Приложение №1
к Приказу от 31.08.2012 № 265

ДОГОВОР №_____
на обслуживание в системе
«iBank 2»

г._____ «___» _____ 20__г.

КОММЕРЧЕСКИЙ БАНК «АГРОПРОМКРЕДИТ» (Открытое акционерное общество), именуемый в дальнейшем «Банк», в лице_____ _____, действующего на основании _____, с одной стороны, и _____, именуем___ в дальнейшем «Клиент», в лице_____ _____, действующего на основании _____, с другой стороны, вместе в дальнейшем именуемые «Стороны», заключили настоящий Договор о нижеследующем.

1. Предмет Договора

1.1. *В соответствии с настоящим Договором Банк осуществляет обслуживание следующих счетов Клиента:*

*№*_____
_____
_____ *в Банке (далее по тексту — «Счет») с использованием системы «iBank2» (далее по тексту – «Система»), позволяющей посредством сети Интернет отправлять в Банк расчетные и иные документы, указанные в п. 3.5. настоящего Договора, а также самостоятельно получать информацию о текущем состоянии Счета.*

1.2. Настоящий Договор является приложением к Договорам _____ _____ _____, заключенным Сторонами (далее по тексту — «Договор банковского счета»). Во всем ином, что не предусмотрено настоящим Договором, Стороны в своих взаимоотношениях в отношении каждого из указанных в п. 1.1 настоящего Договора счетов руководствуются положениями соответствующего данному счету одному из указанных выше договоров.

2. Термины, применяемые в настоящем Договоре

Термины, применяемые в тексте настоящего Договора, используются в следующем значении.

2.1. **«Система «iBank2» (Система)»** – автоматизированная организационно-техническая система «iBank 2» обеспечения электронного документооборота и безбумажных расчетов, согласованно эксплуатируемая Клиентом и Банком, обеспечивающая подготовку, защиту и обработку документов в электронном виде с использованием электронно-вычислительных средств обработки информации и публичной сети Интернет. Система «iBank2» является корпоративной информационной системой и имеет Свидетельство о государственной регистрации программы для ЭВМ Системы электронного банкинга «iBank 2» (iBank 2) № 2011617014, выданное Федеральной службой по интеллектуальной собственности, патентам и товарным знакам ОАО «БИФИТ», зарегистрированное в Реестре программ для ЭВМ 08.09.2011 г.

2.2. **«Документ в электронной форме» (Электронный документ – ЭД)** – документ, в котором информация представлена в электронно-цифровой форме, содержащий сообщение Банка Клиенту или Клиента Банку, в т.ч. поручение Клиента Банку о совершении операции по Счету. Данный документ представлен в виде файла или записи в базе данных.

2.3. **«Электронная подпись» (ЭП)** – вид аналога собственноручной подписи, предназначенный для защиты Электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием Закрытого ключа ЭП и позволяющий идентифицировать владельца Сертификата ключа проверки ЭП, а также установить отсутствие искажения информации в Электронном документе. ЭП однозначно увязывает в одно целое содержание документа и закрытый ключ подписывающего и делает невозможным изменение документа без нарушения подлинности данной подписи. Для создания и проверки ЭП используется средство криптографической защиты – программная библиотека защиты информации «Криптомодуль С23» (Сертификат соответствия ФСБ РФ регистрационный номер

СФ/114-1511, от 08.07.2010г.). ЭП является усиленной неквалифицированной электронной подписью.

Банк вправе в одностороннем порядке менять перечень средств криптографической защиты, используемых в Системе, без дополнительного согласования и уведомления Клиента. При изменении средств криптографической защиты информации Банк уведомляет об этом Клиента любым не запрещенным законом способом, в том числе по Системе, а Клиент обязан получить (принять) от Банка такие средства криптографической защиты и использовать их в работе с Системой.

2.4. **«ЭП Клиента»** – электронная подпись уполномоченного Клиентом лица.

2.5. **«ЭП Банка»** – электронная подпись уполномоченного Банком лица.

2.6. **«Владелец сертификата ключа проверки ЭП»** – физическое лицо, владеющее соответствующим закрытым ключом ЭП, позволяющим создавать свою ЭП в электронных документах (подписывать Электронные документы).

2.7. **«Закрытый ключ ЭП»** – уникальная последовательность символов, известная владельцу сертификата ключа проверки подписи и предназначенная для создания ЭП. Закрытый ключ изготавливается (генерируется) абонентом Системы при помощи указанных выше криптобиблиотек и предназначен для формирования им ЭП в ЭД. Закрытый ключ ЭП хранится в цифровом виде на носителе Клиента (например на USB-токене).

2.8. **«Открытый ключ ЭП»** – уникальная последовательность символов, соответствующая Закрытому ключу ЭП, предназначенная для проверки подлинности ЭП в Электронном документе. Открытый ключ, автоматически формируемый программными средствами Системы при изготовлении Закрытого ключа ЭП и однозначно зависящий (производный) от него. Открытый ключ ЭП предназначен для проверки ЭП, сформированной данным участником Системы при подписании ЭД. Открытый ключ считается принадлежащим абоненту, если он был зарегистрирован в установленном порядке (в Банк представлен Сертификат ключа проверки ЭП с указанием Открытого ключа ЭП).

2.9. **«Сертификат ключа проверки ЭП»** – подписанный владельцем ЭП и заверенный подписью руководителя и оттиском печати Клиента документ на бумажном носителе с указанным в шестнадцатеричном виде Открытым ключом ЭП Клиента (по форме Приложения №4), подтверждающий принадлежность Открытого ключа ЭП Владельцу сертификата ключа проверки ЭП.

2.10. **«Пара ключей ЭП»** – Закрытый ключ и соответствующий ему Открытый ключ ЭП.

2.11. **«Подлинность ЭД»** – означает, что данный документ (экземпляр документа) создан в Системе без отступлений от принятой технологии. ЭД считается подлинным, если он был, с одной стороны, должным образом оформлен, заверен (подписан) ЭП и передан на обработку, а с другой, был принят к исполнению. Свидетельством того, что ЭД принят к исполнению, является уведомление «на исполнении» в строке статуса в соответствующем модуле, загруженном с банковского сервера Системы.

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

- утрата ключевых элементов;
- утрата ключевых элементов с последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевой информации;
- нарушение правил хранения и уничтожения (после окончания срока действия) секретного ключа;
- несанкционированное копирование или подозрение на копирование хранилища (носителя) с секретными ключами;
- возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
- случаи, когда нельзя достоверно установить, что произошло с носителями электронных ключей, содержащими ключевую информацию (в том числе случаи, когда носитель вышел из строя и достоверно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

2.13. **Средства Криптографической Защиты конфиденциальной Информации (СКЗИ)** – аппаратные, программно-аппаратные и программные средства, реализующие криптографические алгоритмы преобразования информации с целью: защиты информации при ее обработке, хранении и передаче по транспортной среде; обеспечения достоверности и целостности информации (в том числе с использованием алгоритмов цифровой подписи) при ее обработке, хранении и передаче по транспортной среде; выработки информации, используемой для идентификации и аутентификации субъектов, пользователей и устройств; выработки информации, используемой для защиты аутентифицирующих элементов защищенной системы при их выработке, хранении, обработке и передаче.

