АКЦИОНЕРНЫЙ КОММЕРЧЕСКИЙ БАНК «ПРИМОРЬЕ»

УТВЕРЖДЕНО
Правлением ПАО АКБ «Приморье»
«24» марта 2026г., Протокол № 17
Председатель Правления
_____ А.Н.Зверев

Действует с «01» апреля 2026г.

Договор на подключение и обслуживание Клиента по системе «iBank» (Публичная оферта)

Акционерный коммерческий банк «Приморье» (публичное акционерное общество) (далее – Банк), с одной стороны, и Клиент, изъявивший в письменной форме свое согласие на присоединение к настоящему «Договору на обслуживание Клиента по системе «iBank», с другой стороны, заключили «Договор Публичной оферты» (далее Договор) о нижеследующем.

1. Общие положения

1.1. Настоящий Договор на обслуживание Клиента по системе «iBank», является Договором присоединения, регулирующим отношения по обслуживанию Клиента по системе «iBank» юридического лица или индивидуального предпринимателя в Банке.

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) 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. Банк подключает Клиента к системе «iBank» на основании комплекта документов: «Заявления об акцепте» (Приложение № 1) и Сертификата ключа проверки электронной подписи (Приложение 2, 2А).

1.5. Банк осуществляет обслуживание Клиента с использованием системы «iBank», позволяющей передавать / принимать электронные документы – информационные (почтовые) сообщения, в том числе с вложением до 5Мб.

2. Термины и определения

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

2.2. **«Вход по логину и паролю»** – способ доступа сотрудника Клиента в систему «iBank», предоставленный руководителем Клиента и подтверждённый сотрудником Клиента, с использованием логина (адрес электронной почты) и пароля. Данный способ доступа не позволяет подписывать и отправлять в Банк документы без использования ЭП (включая Облачную ЭП).

2.3. **«Доверенность» на хранение ключа Облачной ЭП»** – документ на бумажном носителе с представленным в шестнадцатеричном виде ключа проверки ЭП Клиента, с подписями уполномоченных лиц Клиента, которые скреплены печатью Клиента (при наличии) и соответствуют заявленным в карточке образцов подписей и оттиска печати, на основании которого, Клиент доверяет Банку хранить ключ ЭП в защищенном хранилище на удаленном сервере подписи Банка (*в облаке*). Доверенность является неотъемлемой частью Сертификата ключа проверки Облачной ЭП Клиента.

2.4. **«Интернет – Банк»** – сервис, работающий через браузер, поддерживающий технологию Web. Доступ в систему осуществляется в реальном режиме времени при постоянном подключении к сети Интернет.

2.5. **«Ключ ЭП Клиента» / «Ключ Облачной ЭП Клиента» (Ключи ЭП)** – уникальная последовательность символов, самостоятельно генерируемая Клиентом с использованием средств системы «iBank», и предназначенная для формирования Клиентом электронной подписи под электронными документами.
2.6. **«Ключ проверки ЭП Клиента»** – уникальная последовательность символов, однозначно связанная с ключом ЭП Клиента, самостоятельно генерируемого Клиентом с использованием средств системы «iBank», и предназначенная для проверки Банком корректности электронной подписи электронного документа, сформированного Клиентом.
2.7. **«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.

Виды и сроки используемых ключевых носителей определяется законодательством РФ, действующим Российским криптографическим алгоритмом ГОСТ и другими нормативными документами.
2.8. **«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 (Раздел 11 настоящего Договора);
- случаи, 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).

2.9. «**Корректная ЭП Клиента**» – электронная подпись электронного документа Клиента, дающая положительный результат ее проверки с использованием ключа проверки ЭП Клиента.
2.10. **«Облачная электронная подпись» (ОЭП)** – аналог электронной подписи, без физического носителя, хранимый на удаленном сервере Банка.
2.11. **«Облачное хранилище Банка»** – защищенное хранилище Банка, является средством хранения усиленной неквалифицированной ЭП, предназначенное для генерации пары ключей ЭП, хранения сгенерированных ключей ЭП (является носителем, содержащим ЭП), формирования ЭП под документами в соответствии с утвержденными стандартами (ГОСТ Р34.10-2012, ГОСТ Р34.11-2012) с использованием встроенного в программное обеспечение сертифицированного средства криптографической защиты информации (далее – СКЗИ), поддерживающего алгоритмы шифрования, утвержденные ФСБ России в стандарте ГОСТ Р 34.12-2015. Применяется в целях дополнительного повышения безопасности электронного документооборота между Клиентом и Банком и полного исключения возможности несанкционированного копирования ключей ЭП.
2.12. **«Основные услуги»** - пакет основных видов услуг, предоставляемых Клиенту по системе «iBank», при подключении к системе.
2.13. **«Пара ключей ЭП Клиента»** – ключ ЭП Клиента и соответствующий ему ключ проверки ЭП Клиента.
2.14. **«Пароль к ключу ЭП»** - секретная последовательность символов, известная исключительно Клиенту – владельцу ключа ЭП, и используемая для доступа Клиента к ключу ЭП.
2.15. **«Система «iBank»** - совокупность программно-аппаратных средств, устанавливаемых на территории Клиента и Банка с целью предоставления Клиенту услуг по настоящему Договору.
Доступ в систему **«iBank»** осуществляется в зависимости от выбранного Клиентом сервиса:

