

**УТВЕРЖДЕНО**  
На заседании Правления  
ПАО АКБ «Приморье»  
22.02.2018 г. Протокол № 9  
Председатель Правления

\_\_\_\_\_ С.Ю. Белавин

«\_\_» \_\_\_\_\_ 20\_\_ г.

## **Договор на обслуживание Клиента по системе «iBank2» (Публичная оферта)**

### **1. СТАТУС ДОГОВОРА**

**1.1.** Настоящий Договор на обслуживание Клиента по системе «iBank2», далее — «Договор», является Договором присоединения, регулирующим отношения по обслуживанию Клиента по системе «iBank2» юридического лица или индивидуального предпринимателя в ПАО АКБ «Приморье», далее - «Банк».

**1.2.** Опубликование Договора, включая распространение его текста и приложений к нему на web-странице Банка в Интернете (сайт ПАО АКБ «Приморье» по адресу [www.primbank.ru](http://www.primbank.ru)) необходимо рассматривать как публичное предложение (оферта) Банка, адресованное юридическим лицам и индивидуальным предпринимателям для заключения Договора на предлагаемых условиях в соответствии со ст. 428 Гражданского Кодекса РФ.

**1.3.** Заключение Договора производится путем присоединения к его условиям в следующем порядке: Клиенты представляют в Банк подписанное со своей стороны Заявление об акцепте в форме, установленной Банком, приведенной в Приложении № 1 к настоящему Договору.

**1.4.** Оригинал Договора, оформленный надлежащим образом (листы прошиты, пронумерованы, скреплены подписью Председателя Правления и печатью Банка), хранится в Центральном офисе Банка и применяется в качестве доказательства в случае возникновения споров.

### **2. ТЕРМИНЫ, ПРИМЕНЯЕМЫЕ В ДОГОВОРЕ**

**Термины, применяемые в тексте настоящего Договора, используются в следующем значении:**

**2.1.** Система «iBank2» - совокупность программно-аппаратных средств, устанавливаемых на территории Клиента и Банка, и согласовано эксплуатируемых Клиентом и Банком в соответствующих частях, а также организационных мероприятий, проводимых Клиентом и Банком, с целью предоставления Клиенту услуг по настоящему Договору.

**2.2.** В зависимости от выбора Клиента клиентская часть Системы «iBank 2» может работать в одном и/или двух режимах: «РС – банкинг» или «Интернет – банкинг».

**При выборе режима работы «РС - банкинг»** - система работает через программное обеспечение, установленное на компьютер Клиента. Все необходимые электронные документы подготавливаются на компьютере Клиента без подключения к сети Интернет и передаются в Банк при установлении связи с сетью Интернет.

**При выборе режима работы «Интернет - банкинг»** - система работает через браузер, поддерживающий технологию Web. Доступ в систему осуществляется в реальном режиме времени при постоянном подключении к сети Интернет.

**2.3.** «Электронный документ» (ЭД) – совокупность байт, содержащая финансовый документ или информационное сообщение Клиента.

**2.4.** «Электронная подпись» (ЭП) – совокупность символов, формируемая Клиентом, однозначно сопоставляемая электронному документу и используемая для аутентичности (подтверждение авторства и целостности) электронного документа. Количество ЭП, необходимых для подтверждения электронного документа, определяется согласно карточке с образцами подписей и оттиска печати Клиента.

**2.5.** «Ключ ЭП Клиента» – уникальная последовательность символов, самостоятельно генерируемая Клиентом с использованием средств системы «iBank2», и предназначенная для формирования Клиентом электронной подписи электронных документов.

**2.6.** «Ключ проверки ЭП Клиента» – уникальная последовательность символов, однозначно связанная с ключом ЭП Клиента, самостоятельно генерируемый Клиентом с использованием средств системы «iBank2», и предназначенная для проверки Банком корректности электронной подписи электронного документа, сформированного Клиентом.

**2.7.** «Корректная ЭП Клиента» – электронная подпись электронного документа Клиента, дающая положительный результат ее проверки с использованием ключа проверки ЭП Клиента.

**2.8.** «Сертификат ключа проверки ЭП Клиента» – документ на бумажном носителе, с представленным в шестнадцатеричном виде ключа проверки ЭП Клиента, заверенный подписью руководителя и имеющий оттиск печати Клиента.

**2.9.** «Пара ключей ЭП Клиента» – ключ ЭП Клиента и соответствующий ему ключ проверки ЭП Клиента.

**2.10.** «Компрометация ключей» – утрата доверия к тому, что используемые ключи ЭП Клиента обеспечивают безопасность информации. К событиям, связанным с компрометацией ключей ЭП, относятся, включая, но, не ограничиваясь, следующие:

- Утрата ключа ЭП Клиента или носителя с ключом ЭП Клиента (утрата ключа);
- Утрата ключа с последующим обнаружением;
- Увольнение сотрудников, имевших доступ к ключам;
- Нарушение правил хранения и использования Ключевого носителя (Приложение № 4 к настоящему Договору);
- Случай, когда нельзя достоверно установить, что произошло с носителями ключей (в том числе случаи, когда носитель вышел из строя и достоверно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

**2.11. «Блокировочное слово»** - уникальное слово, определяемое Клиентом при регистрации в системе «iBank 2», для блокирования работы Клиента в системе по телефонному звонку.

**2.12. «Ключевой носитель»** - аппаратное устройство для обеспечения неизвлекаемого хранения и использования ключа ЭП Клиента в защищенной области памяти устройства, а также формирования ЭП Клиента под электронным документом по Российскому криптографическому алгоритму ГОСТ Р34.10-2001 непосредственно внутри устройства. С 01.01.2019 ключевым носителем является аппаратное устройство для обеспечения неизвлекаемого хранения и использования ключа ЭП Клиента в защищенной области памяти устройства, а также формирования ЭП Клиента под электронным документом по Российскому криптографическому алгоритму ГОСТ Р34.10-2012 непосредственно внутри устройства.

**2.13. «Генератор одноразовых паролей»** - аппаратное устройство для обеспечения дополнительной авторизации электронных документов и/или аутентификации Клиента в системе «iBank2» персональным одноразовым паролем, действие которого ограничено определенным интервалом времени.

**2.14. «Поставщик»** – организация или физическое лицо, осуществляющее продажу Ключевых носителей и/или Генераторов одноразовых паролей.

**2.15. Услуга «SMS информирование» (Далее Услуга)** - Услуга, порядок оказания и пользования которой регламентируется настоящим Договором, позволяющая Клиенту (Пользователю) получать короткие сообщения на мобильные телефоны, в том числе одноразовые пароли на подтверждение платежных поручений и/или при входе в Систему «iBank2», и об операциях, совершенных по счету (-ам) Клиента, открытому (ым) в Банке и подключенного (ым) к Системе «iBank2»

**2.16. «Клиент»** - юридическое лицо или индивидуальный предприниматель.

**2.17. «Пользователь»** - сотрудник Клиента, номер мобильного телефона которого предоставляется для использования Услуги «SMS информирование».

**2.18. «Лимит на исходящие платежные поручения»** - максимальное ограничение суммы одного платежного поручения и/или ограничение сумм поручений за определенный период времени.

**2.19. «Доверенные получатели»** - перечень получателей определенных Клиентом, в адрес которых могут совершаться переводы денежных средств.

### **3. ПРЕДМЕТ ДОГОВОРА**

**3.1.** Банк подключает счета Клиента к системе «iBank2» на основании Заявления об акцепте (Приложение № 1 к настоящему Договору). В процессе обслуживания Банк подключает дополнительные счета на основании заявлений Клиента, предоставленных на бумажных носителях или переданных по системе дистанционного банковского обслуживания.