2.14. **«Статический IP-адрес» –** это уникальный цифровой адрес компьютера в сети Интернет, который выдается провайдером, и не изменяется при подключении к сети Интернет.

2.15. «**OTP-токен»** – устройство дополнительной аутентификации Клиента, являющееся генератором одноразовых паролей, действительных для подтверждения одной операции Клиентом в Системе,

2.16. «**USB-токен»** - устройство, позволяющего формировать ЭП Клиента внутри SIM-карты токена, предназначенное для противодействия хищениям вредоносными программами (троянами) секретных ключей ЭП.

2.17. «**Одноразовый пароль»** - это пароль, действительный только для одной операции. Действие одноразового пароля может быть ограничено определённым промежутком времени. Источником получения одноразового пароля может быть OTP-токен, SMS-сообщение и др.(в зависимости от условий подключённых услуг).

3. Соглашения Сторон

3.1. Стороны согласны с тем, что алгоритмы создания и функционирования Электронной подписи в Системе при передаче Электронных документов, реализация которых осуществляется в соответствии со стандартами ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001 (ГОСТ Р 34.10-94) (их аналогами в случае их замены), достаточны для обеспечения защиты от несанкционированного доступа, подтверждения авторства и подлинности информации, содержащейся в получаемых Электронных документах, а также сохранения банковской тайны.

3.2. Стороны согласны с тем, что положительный результат проверки ЭП Клиента в Системе на сервере Банка является подтверждением того, что:

- полученный Электронный документ подписывался соответствующей ЭП Клиента,
- Электронный документ получен в том виде, в котором он исходил от Клиента.

3.3. Стороны согласны с тем, что хранящиеся в контрольных архивах Системы Электронные документы, подписанные ЭП Клиента, проверка которых Открытым ключом ЭП Клиента дала положительный результат, являются доказательным материалом для решения спорных вопросов в соответствии с действующим законодательством и Приложением №1 – «Положение о порядке разрешения спорных ситуаций».

Проверка осуществляется путем использования функции «Проверить ЭЦП» или «Проверить ЭП» в модуле операциониста Системы, положительным результатом выполнения которой является выведенное на экран монитора сообщение «ЭЦП верна» или «ЭП верна», а также информация о номере идентификатора ключа, дате и времени подписания документа.

3.4. Стороны согласны с тем, что при изменении Электронного документа, заверенного к моменту внесения изменений Электронной подписью, ЭП становится некорректной, то есть проверка ЭП Открытым ключом ЭП дает отрицательный результат. Исправление или изменение Электронного документа, заверенного электронной подписью, возможно только путем создания нового Электронного документа.

3.5. Стороны считают, что любые Электронные документы, заверенные ЭП Клиента, хранящиеся в виде записи в контрольных архивах Системы или извлеченные из нее в виде отдельного файла, юридически эквивалентны соответствующим документам на бумажном носителе, подписанным уполномоченным(и) представителем(ями) Клиента и имеющим оттиск печати Клиента, обладают юридической силой и подтверждают наличие правовых отношений между Сторонами. Электронные документы, исходящие от Клиента, без ЭП Клиента не имеют юридической силы, Банком не рассматриваются и не исполняются.

Стороны считают, что Электронные документы: «письмо», заверенное ЭП Банка, «выписка по счету», юридически эквивалентны соответствующим документам на бумажном носителе, подписанным уполномоченными лицами Банка и имеющим оттиск печати Банка. Электронные документы, исходящие от Банка, без ЭП Банка не имеют юридической силы.

Вышеуказанный перечень Электронных документов может изменяться Банком с предварительным уведомлением Клиента сообщением по Системе.

Направление Клиентом Банку иных видов Электронных документов может осуществляться после предварительного согласования с Банком посредством обмена подтверждающими Электронными документами, направляемыми по Системе.

3.6. Стороны согласны с тем, что Открытый ключ ЭП, указанный в заверенном подписью руководителя и оттиском печати Клиента Сертификате ключа проверки ЭП, принадлежит Клиенту и достаточен для определения Банком корректности ЭП.

3.7. Стороны признают в качестве единой шкалы времени при работе с системой Московское поясное время. Контрольным является время системных часов Системы. Стороны признают информацию о дате и времени поступления, исполнения, неисполнения Электронных документов в Банк, содержащуюся в

контрольных архивах Банка, необходимым и достаточным доказательством даты и времени передачи, исполнения, неисполнения Клиентом Банку Электронного документа.

3.8. Стороны согласны с тем, что необходимыми и достаточными основаниями для проведения Банком соответствующей операции на основании указанного Электронного документа являются: наличие у Банка надлежаще оформленного Электронного документа, подписанного ЭП Клиента, проверка корректности которой Открытым ключом ЭП Клиента дала положительный результат, а также, подтверждение платежа, осуществляемого в валюте РФ - одноразовым паролем.

3.9. Стороны согласны с тем, что использование всемирной телекоммуникационной сети общего доступа Интернет может вызывать перерывы в приеме и обработке Электронных документов в Системе, связанные с отказами телекоммуникационного оборудования провайдеров телекоммуникационных услуг, а также вирусными и иными атаками на систему. Стороны обязаны принимать все доступные способы защиты от указанных угроз.

3.10. Стороны согласны с тем, что контроль за сроком действия ЭП, а также контроль за наличием соответствующих полномочий у Владельца сертификата ключа проверки ЭП осуществляется Клиентом, а не Банком.

3.11. Стороны договорились, что в Приложении №4 к настоящему Договору:

- наименование «Сертификат открытого ключа ЭЦП Сотрудника клиента в системе “Internet-Банкинг” ОАО КБ “АГРОПРОМКРЕДИТ”» читать как «Сертификат ключа проверки электронной подписи сотрудника клиента в системе “iBank2”»;

- по тексту Приложения №4: «ЭЦП» читать как «ЭП».

4. Права и обязанности Банка

4.1. Банк обязан исполнять принятые от Клиента Электронные документы, указанные в п. 3.5. Договора, подписанные корректной ЭП Клиента и подтверждённые одноразовым паролем, в соответствии с условиями настоящего Договора, Договоров банковского счета и действующим законодательством.

4.2. Банк обязан по получении от Клиента уведомления по форме Приложения №2 временно блокировать (досрочно прекратить действие) пары ключей ЭП Клиента в Системе. Банк не обязан проверять подлинность подписи Клиента на полученном уведомлении, а обязан только установить путем обычного визуального контроля соответствие данной подписи имеющемуся у Банка образцу. Наложенная блокировка снимается только на основании требования Клиента не позднее дня, следующего за днем получения такого требования.

4.3. Банк обязан обеспечить строго контролируемый и ограниченный доступ к помещениям, в которых находятся программно-аппаратные средства, содержащие контрольные архивы Системы.

4.4. Банк обязан хранить в секрете и не передавать третьим лицам Закрытые ключи ЭП Банка и Открытые ключи ЭП Клиента, используемые при работе в Системе. Риск неблагоприятных последствий, связанных с использованием Закрытого Ключа ЭП Банка третьими лицами в случае несоблюдения условий сохранности, несет Банк.

4.5. Банк имеет право по своему усмотрению прекратить принятие от Клиента Электронных документов по Системе и потребовать от Клиента смены пары ключей ЭП Клиента, направив уведомление по форме Приложения №3.