- **«Интернет – Банк»**, доступ осуществляется с использованием Ключевого носителя.
- **«Интернет – МicroБанк»**, доступы предоставляется по «Логину/Паролю», дополнительному Коду подтверждения SMS и с использованием Ключа ОЭП.

2.16. «**Сертификат ключа проверки ЭП Клиента»** (Приложение № 2)/ **«Сертификат ключа проверки облачной ЭП Клиента»** (Приложение № 2А) – документ на бумажном носителе с представленным в шестнадцатеричном виде ключа проверки ЭП Клиента, с подписями уполномоченных лиц Клиента, которые скреплены печатью Клиента (при наличии) и соответствуют заявленным в карточке образцов подписей и оттиска печати.
2.17. «**Средства криптографической защиты информации (СКЗИ)»** – программные модули, в том числе средства электронной подписи, осуществляющие криптографическое преобразование информации на всех этапах взаимодействия Банка и Клиента при использовании системы «iBank» и обеспечивающие защиту информации в соответствии с утвержденными стандартами (ГОСТ) и сертифицированные в соответствии с действующим законодательством.
2.18. **«Удостоверяющий центр (УЦ)»** – юридическое лицо или индивидуальный предприниматель, осуществляющий функции по созданию и выдаче сертификатов ключей проверки ЭП.

2.19. «**Усиленная неквалифицированная электронная подпись (УНЭП)** – электронная подпись, которая:

- получена в результате криптографического преобразования информации с использованием ключа ЭП;
- позволяет определить лицо, подписавшее электронный документ;
- позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
- создается с использованием средств электронной подписи.

2.20. «**Электронный документ**» **(ЭД)** – документированная информация, представленная в электронной форме, в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

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

3. Соглашение сторон

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

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

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

3.4. Стороны признают, что электронные документы, создаваемые с использованием Сервисов «iBank», 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.

3.5. Стороны признают, что электронные документы с электронными подписями Клиента, созданные системой «iBank» и полученные сервером Банка, являются материалом для решения спорных вопросов.

3.6. Стороны согласны с тем, что наличие у Банка надлежаще оформленного электронного документа, подписанного ЭП/ОЭП Клиента, проверка подлинности которой ключом проверки ЭП/ОЭП Клиента дала положительный результат, является основанием для исполнения Банком соответствующего распоряжения на основании указанного Электронного документа.

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

3.8. Стороны признают, что ключ проверки ЭП/ОЭП Клиента, указанный в заверенном подписью руководителя и оттиском печати Клиента Сертификате ключа проверки ЭП/ОЭП Клиента, принадлежит Клиенту и используется для проверки подлинности ЭП/ОЭП Клиента.

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

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

3.11. Стороны признают, что доступ к сервисам системы «iBank» предоставляется только уполномоченным лицам, ранее идентифицированными в Банке.

3.12. Стороны признают, что «Доверенность на хранение ключа Облачной ЭП» (далее Доверенность) (Приложение №3) предоставленная Клиентом на бумажном носителе, с представленным в шестнадцатеричном виде ключа проверки ОЭП Клиента, заверенная подписью руководителя и имеющая оттиск печати Клиента, на основании которого, Клиент доверяет Банку хранить ключ ОЭП в облачном хранилище Банка, является неотъемлемой частью настоящего Договора и Сертификата ключа проверки Облачной ЭП Клиента.

3.13. Стороны признают, что используемые в системе «iBank» средства защиты, являются достаточными для защиты информации при ее передаче по каналам связи от несанкционированного доступа третьих лиц.

3.14. Стороны признают, что в случае расторжения/прекращения настоящего Договора прекращается обслуживание в любом из подключенных сервисов Клиента.