**3.2.** Банк осуществляет обслуживание банковских (расчетных, текущих, специальных, транзитных и др.) счетов Клиента с использованием системы «iBank2», позволяющей передавать электронные документы и принимать выписки и информационные сообщения.

### **4. СОГЛАШЕНИЕ СТОРОН**

**4.1.** Стороны признают, что встроенное средство криптографической защиты информации в системе «iBank2» обеспечивает необходимый уровень защиты информации от несанкционированного доступа, подтверждения подлинности и авторства электронных документов, а также разбора конфликтных ситуаций.

**4.2.** Стороны признают, что при изменении электронного документа, заверенного электронной подписью, ЭП становится некорректной, то есть проверка ЭП дает отрицательный результат.

**4.3.** Стороны признают, что подделка ЭП Клиента, то есть создание корректной электронной подписи электронного документа от имени Клиента, невозможна без знания пароля и наличия ключа ЭП Клиента.

**4.4.** Стороны признают, что электронные документы, заверенные необходимым количеством электронных подписей Клиента, юридически эквивалентны соответствующим документам на бумажном носителе, подписанным Клиентом и имеющим оттиск печати Клиента, обладают юридической силой и подтверждают наличие правовых отношений между Сторонами. Электронные документы без необходимого количества электронных подписей Клиента не имеют юридической силы, Банком не рассматриваются и не исполняются.

**4.5.** Стороны признают, что электронные документы с электронными подписями Клиента, созданные системой «iBank2» и полученные сервером Банка, являются материалом для решения спорных вопросов в соответствии с «Процедурой проведения технической экспертизы при возникновении спорных ситуаций» (Раздел №13 настоящего Договора).

**4.6.** Стороны согласны с тем, что наличие у Банка надлежаще оформленного Электронного документа, подписанного ЭП Клиента, проверка подлинности которой ключом проверки ЭП Клиента дала положительный результат, является основанием для проведения Банком соответствующей операции на основании указанного Электронного документа.

**4.7.** Электронные документы, не имеющие необходимого количества электронных подписей, при наличии спорных вопросов, не являются доказательным материалом.

**4.8.** Стороны признают, что ключ проверки ЭП Клиента, указанный в заверенном подписью руководителем и оттиском печати Клиента Сертификате ключа проверки ЭП Клиента, принадлежит Клиенту и используется для проверки подлинности ЭП Клиента.

**4.9.** В процессе эксплуатации Системы «iBank2» Стороны самостоятельно выполняют на своей территории мероприятия, обеспечивающие безопасность аппаратно-программных средств Системы, защиту ключей, паролей и ресурсов Системы от несанкционированного доступа.

**4.10.** Банк и Клиент обеспечивают хранение архивов электронных документов в течение срока, установленного для хранения соответствующих документов на бумажном носителе.

### **5. ПРАВА И ОБЯЗАННОСТИ КЛИЕНТА**

**5.1.** Для подключения к системе «iBank2» Клиент обязан следовать п.п. 8.1 – 8.6 настоящего Договора.

**5.2.** Клиент обязан назначить из числа своих сотрудников ответственного представителя по взаимодействию с Банком в вопросах обслуживания Клиента с использованием системы «iBank2».

**5.3.** Клиент обязан использовать Ключевые носители и Генераторы одноразовых паролей, передаваемые Банком Клиенту, в качестве устройств для хранения секретного ключа ЭП и обеспечения дополнительной авторизации электронных документов и/или аутентификации Клиента в системе «iBank2» персональным одноразовым паролем соответственно. Ключевые носители и Генераторы одноразовых паролей, предоставляемые другими поставщиками, к использованию не допускаются. В случае внесения изменений в соответствии с законодательными или иными нормативными документами в ГОСТ устанавливающий требования к формированию электронной подписи

на ключевом носителе, смена ключевого носителя осуществляется за счет Клиента. Оплата устройств производится согласно действующим тарифам Банка.

**5.4.** Клиент обязан контролировать доставку электронных документов в Банк и его обработку на основе передаваемого Банком результата приема ЭД. ЭД считается принятым и обработанным Системой «iBank2» только в том случае, если Клиент получил соответствующий положительный результат.

**5.5.** Клиент обязан по требованию Банка заверить подписями и печатью распечатанные Банком, принятые по Системе и проведенные по счету Клиента платежные документы или предоставить оригиналы вышеуказанных документов.

**5.6.** Клиент обязан обеспечить сохранность в тайне от посторонних лиц информацию о ключах ЭП должностных лиц, уполномоченных распоряжаться счетом. Ключевые носители ключа ЭП должны храниться у лиц, для генерации подписи ЭП которых они используются и, как правило, не подлежат выносу из служебного помещения Клиента.

**5.7.** Клиент обязан не передавать третьим лицам программное обеспечение, документацию Системы, сведения по форматам ЭД и технологии их обработки Клиентом и Банком, относящиеся к данному Договору.

**5.8.** Клиент обязан содержать компьютеры, с которых осуществляется работа с системой «iBank2», в технически исправном состоянии, и обеспечить их нахождение в служебном помещении, как правило, доступ в которое разрешен только тем сотрудникам Клиента, которые непосредственно работают с системой.

**5.9.** На любом компьютере/ноутбуке, с которого производится работа с системой «iBank2», Клиент обязан использовать актуальное лицензионное антивирусное программное обеспечение и штатный защитный экран Брандмауэр Windows, либо другой межсетевой экран (*firewall*) в режиме постоянной работоспособности и максимальной степени защиты, а также обеспечить регулярное обновление антивирусных баз и операционной системы.

**5.10.** Клиент обязан допускать к эксплуатации системы только сотрудников, имеющих соответствующую подготовку.

**5.11.** Клиент обязан сообщать Банку об обнаружении попытки несанкционированного доступа к системе «iBank2» не позднее следующего дня с момента обнаружения.

**5.12.** Клиент обязан незамедлительно извещать Банк обо всех случаях компрометации ключей ЭП, а также при утере и выходе из строя Генератора одноразовых паролей.

**5.13.** Клиент обязан производить генерацию новой пары ключей ЭП должностных лиц, уполномоченных распоряжаться счетом, не реже 1 раза в год

**5.14.** В случае изменения в составе руководства Клиента (смена руководителя, главного бухгалтера и иных лиц, указанных в карточке с образцами подписей и оттиска печати) Клиент обязан незамедлительно сообщить об этом Банку (с предоставлением соответствующих документов), сгенерировать новую пару ключей ЭП и зарегистрировать новый ключ проверки ЭП в Банке.

**5.15.** Клиент обязан в случае прекращения использования системы «iBank2» уничтожить ключ ЭП Клиента.

**5.16.** Клиент обязан заполнять электронные документы в системе «iBank2» в соответствии с действующим «Положением о правилах осуществления перевода денежных средств».

**5.17.** Клиент обязан хранить в секрете и не передавать третьим лицам пароль и носитель с ключом ЭП Клиента, а также Генератор одноразовых паролей, используемые в системе.

**5.18.** Клиент обязан по требованию Банка сгенерировать новую пару ключей ЭП Клиента и зарегистрировать новый ключ проверки ЭП Клиента в Банке.

**5.19.** Клиент имеет право досрочно прекратить действие своего активного ключа ЭП Клиента и соответствующего ему ключа проверки ЭП Клиента направив в Банк «Уведомление об отмене действия Пары ключей ЭП Клиента» (Приложение № 5 к настоящему Договору) в двух экземплярах и потребовать от Банка заблокировать этот активный ключ проверки ЭП Клиента.

**5.20.** Клиент имеет право по своему усмотрению генерировать новые пары ключей ЭП Клиента и регистрировать в Банке новые ключи проверки ЭП Клиента.