4.6. Банк имеет право приостановить работу Клиента в Системе и (или) не производить исполнения полученного Электронного документа, сообщив об этом Клиенту не позднее дня, следующего за днем его получения, путем направления сообщения по Системе и, соответственно, затребовать от Клиента оформления документа на бумажном носителе (подлинника) с подписью уполномоченных лиц и оттиском печати Клиента.

4.7. Банк вправе не принимать Сертификат ключа проверки ЭП Клиента, если подписи Владельца сертификата ключа проверки ЭП и (или) руководителя Клиента проставлена не в присутствии уполномоченного представителя Банка или если подлинность вышеуказанных подписей не заверена нотариально.

4.8. Банк имеет право отказать в исполнении Электронного документа Клиента в случае несоответствия реквизитов такого документа обязательным реквизитам, установленным действующим законодательством РФ и банковскими правилами.

4.9. Банк имеет право приостановить работу Клиента в Системе в случае невнесения платы за пользование Системой в соответствие с Тарифами. В этом случае Банк предварительно уведомляет Клиента по Системе либо иным способом о предстоящей приостановке и приостанавливает работу Клиента

по истечении 7 (семи) календарных дней с момента направления уведомления.

4.10. В целях повышения эффективности противодействия хищениям вредоносными программами Банк обязан передать Клиенту за соответствующую плату в соответствии с действующими Тарифами по акту приема передачи OTP-токен (п. 5.16), а также USB–токен (п. 5.11.)..

4.11. Банк отсылает сообщения в формате SMS, предназначенные для Клиента на номер(а) телефона(ов), указанный(ые) Клиентом. В случае подключения режима расширенной аутентификации Банк отсылает сообщение на номер телефона, указанный Клиентом в Заявлении о подключении к услуге SMS-информирования, а в случае подключения режима SMS-уведомления о событии – Банк отсылает сообщение на номер телефона, указанный Клиентом в Системе (настройки в Системе производятся на стороне Клиента). При этом, Клиент осознает, что информация, указанная в SMS (в том числе относительно счета Клиента и операций по нему) может стать известной лицам и организациям, участвующим в передаче SMS (операторы сотовой связи, их контрагенты, задействованные в процессе передачи данной информации).

4.12. Банк обязуется подключить Клиента к Услуге SMS-информирования в течение двух рабочих дней со дня подачи в Банк заявления по форме Банка, подписанного уполномоченным лицом Клиента.

4.13. Банк вправе в одностороннем порядке вводить новые услуги и предлагать Клиенту их подключение. При этом Банк вправе направить Клиенту уведомление о введении новой услуги с описанием порядка предоставления услуги. В этом случае Клиент вправе воспользоваться услугой на условиях указанных в уведомлении. Плата за подключение новых услуг взимается в соответствие с Тарифами.

4.14. Банк вправе по техническим причинам либо в связи с изменениями требований по безопасности в Системе, либо в связи с изменениями в законодательстве Российской Федерации, вводить новые услуги, изменять порядок предоставления услуг (SMS-информирование, IP-фильтрация, OTP-токен, USB-токен, любых иных услуг), либо прекратить их предоставление с предварительным уведомлением Клиента за 5 (пять) рабочих дней до соответствующего изменения/прекращения.

4.15. Банк вправе изменять порядок доступа Клиента в Систему, форму и содержание интерфейса Клиента, порядок пользования Системой, а также устанавливать/ отменять дополнительные требования к мерам безопасности, которые должен соблюдать Клиент при работе с Системой (Банк вправе в одностороннем порядке вносить изменения в Приложение № 5 с предварительным уведомлением Клиента по Системе за 5 рабочих дней).

4.16. В целях соблюдения требований по безопасности Банк имеет право в одностороннем порядке изменять форму Сертификата ключа проверки ЭП в Системе. В этом случае Банк вправе потребовать от Клиента осуществить смену пар ключей ЭП и явиться в Банк для предоставления новых Сертификатов.

4.17. В случаях, предусмотренных законодательством, Банк производит информирование Клиента о совершении каждой операции с использованием электронного средства платежа одним из следующих способов: через Систему, посредством SMS-сообщений или электронной почтой.

5. Права и обязанности Клиента

5.1. Клиент имеет право требовать от Банка предоставления на бумажном носителе копий полученных Банком Электронных документов с проставлением на них соответствующих отметок Банка (об исполнении и др.). Указанные документы предоставляются уполномоченному лицу Клиента при его явке в Банк.

5.2. Клиент имеет право досрочно прекращать действие Открытых ключей ЭП Клиента (вместе с соответствующими Закрытыми ключами ЭП Клиента), направив уведомление по форме Приложения №2, подписанное уполномоченным лицом (данное уведомление может быть направлено в Банк в письменном виде (передано в Банк, направлено в Банк по факсу)) либо направлено в Банк с использованием Системы, при обязательном дублировании сообщения в письменном виде. Для продолжения дальнейшей работы в Системе уполномоченный представитель Клиента должен сгенерировать новую пару ключей ЭП Клиента и передать Банку новый Сертификат ключа проверки ЭП Клиента.

5.3. Клиент имеет право блокировать Открытый ключ ЭП Клиента, т.е. приостановить свою работу в Системе, направив уведомление по форме Приложения №2, подписанное уполномоченным лицом (данное уведомление может быть направлено в Банк в письменном виде (передано в Банк, направлено в Банк по факсу)) либо направлено в Банк с использованием Системы, при обязательном дублировании сообщения в письменном виде. Блокировка снимается не позднее дня, следующего за днем получения Банком письменного требования Клиента о снятии блокировки.

5.4. Клиент обязан при создании Электронных документов в Системе соблюдать условия настоящего Договора, нормы действующего законодательства и банковские правила в отношении обязательных реквизитов данных документов, в отношении мер безопасности при работе с системой (Приложение №5).

5.5. Клиент обязан обеспечить хранение в секрете и отсутствие доступа неуполномоченных лиц к рабочему месту Клиента, Закрытому ключу ЭП Клиента и Открытому ключу ЭП Банка, используемым при работе в Системе, к OTP-токенам и USB-токенам, а также обеспечить отсутствие доступа неуполномоченных лиц к телефонам, к которым подключена услуга SMS-информирование. Клиент несет риск неблагоприятных последствий, связанных с несоблюдением рекомендаций Банка по безопасности (Приложение №5), а также с невыполнением обязанностей, установленных настоящим пунктом, в результате чего может стать возможным использование Закрытого Ключа ЭП Клиента неуполномоченными лицами.

5.6. Клиент обязан сообщать Банку об обнаружении попытки несанкционированного доступа к Системе или к Закрытому ключу ЭП Клиента незамедлительно после ее обнаружения и блокировать свою работу в Системе, направив в Банк уведомление по форме Приложения №2. Клиент несет риск всех последствий, связанных с несанкционированным доступом к Системе или Закрытому ключу ЭП Клиента.

5.7. Клиент обязан по требованию Банка приостановить работу в Системе и для ее возобновления сгенерировать новую пару ключей ЭП Клиента и передать Банку Сертификат ключа проверки ЭП. Сертификат ключа проверки ЭП Клиента должен передаваться в Банк уполномоченным лицом Клиента (единоличным исполнительным органом либо через доверенное лицо при наличии доверенности (например, по форме Приложения №6) либо иным способом, позволяющим установить, что документ исходит от Клиента).