3.15. В отношении «Входа по логину и паролю» Стороны признают следующее:

- Клиентом, по своему усмотрению может быть предоставлен доступ сотруднику Клиента к системе «iBank» посредством входа по логину и паролю в соответствии с предоставленными Банком инструкциями.
- Вход по логину и паролю может быть предоставлен в систему «iBank» (инициирован) только руководителем Клиента и только сотруднику Клиента.

- Вход по логину и паролю не позволяет подписывать и отправлять в Банк документы без использования ЭП (включая Облачную ЭП).

3.16. Стороны признают, что предварительная регистрация Клиента в системе «iBank» с выпуском ОЭП осуществляется в соответствии с предоставленными Банком инструкциями с учётом следующего:

- Выпуск ОЭП в рамках предварительной регистрации Клиента в системе «iBank» возможен только для руководителя Клиента.
- При предварительной регистрации в системе «iBank» Клиентом могут быть использованы только те учетные данные (адрес электронной почты и номер телефона), которые принадлежат непосредственно Клиенту.

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

3.18. Стороны признают, что выпуск ОЭП может быть осуществлен пользователем (руководителем или сотрудником Клиента) только для самого себя в соответствии с предоставленными Банком инструкциями. Выпуск ОЭП для третьего лица невозможен.

3.19. Клиент подтверждает, что, предоставляя сотруднику Клиента возможность входа по логину и паролю, Клиент тем самым изъявляют свою волю на доступ такого лица в систему «iBank» Клиента без возможности подписания и отправки в Банк документов.

3.20. Клиент подтверждает, что, выпуская ОЭП в соответствии с предоставленными Банком инструкциями, Клиент и Владелец ключа ОЭП тем самым изъявляют свою волю использования соответствующей ОЭП для подписания документов в системе «iBank» и отправки их в Банк.

3.21. Клиент согласен с тем, что ЭП, формируемая в системе «iBank» при помощи ключа ОЭП, удовлетворяет всем признакам усиленной неквалифицированной электронной подписи согласно требованиям п. 3 статьи 5 63-ФЗ.

3.22. Клиент согласен на хранение и использование ключа ОЭП на технических средствах банка.

3.23. Стороны признают в качестве единой шкалы времени при работе с системой «iBank, Владивостокское поясное время. Контрольным является время системных часов аппаратных средств Банка.

3.24. Стороны обязуются, не передавать свои права и обязательства по Договору третьей Стороне без письменного согласия на то другой Стороны.

4. Права и обязанности Клиента

4.1. Клиент имеет право выбрать один или несколько сервисов системы «iBank».

4.2. Для подключения к сервисам системы «iBank», Клиент обязан следовать п.п. 7.1 – 7.5 настоящего Договора.

4.3. Клиент обязан назначить из числа своих сотрудников ответственного представителя по взаимодействию с Банком в вопросах обслуживания Клиента с использованием сервисов «iBank».

4.4. В зависимости от вида подключаемого сервиса «iBank», Клиент обязан использовать Ключевые носители, передаваемые Банком Клиенту по Акту (Приложение № 4 к Договору), в качестве устройств для хранения секретного ключа ЭП. Ключевые носители, 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.

4.5. Клиент обязан контролировать доставку электронных документов в Банк и их обработку на основе передаваемого Банком результата приема ЭД. ЭД считается принятым и обработанным системой «iBank» только в том случае, если Клиент получил соответствующий положительный результат в соответствии с п. 8.5 настоящего Договора.

4.6. Клиент обязан обеспечить сохранность в тайне от посторонних лиц информацию о ключах ЭП/ОЭП лиц, уполномоченных подписывать электронные документы, в том числе логин/пароль на вход в систему. Используемые ключевые носители ключа ЭП должны храниться у лиц, для генерации подписи ЭП которых они используются.

4.7. Клиент обязан не передавать третьим лицам программное обеспечение, документацию системы «iBank», сведения по форматам ЭД и технологии их обработки Клиентом и Банком, относящиеся к настоящему Договору.

4.8. Клиент обязан содержать компьютеры, с которых осуществляется работа с системой «iBank», 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.

4.9. На любом компьютере/ноутбуке/мобильном телефоне, с которого производится работа с сервисами «iBank», 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.