**5.21.** Клиент имеет право, позвонив в службу технической поддержки систем дистанционного банковского обслуживания Банка, и произнеся блокировочное слово, впредь до письменного уведомления, заблокировать свою работу в системе «iBank2».

**5.22.** Клиент имеет право отозвать ранее переданный в Банк электронный документ, имеющий корректную подпись ЭП, путем направления в Банк по системе «iBank2» соответствующего уведомления защищенного ЭП, при условии, что Банк к моменту получения уведомления не произвел списание со счета Клиента денежных средств во исполнение ранее полученного от Клиента электронного документа.

**5.23.** Клиент имеет право выбрать один или несколько видов дополнительных услуг по обеспечению безопасности при работе в системе «iBank2»:

- Аутентификация Клиента с помощью одноразового персонального пароля при входе в систему «iBank2» с использованием Генератора одноразовых паролей;
- Авторизация с помощью одноразового персонального пароля при совершении платежа в системе «iBank2» с использованием Генератора одноразовых паролей на сумму выше суммы, указанной Клиентом в Приложении № 2 к настоящему Договору;
- Ограничение доступа Клиента по IP-адресам, с которых разрешена работа с системой «iBank2». Сведения об IP-адресах, с которых будет разрешена работа с системой «iBank2» указывается Клиентом в Приложении № 2 к настоящему Договору;
- Услуга «SMS информирование» - рассылка SMS уведомлений Клиенту о состоянии банковских счетов через SMS (опция «SMS оповещение»), вход в систему «iBank2» с использованием одноразового SMS пароля (опция «Одноразовый пароль на вход в «iBank2»»), подтверждение платежных поручений одноразовым SMS паролем (опция «SMS подтверждение на отправку платежей в «iBank2»»).

При выборе одного или нескольких видов услуг дополнительной защиты Клиент обязан предоставить в Банк Заявление о предоставлении дополнительных услуг по обеспечению безопасности при работе в системе «iBank2» (Приложение №2 к настоящему Договору) или Заявление о подключении Услуги «SMS информирование» (Приложение № 7 к Договору). Оплата услуг Банка по предоставлению дополнительных услуг осуществляется на основании действующих Тарифов Банка.

**5.24.** Клиент имеет право произвести замену неисправных Ключевых носителей и/или Генераторов одноразовых паролей без внесения дополнительной платы в течение 12 месяцев со дня выдачи устройств. Замена устройств без внесения дополнительной платы не распространяется на устройства с видимыми повреждениями, произошедшими в результате внешних воздействий. После истечения указанного срока замена неисправных устройств осуществляется по действующим тарифам Банка.

**5.25.** Клиент обязан оплачивать стоимость услуг за пользование Системой «iBank2» в соответствии с действующими Тарифами Банка.

**5.26.** «Клиент (при отсутствии расчетного счета в Банке) обязуется оплачивать Банку комиссионное вознаграждение за пользование системой «iBank 2» в сроки и в размере, согласно действующим Тарифам Банка, путем самостоятельного перечисления денежных средств на счет требования, открытый в Банке, либо внесением наличных денежных средств на указанный счет, через кассу Банка».

**5.27.** Клиент обязан при использовании Услуги «SMS информирование» указывать/исключать номера мобильных телефонов Пользователей с их согласия.

**5.28.** Клиент обязуется самостоятельно урегулировать все споры и разногласия с Пользователями по поводу поступления им SMS сообщений в рамках Услуги «SMS информирование».

**5.29.** Клиент имеет право получать консультации Банка в рамках оказания Услуги «SMS информирование».

**5.30.** Клиент обязан ежемесячно оплачивать комиссию за предоставление Услуг(и) согласно действующим тарифам Банка.

**5.31.** С целью предотвращения неправомерного (несанкционированного) списания денежных средств Клиент имеет право установить на основании предоставленного Заявления «лимит» и/или список «доверенных получателей» с целью ограничения максимальной суммы исходящих платежных поручений и формирования перечня возможных получателей денежных средств, в адрес которых могут быть совершены переводы (Приложение № 8 к настоящему Договору). Изменение/дополнение вносится в систему «iBank2» только на основании дополнительного письменного распоряжения Клиента.

## **6. ПРАВА И ОБЯЗАННОСТИ БАНКА**

### **Права и обязанности Банка:**

**6.1.** Банк обязан обладать техническим оборудованием, необходимым для эксплуатации Системы «iBank2» в исправном состоянии и количестве, достаточном для надлежащего обслуживания Клиента, располагать кадрами, необходимыми для работы с Клиентом с использованием Системы «iBank2».

**6.2.** Банк обязан передать Клиенту по запросу необходимую документацию и предоставить рекомендации для работы с системой.

**6.3.** Банк обязан размещать на web-странице в Интернете (сайт ПАО АКБ «Приморье» по адресу <http://www.primbank.ru> и <https://client.primbank.ru>) информационные материалы, необходимые для работы Клиента с системой «iBank2», в том числе электронный документ «Руководство пользователя», «Памятка о мерах по защите информации при использовании системы «iBank2», а также инструкция по настройкам SMS сообщений».

**6.4.** Банк обязан произвести блокирование или удаление ключа проверки ЭП Клиента по письменному «Уведомлению об отмене действия Пары ключей ЭП Клиента» (Приложение № 5 к настоящему Договору).

**6.5.** Банк имеет право произвести блокировку ключа проверки ЭП руководителя Клиента в одностороннем порядке, без согласия Клиента, в случае выявления сотрудником Банка факта смены единоличного исполнительного органа (в выписке ЕГРЮЛ внесены данные по новому руководителю).

**6.6.** Банк обязан по требованию Клиента зарегистрировать новые ключи проверки ЭП Клиента на основании предоставленного Сертификата ключа проверки ЭП.

**6.7.** Банк обязан предупредить Клиента о необходимости смены Ключей ЭП не менее чем за 10 дней до даты окончания срока действующих ЭП Клиента.

**6.8.** Банк обязан по телефонному звонку Клиента после произношения Клиентом блокировочного слова, впредь до письменного уведомления, блокировать работу Клиента в системе «iBank2».

**6.9.** При наличии у Клиента расчетного (текущего) счета Банк вправе отказать Клиенту в приеме от него документа на проведение операции по банковскому счету, подписанному аналогом собственноручной подписи, в случае выявления документально подтвержденных сомнительных операций Клиента. Дальнейшее обслуживание Клиента по сделке осуществляется при представлении им документа на бумажном носителе, удостоверенного Клиентом в соответствии с карточкой с образцами подписей и оттиска печати.

**6.10.** В случае возникновения обоснованных подозрений в подлинности электронных документов или возникновения форс-мажорных обстоятельств Банк имеет право затребовать от Клиента оформления платежного документа на бумажном носителе, заверенного необходимыми подписями и печатью, и не производить платеж до оформления бумажного документа, о чем Банк обязан сообщить Клиенту не позднее дня получения электронного документа.

**6.11.** Банк вправе запросить у Клиента подтверждение платежа, вызвавшего сомнение в его подлинности, путем связи с ответственными представителями Клиента или лицами, подписавшими электронный платежный документ.

**6.12.** Клиент предоставляет Банку право без дополнительных распоряжений списывать денежные средства с расчетного и иных счетов Клиента (в том числе счетов для совершения операций с использованием пластиковых карт), в сроки и в размере стоимости предоставляемых Клиенту услуг согласно действующим Тарифам Банка.

**6.13.** Банк вправе в одностороннем порядке изменять действующие тарифы и/или вводить новые тарифы на оказываемые услуги. Извещение Клиента об изменении действующих и/или введении новых тарифов в рамках данного Договора осуществляется Банком путем размещения информации на информационных стендах в помещениях Банка и web-странице Банка в Интернете (сайт ПАО АКБ «Приморье» по адресу [www.primbank.ru](http://www.primbank.ru)), и направления Клиенту соответствующего уведомления по системе «iBank2». Измененные и/или вновь введенные тарифы на услуги Банка вводятся в действие по истечении 10 календарных дней со дня размещения соответствующей информации на web-странице Банка в Интернете (сайт ПАО АКБ «Приморье» по адресу [www.primbank.ru](http://www.primbank.ru)), либо с даты, указанной в соответствующем уведомлении Клиента.