5.8. Клиент обязан уведомлять Банк о смене лиц, уполномоченных работать с Системой и распоряжаться Счетом, а также об изменении полномочий лиц, к телефонам которых подключена услуга SMS – информирование. Для возможности работы с Системой новых лиц обеспечить им возможность сгенерировать Пару ключей ЭП Клиента. Риск неблагоприятных последствий, связанных с несвоевременным уведомлением Банка о том, что необходимо приостановить действие ЭП Клиента несет Клиент.

5.9. Клиент обязан регулярно производить оплату за пользование Системой в соответствии с Тарифами, являющимися неотъемлемой частью Договора, а также регулярно (не менее 1 раза в день) проводить проверки наличия в Системе информационных сообщений от Банка.

5.10. Клиент обязан хранить свой Закрытый ключ ЭП в течение срока действия данного Договора, а также не менее 8 (восьми) лет после расторжения данного Договора. В случае если Клиент после расторжения настоящего Договора оспаривает операции, проведенные Банком с использованием его ЭП (в т.ч. закрытого ключа) и не может предъявить используемый закрытый ключ ЭП для проведения проверки, то считается, что Клиент подтверждает правильность проведения операций Банком с использованием данной ЭП (в т.ч. закрытого ключа).

5.11. В целях повышения эффективности противодействия хищениям вредоносными программами секретных ключей ЭП Клиенту при подключении по акту приема-передачи за соответствующую плату в соответствии с действующими Тарифами предоставляется устройство USB-токен, позволяющее формировать ЭП Клиента внутри SIM-карты токена (Сертификат соответствия ФСБ РФ, регистрационный номер СФ/114-1511 от 08.07.2010). Клиент вправе заказать в Банке дополнительный USB-токен, для этого необходимо предварительно (за 1 месяц) до желаемой даты получения USB-токена подать заявление в письменном/электронном виде и оплатить его стоимость в соответствии с действующими Тарифами.

5.12. Клиент обязуется обеспечить условия сохранения переданного USB-токена в соответствии с требованиями действующего законодательства (в т.ч. Приказа ФАПСИ РФ № 152 от 13.06.2001.)

5.13. Клиент несет персональную ответственность за сохранность переданного USB-токена, после подписания сторонами соответствующего Акта приема-передачи.

5.14. В случае утраты Клиентом мобильного телефона (SIM-карты) Клиент обязан:

- при подключении к режиму SMS-уведомления о событии Клиент обязан в максимально короткие сроки самостоятельно сменить настройки в Системе, в том числе номер(а) мобильного(ых) телефона(ов);
- при подключении Клиента к режиму расширенной аутентификации, Клиент обязан позвонить в Банк и заблокировать режим расширенной аутентификации. При блокировке режима расширенной аутентификации и подозрении на компрометацию Пары Ключей ЭП, Клиент обязан предоставить в Банк в течение 3 (Трех) рабочих дней письменное уведомление о прекращении действия открытого ключа ЭП и соответствующего ему закрытого ключа ЭП (по форме Приложения №2 – являющегося неотъемлемой частью настоящего Договора) и оформить новые Сертификаты ключей проверки ЭП по правилам п. 4.7. Договора. Для продолжения дальнейшей работы в режиме расширенной аутентификации, Клиенту необходимо предоставить в Банк Заявление в соответствии с п. 7.1.2. Договора.

5.15. Клиент обязан самостоятельно обеспечить поддержку функции SMS на своём мобильном телефоне, а также подписку на услугу SMS у своего оператора сотовой связи.

5.16. Для увеличения уровня противодействия возможным попыткам хищения средств Клиента в Системе, Клиенту по акту приема - передачи за соответствующую плату в соответствии с действующими Тарифами предоставляется средство дополнительной аутентификации - OTP-токен. Данное устройство является генератором одноразовых паролей и служит дополнительным средством для аутентификации Клиента.

Клиент вправе заказать в Банке дополнительный (-ые) OTP-токены. Для этого Клиент должен предварительно (за 1 месяц) до планируемой даты начала использования дополнительного OTP-токена подать заявление по форме Банка в письменном/электронном виде и оплатить его стоимость в соответствии с действующими Тарифами.

При использовании Клиентом OTP-токена отправка электронных платежей, проводимых в валюте РФ в Системе без введения одноразового пароля невозможна. При получении Банком Электронного документа с корректной ЭП, Банк считает, что Клиентом введен одноразовый пароль, сгенерированный OTP-токеном и документ отправлен Клиентом. OTP-токен не заменяет ЭП, а является дополнительным средством защиты.

5.17. Клиент несет персональную ответственность за сохранность OTP-токена после подписания сторонами Акта приема-передачи по форме Банка.

5.18. Клиент обязан организовать секретное хранение и обеспечить отсутствие доступа неуполномоченных лиц к OTP-токену. Риск неблагоприятных последствий, связанных с использованием OTP-токена Клиента неуполномоченными лицами, несет Клиент.

5.19. При одновременном пользовании услугой SMS-информирование в режиме расширенной аутентификации и услугой по использованию средства дополнительной аутентификации OTP-токен, Клиент обязан для авторизации в Системе и отправки Электронных документов вводить одноразовый пароль. В этом случае, Клиент самостоятельно выбирает способ подтверждения для авторизации в Системе и отправки Электронных документов: путем получения SMS-сообщения на мобильный телефон или генерации одноразового пароля с помощью OTP-токена. При необходимости (по техническим причинам либо в связи с изменениями требований безопасности) Банк вправе в одностороннем порядке изменить способ и условия получения одноразового пароля с предварительным уведомлением Клиента за 5 (пять) рабочих дней до соответствующего изменения.

При авторизации Клиента в Системе путем подтверждения одноразовым паролем, выбранным Клиентом одним из вышеуказанных способов, Банк считает, что доступ к Системе имеет уполномоченное лицо Клиента.

При получении Банком Электронного документа с корректной ЭП Банк считает, что Клиентом введен одноразовый пароль, выбранный Клиентом при помощи одного из вышеуказанных способов, и документ отправлен Клиентом.

6. Совместные обязательства и ответственность Сторон

6.1. Каждая Сторона обязана за собственный счет поддерживать в рабочем состоянии свои программно-технические средства, используемые при работе с Системой.

6.2. В случае возникновения конфликтных ситуаций между Сторонами при использовании Системы Стороны обязуются участвовать в рассмотрении конфликтов в соответствии с «Положением о порядке разрешения спорных ситуаций» (Приложение №1), выполнять требования указанного Положения и нести ответственность согласно выводам по рассмотрению конфликтной ситуации. В случае, если Клиент отказывается от принятия на себя обязательств по Электронному документу (оспаривает факт или время передачи Электронного документа, его содержание), бремя доказывания обстоятельств, на основании которых он отказывается от принятия на себя обязательств, ложится на него. Ответственность может быть возложена на Банк в случае если создание Электронного документа обусловлено противоправными действиями Банка.

6.3. Стороны обязуются при разрешении споров, которые могут возникнуть в связи с использованием электронной Системы, предоставлять в письменном виде свои оценки, доказательства и выводы по запросу противоположной Стороны.