4.10. Клиент обязан сообщать Банку об обнаружении попытки несанкционированного доступа к любому из сервисов «iBank» незамедлительно, с момента обнаружения.
4.11. Клиент обязан незамедлительно извещать Банк обо всех случаях компрометации ключей ЭП/ОЭП, а также при утере и выходе из строя ключевого носителя.
4.12. Клиент обязан производить генерацию новой пары ключей ЭП/ОЭП должностных лиц, не реже 1 раза в 15 месяцев.
4.13. 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/ОЭП и зарегистрировать новый ключ проверки ЭП/ОЭП в Банке.
4.14. Клиент обязан в случае прекращения использования сервисов «iBank» уничтожить (удалить) ключ/ключи ЭП Клиента, в том числе ОЭП.
4.15. Клиент обязан при осуществлении предварительной регистрации в системе «iBank» с выпуском ОЭП, выпускать ОЭП только для руководителя Клиента и использовать только личные учетные данные (адрес электронной почты и номер телефона).
4.16. Клиент обязан хранить в секрете и не передавать третьим лицам логин, пароль и носитель с ключом ЭП Клиента, используемые в системе.
4.17. Клиент обязан по требованию Банка сгенерировать новые пары ключей ЭП/ОЭП Клиента и зарегистрировать новый ключ проверки ЭП/ОЭП Клиента в Банке.
4.18. Клиент имеет право досрочно прекратить действие своего активного ключа ЭП/ОЭП Клиента и соответствующего ему ключа проверки ЭП/ОЭП Клиента, предоставив в Банк письменное уведомление об отмене действия пары ключей ЭП Клиента и потребовать от Банка блокировать этот активный ключ проверки ЭП/ОЭП Клиента.
4.19. Клиент имеет право по своему усмотрению генерировать новые пары ключей ЭП/ОЭП Клиента и регистрировать в Банке новые/дополнительные ключи проверки ЭП/ОЭП Клиента.
4.20. Клиент имеет право, позвонив в службу технической поддержки систем дистанционного банковского обслуживания Банка и произнеся блокировочное слово, впредь до письменного уведомления, блокировать свою работу в сервисах «iBank».
4.21. Клиент имеет право воспользоваться **«основными видами услуг»** предоставляемые Банком по системе «iBank» согласно перечню определенному п.5.4.
4.22. При выборе сервиса «Интернет – МicroБанк», после предоставления пакета документов на подключение и активации со стороны Банка, Клиент обязан произвести на своей стороне подтверждение регистрации учетной записи и заключительные настройки сервиса, согласно рекомендациям, размещенным на сайте Банка https://client.primbank.ru.
4.23. Клиент имеет право отказаться от использования ранее подключенного сервиса «iBank» в одностороннем порядке, предоставив в Банк письменное уведомление.
4.24. Клиент имеет право отозвать ранее переданный в Банк ЭД, имеющий корректную подпись ЭП, путем направления в Банк по системе «iBank» соответствующего уведомления, при условии, что Банк к моменту получения уведомления не произвел исполнение данного ЭД.
4.25. Клиент имеет право произвести замену неисправных Ключевых носителей 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.
4.26. Клиент обязан оплачивать стоимость услуг за пользование системой «iBank» в соответствии с действующими Тарифами Банка.
4.27. Клиент (при отсутствии расчетного счета в Банке) обязуется оплачивать Банку комиссионное вознаграждение за пользование системой «iBank» 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».
4.28. Клиент обязан выполнять требования по защите информации при использовании системы «iBank», согласно рекомендациям, размещенным на сайте Банка https://client.primbank.ru.
4.29. Клиент обязан не реже одного раза в 10 дней знакомиться с информацией об изменении условий Договора, публикуемой Банком на официальном сайте https://client.primbank.ru.

5. Права и обязанности Банка

5.1. Банк обязан обладать техническим оборудованием, необходимым для эксплуатации системы «iBank» в исправном состоянии и количестве, достаточном для надлежащего обслуживания Клиента, располагать кадрами, необходимыми для работы с Клиентом с использованием системы «iBank».
5.2. Банк обязан передать Клиенту по запросу необходимую документацию и предоставить рекомендации для работы с системой.