**6.14.** В случае задержки уплаты Клиентом абонентской платы, согласно действующим тарифам Банка, более 15-ти дней Банк вправе произвести отключение Клиента от системы в одностороннем порядке. Повторное подключение Клиента к системе «iBank2» производится на следующий рабочий день после оплаты задолженности Клиентом в полном объеме.

**6.15.** В случае нарушения клиентом своих обязанностей, Банк имеет право произвести блокирование Клиента (ключа проверки ЭП Клиента) без предварительного уведомления до момента устранения нарушения.

**6.16.** Банк обязан оказывать Клиентам Услугу «SMS информирование» согласно их заявлениям на подключение, предоставленным в соответствии с настоящим Договором, Тарифами, действующим законодательством РФ и иными договорами, заключенными между Клиентом и Банком.

**6.17.** На основании предоставленного Клиентом Заявления Банк обязан произвести индивидуальные настройки в системе «iBank2» Клиента, по установлению перечня доверенных получателей и/или лимита платежных поручений (п.5.31.). Изменение/дополнение вносится в систему «iBank2» только на основании письменного распоряжения Клиента.

**6.18.** Банк обязан поддерживать рабочее состояние всех предоставляемых дополнительных Услуг по обеспечению безопасности при работе в системе «iBank2».

**6.19.** Банк обязан подключить/отключить Услугу «SMS информирование» на основании предоставленного Клиентом соответствующего письменного Заявления.

**6.20.** В случае задержки уплаты Клиентом абонентской платы за использование Услуги «SMS информирование» в Системе «iBank2», согласно действующим тарифам Банка, более 15-ти дней, Банк вправе произвести отключение Клиента от Услуги в одностороннем порядке. Повторное подключение Клиента к Услуге производится после оплаты задолженности в полном объеме.

## 7. СОВМЕСТНЫЕ ОБЯЗАТЕЛЬСТВА И ОТВЕТСТВЕННОСТЬ СТОРОН

- 7.1** Банк не несёт ответственность за ущерб, причинённый Клиенту в результате использования третьими лицами ключа ЭП Клиента.
- 7.2** Банк не несет ответственность, в том числе и перед третьей стороной в случае указания Клиентом при подключении/настройки Услуги «SMS информирование» неверного номера мобильного телефона.
- 7.3** При расторжении настоящего Договора Стороны несут ответственность по всем ранее сформированным электронным документам с электронными подписями Клиента в системе «iBank2» в соответствии с действующим законодательством РФ.
- 7.4** В случае возникновения конфликтных ситуаций между Клиентом и Банком при использовании системы «iBank2» Стороны обязуются участвовать в рассмотрении конфликтов в соответствии с «Процедурой проведения технической экспертизы при возникновении спорных ситуаций» (Раздел № 13 настоящего Договора), выполнять требования данной Процедуры и следовать выводам по рассмотрению конфликтной ситуации.
- 7.5** Стороны обязуются при разрешении экономических и иных споров, которые могут возникнуть в связи с использованием системы «iBank2», предоставлять в письменном виде свои оценки, доказательства и материалы по запросу заинтересованной Стороны, участвующей в настоящем Договоре.
- 7.6** Стороны освобождаются от ответственности за неисполнение или ненадлежащее исполнение взятых по настоящему Договору обязательств в случае возникновения обстоятельств непреодолимой силы, к которым относятся: стихийные бедствия, пожары, аварии, отключения электроэнергии, повреждение линий связи, массовые беспорядки, забастовки, военные действия, противоправные действия третьих лиц, вступление в силу законодательных актов, актов федеральных или местных органов власти и обязательных для исполнения одной из Сторон, прямо или косвенно запрещающих указанные в Договоре виды деятельности или препятствующие выполнению Сторонами своих обязательств по Договору. Сторона, пострадавшая от их влияния, обязана сообщить другой Стороне о случившемся в срок не позднее 30 дней с момента возникновения этих обстоятельств.

## 8. ПОРЯДОК ПОДКЛЮЧЕНИЯ К СИСТЕМЕ «iBANK2» И СТОИМОСТЬ РАБОТ

**8.1.** Для подключения к системе «iBank2» Клиент предоставляет в Банк Заявление об акцепте установленной формы (Приложение № 1 к настоящему Договору) в одном экземпляре и обеспечивает технические, программные и коммуникационные ресурсы, необходимые для работы с системой, в том числе:

- Компьютер с операционной системой. Работа с сервисом возможна на следующих ОС:
  - Microsoft Windows: 7 (x86/x64), 8 (x86/x64), 8.1 (x86/x64), 10 (x86/x64) и выше;
  - Apple Mac OS X: 10.7 (Lion) и выше;
  - Linux: AltLinux 7 (x86/x64), Debian 7 (x86/x64), Mint 13 (x86/x64), SUSE Linux Enterprise Desktop 12 (x64), openSUSE 13 (x86/x64), Ubuntu 12.04 (x86/x64) и более современные версии указанных дистрибутивов.
- Монитор с разрешением не менее 1280x1024;
- Web-браузер с поддержкой плагина «BIFIT Signer» для использования электронной подписи с применением аппаратных устройств. Поддержка плагина обеспечена в следующих браузерах:
  - Internet Explorer версия 11;
  - Firefox версия 44 и выше;
  - Opera версия 35 и выше;
  - Safari версия 9 и выше;
  - Chrome версия 49 и выше.
- Принтер.

**8.2.** Клиент оплачивает услуги по регистрации и подключению к системе «iBank2», получает Ключевой носитель.

**8.3.** При выборе одного или нескольких видов дополнительных услуг по обеспечению безопасности при работе в системе «iBank2» согласно п. 5.23 на основании предоставленного в Банк Приложения № 2 и/или Приложения № 7 Клиент оплачивает Банку стоимость услуг согласно действующим Тарифам Банка и получает Генератор одноразовых паролей.

**8.4.** Клиент самостоятельно выполняет установку и настройку программного обеспечения необходимого для работы в системе «iBank 2» (плагин Bifit Signer, Java – машина, драйвер USB-токена) и производит предварительную регистрацию в системе на web-странице Банка <https://client.primbank.ru/> (ссылка “Вход в систему” режим «Новый клиент»), осуществляет генерацию ключей ЭП в соответствии с полученными инструкциями и консультациями и предоставляет в Банк два заполненных экземпляра «Сертификата ключа проверки ЭП Клиента» (Приложение № 3 к настоящему Договору) на каждую пару ключей, распечатанные после генерации.

**8.5.** Банк производит окончательную регистрацию Клиента в системе «iBank2».

**8.6.** В случае выбора работы с системой «iBank 2» в режиме «PC - банкинг», Клиент самостоятельно производит загрузку и установку дистрибутива «PC - банкинг» с web-страницы Банка <https://client.primbank.ru/> в соответствии с полученными инструкциями и консультациями.

**8.7.** Началом оказания услуг считается дата начала действия первого Ключа проверки ЭП Клиента в Банке.

**8.8.** С даты начала действия первого Ключа проверки ЭП Клиента в Банке Клиент ежемесячно оплачивает обслуживание по настоящему Договору согласно действующим Тарифам Банка.

**8.9.** С даты начала действия первого Ключа проверки ЭП Клиента в Банке расчет абонентской платы за пользование системой «iBank2» производится за полный календарный месяц.