6.4. Банк не несет ответственности за ущерб, причиненный Клиенту в результате использования третьими лицами Закрытого ключа ЭП Клиента (компрометация ключа).

6.5. Банк не несет ответственности за техническое состояние компьютерного оборудования Клиента, возможные помехи в телефонных линиях связи, прекращение работы Системы из-за отключения электроэнергии и повреждения линий связи, программно-аппаратные сбои Системы, если возникновение указанных обстоятельств не связано с виновными действиями Банка.

6.6. Банк не несет ответственности перед Клиентом, в случае, если Электронный документ подписан корректной ЭП, но исходил не от Клиента.

6.7. Стороны освобождаются от ответственности за неисполнение или ненадлежащее исполнение принятых по настоящему Договору обязательств на период действия обстоятельств непреодолимой силы и их последствий. К таким обстоятельствам относятся, в частности, стихийные бедствия, пожары, аварии, массовые беспорядки, забастовки, военные действия, противоправные действия третьих лиц, вступление в силу законодательных актов, актов органов федеральных или местных органов власти и обязательных для исполнения одной из сторон, прямо или косвенно запрещающих или ограничивающих указанные в настоящем Договоре виды деятельности или препятствующие выполнению сторонами своих обязательств по настоящему Договору. Сторона, пострадавшая от влияния обстоятельств непреодолимой силы, обязана в возможно короткий срок, но не более чем через 7 (Семь) дней после возникновения этих обстоятельств, довести до сведения другой Стороны информацию о случившемся.

6.8. Банк несет ответственность за неисполнение (ненадлежащее исполнение) обязательств по настоящему Договору только при наличии своей вины.

6.9. Банк не несёт ответственности за задержки и сбои, возникающие в сетях операторов сотовой связи, которые могут повлечь за собой задержку или даже недоставку SMS / одноразового пароля Клиенту.

6.10. Клиент несёт ответственность за правильность (достоверность и актуальность) данных, указанных в заявлении (в том числе номера мобильного телефона, на который будет отправляться соответствующая информация). Недостоверность информации, указанной в заявлении, может служить отказом в подключении Клиента к Услуге SMS-информирование.

6.11. Стороны признают, что SMS-сообщения, переданные Банком в соответствии с условиями настоящего Договора, являются сообщениями, надлежащим образом переданные Клиенту.

6.12. Банк не несет ответственности за разглашение информации, связанное с ненадлежащим хранением телефона(ов) и (или) SIM-карты, к которым подключена услуга SMS-информирование.

7. Порядок обслуживания Клиента

7.1. Для начала работы по настоящему Договору Клиент обязан произвести оплату за установку Системы и (или) иные платежи в соответствии с Тарифами Банка и предоставить Банку Сертификат(ы) ключа проверки ЭП Клиента.

При этом при генерации ЭП, Сертификата ключа проверки ЭП Клиент обязан использовать средства защиты, полученные согласно п. 5.11. настоящего Договора.

7.1.1. В целях минимизации вероятности проведения платежей от имени Клиента третьими лицами в случае хищения секретных ключей, Клиент вправе обратиться в Банк с Заявлением о подключении к услуге IP-фильтрации по форме Банка. Данная услуга позволяет обрабатывать информацию только в случае совпадения статического IP-адреса передающего компьютера с ранее указанным статическим IP-адресом Клиента, хранящемся в базе данных Банка. Банк принимает к исполнению Электронные документы, поступающие только с зарегистрированных в Системе статических IP- адресов (количество адресов IP-фильтрации в Системе не ограничено). Попытки доступа с неразрешенного (незарегистрированного) IP-адреса блокируются Системой. При этом Клиент подтверждает, что Электронный документ, исходящий с зарегистрированных статических IP-адресов Клиента исходит от Клиента.

Новый статический IP-адрес может быть добавлен Банком в список разрешенных IP-адресов по письменному заявлению Клиента, поданному по форме Банка, подписанному и переданному в Банк уполномоченным лицом Клиента.

В случае не подключения к услуге IP-фильтрации и последующим хищением средств, ставшим возможным вследствие отправки ЭД подписанного корректной ЭП, но отправленного с IP-адреса третьих лиц, Банк ответственности не несет.

При получении Банком Электронного документа с корректной ЭП, Банк считает, что документ отправлен с IP- адреса Клиента независимо от того подключен ли Клиент к услуге IP – фильтрации.

7.1.2. В целях информационного обслуживания Клиента и минимизации рисков проведения платежей от имени Клиента третьими лицами, Клиент вправе обратиться в Банк с Заявлением о подключении к услуге SMS-информирования по форме Банка. Услуга SMS-информирования предоставляется в двух режимах: SMS- уведомление о событии и расширенная аутентификация. Клиент вправе подключиться к одному или нескольким режимам одновременно. Отключение от Услуги осуществляется на основании Заявления Клиента подаваемого по форме Банка.

Режим SMS-уведомления о событии предназначен для уведомления Клиента о событиях, которые произошли в Системе. Условия и параметры сообщений Клиент настраивает в Системе самостоятельно. Клиент имеет право самостоятельно изменять в Системе набор рассылок в режиме SMS-уведомления о событии при наступлении определенных событий (утрата мобильного телефона, SIM-карты и др.), номера телефонов, список обслуживаемых счетов и др. Клиент вправе выбрать следующие сообщения:

- об отвержении документа;
- о поступлении в Банк документа;
- о входящих банковских письмах;
- о движении средств по счету;
- о входе в систему;
- о текущих остатках;
- выписка по счету;
- иные сообщения (в случае наличия в Системе).

Перечень доступных для выбора сообщений может изменяться Банком самостоятельно без дополнительного уведомления Клиента.
Режим расширенной аутентификации предназначен для минимизации вероятности проведения платежей от имени Клиента третьими лицами. Данный режим позволяет при авторизации в Системе получать SMS-сообщения на мобильный(ые) телефон(ны) Клиента. Режим расширенной аутентификации устанавливается Банком по заявлению Клиента, в котором указываются номер(а) мобильного(ых) телефона(ов), на который(ые) клиент рассчитывает получать SMS-сообщения с дополнительным кодом. При подключении режима расширенной аутентификации работа в системе без введения дополнительного кода не возможна, за исключением случаев, указанных в настоящем договоре (5.19., 4.14-4.16 и др.)

Комиссия за фактически предоставленные Услуги SMS-информирования за период, в который произошло подключение или отключение (как по инициативе Банка, так и по инициативе Держателя), приравнивается к комиссии за полный месяц предоставления Услуги. Комиссия за предоставление услуги SMS-информирования взимается в соответствии с Тарифами Банка.

7.1.3. Банк начинает прием Электронных документов от Клиента не позднее рабочего дня следующего за днем предоставления в Банк надлежаще оформленных Сертификатов ключей проверки ЭП, получения Клиентом OTP-токена, USB-токена согласно п.4.13 договора и оплаты. До этого момента Банк не принимает Электронные документы Клиента.

При получении Банком Электронных документов, либо соответствующих документов на бумажных носителях, подтверждающих прекращение полномочий какого-либо из представителей Клиента, Банк прекращает прием Электронных документов, подписанных ЭП данного лица.

