполнением ЭД в случае несоблюдения правил пользования предоставленными ему программными средствами;

10.6. БАНК освобождается от ответственности в случаях, если:

- КЛИЕНТОМ допущено несвоевременное оповещение об утрате или раскрытии ключей ЭЦП;
- КЛИЕНТОМ не была обеспечена конфиденциальность хранения ключей ЭЦП;
- КЛИЕНТ не обеспечил сохранность программных средств в процессе их использования;
- Владелец сертификата ключа подписи нарушил обязательства по хранению и использованию сертификата ключа подписи, установленные законом (ст. 12 Закона РФ «Об электронной цифровой подписи»), и обязательства, принятые им на себя при подписании настоящего Соглашения и требований информационной безопасности, изложенных в Приложении 1 настоящего соглашения.

## 11. Срок действия Соглашения

11.1. Настоящее Соглашение вступает в действие с момента его подписания Сторонами и прекращается одновременно с прекращением действия Договоров.

11.2. Права и обязанности по ЭД, подписанным ЭЦП, возникают после подписания Сторонами Акта приемки-сдачи работ по подключению клиента к услуге «Электронный банк» (Приложение 5).

11.3. Настоящее Соглашение может быть также расторгнуто:

11.3.1. По инициативе одной из Сторон, в связи с отказом от использования системы «iBank 2» в отношениях с другой Стороной, о чем иницилирующая Сторона обязана предупредить другую Сторону не позднее чем за 10 рабочих дней до досрочного расторжения;

11.3.2. В одностороннем порядке БАНКОМ в случае нарушения КЛИЕНТОМ правил обмена ЭД и обеспечения безопасности проведения безналичных расчетов и иных операций с использованием ЭД, предусмотренных действующим законодательством Российской Федерации.

11.3.3. По соглашению Сторон.

11.4. В случае расторжения настоящего Соглашения платежные документы КЛИЕНТА принимаются БАНКОМ на бумажных носителях на общих основаниях.

11.5. БАНК вправе отказать в исполнении ЭД (приостановить обслуживание КЛИЕНТА в системе «iBank 2») без расторжения настоящего Соглашения в случае совершения КЛИЕНТОМ сомнительных операций либо при наличии оснований полагать, что система «iBank 2» используется неуполномоченными КЛИЕНТОМ перед БАНКОМ лицами.

11.5.1. Решение о приостановлении операций принимается БАНКОМ согласно его внутренним правилам, которые КЛИЕНТУ не сообщаются.

11.5.2. Об отказе (приостановлении обслуживания в системе «iBank 2») БАНК немедленно уведомляет КЛИЕНТА по телефону, по системе «iBank 2», также направляет в адрес КЛИЕНТА уведомление заказным письмом.

11.5.3. В случае предоставления КЛИЕНТОМ информации и документов либо совершения иных действий (включая прибытие в Банк руководителя, акционеров (участников), иных уполномоченных лиц), которые позволят устранить сомнения, послужившие основаниями для отказа (приостановления) от обслуживания, БАНК возобновляет обслуживание КЛИЕНТА в системе «iBank 2».

11.5.4. БАНК не несет ответственности перед КЛИЕНТОМ за отказ (приостановление обслуживания в системе «iBank 2»), предусмотренный пунктом 11.5. настоящего Соглашения, поскольку такой отказ (приостановление) не лишает КЛИЕНТА возможности проведения операций по его счетам на основании документов на бумажных носителях.

11.6. После расторжения настоящего Соглашения Клиент обязан самостоятельно удалить установленные у него программное обеспечение системы «iBank 2» и вернуть Банку полученные при заключении Соглашения носители с дистрибутивом программного обеспечения «iBank 2» и инструкцией по формированию ключей ЭЦП, либо уничтожить дистрибутив программного обеспечения, если он был получен из Банка другим способом. Удаление или уничтожение программного обеспечения системы «iBank 2» оформляется Клиентом односторонним актом произвольной формы, который Клиент обязан предоставить в Банк в течение 3 (Трех) дней с момента прекращения действия настоящего Соглашения. Возврат носителя с дистрибутивом программного обеспечения «iBank 2» и инструкцией по формированию ключей ЭЦП оформляется двусторонним актом произвольной формы, который Клиент обязан предоставить в Банк для подписания в течение 3 (Трех) дней с момента прекращения действия настоящего Соглашения.

11.7. Настоящее Соглашение составлено в двух экземплярах, имеющих равную юридическую силу, по одному экземпляру для БАНКА и КЛИЕНТА.

## **12. Порядок расчетов по Соглашению**

12.1. Оплата услуг БАНКА, оказываемых в рамках настоящего Соглашения, осуществляется в размере и в порядке, установленном действующими Тарифами БАНКА.

12.2. Настоящим КЛИЕНТ предоставляет БАНКУ полномочия, а БАНК на этом основании имеет право списать платежным требованием в безакцептном порядке со счета КЛИЕНТА, открытого в БАНКЕ, без дополнительного распоряжения КЛИЕНТА, денежные средства в счет оплаты комиссии за оказание КЛИЕНТУ услуг, предусмотренных настоящим Соглашением, а также в счет возмещения БАНКУ расходов, связанных с оплатой услуг эксперта, участвующего в Согласительной комиссии (п. 9.11 настоящего Соглашения).

## **13. Порядок рассмотрения споров**

13.1. Не урегулированные Сторонами споры и разногласия, возникающие при исполнении настоящего Соглашения, а также при исполнении всех сделок, совершенных в связи и в соответствии с настоящим Соглашением, включая споры о возмещении убытков, причиненных сторонам в связи с использованием аналога собственноручной подписи, разрешаются в Арбитражном суде Приморского края после обязательного выполнения досудебного порядка разрешения споров в соответствии с п.9 настоящего Соглашения. Применимым правом является материальное право Российской Федерации.

**14. Адреса, реквизиты и подписи Сторон:**

Банк: *Акционерный коммерческий банк "Балтийский Банк Развития" (закрытое акционерное общество)*

Российская Федерация, 121099, г. Москва, 1-ый Николощеповский пер., д. 6, стр. 1.

тел.: (495)363-9162

ИНН 3900001002, ОГРН 1027700074775

*Филиал Акционерного коммерческого банка "Балтийский Банк Развития" (закрытое акционерное общество) в г. Владивостоке*

Российская Федерация, 690002, г. Владивосток, Океанский проспект, дом 131 в

тел./факс:(4232) 32-56-65

ИНН 3900001002/КПП 254043001, ОКПО 53650318,

ОКВЭД 65.12,

к/с 30101810000000000867 в ГРКЦ ГУ Банка России по Приморскому краю, БИК 040507867

Заместитель Управляющего ФАКБ "Балтийский Банк Развития", Владивосток

\_\_\_\_\_/ А.В. Просянников

Главный бухгалтер ФАКБ "Балтийский Банк Развития", Владивосток

\_\_\_\_\_/ Н.А.Козуб

м.п.

**Ответственный сотрудник ФАКБ «Балтийский Банк Развития», Владивосток**

**Контактные телефоны: (4232)\_\_\_\_\_**

Клиент: \_\_\_\_\_

Местонахождение: \_\_\_\_\_

тел: \_\_\_\_\_

ИНН \_\_\_\_\_

\_\_\_\_\_  
(должность руководителя)

\_\_\_\_\_  
(И.О.Ф. руководителя)

Главный бухгалтер

\_\_\_\_\_  
(И.О.Ф. главного бухгалтера)

м.п.