5.3. Банк обязан размещать на web-странице в Интернете (сайт ПАО АКБ «Приморье» по адресу: https://client.primbank.ru) информационные материалы, необходимые для работы Клиента с системой «iBank», в том числе электронный документ «Руководство пользователя», «Требования по защите информации при использовании системы Интернет Клиент-Банк «iBank».
5.4. Банк обязан произвести подключение **«основных видов услуг»** предоставляемых по системе «iBank»:

- **«Письма» (**«Почтовое сообщение»)
- **«Отзыв»**

5.5. Банк имеет право блокировать в системе «iBank» существующие активные ЭП Клиента (токен) в случае изменения действующего законодательства РФ, регулирующего использование ЭП.
5.6. Банк обязан произвести блокирование или удаление ключа проверки ЭП/ОЭП Клиента по заявлению Клиента.
5.7. Банк имеет право произвести блокировку ключа проверки ЭП/ОЭП 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).
5.8. Банк обязан по требованию Клиента зарегистрировать новые ключи проверки ЭП/ОЭП Клиента на основании предоставленного Сертификата ключа проверки ЭП/ОЭП.
5.9. Банк обязан предупредить Клиента о необходимости смены Ключей ЭП/ОЭП не менее чем за 10 дней до даты окончания срока действующих ЭП/ОЭП Клиента.
5.10. Банк обязан по телефонному звонку Клиента после произношения Клиентом блокировочного слова, впредь до письменного уведомления, блокировать работу Клиента в системе «iBank».
5.11. Банк обязан по требованию Клиента произвести изменение/удаление Учетной записи в сервисе «Интернет - МicroБанк» Клиента, на основании предоставленного Клиентом письменного уведомления.
5.12. Банк имеет право отказать в подключении сервиса «Интернет - МicroБанк», в случае расхождения данных Клиента/Пользователя в системе «iBank», указанных Клиентом на сайте Банка при регистрации УЗ.
5.13. Банк имеет право отказать в подключении ключа проверки ОЭП, в случае расхождения идентификационных данных Пользователя с ранее предоставленными и подключенными данными в системе «iBank».
5.14. В случае задержки уплаты Клиентом абонентской платы, за пользование системой «iBank», предусмотренными Тарифами Банка, Банк вправе произвести отключение Клиента от системы в одностороннем порядке. Повторное подключение Клиента к системе «iBank» производится на следующий рабочий день после оплаты задолженности Клиентом в полном объеме.
5.15. Банк вправе в одностороннем порядке вносить изменения в настоящий Договор.
5.16. Банк не несет ответственности, если с информацией об изменении условий Договора, опубликованной в порядке и в сроки, установленные настоящим Договором (п.4.29), не был ознакомлен Клиент.

6. Совместные обязательства и ответственность сторон

6.1. Банк не несёт ответственность за ущерб, причинённый Клиенту в результате использования третьими лицами ключа секретного ключа ОЭП Клиента, полученного или от самого Клиента, или по его вине, а также в случае доступа третьих лиц к логину/паролю к ключу ОЭП Клиента.
6.2. При прекращении действия настоящего Договора Стороны несут ответственность по всем ранее сформированным ЭД с электронными подписями Клиента в системе «iBank» в соответствии с действующим законодательством РФ.
6.3. Стороны освобождаются от ответственности за неисполнение или ненадлежащее исполнение взятых в соответствии с настоящим Договором 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 в соответствии с настоящим Договором. Сторона, пострадавшая от их влияния, обязана сообщить другой Стороне о случившемся в срок не позднее 30 дней с момента возникновения этих обстоятельств.

7. Порядок подключения к системе «iBank»

Для подключения к системе «iBank» Клиент:

7.1. Оплачивает услуги по подключению к системе «iBank» согласно действующим тарифам, при необходимости и в зависимости от выбранного подключаемого сервиса получает Ключевой носитель.
7.2. Обеспечивает технические, программные и коммуникационные ресурсы, необходимые для работы с системой, в том числе:

- Компьютер с операционной системой. Работа с системой возможна на следующих ОС:
  — Microsoft Windows: 7 (x86/x64), 8 (x86/x64), 8.1 (x86/x64), 10 (x86/x64) и выше;

— Apple Mac OC X: 10.10 (Yosemite) 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:
  — Firefox версия 44 и выше;
  — Opera версия 35 и выше;
  — Safari версия 9 и выше;
  — Chrome версия 49 и выше.
- Принтер (по необходимости).