**8.10.** В случае если настоящий договор будет расторгнут по инициативе Клиента в период, за который Клиент произвел оплату услуг Банка в виде абонентской платы за очередной месяц, возврат Банком перечисленных сумм не производится.

**8.11.** Для подключения к Услуге, «SMS информирование» Клиент должен быть пользователем Системы «iBank2». Услуга «SMS информирование», доступна Клиентам по активным счетам подключенным к системе «iBank2».

**8.12.** При подключении опции «SMS оповещение» Услуги «SMS информирование» в Системе «iBank2» Клиент самостоятельно производит настройку рассылки SMS сообщений согласно Инструкции, а также выбор и детализацию Событий, о которых хочет получать сообщения (кроме опций «Одноразовый SMS пароль на вход в «iBank2» и «SMS подтверждение на отправку платежей в «iBank2»»). Одно SMS уведомление может состоять из нескольких SMS сообщений. Чем больше детализировано Событие, тем больше SMS сообщений в одном SMS уведомлении.

**8.13.** Абонентская плата за Услугу «SMS информирование» взимается ежемесячно вне зависимости от вида и количества выбранных опций, не позднее 5-го рабочего дня следующего за расчетным периодом, путем списания денежных средств с расчетного и/или иных счетов клиента на основании действующих Тарифов Банка. Комиссия формируется исходя из количества различных номеров мобильных телефонов внесенных Клиентом в систему, на которые осуществлялась рассылка хотя бы 1-го SMS уведомления.

**8.14.** Сообщения направляются Клиенту в виде SMS сообщений на мобильный номер телефона оператора связи, действующего на территории РФ.

**8.15.** Клиент может в любой момент отказаться от Услуги «SMS информирование» путем направления в Банк письменного уведомления на бумажном носителе.

**8.16.** Услуга «SMS информирование» блокируется в автоматическом режиме в случае:

- ✓ задержки уплаты Клиентом абонентской платы за использование услуги «SMS информирование»;
- ✓ расторжения договора по системе «iBank2».

**8.17.** Опция «Одноразовый SMS пароль на вход в «iBank2»» подключается к каждому сотруднику Клиента, имеющему активный ключ ЭП.

**8.18.** Банк не несет ответственности за время доставки SMS, ответственность лежит на операторе, предоставляющем услугу.

**8.19.** Услуга «SMS информирование» предоставляется круглосуточно, 7 дней в неделю.

**8.20.** При проведении Банком корректировок, дополнительных (исправительных) операций по счетам Клиента (при условии, что у пользователя подключена опция «SMS оповещение» и подключено событие «О движении по счету»), пользователю будут поступать соответствующие SMS уведомления.

**8.21.** Если система «iBank2» заблокирована по какой-либо причине, но при этом услуга «SMS информирование» активна (при условии, что у пользователя подключена опция «SMS оповещение» и подключено событие «О движении по счету»), пользователю будут поступать соответствующие SMS уведомления.

## 9. ПОРЯДОК ОБСЛУЖИВАНИЯ КЛИЕНТА

**9.1.** Банк осуществляет прием и выдачу документов, передаваемых по электронной системе «iBank2», в соответствии с утвержденным Банком времени приема-передачи электронных документов. При невозможности передачи документов в Банк с использованием электронной системы «iBank2», документы могут быть предоставлены Клиентом на бумажном носителе, оформленные надлежащим образом.

**9.2.** При получении электронного документа Банк производит проверку корректности электронных подписей Клиента, проверку правильности заполнения реквизитов документа. В случае отбраковки документ Банком не принимается, о чем информируется Клиент по системе «iBank2».

**9.3.** При недостаточности денежных средств на счете Клиента для исполнения его платежей 6 группы очередности (в соответствии со ст.855 ГК РФ) на конец текущего операционного дня в соответствии с утвержденным Банком времени приема-передачи электронных документов указанные платежные поручения подлежат возврату Клиенту без исполнения Банком.

**9.4.** При наличии у Клиента расчетного (текущего) счета выписки по счетам, дебетовые и кредитовые приложения по проведенным операциям предоставляются Клиенту в электронном виде посредством системы «iBank2» с отметками Банка об исполнении документов без последующего их предоставления на бумажных носителях, за исключением документов по кассовым операциям и иных первичных документов, получение которых по системе «iBank2» не представляется возможным (требования кредиторов, налоговых органов и т.п.).

## 10. РАЗРЕШЕНИЕ СПОРОВ

**10.1.** Споры и разногласия, возникающие в связи с настоящим Договором, разрешаются Сторонами путем переговоров, результаты которых оформляются Протоколом согласований.

**10.2.** Если Стороны не достигли соглашения путем переговоров, споры по настоящему Договору передаются на разрешение в Арбитражный суд Приморского края.

## 11. СРОКИ И УСЛОВИЯ ДЕЙСТВИЯ ДОГОВОРА

**11.1.** Настоящий Договор вступает в силу с момента подписания Сторонами Заявления об акцепте (Приложение №1 к настоящему Договору) установленной формы и заключается на неопределенный срок.

**11.2.** Договор может быть расторгнут по требованию любой из Сторон.

**11.3.** В случае расторжения Договора по инициативе Банка, последний направляет письменное уведомление Клиенту по системе «iBank2», прекращает прием и исполнение электронных документов, передаваемых от имени Клиента при помощи Системы. Договор считается расторгнутым с даты и времени, указанных в уведомлении.

**11.4.** В случае расторжения Договора по инициативе Клиента последний передает в Банк письменное уведомление о расторжении Договора составленное в произвольной форме либо по форме согласно Приложения № 6 к настоящему Договору. Договор считается расторгнутым по инициативе Клиента с момента регистрации в Банке уведомления Клиента о расторжении Договора.

**11.5.** Настоящий договор прекращает свое действие без каких-либо дополнительных уведомлений и/или извещений между Сторонами в следующих случаях:

- в случае расторжения Клиентом последнего «Договора банковского счета в валюте РФ/иностранной валюте» или иного договора, предусматривающего использование системы «iBank2»;
- в случае неоплаты или неполной оплаты услуг Банка за последние шесть месяцев.

**11.6.** При расторжении Договора Клиент обязуется уничтожить или передать в Банк все принадлежащие ему конфиденциальные документы, ключи ЭП, относящиеся к настоящему Договору, и не передавать их третьим лицам.

## 12. ДОПОЛНИТЕЛЬНЫЕ УСЛОВИЯ

**12.1.** Все возникшие вопросы при реализации настоящего Договора решаются путем переговоров с учетом взаимных интересов в соответствии с «Процедурой проведения технической экспертизы при возникновении спорных ситуаций» (Раздел № 13 настоящего Договора), а при не достижении соглашения - в судебном порядке.

**12.2.** При изменении реквизитов Стороны обязуются своевременно уведомлять об этом друг друга путем направления по системе «iBank2» соответствующего уведомления в виде информационного документа (письма), защищенного ЭП.

**12.3.** Ни одна из Сторон не может передавать свои права и обязательства по Договору третьей Стороне без письменного согласия на то другой Стороны.

**12.4.** Банк вправе в одностороннем порядке вносить изменения в настоящий Договор.

**12.5.** Для вступления в силу изменений, внесенных в договор, Банк обязан опубликовать информацию об изменениях на информационных стендах в помещениях Банка и web-странице Банка в Интернете (сайт ПАО АКБ «Приморье» по адресу [www.primbank.ru](http://www.primbank.ru)).

**12.6.** Изменения Договора вступают в силу по истечении 10 календарных дней с даты опубликования Банком информации, либо с даты вступления изменений в силу, если такая дата указана в опубликованной информации, но не ранее 10 календарных дней с даты опубликования информации.