При предоставлении Клиентом полномочий по работе с Системой и распоряжению Счетом новому лицу, Банк начинает прием от Клиента Электронных документов, подписанных ЭП данного лица, начиная со дня, следующего за днем получения Сертификата ключа проверки ЭП, содержащего Открытый ключ ЭП данного лица, а также документов подтверждающих полномочия нового Владельца сертификата ключа проверки ЭП.

7.2. Банк осуществляет прием Электронных документов, передаваемых по электронной Системе, круглосуточно, за исключением времени проведения требуемых работ, связанных с обновлением Системы, о времени и длительности которых Клиент извещается заранее электронным письмом из Банка, отправляемым по Системе. Использование Системы не лишает Клиента права предоставлять Банку расчетные и иные документы на бумажном носителе.

7.3. Исполнение документов осуществляется в сроки, установленные Договором банковского счета.

7.4. При получении Электронного документа Банк производит проверку:

- корректности ЭП Клиента Открытым ключом ЭП Клиента;
- правильности заполнения реквизитов Электронного документа в соответствии с требованиями законодательства РФ и Банка России (при этом Банк проверяет правильность заполнения реквизитов строго по формальным признакам, а именно проверяет факт заполнения обязательных реквизитов. Банк не проверяет корректность указанных Клиентом реквизитов ЭД, в том числе количество знаков в заполненных клиентом полях ЭД, последовательность нумерации ЭД);
- возможности возникновения дебетового сальдо на Счете Клиента, за исключением случаев, когда возникновение дебетового сальдо допустимо в соответствии с соглашением Сторон.

При выявлении отрицательного результата проверки любого из вышеуказанных обстоятельств полученный Электронный документ Банком не принимается, считается возвращенным Клиенту, поручение, содержащееся в нем, Банком не исполняется. Статус документа «отвергнут» в Системе информирует Клиента о неисполнении переданного им по Системе Электронного документа. Иного информирования Клиента о неисполнении Электронного документа Банк не осуществляет. Свидетельством того, что документ принят, является статус Электронного документа «исполнен» в Системе.

7.5. Дальнейшее оформление Электронных документов, переданных в Банк по Системе, осуществляется Банком без участия Клиента, в том числе оформление копий таких документов на бумажном носителе для передачи иным участникам расчетов. При этом дополнительное оформление документов по сравнению с установленными Банком России правилами безналичных расчетов осуществляется Банком только по требованию Клиента при явке его представителя в Банк.

7.6. Если по истечении 10 (десяти) рабочих дней с момента проведения Банком операции по Счету на основании полученного от Клиента Электронного документа, Клиентом не заявляется претензий по такой операции, признается, что Клиент подтвердил правильность проведения операции по его Счету.

7.7. Клиент имеет право с использованием Системы самостоятельно получать информацию о состоянии своего Счета на начало текущего операционного дня.

7.8. Работа с Системой осуществляется через сеть Интернет по электронному адресу, который сообщается Клиенту сотрудником Банка. Об изменении адреса в сети Интернет Банк уведомляет Клиента по Системе.

8. Действие Договора

8.1. Настоящий Договор вступает в силу с момента его подписания обеими сторонами и заключается на неопределенный срок.

8.2. Каждая из Сторон вправе расторгнуть настоящий Договор в одностороннем порядке не ранее, чем через 5 (Пять) рабочих дней после письменного уведомления об этом противоположной Стороны. При этом обязательства по настоящему Договору, возникшие в период его действия, не прекращаются до полного исполнения их Сторонами.

8.3. Расторжение настоящего Договора не влечет недействительности Электронных документов, содержащих корректную ЭП Клиента, переданных Клиентом по Системе до дня расторжения настоящего Договора включительно.

8.4. Настоящий Договор прекращает свое действие в случае расторжения всех, указанных в п.1.2. Договоров банковского счета.

9. Заключительные положения

9.1. Споры по настоящему Договору решаются путем переговоров в соответствии с Приложением №1, а при не достижении согласия — в Арбитражном суде _____. Применимым правом является право РФ.

9.2. Все приложения, изменения и дополнения к настоящему Договору оформляются в письменном виде, подписываются полномочными представителями Сторон и являются его неотъемлемой частью.

9.3. Настоящий Договор составлен в двух экземплярах по одному для каждой Стороны, оба экземпляра имеют одинаковую юридическую силу.

10. Юридические адреса Сторон

АГРОПРОМКРЕДИТ
коммерческий банк

Приложение №1
к Договору на обслуживание
в системе «iBank2»,
утвержденному Приказом от
31.08.2012 № 265

ПОЛОЖЕНИЕ
о порядке разрешения спорных ситуаций

1. В соответствии с настоящим Положением подлежат рассмотрению споры, связанные с наличием у Клиента к Банку претензий по поводу:

- факта передачи Клиентом Банку Электронного документа;
- дня передачи Клиентом Банку Электронного документа;
- содержания переданного Клиентом Банку Электронного документа.

Стороны договорились считать наличие корректной ЭП Клиента в оспариваемом Электронном документе необходимым и достаточным доказательством, подтверждающим принадлежность данного Электронного документа Клиенту и, соответственно, фактом, удостоверяющим передачу Электронного документа или содержание переданного Электронного документа. Стороны признают информацию о дате и времени поступления Электронных документов в Банк, содержащуюся в контрольных архивах Банка, необходимым и достаточным доказательством даты и времени передачи Клиентом Банку Электронного документа, если разрешительной комиссией не будет установлен факт внесения Банком изменений в указанную информацию в части, касающейся предмета спора. Корректность ЭП Клиента в оспариваемом Электронном документе устанавливается разрешительной комиссией в установленном ниже порядке. Иные споры разрешаются в соответствии с действующим законодательством в Арбитражном суде _____.

Проверка ЭП осуществляется путем использования функции «Проверить ЭЦП» или «Проверить ЭП» в модуле операциониста Системы, положительным результатом выполнения которой является выведенное на экран монитора сообщение «ЭЦП верна» или «ЭП верна», а также информация о номере идентификатора ключа, дате и времени подписания документа.

Стороны согласны с тем, что совпадение идентификатора ключа при проверке ЭП с идентификатором на Сертификате ключа проверки ЭП Клиента на бумажном носителе, представляемом Клиентом при регистрации ключа, подтверждает подлинность ЭП Клиента на документах, подвергавшихся проверке.

Электронные документы, не имеющие ЭП, при наличии спорных вопросов не являются доказательным материалом.

2. Клиент предоставляет Банку заявление, содержащее существо претензий с указанием на Электронный документ, содержащий ЭП Клиента, на основании которого Банк выполнил, не выполнил или не надлежаще выполнил какую-либо операцию. В данном Заявлении должно содержаться предложение о формировании разрешительной комиссии с указанием фамилий представителей Клиента, которые будут участвовать в работе комиссии.

3. Банк обязан в срок не более 10 (десяти) календарных дней рассмотреть указанное заявление Клиента. При несогласии Банка с претензиями Клиента Банк направляет Клиенту письмо с ответным предложением о формировании разрешительной комиссии. Письмо должно содержать фамилии представителей Банка, которые будут участвовать в работе комиссии.