7.3. Самостоятельно выполняет установку и настройку программного обеспечения, необходимого для работы в системе «iBank» (плагин Bifit Signer) и производит предварительную регистрацию в системе на web-странице Банка: https://client.primbank.ru/ («Вход в Интернет-банкинг» раздел «Регистрация – Подключение к системе новых клиентов»).
7.4. Осуществляет генерацию ключей ЭП/ОЭП (в зависимости от подключаемого сервиса) в соответствии с полученными инструкциями и консультациями.
7.5. Предоставляет в Банк:
- для сервиса «Интернет – Банк», «Заявления об акцепте» (Приложение № 1) и Сертификата ключа проверки ЭП (Приложение № 2), распечатанный после генерации.
- для сервиса «Интернет – МicroБанк», «Заявления об акцепте» (Приложение № 1), Сертификата ключа проверки ОЭП (Приложение № 2А) и «Доверенность на хранение ключа ОЭП» (Приложение № 3) на каждый ключ ЭП, распечатанные после генерации.
7.6. Окончательная регистрация Клиента в системе «iBank» производится Банком после выполнения Клиентом пп.7.1.-7.5.
7.7. После регистрации сервиса «Интернет – МicroБанк» на стороне Банка, Клиент самостоятельно производит подтверждение своей учетной записи и заключительные настройки сервиса, согласно инструкции размещенной на сайте Банка https://client.primbank.ru/.
7.8. Началом оказания услуг считается дата начала действия первого ключа проверки ЭП/ОЭП Клиента в Банке.

8. Порядок обслуживания Клиента

8.1. Банк осуществляет прием и выдачу ЭД, передаваемых по электронной системе «iBank», в соответствии с утвержденным Банком временем приема-передачи ЭД. При невозможности передачи документов в Банк с использованием системы «iBank», документы могут быть предоставлены Клиентом на бумажном носителе, оформленные надлежащим образом.
8.2. ЭД Клиента, подписанные необходимым количеством ЭП Клиента, в том числе ОЭП, считаются доставленными в Банк и им присваивается статус «Доставлен». Доставленные по системе «iBank» ЭД проходят дальнейшую проверку в Банке. По результатам этой проверки Клиенту выдается окончательное решение о принятии в обработку или об отбраковке документа.
8.3. При получении ЭД, Банк производит проверку корректности ЭП/ОЭП Клиента, проверку правильности заполнения документа. В случае отбраковки, ЭД Банком не принимается и ему присваивается статус «Отвергнут» с указанием причины.
8.4. ЭД, полностью прошедшим автоматическую проверку в Банке, присваивается статус «На исполнении». Окончательное решение о приеме ЭД к исполнению принимает уполномоченный сотрудник Банка.
8.5. ЭД, исполненные Банком, принимают статус «Исполнен».
8.6. ЭД, поступивший в Банк и имеющий статус «Доставлен», «На обработке», «На исполнении», может быть отозван Клиентом путем формирования специального электронного документа «Отзыв». ЭД «Отзыв» должен быть подписан ЭП/ОЭП Клиента. В случае успешного «Отзыва» отозванному документу присваивается статус «Отвергнут».

9. Разрешение споров

9.1. Споры и разногласия, возникающие в связи с настоящим Договором, разрешаются Сторонами путем переговоров, результаты которых оформляются Протоколом согласований.
9.2. Если Стороны не достигли соглашения путем переговоров, споры по настоящему Договору передаются на разрешение в Арбитражный суд Приморского края.

10. Сроки действия настоящих Условий

10.1. Настоящие Условия вступают в силу с момента окончательной регистрации Клиента в любом из сервисов «iBank» (п. 7.6.) и действуют неопределенный срок.
10.2. Обязательства и права Сторон по настоящему Договору, относящимся к обслуживанию Клиента в системе «iBank», вступают в силу после подписания Сторонами «Заявления об акцепте» (Приложение № 1).

10.3. Действие Договора могут быть прекращены по требованию любой из Сторон.
10.4. В случае прекращения оказания услуги по обслуживанию в системе «iBank» по инициативе Банка последний направляет письменное уведомление Клиенту по системе «iBank», прекращает прием и исполнение ЭД, передаваемых от имени Клиента при помощи системы «iBank». Данная услуга не предоставляется с даты и времени, указанных в уведомлении.
10.5. В случае прекращения получения услуги по обслуживанию в системе «iBank» одного из сервисов или самой системы по инициативе Клиента, последний передает в Банк письменное уведомление об отказе от данной услуги. Данная услуга не предоставляется по инициативе Клиента с момента регистрации в Банке уведомления Клиента об отказе от услуги.
10.6. Настоящие Условия прекращают свое действие без каких-либо дополнительных уведомлений и/или извещений между Сторонами в следующих случаях:

- в случае выявления факта внесения записи в единый государственный реестр юридических лиц о прекращении деятельности Клиента без образования правопреемника;
- в случае неоплаты или неполной оплаты услуг Банка за последние шесть месяцев.
- в случае отсутствия активности Клиента в системе более 2-х лет и при отсутствии активных ключей ЭП (*активность определяется датой последнего входа в систему*).