**12.7.** Клиент обязан не реже одного раза в 10 дней знакомиться с информацией, публикуемой Банком.

**12.8.** Банк не несет ответственности, если с информацией об изменении условий Договора, опубликованной в порядке и в сроки, установленные настоящими Договором, не был ознакомлен Клиент.

### **13. ПРОЦЕДУРА ПРОВЕДЕНИЯ ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ ПРИ ВОЗНИКНОВЕНИИ СПОРНЫХ СИТУАЦИЙ**

**13.1.** В настоящем Разделе под спорной ситуацией понимается существование претензий у Клиента к Банку, справедливость которых может быть установлена только по результату проверки электронных подписей Клиента под электронным документом.

**13.2.** Клиент представляет Банку заявление, содержащее существо претензии со ссылкой на электронный документ, на основании которого Банк выполнил операции по счёту Клиента.

**13.3.** Банк обязан в течение пяти рабочих дней от даты подачи заявления Клиента сформировать разрешительную комиссию для рассмотрения заявления. В состав комиссии включаются представители Клиента, представители Банка и, при необходимости независимые эксперты. Выбор членов комиссии осуществляется по согласованию Сторон. При невозможности согласованного выбора, последний проводится случайно (по жребию).

**13.4.** Результатом рассмотрения спорной ситуации разрешительной комиссией является определение истинности электронных подписей Клиента под спорным документом.

**13.5.** Разрешительная комиссия в течение не более пяти рабочих дней проводит рассмотрение заявления. Рассмотрение заявления включает следующие этапы:

13.5.1. Разрешительная комиссия проводит техническую экспертизу электронного документа, на основании которого Банком выполнены оспариваемые Клиентом действия с его счётом.

13.5.2. Разрешительная комиссия проводит техническую экспертизу ключей проверки ЭП Клиента:

- С использованием штатного программного обеспечения Системы «iBank» АРМ «Операционист» выполняется распечатка Сертификата ключа проверки ЭП Клиента. По согласованию сторон печатная форма сертификата может быть получена с использованием ПО АРМ «Администратор».
- Распечатанный сертификат сверяется с Сертификатом ключа проверки ЭП Клиента, заверенным подписью уполномоченного лица Клиента и являющимся приложением к договору. Сверяются ID ключа и его шестнадцатеричное представление.

13.5.3. Разрешительная комиссия проводит техническую экспертизу подлинности ЭП Клиента в Электронном документе:

- С использованием штатного программного обеспечения Системы «iBank2» АРМ «Операционист» выбирается документ и выполняется операция «Проверить ЭП». При необходимости, комиссией также могут использоваться специализированные утилиты разработчика Системы «iBank2» для выгрузки документа из Базы данных Системы «iBank2» и автономной проверки.

13.5.4. На основании данных технической экспертизы разрешительная комиссия составляет акт, содержащий:

- обстоятельства, послужившие основанием возникновения разногласий;
- порядок работы членов комиссии;
- вывод о подлинности ЭП в оспариваемом Электронном документе и его обоснование.

**13.6.** Банк несет ответственность перед Клиентом в случае, когда имело место хотя бы одна из следующих ситуаций:

- Банк не предъявляет электронного документа, переданного Клиентом, на основании которого Банк выполнил операции по счёту Клиента;
- ID ключа и/или шестнадцатеричное представление распечатанного сертификата ключа проверки ЭП Клиента, который хранится в Банке, отличается от сертификата ключа проверки ЭП Клиента, заверенным подписью уполномоченного лица Клиента и являющимся приложением к договору;
- Хотя бы одна электронная подпись Клиента в электронном документе оказалась некорректной;
- Клиент предоставляет «Уведомление об отмене действия Пары ключей ЭП Клиента», подписанное должностным лицом Банка и имеющим отпечаток печати Банка. При этом указанная в Уведомлении дата блокировки действия ключа проверки ЭП Клиента раньше даты, указанной в рассматриваемом электронном документе.

**13.7.** Банк не несет ответственность перед Клиентом в случае, если:

- Банк предъявляет электронный документ с корректными электронными подписями Клиента и принадлежность ключей проверки ЭП Клиента подтверждена;

### **14. ЮРИДИЧЕСКИЙ АДРЕС И РЕКВИЗИТЫ БАНКА**

#### **БАНК ПАО АКБ "Приморье"**

Адрес 690990, Владивосток, ул. Светланская, д. 47

Телефон (423) 220-88-00, Факс (423) 222-68-75

Телекс PRIMV RU 2-213-265

БИК 040507795

Корр. Счет 30101810800000000795

в Дальневосточном ГУ Банка России

От: \_\_\_\_\_

(полное / сокращенное наименование Клиента,  
ФИО индивидуального предпринимателя, адвоката, нотариуса)**ЗАЯВЛЕНИЕ ОБ АКЦЕПТЕ**

Настоящим заявляем об акцепте в порядке, предусмотренном ст. 428 Гражданского кодекса Российской Федерации, условий Договора на обслуживание Клиента по системе «iBank2» ПАО АКБ «Приморье», являющегося Договором присоединения, принимаем на себя обязательства следовать положениям и условиям Договора на обслуживание Клиента по системе «iBank2». Банк осуществляет обслуживание счета (счетов) с использованием системы «iBank2», позволяющей осуществлять платежи, отправлять информационные сообщения и получать выписки.

Настоящее заявление об акцепте является приложением к Договору на обслуживание Клиента по системе «iBank2» заключенному Сторонами.

Ответственными представителями Сторон для контроля и решения организационно-технических вопросов по настоящему Договору являются:

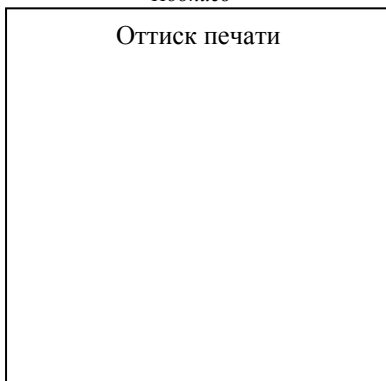
от Банка: *специалисты Отдела Электронных Платежей,*  
**8 (423) 2-433-519 – для звонков из г. Владивосток**  
**8 (423) 2-400-300 – для звонков из г. Владивосток**  
**8-800-200-20-86 – для звонков из других городов (звонок бесплатный)**

от Клиента (ФИО, контактный телефон): \_\_\_\_\_

Руководитель: \_\_\_\_\_ « \_\_\_\_ » \_\_\_\_\_ 201\_ г.

*Подпись**Ф.И.О*

Оттиск печати




---

 Заполняется Банком

С КАРТОЧКОЙ С ОБРАЗЦАМИ ПОДПИСЕЙ И ОТТИСКА ПЕЧАТИ СВЕРЕНО:

 Отметка сотрудника Банка, принявшего заявление: \_\_\_\_\_ / \_\_\_\_\_ « \_\_\_\_ » \_\_\_\_\_ 201\_ г.  
подпись Ф.И.О.

Договор на обслуживание Клиента по системе «iBank2»

№ ОФ - ИКБ- ( \_\_\_\_\_ ) \_\_\_\_\_

*Код клиента*

Дата заключения: « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

---

 Руководитель  
 подразделения Банка: \_\_\_\_\_
*подпись*  
М.П.*Ф.И.О*



**ЗАЯВЛЕНИЕ**  
**о предоставлении дополнительных услуг по обеспечению безопасности**  
**при работе в системе «iBank 2»**

Настоящим \_\_\_\_\_ (КЛИЕНТ)

в соответствии с п. 5.23 и п. 6.12 настоящего Договора просит ПАО АКБ «Приморье» предоставить дополнительные услуги по обеспечению безопасности при работе в системе «iBank2» (отметьте нужное):

Аутентификация КЛИЕНТА с помощью одноразового персонального пароля при входе в систему «iBank2» с использованием Генератора одноразовых паролей, полученного от Банка.