4. Окончательное формирование комиссии осуществляется в течение трех рабочих дней с даты получения Клиентом указанного в п. 3 настоящего Положения письма Банка. В состав комиссии включаются в равном количестве представители Клиента и представители Банка (не более пяти с каждой стороны, включая Владельца оспариваемой ЭП), и, при необходимости, независимые эксперты, в т.ч. представители компании-разработчика Системы. В случае если за участие представителя компании-разработчика (либо за его письменное заключение) компанией-

разработчиком взимается плата, то данные расходы возлагаются на Клиента.

Независимый эксперт считается назначенным только при письменном согласии обеих Сторон. Место работы комиссии — местонахождение Банка, если иное не будет согласовано Сторонами. Если разрешительная комиссия без уважительных причин (под уважительными причинами подразумеваются: согласование Сторонами иного срока начала работы комиссии, временная нетрудоспособность одного из членов комиссии и др.) не приступит к работе по истечении пяти рабочих дней с даты получения Клиентом вышеуказанного письма Банка с предложением о ее формировании, считается, что Клиент отказался от заявленных им претензий.

5. Стороны обязуются способствовать работе комиссии и не допускать отказа от предоставления необходимых документов (информации), если предоставление таких документов (информации) будет допустимо в соответствии с действующим законодательством. Стороны обязуются предоставить комиссии возможность ознакомления с условиями и порядком работы своих программных и аппаратных средств, используемых для обмена Электронными документами по Системе.

6. Разрешительная комиссия в срок не более пяти дней проводит рассмотрение спорного вопроса. Рассмотрение в обязательном порядке должно включать следующие этапы.

6.1. Разрешительная комиссия проводит проверку Открытого ключа ЭП Клиента в Системе на его соответствие Сертификату ключа проверки ЭП Клиента, предоставленного Клиентом и Банком, (т.е. устанавливает его принадлежность Клиенту), проверяет период действия Открытого ключа ЭП Клиента.

6.2. Разрешительная комиссия проводит проверку Электронного документа, подписанного Электронной подписью Клиента, на основании которого Банком выполнены (не выполнены) оспариваемые Клиентом действия, т.е. принадлежность Клиенту и неизменность содержания спорного Электронного документа проверяется Открытым ключом ЭП Клиента. Проверка производится в соответствии с п. 3.3. Договора.

6.3. На основании полученных данных в результате указанной в п.п. 6.1 и 6.2 проверки разрешительная комиссия составляет акт, содержащий выводы по указанным выше вопросам. Выводы, содержащиеся в акте, являются обязательными для Сторон.

7. Результатом рассмотрения спорной ситуации разрешительной комиссией является определение Стороны, несущей ответственность согласно выводу о корректности Электронной подписи Клиента под Электронным документом.

8. Банк несет ответственность перед Клиентом в случае, когда имела место хотя бы одна из следующих ситуаций:

8.1. Банк не предъявляет Электронного документа, на основании которого Банк выполнил оспариваемую операцию.

8.2. Электронная подпись Клиента в Электронном документе оказалась некорректной.

Приложение №2
к Договору на обслуживание
в системе «iBank2»,
утвержденному Приказом от
31.08.2012 № 265

УВЕДОМЛЕНИЕ

о прекращении (приостановлении) действия Закрытого ключа ЭП и соответствующего ему Открытого ключа ЭП (_____)

Наименование Владельца ЭП Клиента

(Наименование Клиента) уведомляет Банк о том, что с «___» _____20___г. следует считать недействительным / следует заблокировать на срок ___ _____ _____ (нужное подчеркнуть) Открытый ключ ЭП (Наименование Владельца ЭП Клиента), имеющий регистрационный номер: _____ и соответствующий ему Закрытый ключ ЭП (Наименование Владельца ЭП Клиента).

_____
_____
_____
_____
(должность, наименование организации, ФИО) (подпись)

М.П.

Приложение №3
к Договору на обслуживание
в системе «iBank2»,
утвержденному Приказом от
31.08.2012 № 265

УВЕДОМЛЕНИЕ

о прекращении действия Закрытого ключа ЭП и соответствующего ему Открытого ключей ЭП
(Наименование Владельца ЭП Клиента)

Банк уведомляет (Наименование Клиента) о том, что с «___» _____ 20__г. следует считать недействительным Открытый ключ ЭП (Наименование Владельца ЭП Клиента), имеющий следующий регистрационный номер: _____.

С вышеуказанной даты соответствующий ему Закрытый ключ ЭП утрачивает силу для дальнейшего применения.

Для возобновления работы в Системе «iBank2» необходимо обратиться в обслуживающее (Наименование Владельца ЭП Клиента) подразделение Банка.

_____
_____
_____
(ФИО, должность, уполномоченного лица Банка) (подпись)
М.П.

Приложение №4
к Договору на обслуживание
в системе «iBank2»,
утвержденному Приказом от
31.08.2012 № 265

СЕРТИФИКАТ ОТКРЫТОГО КЛЮЧА ЭЦП СОТРУДНИКА КЛИЕНТА В СИСТЕМЕ «Internet-Банкинг» ОАО КБ «АГРОПРОМКРЕДИТ»

1. Наименование организации_____
_____
2. Юридический адрес_____
_____
3. ОГРН_____ дата регистрации «____»_____ года
4. Тел. _____ 5. ИНН _____ 6. КПП _____
7. Факс _____ 8. E-mail _____
9. Сведения о владельце ключа
Фамилия, имя, отчество_____
Должность_____
Удостоверение личности_____, серия _____
номер _____, дата выдачи « ___» _____ года,
кем выдан_____
_____
11. Примечания _____
**необязательно для заполнения*

Открытый ключ ЭЦП сотрудника клиента

Идентификатор ключа _____
Наименование криптосредств_____ Алгоритм_____
Дата начала действия «___»_____20__г. (заполняется Банком)
Дата окончания действия «___»_____20__г. (заполняется Банком)
Представление открытого ключа ЭЦП в шестнадцатеричном виде
_____
_____
_____
_____
_____
_____

Личная подпись владельца ключа ЭЦП

Сертификат открытого ключа ЭЦП клиента действует в рамках договора на обслуживание в системе «iBank 2» N___ от «__»_____20__ г.

Группа подписи _____

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
Открытого ключа ЭЦП
«__»_____20__ г.

Администратор безопасности системы

_____/_____/
подпись Ф.И.О.

Дата регистрации сертификата
Открытого ключа ЭЦП
«__»_____20__ г.

Банк _____ Клиент_____

АГРОПРОМКРЕДИТ
коммерческий банк

Приложение №5
к Договору на обслуживание
в Системе «iBank2»,
утвержденному Приказом от
31.08.2012 № 265

ОСНОВНЫЕ
требования для организации Рабочего места «iBank2» Клиента:

1. Отдельная Рабочая станция «iBank2» для проведения платежных операций - любой современный компьютер с любой операционной системой с Web-браузером и виртуальной Java-машиной версия не ниже JRE 1.1.4.

Минимальные системные требования:

- процессор: Intel Pentium 166 MHz;
- оперативная память: 64 Mb;
- любая операционная система, в которой можно установить Java-машину;
- наличие USB-порта.