11. Правила хранения и использования Ключевого носителя

11.1. Правила хранения и использования Ключевого носителя (далее – электронного ключа) должны исключать возможность несанкционированного доступа к нему.
11.2. По окончании рабочего дня, а также вне времени сеансов связи электронный ключ должен храниться в сейфе.
11.3. Во время работы должен быть исключен доступ к электронному ключу неуполномоченных лиц.
11.4. 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.
11.5. 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.

11.6. 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.
11.7. 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.
11.8. Недопустимо 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.
11.9. Разрешается подключать USB-токен только к исправному оборудованию. Параметры USB-порта должны соответствовать спецификации для USB.
11.10. Не рекомендуется использовать длинные переходники или USB-хабы без дополнительного питания, поскольку из-за этого на вход, предназначенный для USB-токена, может подаваться несоответствующее напряжение.
11.11. Запрещается извлекать USB-токен из порта компьютера, за исключением случаев подозрения на компрометацию, 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.
11.12. 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.
11.13. Не рекомендуется оставлять устройство подключенным к компьютеру, когда он не используется.

Приложение № 1
к Договору на обслуживание
Клиента по системе «iBank»

Заявление на подключение Системы «iBank»

Настоящим заявляем об акцепте в порядке, предусмотренном ст. 428 Гражданского кодекса Российской Федерации, условий Договора на обслуживание Клиента по системе «iBank» ПАО АКБ «Приморье», принимаем на себя обязательства следовать положениям и условиям Договора.

Банк осуществляет подключение и обслуживание Клиента с использованием системы «iBank», позволяющие производить обмен электронными документами - информационными сообщениями.

От:

_____

(полное/сокращенное наименование Клиента, ФИО индивидуального предпринимателя, адвоката, нотариуса)

ИНН Клиента:_____

Прошу подключить систему «iBank» к сервису:

☐ **«Интернет – Банк»**, *доступ осуществляется с использованием Ключевого носителя.*

☐ **«Интернет – MicroБанк»**, *доступы предоставляется по «Логину/Паролю», дополнительному Коду подтверждения SMS и с использованием Ключа Облачной ЭП.*

С «Условиями подключения и обслуживания Клиента по системе «iBank»» установленными Банком, ознакомлен и согласен:

Руководитель:

_____ _____ «____» __.__.____ 20__ г.
Подпись *Ф.И.О*

М.П.

Заполняется Банком

Отметка сотрудника Банка, принявшего заявление: _____/_____ «__»_____ 20__г.
подпись Ф.И.О.

Договор о комплексном банковском обслуживании корпоративных клиентов
№ ОФ-ИКБ- _____ Дата заключения: «_____» _____ 20___ г.

Руководитель подразделения Банка: _____ _____
подпись Ф.И.О
М.П.

Приложение № 2
к Договору на обслуживание
Клиента по системе «iBank»

Приложение № __ к договору № _____ от "____"_____20___ г.

СЕРТИФИКАТ КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ СОТРУДНИКА КЛИЕНТА
В СИСТЕМЕ "iBank"
ПАО АКБ "Приморье"

1. Наименование организации _____
_____
2. Место нахождения юр. лица _____
_____
3. ОГРН* _____ дата внесения в ЕГРЮЛ (ЕГРИП)* "____" _____ года
4. ИНН (КИО) _____ 5. КПП* _____
6. Тел. _____ 7. Факс* _____ 8. E-mail* _____
9. Сведения о владельце ключа
Фамилия, имя, отчество _____
Документ, удостоверяющий личность Паспорт гражданина РФ
_____
серия _____ номер _____ дата выдачи"____" _____ _____ года
кем выдан _____
код подразделения _____
10. Примечания* _____

* необязательно для заполнения

Ключ проверки ЭП сотрудника клиента

Идентификатор ключа проверки ЭП _____ Идентификатор устройства _____
Наименование криптосредств _____
Алгоритм ГОСТ Р 34.10-2012 256 бит (1.2.643.7.1.1.1.1) ID набора параметров алгоритма 1.2.643.2.2.35.1

Представление ключа проверки ЭП в шестнадцатеричном виде

```
D2 6E 76 DD 36 E5 DA AB 53 E7 50 5F 54 F9
E9 33 9E 83 FC 92 12 70 4F 85 5A 71 C8 A5
5B 8D 0A 8A B6 B0 6C 4A 23 77 D5 AF B9 4D
1D 9D 2E 1C D0 77 28 5A 80 53 42 D4 70 F8
```

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.