	Серийный номер (S/N)									
Генератор одноразовых паролей										
Генератор одноразовых паролей										
Генератор одноразовых паролей										
Генератор одноразовых паролей										

Авторизация с помощью одноразового персонального пароля при совершении платежа в системе «iBank2» с использованием Генератора одноразовых паролей, полученного от Банка.

	Серийный номер (S/N)									
Генератор одноразовых паролей										
Генератор одноразовых паролей										
Генератор одноразовых паролей										
Генератор одноразовых паролей										

Укажите сумму, свыше которой необходимо будет провести аутентификацию платежа (цифрами и прописью):

\_\_\_\_\_

Ограничение доступа КЛИЕНТА по IP-адресам, с которых разрешена работа с системой «iBank2».

Укажите IP-адрес или диапазон IP-адресов, с которых разрешена работа в системе «iBank2» \_\_\_\_\_

\_\_\_\_\_

Руководитель: \_\_\_\_\_ «\_\_» \_\_\_\_\_ 201\_ г.

*Подпись*

*Ф.И.О*

Оттиск печати

Заполняется Банком

С КАРТОЧКОЙ С ОБРАЗЦАМИ ПОДПИСЕЙ И ОТТИСКА ПЕЧАТИ СВЕРЕНО:  
Отметка сотрудника Банка, принявшего заявление: \_\_\_\_\_ / \_\_\_\_\_  
подпись / Ф.И.О.

«\_\_» \_\_\_\_\_ 201\_ г.

Руководитель  
подразделения Банка: \_\_\_\_\_  
подпись / Ф.И.О.  
М.П.

Приложение № \_\_\_ к договору № \_\_\_\_\_ от "\_\_\_" "\_\_\_" 20\_\_ г.

**СЕРТИФИКАТ КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ СОТРУДНИКА КЛИЕНТА  
В СИСТЕМЕ "iBank 2"**

1. Наименование организации \_\_\_\_\_

2. Место нахождения юр. лица \_\_\_\_\_

3. ОГРН\* \_\_\_\_\_ дата внесения в ЕГРЮЛ (ЕГРИП)\* "\_\_\_" "\_\_\_" \_\_\_\_\_ года

4. Тел. \_\_\_\_\_ 5. ИНН (КИО) \_\_\_\_\_ 6. КПП\* \_\_\_\_\_

7. Факс\* \_\_\_\_\_ 8. E-mail\* \_\_\_\_\_

9. Сведения о владельце ключа  
 Фамилия, имя, отчество \_\_\_\_\_  
 Должность \_\_\_\_\_  
 Документ, удостоверяющий личность \_\_\_\_\_  
 серия \_\_\_\_\_ номер \_\_\_\_\_ дата выдачи "\_\_\_" "\_\_\_" \_\_\_\_\_ года  
 кем выдан \_\_\_\_\_  
 код подразделения \_\_\_\_\_

10. Примечания\* \_\_\_\_\_

\* обязательно для заполнения

**Ключ проверки ЭП сотрудника клиента**

Идентификатор ключа проверки ЭП \_\_\_\_\_ Идентификатор устройства \_\_\_\_\_

Наименование криптосредств \_\_\_\_\_

Алгоритм ГОСТ Р 34.10-2012 (1.2.643.7.1.1.1) ID набора параметров алгоритма 1.2.643.2.2.35.1

Представление ключа проверки ЭП в шестнадцатеричном виде

E4 12 C8 D6 E3 E4 C3 F1 B2 B9 32 EF E5 0E 44 26  
 43 4D 43 E2 9A 83 87 69 EC 82 9A 95 16 E9 2D 29  
 0B 9B C2 7C F1 47 35 86 84 0C 77 5E F8 3B 70 1E  
 49 2F E9 C9 BC 2A 07 ED BC 82 F8 3B 52 9A BB 66

Личная подпись владельца ключа проверки ЭП

Срок действия (заполняется банком):

с "\_\_\_" "\_\_\_" 20\_\_ г.  
 по "\_\_\_" "\_\_\_" 20\_\_ г.

Сертификат ключа проверки ЭП сотрудника клиента действует в рамках договора. Владелец ключа проверки ЭП личной подписью подтверждает свое согласие на обработку банком его персональных данных.

**Достоверность приведенных данных подтверждаю**

Руководитель организации

\_\_\_\_\_/\_\_\_\_\_/\_\_\_\_\_  
 подпись / Ф.И.О.

Оттиск печати

Уполномоченный представитель банка

\_\_\_\_\_/\_\_\_\_\_/\_\_\_\_\_  
 подпись / Ф.И.О.

Оттиск печати  
Банка

Дата приема сертификата  
 ключа проверки ЭП  
 "\_\_\_" "\_\_\_" 20\_\_ г.

Администратор безопасности системы

\_\_\_\_\_/\_\_\_\_\_/\_\_\_\_\_  
 подпись / Ф.И.О.

Оттиск печати

Дата регистрации сертификата  
 ключа проверки ЭП  
 "\_\_\_" "\_\_\_" 20\_\_ г.

**Правила хранения и использования Ключевого носителя.**

1. Правила хранения и использования Ключевого носителя с первой группой подписи (далее – электронного ключа) должны исключать возможность несанкционированного доступа к нему.
2. По окончании рабочего дня, а так же вне времени сеансов связи электронный ключ должен храниться в сейфе.
3. Во время работы должен быть исключен доступ к электронному ключу неуполномоченных лиц.
4. Хранение USB-токена, содержащего электронный ключ, допускается в одном хранилище с другими документами, при этом отдельно от них и в упаковке, исключающей возможность негласного доступа к ним посторонних лиц.
5. Не допускается:
  - изготавливать несанкционированные копии с электронного ключа;
  - знакомить или передавать электронный ключ лицам, к ним не допущенным;
  - вставлять ключ в компьютер в режимах, не предусмотренных функционированием системы;
  - разбирать электронный ключ.
6. Необходимо оберегать USB-токен, содержащий электронный ключ, от механических воздействий (ударов, падения, сотрясения, вибрации и т. п.), от воздействия высоких и низких температур, агрессивных сред, высокого напряжения — все это может привести к его поломке.
7. Важно не прилагать излишних усилий при подсоединении USB-токена к порту компьютера, не допускать попадания на USB-токен (особенно на его разъем) пыли, грязи, влаги и т. п. При засорении разъема нужно принять меры для их очистки. Для очистки корпуса и разъема устройства необходимо использовать сухую безворсовую ткань. Использование растворителей и моющих средств недопустимо.
8. Не допустимо разбирать устройство! Кроме того, что при этом будет утрачена гарантия на устройство, такие действия могут привести к поломке корпуса, а также к порче или поломке элементов печатного монтажа и, как следствие — к ненадежной работе или выходу из строя самого USB-токена.
9. Разрешается подключать USB-токен только к исправному оборудованию. Параметры USB-порта должны соответствовать спецификации для USB.
10. Не рекомендуется использовать длинные переходники или USB-хабы без дополнительного питания, поскольку из-за этого на вход, предназначенный для USB-токена или считывателя смарт-карт, может подаваться несоответствующее напряжение.
11. Запрещается извлекать USB-токен из порта компьютера, **ЗА ИСКЛЮЧЕНИЕМ СЛУЧАЕВ ПОДОЗРЕНИЯ НА КОМПРОМЕТАЦИЮ КЛЮЧА**, если на нем мигает индикатор, поскольку это обозначает работу с данными, и прерывание работы может негативно сказаться как на данных, так и на работоспособности устройства.
12. Запрещается оставлять устройство подключенным к компьютеру во время включения, выключения, перезагрузки, ухода в режимы sleep или hibernate, поскольку в это время возможны перепады напряжения на USB-порте и, как следствие, выход устройства из строя.
13. Не рекомендуется оставлять устройство подключенным к компьютеру, когда он не используется.