2. Выход в Интернет со скоростью обмена данных не ниже 56 Кбит/сек и возможностью использования для обмена порт 443.
3. Лицензионные и регулярно обновляемые программные продукты:
   - операционная система;
   - антивирусный пакет.
4. Внешний носитель ключевой информации для хранения ЭП («USB- токен»).
5. Сеансовый ключ для дополнительной идентификации Клиента («OTP-токен»).
6. Ограниченный и контролируемый доступ только официально зарегистрированных лиц к Рабочей станции «iBank2» и к внешнему носителю ключевой информации.
7. Действующая защита внешнего периметра и ресурсов вычислительной сети.
8. Ограничение использования электронной почты, Интернет-ресурсов, систем мгновенного обмена сообщениями, не связанных с работой Системы «iBank2».
9. Парольная защита при загрузке операционной системы (ОС) и доступе к «Базовой системе ввода-вывода» («BIOS»).

Таким образом, в целях обеспечения безопасного функционирования Системы «iBank2» и снижения возможных рисков при осуществлении расчетов в Системе «iBank2» Клиент должен соблюдать следующие требования безопасности:

Организационные меры:

1. Выделить для установки Системы «iBank2» отдельную Рабочую станцию, изолированную от сети организации (в случае наличия нескольких электронных подписей (ЭП) использовать соответствующее количество Рабочих станций).
2. Исключить бесконтрольный доступ в помещение, в котором установлена Рабочая станция Системы «iBank2».
3. Исключить доступ к Рабочей станции Системы «iBank2» лиц, не являющихся администраторами системы и/или владельцами секретных ключей.
4. Носители, содержащие ключи ЭП, должны храниться вне зоны доступа посторонних лиц.
5. Подключение внешних носителей, содержащих секретные ключи («USB-токен» и т.п.), должно осуществляться только на период проведения платежных операций.
6. В случае бездействия Рабочей станции «iBank2» доступ в Систему должен быть заблокирован хранителем экрана, или Рабочая станция должна быть выключена.
7. В случае обнаружения подозрительных сообщений или сбоя в Системе (потеря GSM-связи, DDoS-атака и т.п.) необходимо незамедлительно связаться с Банком, заблокировать ключи доступа, прекратить совершение платежных операций.

Технические и аппаратно-программные меры:

Организация внешнего периметра защиты вычислительной сети и ресурсов:

1. Настройки Системы «iBank2» должны быть строго фиксированы (все порты и сервисы, не участвующие в рабочих процессах Системы «iBank2», запрещены (отключены)).
2. Внешний доступ к внутренним ресурсам Системы «iBank2» должен быть ограничен/минимизирован (например, через «VPN-тоннель») или запрещен.
3. Несанкционированное подключение сторонних компьютеров к внутренней локальной вычислительной сети («ноутбук», устройство мобильной связи и т.п.) должно быть запрещено.
4. Фильтрация трафика должна быть установлена на уровне внешних и персональных «межсетевых экранов» («FireWall»).
5. Настройка внешнего и персонального «межсетевых экранов» Рабочей станции «iBank2», должно быть только с адресом сервера Системы «iBank2».

Организация защиты Рабочей станции Системы «iBank2»:

1. На Рабочей станции «iBank2», разрешено использовать только лицензионное прикладное ПО (ОС, антивирус и пр.) с получением постоянных требуемых обновлений.
2. Набор программных продуктов должен быть минимален, а сервисы доступа и подключения внешних устройств хранения/записи информации - минимизированы.
3. Необходим постоянный контроль за корректностью работы Рабочей станции Системы «iBank2». Присутствие вредоносного кода может проявляться наличием различных аномалий в работе (нестандартная загрузка операционной системы или программных приложений, увеличение периода отклика файла с ключами и т.п.).
4. Защита «BIOS» и загрузчика ОС должна исключать: доступ неавторизованного пользователя; получение доступа к ресурсам; загрузку «без пароля»; загрузку в монопольном режиме или режиме восстановления.
5. Необходимо исключить использование на Рабочей станции «iBank2» почтовых сервисов и систем мгновенного обмена сообщениями («ICQ», «Skype», «Mail Agent» и т.п.).
6. Необходимо исключить посещение с Рабочей станции Интернет-ресурсов, несвязанных с работой и взаимодействием Системы «iBank2».
7. Необходимо исключить удаленный доступ к Рабочей станции «iBank2» для дистанционного управления Системой «iBank2».
8. Необходимо исключить скачивание, активацию и использование программ/отдельных файлов из Интернета, в том числе полученных по системам электронной почты (за исключением файлов и пакетов обновлений лицензионного ПО).
9. Пользователи вычислительной сети не должны иметь прав «локального администратора».

Системные пароли должны формироваться с учетом следующих требований:

1. При создании паролей обязательно использовать метод двойной учетной записи («Администратор» использует «административную учетную запись» только для выполнения действий, требующих именно этих привилегий; «Пользователь» Системы «iBank2», использует «пользовательскую учетную запись» с минимизацией привилегий).
2. Пароли доступа формируются ответственными лицами организации самостоятельно, не записываются и не хранятся в открытом доступе.
3. Длина пароля должна быть: для «Пользователя» – не менее 8-ми символов; для «Администратора» – не менее 10-и символов.
4. В пароле обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, %, №, *, ^, & и т.п.).
5. Пароль не должен содержать: встроенные учетные записи; легко вычисляемые сочетания символов; имена; фамилии; наименования и т.п.; общепринятые сокращения («admin», «guest», «эвм», «user», «administrator» и т.п.).
6. При смене пароля новое значение должно отличаться от предыдущего не менее чем на пять символов.
7. Пароль подлежит обязательной смене при кадровых изменениях ответственных сотрудников («пользователь» / «администратор»).

Антивирусная защита:

1. Антивирусной защите подлежат все элементы вычислительной сети организации.
2. При работе с Системой «iBank2» должен использоваться лицензионный пакет из антивируса и антиспама, постоянно получающий обновления сигнатур.
3. Целесообразно использование эшелонированной антивирусной защиты различными антивирусными пакетами.

Приложение №6
к Договору на обслуживание
в системе «iBank2»,
утвержденному Приказом от
31.08.2012 № 265

Доверенность № _____

г. _____ _____
(место выдачи) (дата выдачи)

_____ (далее именуемый Клиент)
(полное наименование организации)

в лице _____,
(должность, фамилия, имя, отчество)

действующего на основании _____, уполномочивает _____

_____ _____
(должность, фамилия, имя, отчество полномочного представителя)

- *паспортные данные: серия, номер, орган, выдавший паспорт, дата выдачи;*
- *телефон для связи,*
- *E-Mail,*

на выполнение следующих действий от имени Клиента[1]:

- передать в ОАО КБ «АГРОПРОМКРЕДИТ» подписанный _____ Договор № ____ на обслуживание по электронной системе “iBank2” от «___»_____20__г. (далее – Договор)
- передать в ОАО КБ «АГРОПРОМКРЕДИТ» Сертификат открытого ключа ЭП КЛИЕНТА № _____, подписанный Владельцем ЭП _____ к Договору.

Настоящая доверенность действительна до «___» _____ 20__ г. (включительно)

Подпись (фамилия, инициалы) _____ удостоверяю.
(личная подпись)

Руководитель организации _____ (инициалы, фамилия)
(личная подпись)

М.П.

[1] Могут указываться иные полномочия передаваемые Доверенному лицу