Приложение № 2А
к Договору на обслуживание
Клиента по системе «iBank»

Приложение № __ к договору № _____ от "____"_____20___ г.

СЕРТИФИКАТ КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ СОТРУДНИКА КЛИЕНТА
В СИСТЕМЕ "iBank"
ПАО АКБ "Приморье"

1. Наименование организации _____
_____
2. Место нахождения юр. лица _____
_____
3. ОГРН* _____ дата внесения в ЕГРЮЛ (ЕГРИП)* "____" _____ года
4. ИНН (КИО) _____ 5. КПП* _____
6. Тел. _____ 7. Факс* _____ 8. E-mail* _____
9. Сведения о владельце ключа
Фамилия, имя, отчество _____
E-mail владельца ключа _____ Тел. владельца ключа _____
Документ, удостоверяющий личность Паспорт гражданина РФ
_____
серия _____ номер _____ дата выдачи"____" _____ ____ года
кем выдан _____
код подразделения _____
10. Примечания* _____
* необязательно для заполнения

Ключ проверки ЭП сотрудника клиента

Идентификатор ключа проверки ЭП _____
Наименование криптосредств _____
Алгоритм ГОСТ Р 34.10-2012 256 бит (1.2.643.7.1.1.1.1) ID набора параметров алгоритма 1.2.643.2.2.35.1

Представление ключа проверки ЭП в шестнадцатеричном виде

```
38 1A 44 82 DF 94 DC CC 19 FF 68 6B 92 4E
B1 D7 8A 2E 35 56 02 C3 78 DD 2D B8 79 37
84 08 1D 23 6C B4 42 C0 37 2D 28 97 8A BE
39 A3 0D 0E E4 42 B0 99 E4 A0 B7 A9 EC F8
```

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.

Приложение № 3
к Договору на обслуживание
Клиента по системе «iBank»

Доверенность

Банку ПАО АКБ "Приморье"

от клиента _____

Настоящим доверяем банку хранить ключ ЭП в защищенном хранилище и использовать его для формирования ЭП под документами системы "iBank".

1. Сведения о ключе проверки ЭП		
1.1	**Идентификатор**	
1.2	**Хранилище**	
1.3	**Наименование криптосредств**	
1.4	**Алгоритм**	
1.5	**ID набора параметров алгоритма**	
1.6	**Представление ключа проверки ЭП**	

Руководитель организации

_____ / _____ /
подпись Ф.И.О.

Владелец ключа

_____ / _____ /
подпись Ф.И.О.

Оттиск печати

Приложение № 4
к Договору на обслуживание
Клиента по системе «iBank»

Часть 1 Клиенту

г. _____ «___»_____20___г.

Акт об оказании услуг подключения рабочего места к системе ДБО

ПАО АКБ «Приморье» (публичное акционерное общество), именуемое далее Банк, в лице _____

и_____,

(полное / сокращенное наименование клиента)

именуемое (ый) далее Клиент, в лице _____

составили акт о нижеследующем:

Банк выполнил услуги по подключению рабочего места Клиента к системам ДБО с использованием следующих устройств и защитных средств:

	Тип устройства	**Наименование устройств**	**Идентификатор устройства, S/N**	**Количество (шт.)**	**Стоимость услуги (руб.)**
□	USB токен				

Стоимость оказанной услуги: _____ (_____) руб. ___ коп.

(цифрами) *(прописью)*

Вышеуказанная услуга выполнена полностью и в срок. Клиент претензий по объему, качеству и срокам оказания услуги не имеет.

Банк: **Клиент:**

_____ _____

_____ _____

Часть 2

В юридическое дело

(код_____)

г. _____ «___»_____20___г.

Акт об оказании услуг подключения рабочего места к системе ДБО

ПАО АКБ «Приморье» (публичное акционерное общество), именуемое далее Банк, в лице _____

и_____,

(полное / сокращенное наименование клиента)

именуемое (ый) далее Клиент, в лице _____

составили акт о нижеследующем:

Банк выполнил услуги по подключению рабочего места Клиента к системам ДБО с использованием следующих устройств и защитных средств:

	Тип устройства	**Наименование устройств**	**Идентификатор устройства, S/N**	**Количество (шт.)**	**Стоимость услуги (руб.)**
□	USB токен				

Стоимость оказанной услуги: _____ (_____) руб. ___ коп.

(цифрами) *(прописью)*

Вышеуказанная услуга выполнена полностью и в срок. Клиент претензий по объему, качеству и срокам оказания услуги не имеет.

Банк: **Клиент:**

_____ _____

_____ _____

_____ _____