**УВЕДОМЛЕНИЕ**  
об отмене действия Пары ключей ЭП Клиента

Настоящим \_\_\_\_\_  
\_\_\_\_\_ (КЛИЕНТ)

уведомляет ПАО АКБ «Приморье» о том, что с «\_\_\_» \_\_\_\_\_ 201\_ г. считать недействительным ключ ЭП Клиента:

ФИО Владельца ключа ЭП \_\_\_\_\_

Дата начала действия сертификата ключа проверки ЭП "\_\_\_" \_\_\_\_\_ 201\_ г.

Дата окончания действия сертификата ключа проверки ЭП "\_\_\_" \_\_\_\_\_ 201\_ г.

Соответствующий ему ключ проверки ЭП Клиента утрачивает силу для дальнейшего применения.

Руководитель: \_\_\_\_\_ «\_\_\_» \_\_\_\_\_ 201\_ г.

*Подпись*

*Ф.И.О*

Оттиск печати



---

Заполняется Банком

С КАРТОЧКОЙ С ОБРАЗЦАМИ ПОДПИСЕЙ И ОТТИСКА ПЕЧАТИ СВЕРЕНО:

Отметка сотрудника Банка, принявшего заявление: \_\_\_\_\_ / \_\_\_\_\_  
подпись Ф.И.О.

«\_\_\_» \_\_\_\_\_ 201\_ г.

**Отметки Администратора системы**

Ключ проверки ЭП Клиента заблокирован в системе «iBank2» с «\_\_\_» \_\_\_\_\_ 201\_ г.

Администратор системы \_\_\_\_\_ / \_\_\_\_\_  
подпись Ф.И.О.

Руководитель  
подразделения Банка: \_\_\_\_\_

подпись  
М.П.

Ф.И.О

**Уведомление  
о расторжении Договора на обслуживание Клиента по системе «iBank2».**

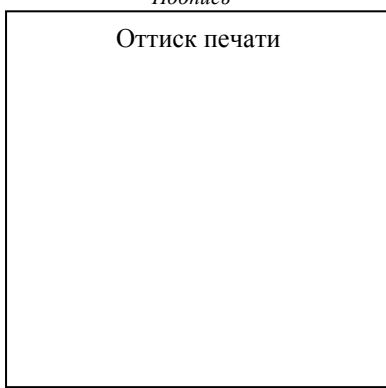
Настоящим \_\_\_\_\_ (КЛИЕНТ)  
уведомляет ПАО АКБ «Приморье» о расторжении Договора на обслуживание Клиента по системе «iBank2»  
№ ОФ - ИКБ- (\_\_\_\_\_) \_\_\_\_\_ от «\_\_» \_\_\_\_\_ 201\_ г.  
*Код клиента*

Руководитель: \_\_\_\_\_ «\_\_» \_\_\_\_\_ 201\_ г.

*Подпись*

*Ф.И.О*

Оттиск печати



Заполняется Банком

С КАРТОЧКОЙ С ОБРАЗЦАМИ ПОДПИСЕЙ И ОТТИСКА ПЕЧАТИ СВЕРЕНО:

Отметка сотрудника Банка, принявшего заявление: \_\_\_\_\_ / \_\_\_\_\_  
подпись Ф.И.О.

«\_\_» \_\_\_\_\_ 201\_ г.

**Отметки Администратора системы**

Ключ(и) проверки ЭП Клиента блокирован в системе «iBank2» «\_\_» \_\_\_\_\_ 201\_ г

Администратор системы \_\_\_\_\_ / \_\_\_\_\_  
подпись Ф.И.О.

Руководитель  
подразделения Банка:

подпись  
М.П.

Ф.И.О

**Заявление о подключении Услуги «SMS информирование» в системе «iBank2»**

Настоящим \_\_\_\_\_

(КЛИЕНТ)

просит ПАО АКБ «Приморье» подключить следующие виды опций Услуги «SMS информирование» (отметьте нужное галочкой):

«SMS оповещение»

«Одноразовый SMS пароль на вход в «iBank2»»

Указать номер мобильного телефона для получения одноразового пароля

+7																			
+7																			

+7																			
+7																			

«SMS подтверждение на отправку платежей в «iBank2»»

Указать номер мобильного телефона для получения одноразового пароля

+7																			
+7																			

+7																			
+7																			

Осуществлять подтверждение одноразовым паролем отправку по системе «iBank» документов в Банк, для платежей на сумму от:

\_\_\_\_\_ / \_\_\_\_\_ руб.

**Ознакомлены и согласны:**

- ✓ С Условиями оказания услуги «SMS информирование»
- ✓ С тарифами ПАО АКБ «Приморье» на предоставление Услуг

Руководитель: \_\_\_\_\_

Подпись

Ф.И.О

«\_\_\_» \_\_\_\_\_ 201\_\_ г.

Оттиск печати

Заполняется Банком

С КАРТОЧКОЙ С ОБРАЗЦАМИ ПОДПИСЕЙ И ОТТИСКА ПЕЧАТИ СВЕРЕНО:

Отметка сотрудника Банка, принявшего заявление: \_\_\_\_\_ / \_\_\_\_\_ «\_\_\_» \_\_\_\_\_ 201\_\_ г.  
подпись Ф.И.О.

**Договор на обслуживание Клиента по системе «iBank2»**

№ ОФ - ИКБ- \_\_\_\_\_ дата заключения «\_\_\_» \_\_\_\_\_ 20\_\_ г.  
Код клиента

Руководитель

подразделения Банка: \_\_\_\_\_

подпись

Ф.И.О

М.П.

**Заявление на установление лимита и/или ограничение списка получателей для исходящих платежных поручений Клиента в системе «iBank2»**

Настоящим \_\_\_\_\_ (КЛИЕНТ)  
просит ПАО АКБ «Приморье» установить индивидуальные настройки в системе «iBank2» (отметьте нужное галочкой):

**Установить лимит\* на исходящие платежные поручения** (нужное подчеркнуть):

Лимит на разовый платеж \_\_\_\_\_ руб./ \_\_\_\_\_ /

Лимит на день \_\_\_\_\_ руб./ \_\_\_\_\_ /

Лимит на месяц \_\_\_\_\_ руб./ \_\_\_\_\_ /

\*Лимит – максимальное ограничение суммы поручения(ий) за определенный период времени

**Установить список доверенных\* получателей:**

\*перечень получателей, в адрес которых могут совершаться переводы денежных средств

№ пп	Наименование получателя (контрагента)	БИК Банка получателя	Счет получателя
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
...			

**С Условиями оказания услуги Ознакомлены**

« \_\_\_\_ » \_\_\_\_\_ 201\_\_ г.

Руководитель:

\_\_\_\_\_  
Подпись  
\_\_\_\_\_  
Ф.И.О.  
  
М.П.

Заполняется Банком

**С КАРТОЧКОЙ С ОБРАЗЦАМИ ПОДПИСЕЙ И ОТТИСКА ПЕЧАТИ СВЕРЕНО:**

(подчеркнуть в случае поступления документа на бумажном носителе)

Отметка сотрудника Банка, принявшего заявление: \_\_\_\_\_ / \_\_\_\_\_ « \_\_\_\_ » \_\_\_\_\_ 201\_\_ г.  
подпись Ф.И.О.

**Договор на обслуживание Клиента по системе «iBank2»**

№ **ОФ-ИКБ** - \_\_\_\_\_ - \_\_\_\_\_ дата заключения « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.  
Код клиента № пп

Руководитель

подразделения Банка:

\_\_\_\_\_ / \_\_\_\_\_  
подпись Ф.И.О.

М.П.